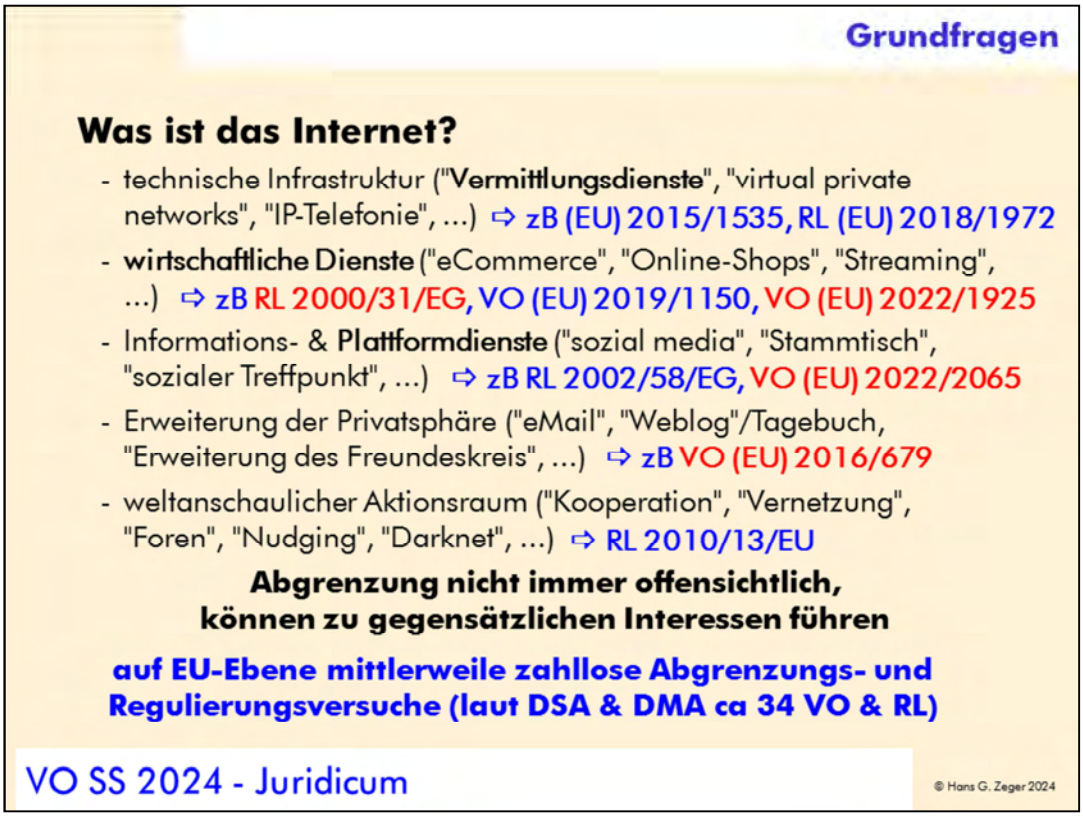
Download Vorlesungsunterlagen:
http://www.argedaten.at/static/vo-ds-internet.pdf

Dr. Hans G. Zeger
A-1160 Wien, Redtenbachergasse 20

Mail persönlich: hans@zeger.at

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. ..."

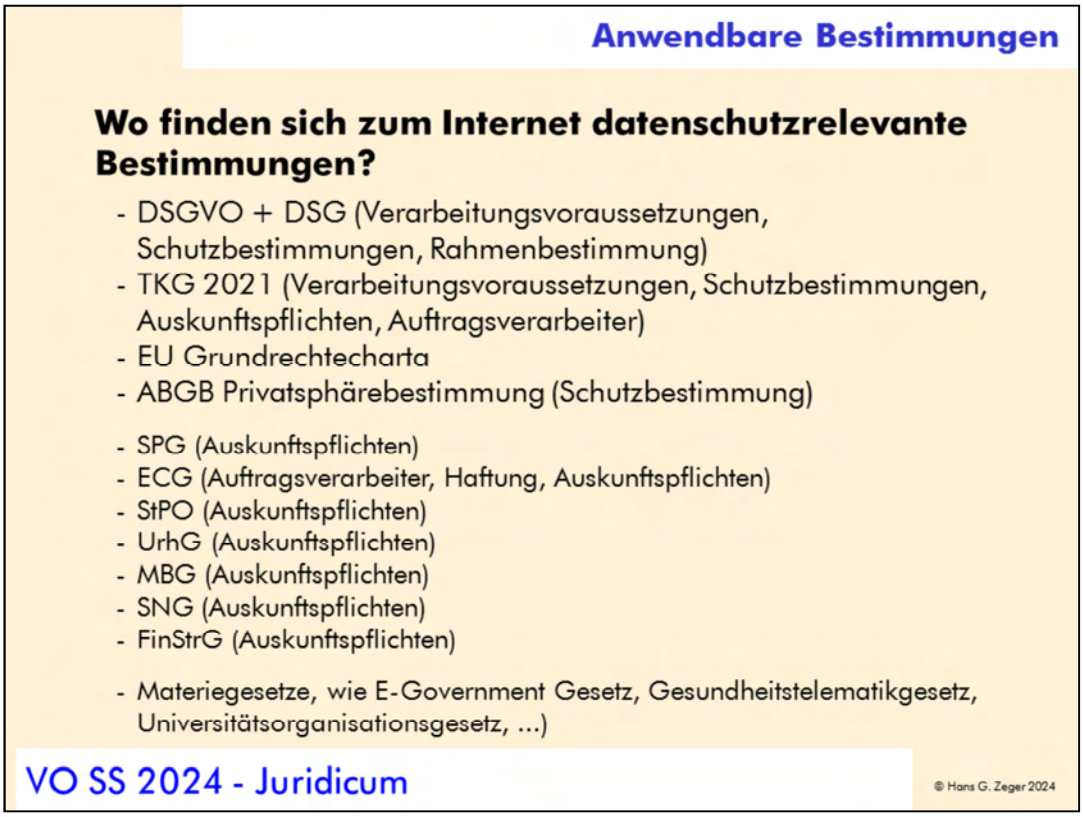


Auswahl an EU-Rechtsvorschriften

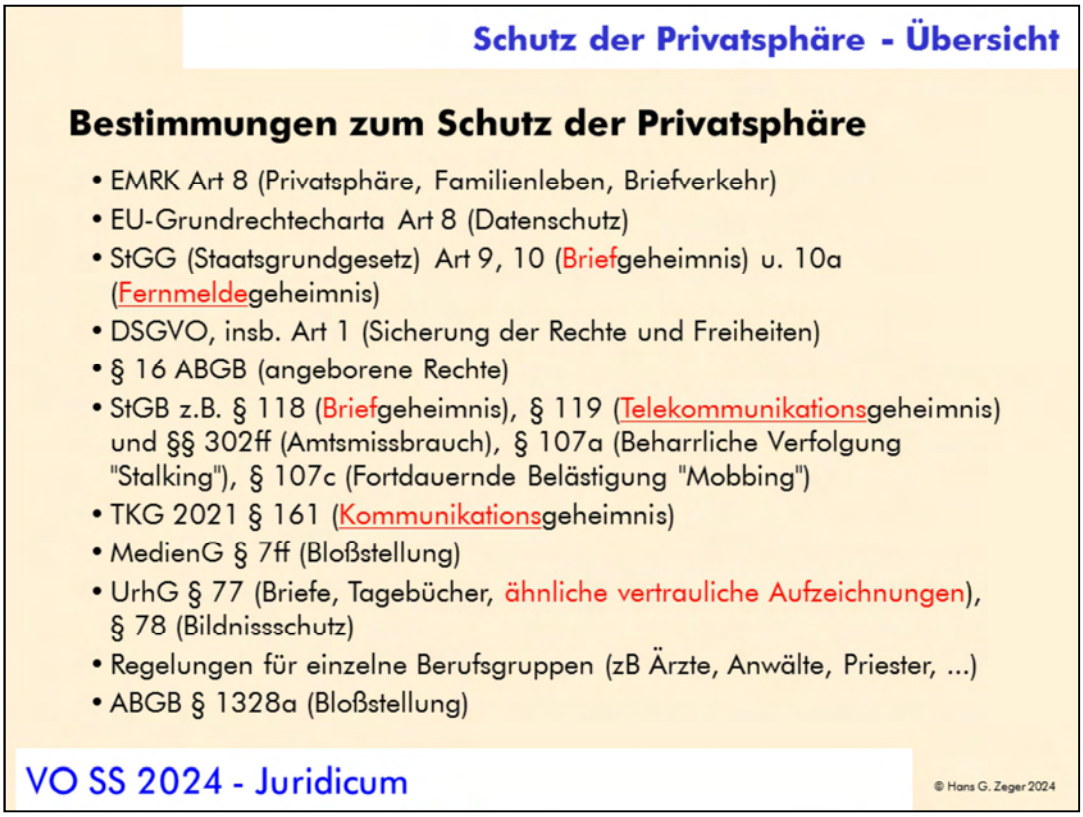
- **Richtlinie 2000/31/EG** des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") (ABl. L 178 vom 17.7.2000, S. 1). **["e-commerce"]**
- **Richtlinie 2002/58/EG** des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37). **["ePrivacy"]**
- **Richtlinie 2010/13/EU** des Europäischen Parlaments und des Rates vom 10. März 2010 zur Koordinierung bestimmter Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Bereitstellung audiovisueller Mediendienste (Richtlinie über audiovisuelle Mediendienste) (ABl. L 95 vom 15.4.2010, S. 1).
- **Richtlinie (EU) 2015/1535** des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).
- **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) (ABl. L 119 vom 4.5.2016, S. 1). **["DSGVO"]**
- **Richtlinie (EU) 2018/1972** des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36).
- **Verordnung (EU) 2019/1150** des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57).
- **Verordnung (EU) 2022/1925** des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (ABl. L 265 vom 12.10.2022, S. 1) **["DMA"]**
- **Verordnung (EU) 2022/2065** des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur **Änderung der Richtlinie 2000/31/EG** (Gesetz über digitale Dienste) **["DSA"]**


Anwendungsfälle Datenschutz
Welche (Internet-)Situationen sind datenschutzrelevant?
- Nutzung von Informationsdiensten ("Online-Services"): personalisiert vs. "anonym" und/oder kostenpflichtig vs. "gratis"
- Bestellungen im Internet ("eCommerce", Online-Shop): identifiziert
- elektronische Amtswege, öffentliche Verwaltung, Vorschreibungen ("eGovernment"): identifiziert
- Meinungsäußerung / Selbstdarstellung ("Social Media"): personalisiert vs. "anonym"
- Veröffentlichung persönlicher Daten durch Dritte ("Mediendienste"): Meinungsfreiheit vs. Privatsphäre
- Internet als Infrastruktur (virtuelle Unternehmensnetze / VPN, Intranet, Cloud Service, ...): Sicherheit vs. Privatsphäre
- Verträge im Zusammenhang mit Internet (z.B Vertraulichkeit von eMails, Nutzung Kundendaten, ...): Erwerbsfreiheit vs. Privatsphäre
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Anwendbare Bestimmungen
Wo finden sich zum Internet datenschutzrelevante Bestimmungen?
- DSGVO + DSG (Verarbeitungsvoraussetzungen, Schutzbestimmungen, Rahmenbestimmung)
- TKG 2021 (Verarbeitungsvoraussetzungen, Schutzbestimmungen, Auskunftspflichten, Auftragsverarbeiter)
- EU Grundrechtecharta
- ABGB Privatsphärebestimmung (Schutzbestimmung)
- SPG (Auskunftspflichten)
- ECG (Auftragsverarbeiter, Haftung, Auskunftspflichten)
- StPO (Auskunftspflichten)
- UrhG (Auskunftspflichten)
- MBG (Auskunftspflichten)
- SNG (Auskunftspflichten)
- FinStrG (Auskunftspflichten)
- Materiegesetze, wie E-Government Gesetz, Gesundheitstelematikgesetz, Universitätsorganisationsgesetz, ...)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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.

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 2021 – Kommunikationsgeheimnis

§ 161. (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 oder Anbieter eines öffentlichen Kommunikationsnetzes oder -dienstes und alle Personen, die an der Tätigkeit des Betreibers oder Anbieters 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 und Abwicklung von Notrufen und die Fälle der Fangschaltung, der Überwachung von Nachrichten nach § 135 Abs. 3 StPO, der Auskunft über Daten einer Nachrichtenübermittlung nach § 135 Abs. 2 StPO, der Auskunft über Daten nach § 99 Abs. 3a des Bundesgesetzes vom 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (FinStrG), BGBl. Nr. 129/1958 idF BGBl. Nr. 21/1959 (DFB), der Auskunft über Daten nach § 11 Abs. 1 Z 7 des Bundesgesetzes über die Organisation, Aufgaben und Befugnisse des Verfassungsschutzes (SNG), BGBl. I Nr. 5/2016, und der Auskunft über Daten nach § 22 Abs. 2a und 2b des Militärbefugnisgesetzes (MBG), BGBl. I Nr. 86/2001, sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

(4) Werden mittels einer Funkanlage, einer Endeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Endeinrichtung 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. […]

ABGB 1b. am Recht auf Wahrung der Privatsphäre

§ 1328a. (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.

(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 bei Dazwischentreten eines medienrechtlich Verantwortlichen allein nach den Bestimmungen des Mediengesetzes,

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

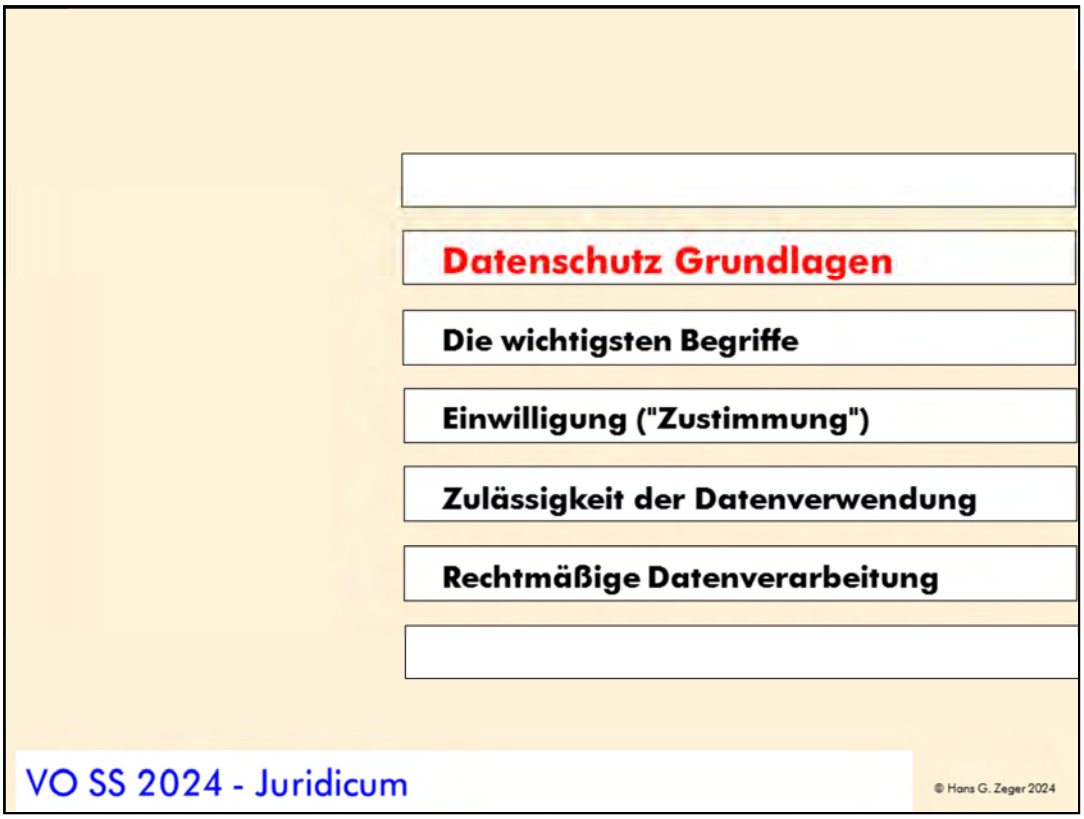
§ 118. (1) Wer einen nicht zu seiner Kenntnisnahme bestimmten verschlossenen Brief oder ein anderes solches Schriftstück öffnet, ist mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.
(2) Ebenso ist zu bestrafen, wer, um sich oder einem anderen Unbefugten 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-

EU Datenschutz-Grundverordnung

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

ergänzende Rechtsakte (AT)

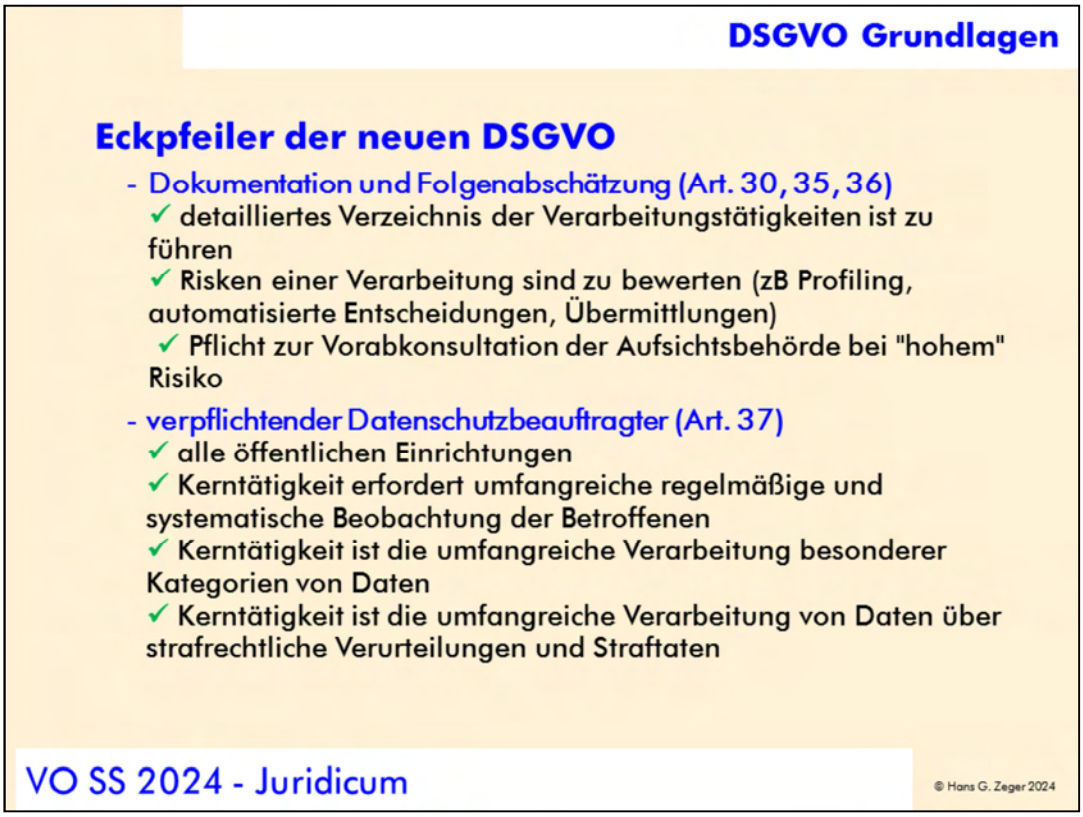
- Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) - BGBl. II Nr. 108/2018
- Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) StF: BGBl. II Nr. 278/2018
- Zertifizierungsstellen-Akkreditierungs-Verordnung - ZeStAkk-V - BGBl. II Nr. 79/2021


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 Anwendung der EU-Grundverordnung Datenschutz (DSGVO) EU-weit + DSG in Österreich
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

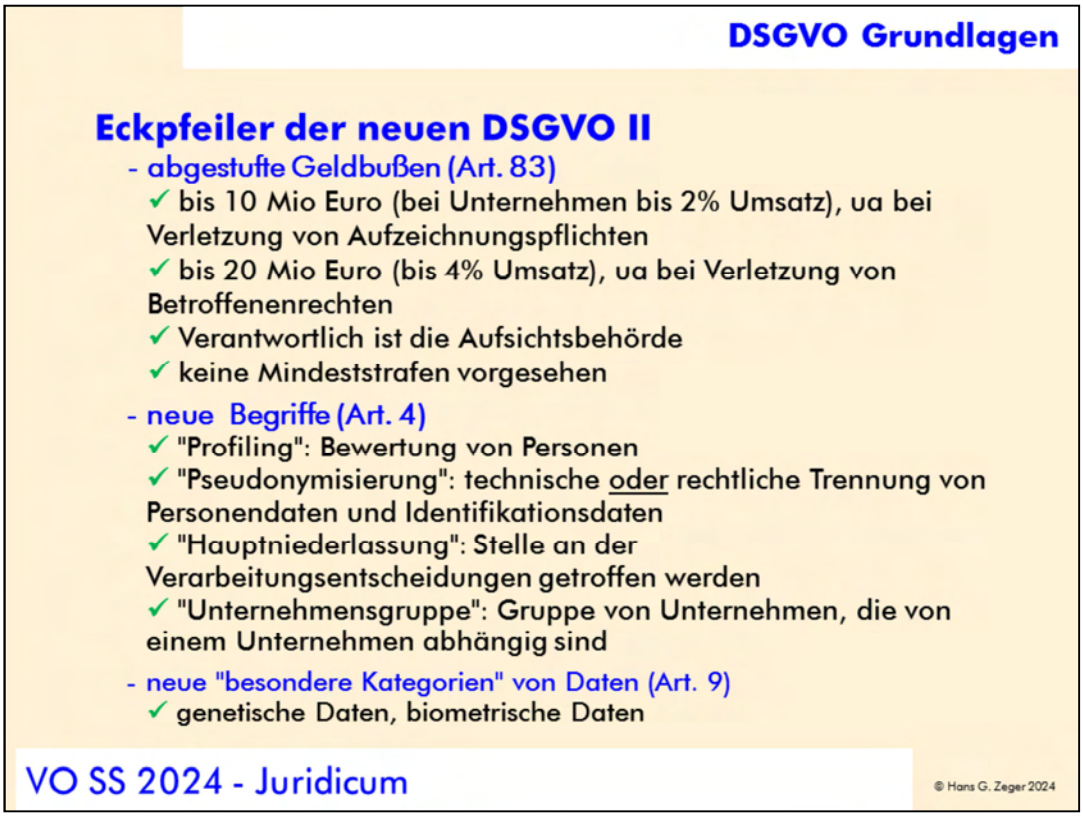
-


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 27 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 (oft auch "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 SS 2024 - Juridicum
© Hans G. Zeger 2024

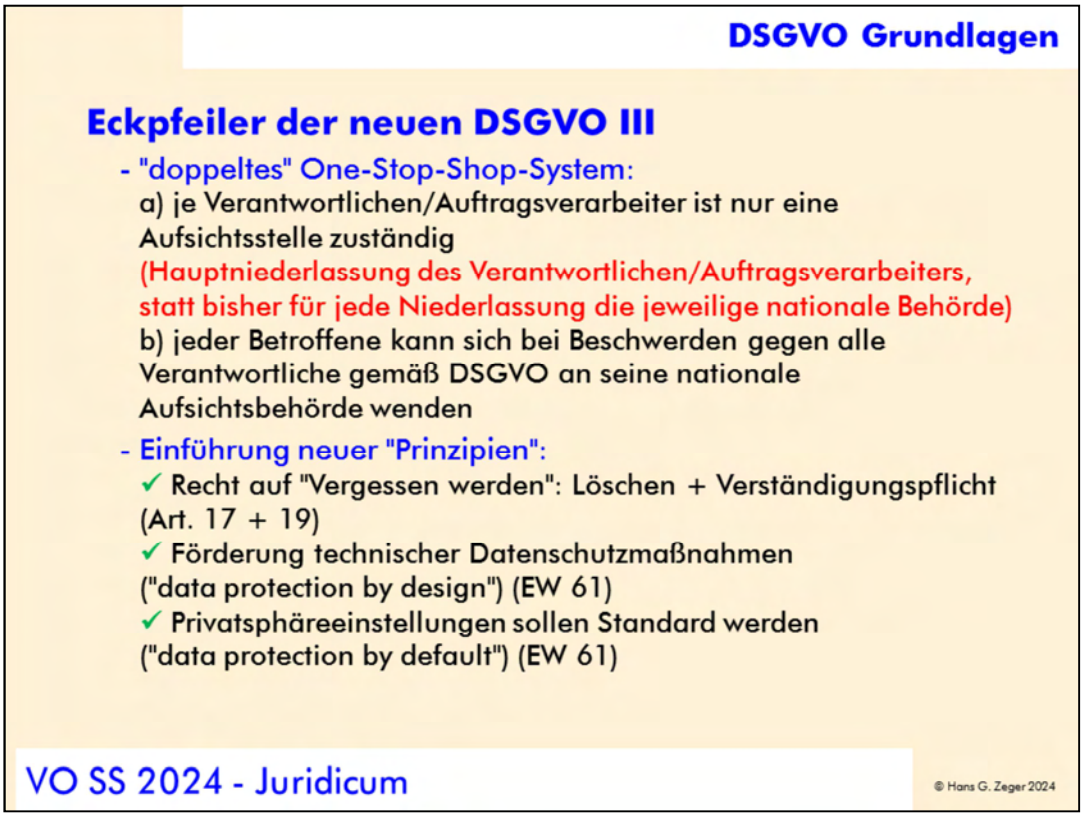
-


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 SS 2024 - Juridicum
© Hans G. Zeger 2024

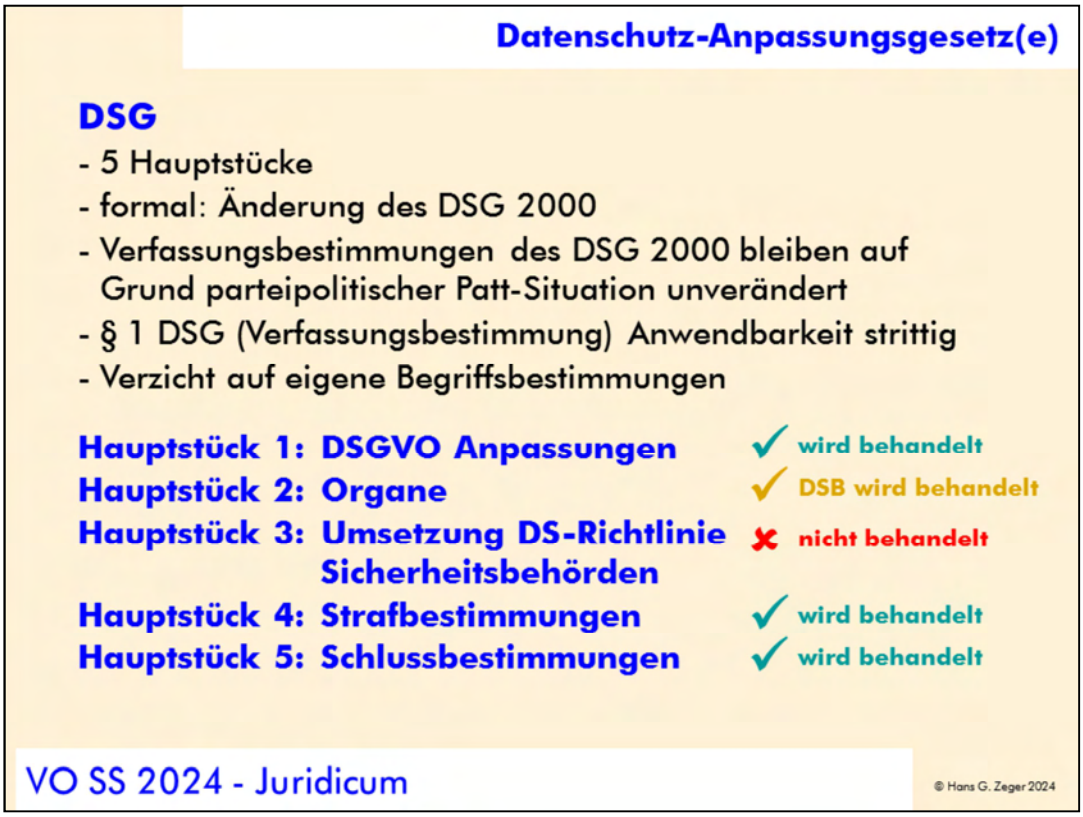
-


DSGVO Grundlagen
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
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


DSGVO Grundlagen
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 "Vergessen werden": Löschen + Verständigungspflicht (Art. 17 + 19)
✓ Förderung technischer Datenschutzmaßnahmen ("data protection by design") (EW 61)
✓ Privatsphäreeinstellungen sollen Standard werden ("data protection by default") (EW 61)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



DSG § 1

(1) **Jedermann** hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, **Anspruch auf Geheimhaltung** der ihn betreffenden personenbezogenen Daten, **soweit ein schutzwürdiges Interesse** daran besteht. Das Bestehen eines solchen Interesses ist **ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit** oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

...

(3)Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, **nach Maßgabe gesetzlicher Bestimmungen**

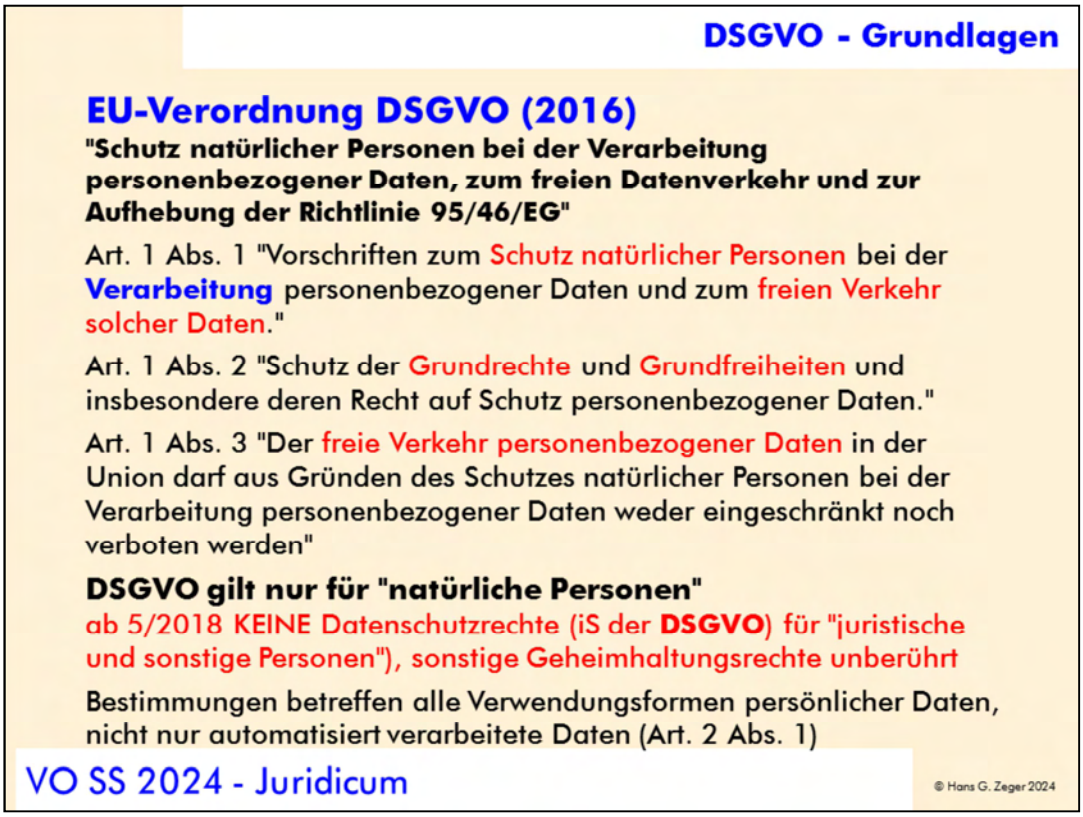
1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

...

aus Kommentar Feiler/Foró EU-DSGVO und DSG 2. Auflage 2022

- Existenzberechtigung des §1 DSG fraglich, ua
- EU-Umsetzungsverbot: Normen einer EU-Verordnung dürfen nicht wort- bzw. sinngleich national wiederholt werden
- genereller Ausschluss des Schutzinteresses bei öffentlich verfügbaren Daten ist EU-widrig
- Schutz als "Jedermannsrecht" (also auch juristische Personen) und erlaubt juristischen Personen eine Aktivlegitimation hinsichtlich Verletzungen nach § 1 DSG (siehe auch *DSB 2020-0.191.240 vom 25.5.2020*), nicht jedoch nach DSGVO, Anwendbarkeit jedoch nur bei rein innerstaatlichen Fällen gegeben
- §1 umfasst alle Arten von Daten und nicht bloß automationsunterstützte bzw. in einem Dateisystem verarbeitet Date - weicht damit in seiner Systematik von DSGVO ab
- Schutz des § 1 ist nur auf Geheimhaltung abgestellt, während DSGVO jede Form der Datenverwendung regelt
- die in Abs 3 gennanten Rechte nach " **nach Maßgabe gesetzlicher Bestimmungen** " sind mangels gesetzlicher Bestimmungen nicht durchsetzbar



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)

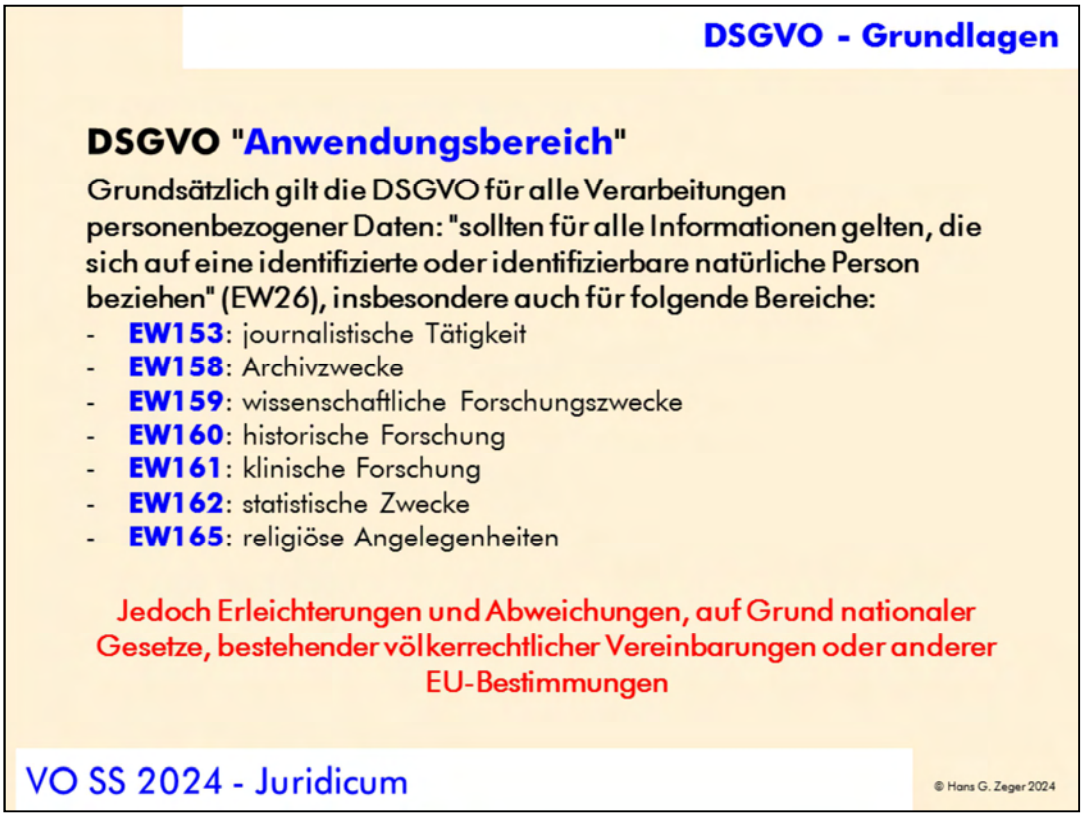
Die Richtlinie soll gleichermaßen den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten sichern

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.

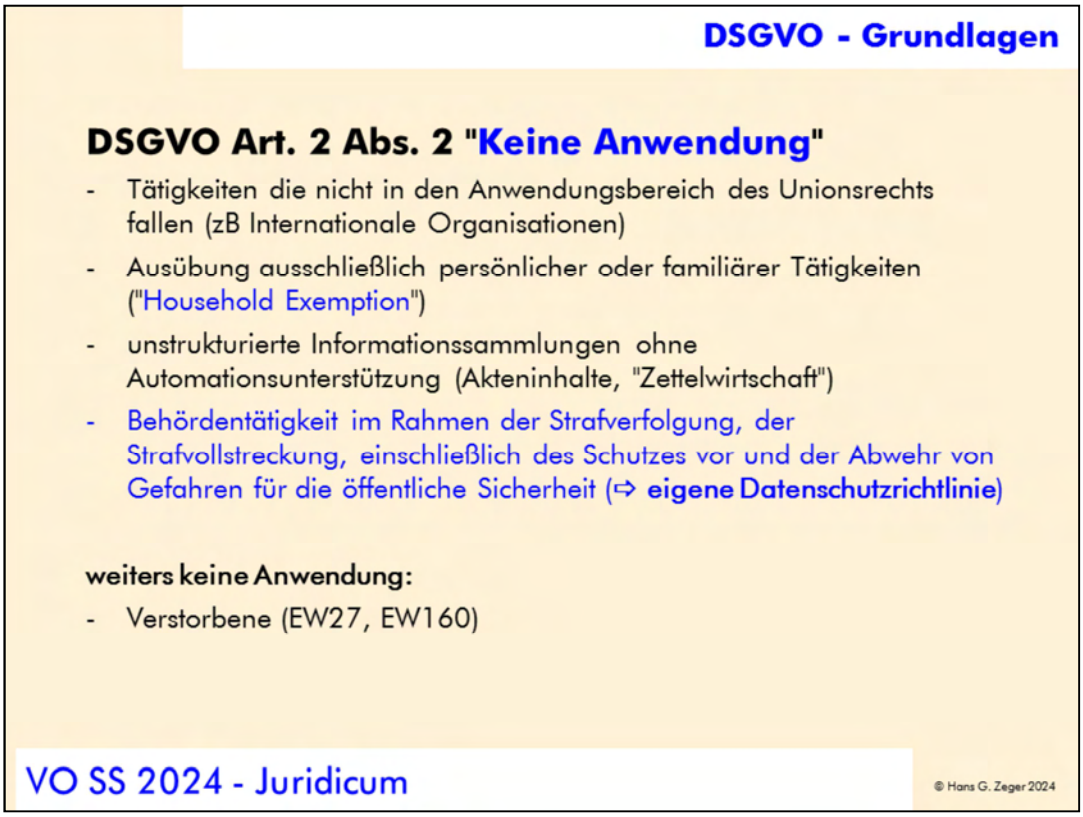
(2)Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(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 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 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,

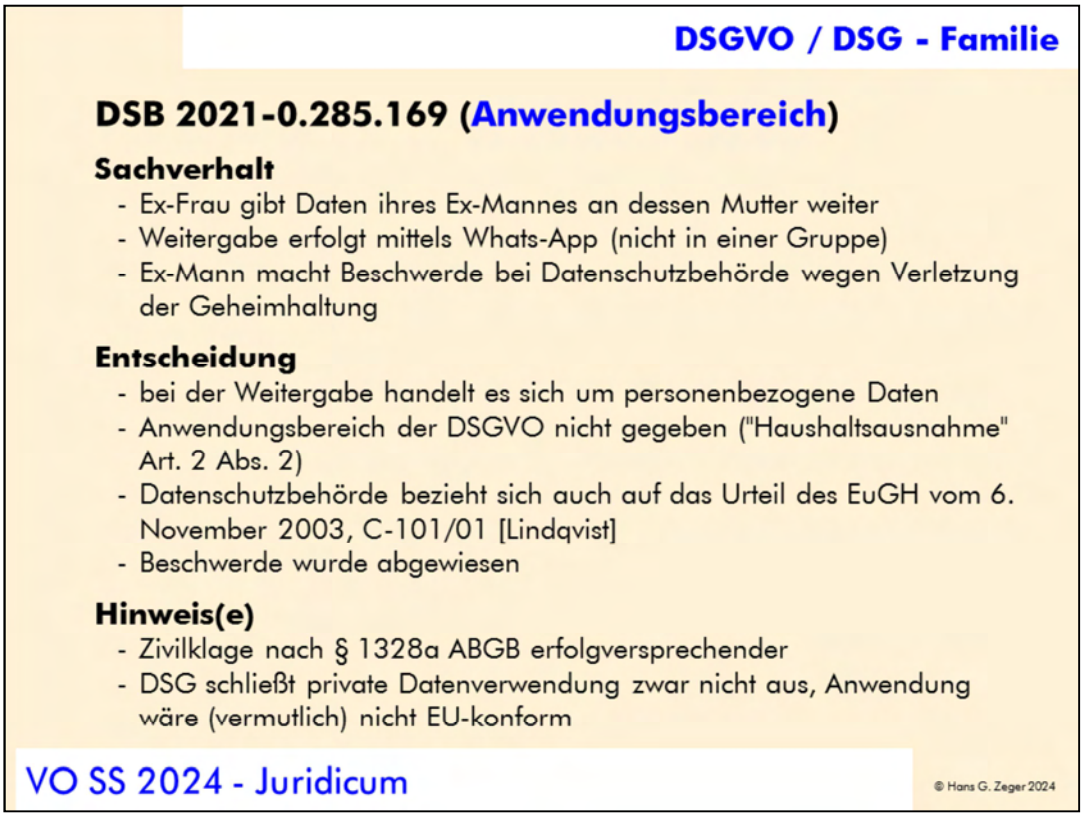
d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

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.



aus DSB 2021-0.285.169

D.3. Zur (Nicht-)Anwendbarkeit der DSGVO und zur sog. „Haushaltsausnahme"

...

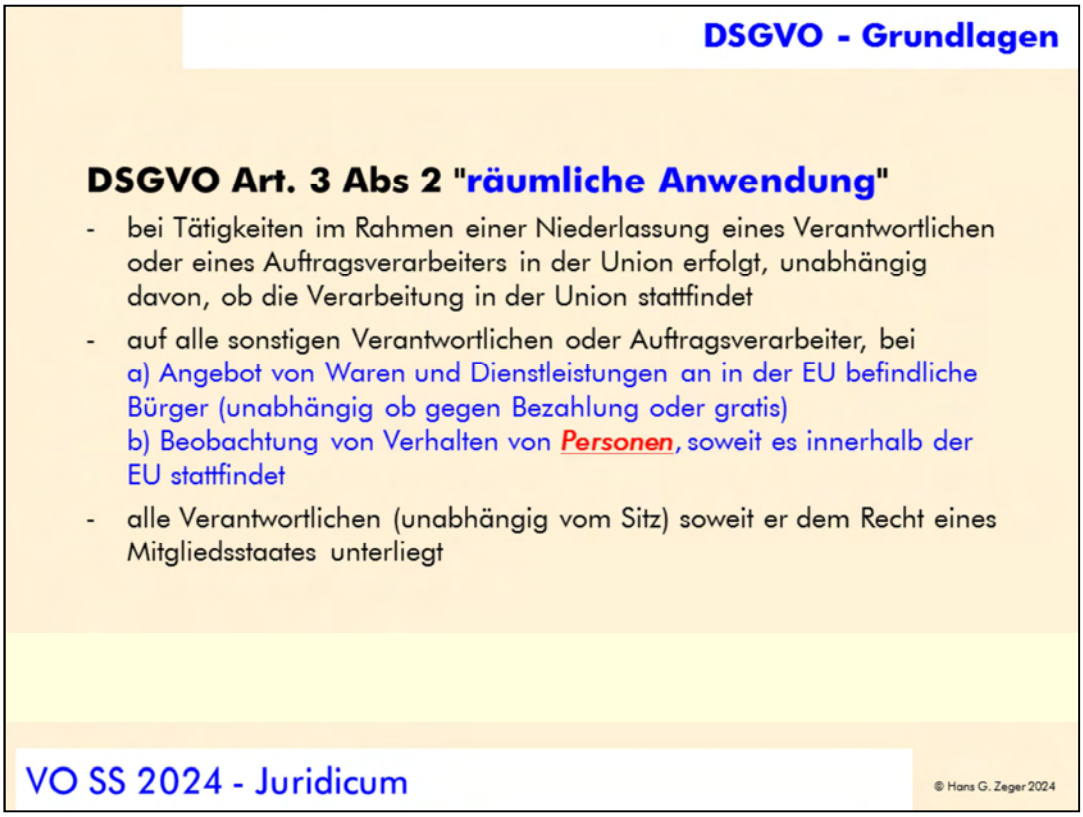
Die Normierung der „Haushaltsausnahme" stellt eine Abwägungsentscheidung des Unionsgesetzgebers in Bezug auf das in Art. 8 EU-GRC primärrechtlich festgelegte Recht auf Schutz personenbezogener Daten dar. Gemäß Art. 52 Abs. 1 EU-GRC müssen Einschränkungen der durch sie gewährleisteten Rechte und Freiheiten müssen daher entsprechend gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten.

Nach herrschender Auffassung ist diese Ausnahme folglich restriktiv auszulegen (vgl. zur weitestgehend inhaltsgleichen Bestimmung des Art. 3 Abs. 2 zweiter Spiegelstrich der Richtlinie 95/46/EG das **Urteil des EuGH vom 6. November 2003, C-101/01 [Lindqvist]**).

Als Abgrenzungskriterium gilt das Fehlen jeglichen Bezugs zu einer beruflichen oder wirtschaftlichen Tätigkeit. D.h. das zentrale Kriterium für die Anwendbarkeit der „Haushaltsausnahme" – und damit für die Nichtanwendbarkeit der DSGVO – ist die Zurechenbarkeit der Datenverarbeitung zum privaten Bereich (vgl. Heißl in Knyrim [Hrsg.], DatKomm Art. 2 DSGVO, Rz. 70).

Hierbei gilt es zu beachten, dass sich die Ausdrücke „**persönlich**" und „**familiär**" auf die **Tätigkeit der Person**, die personenbezogene Daten verarbeitet, und nicht auf die Person, deren Daten verarbeitet werden, beziehen. (vgl. das Urteil des EuGH vom 10. Juli 2018, C-25/17 [Jehovan todistajat], Rz. 41 mwN.).

Die DSGVO selbst nennt diesbezüglich etwa das Führen eines Schriftverkehrs oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen einer persönlichen oder familiären Tätigkeit (vgl. ErwGr. 18 DSGVO). Dies gilt allerdings nur insoweit, als Daten in geschlossenen Gruppen ausgetauscht werden, die keinen Bezug zu beruflichen oder wirtschaftlichen Tätigkeiten der Nutzer haben (vgl. Ennöckl in Sydow [Hrsg.], Europäische Datenschutzgrundverordnung. Handkommentar, Art. 2, Rz. 13; vgl. auch das zuvor zitierte Urteil des EuGH vom 10. Juli 2018, C-25/17, Rz. 42 mwN., wonach eine Tätigkeit dann **„nicht als ausschließlich persönlich oder familiär im Sinne dieser Vorschrift angesehen werden [kann], wenn sie zum Gegenstand hat, personenbezogene Daten einer unbegrenzten Zahl von Personen zugänglich zu machen, oder wenn sie sich auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten verarbeitet")**. Die ausschließlich private Nutzung von Diensten wie WhatsApp wird, sofern damit keine uneingeschränkte Veröffentlichung personenbezogener Daten im Internet einhergeht, vom Anwendungsbereich der „Haushaltsausnahme" erfasst (vgl. Bergauer in Jahnel [Hrsg.], DSGVO. Kommentar, Art. 2, Rz. 27).

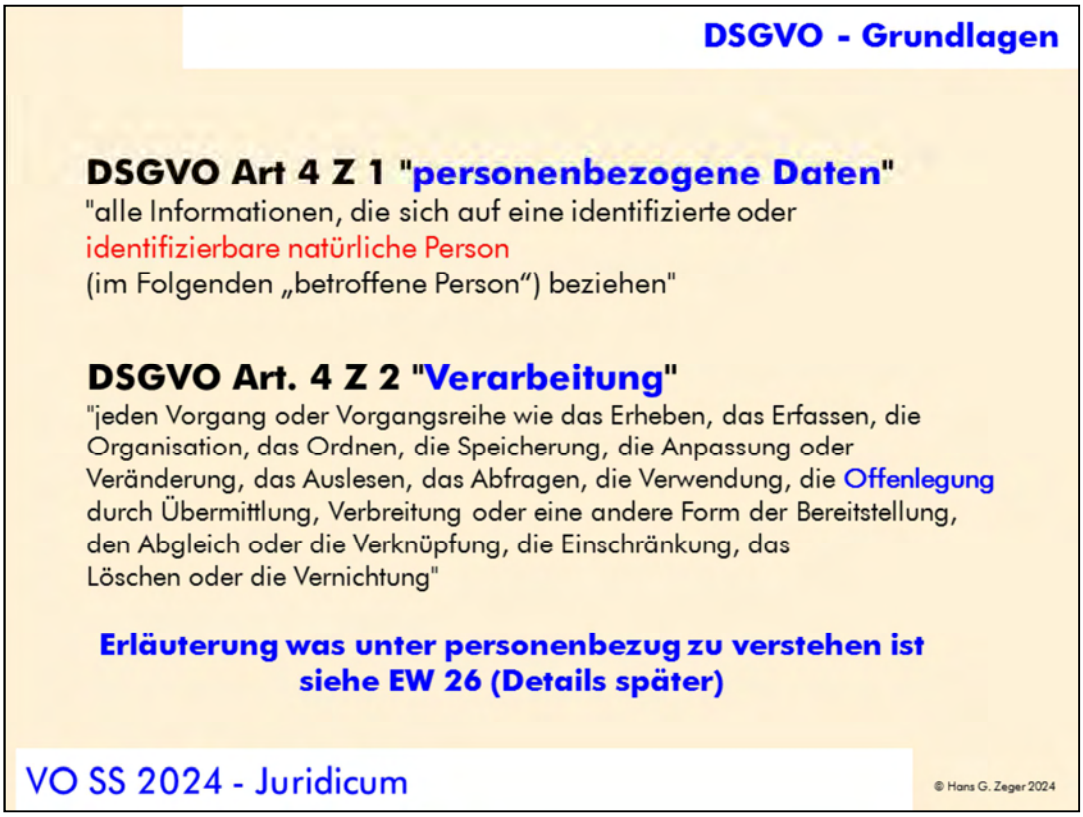


DSGVO Art. 3 Räumlicher Anwendungsbereich

(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.



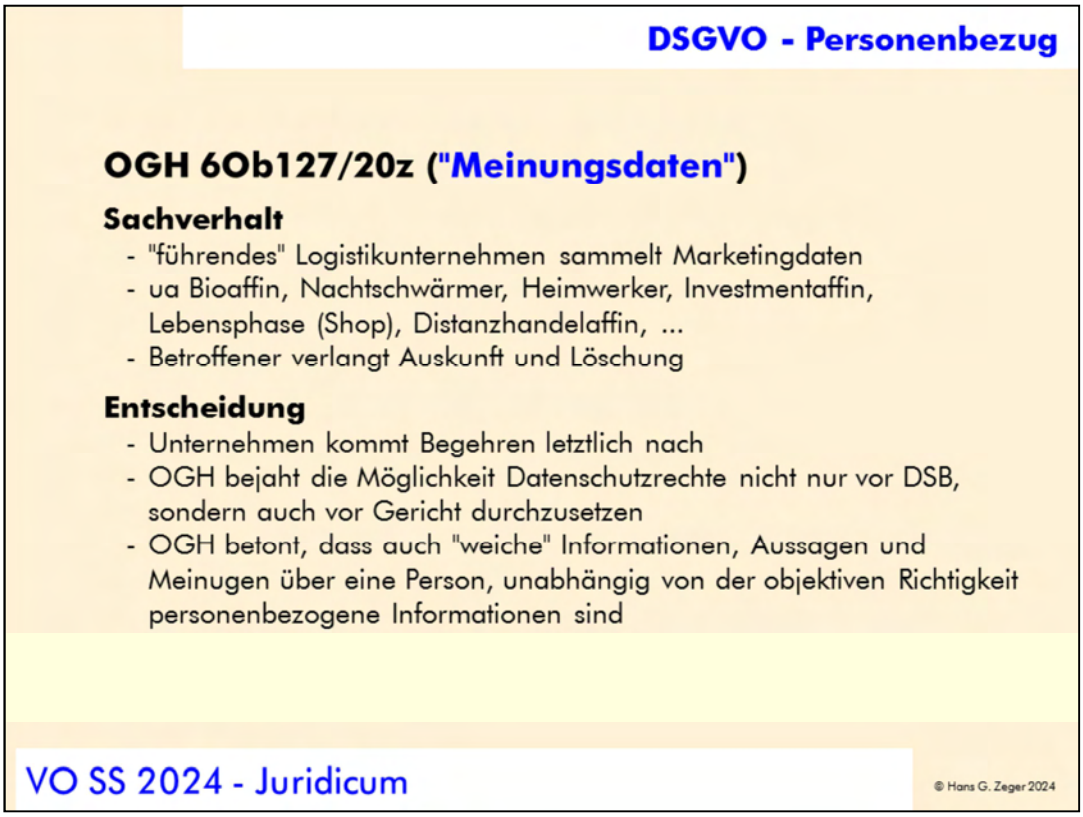
DSGVO Art. 4 Begriffsbestimmungen

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 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.



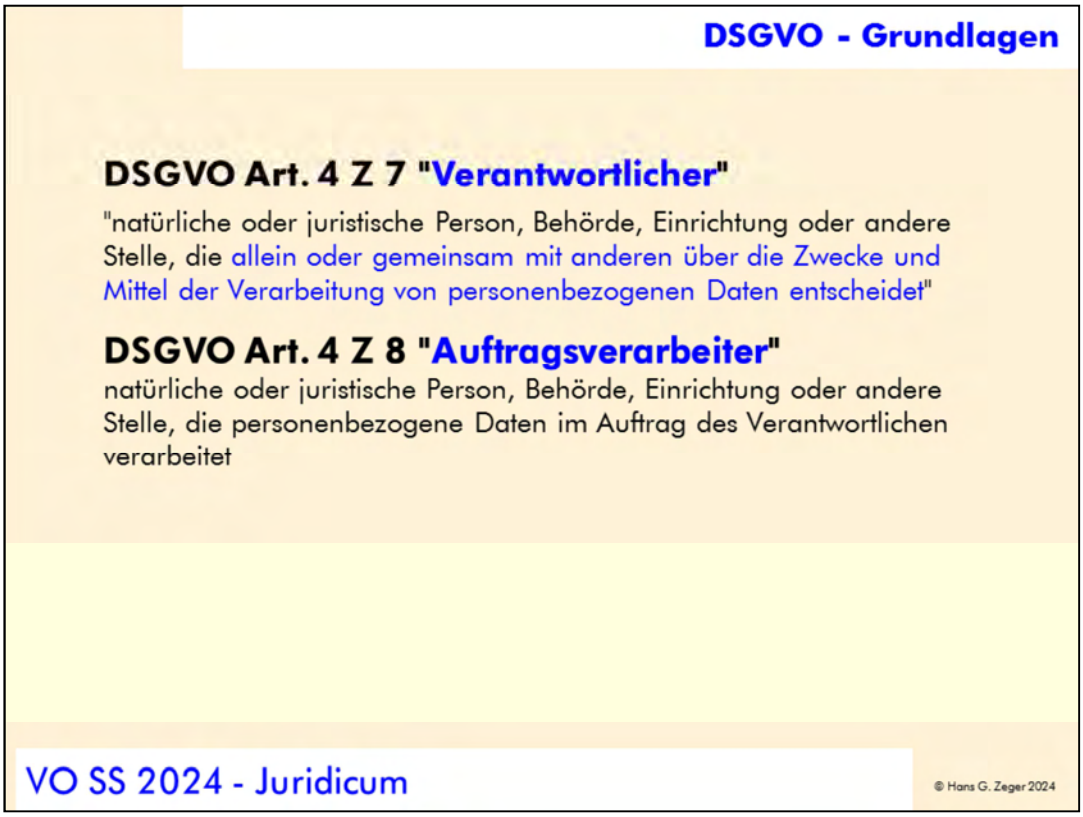
OGH 6Ob127/20z

[2] Über Aufforderung des Klägers, eines Rechtsanwalts, vom 14. 1. 2019 erteilte ihm die Beklagte mit Schreiben vom 14. 2. 2019 Auskunft über die in Bezug auf seine Person verarbeiteten, personenbezogenen Daten. Demnach seien über den Kläger folgende Daten gespeichert: Telefonnummer, Akademiker, Bioaffin, Nachtschwärmer, Heimwerker, Investmentaffin, Lebensphase (Shop), Distanzhandelaffin, Paketfrequenz, Paketrecency; Anzahl der Pakete pro Jahr; Anzahl der Wochen/Jahr, in der man Pakete bekommt; Versandhandelskäufer; Anzahl der Pakete im Zeitraum vor 6 bis 12 Monaten. Die in diesem Auskunftsschreiben angeführten Marketingdaten über den Kläger waren von der Beklagten auf der Rechtsgrundlage der Gewerbeberechtigung der Beklagten erhoben worden. Die genannten Affinitäten stell(t)en lediglich die Zuordnung einer bestimmten Person aufgrund der Zuschreibung bestimmter Marketing-Klassifikationen im Wege eines Marketing-Analyseverfahrens zu einer Marketinggruppe dar. Der eigentliche Aussagegehalt etwa des Attributs „Investmentaffin" war daher nicht, dass damit über eine bestimmte Person Daten über deren Finanzgebarung erhoben und bewertet würden, sondern lediglich, dass diese Person aufgrund bestimmter soziodemographischer Umstände (Alter, Wohnort, Bildungsgrad udgl) einer Marketinggruppe zugeordnet wurde, hinsichtlich der das Vorliegen des Attributs (investmentaffin) mit einer bestimmten Wahrscheinlichkeit angenommen worden sei.

...

[16] 2.1. Deshalb weisen auch innere Zustände wie Meinungen, Motive, Wünsche, Überzeugungen und Werturteile sowie statistische Wahrscheinlichkeitsaussagen, die nicht bloße Prognose- oder Planungswerte darstellen, sondern subjektive und/oder objektive Einschätzungen zu einer identifizierten oder identifizierbaren Person liefern, einen Personenbezug auf (Hödl aaO; Klar/Kühling in Kühling/Buchner, DS-GVO Art 4 Nr 1 Rz 10; ebenso persönliche Überzeugungen, Vorlieben, Verhaltensweisen oder Einstellungen nennend Ernst in Paal/Pauly, DSGVO-BDSG² Art 4 DSGVO Rz 14). Damit umfasst der Begriff der „Information" nicht nur Aussagen zu überprüfbaren Eigenschaften oder sachlichen Verhältnissen der betroffenen Person, sondern auch Einschätzungen und Urteile über sie, wie etwa „X ist ein zuverlässiger Mitarbeiter" (Klabunde in Ehmann/Selmayer, DS-GVO² Art 4 Rz 9; vgl auch Gola in Gola, DSGVO² Art 4 Rz 13). In diesem Sinne sind Daten mit Bezug zu einer Person auch dann personenbezogen, wenn sie unzutreffend sind (Reimer in Sydow, DSGVO² Art 4 Rz 41); der Wahrheitsgehalt ist für die Betrachtung unerheblich (Klabunde aaO). Wahrscheinlichkeitsangaben haben Personenbezug, gleich ob sie sich auf Sachverhalte in der Vergangenheit, Gegenwart oder Zukunft beziehen (Ernst aaO).

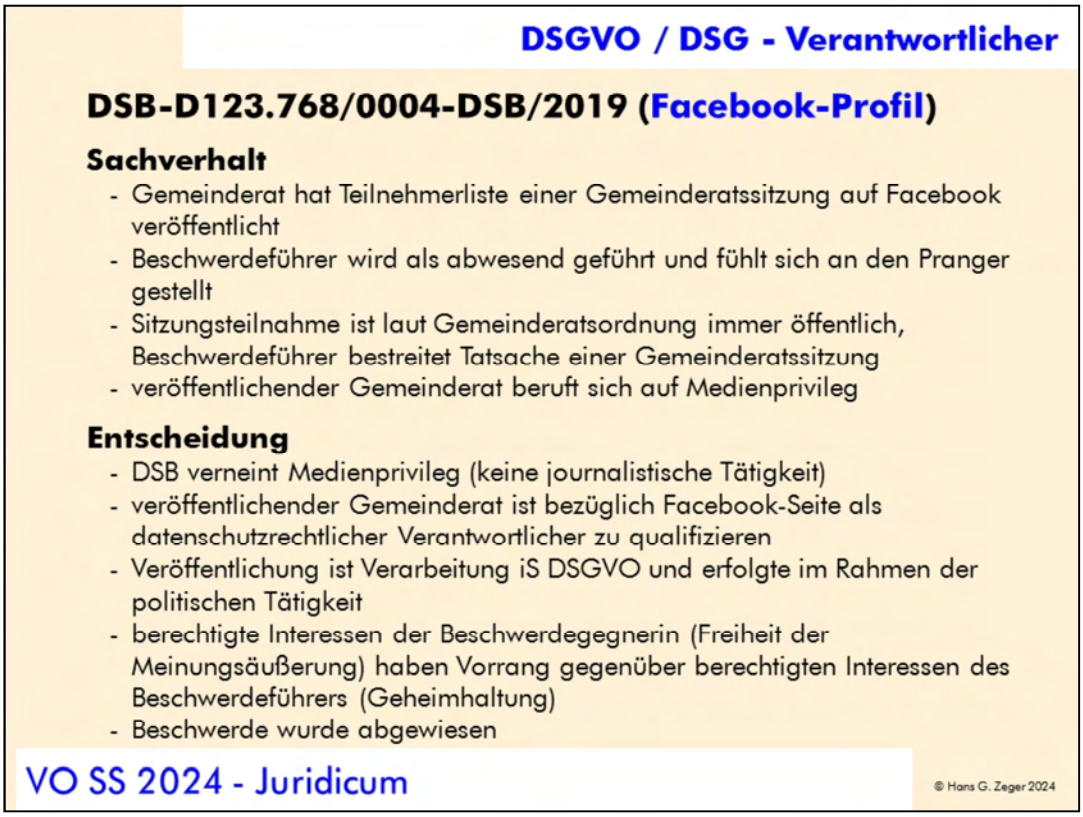
...



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;



aus DSB-D123.768/0004-DSB/2019

Zwar kann die Beschwerdegegnerin definitionsgemäß als Medieninhaberin im Sinne des § 1 Z 8 lit. c des Mediengesetzes – MedienG angesehen werden. Jedoch verlangt § 9 Abs. 1 DSG, dass die Verarbeitung von Daten „zu journalistischen Zwecken des Medienunternehmens oder Mediendienstes“ erfolgen muss.

Bei der Beschwerdegegnerin handelt es sich definitionsgemäß aber nicht um ein Medienunternehmen (§ 1 Z 6 MedienG) oder einen Mediendienst (§ 1 Z 7 MedienG).

Darüber hinaus kann im vorliegenden Fall aus nachstehenden Gründen auch nicht von einer „journalistischen Zwecken“ ausgegangen werden:

Es kann nämlich nicht davon ausgegangen werden, dass jegliche im Internet veröffentlichte Information, die sich auf personenbezogene Daten bezieht, unter den Begriff der „journalistischen Tätigkeiten“ fiele und daher für sie die in Art. 9 der Richtlinie 95/46 vorgesehenen Abweichungen und Ausnahmen gelten (siehe dazu EuGH 01.06.2017, C-345/17, Rz 58 [Sergejs Buivids und Datu valsts inspekcija]). Zwar bezieht sich die gegenständliche Rsp. auf die alte Rechtslage, jedoch ist Art. 9 der Richtlinie 95/46 als Pendantbestimmung zu Art. 85 DSGVO zu verstehen.

Selbst bei einer weiten Auslegung des Begriffes „Journalismus“ kann verfahrensgegenständlich keine Verarbeitung zu journalistischen Zwecken erkannt werden. Auch die Tatsache, dass die Facebook-Seite durch Medienmitarbeiter der N***-Partei betreut wird, vermag daran nichts ändern. Politische Parteien sind oft publizistisch tätig und mit Redaktionen und Mitarbeitern versehen, die oft ausschließlich im Rahmen der Öffentlichkeitsarbeit tätig sind. Ziel politischer Parteien ist aber nicht die inhaltliche Gestaltung des Mediums, sondern vielmehr durch politische Tätigkeit die staatliche Willensbildung umfassend – vor allem durch Öffentlichkeitsarbeit – zu beeinflussen. Die Medientätigkeit kann nur als eine „Nebenerscheinung“ im Zuge der angestrebten Erreichung dieser Ziele verstanden werden.

Da § 9 Abs. 1 DSG nicht zur Anwendung kommt, ist folglich eine Zuständigkeit der Datenschutzbehörde zur Behandlung der Beschwerde gegeben.

Gemäß Art. 4 Z 7 DSGVO ist „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.

Gegenständlich ist die Beschwerdegegnerin als Betreiberin eines öffentlich-zugänglichen Facebook-Profils als datenschutzrechtlicher Verantwortlicher nach Art. 4 Z 7 DSGVO zu qualifizieren, da sie über Zwecke (Teilen von Inhalten) und Mittel (Einsatz eines öffentlich-zugänglichen Facebook-Profils) entscheidet.

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

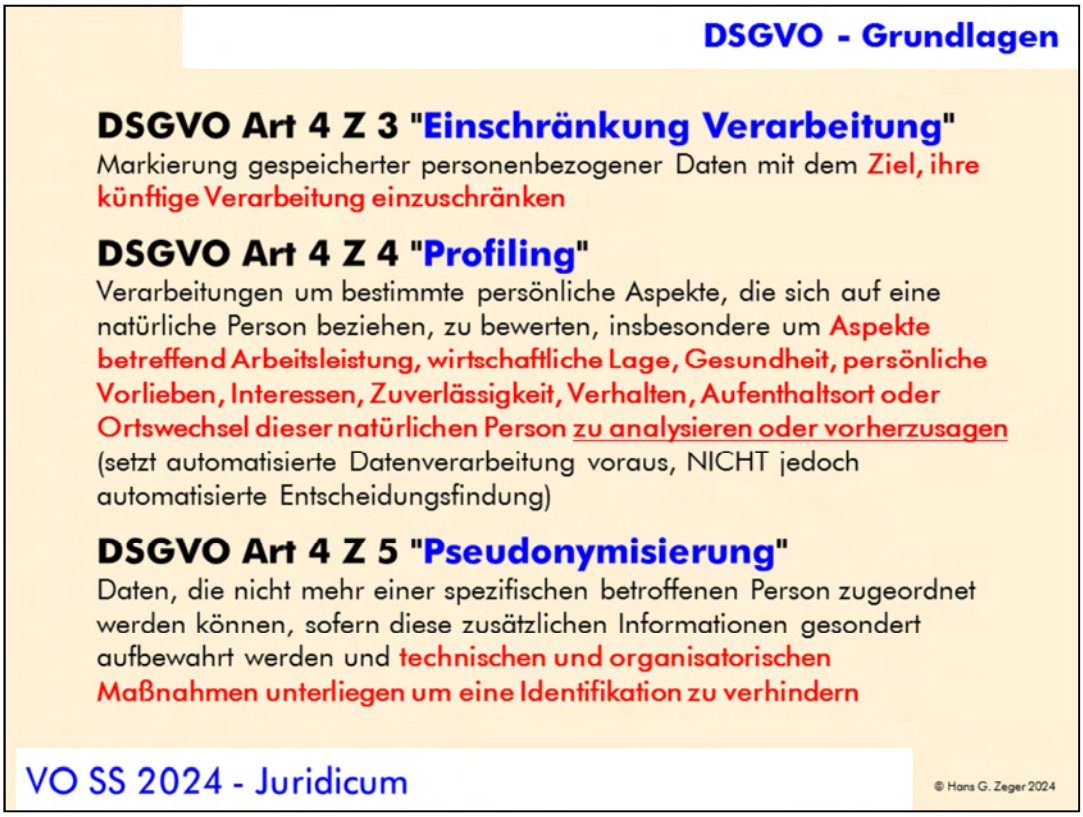
(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung 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;

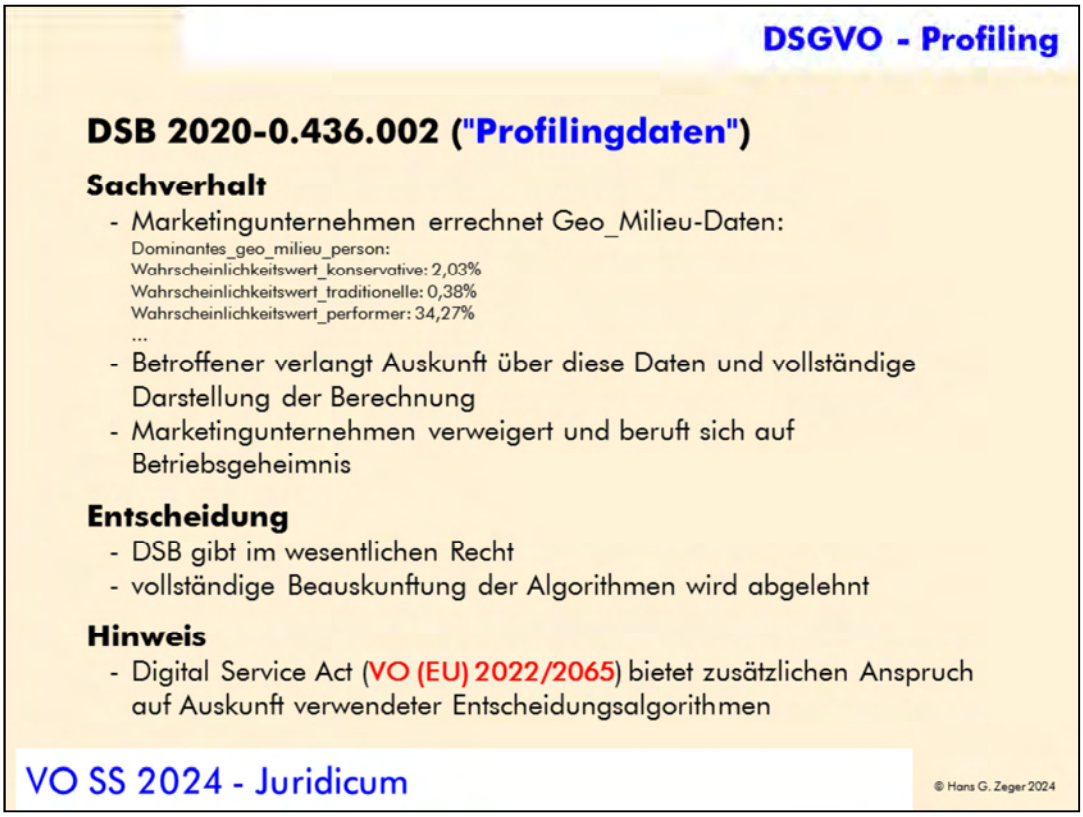


DSGVO Art. 4 Begriffsbestimmungen

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;



DSB 2020-0.436.002

c. Wie die Beschwerdegegnerin selbst ausführt, werden bei den sogenannten Geo_Milieus ähnliche Grundorientierungen, Werte, Lebensstile und Wohnumfelder zusammengefasst und vergleichbar gemacht, wobei das Berechnungsmodell auf einer „Hypothesenbildung" auf Grundlage eigener Forschung und vorhandener Daten (...) unter Einbeziehung von Milieuexperten beruhe, samt anschließender Überprüfung und Korrektur der Hypothesen durch die Firma Z***Marketing GmbH in E***, um Marketingplanungen durchzuführen.

...

e. Bei der Segmentierung, Errechnung und Zuordnung von Geo_Milieus werden in einer automatisierten Verarbeitung personenbezogener Daten verarbeitet, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, diesfalls insbesondere, um Aspekte bezüglich wirtschaftlicher Lage, persönlicher Vorlieben, Interessen etc. zu analysieren, zu segmentieren und Wahrscheinlichkeiten einer Zuordnung zu Geo_Milieus zu errechnen, um zielgerichtetes strategisches Marketing, Produktplanung und Werbezusendungen vorzunehmen.

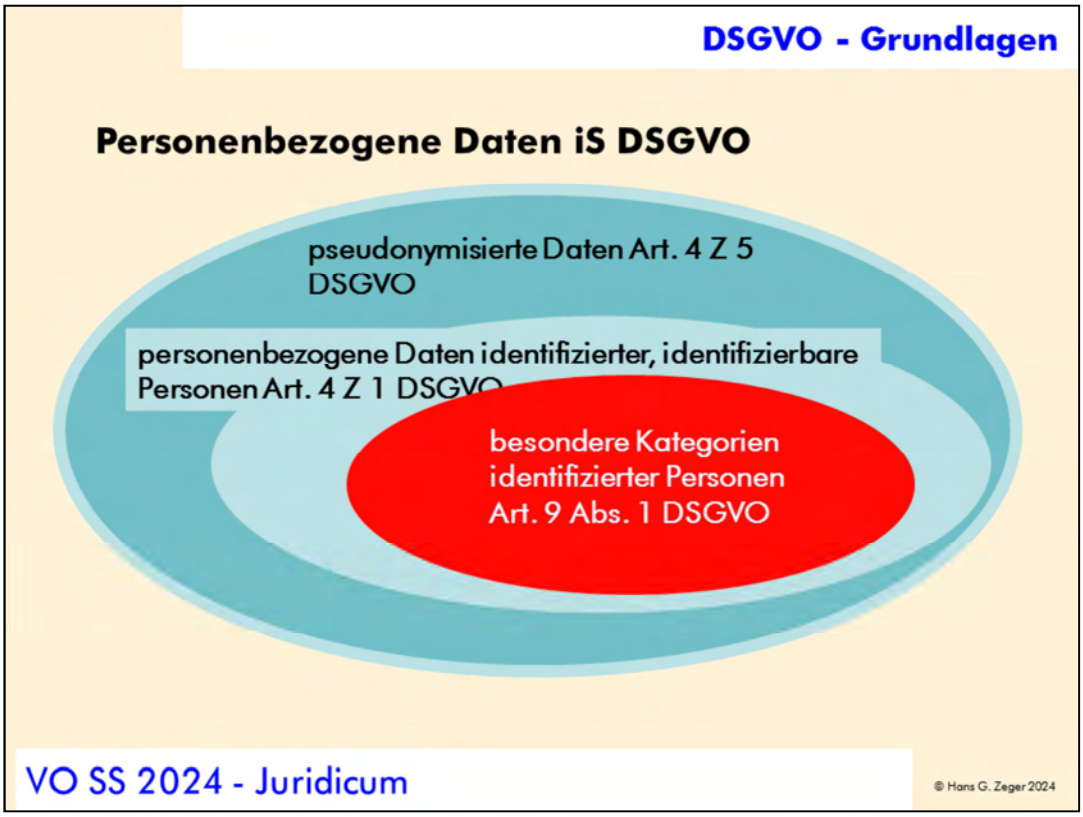
f. Die Subsummierung unter den Begriff des Profilings erfordert – dem Wortlaut des Art 4 Z 4 DSGVO zufolge – nicht, dass Analysen oder Vorhersagen über eine natürliche Person ausschließlich automationsunterstützt erfolgen, wie dies etwa Art. 22 DSGVO für „automatisierte Entscheidungen im Einzelfall" normiert. Vielmehr ist aus dem letzten Satz zu ErwGr 71 klar ersichtlich, dass der Unionsgesetzgeber die Begriffe „Profiling" und „automatisierte Entscheidungsfindung" getrennt betrachten wollte, wenn normiert ist („(…) Automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein").

Dementsprechend ist in den Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679" (WP 251 rev.01) vom 6. Februar 2018 unter Punkt A. („Profiling") zu lesen:

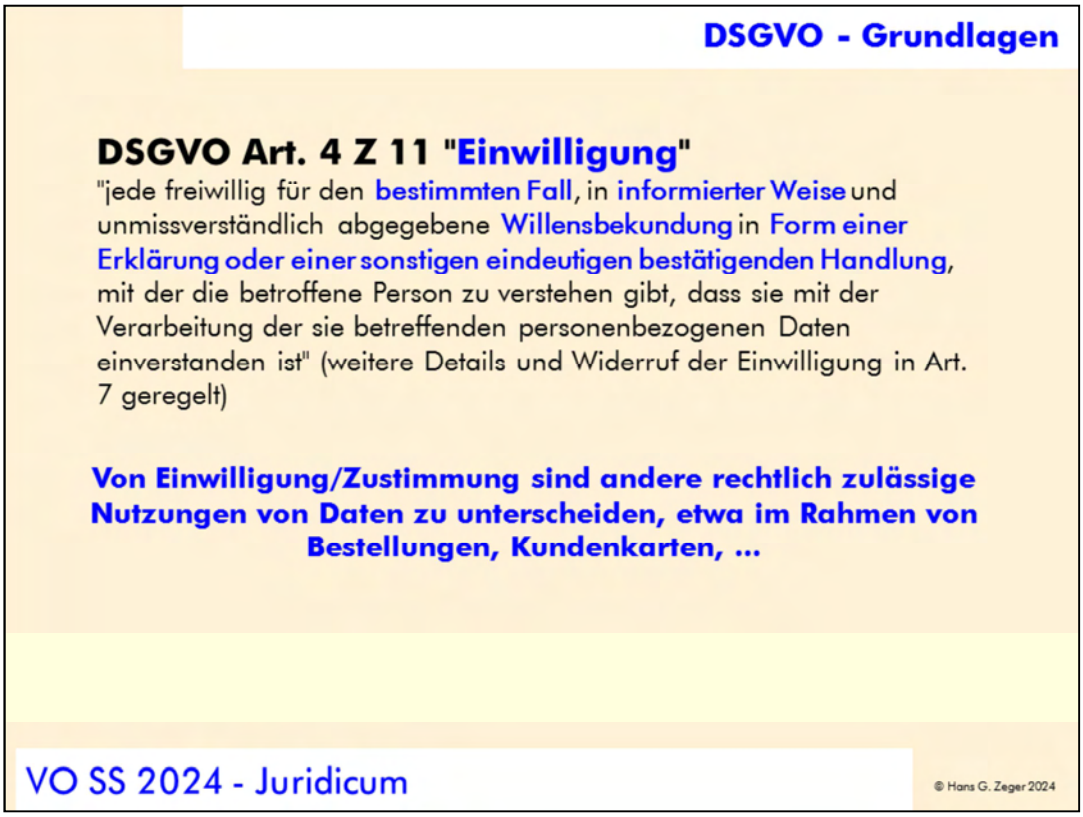
„Artikel 4 Absatz 4 bezieht sich auf „jede Art der automatisierten Verarbeitung", nicht auf eine „ausschließlich" automatisierte Verarbeitung (wie sie in Artikel 22 beschrieben wird). Es muss sich bei Profiling um eine Art der automatisierten Verarbeitung handeln – auch wenn ein Eingreifen einer Person nicht unbedingt die Aktivität aus der Definition ausschließt."

Die Datenschutzbehörde erachtet daher, die Errechnung und Zuordnung von Geo_Milieu-Wahrscheinlichkeiten zu einer bestimmten Person als Form eines Profilings im Sinne des Art. 4 Z 4 DSGVO für Zwecke des strategischen Marketings, der Produktplanung und Werbezusendung.

...


DSGVO - Grundlagen
Personenbezogene Daten iS DSGVO
pseudonymisierte Daten Art. 4 Z 5 DSGVO
personenbezogene Daten identifizierter, identifizierbare Personen Art. 4 Z 1 DSGVO
besondere Kategorien identifizierter Personen Art. 9 Abs. 1 DSGVO
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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 Art. 4 Begriffsbestimmungen

16. **„Hauptniederlassung“**

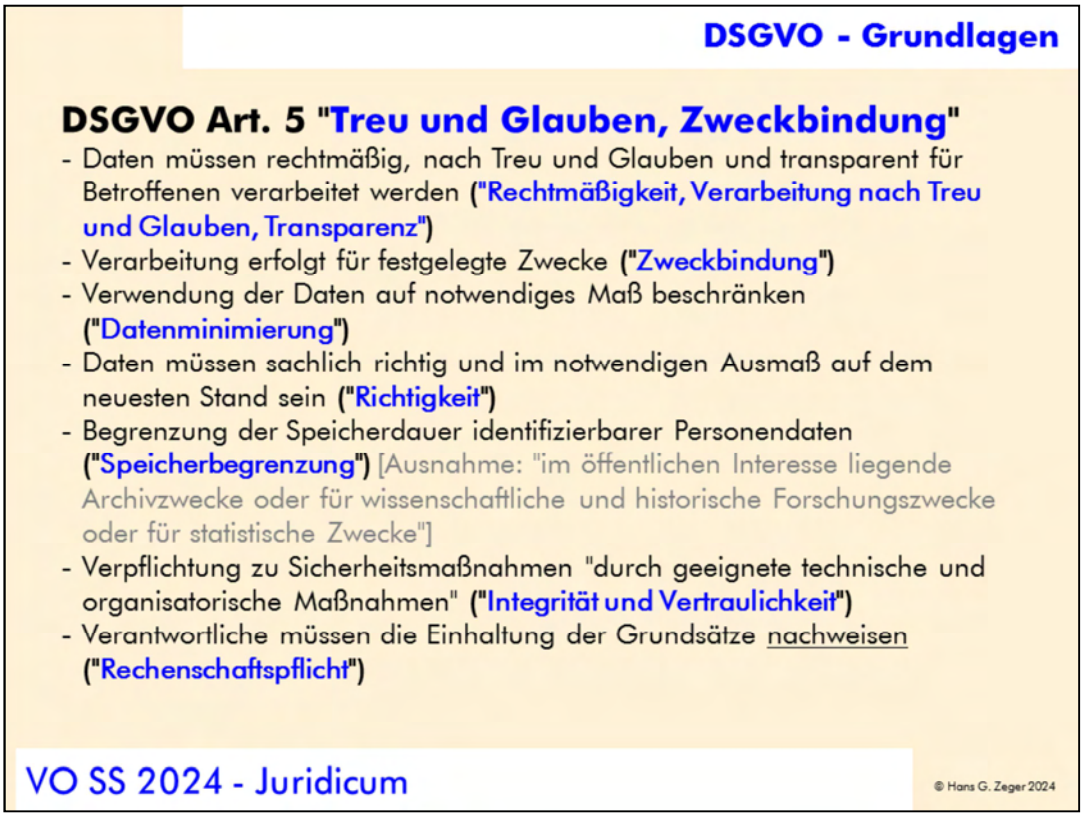
a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in 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,

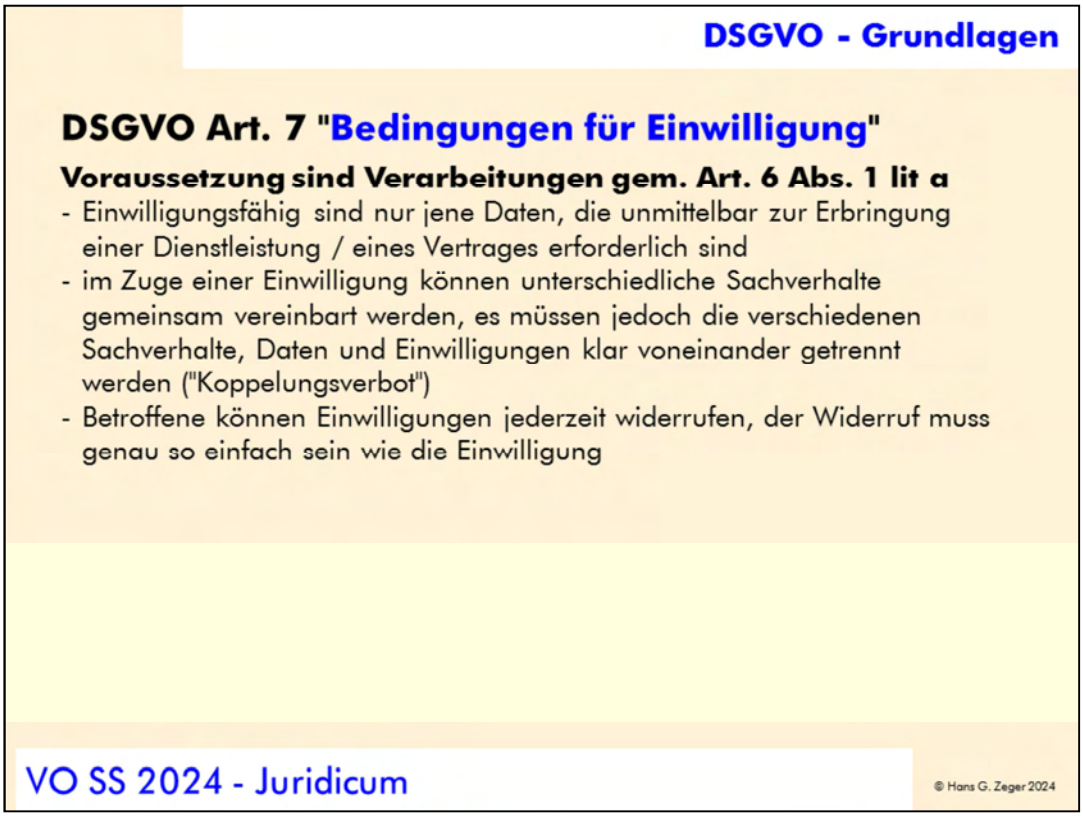
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen, e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

DSB-Entscheidung D124.3614/22 KSV 1870

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von (Beschwerdeführer), vertreten durch den Verein noyb - Europäisches Zentrum für digitale Rechte, vom 2. Februar 2021 gegen die KSV 1870 Information GmbH (Beschwerdegegnerin), vertreten durch die Putz & Rischka Rechtsanwälte KG in 1030 Wien, wegen einer behaupteten Verletzung im Recht auf Geheimhaltung wie folgt:

1. Der Beschwerde wird stattgegeben und es wird festgestellt, dass die Beschwerdegegnerin den Beschwerdeführer dadurch in seinem Recht auf Geheimhaltung verletzt hat, indem sie anlässlich seines Auskunftsbegehrens nach Art. 15 DSGVO zunächst eine ihn betreffende Melderegisterabfrage eingeholt und seine personenbezogenen Daten in der Folge in dem von ihr betriebenen Dateisystem "Wirtschaftsfdatenbank" gespeichert hat,

2. Der Beschwerdegegnerin wird amtswegig aufgetragen, innerhalb einer Frist von zwei Wochen bei sonstiger Exekution, die den Beschwerdeführer betreffende Eintragung aus dem von ihr betriebenen Dateisystem "Wirtschaftsfdatenbank" zu löschen.



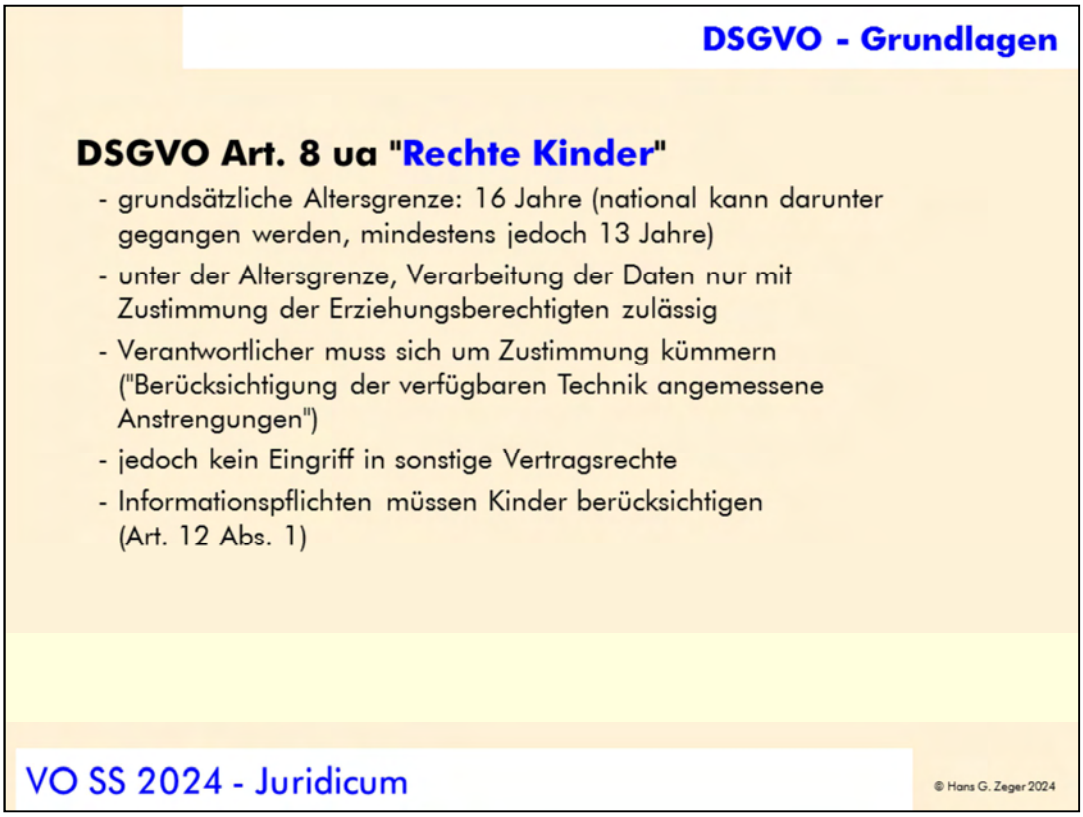
DSGVO Art. 7 Bedingungen für die Einwilligung

(1)Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2)Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3)Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4)Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.



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.

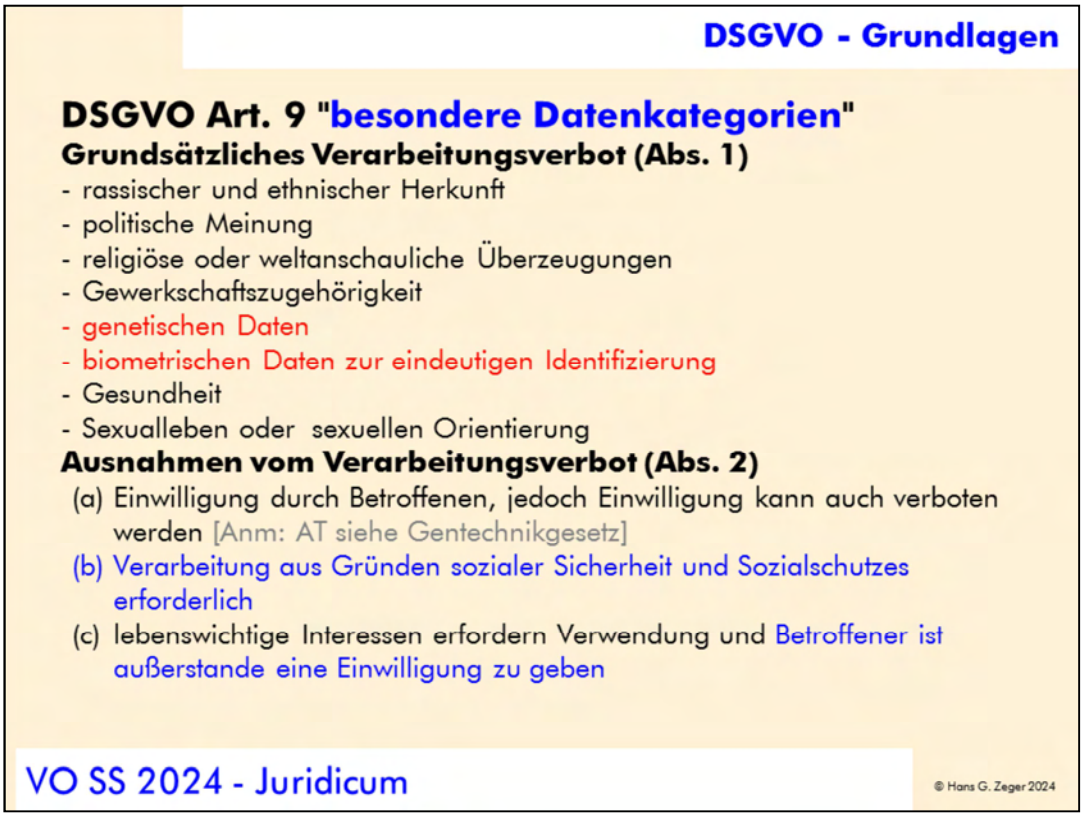
(3)Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, wie etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, unberührt.

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 - Grundlagen
Beispiel Online-Kauf eines "Haushaltsgerätes"
- Kaufdaten: Produkt, Besteller, Lieferadresse, Preis, Zahlungskonditionen, Kontaktdaten ⇨ Vertrag, für Verwendung der genannten Daten zur Abwicklung der Bestellung KEINE Einwilligung iS Art. 6 Abs. 1 lit a erforderlich ⇨ kein Widerruf iS Art. 7 möglich
- Newsletter-Bezug: eMailadresse ⇨ Zusätzlicher Dienst, Einwilligung iS Art. 6 Abs. 1 lit a erforderlich ⇨ Widerruf iS Art. 7 möglich, TKG Bestimmung zusätzlich beachten
- Kundenkarte + Rabattvereinbarungen: Interessensdaten, Familienverhältnisse, Umsatzdaten, ... ⇨ Zusätzlicher Vertrag, KEINE Einwilligung iS Art. 6 Abs. 1 lit a erforderlich ⇨ kein Widerruf iS Art. 7 möglich
- Referenzkunde: Angaben zum Besteller, persönliche Meinung zu Service, Händler und Firma sollen veröffentlicht werden ⇨ Zusätzlicher Dienst, wird in der Regel als Einwilligung iS Art. 6 Abs. 1 lit a gestaltet sein ⇨ Widerruf iS Art. 7 möglich, potentieller Konflikt mit Medienrecht! ⇨ auch als Vertrag gestaltbar
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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.

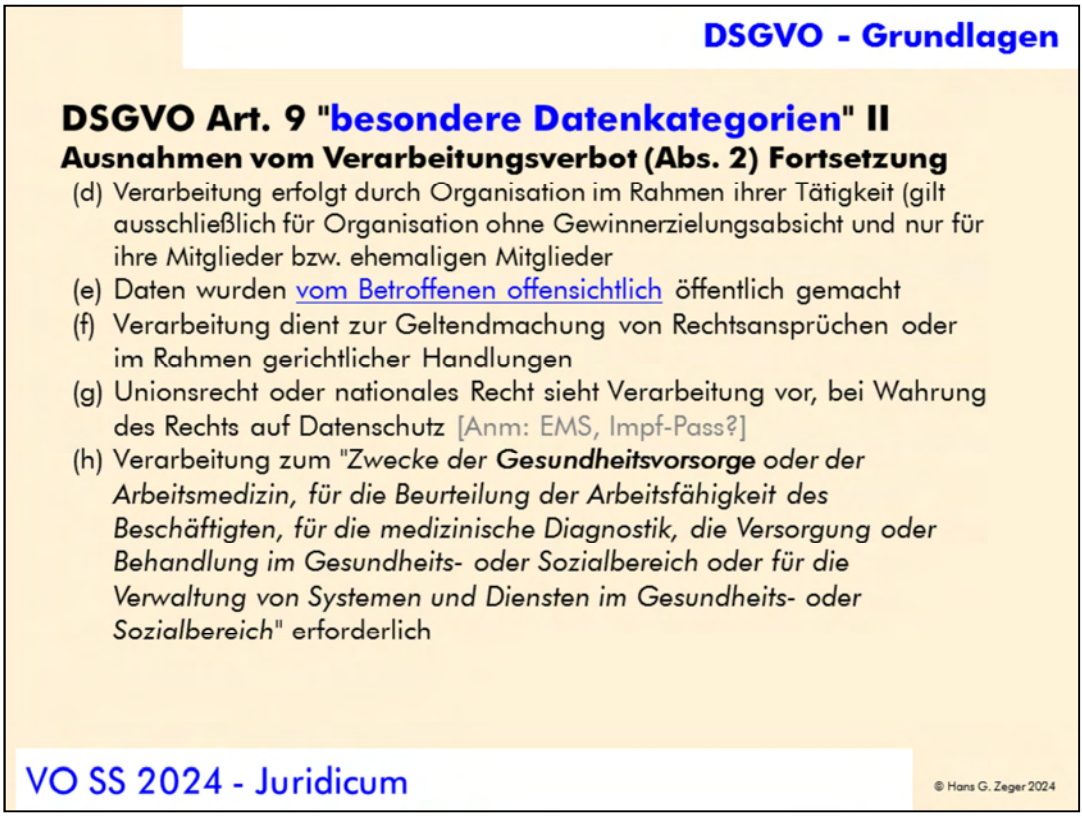
(2)Absatz 1 gilt nicht in folgenden Fällen:

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 Verarbeitung besonderer Kategorien personenbezogener Daten (Fortsetzung)

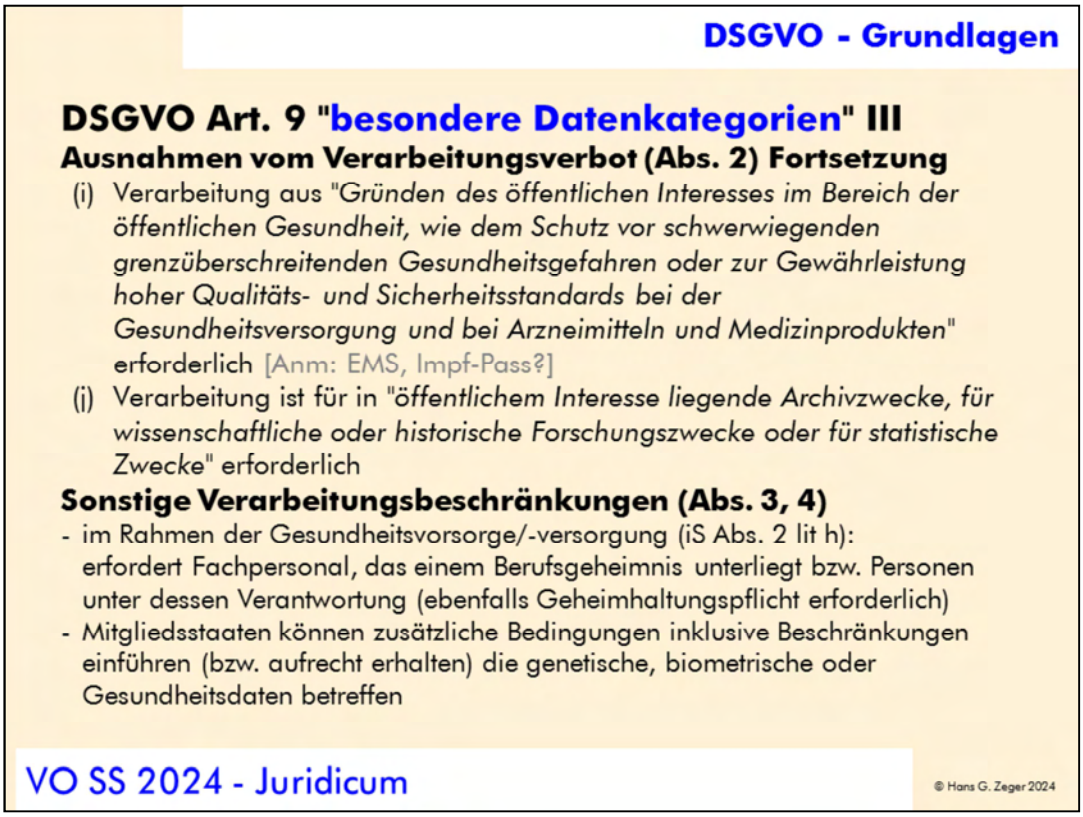
e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

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

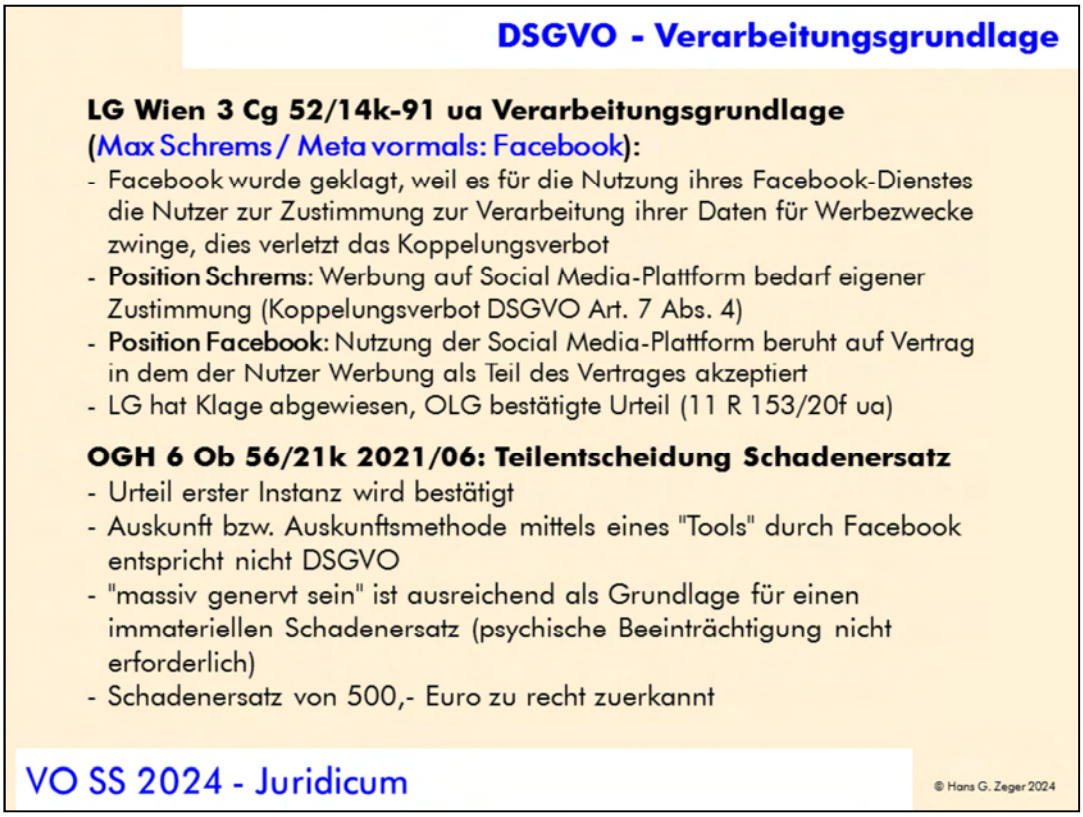


DSGVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten (Fortsetzung)

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.



Auszug aus OGH-Entscheidung 6 Ob 56/21k 2021/06

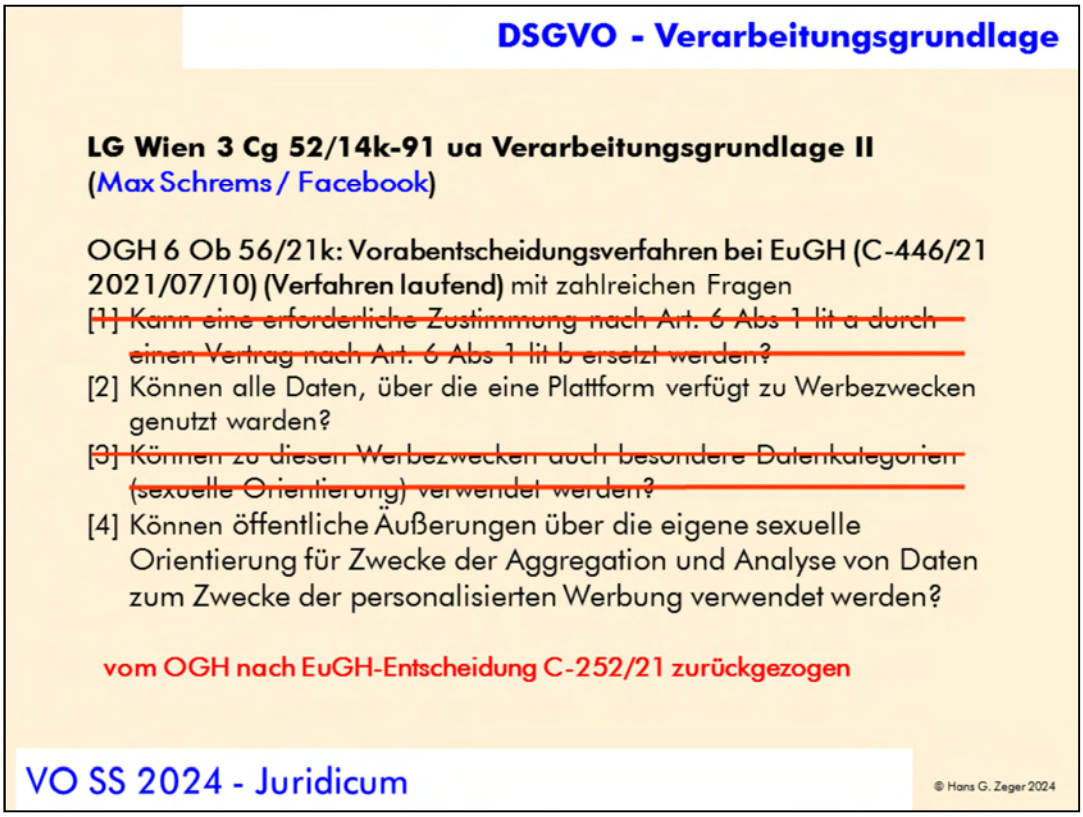
[32] Der Schaden des Klägers fuße auf einem emotionalen Ungemach aufgrund der bereits jahrelang andauernden Unsicherheit in Bezug auf die immense Verarbeitung seiner Daten. Der Kläger habe bis heute keinen abschließenden Überblick, wofür seine Daten tatsächlich verwendet bzw an wen sie weitergegeben wurden. Er habe unwiederbringlich die Kontrolle über seine Daten verloren. Hinzu komme die Verarbeitung von Daten nach Art 9 DSGVO, die sich beispielsweise in der unaufgeforderten Übermittlung von Einladungen zu Events für Homosexuelle widerspiegle. Durch die unvollständige Beauskunftung werde der Kläger auch an einer Kontrolle seiner Daten gehindert. Er könne nicht einmal abschätzen, an wen seine Daten weitergegeben werden. All dies führe zu einer enormen Beeinträchtigung des Klägers in seinem Grundrecht auf Datenschutz und seinen damit verbundenen Freiheiten. Darüber hinaus liege unter anderem ein Verstoß gegen den Grundsatz der Datenminimierung und Speicherbegrenzung vor.

...

[41] Das „AYI Tool" („Access Your Information Tool", „Zugriff auf deine Informationen Tool" bzw „Zugriff auf deine Daten Tool") ermöglicht den Zugriff auf Daten, gegliedert in „Deine Informationen", die aus Informationen bestehen, die der Nutzer hochgeladen und weitergegeben hat, wie zB Profil, Beiträge und Kommentare, und „Informationen über Dich", wie Informationen über den Nutzer, zB welche Geräte er verwendet hat, der Standort, die IP Adressen, von denen er sich angemeldet hat. Unter der Kategorie „Freunde" sieht man auch die gelöschten Freunde und wann sie gelöscht wurden. Es ist dort möglich Werbeanzeigen und Unternehmen anzuklicken; man hat dort Zugang zu seinen Werbeinteressen und die Möglichkeit, die mit dem Konto verbundenen Werbeinteressen einzusehen und zu verbergen. Es informiert auch darüber, dass es ein separates Tool zum Herunterladen („DYI Tool" „Download deiner Informationen Tool") dieser Informationen gibt, und leitet zu diesem Tool weiter. Insgesamt gibt es 60 Datenkategorien wie im Detail aus Beilage./151 ersichtlich. Das Tool ermöglicht zu sehen, welche Kategorien von personenbezogenen Daten die Beklagte speichert, gegliedert nach Jahren und Tagen. Wenn man etwas zum Zweck und der Dauer der Speicherung dieser Daten wissen will, muss man die Datenrichtlinie lesen, die dazu eine allgemeine Auskunft gibt. Dort finden sich allgemeine Informationen zur Verarbeitung, Personalisierung, Empfängern, Herkunft, Aufbewahrungsfrist und Speicherdauer.

...

[109] Der geltend gemachte immaterielle Schadenersatzanspruch sei berechtigt. Der Kläger habe einen immateriellen Schaden behauptet, der durch die Verletzung der Auskunftspflicht verursacht worden sei. Dieses Ungemach spiegle sich auch in den Feststellungen wider. Die geforderten 500 EUR harmonierten mit dem geringen Ausmaß dieses Unwohlseins.



Fragen gemäß Art 267 AEUV zur Vorabentscheidung

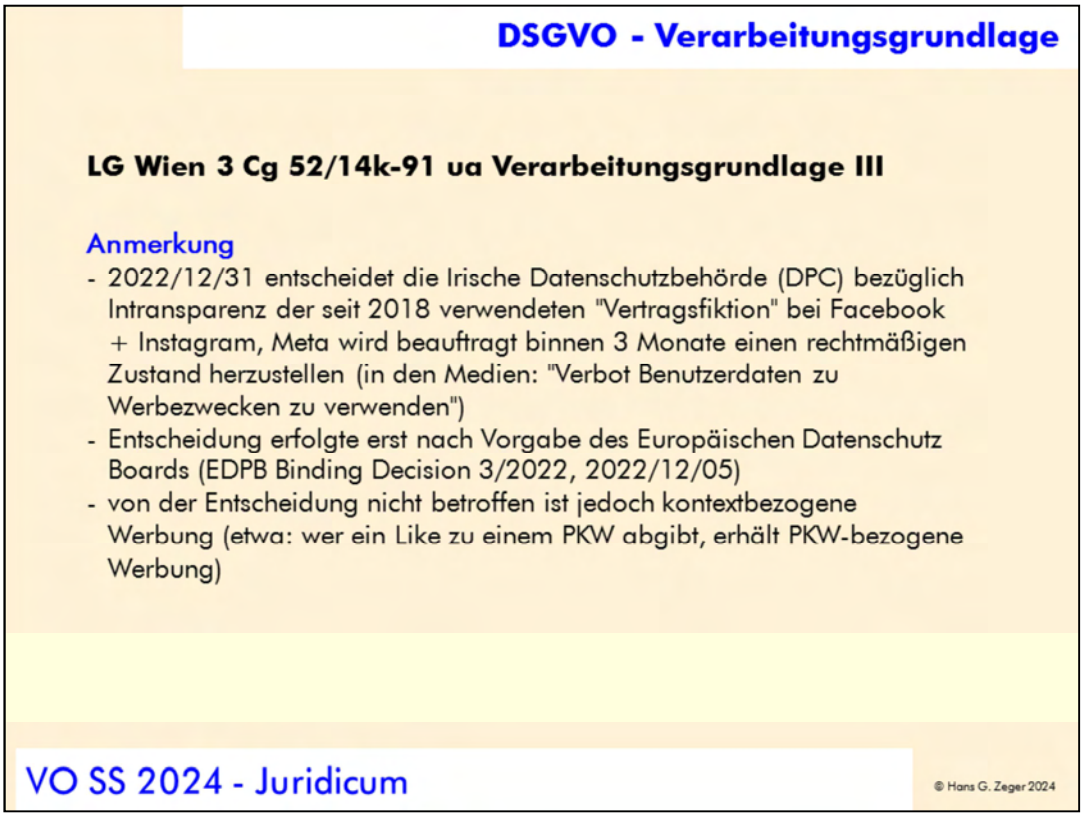
~~1. Sind die Bestimmungen der Art 6 Abs 1 lit a und b DSGVO dahingehend auszulegen, dass die Rechtmäßigkeit von Vertragsbestimmungen in allgemeinen Nutzungsbedingungen über Plattformverträge wie jenem im Ausgangsverfahren (insbesondere Vertragsbestimmungen wie:~~

~~„Anstatt dafür zu zahlen [...] erklärst du dich durch Nutzung der Facebook-Produkte, für die diese Nutzungsbedingungen gelten, einverstanden, dass wir dir Werbeanzeigen zeigen dürfen ... Wir verwenden deine personenbezogenen Daten [...] um dir Werbeanzeigen zu zeigen, die relevanter für dich sind."), die die Verarbeitung von personenbezogenen Daten für Aggregation und Analyse von Daten zum Zwecke der personalisierten Werbung beinhalten, nach den Anforderungen des Art 6 Abs 1 lit a iVm Art 7 DSGVO zu beurteilen sind, die nicht durch die Berufung auf Art 6 Abs 1 lit b DSGVO ersetzt werden können?~~

2. Ist Art 5 Abs 1 lit c DSGVO (Datenminimierung) dahin auszulegen, dass alle personenbezogenen Daten, über die eine Plattform wie im Ausgangsverfahren verfügt (insbesondere durch den Betroffenen oder durch Dritte auf und außerhalb der Plattform), ohne Einschränkung nach Zeit oder Art der Daten für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden können?

~~3. Ist Art 9 Abs 1 DSGVO dahin auszulegen, dass er auf die Verarbeitung von Daten anzuwenden ist, die eine gezielte Filterung von besonderen Kategorien personenbezogener Daten wie politische Überzeugung oder sexuelle Orientierung (etwa für Werbung) erlaubt, auch wenn der Verantwortliche zwischen diesen Daten nicht differenziert?~~

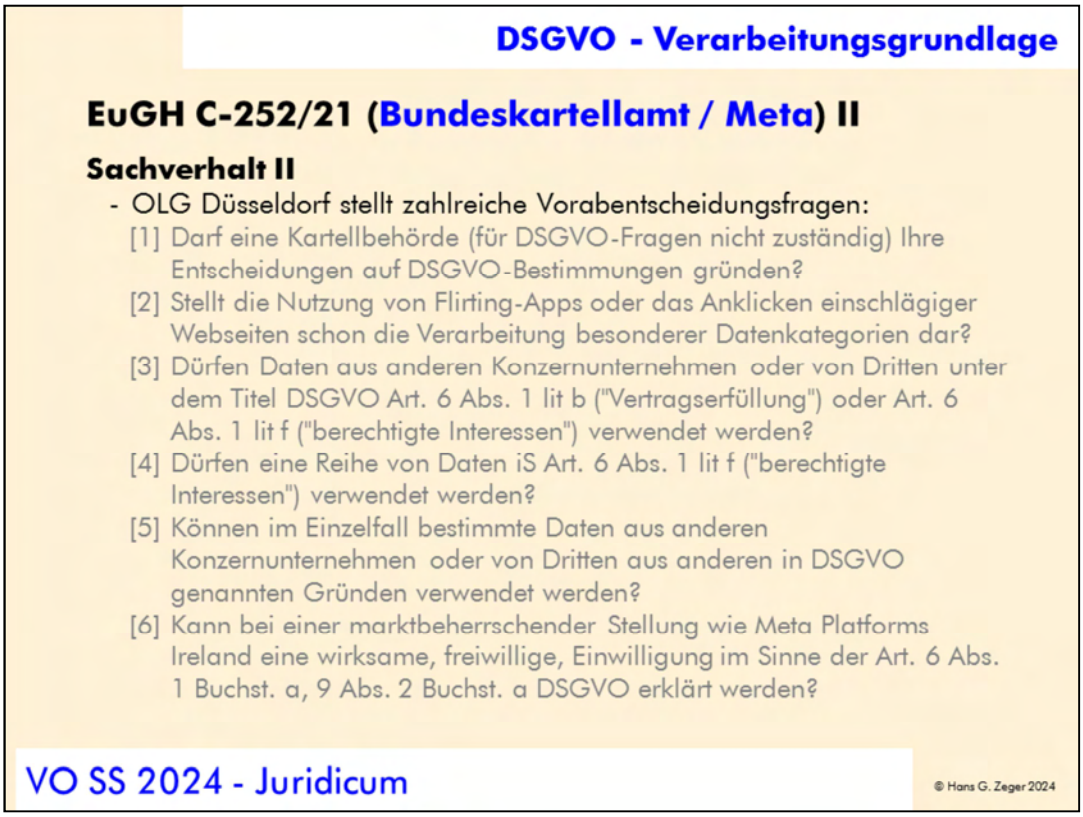
4. Ist Art 5 Abs 1 lit b iVm Art 9 Abs 2 lit e DSGVO dahin auszulegen, dass eine Äußerung über die eigene sexuelle Orientierung für die Zwecke einer Podiumsdiskussion die Verarbeitung von anderen Daten zur sexuellen Orientierung für Zwecke der Aggregation und Analyse von Daten zum Zwecke der personalisierten Werbung erlaubt?


DSGVO - Verarbeitungsgrundlage
LG Wien 3 Cg 52/14k-91 ua Verarbeitungsgrundlage III
Anmerkung
- 2022/12/31 entscheidet die Irische Datenschutzbehörde (DPC) bezüglich Intransparenz der seit 2018 verwendeten "Vertragsfiktion" bei Facebook + Instagram, Meta wird beauftragt binnen 3 Monate einen rechtmäßigen Zustand herzustellen (in den Medien: "Verbot Benutzerdaten zu Werbezwecken zu verwenden")
- Entscheidung erfolgte erst nach Vorgabe des Europäischen Datenschutz Boards (EDPB Binding Decision 3/2022, 2022/12/05)
- von der Entscheidung nicht betroffen ist jedoch kontextbezogene Werbung (etwa: wer ein Like zu einem PKW abgibt, erhält PKW-bezogene Werbung)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


DSGVO - Verarbeitungsgrundlage
EuGH C-252/21 (Bundeskartellamt / Meta)
Sachverhalt
- Facebook verwendet für personenbezogene Werbung neben den Facebook-Benutzerdaten auch Daten anderer Konzernunternehmen oder von Dritten ("Off-Facebook-Daten")
- Bundeskartellamt Deutschland untersagt 6. Februar 2019 die Verarbeitung von Off-Facebook-Daten auf Basis der Allgemeinen Nutzungsbedingungen
- Facebook/Meta legt am 11. Februar 2019 dagegen Beschwerde ein, ua mit folgenden Einwänden:
- Bundeskartellamt zur Prüfung der DSGVO-Konformität nicht berechtigt
- konzernweite Datenverarbeitung ist zur nahtlosen Nutzung der Dienste erforderlich
- Daten zur Personalisierung des Facebookdienstes erforderlich
- Daten zur Netzsicherheit, Produktentwicklung, Forschung, ... erforderlich
- Facebook/Meta ändert 31. Juli 2019 Nutzungsbedingungen
Nutzer müssen der Off-Facebook-Nutzung zustimmen oder bezahlen ("Pay" or "Okay")
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



EuGH C-252/21 Vorabentscheidungsfragen I

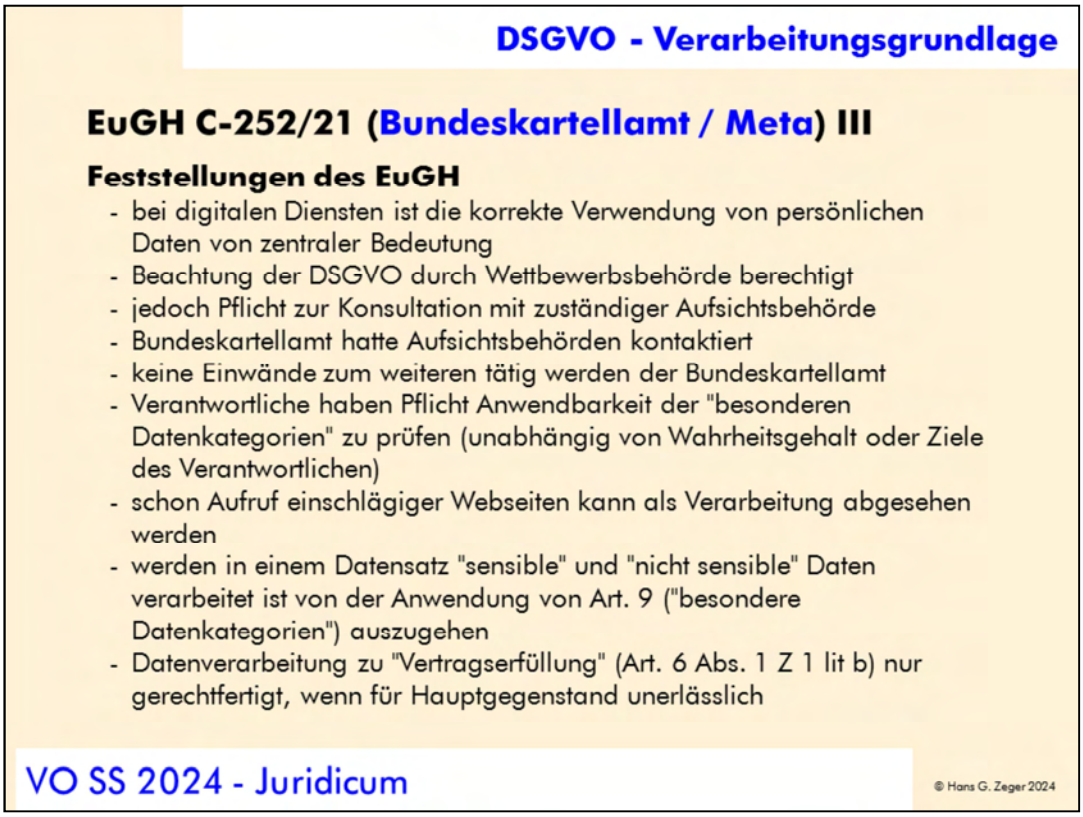
1. a) Ist es mit den Art. 51 ff. DSGVO vereinbar, wenn eine nationale Kartellbehörde eines Mitgliedstaats, wie das Bundeskartellamt, die nicht Aufsichtsbehörde im Sinne der Art. 51 ff. DSGVO ist und in deren Mitgliedstaat ein außerhalb der Europäischen Union ansässiges Unternehmen eine Niederlassung unterhält, die die in einem anderen Mitgliedstaat belegene Hauptniederlassung dieses Unternehmens, welcher die ausschließliche Verantwortung für die Verarbeitung personenbezogener Daten für das gesamte Gebiet der Europäischen Union obliegt, im Bereich Werbung, Kommunikation und Öffentlichkeitsarbeit unterstützt, für die kartellrechtliche Missbrauchsaufsicht einen Verstoß von Vertragsbedingungen der Hauptniederlassung zur Datenverarbeitung und von deren Durchführung gegen die DSGVO feststellt und eine Verfügung zur Abstellung dieses Verstoßes erlässt?

b) Wenn ja: Ist dies mit Art. 4 Abs. 3 EUV vereinbar, wenn gleichzeitig die federführende Aufsichtsbehörde im Mitgliedstaat der Hauptniederlassung im Sinne des Art. 56 Abs. 1 DSGVO deren Vertragsbedingungen zur Datenverarbeitung einem Untersuchungsverfahren unterzieht?

2. a) Handelt es sich dann, wenn ein Internetnutzer Webseiten oder Apps, die Bezug zu den Kriterien des Art. 9 Abs. 1 DSGVO haben, wie etwa Flirting-Apps, Homosexuellen-Partnerbörsen, Webseiten politischer Parteien, gesundheitsbezogene Webseiten, entweder nur aufruft oder dort auch Eingaben tätigt, etwa bei Registrierung oder Bestellungen, und ein … Unternehmen wie Meta Platforms Ireland über in die Webseiten und Apps eingebundene Schnittstellen, wie „Facebook Business Tools“, oder über auf dem Computer oder mobilen Endgerät des Internetnutzers eingesetzte Cookies oder ähnliche Speichertechnologien die Daten über den Aufruf der Webseiten und Apps durch den Nutzer und über dort getätigte Eingaben des Nutzers erfasst, mit den Daten des Facebook.com-Kontos des Nutzers verknüpft und verwendet, bei der Erfassung und/oder der Verknüpfung und/oder der Verwendung um die Verarbeitung sensibler Daten im Sinne der Norm?

b) Wenn ja: Stellt der Aufruf dieser Webseiten und Apps und/oder die Tätigung von Eingaben und/oder die Betätigung der in diese Webseiten oder Apps eingebundenen Schaltflächen („soziale Plug-ins“ wie „Gefällt mir“, „Teilen“ oder „Facebook Log-in“ oder „Account Kit“) eines Anbieters wie Meta Platforms Ireland ein offensichtliches Öffentlichmachen der Daten über den Aufruf als solchen und/oder die Eingaben durch den Nutzer im Sinne des Art. 9 Abs. 2 Buchst. e DSGVO dar?

3. Kann ein Unternehmen wie Meta Platforms Ireland, das ein werbefinanziertes, digitales soziales Netzwerk betreibt und in seinen Nutzungsbedingungen die Personalisierung der Inhalte und der Werbung, Netzwerksicherheit, Produktverbesserung und durchgängige und nahtlose Nutzung aller konzerneigenen Produkte anbietet, sich auf den Rechtfertigungsgrund der Erforderlichkeit zur Vertragserfüllung gemäß Art. 6 Abs. 1 Buchst. b DSGVO oder der Wahrnehmung berechtigter Interessen gemäß Art. 6 Abs. 1 Buchst. f DSGVO berufen, wenn es zu diesen Zwecken Daten aus anderen konzerneigenen Diensten und aus dritten Webseiten und Apps über in diese eingebundene Schnittstellen, wie „Facebook Business Tools“, oder über auf dem Computer oder mobilen Endgerät des Internetnutzers eingesetzte Cookies oder ähnliche Speichertechnologien erfasst, mit dem Facebook.com-Konto des Nutzers verknüpft und verwendet?



EuGH C-252/21 Vorabentscheidungsfragen II

4. Können in einem solchen Fall auch

– die Minderjährigkeit der Nutzer für die Personalisierung von Inhalten und Werbung, Produktverbesserung, Netzwerksicherheit und Nicht-Marketing-Kommunikation mit dem Nutzer,

– die Bereitstellung von Messungen, Analysen und sonstigen Unternehmens-Services an Werbekunden, Entwickler und sonstige Partner, damit diese ihre Leistungen bewerten und verbessern können,

– die Bereitstellung von Marketing-Kommunikation mit dem Nutzer, damit das Unternehmen seine Produkte verbessern und Direktmarketing durchführen kann,

– Forschung und Innovation für soziale Zwecke, um den Stand der Technik bzw. das wissenschaftliche Verständnis bezüglich wichtiger sozialer Themen zu fördern und um die Gesellschaft und Welt positiv zu beeinflussen,

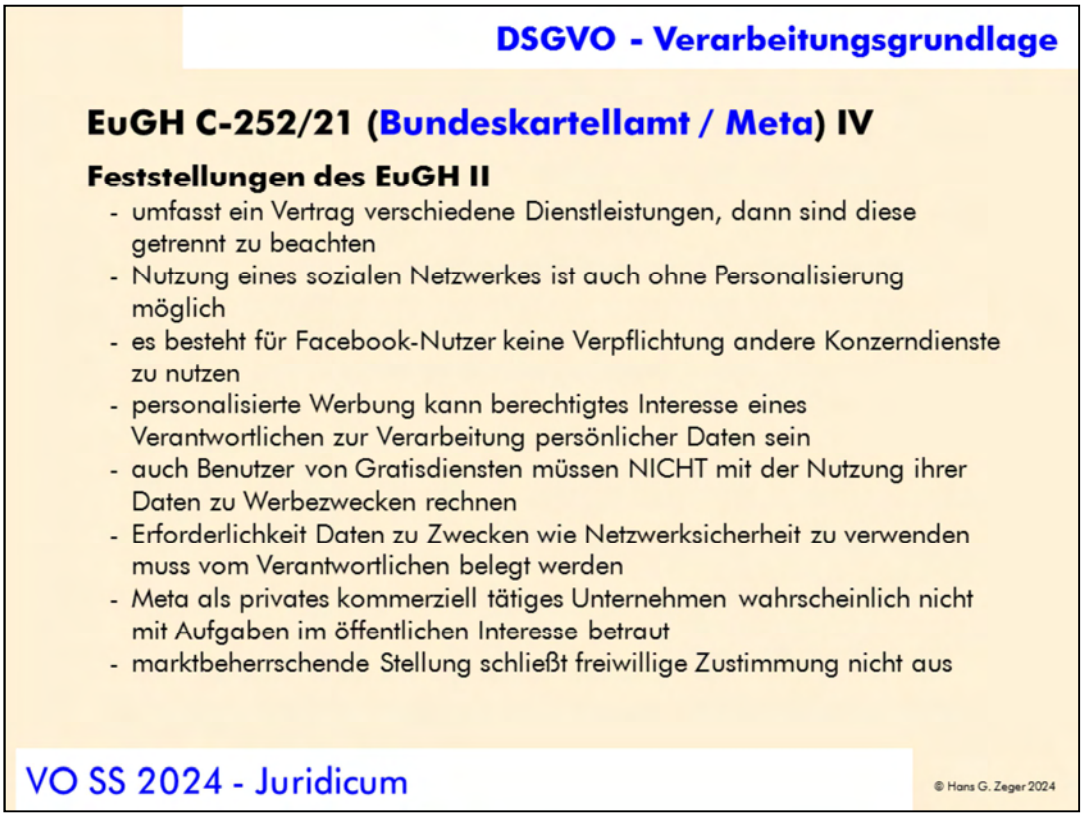
– die Information von Strafverfolgungs- und Vollstreckungsbehörden und die Antwort auf rechtliche Anfragen, um Straftaten, unberechtigte Nutzung, Verstöße gegen die Nutzungsbedingungen und Richtlinien und sonstige schädliche Verhaltensweisen zu verhindern, aufzudecken und zu verfolgen,

berechtigte Interessen im Sinne des Art. 6 Abs. 1 Buchst. f DSGVO sein, wenn das Unternehmen zu diesen Zwecken Daten aus anderen konzerneigenen Diensten und aus dritten Webseiten und Apps über in diese eingebundene Schnittstellen, wie „Facebook Business Tools“, oder über auf dem Computer oder mobilen Endgerät des Internetnutzers eingesetzte Cookies oder ähnliche Speichertechnologien erfasst, mit dem Facebook.com-Konto des Nutzers verknüpft und verwendet?

5. Kann in einem solchen Fall die Erfassung von Daten aus anderen konzerneigenen Diensten und aus dritten Webseiten und Apps über in diese eingebundene Schnittstellen, wie „Facebook Business Tools“, oder über auf dem Computer oder mobilen Endgerät des Internetnutzers eingesetzte Cookies oder ähnliche Speichertechnologien, die Verknüpfung mit dem Facebook.com-Konto des Nutzers und die Verwendung oder die Verwendung bereits anderweit rechtmäßig erfasster und verknüpfter Daten im Einzelfall auch gemäß Art. 6 Abs. 1 Buchst. c, d und e DSGVO gerechtfertigt sein, um etwa eine rechtsgültige Anfrage für bestimmte Daten zu beantworten (Buchst. c), um schädliches Verhalten zu bekämpfen und die Sicherheit zu fördern (Buchst. d), zur Forschung zum Wohle der Gesellschaft und zur Förderung von Schutz, Integrität und Sicherheit (Buchst. e)?

6. Kann gegenüber einem marktbeherrschenden Unternehmen wie Meta Platforms Ireland eine wirksame, insbesondere nach Art. 4 Nr. 11 DSGVO freiwillige, Einwilligung im Sinne der Art. 6 Abs. 1 Buchst. a, 9 Abs. 2 Buchst. a DSGVO erklärt werden?

...



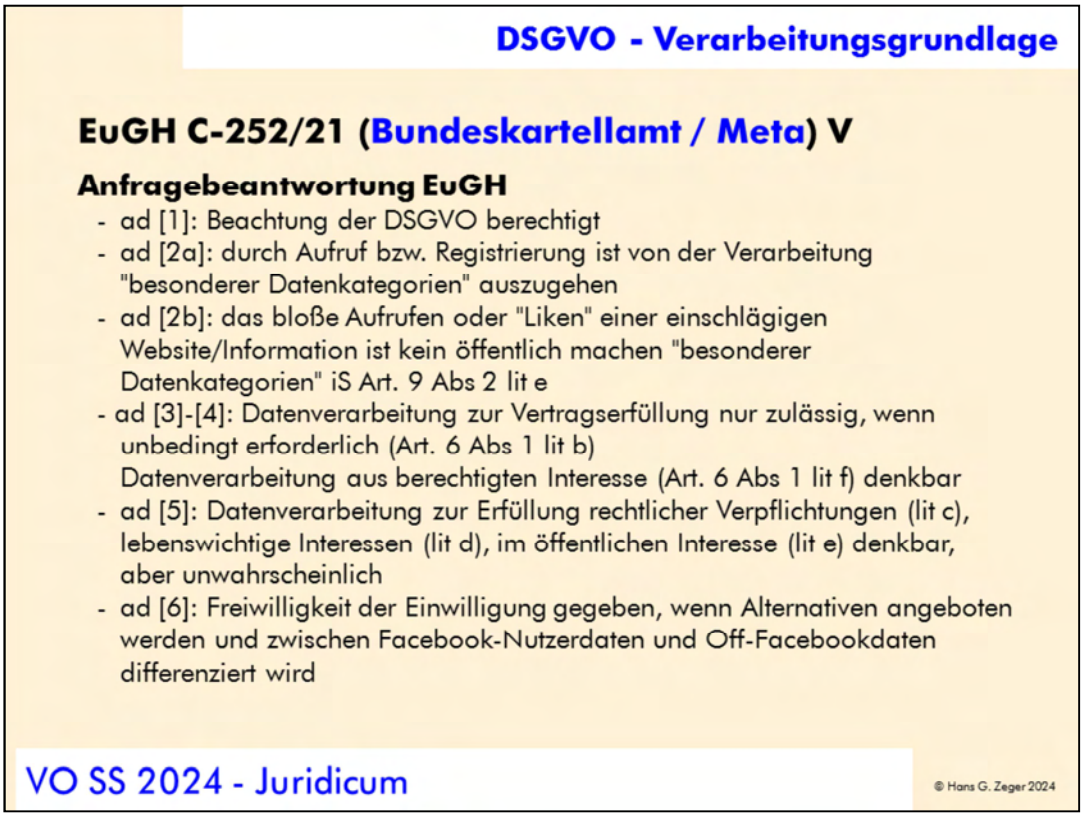
EuGH C-252/21 Vorabentscheidungsfragen III

Wenn Frage 1 zu verneinen ist:

7. a) Kann eine nationale Kartellbehörde eines Mitgliedstaats, wie das Bundeskartellamt, die nicht Aufsichtsbehörde im Sinne der Art. 51 ff. DSGVO ist und die einen Verstoß eines marktbeherrschenden Unternehmens gegen das kartellrechtliche Missbrauchsverbot prüft, der nicht in einem Verstoß von dessen Datenverarbeitungsbedingungen und ihrer Durchführung gegen die DSGVO besteht, etwa im Rahmen der Interessenabwägung Feststellungen dazu treffen, ob die Datenverarbeitungsbedingungen dieses Unternehmens und ihre Durchführung der DSGVO entsprechen?

b) Wenn ja: Gilt dies im Hinblick auf Art. 4 Abs. 3 EUV auch dann, wenn gleichzeitig die gemäß Art. 56 Abs. 1 DSGVO zuständige federführende Aufsichtsbehörde die Datenverarbeitungsbedingungen dieses Unternehmens einem Untersuchungsverfahren unterzieht?

Wenn Frage 7 zu bejahen ist, bedarf es der Beantwortung der Fragen 3 bis 5 in Bezug auf die Daten aus der Nutzung des konzerneigenen Dienstes Instagram



EuGH C-252/21 Entscheidung (Ausschnitte)

1. Die Art. 51 ff. der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sowie Art. 4 Abs. 3 EUV
sind dahin auszulegen, dass
eine mitgliedstaatliche Wettbewerbsbehörde im Rahmen der Prüfung, ob ein Missbrauch einer beherrschenden Stellung durch ein Unternehmen im Sinne von Art. 102 AEUV vorliegt, vorbehaltlich der Erfüllung ihrer Pflicht zur loyalen Zusammenarbeit mit den Aufsichtsbehörden feststellen kann, dass die Allgemeinen Nutzungsbedingungen dieses Unternehmens, soweit sie sich auf die Verarbeitung personenbezogener Daten beziehen, und die Durchführung dieser Nutzungsbedingungen nicht mit der Verordnung 2016/679 vereinbar sind, wenn diese Feststellung erforderlich ist, um das Vorliegen eines solchen Missbrauchs zu belegen.
...

2. Art. 9 Abs. 1 der Verordnung 2016/679
ist dahin auszulegen, dass
in dem Fall, dass ein Nutzer eines sozialen Online-Netzwerks Websites oder Apps mit Bezug zu einer oder mehreren der in dieser Bestimmung genannten Kategorien aufruft und dort gegebenenfalls Daten eingibt, indem er sich registriert oder Online-Bestellungen aufgibt, die Verarbeitung personenbezogener Daten durch den Betreiber dieses sozialen Online-Netzwerks, die darin besteht, dass dieser Betreiber die aus dem Aufruf dieser Websites und Apps stammenden Daten sowie die vom Nutzer eingegebenen Daten über integrierte Schnittstellen, Cookies oder ähnliche Speichertechnologien erhebt, die Gesamtheit dieser Daten mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und diese Daten verwendet, als eine „Verarbeitung besonderer Kategorien personenbezogener Daten“ im Sinne dieser Bestimmung anzusehen ist, die vorbehaltlich der in Art. 9 Abs. 2 der Verordnung 2016/679 vorgesehenen Ausnahmen grundsätzlich untersagt ist, wenn diese Datenverarbeitung die Offenlegung von Informationen ermöglicht, die in eine dieser Kategorien fallen, unabhängig davon, ob diese Informationen einen Nutzer dieses Netzwerks oder eine andere natürliche Person betreffen.
...

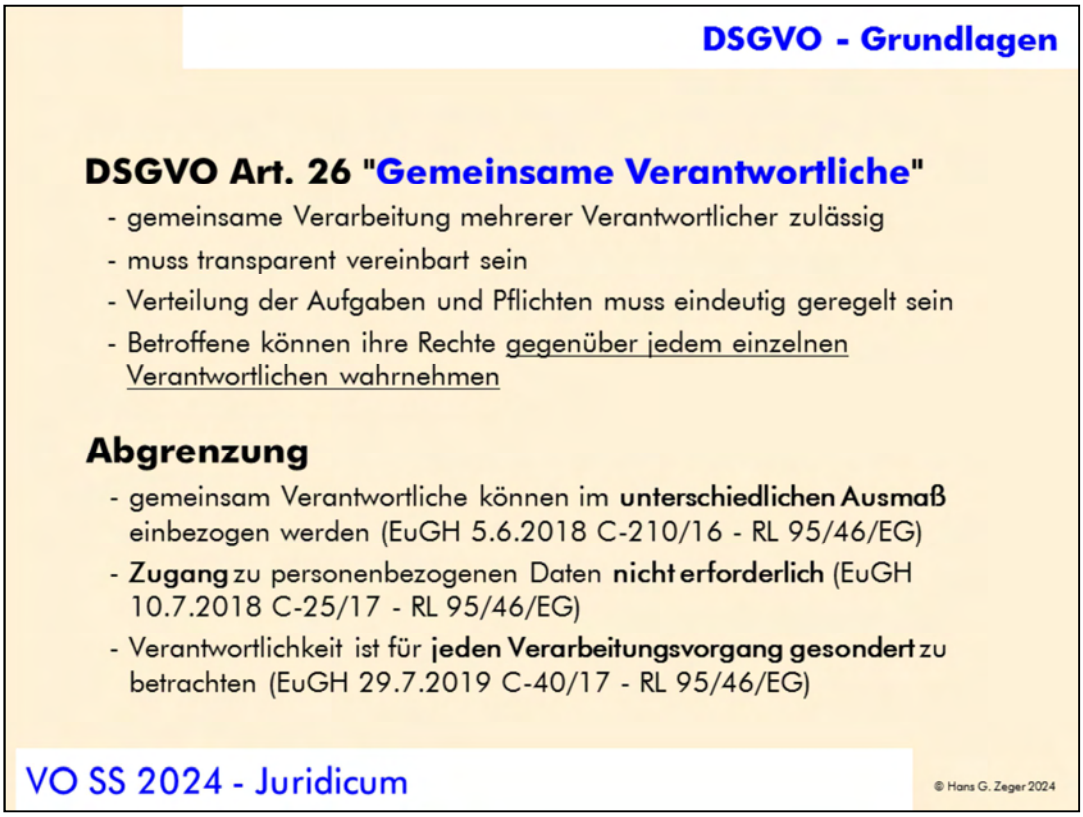
8. Art. 6 Abs. 1 Unterabs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a der Verordnung 2016/679
sind dahin auszulegen, dass
der Umstand, dass der Betreiber eines sozialen Online-Netzwerks eine beherrschende Stellung auf dem Markt für soziale Online-Netzwerke einnimmt, für sich genommen nicht ausschließt, dass die Nutzer eines solchen Netzwerks im Sinne von Art. 4 Nr. 11 dieser Verordnung wirksam in die Verarbeitung ihrer personenbezogenen Daten durch diesen Betreiber einwilligen können. Gleichwohl ist dieser Umstand ein wichtiger Aspekt für die Prüfung, ob die Einwilligung tatsächlich wirksam, insbesondere freiwillig, erteilt wurde, wofür der betreffende Betreiber die Beweislast trägt.

EuGH C-252/21 Entscheidung (Ausschnitte)

1. Die Art. 51 ff. der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sowie Art. 4 Abs. 3 EUV
sind dahin auszulegen, dass
eine mitgliedstaatliche Wettbewerbsbehörde im Rahmen der Prüfung, ob ein Missbrauch einer beherrschenden Stellung durch ein Unternehmen im Sinne von Art. 102 AEUV vorliegt, vorbehaltlich der Erfüllung ihrer Pflicht zur loyalen Zusammenarbeit mit den Aufsichtsbehörden feststellen kann, dass die Allgemeinen Nutzungsbedingungen dieses Unternehmens, soweit sie sich auf die Verarbeitung personenbezogener Daten beziehen, und die Durchführung dieser Nutzungsbedingungen nicht mit der Verordnung 2016/679 vereinbar sind, wenn diese Feststellung erforderlich ist, um das Vorliegen eines solchen Missbrauchs zu belegen.
...

2. Art. 9 Abs. 1 der Verordnung 2016/679
ist dahin auszulegen, dass
in dem Fall, dass ein Nutzer eines sozialen Online-Netzwerks Websites oder Apps mit Bezug zu einer oder mehreren der in dieser Bestimmung genannten Kategorien aufruft und dort gegebenenfalls Daten eingibt, indem er sich registriert oder Online-Bestellungen aufgibt, die Verarbeitung personenbezogener Daten durch den Betreiber dieses sozialen Online-Netzwerks, die darin besteht, dass dieser Betreiber die aus dem Aufruf dieser Websites und Apps stammenden Daten sowie die vom Nutzer eingegebenen Daten über integrierte Schnittstellen, Cookies oder ähnliche Speichertechnologien erhebt, die Gesamtheit dieser Daten mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und diese Daten verwendet, als eine „Verarbeitung besonderer Kategorien personenbezogener Daten“ im Sinne dieser Bestimmung anzusehen ist, die vorbehaltlich der in Art. 9 Abs. 2 der Verordnung 2016/679 vorgesehenen Ausnahmen grundsätzlich untersagt ist, wenn diese Datenverarbeitung die Offenlegung von Informationen ermöglicht, die in eine dieser Kategorien fallen, unabhängig davon, ob diese Informationen einen Nutzer dieses Netzwerks oder eine andere natürliche Person betreffen.
...

8. Art. 6 Abs. 1 Unterabs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a der Verordnung 2016/679
sind dahin auszulegen, dass
der Umstand, dass der Betreiber eines sozialen Online-Netzwerks eine beherrschende Stellung auf dem Markt für soziale Online-Netzwerke einnimmt, für sich genommen nicht ausschließt, dass die Nutzer eines solchen Netzwerks im Sinne von Art. 4 Nr. 11 dieser Verordnung wirksam in die Verarbeitung ihrer personenbezogenen Daten durch diesen Betreiber einwilligen können. Gleichwohl ist dieser Umstand ein wichtiger Aspekt für die Prüfung, ob die Einwilligung tatsächlich wirksam, insbesondere freiwillig, erteilt wurde, wofür der betreffende Betreiber die Beweislast trägt.

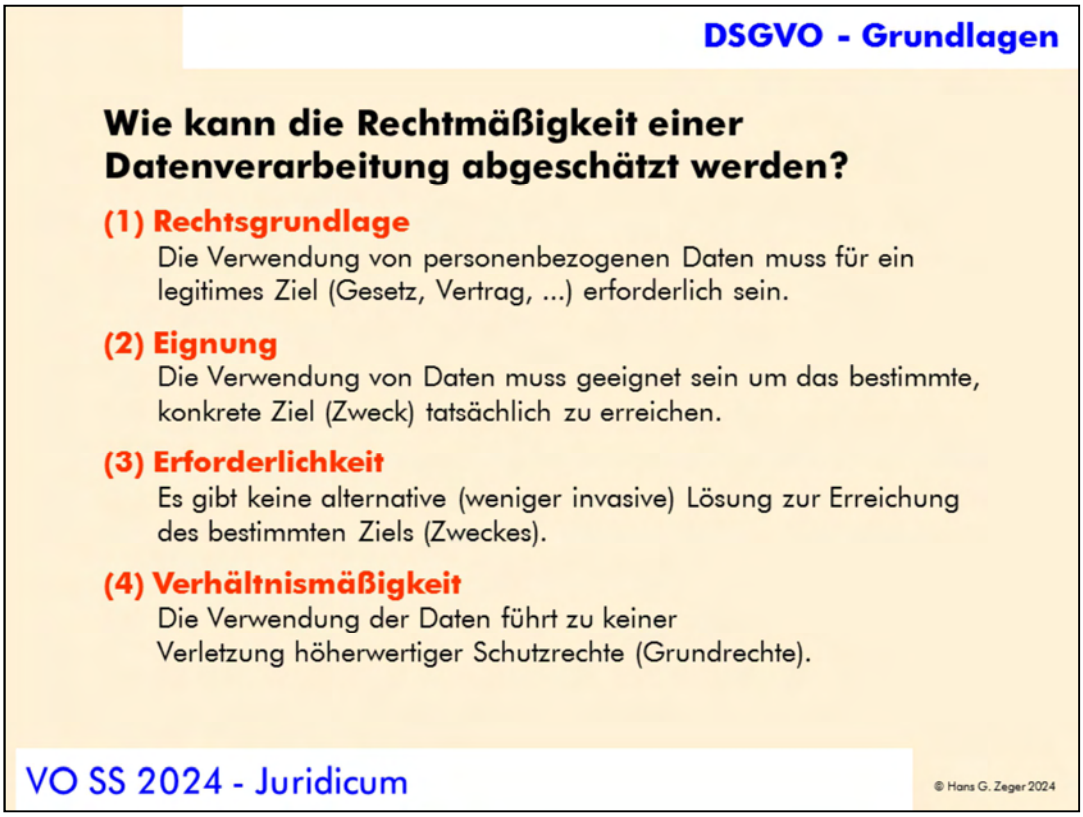


DSGVO Art. 26 Gemeinsam für die Verarbeitung Verantwortliche

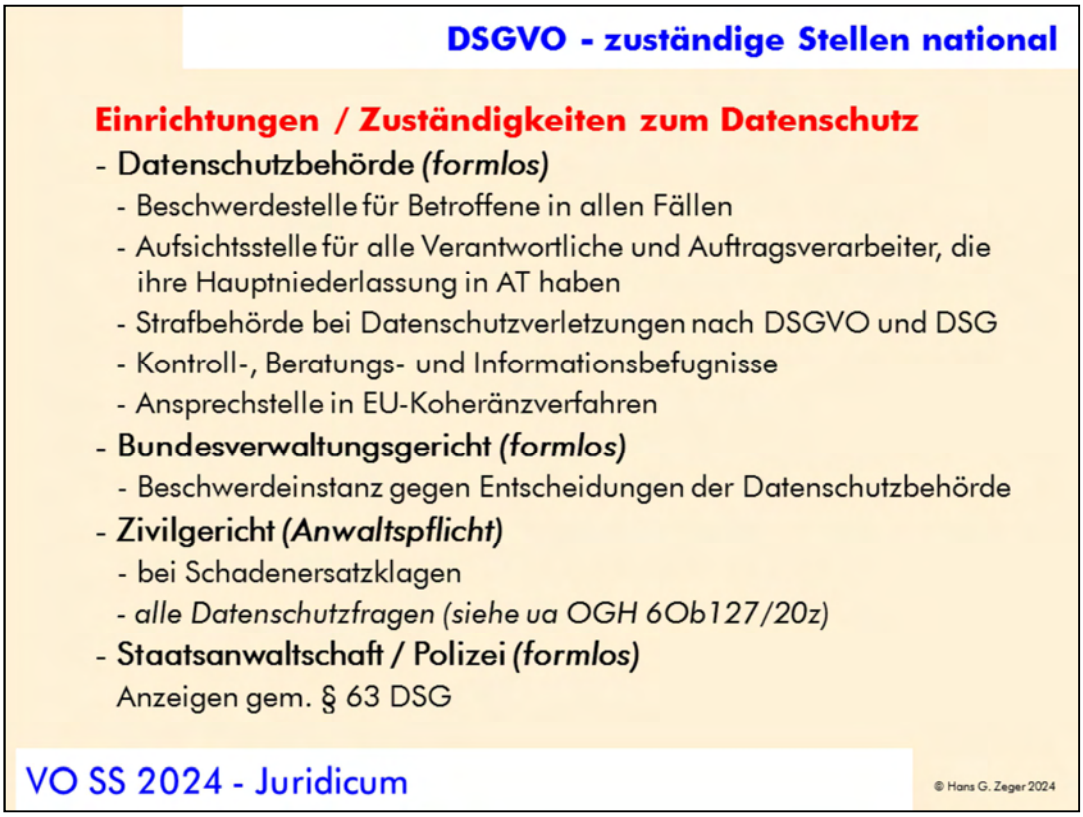
(1)Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

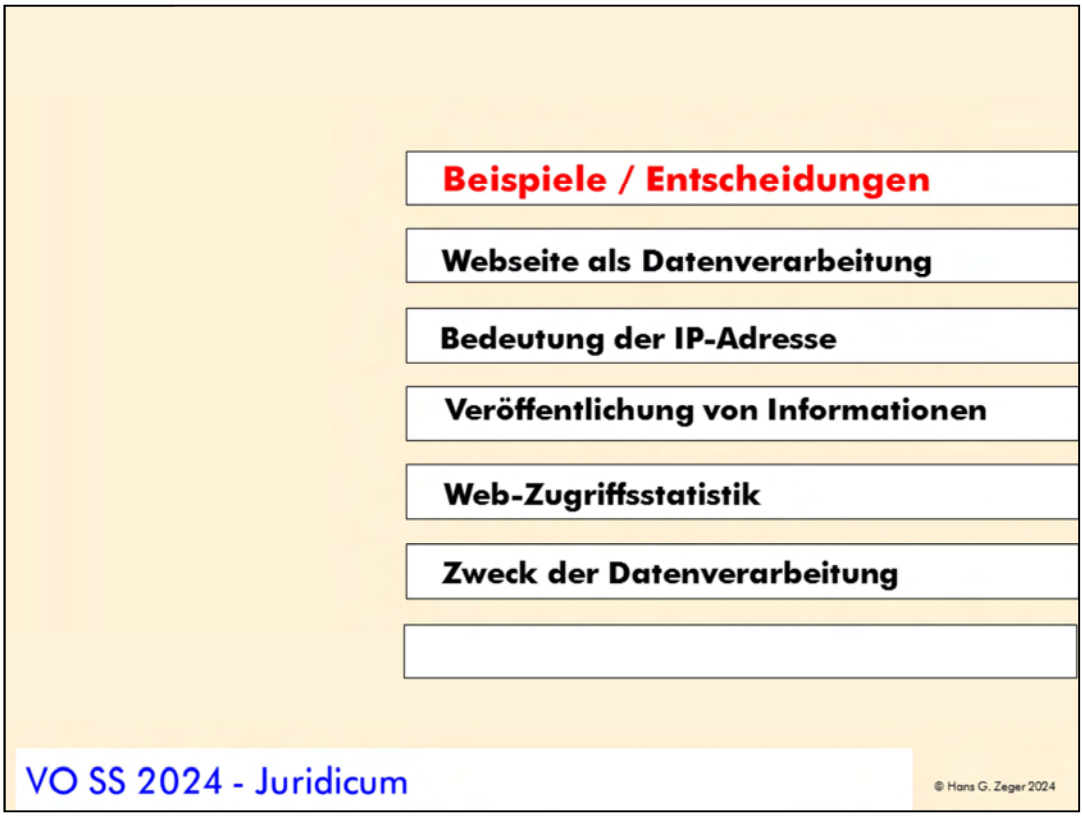
-



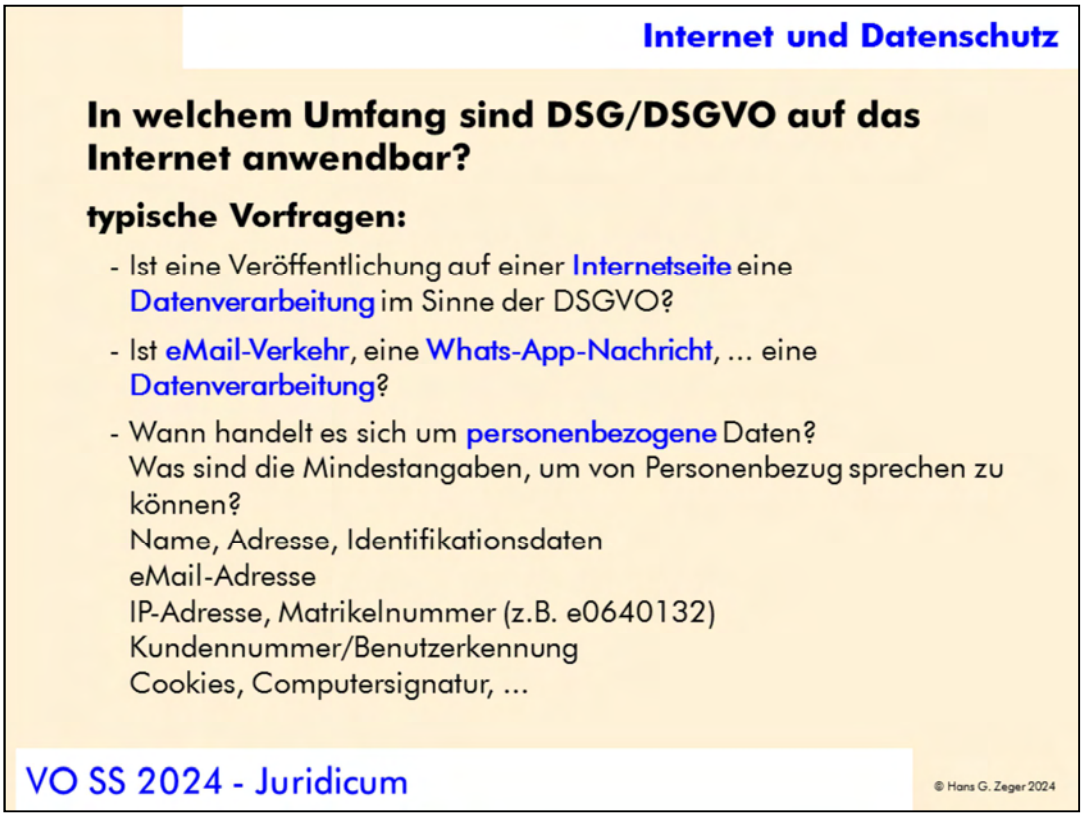
Zivilgerichte / Landesgerichte zuständig:

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

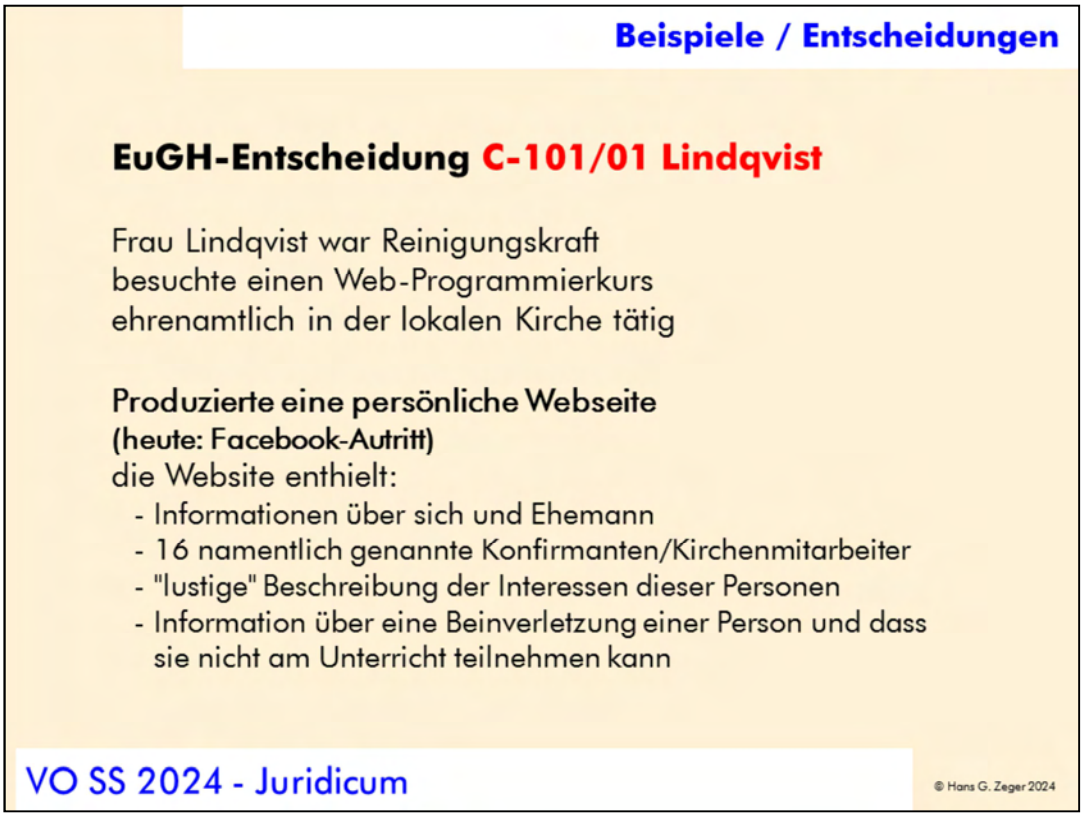
(http://www.bmj.gv.at/_cms_upload/_docs/gerichte_und_behoerden2005.pdf)


Beispiele / Entscheidungen
Webseite als Datenverarbeitung
Bedeutung der IP-Adresse
Veröffentlichung von Informationen
Web-Zugriffsstatistik
Zweck der Datenverarbeitung
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

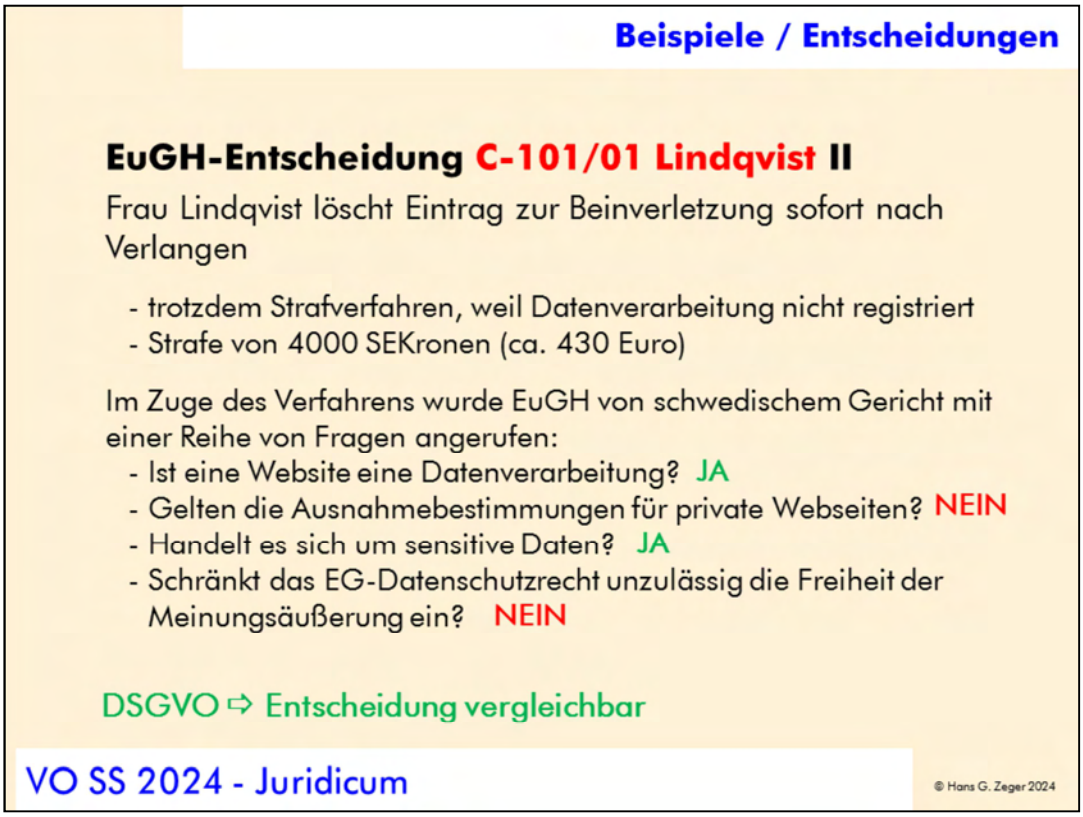
-


Internet und Datenschutz
In welchem Umfang sind DSG/DSGVO auf das Internet anwendbar?
typische Vorfragen:
- Ist eine Veröffentlichung auf einer Internetseite eine Datenverarbeitung im Sinne der DSGVO?
- Ist eMail-Verkehr, eine Whats-App-Nachricht, ... 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, ...
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Beispiele / Entscheidungen
EuGH-Entscheidung C-101/01 Lindqvist
Frau Lindqvist war Reinigungskraft
besuchte einen Web-Programmierkurs
ehrenamtlich in der lokalen Kirche tätig
Produzierte eine persönliche Webseite
(heute: Facebook-Autritt)
die Website enthielt:
- 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-



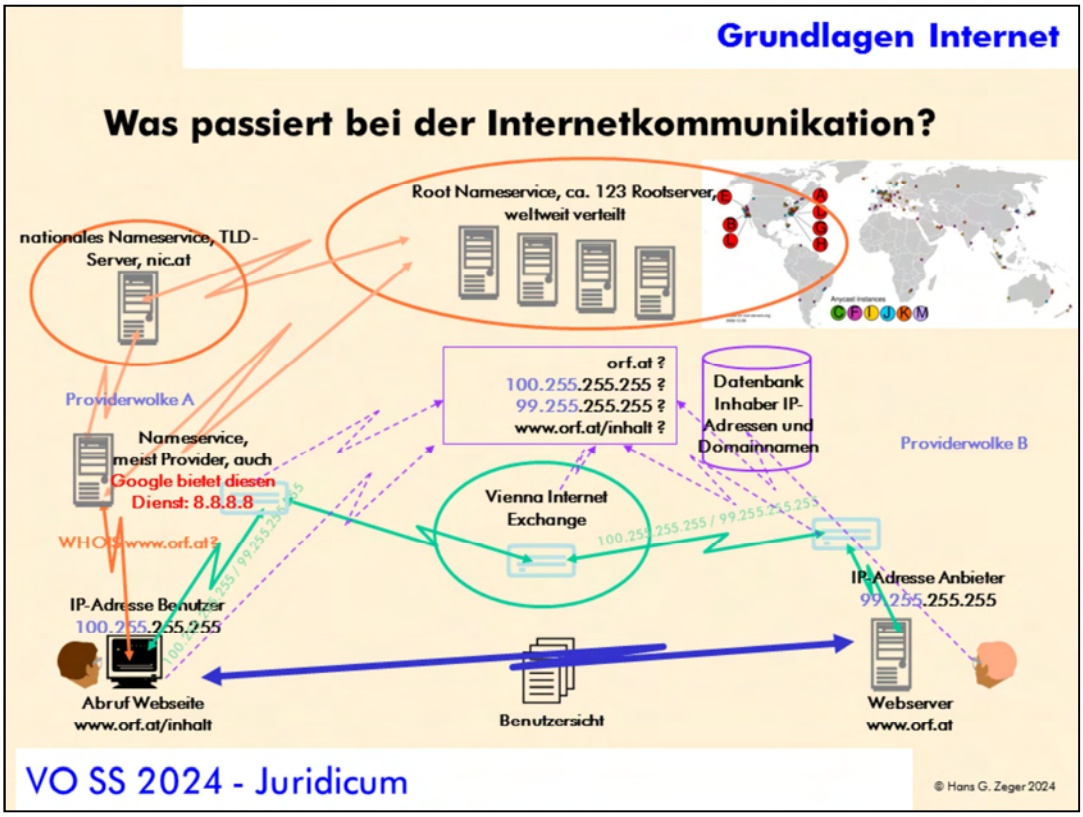
Ausnahme des Art. 3 Abs. 2 95/46/EG (Anwendungsbereich):

...

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

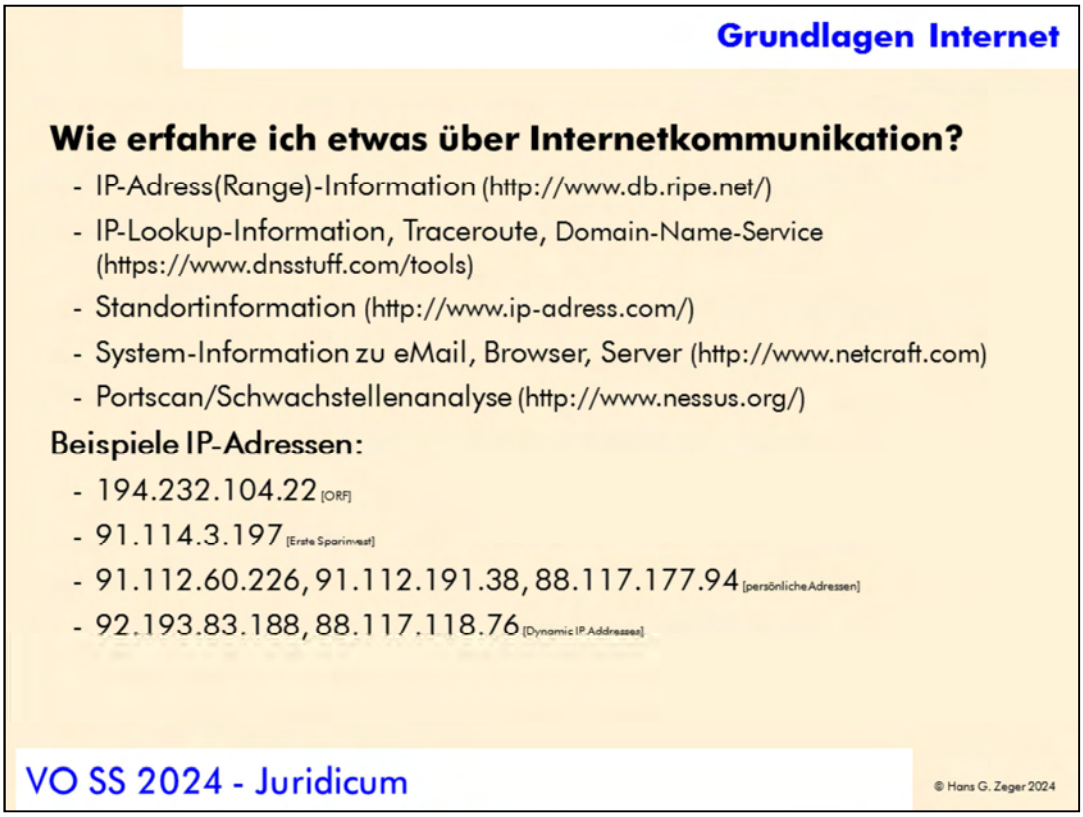
...

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

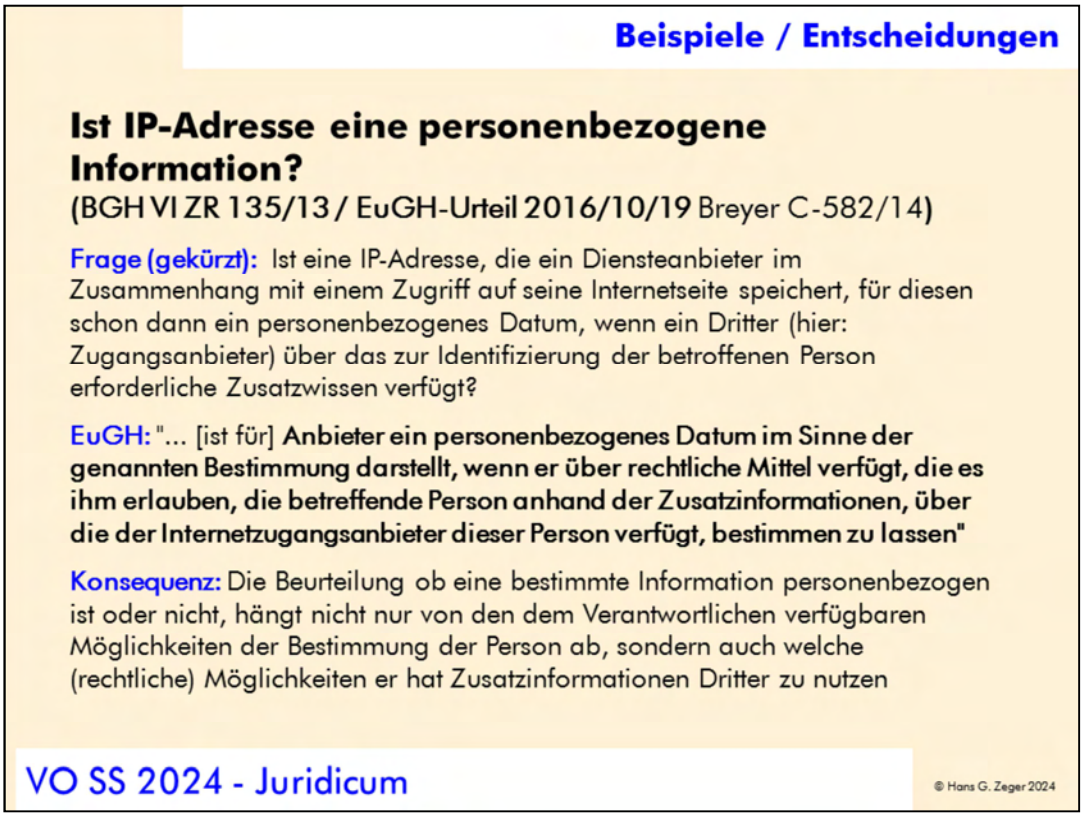


Betreiber eines weltweit agierenden "zentralen" Nameservers hätte einen Überblick über die weltweiten Datenströme.

Google bietet mit 8.8.8.8 ein derartiges zentrales Nameservice an


Grundlagen Internet
Wie erfahre ich etwas über Internetkommunikation?
- IP-Adress(Range)-Information (http://www.db.ripe.net/)
- IP-Lookup-Information, Traceroute, Domain-Name-Service (https://www.dnsstuff.com/tools)
- 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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

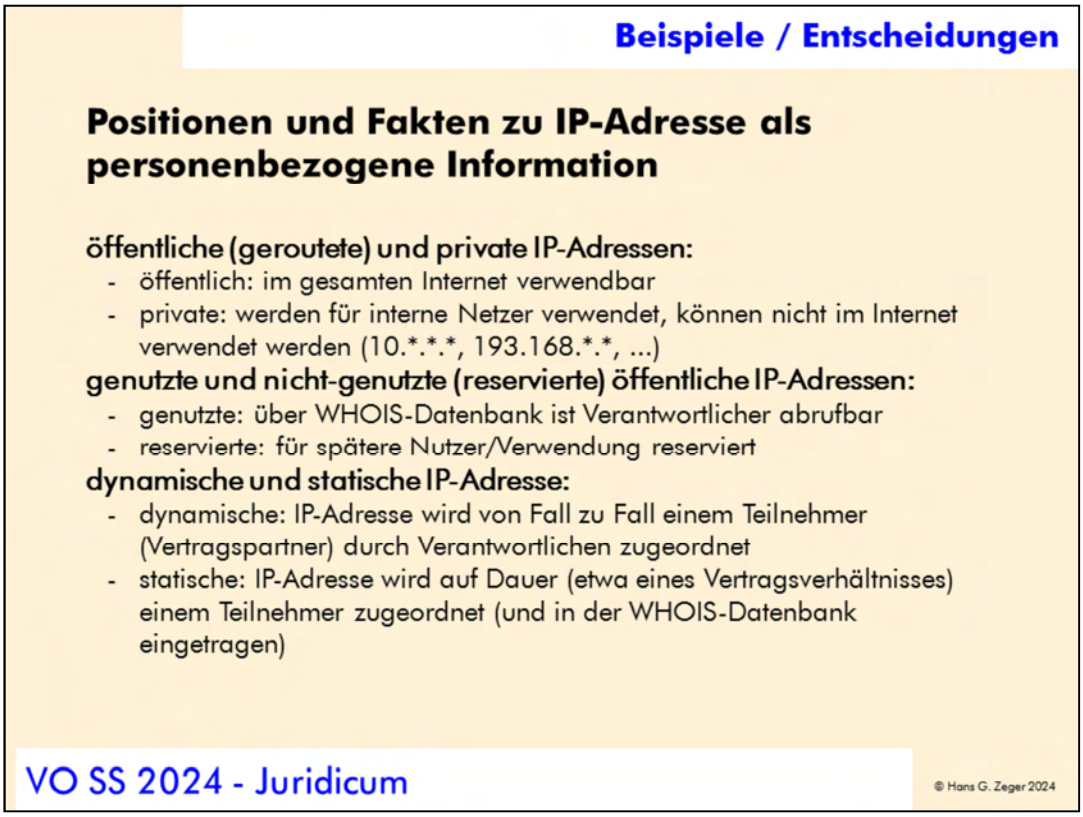
1. Ist Art.2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verar-beitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG 1995, L 281/31) Datenschutz-Richtlinie - dahin auszulegen, dass eine Internetprotokoll-Adresse (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?

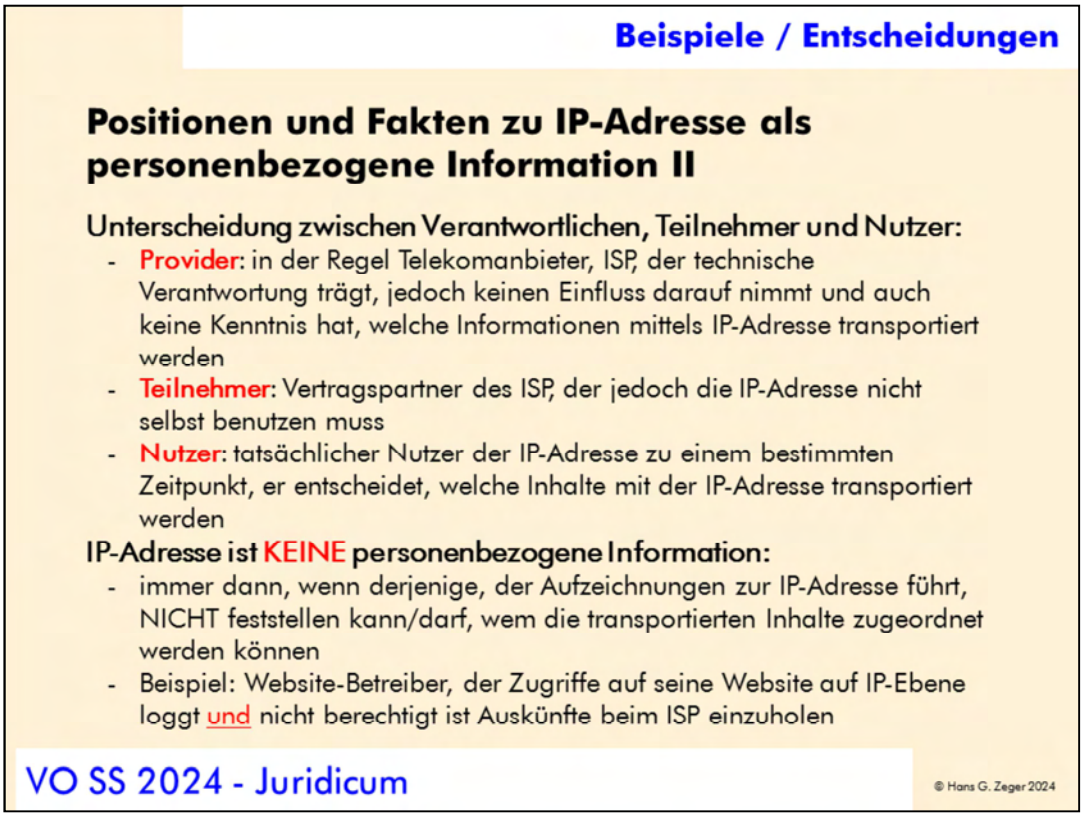
BGH, Beschluss vom 28. Oktober 2014 - VI ZR 135/13 - LG Berlin, AG Berlin-Mitte

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

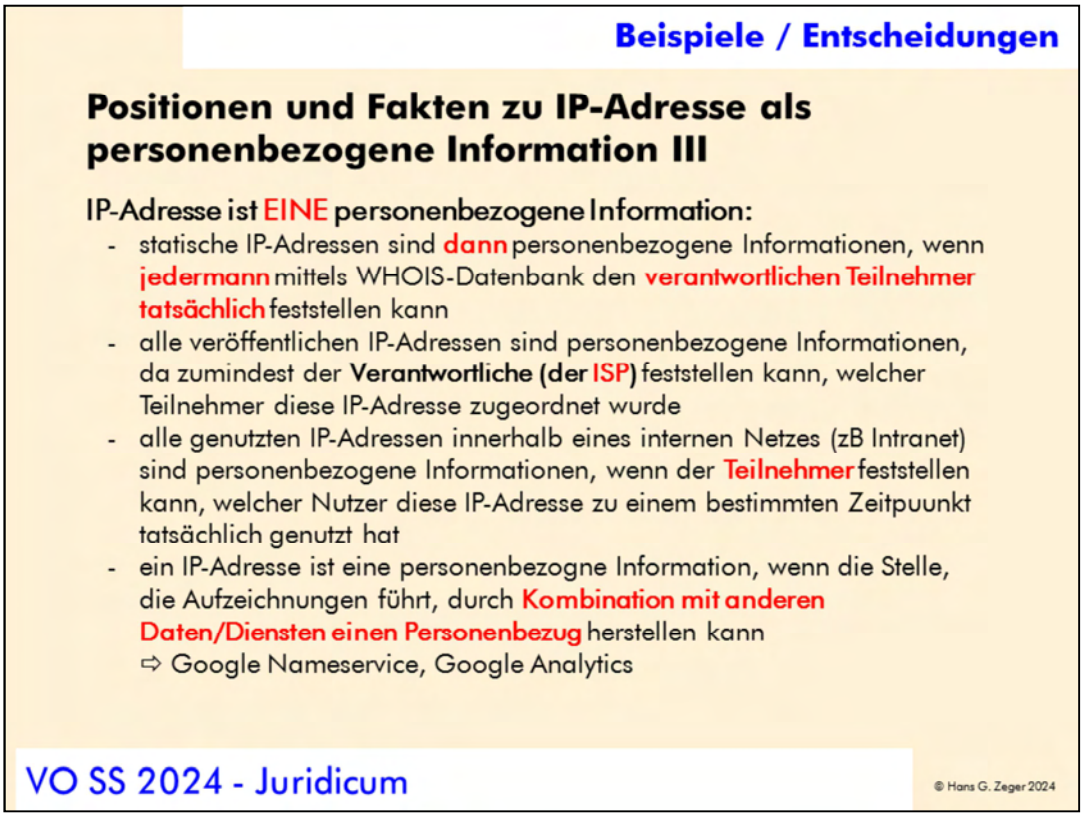
ad Frage 1. Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem 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
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)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

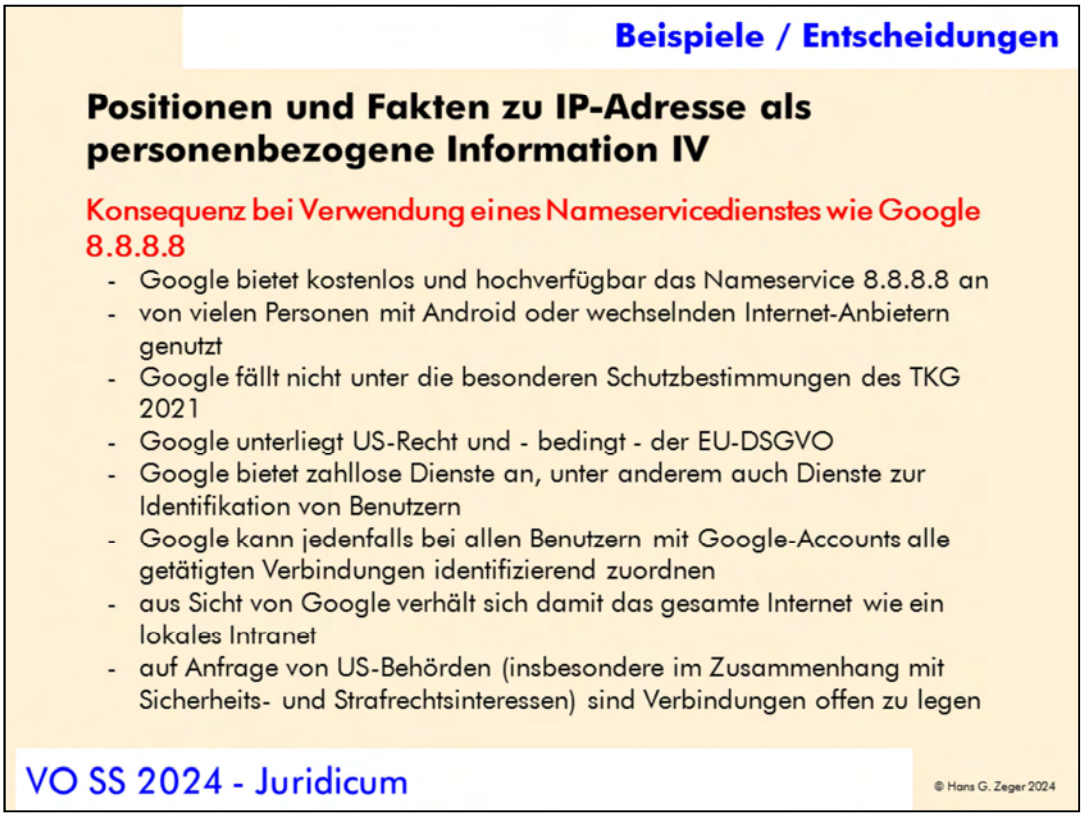
-


Beispiele / Entscheidungen
Positionen und Fakten zu IP-Adresse als personenbezogene Information II
Unterscheidung zwischen Verantwortlichen, Teilnehmer und Nutzer:
- Provider: in der Regel Telekomanbieter, ISP, der technische Verantwortung 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, wem die transportierten Inhalte zugeordnet werden können
- Beispiel: Website-Betreiber, der Zugriffe auf seine Website auf IP-Ebene loggt und nicht berechtigt ist Auskünfte beim ISP einzuholen
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Beispiele / Entscheidungen
Positionen und Fakten zu IP-Adresse als personenbezogene Information III
IP-Adresse ist EINE personenbezogene Information:
- statische IP-Adressen sind dann personenbezogene Informationen, wenn jedermann mittels WHOIS-Datenbank den verantwortlichen Teilnehmer tatsächlich feststellen kann
- alle veröffentlichen IP-Adressen 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
- ein IP-Adresse ist eine personenbezogne Information, wenn die Stelle, die Aufzeichnungen führt, durch Kombination mit anderen Daten/Diensten einen Personenbezug herstellen kann
⇨ Google Nameservice, Google Analytics
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Beispiele / Entscheidungen
Positionen und Fakten zu IP-Adresse als personenbezogene Information IV
Konsequenz bei Verwendung eines Nameservicedienstes wie Google 8.8.8.8
- Google bietet kostenlos und hochverfügbar das Nameservice 8.8.8.8 an
- von vielen Personen mit Android oder wechselnden Internet-Anbietern genutzt
- Google fällt nicht unter die besonderen Schutzbestimmungen des TKG 2021
- Google unterliegt US-Recht und - bedingt - der EU-DSGVO
- Google bietet zahllose Dienste an, unter anderem auch Dienste zur Identifikation von Benutzern
- Google kann jedenfalls bei allen Benutzern mit Google-Accounts alle getätigten Verbindungen identifizierend zuordnen
- aus Sicht von Google verhält sich damit das gesamte Internet wie ein lokales Intranet
- auf Anfrage von US-Behörden (insbesondere im Zusammenhang mit Sicherheits- und Strafrechtsinteressen) sind Verbindungen offen zu legen
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-

Auszug aus BvwG W245 2252208-1

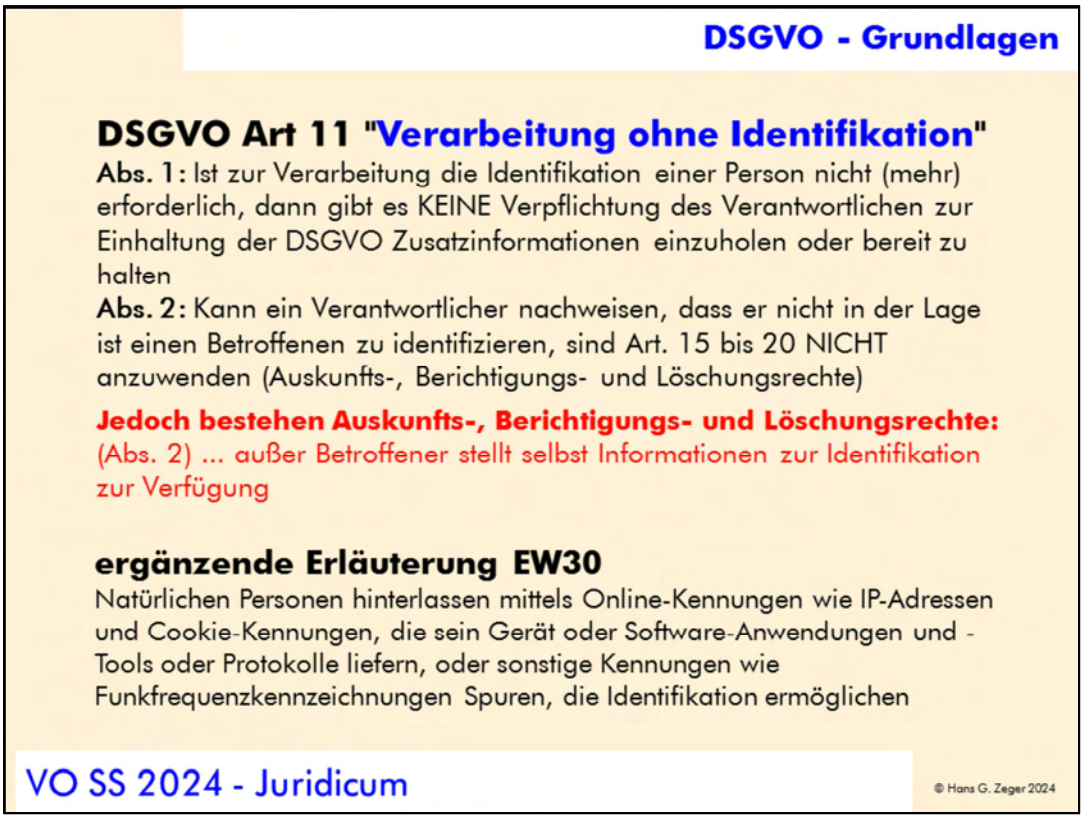
II.1.3.1. Zur zusammenfassenden Darstellung der Informationen, welche am 14.08.2020 der BF2 übermittelt wurden:
Als Folge der Implementierung des Tools XXXX -Analytics wurden am 14.08.2020 – zusammengefasst – folgende Informationen vom Browser des BF1, der die Website XXXX besucht hat, an die Server der BF2 übermittelt:
· einzigartige Online-Kennungen (unique identifier), die sowohl den Browser bzw. das Gerät des BF1 als auch die MB (durch die XXXX -Analytics-Account-ID der MB als Websitebetreiberin) identifizieren;
· die Adresse und den HTML-Titel der Website sowie die Unterseiten, die der BF1 besucht hat;
· Informationen zum Browser, Betriebssystem, Bildschirmauflösung, Sprachauswahl sowie Datum und Uhrzeit des Website-Besuchs;
· die IP-Adresse des Geräts, welches der BF1 verwendet hat.
...
Wenn nämlich dem Wunsch eines XXXX -Account-Nutzers nach „Personalisierung" der erhaltenen Werbeinformationen aufgrund einer Willenserklärung im Konto entsprochen werden kann, so besteht aus rein technischer Sicht die Möglichkeit, die Information über die besuchte Website des XXXX -Account-Nutzers zu erhalten.

Unabhängig davon standen der BF2 am 14.08.2020 zahlreiche Metadaten zur Verfügung (OZ 25 zu W245 2252208-1, Seite 3), die bei einem Aufruf einer Anwendung (wie z.B. XXXX -Konto) übermittelt werden. Im verfahrensgegenständlichen Zeitpunkt (14.08.2020) hat der BF1 auch sein XXXX -Konto genutzt. Mit den Metadaten, welche bei der Nutzung des XXXX -Kontos übermittelt wurden, war eine Verknüpfung mit den übermittelten Metadaten im Zuge des XXXX (über XXXX -analytics) möglich.

Zudem war zweifelsfrei eine Verknüpfung mit der IP-Adresse möglich. Der BF1 hat am 14.08.2020 im Homeoffice gearbeitet. In diesem Zusammenhang wurde die IP-Adresse direkt vom BF1 der BF2 übermittelt (Verhandlungsprotokoll vom 31.03.2022, OZ 29 zu W245 2252208, Seite 14). Da der BF1 bei seinem Besuch der Website XXXX (XXXX -Analytics) gleichzeitig im XXXX -Konto angemeldet war, kann zwischen diesen Anwendungen problemlos eine Verknüpfung über die IP-Adresse hergestellt werden. Bei beiden Anwendungen wird die IP-Adresse schon aus technischen Gründen übertragen. Vor diesem Hintergrund kann auf Grund der Übertragung der IP-Adresse über die Anwendung XXXX -Analytics, ein Personenbezug zum XXXX -Konto (bzw. zu den Anmeldeinformationen des BF1) hergestellt werden. Da der BF1 zu diesem Zeitpunkt im Homeoffice gearbeitet hat und er alleine lebt, konnte nur er die übermittelte IP-Adresse nutzen.

Aufgrund der einfachen Verknüpfbarkeit von Metadaten und IP-Adresse zwischen den einzelnen Anwendungen (XXXX -Konto und XXXX -Analytics) kann unstrittig ein Personenbezug (Anmeldedaten zum XXXX) hergestellt werden.

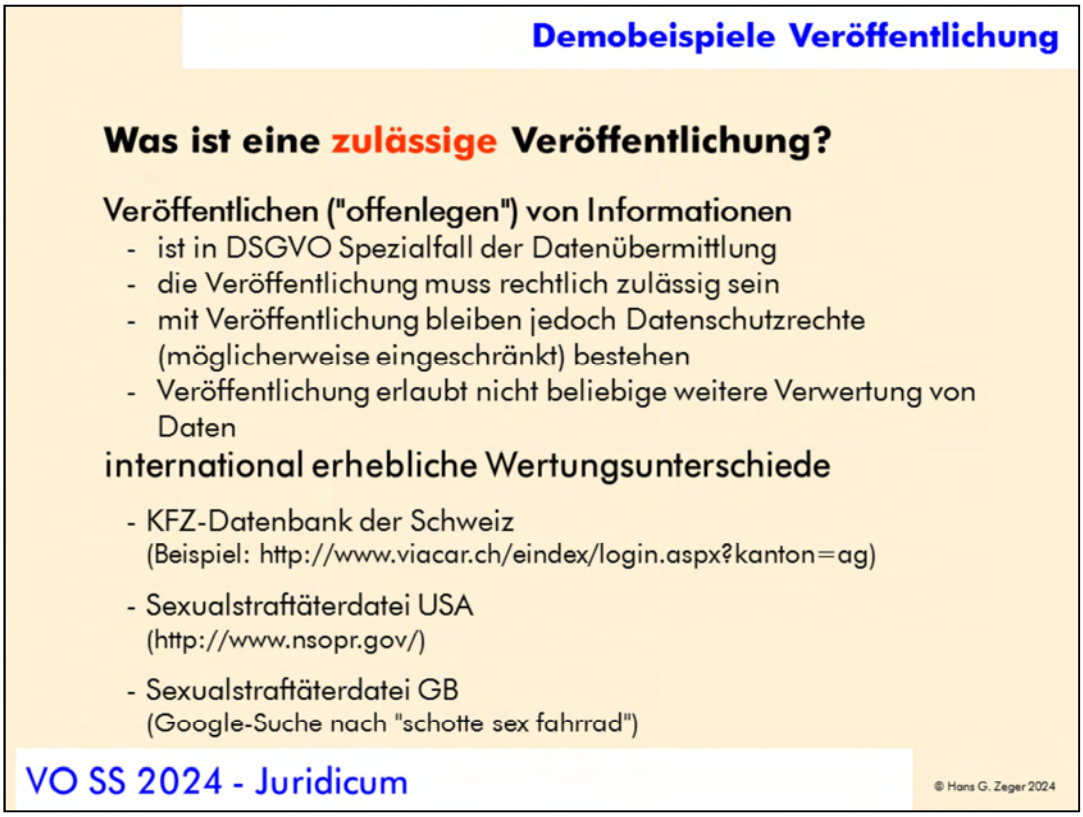
Auch war festzustellen, dass Metadaten von XXXX -Anwendungen (wie z.B. XXXX -Account) in die Vereinigten Staaten übertragen wurden, die der BF1 am 14.08.2020 genutzt hat (Verhandlungsprotokoll vom 31.03.2022, OZ 29 zu W245 2252208, Seite 11 f).



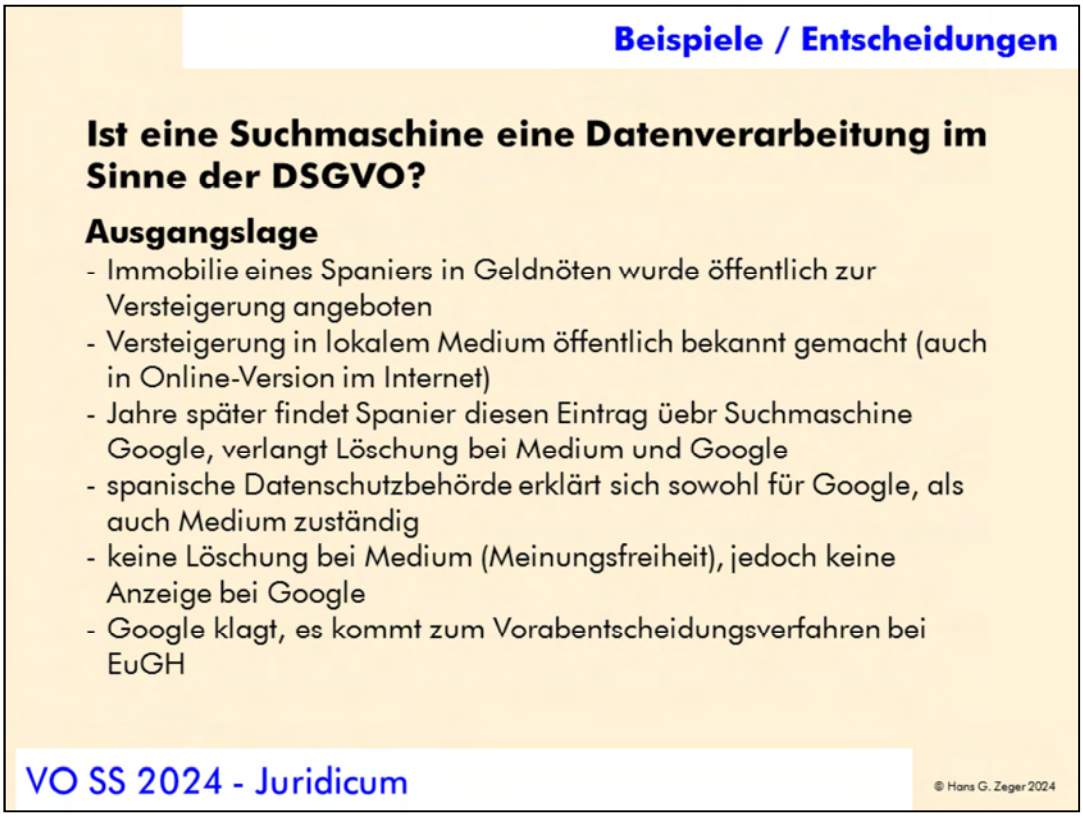
DSGVO Art. 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

(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
- mit Veröffentlichung bleiben jedoch Datenschutzrechte (möglicherweise eingeschränkt) bestehen
- Veröffentlichung erlaubt nicht beliebige weitere Verwertung von Daten
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")
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

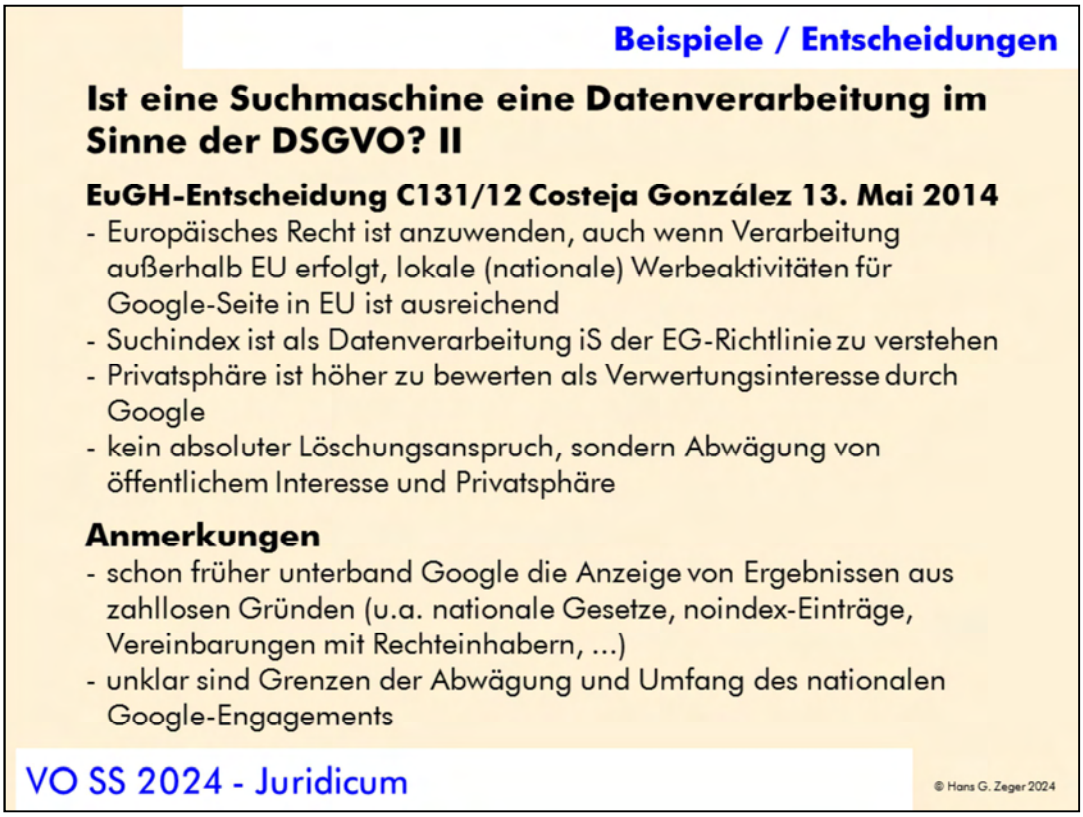
-



Entscheidung EuGH 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.



Entscheidung EuGH 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.

Was ist eine personenbezogene Veröffentlichung?

Mittwoch, 29.10.14 | 11

Inkasso-Bande schickt Unternehmer Schläger-Truppe!

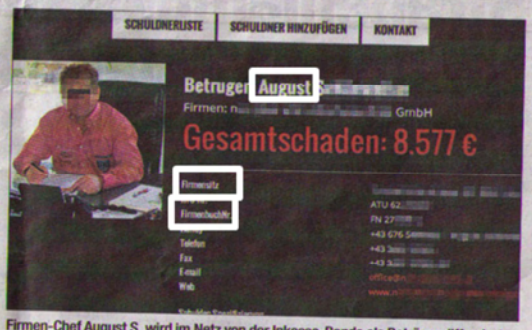
Um Schulden einzutreiben, schwärzte ein Inkassobüro einen Steirer im Internet als „Betrüger" an. Ein Rollkommando stürmte sein Büro und drohte August S. (50), ihm die Kehle durchzuschneiden!

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 Peterthaler

„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



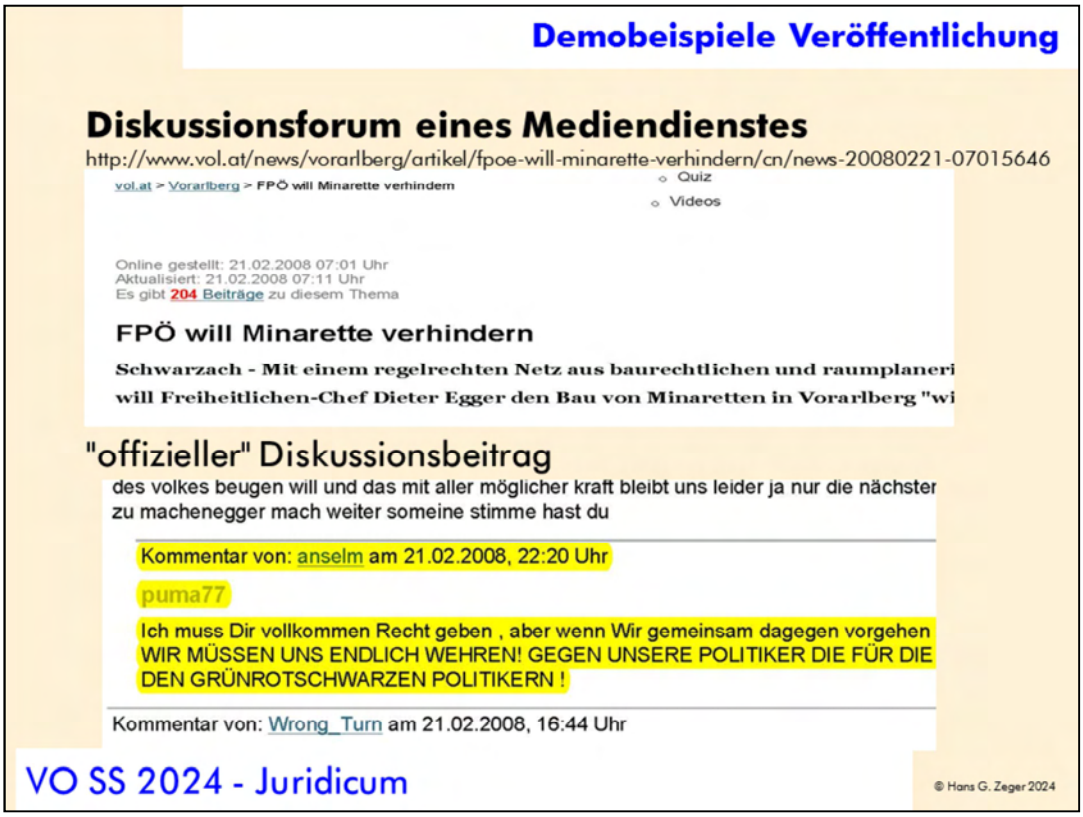
Firmen-Chef August S. wird im Netz von der Inkasso-Bande als Betrüger diffamiert.

VO SS 2024 - Juridicum

-


Was ist eine personenbezogene Veröffentlichung?
verwendete Suchworte: firmensitz firmenbuchnr august
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 S[redacted] | betruger.at
betruger.at/defaulter/august-so[redacted]/
Firmensitz: Trauterfelserstrasse 281 8952 Irdning. ATU Nr. ATU 62255669 FirmenbuchNr. FN 27[redacted] Handy: +43 676 5666665 – August S[redacted]
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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-



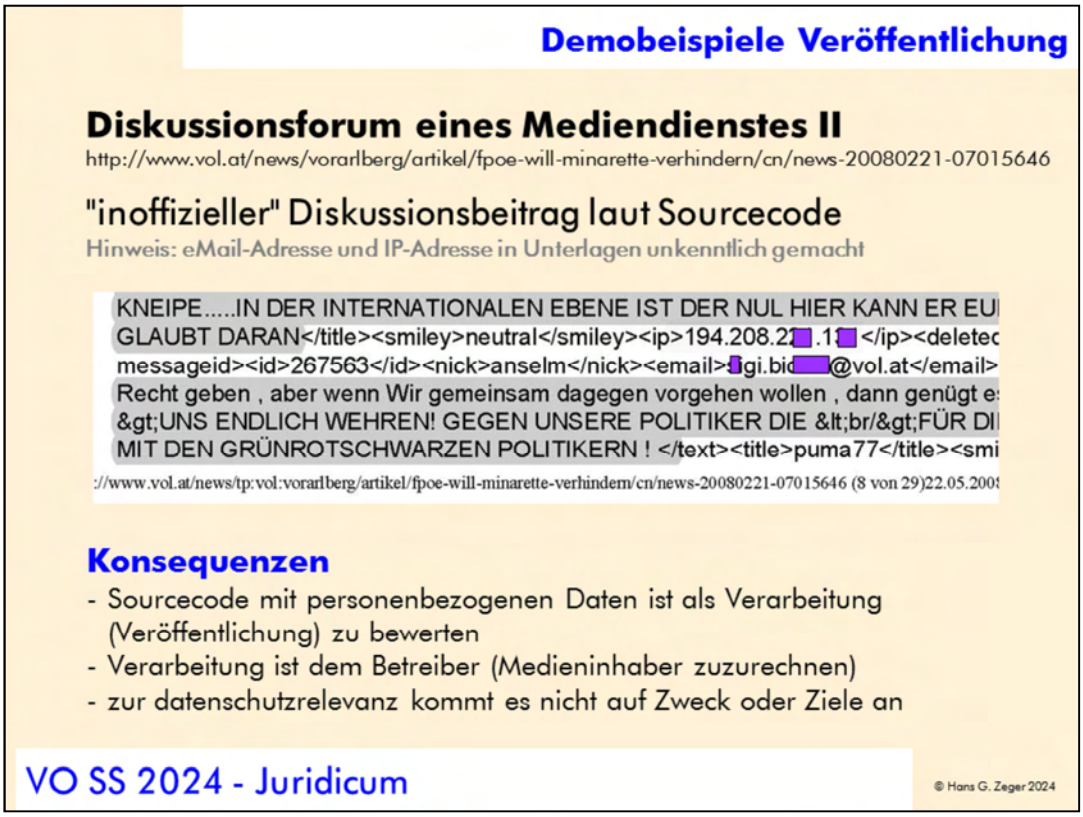
Offizielle Version:

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</

Googles Street-View

Aufzeichnung "öffentlichen" Verhaltens

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

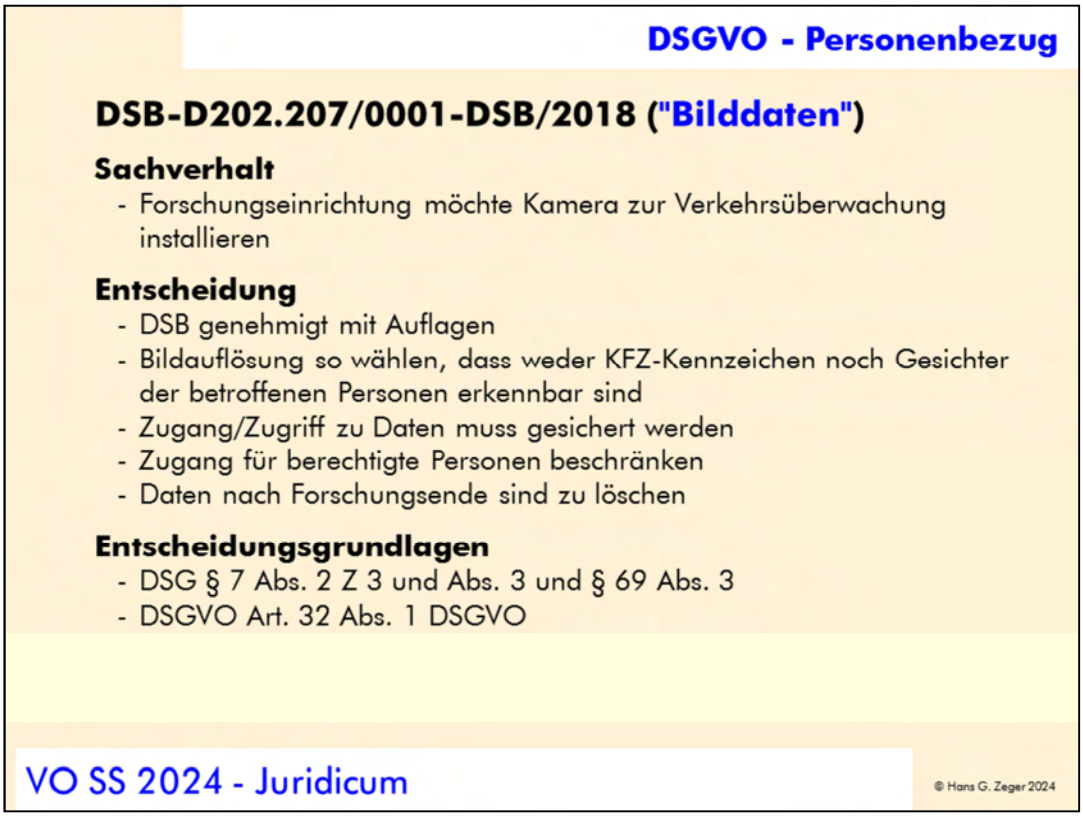
- handelt es sich überhaupt um personenbezogene Datenverarbeitung?
- Google sagt zu, Personen vor Veröffentlichung zu "verpixeln"

VO SS 2024 - 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-



DSB-D202.207/0001-DSB/2018

Die ehemalige Datenschutzkommission hat bereits mehrfach festgestellt, dass Bilddaten (bestimmbare) personenbezogene Daten sind (vgl. etwa die Ausführungen zum ehemaligen § 4 Z DSG 2000 im Bescheid der DSK vom 21. Jänner 2009, GZ K121.425/0003-DSK/2009). Diese Erwägungen lassen sich auch auf Art. 4 Z 1 DSGVO umlegen. Die DSGVO ist somit einschlägig. Gleichzeitig liegt mit diesen Bilddaten aber keine Verarbeitung besonderer Kategorien personenbezogener Daten iSd Art. 9 DSGVO vor (vgl. die Ausführungen zum ehemaligen § 4 Z 2 DSG 2000 den Bescheid der DSK vom 10. April 2013, GZ K202.120/0002-DSK/2013).

Bilddaten sollen nun für wissenschaftliche Zwecke ermittelt und ausgewertet werden. Die Verwendung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik unterliegt der Sondervorschrift des § 7 DSG (und richtet sich nicht nach den §§ 12 und 13 DSG, die die Bildverarbeitung zu anderen Zwecken regeln). Aus dem festgestellten Sachverhalt ergibt sich, dass die Voraussetzungen des § 7 Abs. 1 und Abs. 2 Z 1 und Z 2 nicht vorliegen, sodass die geplante Datenverwendung nur aufgrund einer Genehmigung durch die Datenschutzbehörde gemäß § 7 Abs. 2 Z 3 iVm Abs. 3 DSG erfolgen kann.

2. Voraussetzungen der Genehmigung nach § 7 Abs. 3 DSG

Die Verwendung personenbezogener Daten für wissenschaftliche Zwecke ist gemäß § 7 Abs. 3 DSG dann zulässig, wenn eine Genehmigung der Datenschutzbehörde hierfür vorliegt, wobei gemäß Abs. 3 leg. cit. folgende Voraussetzungen für die Erteilung der Genehmigung gegeben sein müssen:

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird.

...


Social Media und Datenschutz
facebook
E-Mail-Adresse oder Ha
Passwort
vergessen?
Daniel Demant
Ralph K. Bauer
Sigmar Gabriel
Alexander Lingsch
Ich dachte erst Heilbronn...
Ralph K. Bauer
... aber was machen wir da?
Melde dich ... der registriere dich bei Facebook, um dich mit Freunden, Verwandten und Personen, die du kenn...
Anmelden
oder
Neues Konto erstellen
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

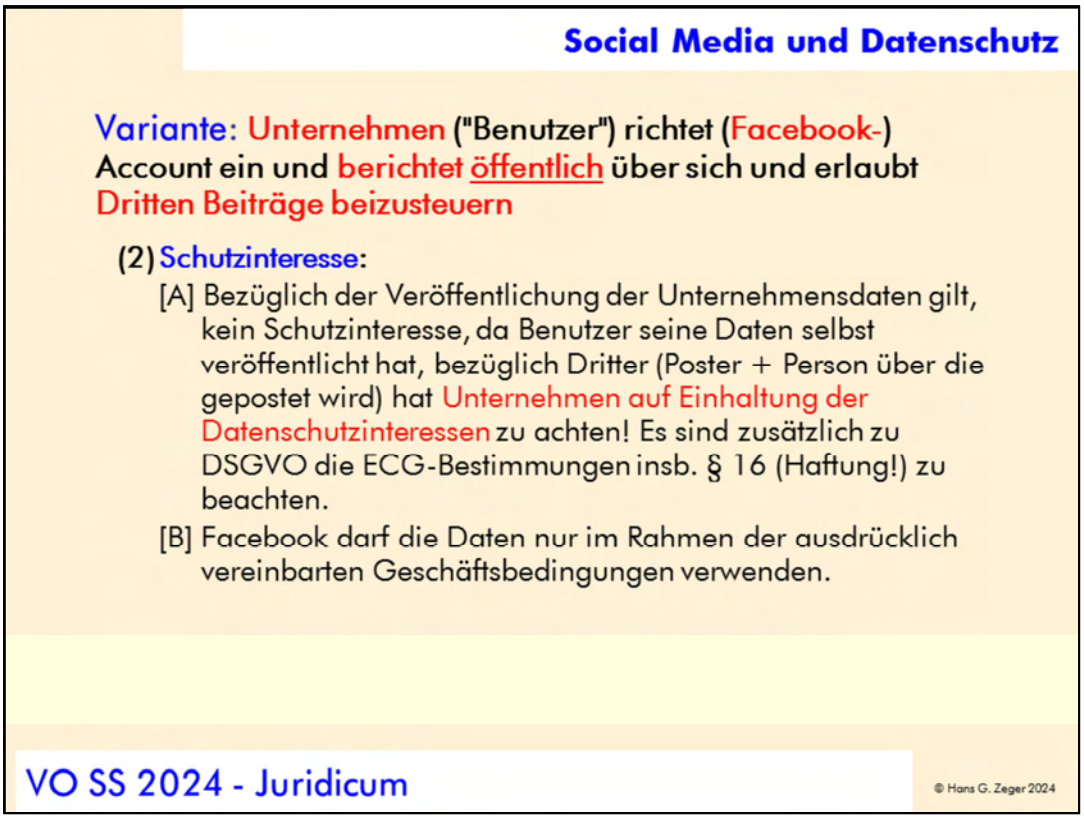
-


Social Media und Datenschutz
Datenschutzspezifische Fragestellungen
Vorgaben DSGVO:
(1) Rollenkonzept: Verantwortlicher, Betroffener, Auftragsverarbeiter
(2) Schutzinteressen der persönlichen Daten: allgemein verfügbare Daten, pseudonymisierte Daten, vertrauliche Daten, Daten besonderer Kategorien
(3) berechtigter Zweck: Meinungsfreiheit / Meinungsbildung, persönliche Kommunikation, Förderung des Erwerbs / Werbung, politische, weltanschauliche, religiöse Betätigung
(4) Aufsicht: keine vorbeugende Aufsicht, potentiell Genehmigung eines internationalen Datenverkehrs / Konsultation bei Datenschutzfolgenabschätzung erforderlich Datenschutzbehörde jedoch grundsätzlich zuständig
Datenschutzregeln treffen sowohl Betreiber des Accounts ("Benutzer" [A]), als auch Plattformbetreiber ("Facebook" [B]),
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

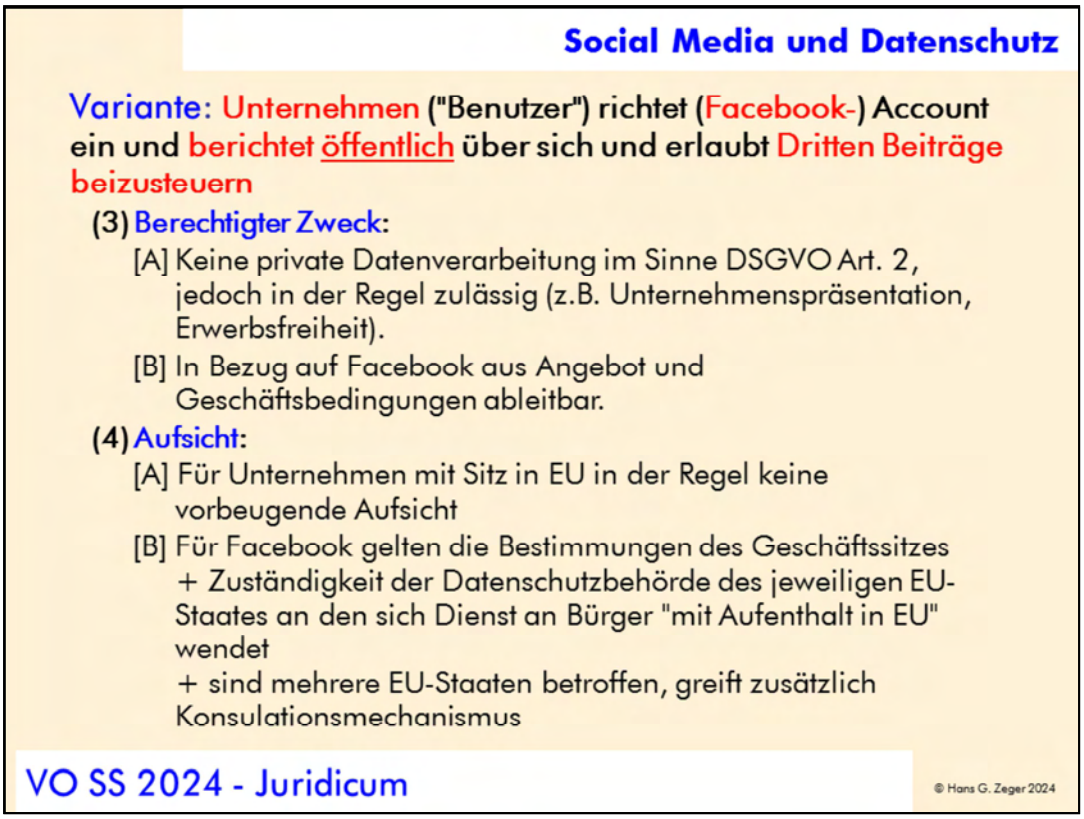
-


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 SS 2024 - Juridicum
© Hans G. Zeger 2024

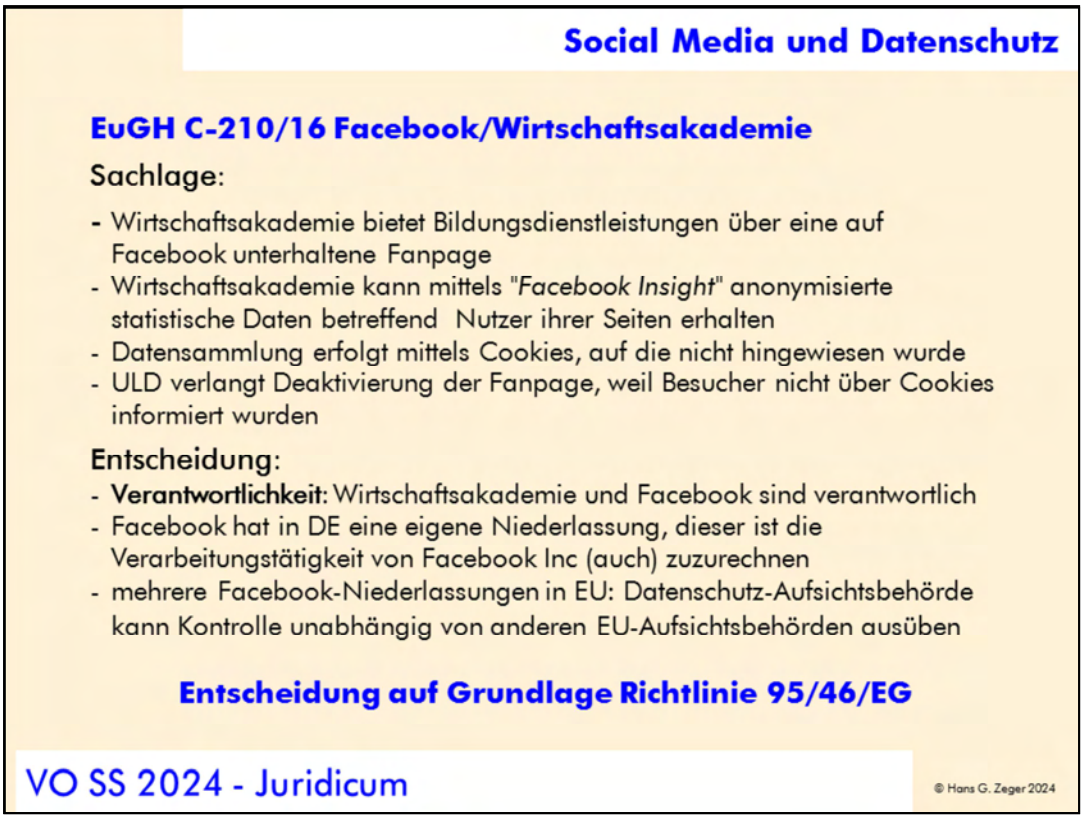
-


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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-


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 + Zuständigkeit der Datenschutzbehörde des jeweiligen EU-Staates an den sich Dienst an Bürger "mit Aufenthalt in EU" wendet
+ sind mehrere EU-Staaten betroffen, greift zusätzlich Konsulationsmechanismus
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



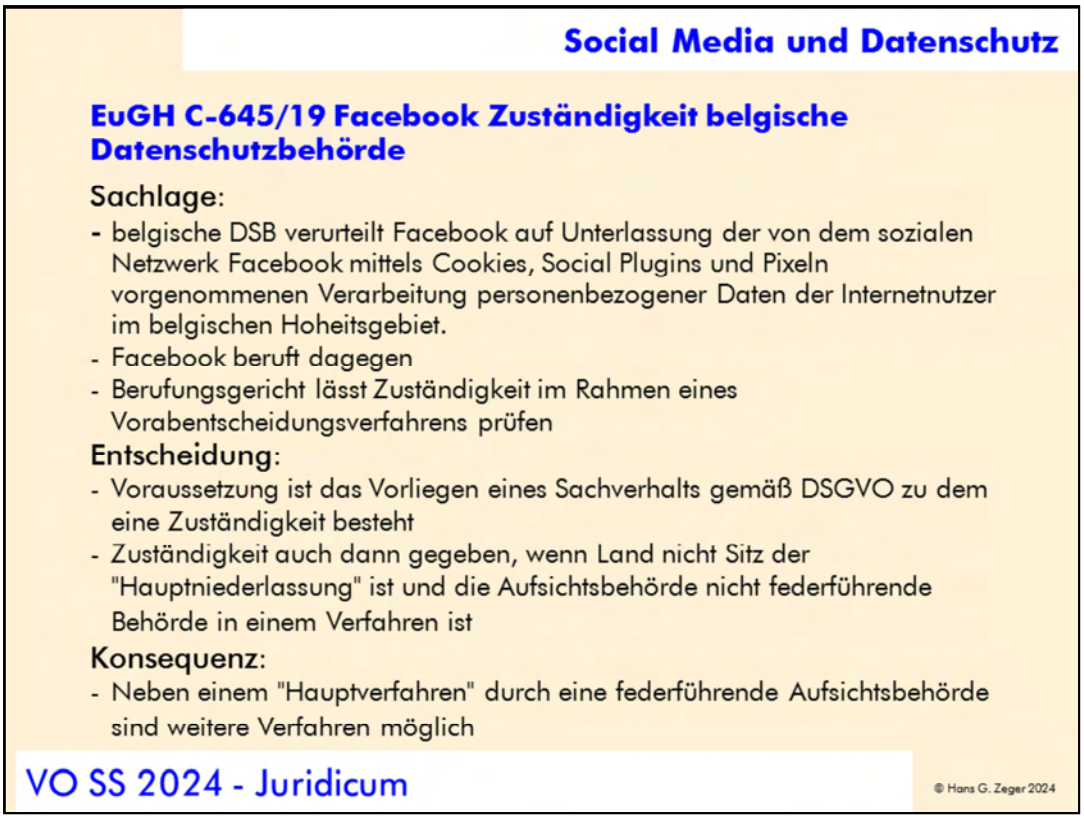
C-210/16 Anordnung zur Deaktivierung einer Facebook-Seite (Fanpage)

... hat der Gerichtshof (Große Kammer) für Recht erkannt:

1. Art. 2 Buchst. 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 der Begriff des „für die Verarbeitung Verantwortlichen" im Sinne dieser Bestimmung den Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage umfasst.

2. Die Art. 4 und 28 der Richtlinie 95/46 sind dahin auszulegen, dass dann, wenn ein außerhalb der Europäischen Union ansässiges Unternehmen mehrere Niederlassungen in verschiedenen Mitgliedstaaten unterhält, die Kontrollstelle eines Mitgliedstaats zur Ausübung der ihr durch Art. 28 Abs. 3 dieser Richtlinie übertragenen Befugnisse gegenüber einer im Hoheitsgebiet dieses Mitgliedstaats gelegenen Niederlassung dieses Unternehmens auch dann befugt ist, wenn nach der konzerninternen Aufgabenverteilung zum einen diese Niederlassung allein für den Verkauf von Werbeflächen und sonstige Marketingtätigkeiten im Hoheitsgebiet dieses Mitgliedstaats zuständig ist und zum anderen die ausschließliche Verantwortung für die Erhebung und Verarbeitung personenbezogener Daten für das gesamte Gebiet der Europäischen Union einer in einem anderen Mitgliedstaat gelegenen Niederlassung obliegt.

3. Art. 4 Abs. 1 Buchst. a und Art. 28 Abs. 3 und 6 der Richtlinie 95/46 sind dahin auszulegen, dass die Kontrollstelle eines Mitgliedstaats, wenn sie beabsichtigt, gegenüber einer im Hoheitsgebiet dieses Mitgliedstaats ansässigen Stelle wegen Verstößen gegen die Vorschriften über den Schutz personenbezogener Daten, die von einem Dritten begangen wurden, der für die Verarbeitung dieser Daten verantwortlich ist und seinen Sitz in einem anderen Mitgliedstaat hat, die Einwirkungsbefugnisse nach Art. 28 Abs. 3 dieser Richtlinie auszuüben, zuständig ist, die Rechtmäßigkeit einer solchen Datenverarbeitung unabhängig von der Kontrollstelle des letztgenannten Mitgliedstaats zu beurteilen und ihre Einwirkungsbefugnisse gegenüber der in ihrem Hoheitsgebiet ansässigen Stelle auszuüben, ohne zuvor die Kontrollstelle des anderen Mitgliedstaats um ein Eingreifen zu ersuchen.



EuGH Entscheidung C-645/19 Zuständigkeit

1. Sind Art. 55 Abs. 1 und die Art. 56 bis 58 und 60 bis 66 der Verordnung 2016/679 in Verbindung mit den Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass eine Aufsichtsbehörde, die nach den in Umsetzung von Art. 58 Abs. 5 der Verordnung erlassenen nationalen Rechtsvorschriften befugt ist, bei Verstößen gegen die Verordnung eine Klage vor einem Gericht ihres Mitgliedstaats zu erheben, diese Befugnis bei einer grenzüberschreitenden Verarbeitung, bei der sie nicht die federführende Aufsichtsbehörde ist, nicht ausüben kann?

...

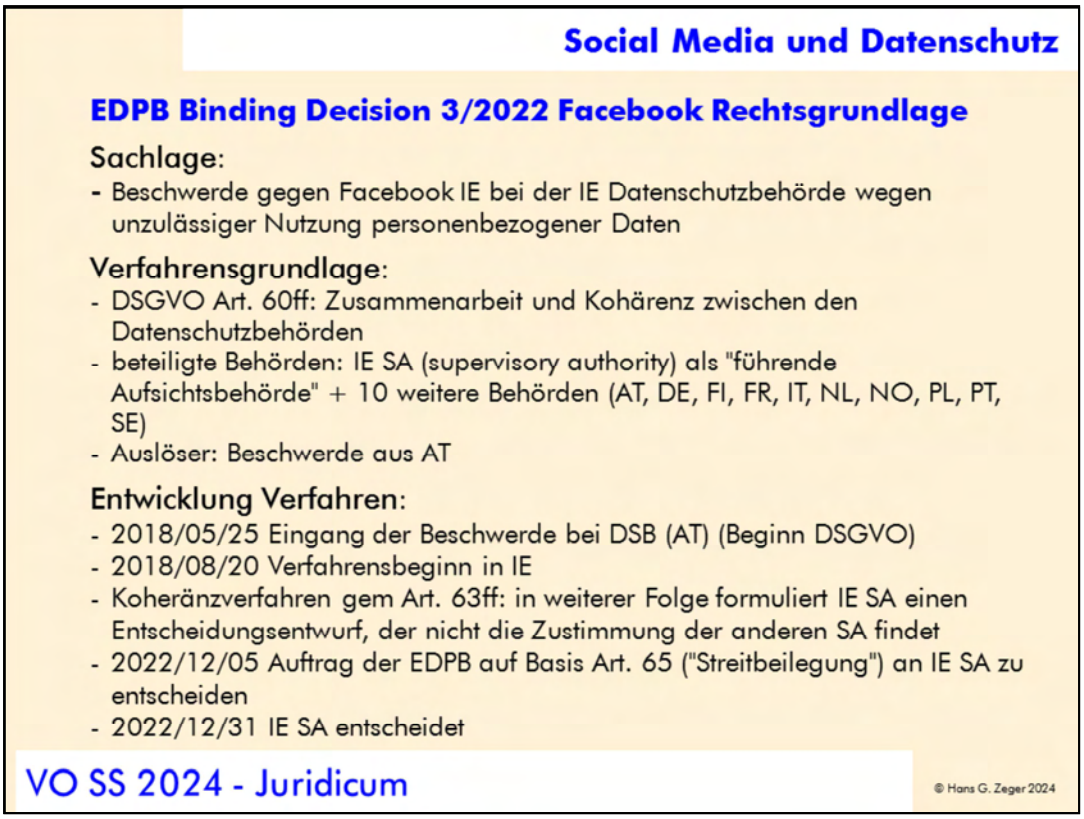
Nach alledem ist auf Frage 1 zu antworten, dass Art. 55 Abs. 1 und die Art. 56 bis 58 sowie 60 bis 66 der Verordnung 2016/679 in Verbindung mit den Art. 7, 8 und 47 der Charta dahin auszulegen sind, dass eine Aufsichtsbehörde eines Mitgliedstaats, die nach den zur Durchführung von Art. 58 Abs. 5 der Verordnung erlassenen nationalen Rechtsvorschriften befugt ist, vermeintliche Verstöße gegen die Verordnung einem Gericht dieses Mitgliedstaats zur Kenntnis zu bringen und gegebenenfalls die Einleitung eines gerichtlichen Verfahrens zu betreiben, von dieser Befugnis, wenn eine grenzüberschreitende Datenverarbeitung in Rede steht, Gebrauch machen darf, obgleich sie für diese Datenverarbeitung nicht die „zuständige federführende Aufsichtsbehörde“ im Sinne von Art. 56 Abs. 1 der Verordnung ist, sofern es sich um einen der Fälle handelt, in denen die Verordnung 2016/679 der Aufsichtsbehörde eine Zuständigkeit einräumt, einen Beschluss zu erlassen, mit dem festgestellt wird, dass die fragliche Verarbeitung gegen die Vorschriften der Verordnung verstößt, und die in der Verordnung vorgesehen Verfahren der Zusammenarbeit und der Kohärenz eingehalten werden.

2. Macht es dabei einen Unterschied, dass der für eine solche grenzüberschreitende Verarbeitung Verantwortliche in diesem Mitgliedstaat nicht seine Hauptniederlassung hat, wohl aber eine andere Niederlassung?

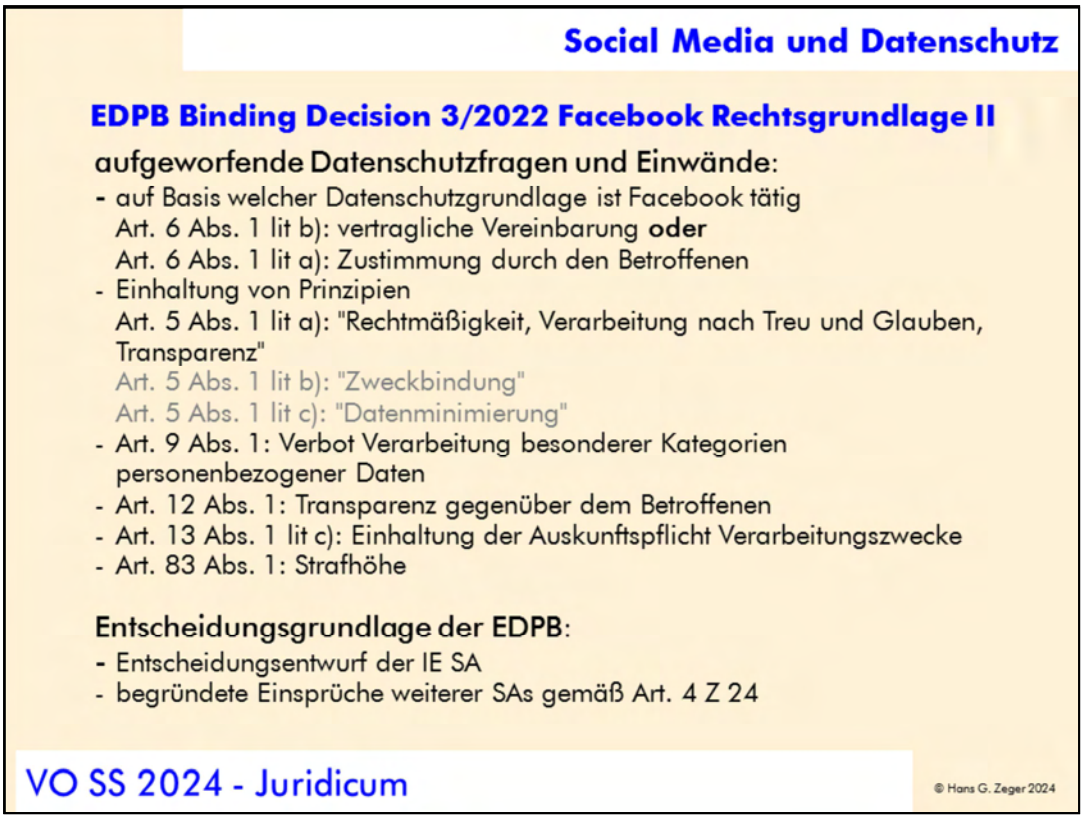
...

Somit ist auf Frage 2 zu antworten, dass Art. 58 Abs. 5 der Verordnung 2016/679 dahin auszulegen ist, dass die Ausübung der einer Aufsichtsbehörde eines Mitgliedstaats, die nicht die federführende Aufsichtsbehörde ist, nach dieser Vorschrift zustehenden Befugnis zur Klageerhebung bei einer grenzüberschreitenden Verarbeitung personenbezogener Daten nicht voraussetzt, dass der für die grenzüberschreitende Verarbeitung personenbezogener Daten Verantwortliche oder der Auftragsverarbeiter, gegen den die Klage erhoben wird, im Hoheitsgebiet des Mitgliedstaats der fraglichen Aufsichtsbehörde eine Hauptniederlassung oder eine andere Niederlassung hat.

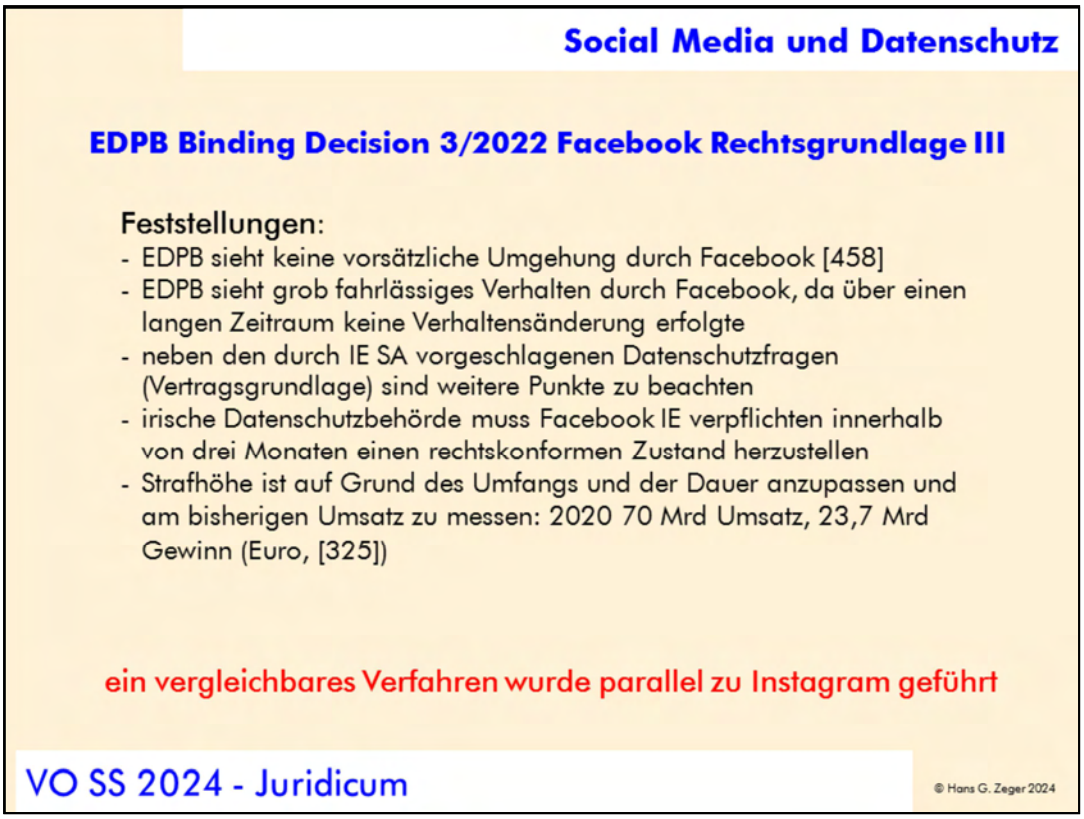
...


Social Media und Datenschutz
EDPB Binding Decision 3/2022 Facebook Rechtsgrundlage
Sachlage:
- Beschwerde gegen Facebook IE bei der IE Datenschutzbehörde wegen unzulässiger Nutzung personenbezogener Daten
Verfahrensgrundlage:
- DSGVO Art. 60ff: Zusammenarbeit und Kohärenz zwischen den Datenschutzbehörden
- beteiligte Behörden: IE SA (supervisory authority) als "führende Aufsichtsbehörde" + 10 weitere Behörden (AT, DE, FI, FR, IT, NL, NO, PL, PT, SE)
- Auslöser: Beschwerde aus AT
Entwicklung Verfahren:
- 2018/05/25 Eingang der Beschwerde bei DSB (AT) (Beginn DSGVO)
- 2018/08/20 Verfahrensbeginn in IE
- Koheränzverfahren gem Art. 63ff: in weiterer Folge formuliert IE SA einen Entscheidungsentwurf, der nicht die Zustimmung der anderen SA findet
- 2022/12/05 Auftrag der EDPB auf Basis Art. 65 ("Streitbeilegung") an IE SA zu entscheiden
- 2022/12/31 IE SA entscheidet
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

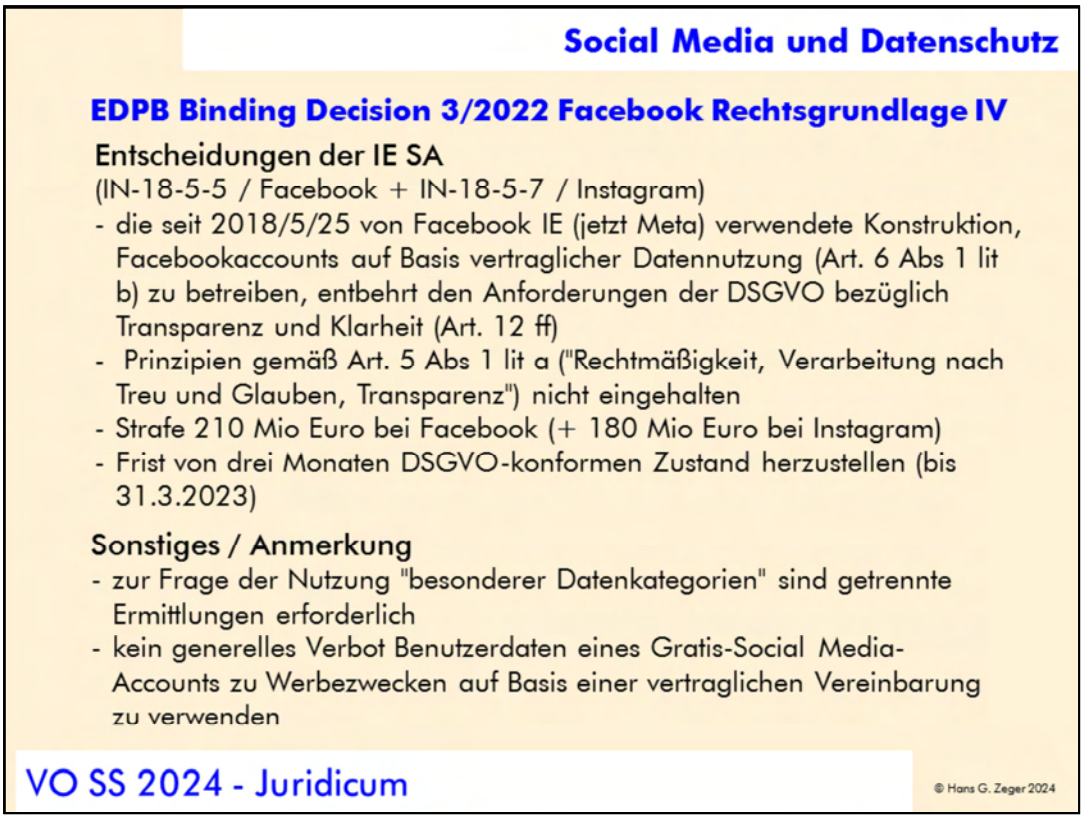
-


Social Media und Datenschutz
EDPB Binding Decision 3/2022 Facebook Rechtsgrundlage II
aufgeworfende Datenschutzfragen und Einwände:
- auf Basis welcher Datenschutzgrundlage ist Facebook tätig
Art. 6 Abs. 1 lit b): vertragliche Vereinbarung oder
Art. 6 Abs. 1 lit a): Zustimmung durch den Betroffenen
- Einhaltung von Prinzipien
Art. 5 Abs. 1 lit a): "Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz"
Art. 5 Abs. 1 lit b): "Zweckbindung"
Art. 5 Abs. 1 lit c): "Datenminimierung"
- Art. 9 Abs. 1: Verbot Verarbeitung besonderer Kategorien personenbezogener Daten
- Art. 12 Abs. 1: Transparenz gegenüber dem Betroffenen
- Art. 13 Abs. 1 lit c): Einhaltung der Auskunftspflicht Verarbeitungszwecke
- Art. 83 Abs. 1: Strafhöhe
Entscheidungsgrundlage der EDPB:
- Entscheidungsentwurf der IE SA
- begründete Einsprüche weiterer SAs gemäß Art. 4 Z 24
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Social Media und Datenschutz
EDPB Binding Decision 3/2022 Facebook Rechtsgrundlage III
Feststellungen:
- EDPB sieht keine vorsätzliche Umgehung durch Facebook [458]
- EDPB sieht grob fahrlässiges Verhalten durch Facebook, da über einen langen Zeitraum keine Verhaltensänderung erfolgte
- neben den durch IE SA vorgeschlagenen Datenschutzfragen (Vertragsgrundlage) sind weitere Punkte zu beachten
- irische Datenschutzbehörde muss Facebook IE verpflichten innerhalb von drei Monaten einen rechtskonformen Zustand herzustellen
- Strafhöhe ist auf Grund des Umfangs und der Dauer anzupassen und am bisherigen Umsatz zu messen: 2020 70 Mrd Umsatz, 23,7 Mrd Gewinn (Euro, [325])
ein vergleichbares Verfahren wurde parallel zu Instagram geführt
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

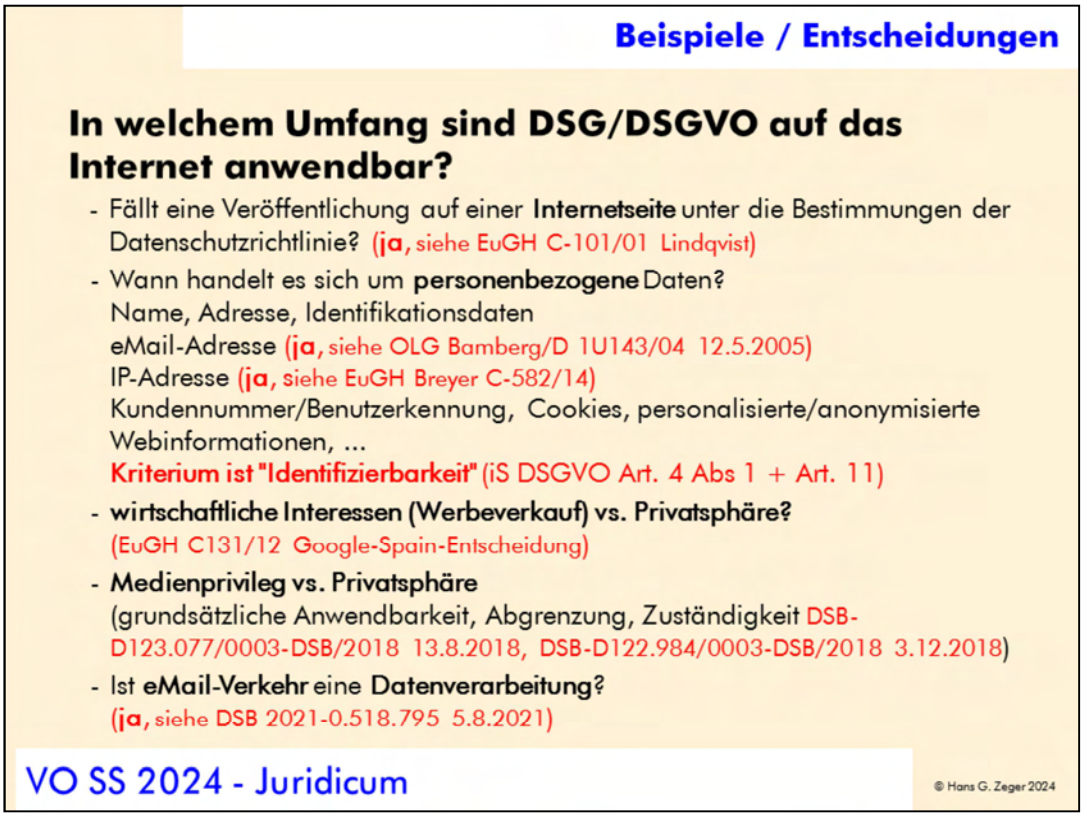
-


Social Media und Datenschutz
EDPB Binding Decision 3/2022 Facebook Rechtsgrundlage IV
Entscheidungen der IE SA
(IN-18-5-5 / Facebook + IN-18-5-7 / Instagram)
- die seit 2018/5/25 von Facebook IE (jetzt Meta) verwendete Konstruktion, Facebookaccounts auf Basis vertraglicher Datennutzung (Art. 6 Abs 1 lit b) zu betreiben, entbehrt den Anforderungen der DSGVO bezüglich Transparenz und Klarheit (Art. 12 ff)
- Prinzipien gemäß Art. 5 Abs 1 lit a ("Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz") nicht eingehalten
- Strafe 210 Mio Euro bei Facebook (+ 180 Mio Euro bei Instagram)
- Frist von drei Monaten DSGVO-konformen Zustand herzustellen (bis 31.3.2023)
Sonstiges / Anmerkung
- zur Frage der Nutzung "besonderer Datenkategorien" sind getrennte Ermittlungen erforderlich
- kein generelles Verbot Benutzerdaten eines Gratis-Social Media-Accounts zu Werbezwecken auf Basis einer vertraglichen Vereinbarung zu verwenden
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

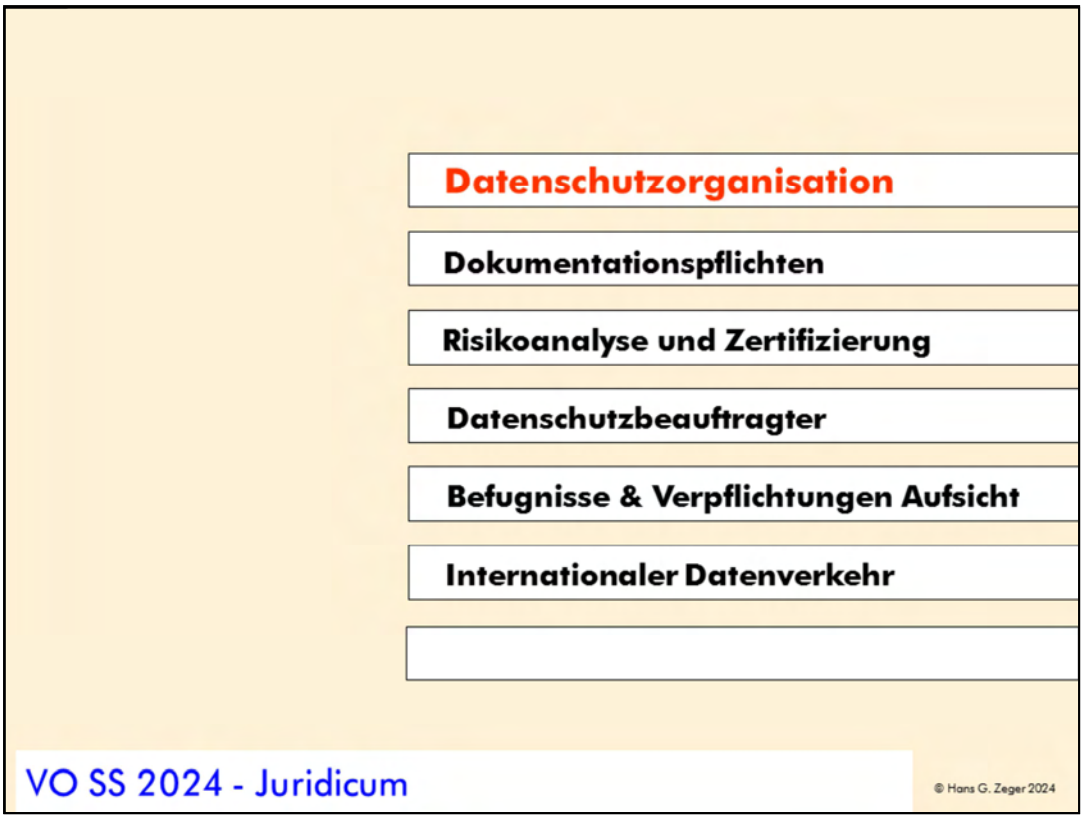
-


Beispiele / Entscheidungen
Weitere Themen
DSB 2021-0.518.795 5.8.2021
("Straferkenntnis Übermittlung Personendaten per eMail")
e-Mail-Versender ist Verantwortlicher iS der DSGVO - Strafhöhe 600,- Euro)
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 SS 2024 - Juridicum
© Hans G. Zeger 2024

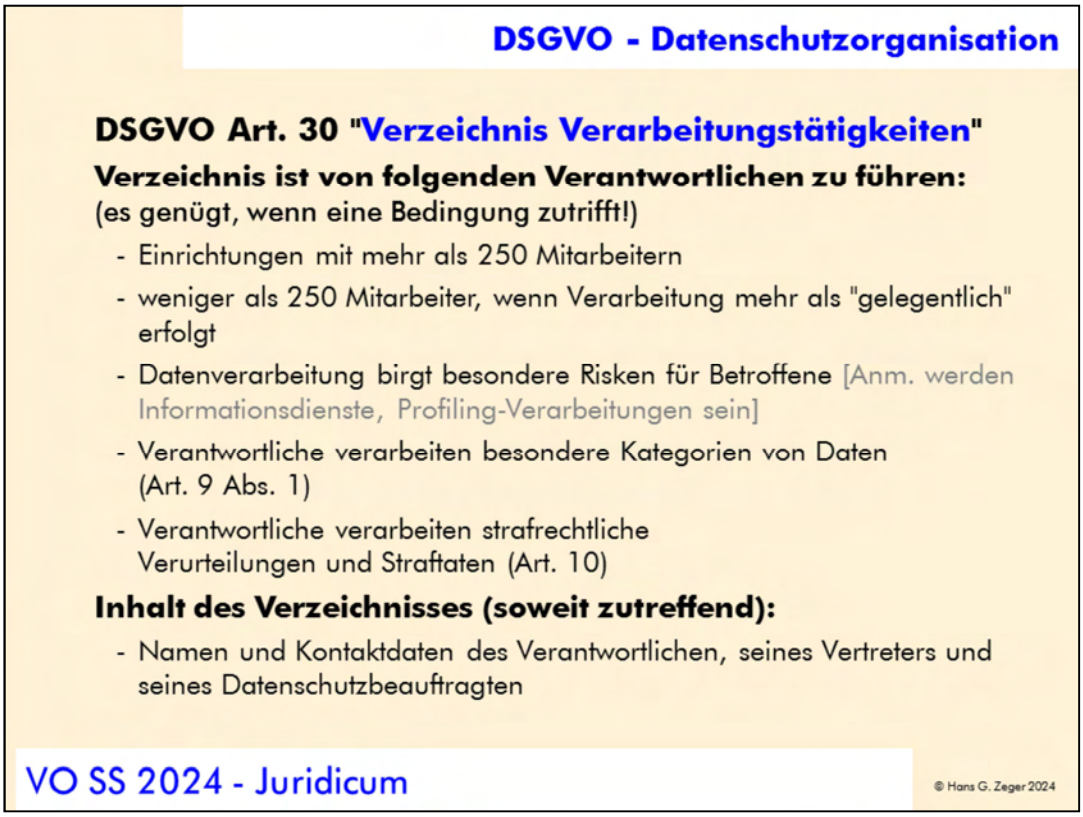
-


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, Abgrenzung, 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 DSB 2021-0.518.795 5.8.2021)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Datenschutzorganisation
Dokumentationspflichten
Risikoanalyse und Zertifizierung
Datenschutzbeauftragter
Befugnisse & Verpflichtungen Aufsicht
Internationaler Datenverkehr
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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;

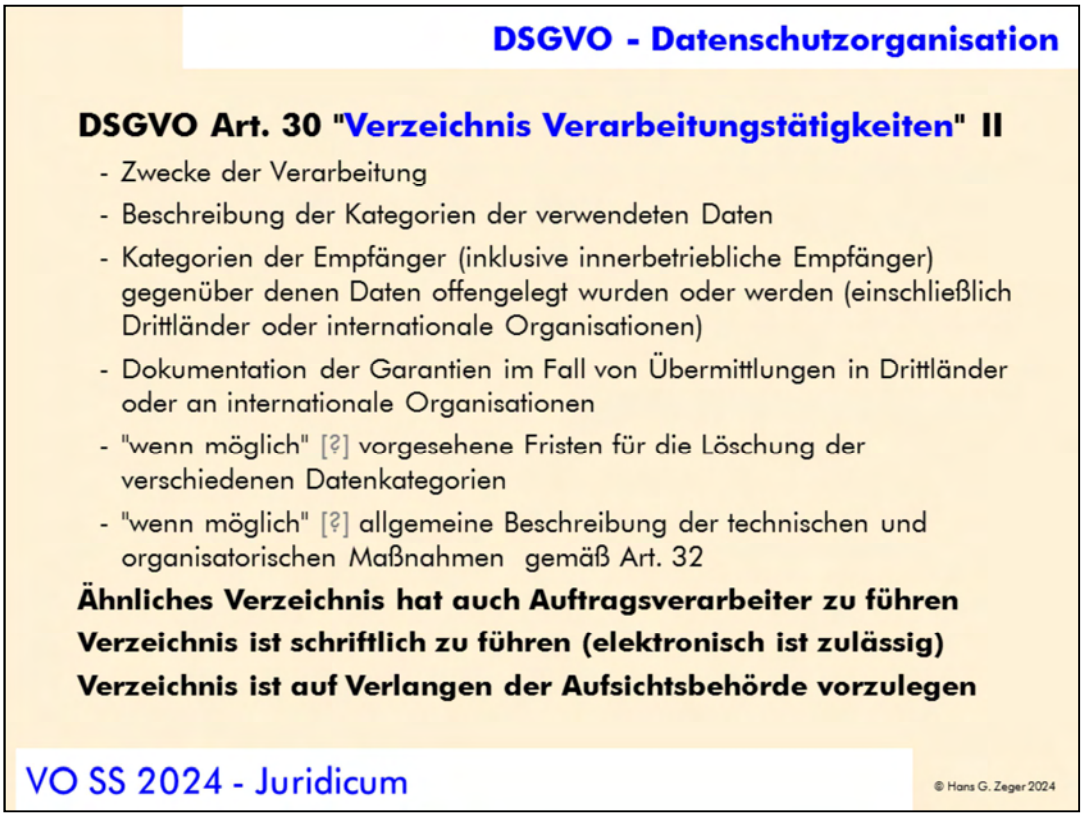
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

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 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;

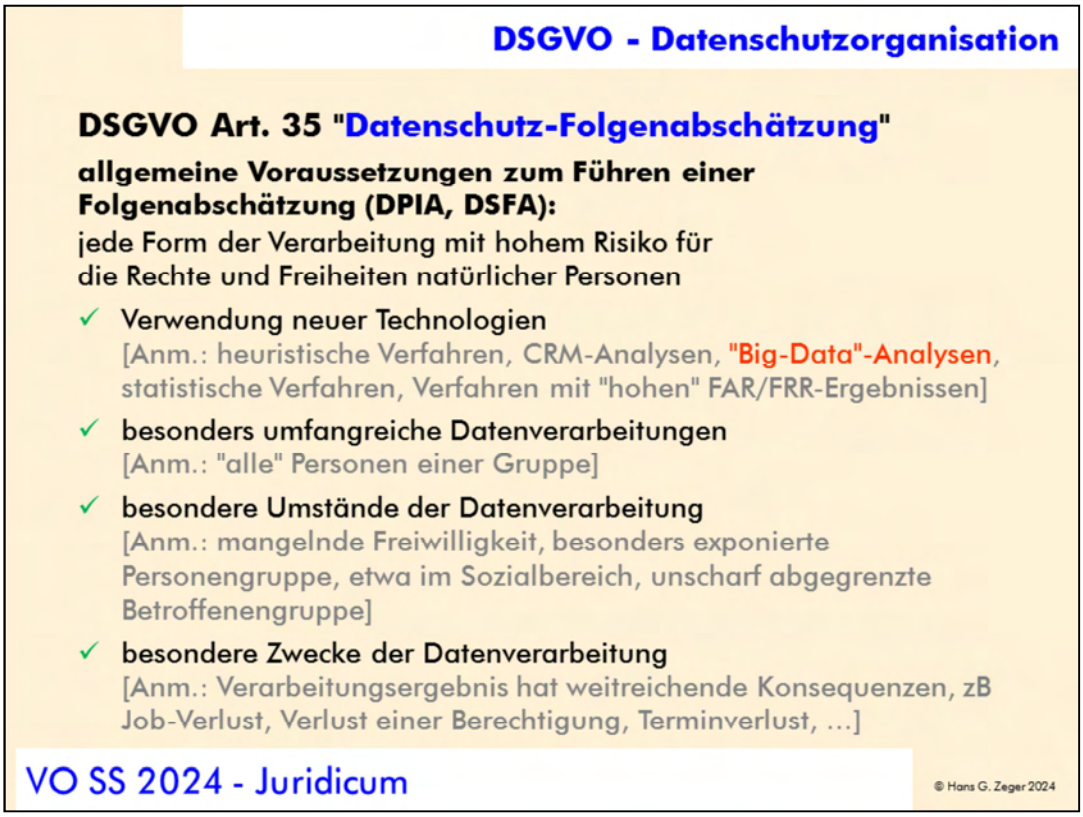
c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen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

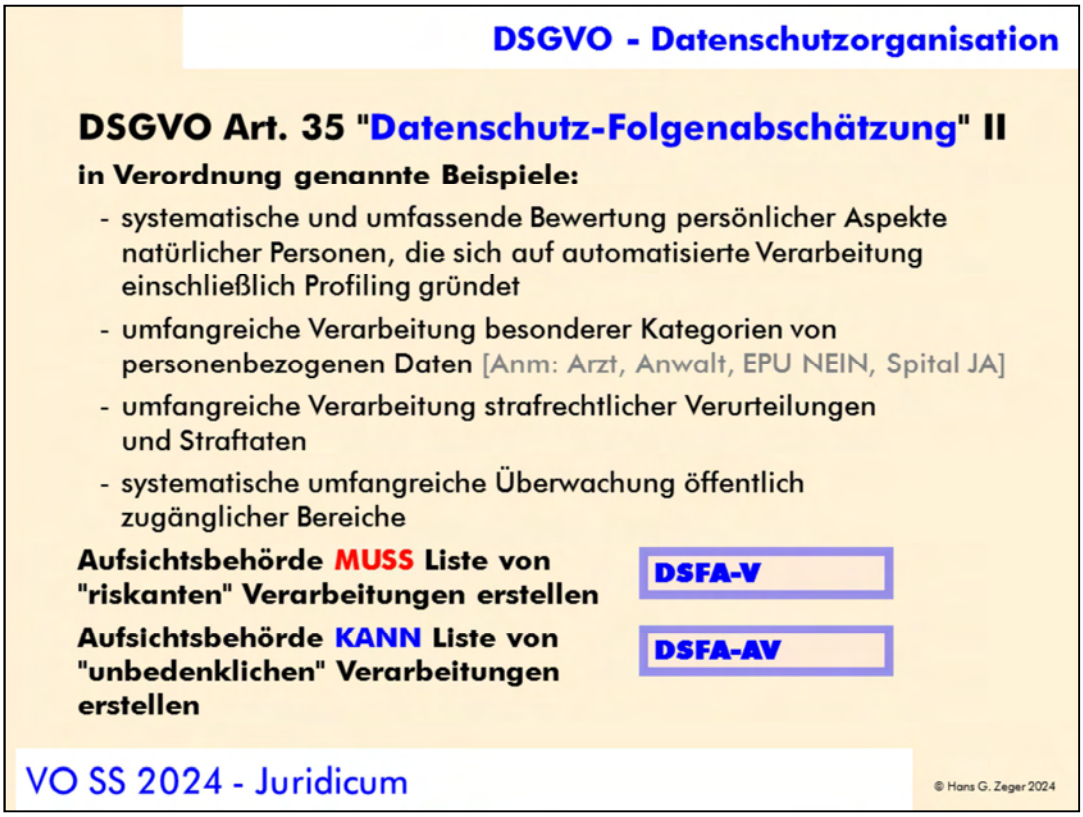
(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

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.

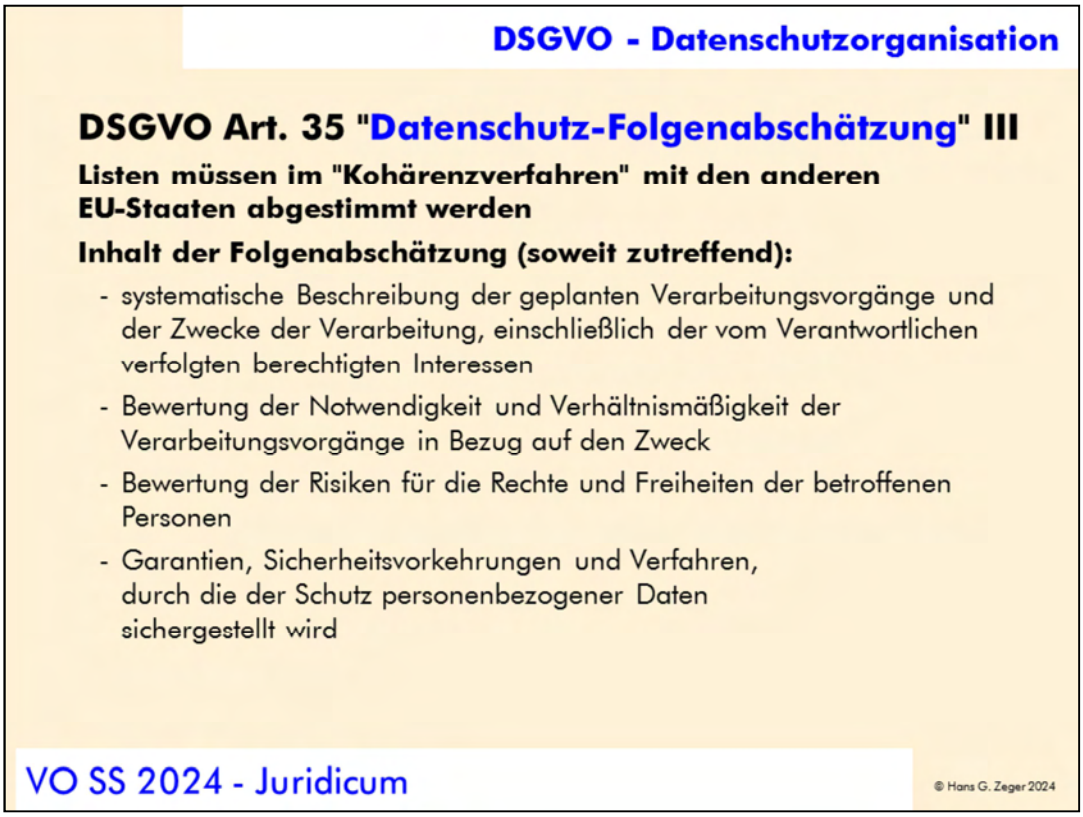
(7) Die Folgenabschätzung enthält zumindest Folgendes:

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

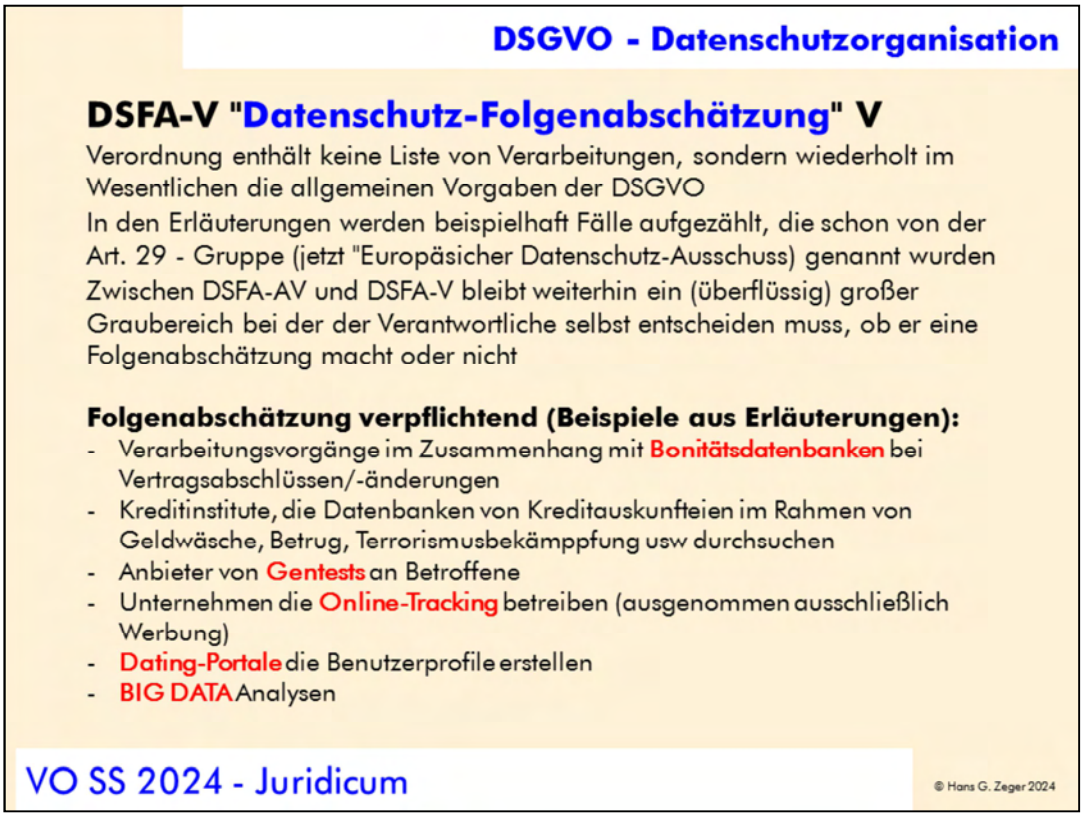
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-

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



DSFA-V:

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,

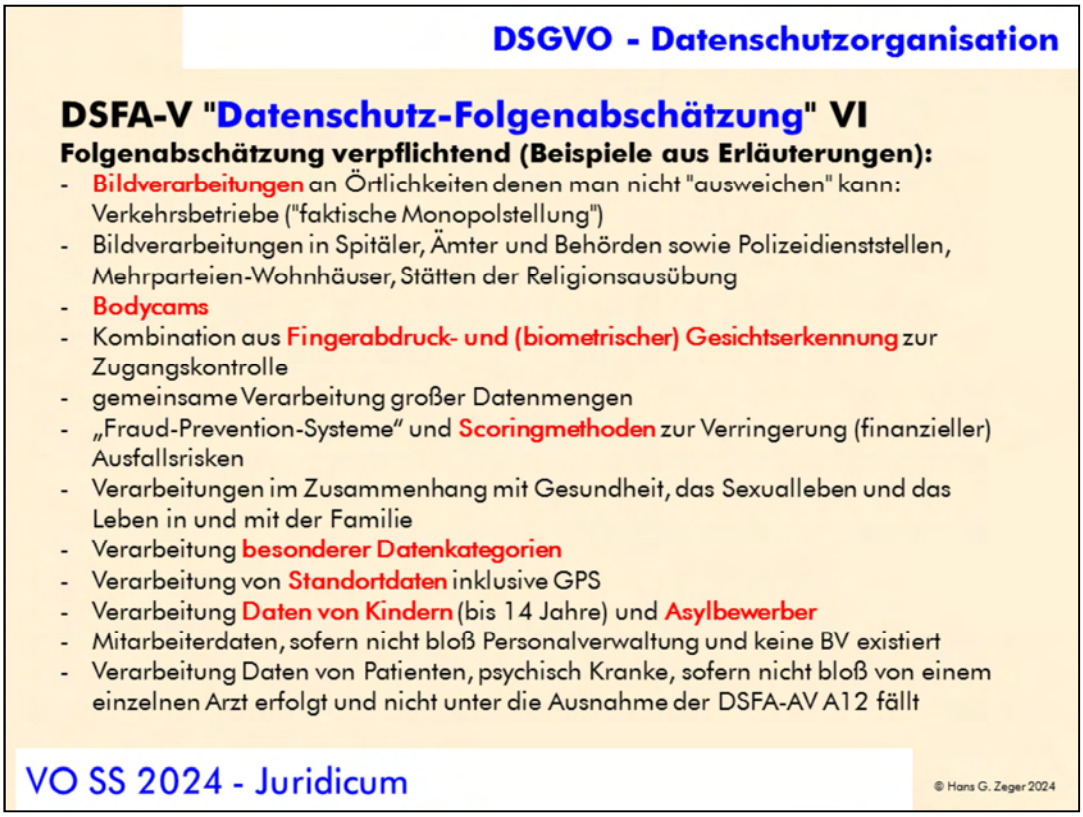
c) Straßen mit öffentlichem Verkehr, die gemäß § 1 Straßenverkehrsordnung 1960 (StVO 1960), BGBl. Nr. 159/1960, von jedermann unter den gleichen Bedingungen benützt werden können, erfassen,

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



DSFA-V:

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.

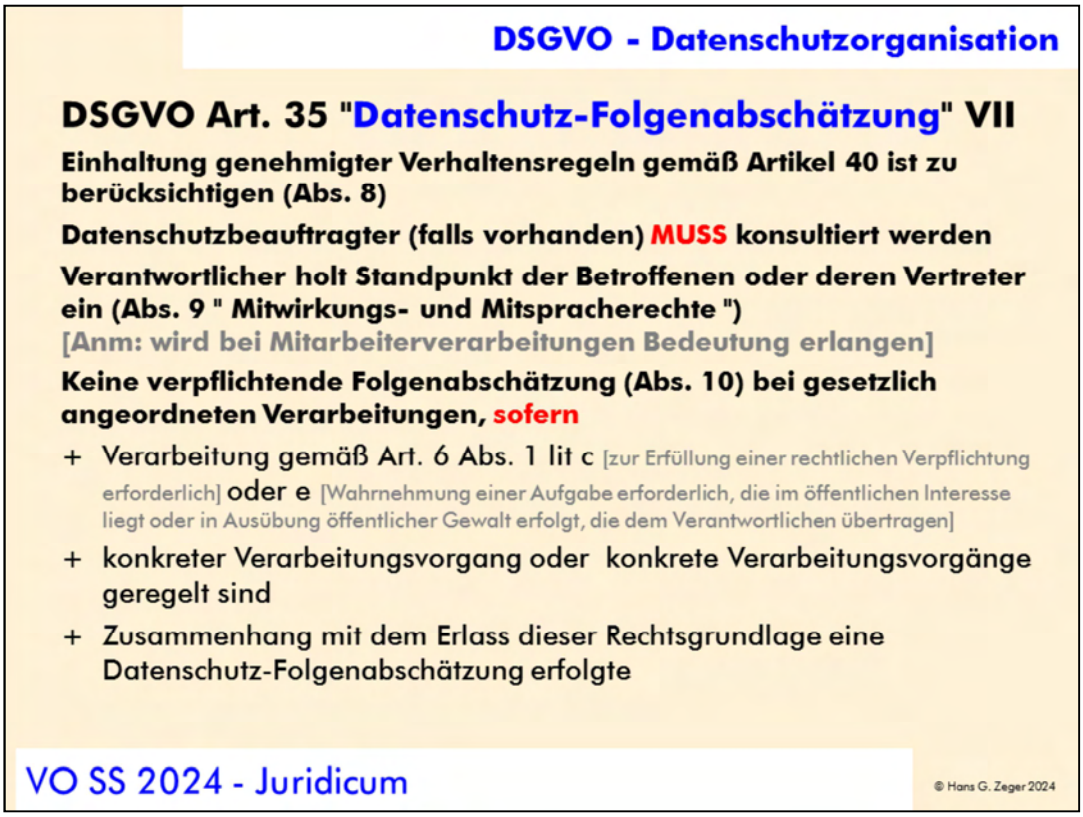
(3) Eine Datenschutz-Folgenabschätzung ist durch den Verantwortlichen durchzuführen, wenn ein Verarbeitungsvorgang zwei oder mehr der nachstehenden Kriterien erfüllt:

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.



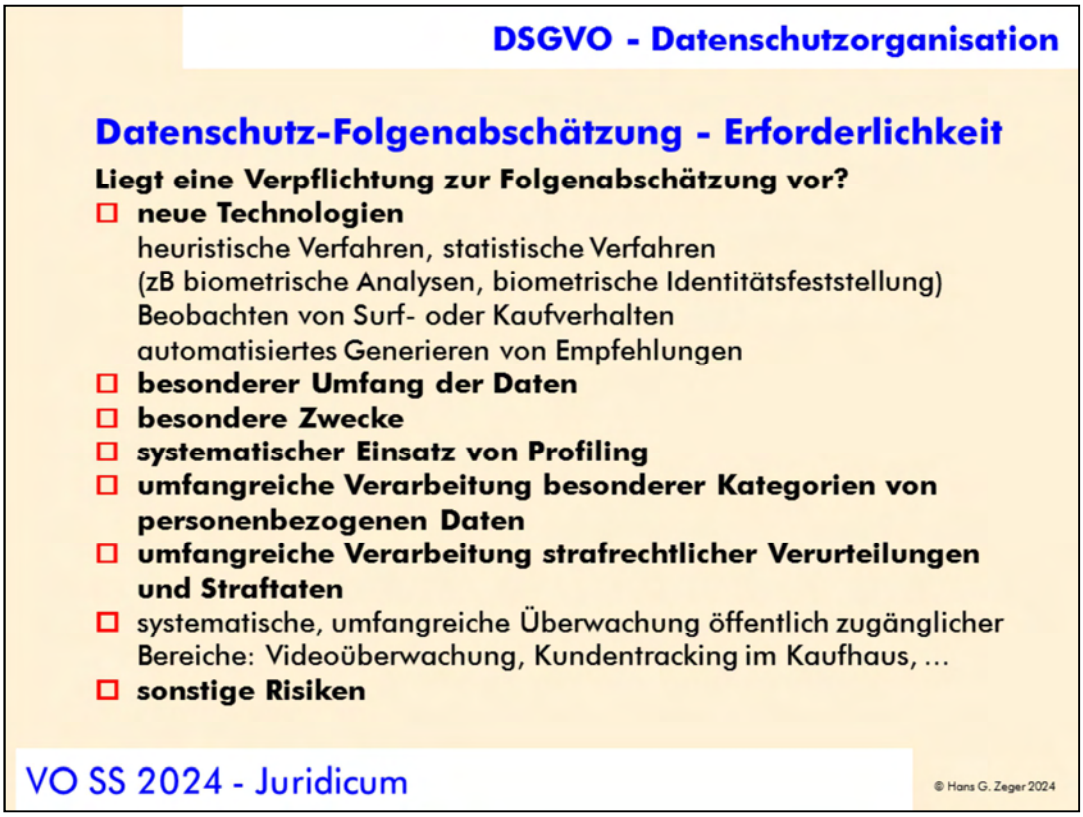
DSGVO Art. 35 Datenschutz-Folgenabschätzung (Fortsetzung)

(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 SS 2024 - Juridicum
© Hans G. Zeger 2024

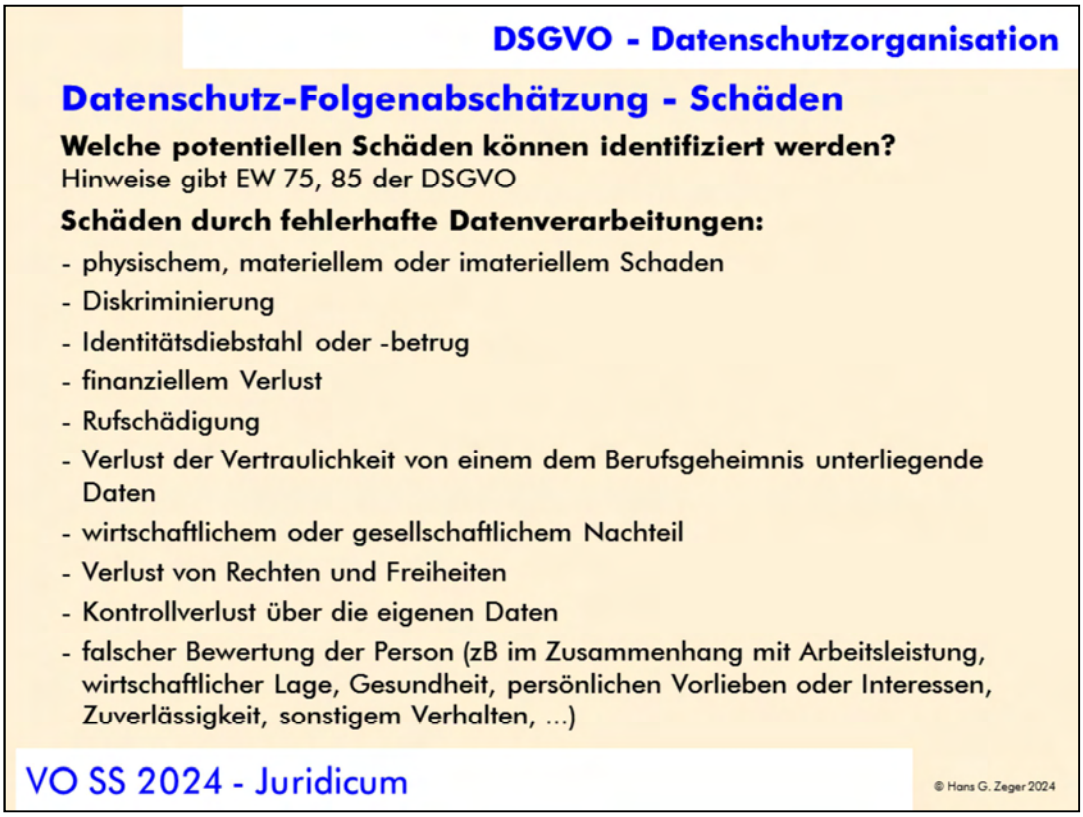
-


DSGVO - Datenschutzorganisation
DSFA Beispiele - Internetanwendungen
Parkplatz-Suchsystem
Online-Authentifizierung (zB Video-Identifikation)
Online-Kreditantragsbearbeitung
Smart-TV
Sprachassistenten
Routen-Planer
Kreditscoring
Matching-Algorithmen
Bewertungsplattformen
Benutzer-Tracking
Partnerbörse
...
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-

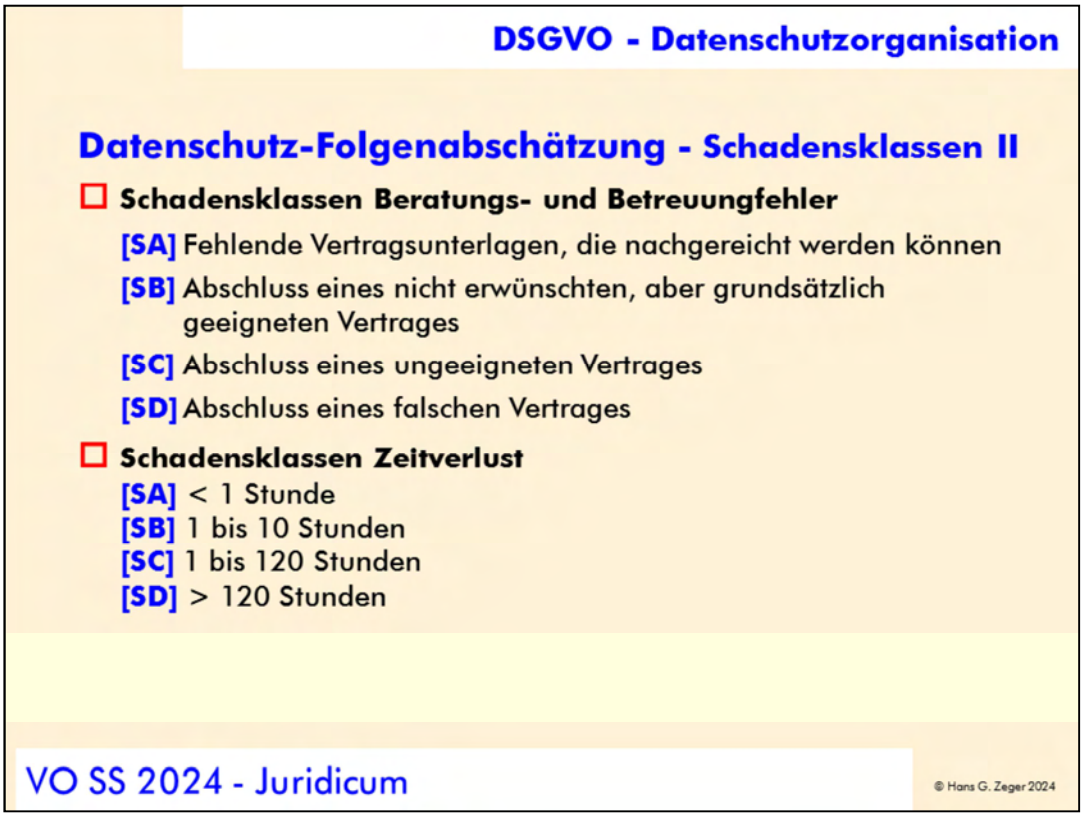


DSGVO EW75

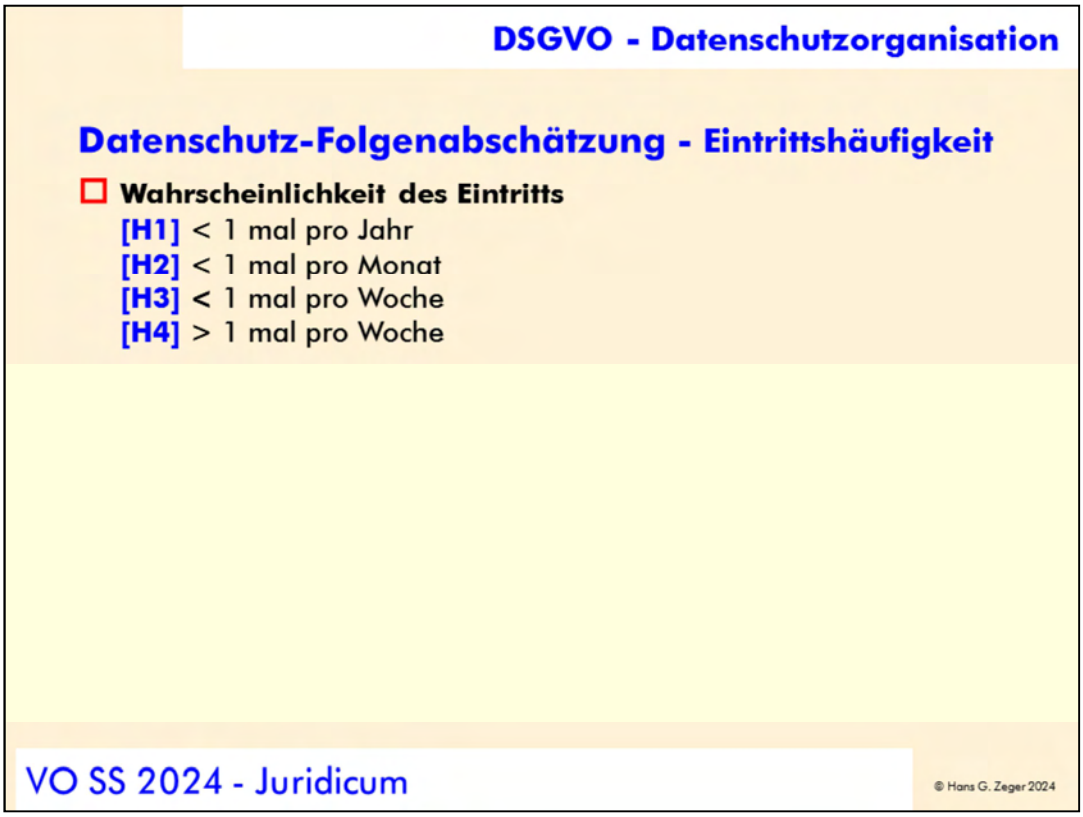
(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

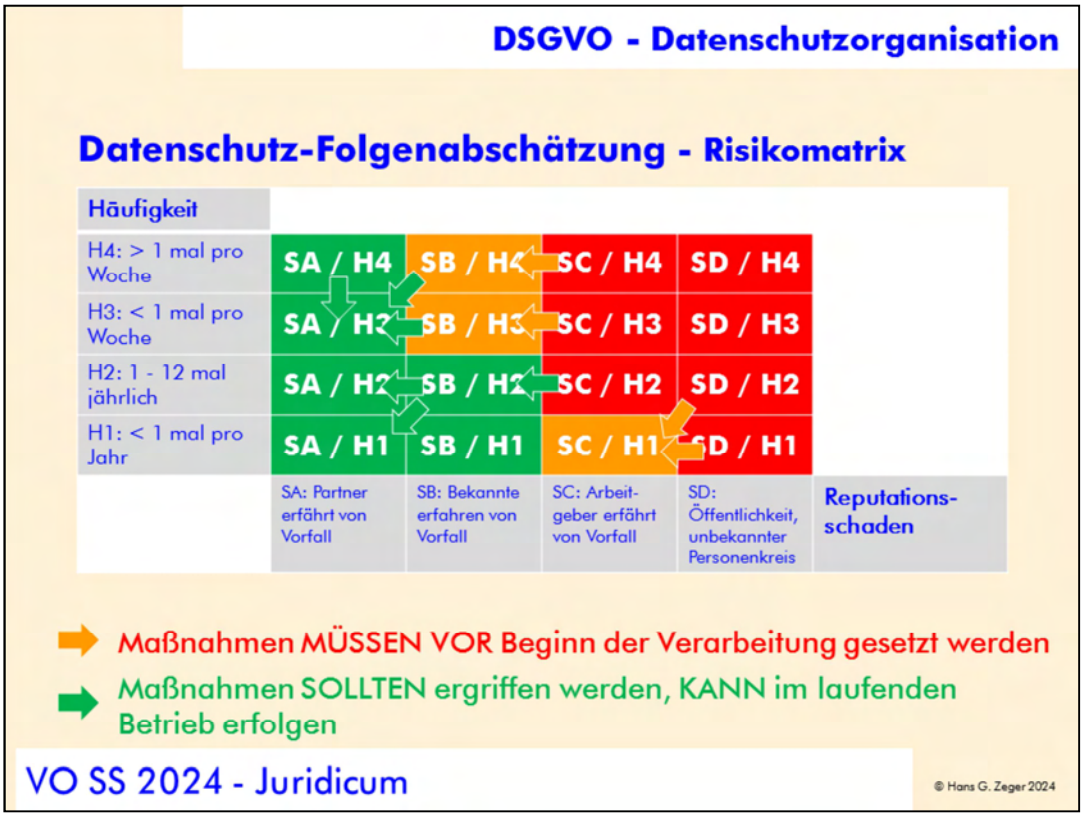
-


DSGVO - Datenschutzorganisation
Datenschutz-Folgenabschätzung - Schadensklassen II
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
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


DSGVO - Datenschutzorganisation
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
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


DSGVO - Datenschutzorganisation
Datenschutz-Folgenabschätzung - Risikomatrix
Häufigkeit
H4: > 1 mal pro Woche
H3: < 1 mal pro Woche
H2: 1 - 12 mal jährlich
H1: < 1 mal pro Jahr
SA / H4
SB / H4
SC / H4
SD / H4
SA / H3
SB / H3
SC / H3
SD / H3
SA / H2
SB / H2
SC / H2
SD / H2
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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-

DSGVO - Datenschutzorganisation

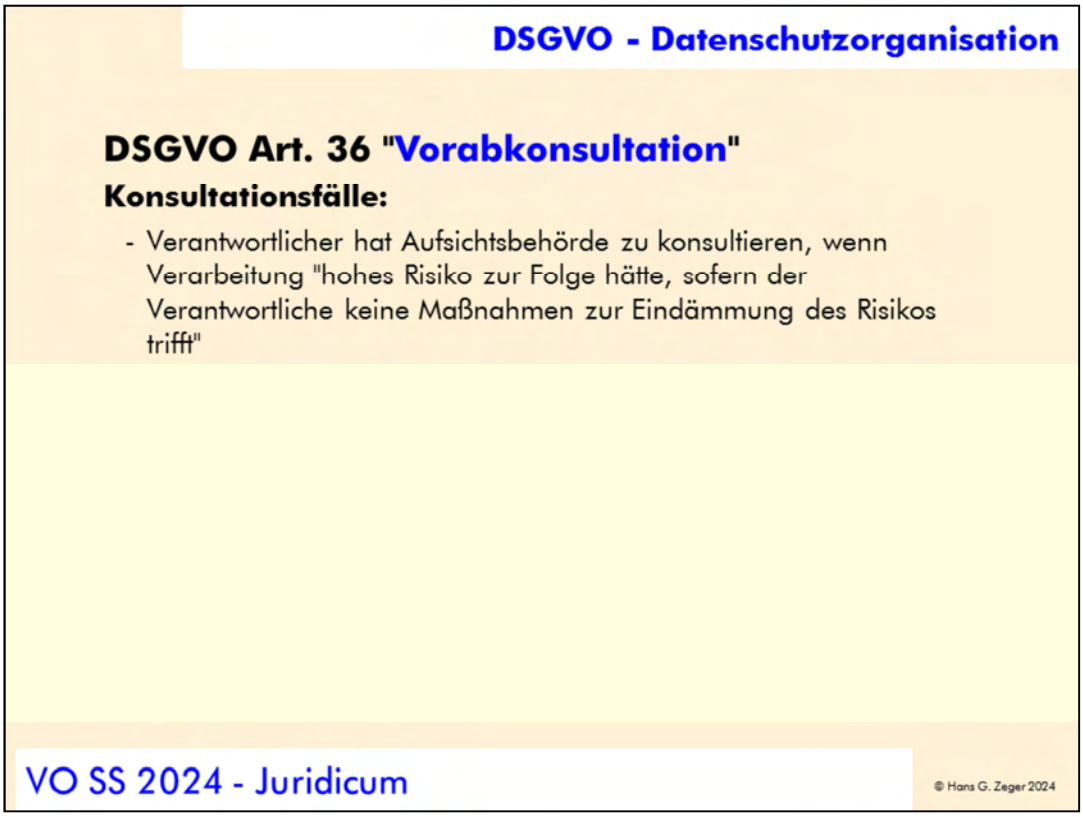
Datenschutz-Folgenabschätzung - Fallbeispiel

- ☐ **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 SS 2024 - 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.

DSB Bescheid 2021-0.024.862

Die Datenschutzbehörde entscheidet aufgrund des von der A** Verkehrsbetriebe GmbH (Verantwortliche), vertreten durch N** Rechtsanwälte GmbH, am 10. Dezember 2020 eingeleiteten Verfahrens gemäß Art. 36 DSGVO betreffend eine beabsichtige Datenverarbeitung („Testbetrieb Anpralldetektion bei Brücken") wie folgt:

- Der Antrag auf vorherige Konsultation nach Art. 36 DSGVO wird abgewiesen.

...

1. Die Verantwortliche führt aus, dass ein hohes Risiko in Bezug auf die Erteilung der zuverlässigen Information an die betroffenen Personen über die Datenverarbeitung dahingehend gegeben ist, dass die betroffenen Personen von der Datenverarbeitung in Form einer Videoüberwachung in ihrem privaten oder beruflichen Lebensbereich erfasst werden, ohne über die Tatsache der Verarbeitung und/oder die Identität des Verantwortlichen informiert zu sein. Konkret definiert die Verantwortliche das Risiko im Rahmen ihrer Datenschutz-Folgenabschätzung als „Risik[o] für die Effektivität der Erfüllung der Informationspflichten durch Kennzeichnung". Es handelt sich hierbei – in Hinblick auf die zuvor festgehaltenen Überlegungen – um ein „Risiko" iSd Art. 35 DSGVO.

Da lediglich jene Verarbeitungen – die auch nach Vorsehen der im Zuge der Datenschutz-Folgenabschätzung definierten Abhilfemaßnahmen weiterhin hohe Risiken für natürliche Personen bergen – dem Konsultationsmechanismus unterzogen werden sollen (Trieb in Knyrim, Art 35, Rz 28 ff; Trieb in Knyrim, Art. 36 Rz 1), ist in einem nächsten Schritt zu prüfen, ob die Verantwortliche geeignete Maßnahmen zur Eindämmung des identifizierten Risikos getroffen hat.

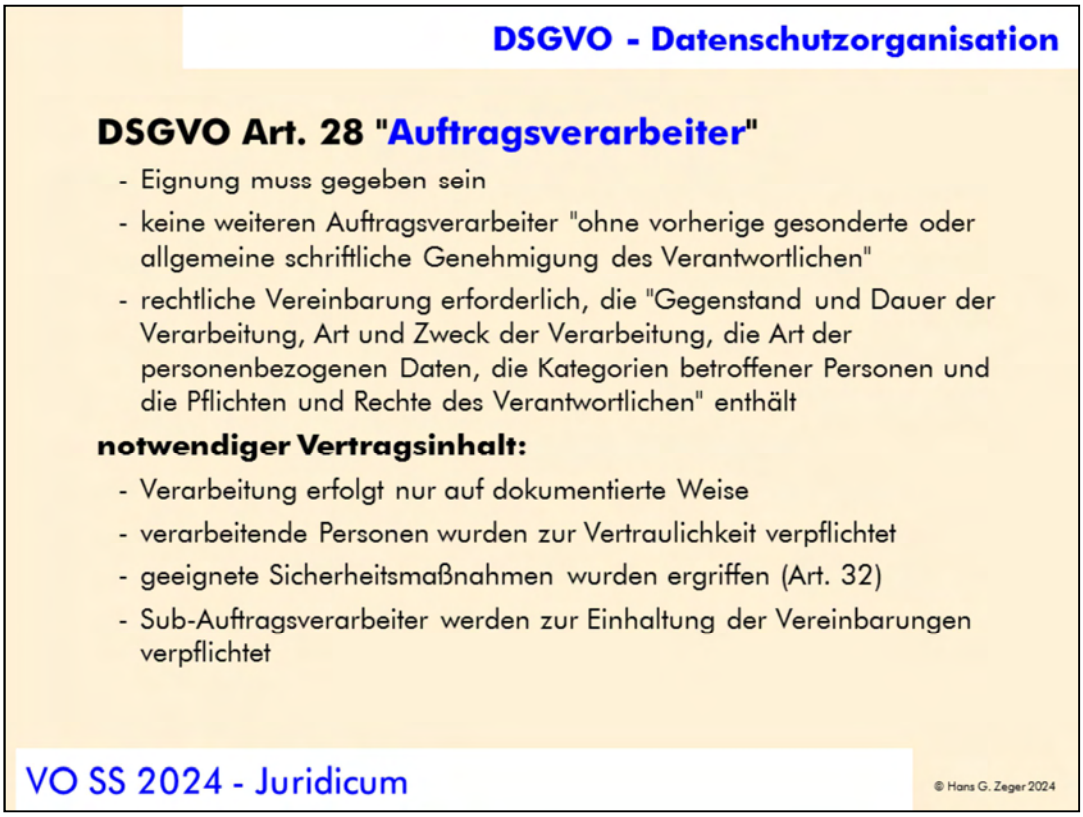
...

4. Aufgrund der von der Verantwortlichen in der Datenschutz-Folgenabschätzung vorgenommenen Beurteilung ist die Zulässigkeit der gegenständlichen Datenverarbeitung zu bejahen und hat die Datenschutzbehörde der Interessensabwägung der Verantwortlichen nichts entgegenzusetzen.

Das von der Verantwortlichen aufgeworfene „hohe Restrisiko" wird jedenfalls durch die geplanten Aufnahme-, Auswertungs- und Löschmodalitäten derart stark reduziert, dass im Ergebnis kein hohes Restrisiko für Betroffene erkannt werden kann.

Entgegen der Ansicht der Verantwortlichen hat sie daher insgesamt unter Zusammenschau der dargelegten Maßnahmen nach Art. 35 Abs. 7 lit. d DSGVO das bestehende Risiko hinreichend eingedämmt.

Die Voraussetzungen für eine vorherige Konsultation gemäß Art. 36 DSGVO sind daher mangels hohem Risiko nicht gegeben und es war sohin spruchgemäß zu entscheiden.



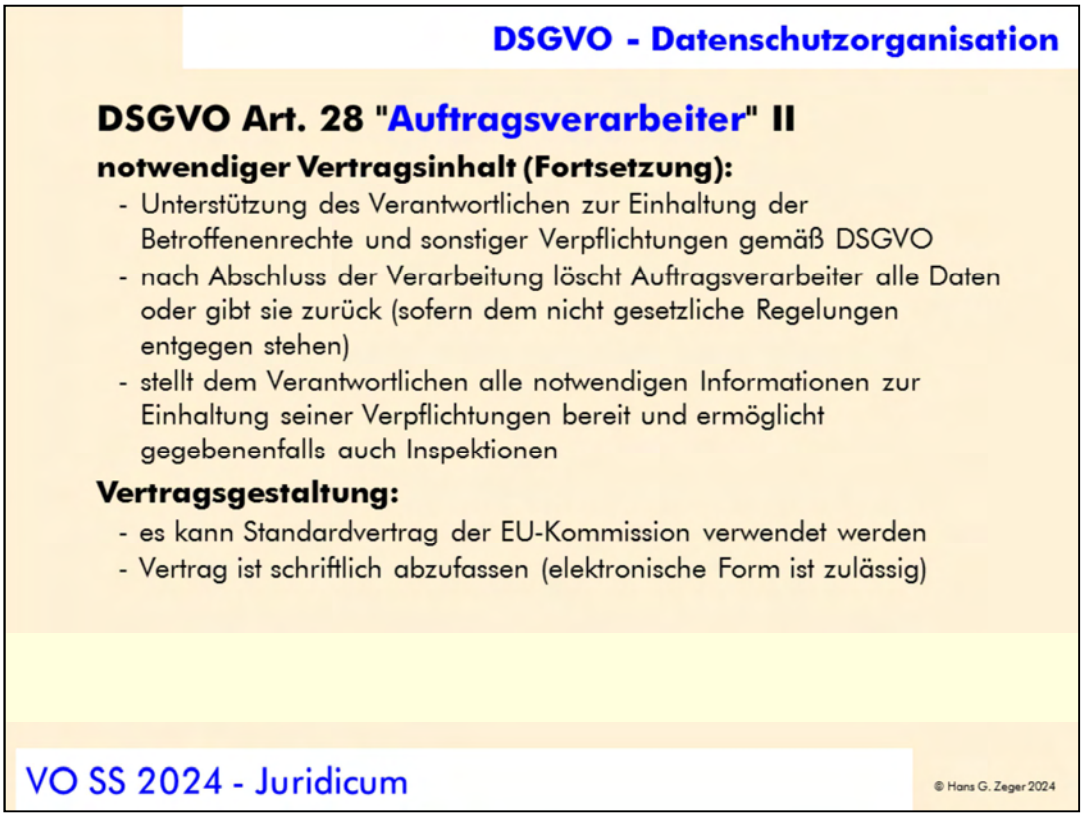
DSGVO Art. 28 Auftragsverarbeiter

(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 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;

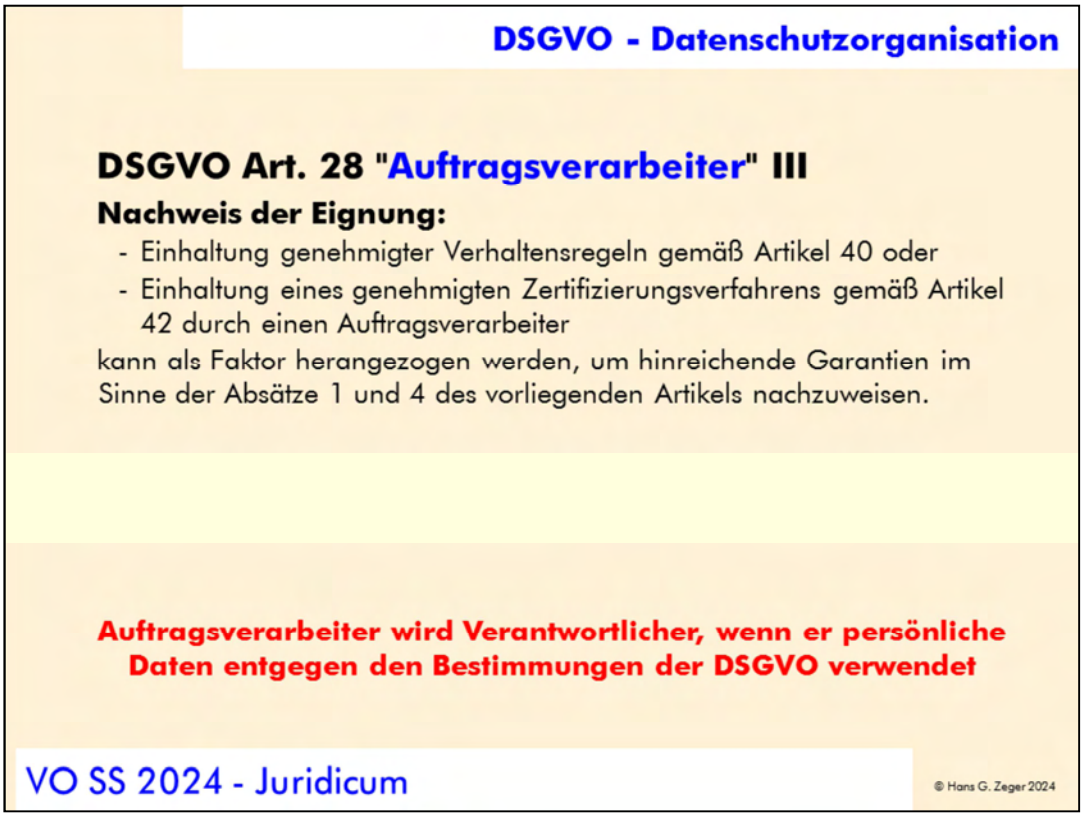
e)angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

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 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.

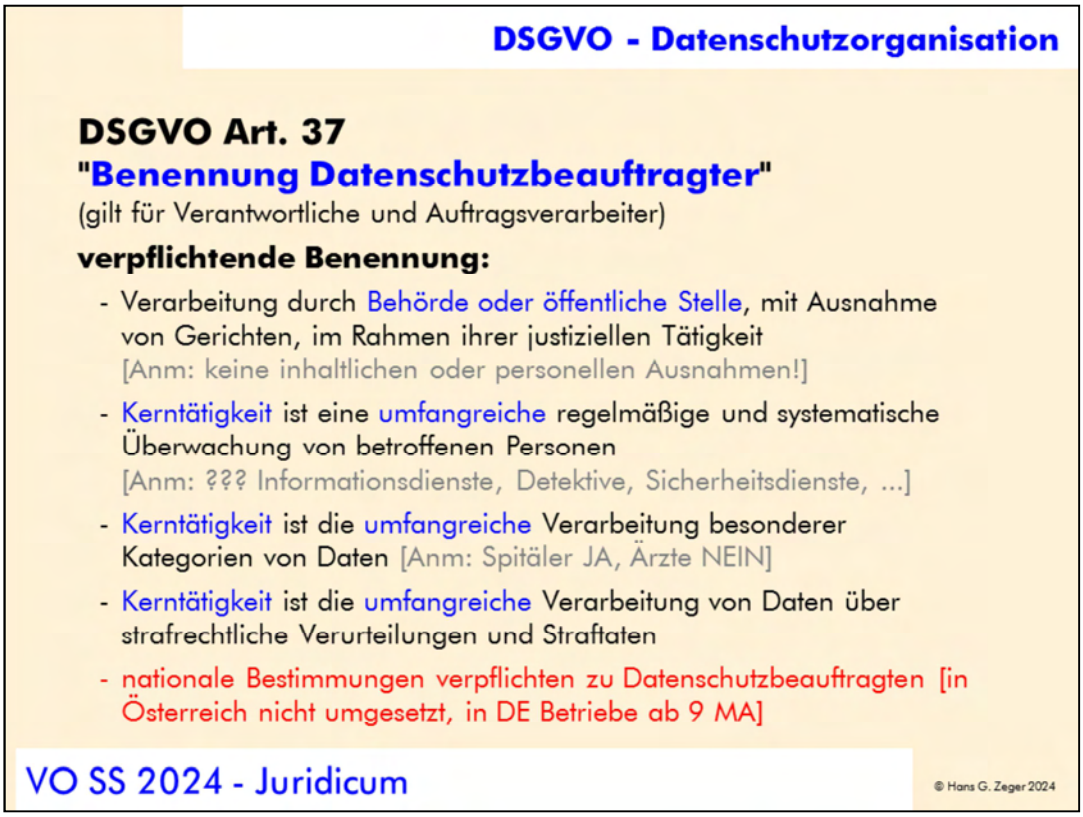
(7)Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(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.

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



DSGVO Art. 37 Benennung eines Datenschutzbeauftragten

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

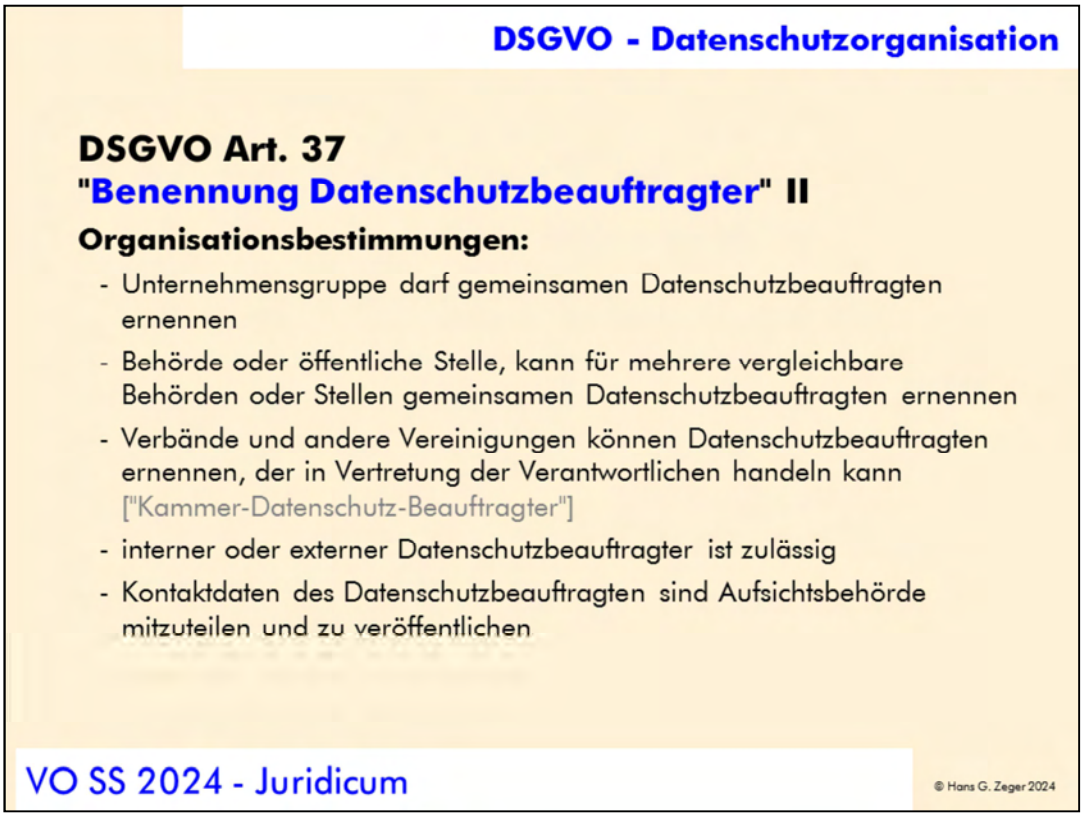
a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

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.



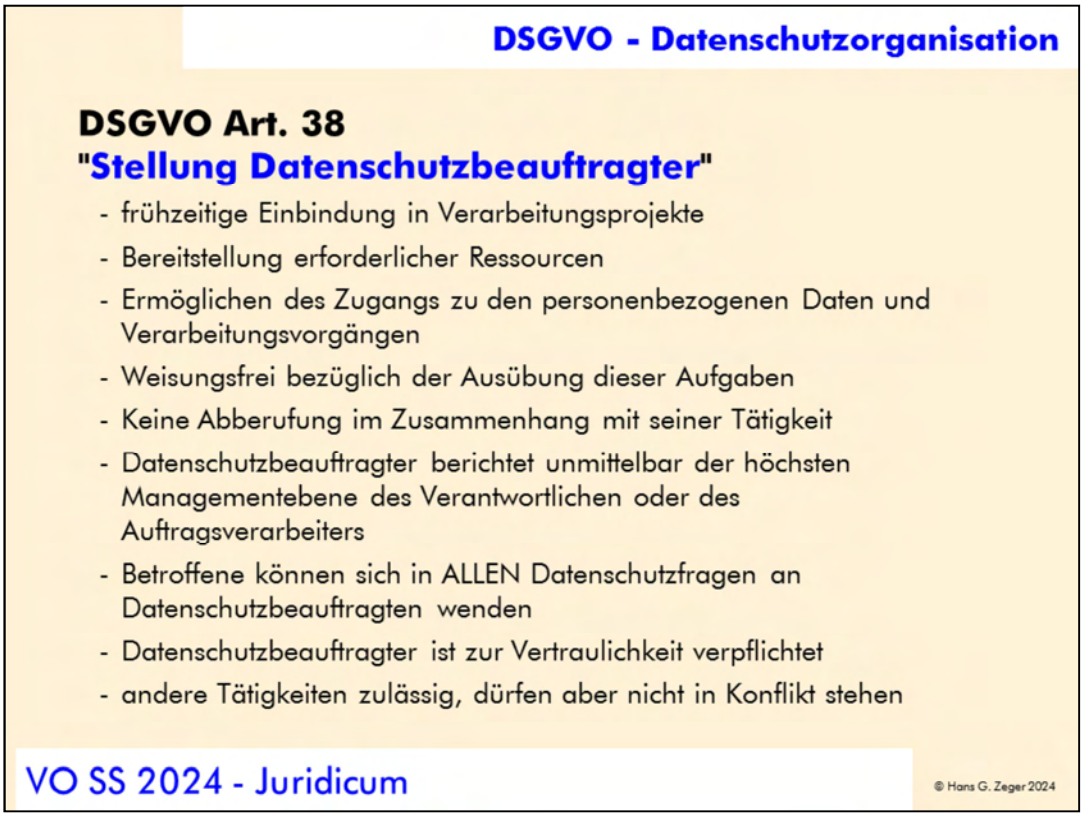
DSGVO Art. 37 Benennung eines Datenschutzbeauftragten (Fortsetzung)

(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 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.

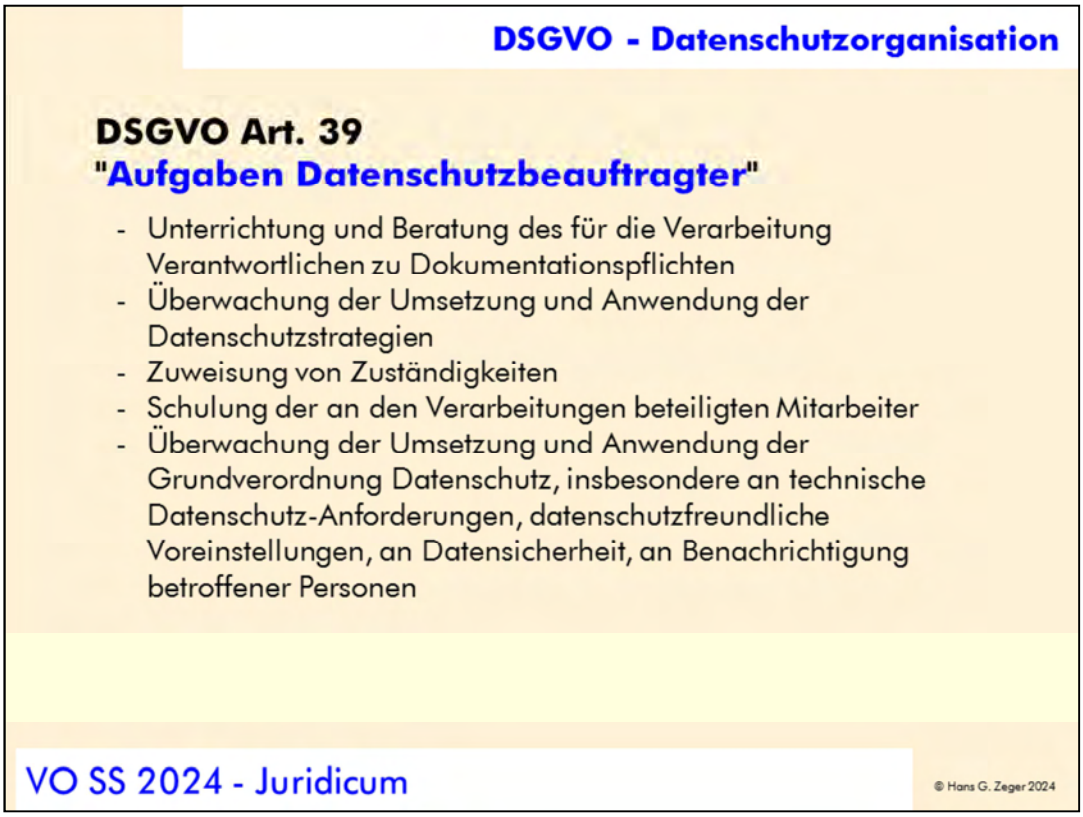
(2)Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur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

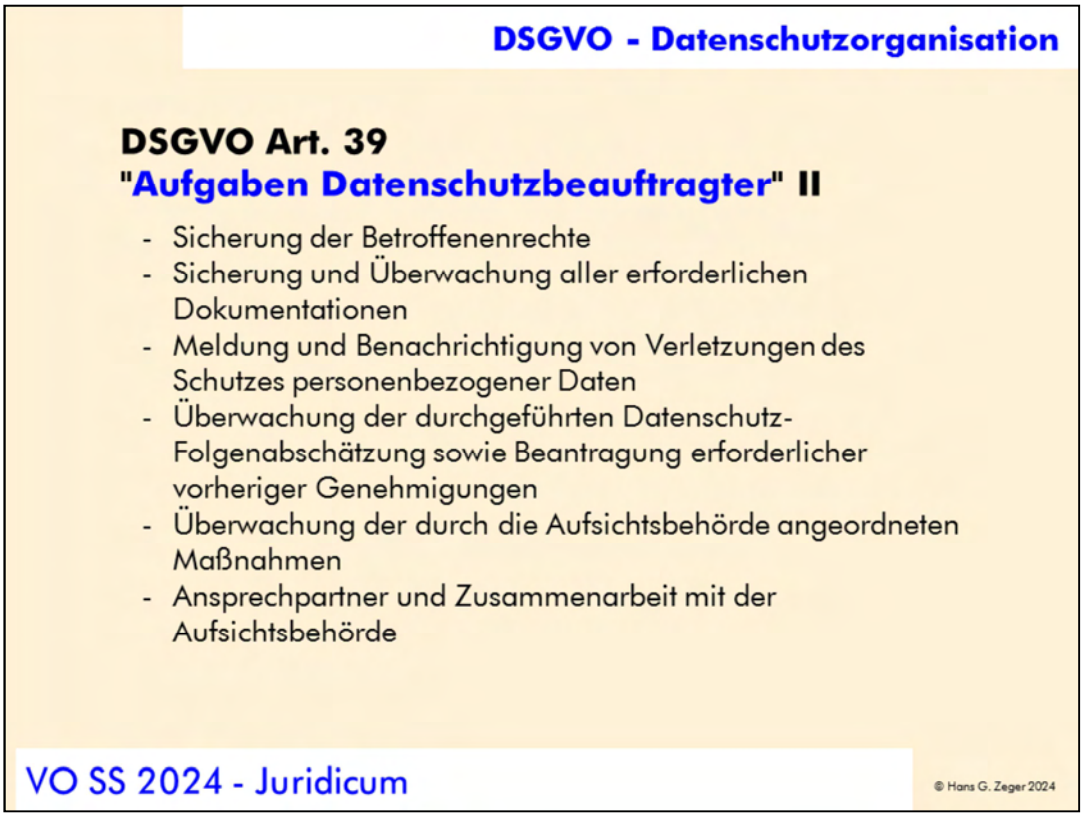
b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und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

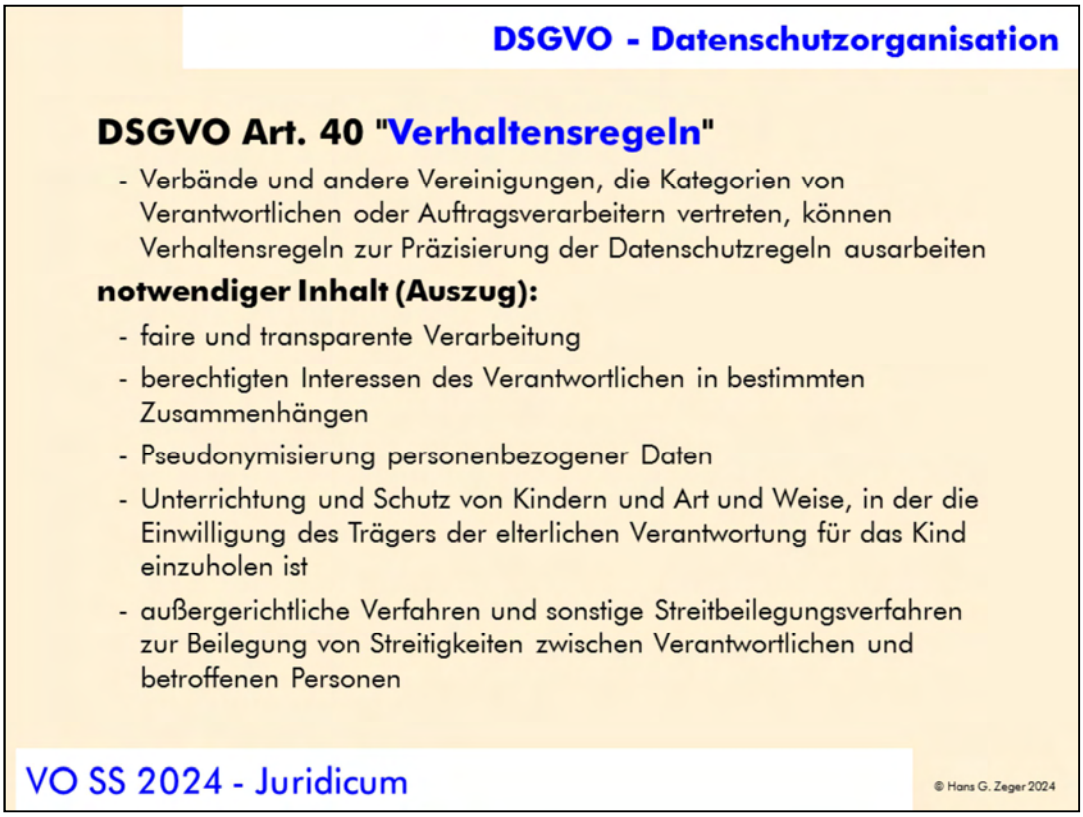
d) Zusammenarbeit mit der Aufsichtsbehörde;

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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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.

ISPA CoC

https://www.ispa.at/wissenspool/datenschutz/

...

VI. Datenschutzverletzungen

...

5. Da vom ISP nur der eigene Vertragskunde kontaktiert werden kann, nicht jedoch etwaige Gesprächspartner, welche von einer Datenschutzverletzung ebenso betroffen sein könnten, ist es den unterzeichnenden ISPs nur möglich, eine Benachrichtigung des jeweiligen Vertragskunden durchzuführen. Sofern von der Datenschutzverletzung eine hohe Anzahl an Nicht-Vertragskunden betroffen ist, wird der ISP diese mittels öffentlicher Bekanntmachung der Datenschutzverletzung informieren.

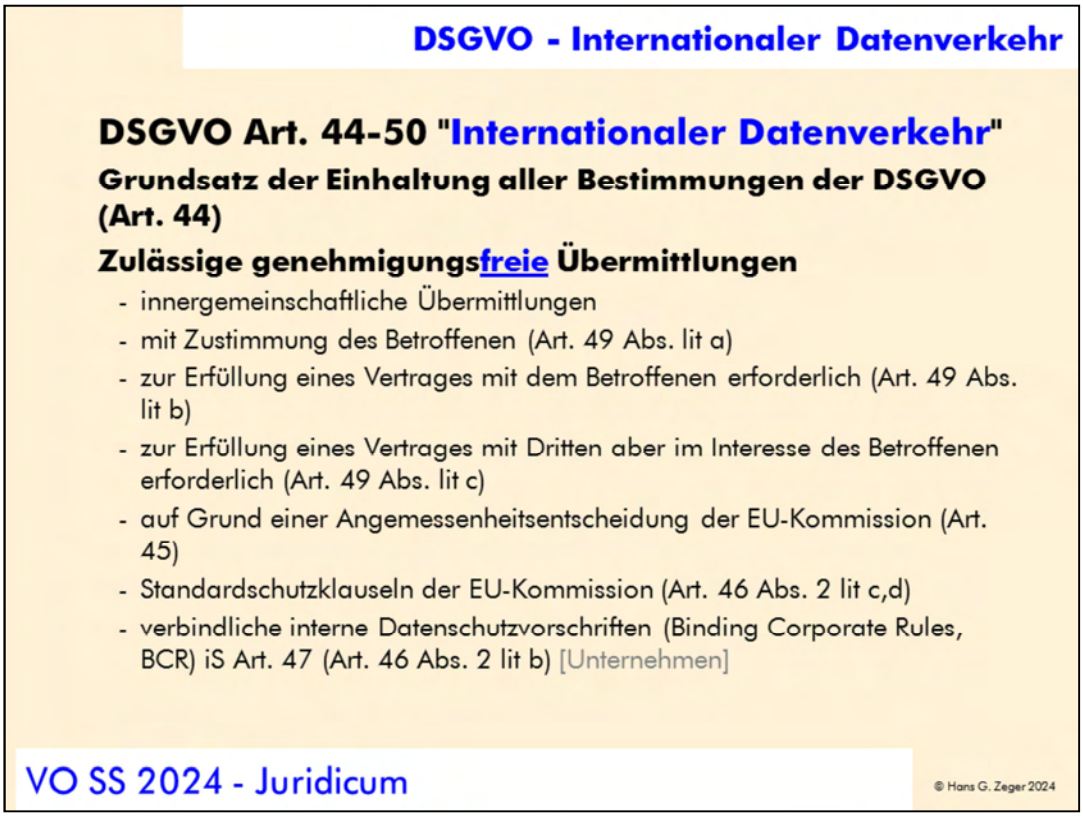
Bemessungskriterien

6. Die unterzeichnenden ISPs bemessen die drohende Schadensschwere sowie dessen Eintrittswahrscheinlichkeit jeweils im Einzelfall anhand der Art des Sicherheitsvorfalls, der Kategorien der betroffenen Daten sowie der sich daraus ergebenden Missbrauchsmöglichkeiten durch Dritte.

7. Insbesondere wird dabei berücksichtigt ob eines der folgenden Szenarios droht:
a. Verlust der Kontrolle über die Daten,
b. Diskriminierung,
c. Identitätsdiebstahl oder -betrug,
d. finanzielle Verluste,
e. unbefugte Aufhebung der Pseudonymisierung,
f. Rufschädigung
g. Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

8. Durch technische und organisatorische Maßnahmen, die der ISP in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat oder ergreifen wird, kann die Eintrittswahrscheinlichkeit entsprechend gesenkt werden.

9. Ein **hohes Risiko** für materielle und immaterielle Schäden beim Betroffenen wird von den unterzeichnenden Unternehmen insbesondere dann angenommen, **wenn unverkürzte Kreditkartennummern, Passwörter oder Kommunikationsinhalte betroffen sind**.



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

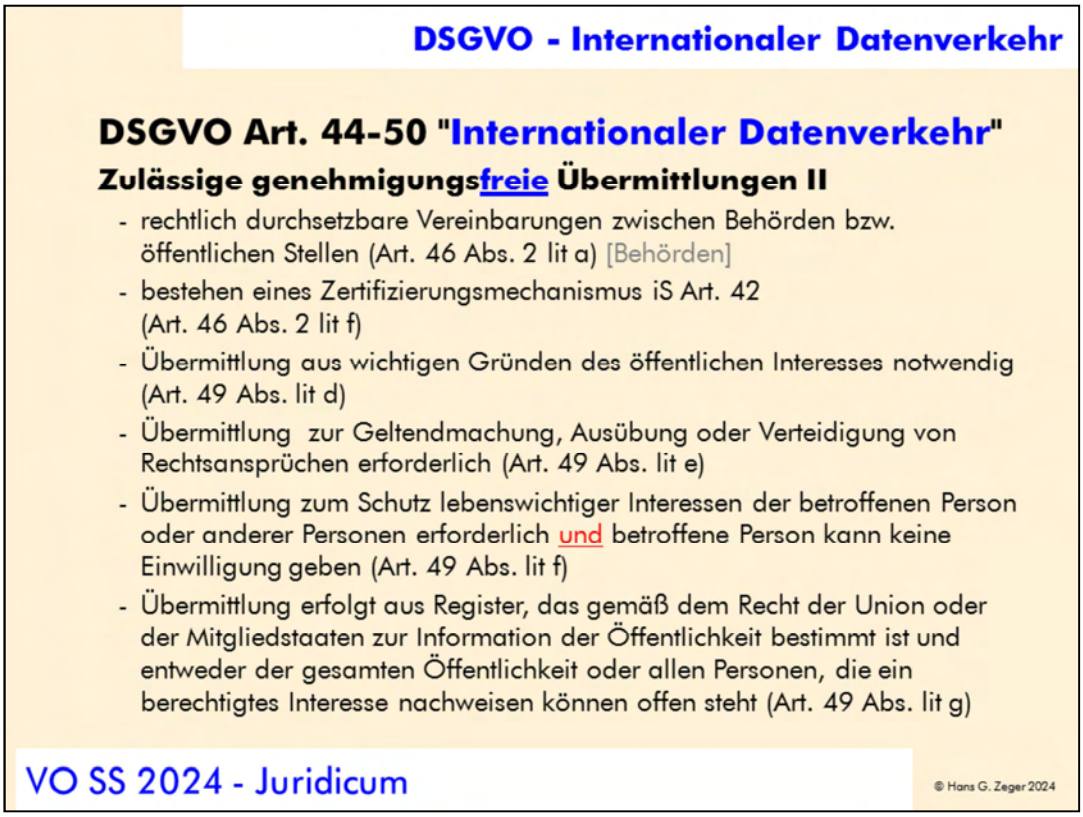
(1)Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale 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. 49 Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,

b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,

c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,

d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,

e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,

f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 — einschließlich der verbindlichen internen Datenschutzvorschriften — gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.

(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

(5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.

(6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.

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.

Aktueller Stand der gleichwertigen Länder:

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
(STAND: 3/2024)

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 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 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;

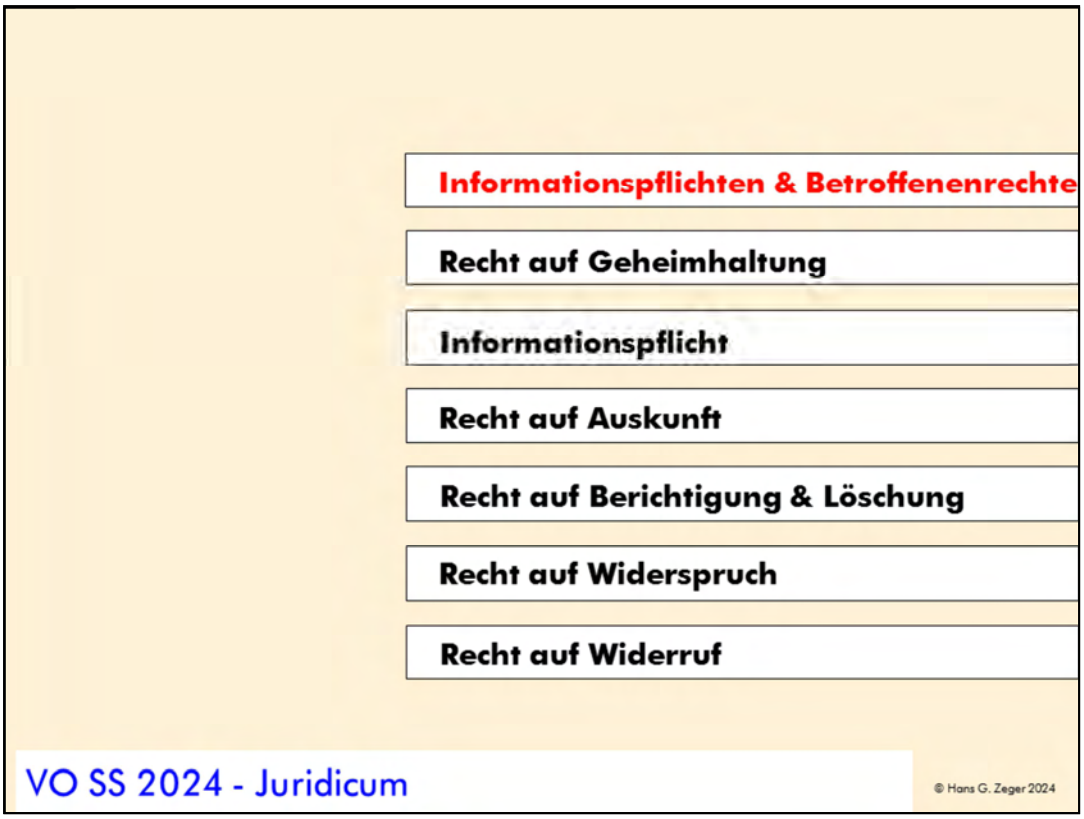
k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

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;

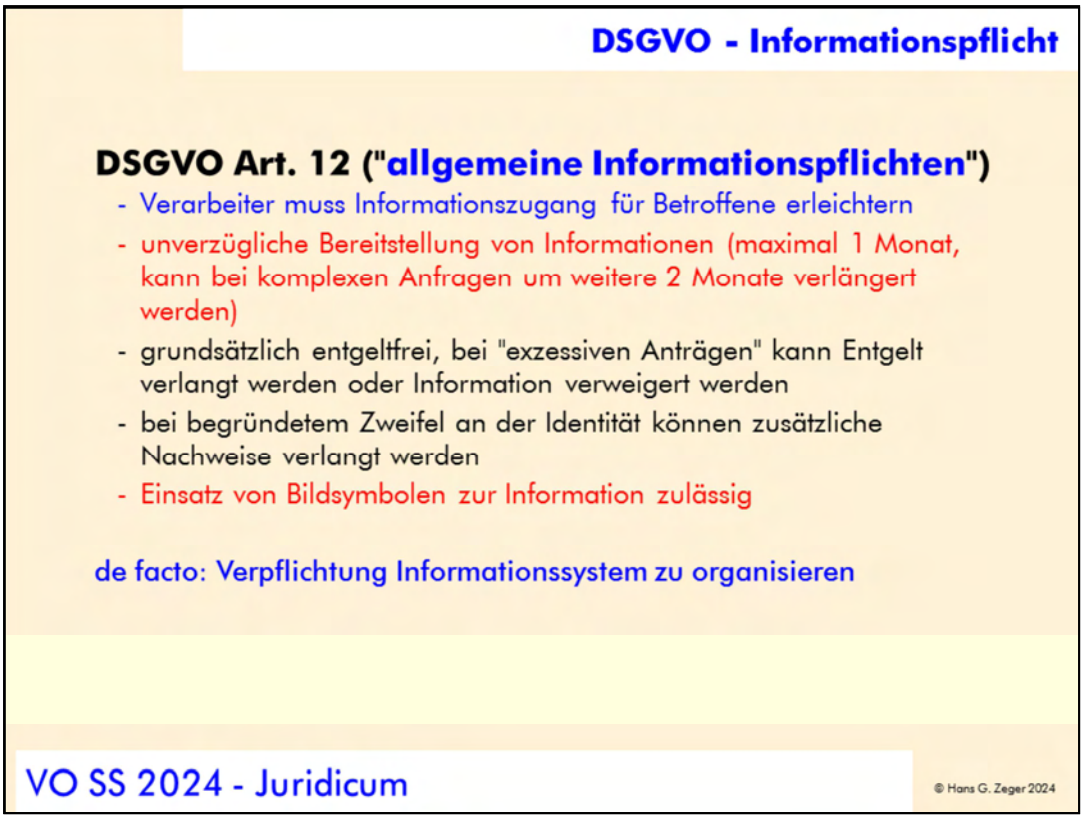
m)die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken 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 SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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 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;

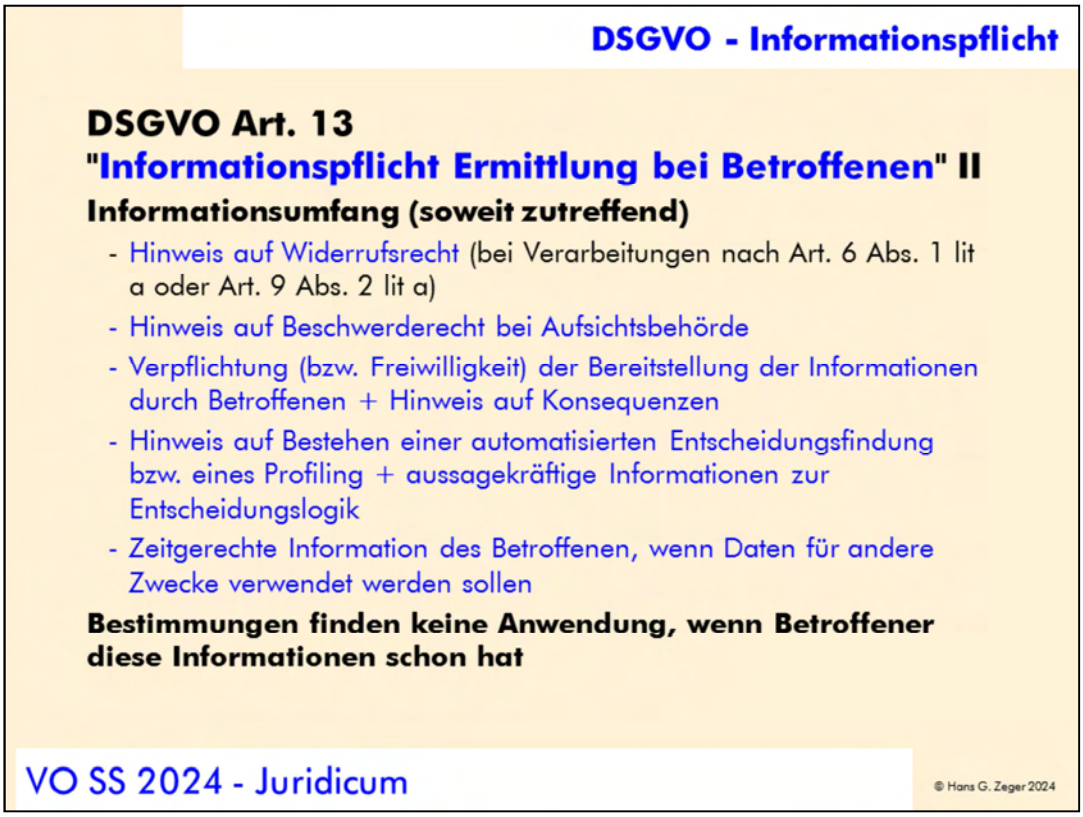
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

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 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 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:

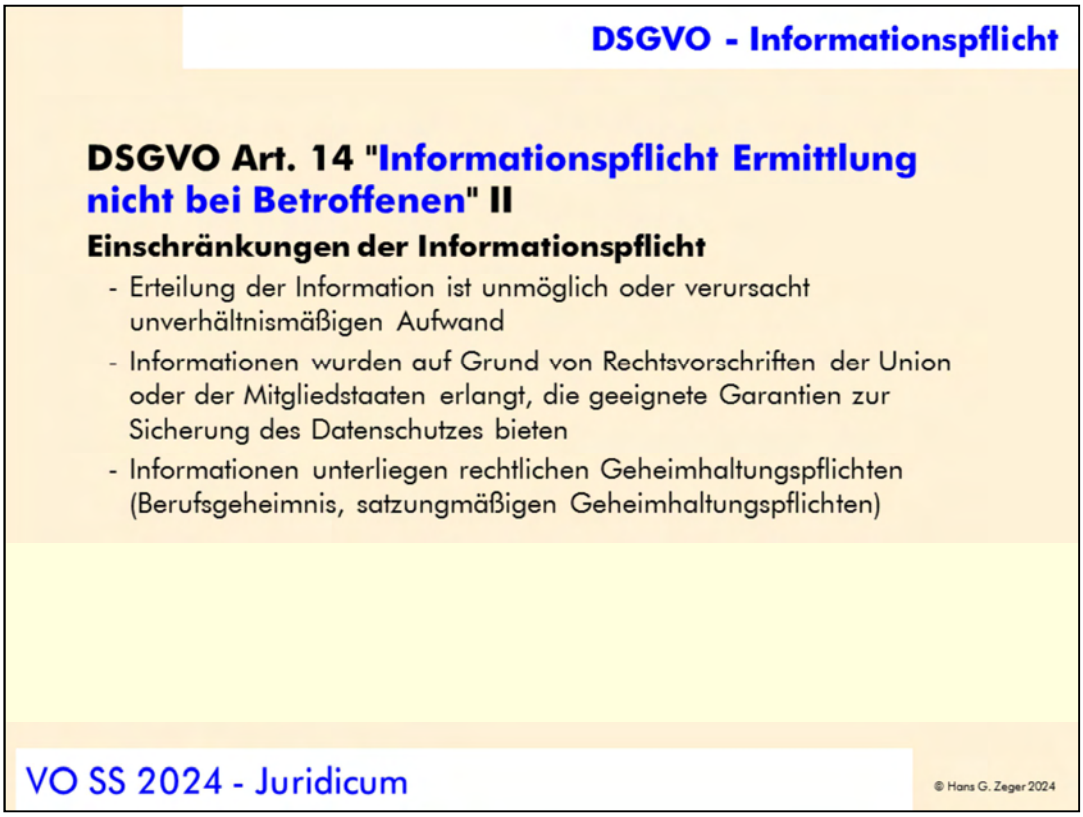
a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

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.

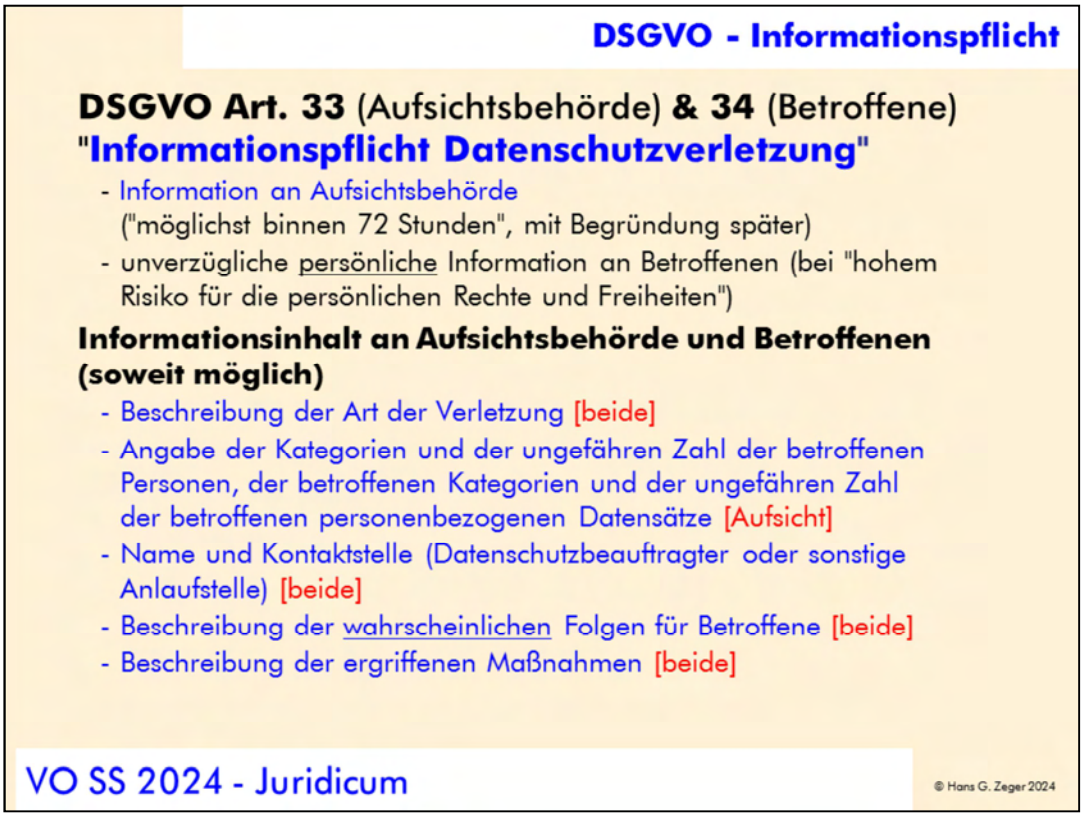
(5)Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

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 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.

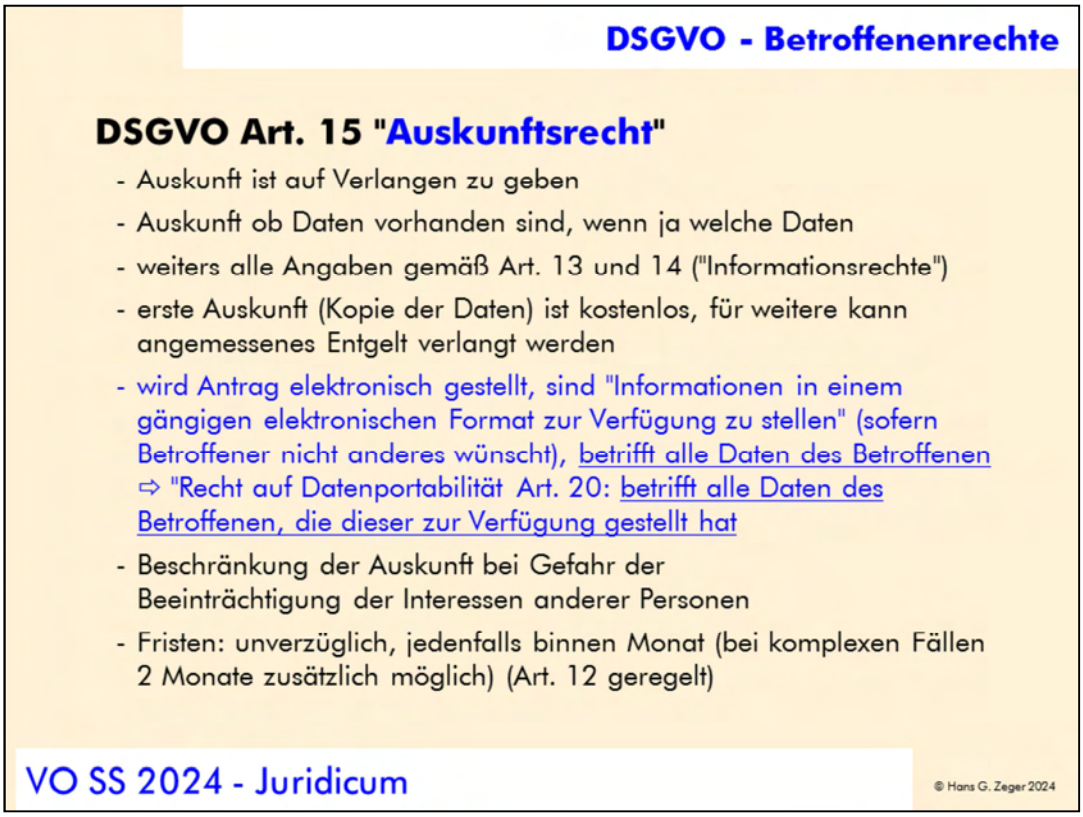
(3)Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

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;

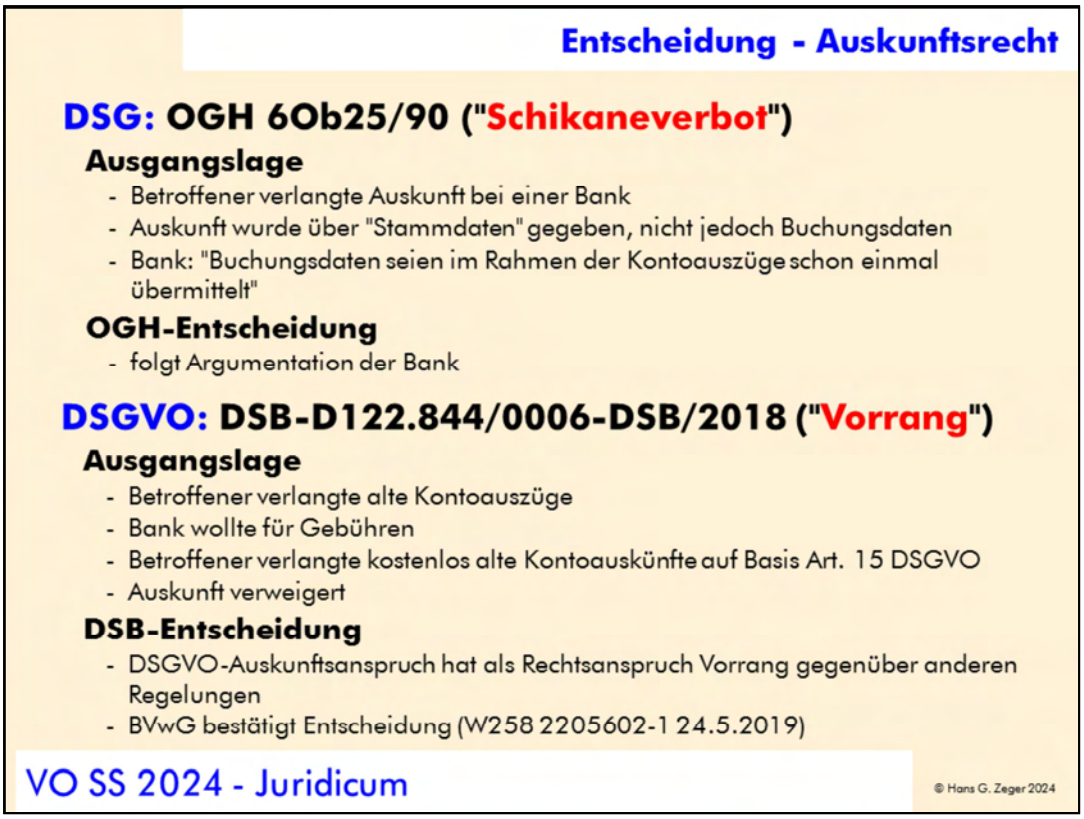
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

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.

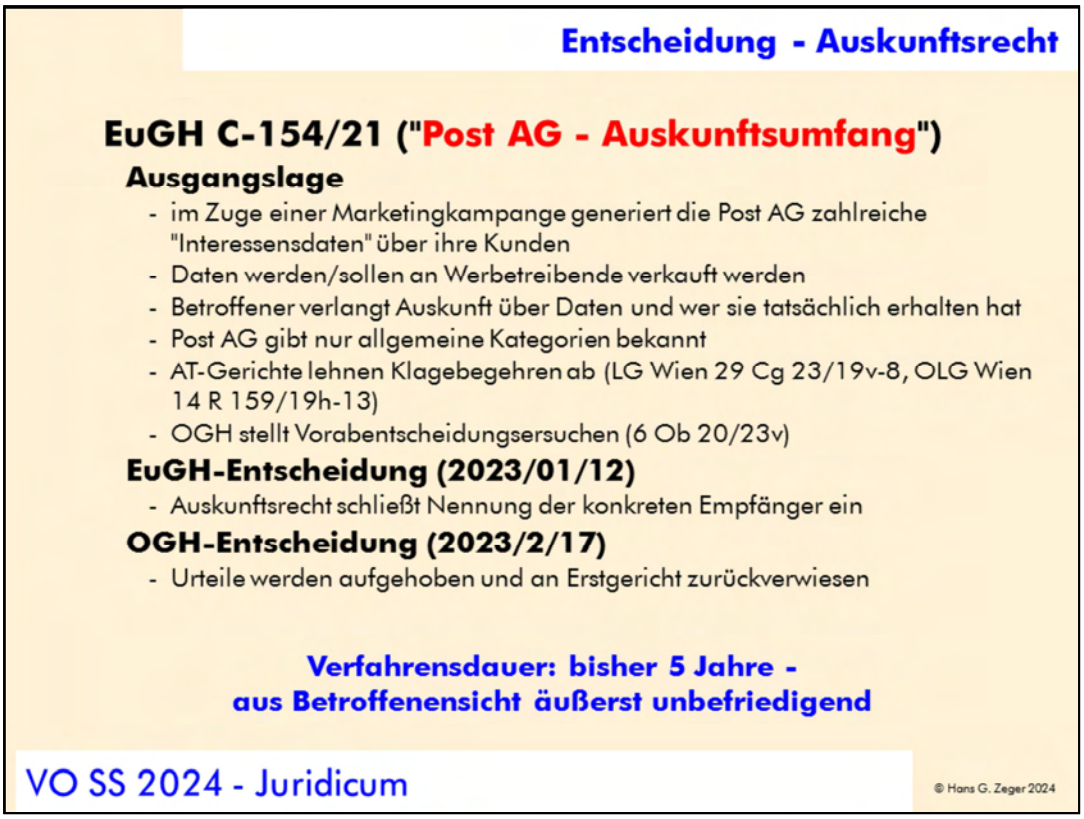


DSGVO Art. 15 Auskunftsrecht der betroffenen Person (Fortsetzung)

(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
EuGH C-154/21 ("Post AG - Auskunftsumfang")
Ausgangslage
- im Zuge einer Marketingkampange generiert die Post AG zahlreiche "Interessensdaten" über ihre Kunden
- Daten werden/sollen an Werbetreibende verkauft werden
- Betroffener verlangt Auskunft über Daten und wer sie tatsächlich erhalten hat
- Post AG gibt nur allgemeine Kategorien bekannt
- AT-Gerichte lehnen Klagebegehren ab (LG Wien 29 Cg 23/19v-8, OLG Wien 14 R 159/19h-13)
- OGH stellt Vorabentscheidungsersuchen (6 Ob 20/23v)
EuGH-Entscheidung (2023/01/12)
- Auskunftsrecht schließt Nennung der konkreten Empfänger ein
OGH-Entscheidung (2023/2/17)
- Urteile werden aufgehoben und an Erstgericht zurückverwiesen
Verfahrensdauer: bisher 5 Jahre -
aus Betroffenensicht äußerst unbefriedigend
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-

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.

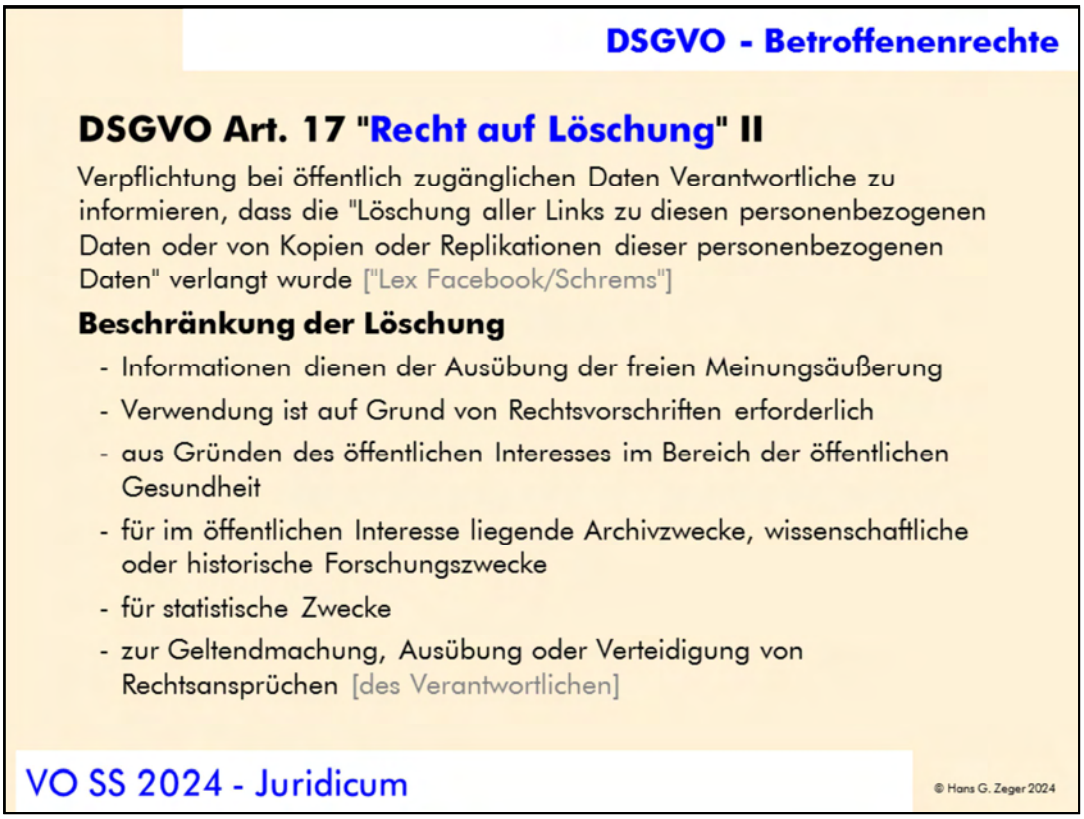
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

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 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

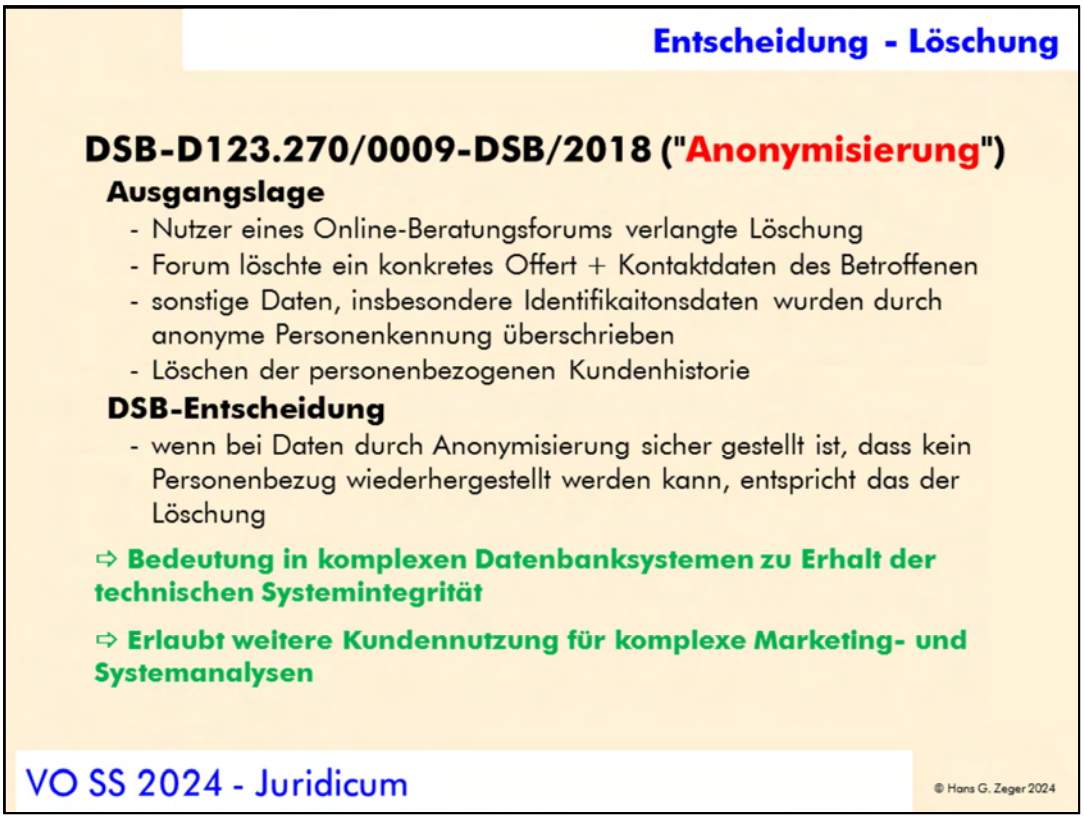
a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

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.



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.

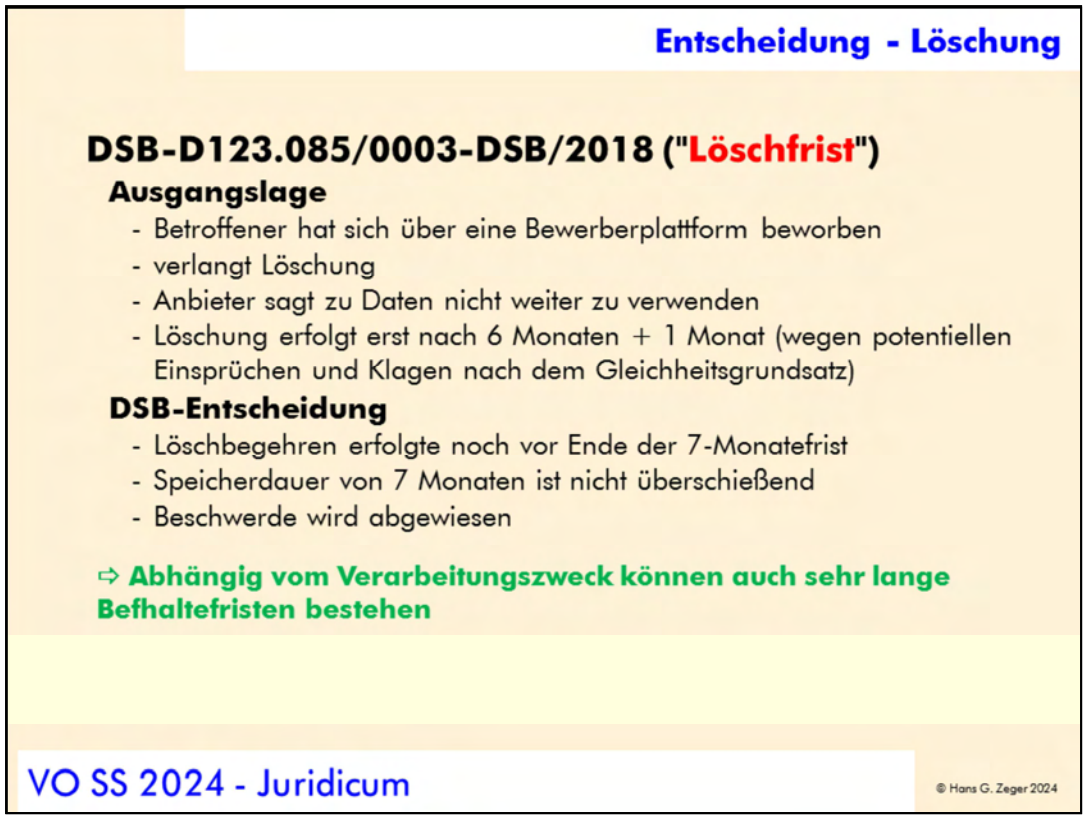
4) Die nun inhaltsleere Kundenverbindung sei nur mehr Max Mustermann zugeordnet.

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).

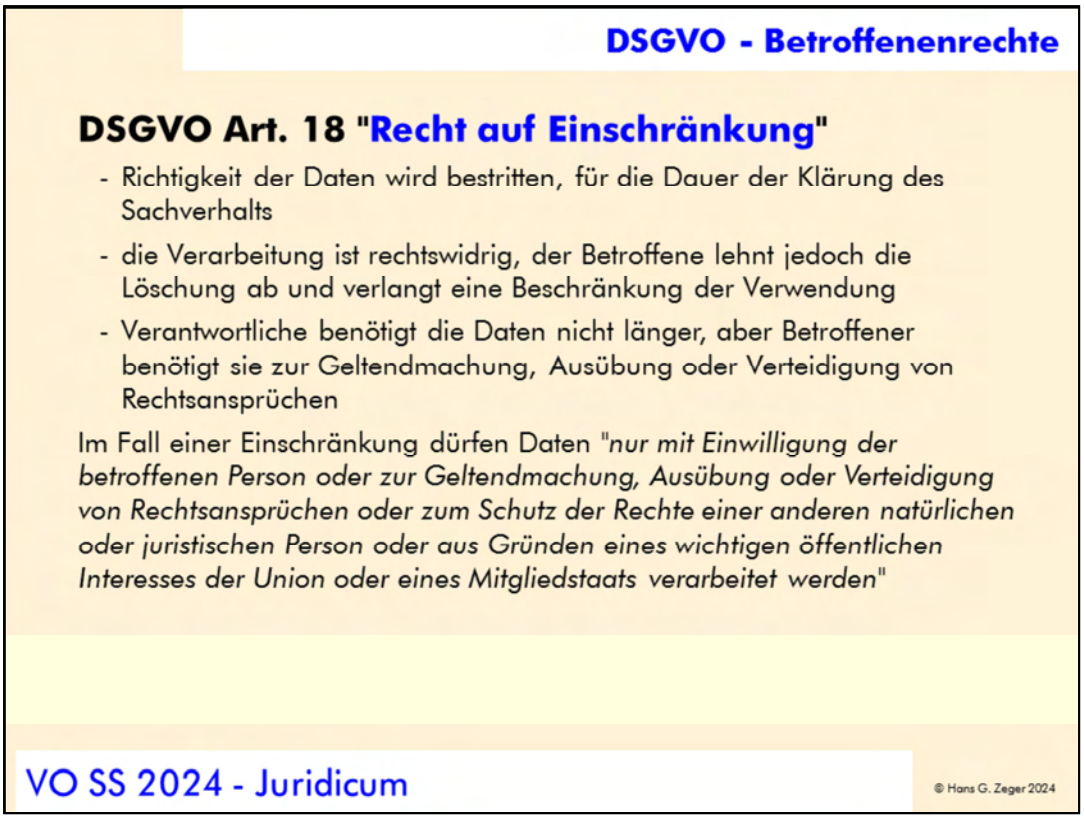
Durch die Umsetzung all dieser beschriebenen Schritte sei eine faktische Anonymisierung der ursprünglichen Kundenverbindung durch das Überschreiben mit einer „Dummy Kundenverbindung" herbeigeführt worden. Es wären nunmehr keine personenbezogenen Daten und somit keine identifizierenden Merkmale vorhanden, 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.



DSB-D123.085/0003-DSB/2018
Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Richard A*** (Beschwerdeführer) vom 26. Juni 2018 gegen die N*** Personaldienstleistungen GmbH (Beschwerdegegnerin) wegen Verletzung im Recht auf Löschung wie folgt:
- Die Beschwerde wird abgewiesen.

Rechtsgrundlagen: Art. 17 Abs. 3 lit e, 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 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999 idgF; §§ 17 Abs. 1 Z 1, 26 Abs. 1 und 29 Abs. 1 des Bundesgesetzes über die Gleichbehandlung (Gleichbehandlungsgesetz - GlBG), BGBl. I Nr. 66/2004 idgF.
...
Für den Beschwerdeführer ist somit klar erkennbar, ab welchem Zeitpunkt seine Bewerberdaten gelöscht werden. Darüber hinaus erklärte sich die Beschwerdegegnerin auch bereit, die Bewerberdaten des Beschwerdeführers zum ehest möglichen Zeitpunkt zu löschen, also nach Ablauf der Frist von § 29 Abs. 1 GlBG (gegenständlich sieben Monate nach Bewerbungseingang, somit berechnet ab dem 17. Mai 2018 bzw. 11. Juni 2018).
Der zusätzlich berechnete Monat zu der sechsmonatigen Frist nach § 29 Abs. 1 GlBG, um einen potenziellen Klageweg einzuberechnen, sohin sieben Monate ab Bewerbungseingang, ist angemessen und nicht unverhältnismäßig lange. Die Beschwerdegegnerin erklärte sich ebenfalls dazu bereit, die gegenständlichen Bewerberdaten zwecks Verteidigung gegen einen Ersatzanspruch nach dem GlBG aufzubewahren, und diese nicht mehr für die Besetzung etwaiger Stellen heranzuziehen.

D. 4 Ergebnis
Im vorliegenden Fall ist die sechsmonatige Frist von § 29 Abs. 1 GlBG (bzw. sieben Monate ab Bewerbungseingang) zum Zeitpunkt der Entscheidung der Datenschutzbehörde noch nicht abgelaufen.
Vor diesem Hintergrund liegen die Voraussetzungen von Art. 17 Abs. 3 lit e DSGVO vor, weshalb im Ergebnis ein Löschungsanspruch zu verneinen ist.



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,

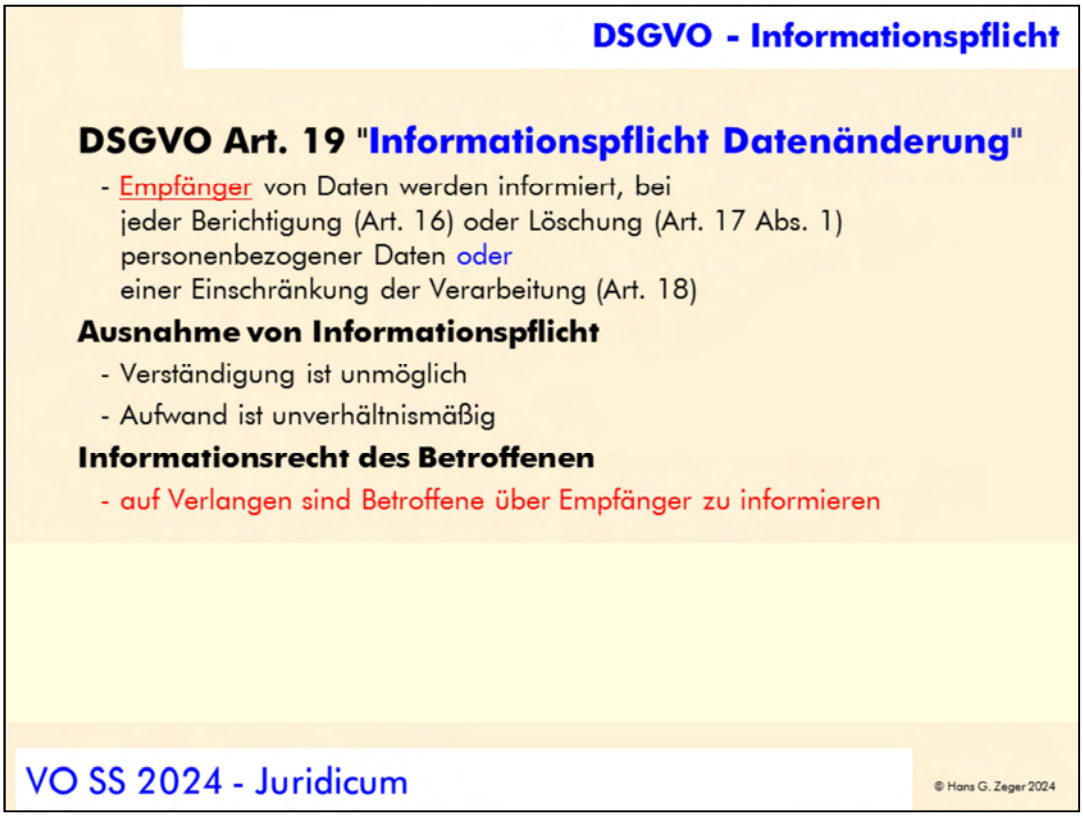
b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

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.

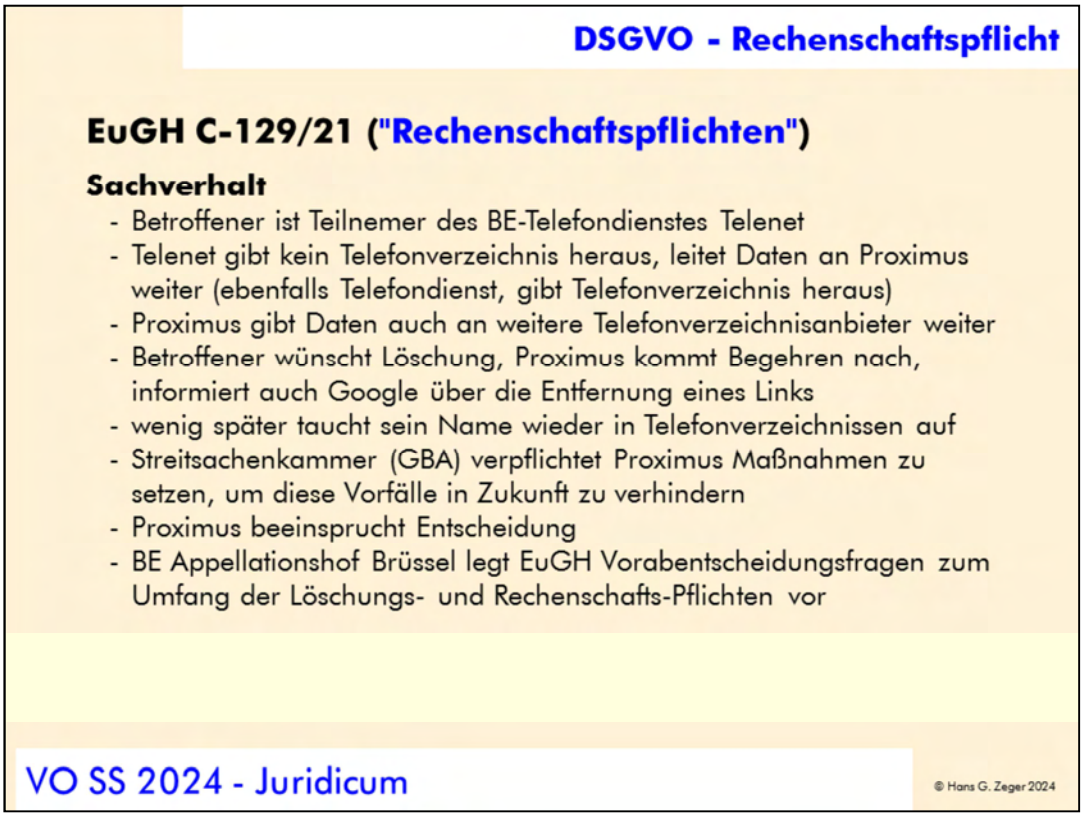
(2)Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten — von ihrer Speicherung abgesehen — nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen 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 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.



EuGH Entscheidung C-129/21

36 Unter diesen Umständen hat der Hof van beroep te Brussel (Appellationshof Brüssel) beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 12 Abs. 2 der Richtlinie 2002/58 in Verbindung mit Art. 2 Buchst. f dieser Richtlinie und Art. 95 DSGVO dahin auszulegen, dass es zulässig ist, dass eine nationale Aufsichtsbehörde mangels anderslautender nationaler Rechtsvorschriften eine „Einwilligung" des Teilnehmers im Sinne der DSGVO als Grundlage für die Veröffentlichung seiner personenbezogenen Daten in öffentlich zugänglichen Teilnehmerverzeichnissen und Telefonauskunftsdiensten, die vom Betreiber selbst oder von Drittanbietern herausgegeben werden, verlangt?

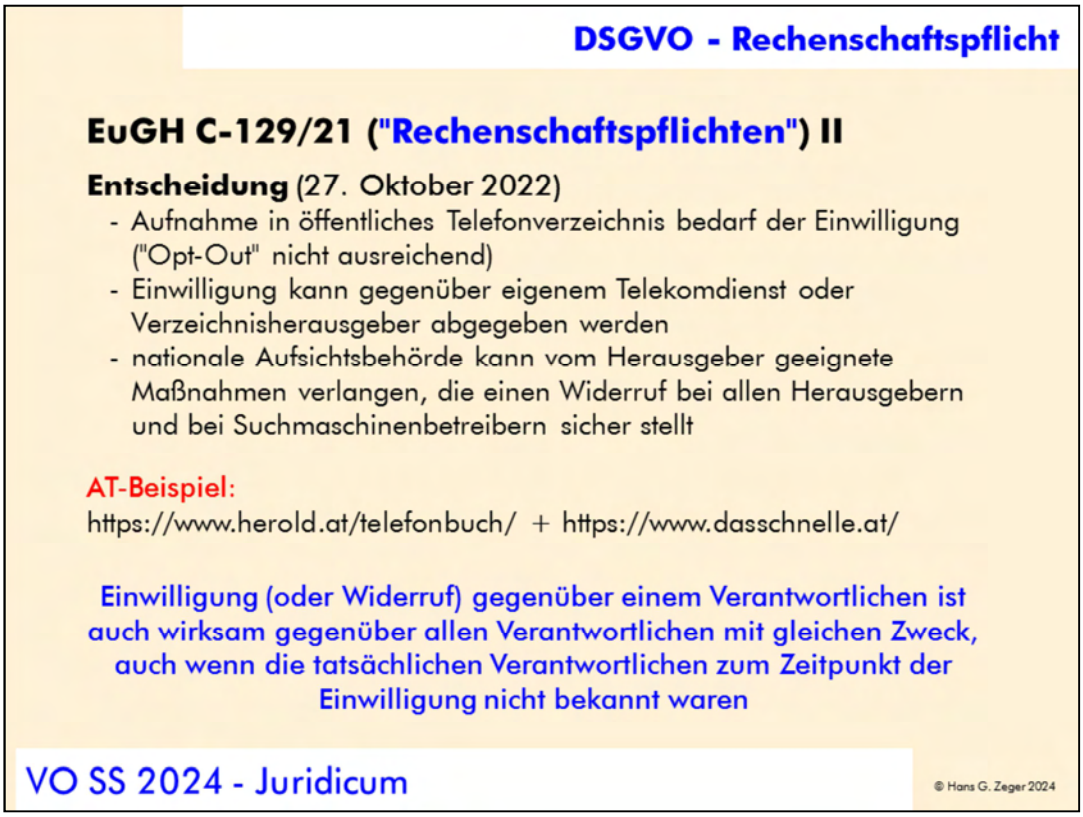
2. Ist das Recht auf Löschung nach Art. 17 DSGVO dahin auszulegen, dass es dem entgegensteht, dass eine nationale Aufsichtsbehörde einen Antrag eines Teilnehmers auf Löschung aus öffentlich zugänglichen Teilnehmerverzeichnissen und Telefonauskunftsdiensten als einen Antrag auf Löschung im Sinne von Art. 17 DSGVO einstuft?

3. Sind Art. 24 und Art. 5 Abs. 2 DSGVO dahin auszulegen, dass sie dem entgegenstehen, dass eine nationale Aufsichtsbehörde aus der darin verankerten Rechenschaftspflicht ableitet, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen ergreifen muss, um weitere Verantwortliche, nämlich den Telefondienstanbieter und andere Anbieter von Teilnehmerverzeichnissen und Telefonauskunftsdiensten, die Daten von dem erstgenannten Verantwortlichen empfangen haben, über den Widerruf der Einwilligung durch die betroffene Person gemäß Art. 6 in Verbindung mit Art. 7 DSGVO zu informieren?

4. Ist Art. 17 Abs. 2 DSGVO dahin auszulegen, dass er dem entgegensteht, dass eine nationale Aufsichtsbehörde einem Anbieter öffentlich zugänglicher Teilnehmerverzeichnisse und Telefonauskunftsdienste, bei dem beantragt wird, die Daten einer Person nicht mehr zu veröffentlichen, aufgibt, angemessene Maßnahmen zu treffen, um Suchmaschinen über diesen Antrag auf Löschung zu informieren?

...

78 Insoweit ist erstens daran zu erinnern, dass nach Art. 6 Abs. 1 Buchst. a DSGVO eine Verarbeitung rechtmäßig ist, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat. Aus der Vorlageentscheidung ergibt sich jedoch, dass der Beschwerdeführer seine Einwilligung zur Verarbeitung seiner personenbezogenen Daten zum Zweck der Veröffentlichung in Teilnehmerverzeichnissen im Sinne von Art. 7 Abs. 3 DSGVO widerrufen hat.



EuGH Entscheidung C-129/21 (Fortsetzung)

Nach einem solchen Widerruf hat die Verarbeitung dieser Daten zum Zweck ihrer Aufnahme in öffentliche Teilnehmerverzeichnisse – wozu auch die Verarbeitung zählt, die von Telefondienstanbietern oder anderen Anbietern von Teilnehmerverzeichnissen, die sich auf dieselbe Einwilligung stützen, zu demselben Zweck vorgenommen wird – keine Rechtsgrundlage mehr und ist somit nach Maßgabe von Art. 6 Abs. 1 Buchst. a DSGVO rechtswidrig.

...

82 In diesem Sinne sieht Art. 19 DSGVO u. a. vor, dass der Verantwortliche allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Löschung der personenbezogenen Daten nach Art. 17 Abs. 1 dieser Verordnung mitteilt, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

...

83 Aus den allgemeinen Verpflichtungen nach Art. 5 Abs. 2 und Art. 24 DSGVO in Verbindung mit deren Art. 19 ergibt sich, dass ein für die Verarbeitung personenbezogener Daten Verantwortlicher wie Proximus geeignete technische und organisatorische Maßnahmen ergreifen muss, um die anderen Anbieter von Teilnehmerverzeichnissen, denen er solche Daten geliefert hat, über den an ihn gerichteten Widerruf der Einwilligung der betroffenen Person zu informieren. Unter Umständen wie den in Rn. 76 des vorliegenden Urteils beschriebenen muss ein solcher Verantwortlicher auch den Telefondienstanbieter, der ihm die personenbezogenen Daten übermittelt hat, informieren, damit dieser die Liste der personenbezogenen Daten, die er dem Anbieter von Teilnehmerverzeichnissen nach einem automatisierten Verfahren übermittelt, anpasst und die Daten seiner Teilnehmer herausfiltert, die ihren Willen bekundet haben, ihre Einwilligung zur Veröffentlichung dieser Daten zu widerrufen.

...

3. Art. 5 Abs. 2 und Art. 24 der Verordnung 2016/679 sind dahin auszulegen, dass eine nationale Aufsichtsbehörde verlangen kann, dass ein Anbieter von öffentlich zugänglichen Teilnehmerverzeichnissen und Telefonauskunftsdiensten als Verantwortlicher geeignete technische und organisatorische Maßnahmen ergreift, um weitere Verantwortliche, nämlich den Telefondienstanbieter, der ihm die personenbezogenen Daten seines Teilnehmers übermittelt hat, sowie die anderen Anbieter von öffentlich zugänglichen Teilnehmerverzeichnissen und Telefonauskunftsdiensten, denen er selbst solche Daten geliefert hat, über den Widerruf der Einwilligung dieses Teilnehmers zu informieren.

4. Art. 17 Abs. 2 der Verordnung 2016/679 ist dahin auszulegen, dass er es einer nationalen Aufsichtsbehörde nicht verwehrt, einen Anbieter von öffentlich zugänglichen Teilnehmerverzeichnissen und Telefonauskunftsdiensten, von dem der Teilnehmer eines Telefondienstanbieters verlangt hat, die ihn betreffenden personenbezogenen Daten nicht mehr zu veröffentlichen, zu verpflichten, „angemessene Maßnahmen“ im Sinne dieser Bestimmung zu ergreifen, um Suchmaschinenanbieter über diesen Antrag auf Löschung von Daten zu informieren.

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.

VO (EU) 2022/1925 ("Digital Markets Act", DMA)

Artikel 2 Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „**Torwächter**“ ein Unternehmen, das **zentrale Plattformdienste** bereitstellt und nach Artikel 3 benannt worden ist;
2. **„zentraler Plattformdienst“** die folgenden Dienste:

a) Online-Vermittlungsdienste,
b) Online-Suchmaschinen,
c) Online-Dienste sozialer Netzwerke,
d) Video-Sharing-Plattform-Dienste,
e) nummernunabhängige interpersonelle Kommunikationsdienste,
f) Betriebssysteme,
g) Webbrowser,
h) virtuelle Assistenten,
i) Cloud-Computing-Dienste,
j) Online-Werbedienste, einschließlich Werbenetzwerken, Werbebörsen und sonstiger Werbevermittlungsdienste, die von einem Unternehmen, das einen der unter den Buchstaben a bis i genannten zentralen Plattformdienste bereitstellt, bereitgestellt werden;

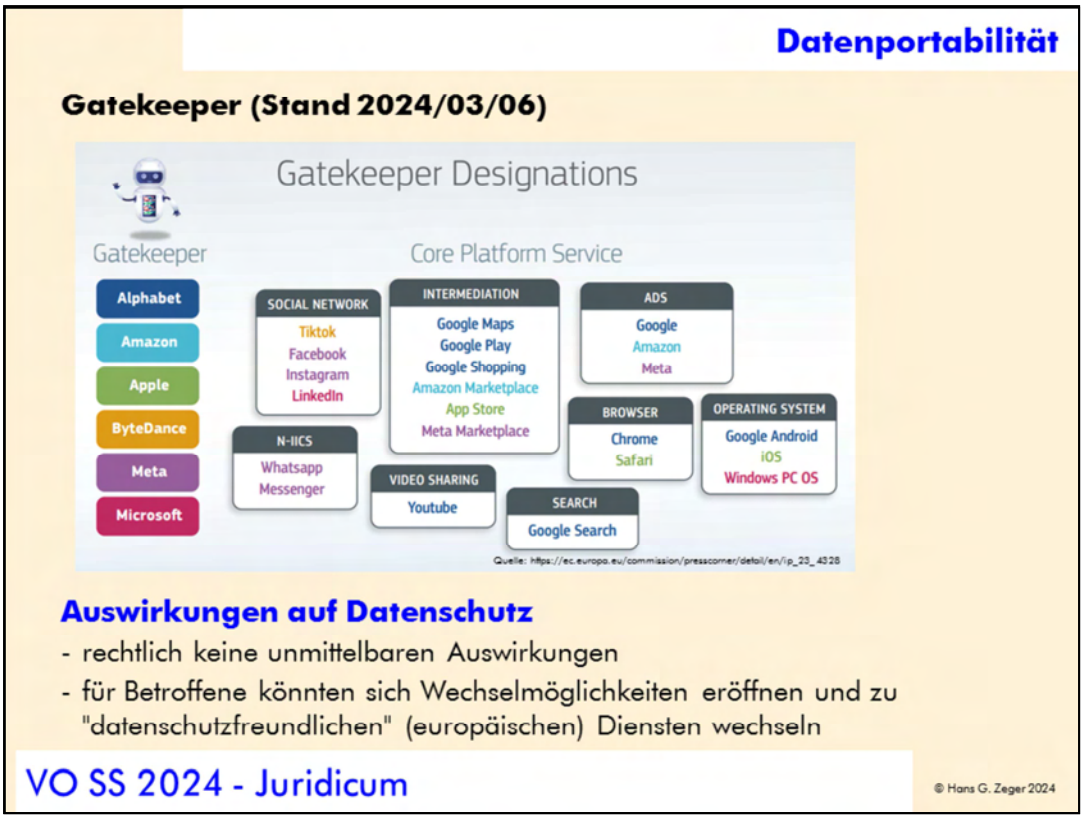
...

Artikel 3 Benennung von Torwächtern

(1) Ein Unternehmen wird als Torwächter benannt, wenn es
a) erheblichen Einfluss auf den Binnenmarkt hat,
b) einen zentralen Plattformdienst bereitstellt, der gewerblichen Nutzern als wichtiges Zugangstor zu Endnutzern dient, und
c) hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar ist, dass es eine solche Position in naher Zukunft erlangen wird.

(2) Es wird davon ausgegangen, dass ein Unternehmen die jeweiligen Anforderungen des Absatzes 1 erfüllt, wenn es
a) in Bezug auf Absatz 1 Buchstabe a in jedem der vergangenen drei Geschäftsjahre in der Union einen Jahresumsatz von mindestens 7,5 Mrd. EUR erzielt hat oder wenn seine durchschnittliche Marktkapitalisierung oder sein entsprechender Marktwert im vergangenen Geschäftsjahr mindestens 75 Mrd. EUR betrug und es in mindestens drei Mitgliedstaaten denselben zentralen Plattformdienst bereitstellt;
b) in Bezug auf Absatz 1 Buchstabe b einen zentralen Plattformdienst bereitstellt, der im vergangenen Geschäftsjahr mindestens 45 Millionen in der Union niedergelassene oder aufhältige monatlich aktive Endnutzer und mindestens 10 000in der Union niedergelassene jährlich aktive gewerbliche Nutzer hatte, wobei die Ermittlung und Berechnung gemäß der Methode und den Indikatoren im Anhang erfolgt;

...



VO (EU) 2022/1925 ("Digital Markets Act", DMA) (Fortsetzung)

c) in Bezug auf Absatz 1 Buchstabe c die unter Buchstabe b des vorliegenden Absatzes genannten Schwellenwerte in jedem der vergangenen drei Geschäftsjahre erreicht hat.

(3) Wenn ein Unternehmen, das zentrale Plattformdienste bereitstellt, alle in Absatz 2 genannten Schwellenwerte erreicht, teilt es dies der Kommission unverzüglich, in jedem Fall aber innerhalb von zwei Monaten nach Erreichen der Schwellenwerte mit und übermittelt ihr die in Absatz 2 genannten einschlägigen Angaben. Die entsprechende Mitteilung muss die in Absatz 2 genannten einschlägigen Angaben für jeden zentralen Plattformdienst des Unternehmens enthalten, der die in Absatz 2 Buchstabe b genannten Schwellenwerte erreicht. Erreicht ein weiterer zentraler Plattformdienst, der von dem zuvor als Torwächter benannten Unternehmen erbracht wird, die in Absatz 2 Buchstaben b und c genannten Schwellenwerte, so teilt das Unternehmen dies der Kommission innerhalb von zwei Monaten nach Erreichen dieser Schwellenwerte mit

Versäumt es das Unternehmen, das den zentralen Plattformdienst bereitstellt, die Kommission gemäß Unterabsatz 1 des vorliegenden Absatzes zu benachrichtigen und innerhalb der von der Kommission in dem Auskunftsverlangen gemäß Artikel 21 gesetzten Frist alle einschlägigen Angaben zu übermitteln, die die Kommission benötigt, um das betroffene Unternehmen gemäß Absatz 4 des vorliegenden Artikels als Torwächter zu benennen, so ist die Kommission dennoch berechtigt, das Unternehmen auf der Grundlage der ihr vorliegenden Angaben als Torwächter zu benennen.

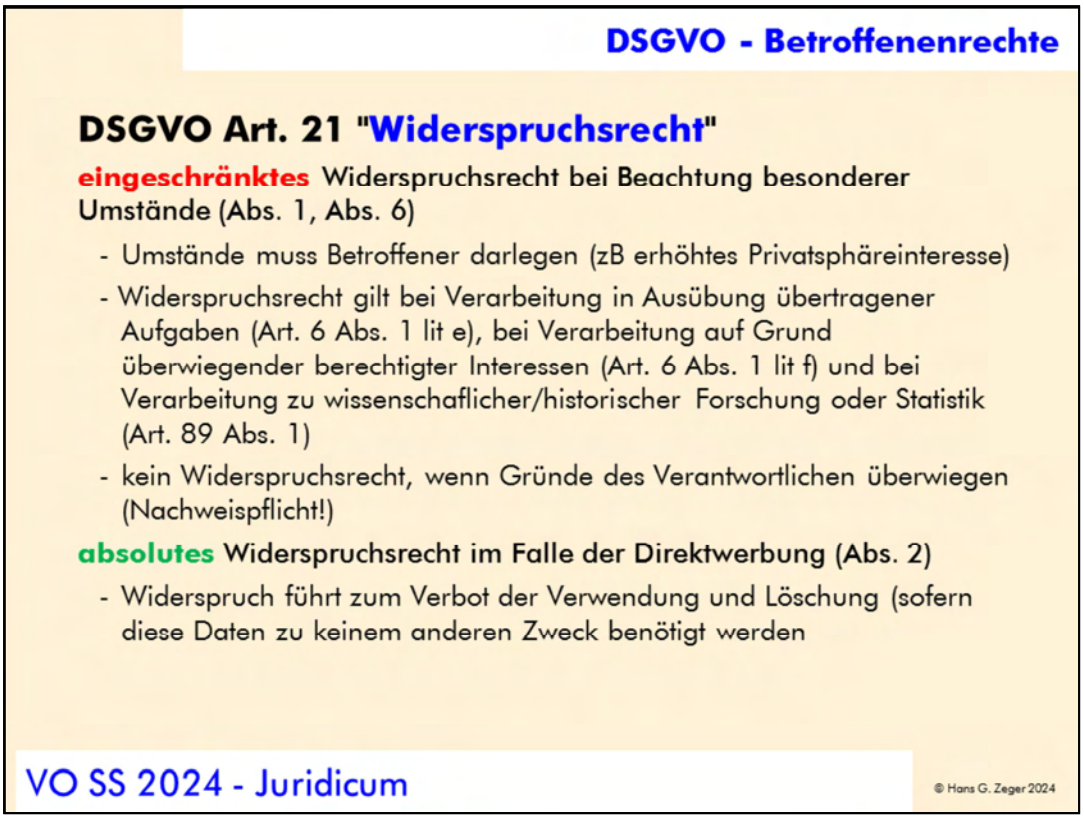
Kommt das Unternehmen, das zentrale Plattformdienste bereitstellt, dem Auskunftsverlangen gemäß Unterabsatz 2 des vorliegenden Absatzes nach oder werden die Informationen übermittelt nachdem die in jenem Unterabsatz genannte Frist abgelaufen ist, so wendet die Kommission das Verfahren nach Absatz 4 an.

(4) Die Kommission benennt ein Unternehmen, das zentrale Plattformdienste bereitstellt und alle in Absatz 2 genannten Schwellenwerte erreicht, unverzüglich und spätestens innerhalb von 45 Arbeitstagen nach Erhalt der vollständigen Angaben nach Absatz 3 als Torwächter.

(5) Das Unternehmen, das zentrale Plattformdienste bereitstellt, kann im Rahmen seiner Mitteilung hinreichend substanziierte Argumente dafür vorbringen, dass es in Anbetracht der Umstände, unter denen der betreffende zentrale Plattformdienst bereitgestellt wird, die in Absatz 1 aufgeführten Anforderungen ausnahmsweise nicht erfüllt, obwohl es alle in Absatz 2 genannten Schwellenwerte erreicht.

Ist die Kommission der Auffassung, dass die von dem Unternehmen, das zentrale Plattformdienste bereitstellt, gemäß Unterabsatz 1 vorgebrachten Argumente nicht hinreichend substanziiert sind, weil sie die Vermutungen nach Absatz 2 dieses Artikels nicht eindeutig entkräften, so kann sie diese Argumente innerhalb der in Absatz 4 genannten Frist zurückweisen, ohne das Verfahren nach Artikel 17 Absatz 3 anzuwenden.

...



DSGVO Art. 21 Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

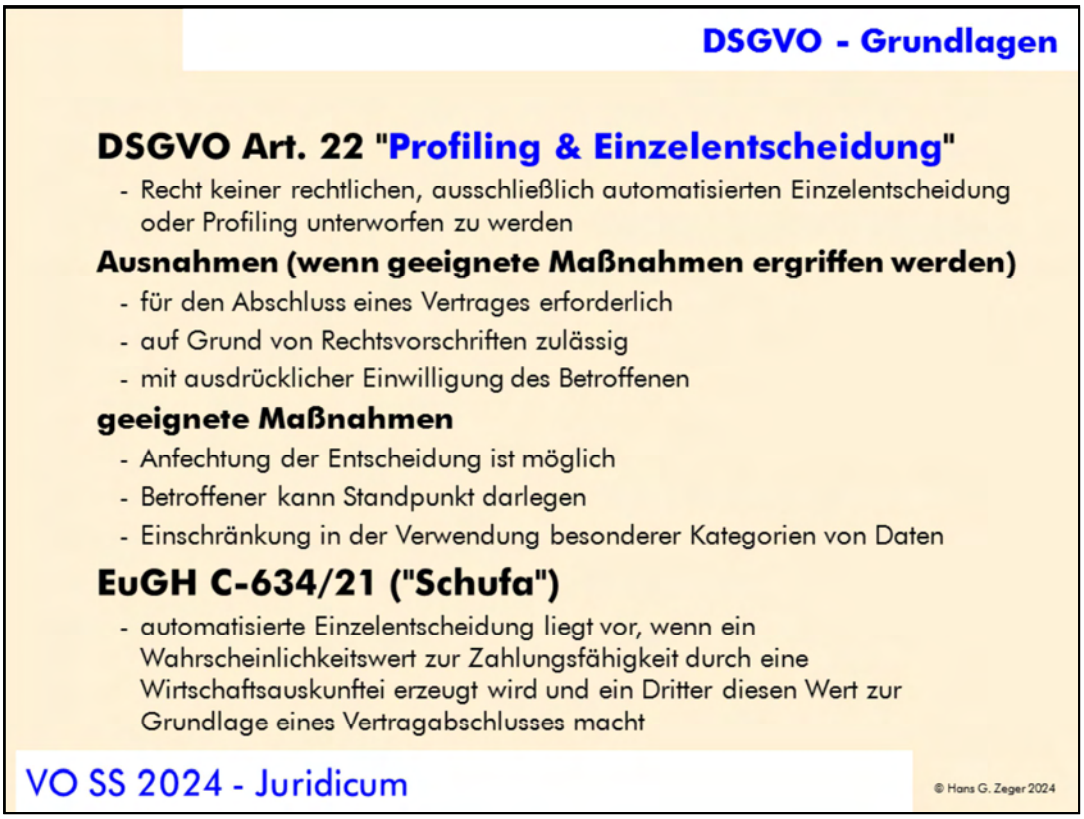
(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

(4) Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in den Absätzen 1 und 2 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(5) Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

(6) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1 erfolgt, Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.



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.

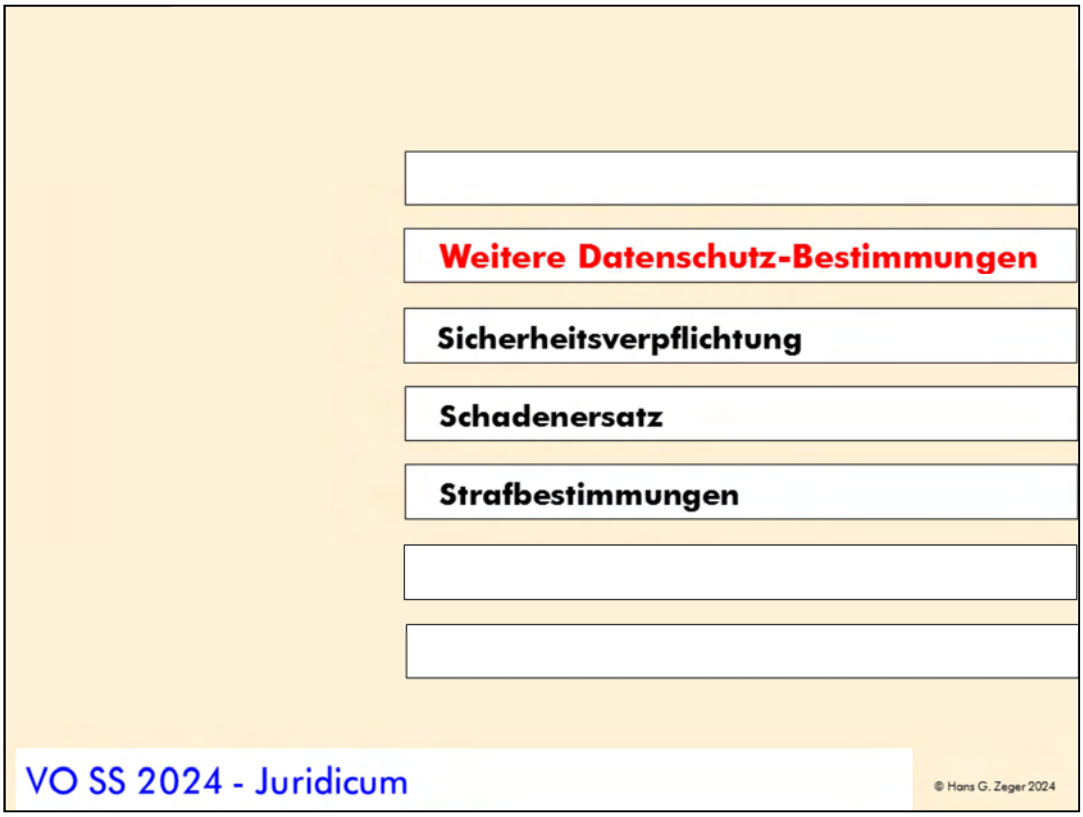
(4)Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person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

EuGH Entscheidung C-634/21

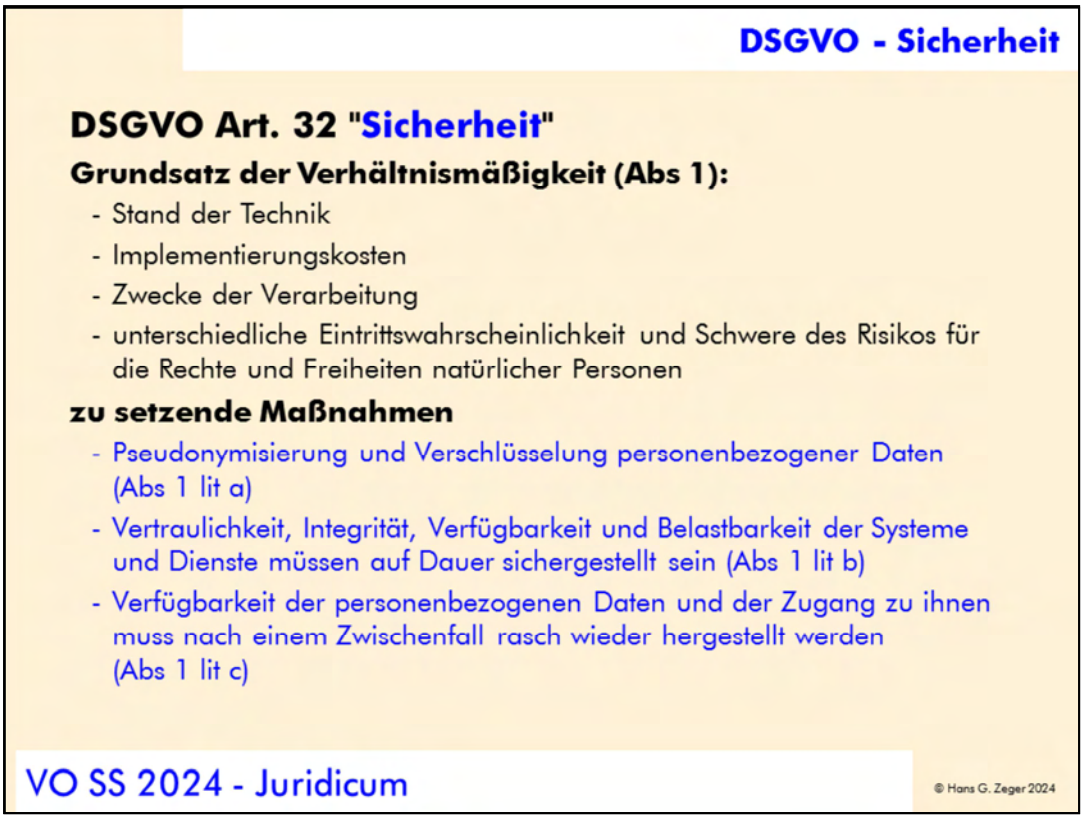
Art. 22 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
ist dahin auszulegen, dass
eine „automatisierte Entscheidung im Einzelfall“ im Sinne dieser Bestimmung vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet.


DSGVO - Grundlagen
Beispiele "Profiling & E-Commerce"
Produktpräsentation
- Vorschläge bestimmte Produkte zu kaufen, abhängig von:
-- besuchten Webseiten
-- Produkten im Warenkorb
-- Angaben in den Stammdaten (Alter, Wohnort, ...)
Zahlungsangebote
- Auswahlmöglichkeit bestimmte Zahlungsarten, abhängig von:
-- Angaben in den Stammdaten (Alter, Wohnort, ...)
-- früheres Zahlungsverhalten
-- technische Informationen des verwendeten Gerätes (Betriebssystem, Browser, Fonts, PlugIns, ...)
Preisgestaltung / Konditionen
- Preise, abhängig von:
-- früheres Zahlungsverhalten
-- technische Informationen des verwendeten Gerätes
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Weitere Datenschutz-Bestimmungen
Sicherheitsverpflichtung
Schadenersatz
Strafbestimmungen
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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;

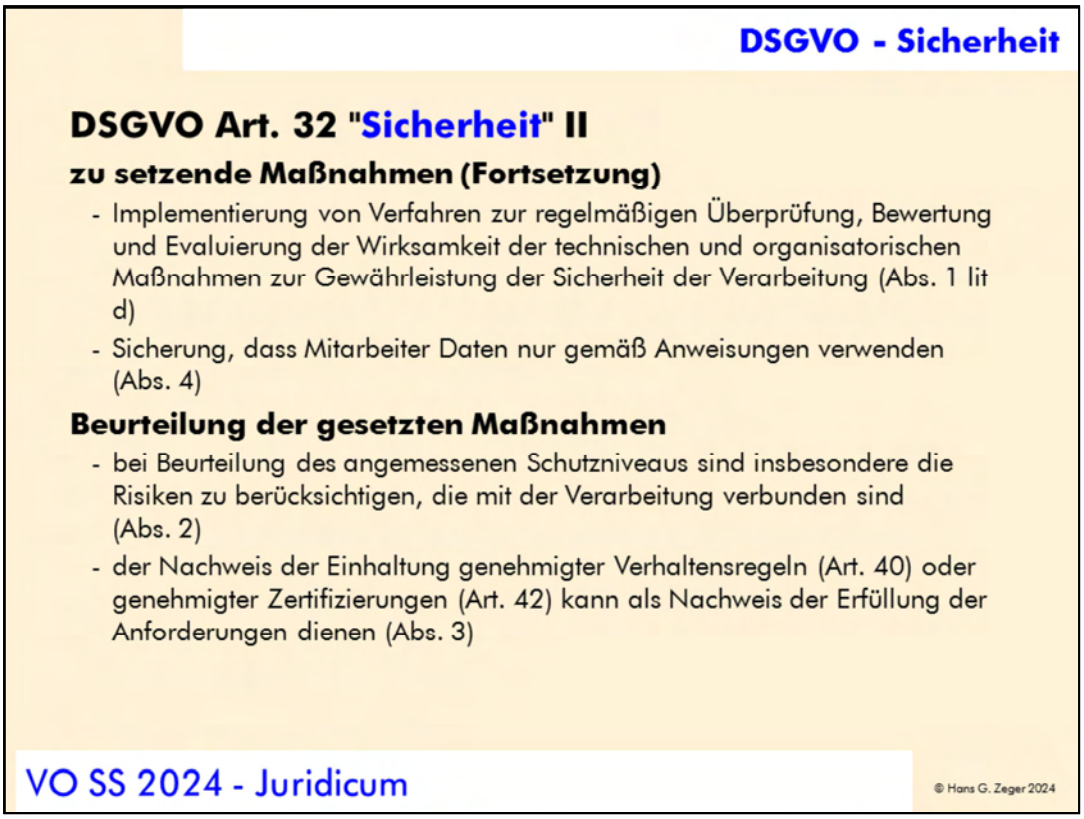
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

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.

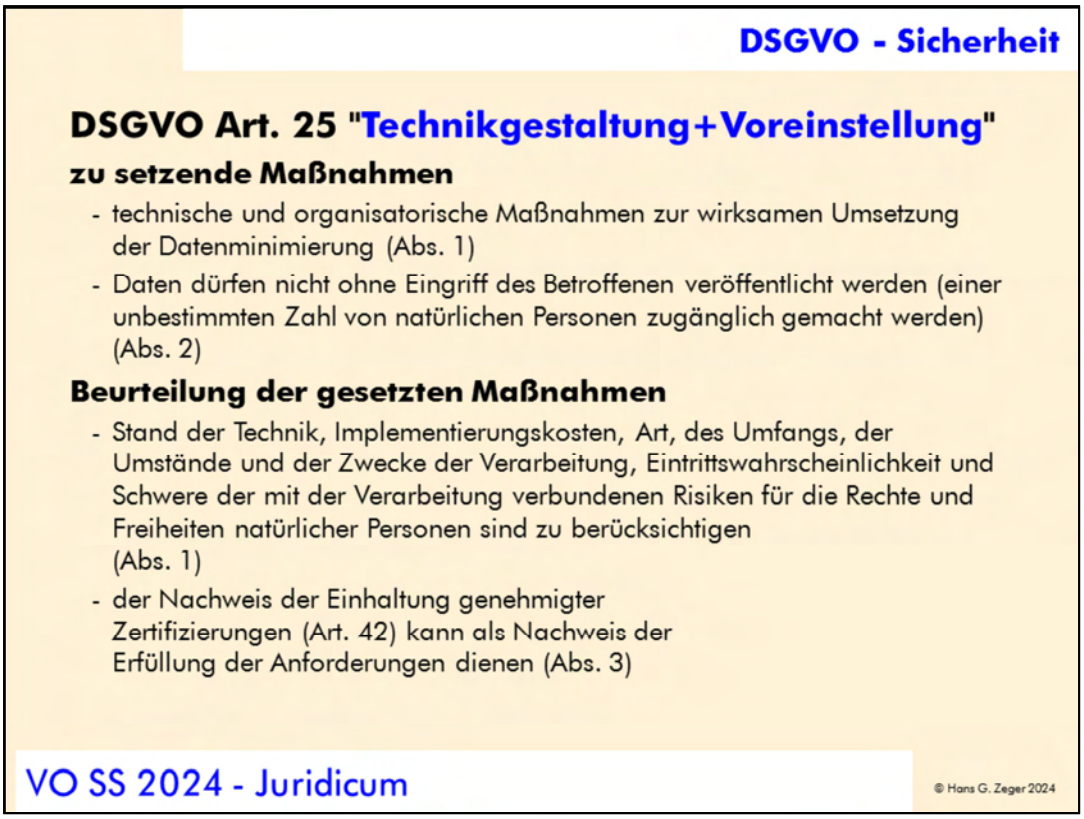
(2)Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang 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.



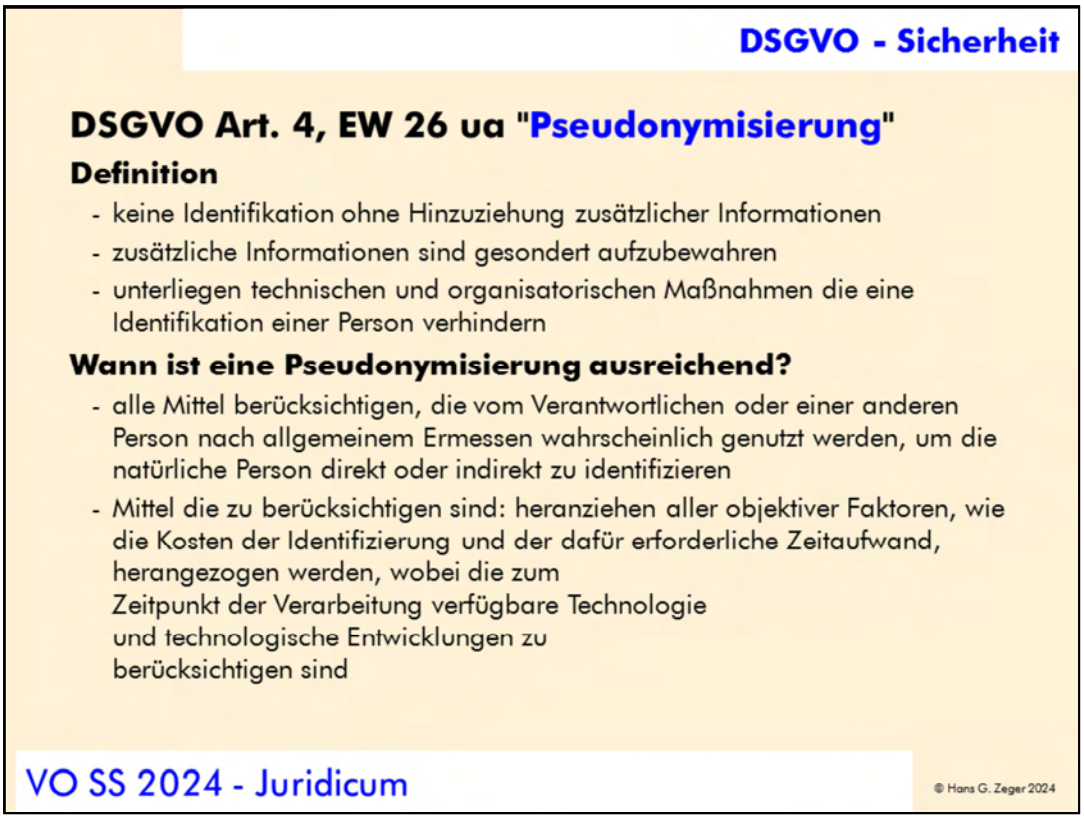
DSGVO Art. 32 Sicherheit der Verarbeitung (Fortsetzung)

(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.

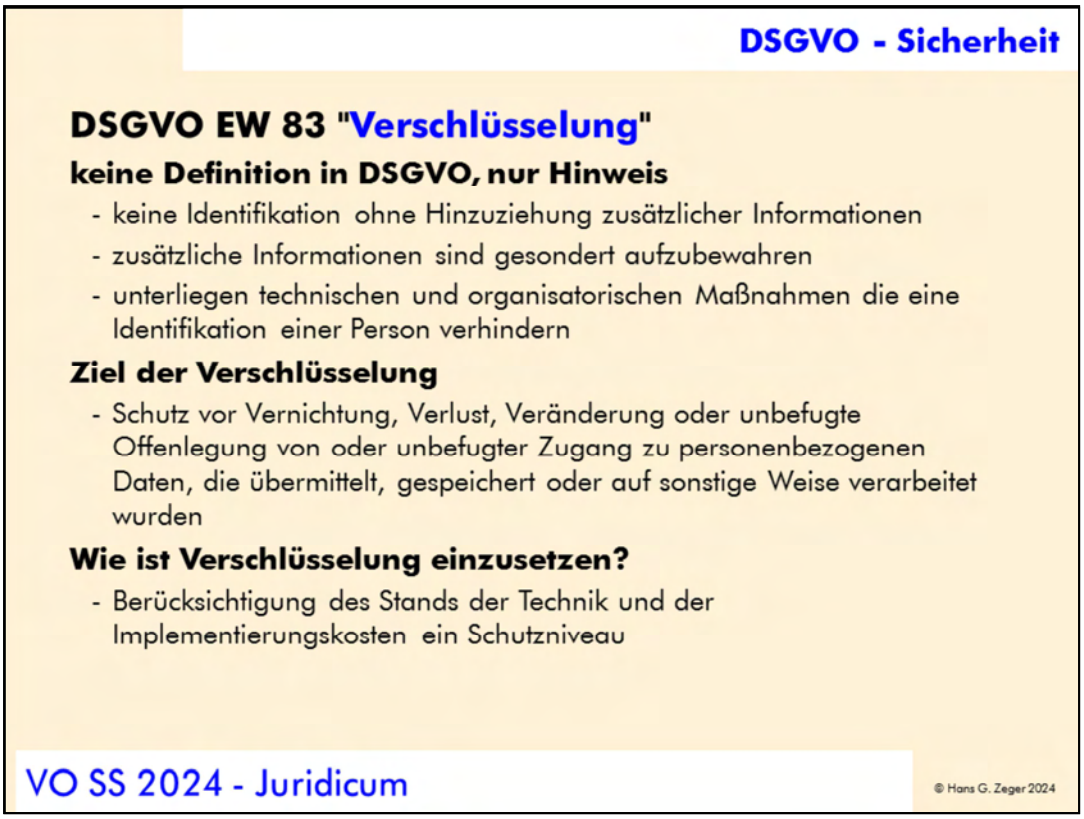


DSGVO Art. 4 Begriffsbestimmungen

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.



EW83

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.

Beachtung technischer Maßnahmen

laufende Beobachtung diverser Mailinglisten (CERT),

Publikationen der Art. 29 Datenschutzgruppe der EU,

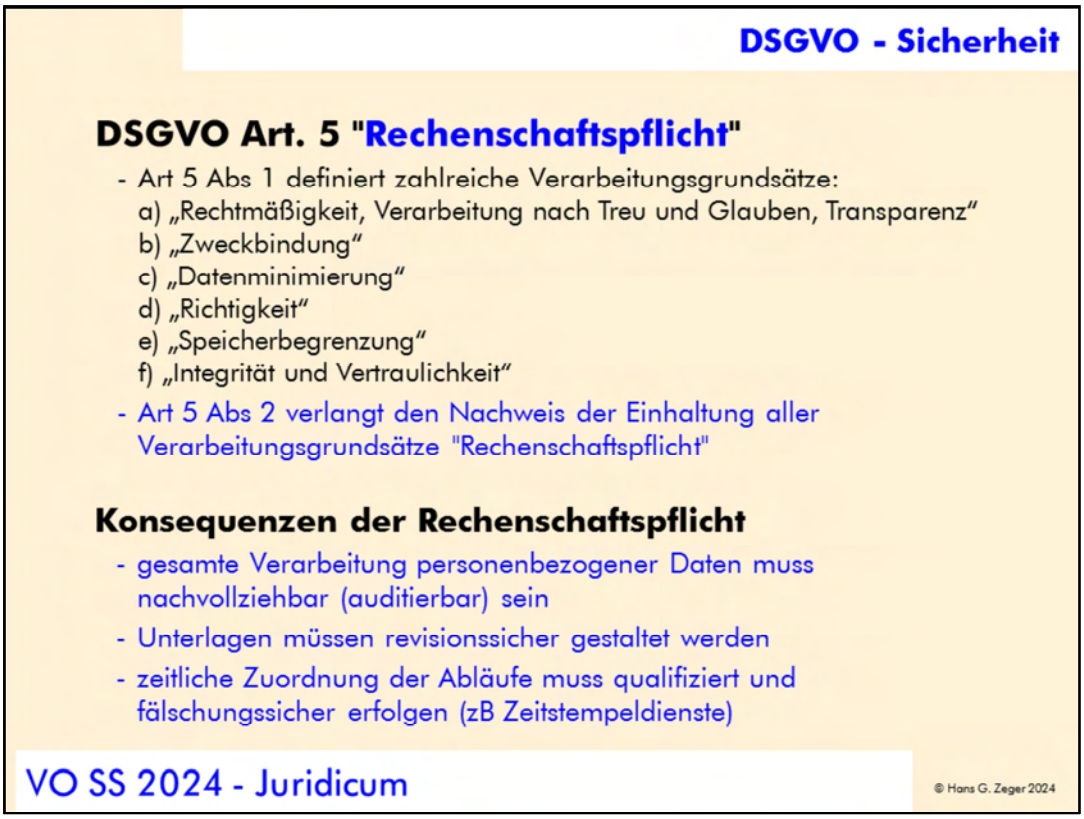
Anlehnung an bestehende Konzepte und Empfehlungen
BSI-Handbuch, IT-Sicherheitshandbücher, Datenschutzgütesiegel

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

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

Arbeitspapiere des European Data Protection Board (EDPB)

https://www.edpb.europa.eu/



Artikel 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"**);

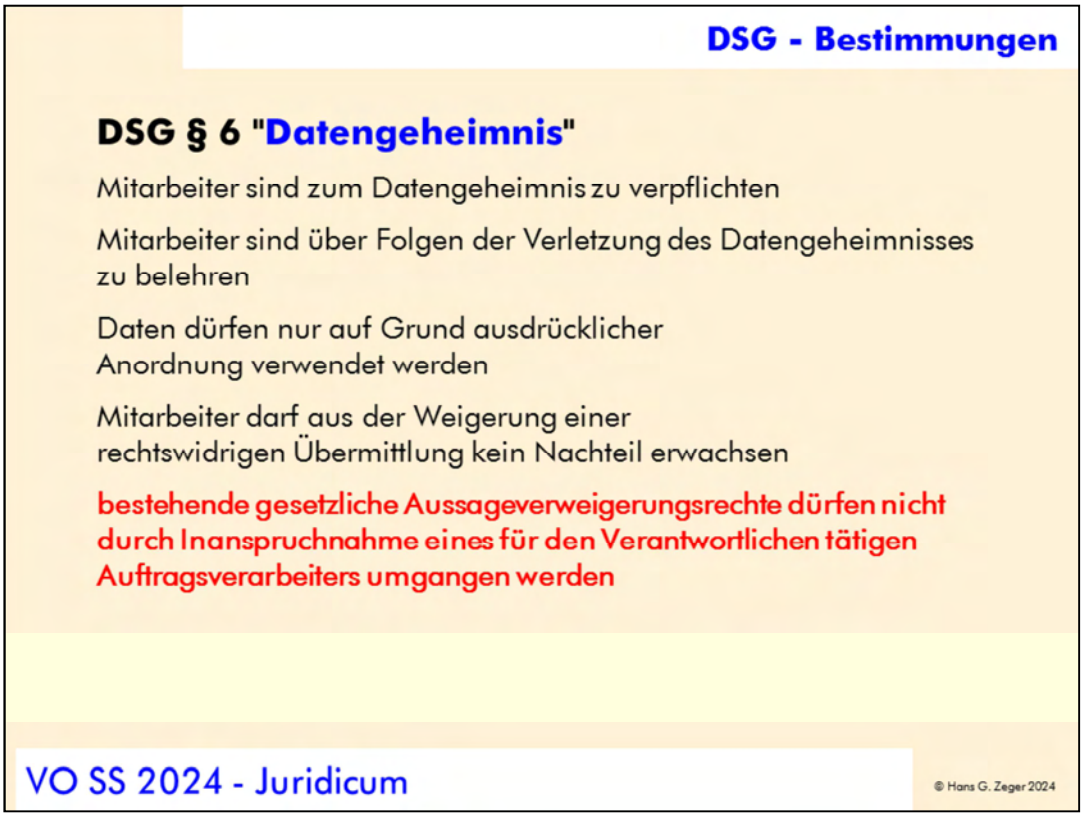
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**„Datenminimierung"**);

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"**).



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 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.

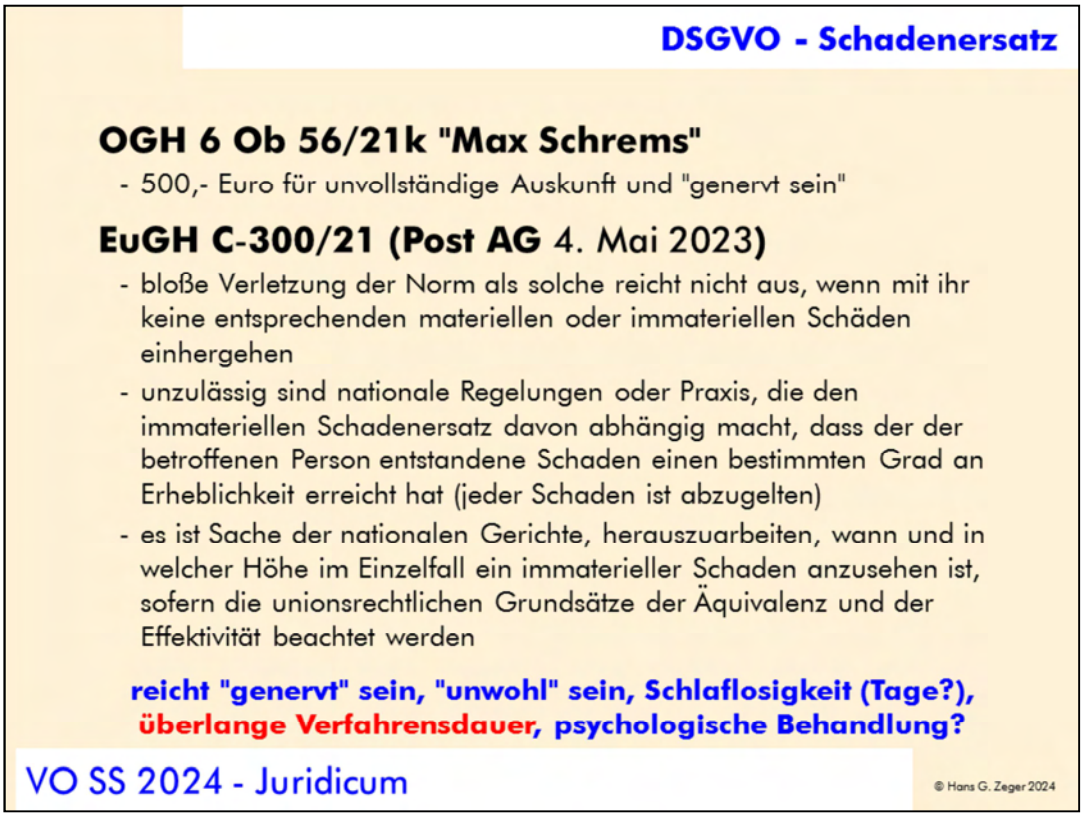
(6)Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

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.



Entscheidung EuGH C-300/21 UI gegen Österreichische Post AG

(Vorabentscheidungsersuchen des Obersten Gerichtshofs [Österreich])

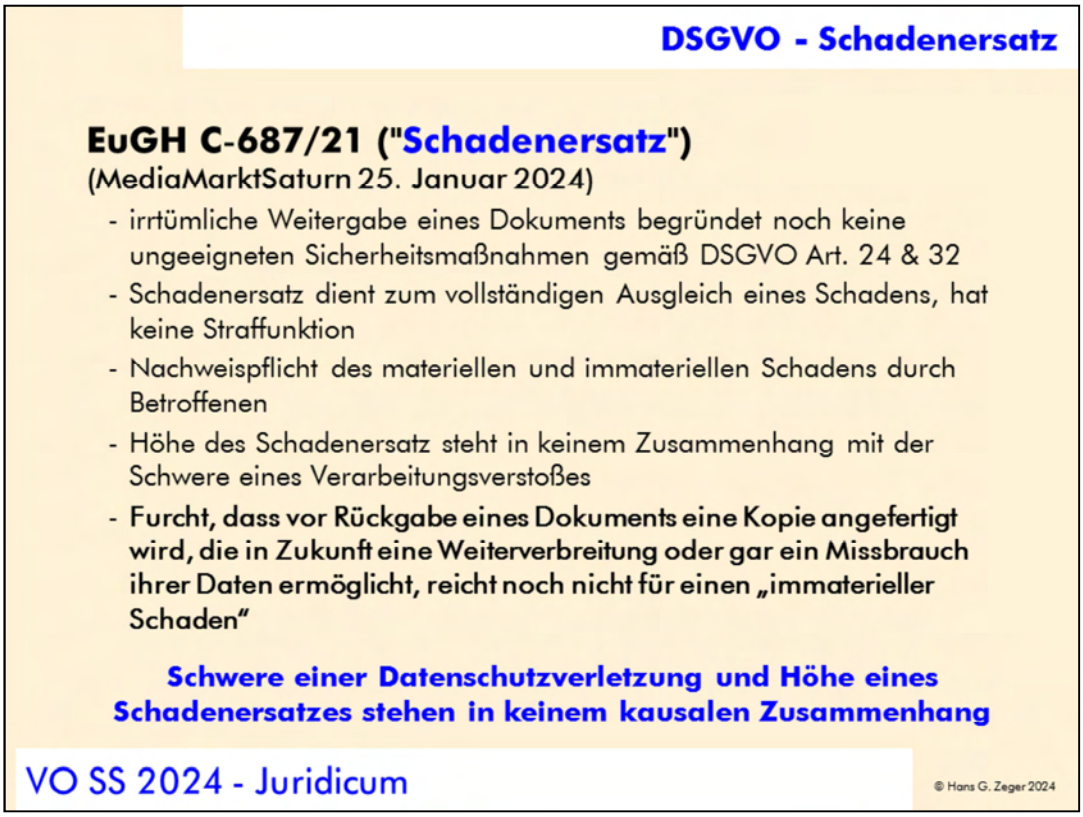
„Vorlage zur Vorabentscheidung – Schutz personenbezogener Daten – Verordnung (EU) 2016/679 – Immaterieller Schaden, der aus einer rechtswidrigen Verarbeitung von Daten resultiert – Erfordernisse des Schadensersatzanspruchs – Schäden, die einen gewissen Schweregrad überschreiten“

Ergebnis

1. Art. 82 Abs. 1 der 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)
ist dahin auszulegen,
dass der bloße Verstoß gegen die Bestimmungen dieser Verordnung nicht ausreicht, um einen Schadenersatzanspruch zu begründen.

2. Art. 82 Abs. 1 der Verordnung 2016/679
ist dahin auszulegen,
dass er einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat.

3. Art. 82 der Verordnung 2016/679
ist dahin auszulegen,
dass die nationalen Gerichte bei der Festsetzung der Höhe des Schadenersatzes, der aufgrund des in diesem Artikel verankerten Schadenersatzanspruchs geschuldet wird, die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden haben, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden.



Entscheidung EuGH C-687/21 (MediaMarktSaturn 25. Januar 2024)

1. Die Art. 5, 24, 32 und 82 der 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)
sind zusammen betrachtet dahin auszulegen, dass
im Rahmen einer auf Art. 82 gestützten Schadensersatzklage der Umstand, dass Mitarbeiter des für die Verarbeitung Verantwortlichen irrtümlich ein Dokument mit personenbezogenen Daten an einen unbefugten Dritten weitergegeben haben, für sich genommen nicht ausreicht, um davon auszugehen, dass die technischen und organisatorischen Maßnahmen, die der für die betreffende Verarbeitung Verantwortliche getroffen hat, nicht „geeignet" im Sinne der Art. 24 und 32 waren.

2. Art. 82 Abs. 1 der Verordnung 2016/679
ist dahin auszulegen, dass
der in dieser Bestimmung vorgesehene Schadensersatzanspruch, insbesondere im Fall eines immateriellen Schadens, eine Ausgleichsfunktion hat, da eine auf sie gestützte Entschädigung in Geld es ermöglichen soll, den konkret aufgrund des Verstoßes gegen die Verordnung 2016/679 erlittenen Schaden vollständig auszugleichen, und keine Straffunktion erfüllt.

3. Art. 82 der Verordnung 2016/679
ist dahin auszulegen, dass
er nicht verlangt, dass die Schwere des von dem für die Verarbeitung Verantwortlichen begangenen Verstoßes für die Zwecke des Ersatzes eines Schadens auf der Grundlage dieser Bestimmung berücksichtigt wird.

4. Art. 82 Abs. 1 der Verordnung 2016/679
ist dahin auszulegen, dass
die Person, die aufgrund dieser Bestimmung Schadensersatz verlangt, nicht nur den Verstoß gegen Bestimmungen der Verordnung 2016/679 nachweisen muss, sondern auch, dass ihr dadurch ein materieller oder immaterieller Schaden entstanden ist.

5. Art. 82 Abs. 1 der Verordnung 2016/679
ist dahin auszulegen, dass
in einem Fall, in dem ein Dokument, das personenbezogene Daten enthält, an einen unbefugten Dritten weitergegeben wurde, der diese Daten erwiesenermaßen nicht zur Kenntnis genommen hat, nicht schon deshalb ein „immaterieller Schaden" im Sinne dieser Bestimmung vorliegt, weil die betroffene Person befürchtet, dass im Anschluss an die Weitergabe, die es ermöglichte, vor der Rückgabe des Dokuments eine Kopie von ihm anzufertigen, in der Zukunft eine Weiterverbreitung oder gar ein Missbrauch ihrer Daten stattfindet.

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 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.

Verwaltungsstrafbestimmung

DSG § 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.

DSGVO / DSG - Strafbestimmungen

DSB-D213.747/0002-DSB/2019 (Post AG)

Sachverhalt

- Post AG generierte aus öffentlich zugänglichen Daten vermutete politische Präferenzen von Personen ("liberal", "konservativ", "grün", ...)

Entscheidung(en)

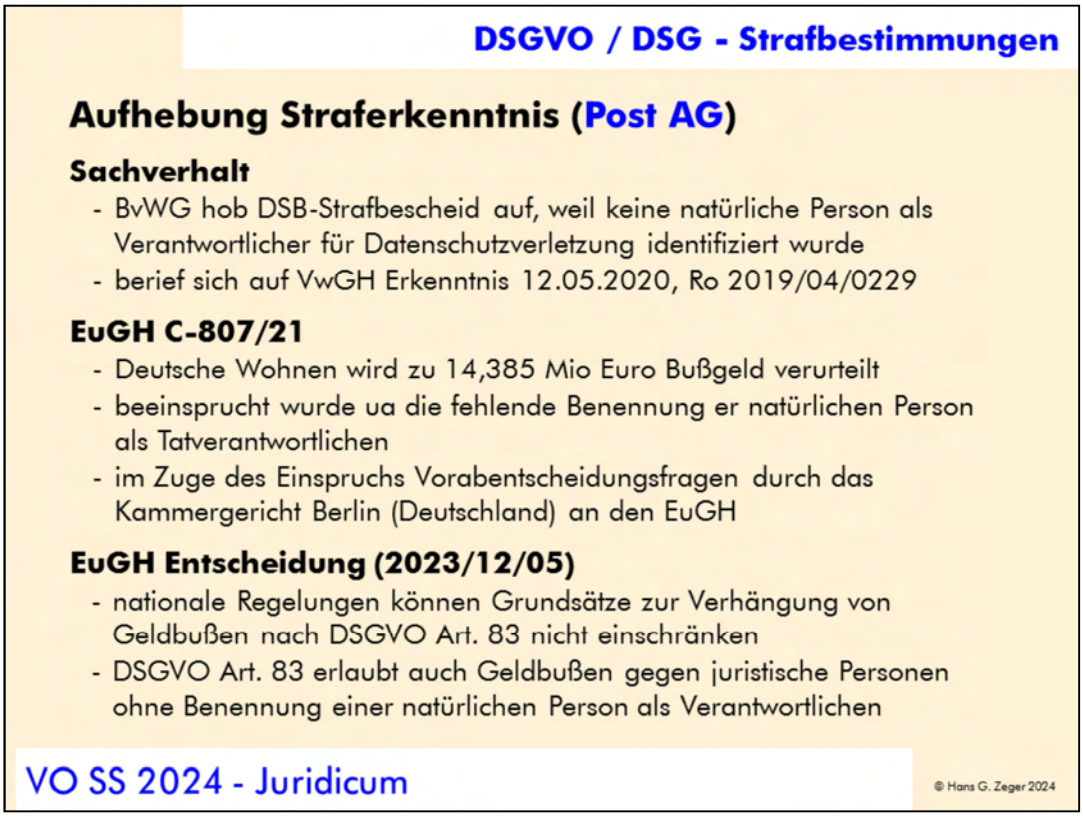
- unzulässige Datenverwendung
- besondere Datenkategorie, daher besonders strafwürdig
- DSB spricht 18 Mio Euro Strafe aus
- Einspruch bei BvWG: Bescheid 2020 zugunsten Post AG aufgehoben (W258 2227269-1/14E)
- neuer Entscheid DSB: 9,5 Mio Euro, Verfahren offen

vergleichbare Entscheidungen EU

- CNIL (FR) **SAN-2019-001**: ⇨ siehe Tracking
  Google 50 Mio Euro - intransparente DS-Bestimmungen
- Garante (IT) **9256486: Telekom-Unternehmen TIM S.p.A. 27 Mio Euro unerlaubte Werbeanrufe**

VO SS 2024 - Juridicum

-



Entscheidung EuGH C-807/21

...

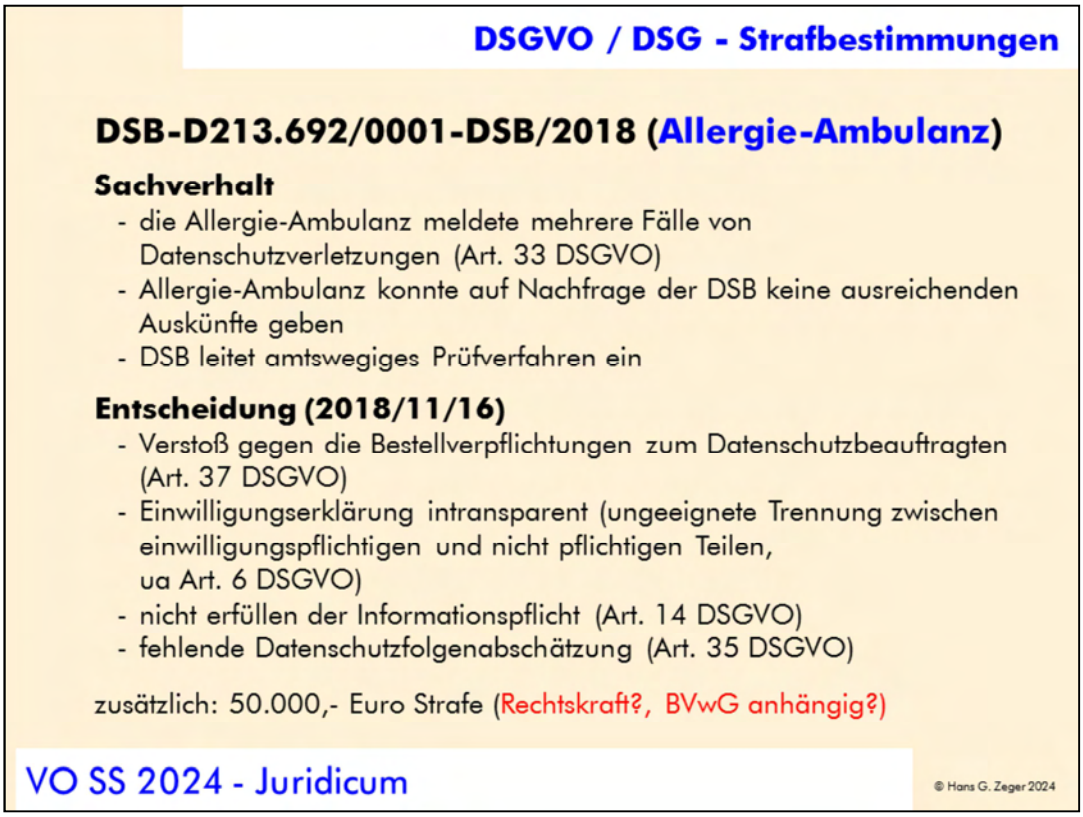
Aus diesen Gründen hat der Gerichtshof (Große Kammer) für Recht erkannt:

1. Art. 58 Abs. 2 Buchst. i und Art. 83 Abs. 1 bis 6 der 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) sind dahin auszulegen, dass

sie einer nationalen Regelung entgegenstehen, wonach eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoßes gegen eine juristische Person in ihrer Eigenschaft als Verantwortliche nur dann verhängt werden kann, wenn dieser Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde.

2. Art. 83 der Verordnung 2016/679 ist dahin auszulegen, dass

nach dieser Bestimmung eine Geldbuße nur dann verhängt werden darf, wenn nachgewiesen ist, dass der Verantwortliche, der eine juristische Person und zugleich ein Unternehmen ist, einen in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoß vorsätzlich oder fahrlässig begangen hat.


DSGVO / DSG - Strafbestimmungen
DSB-D213.692/0001-DSB/2018 (Allergie-Ambulanz)
Sachverhalt
- die Allergie-Ambulanz meldete mehrere Fälle von Datenschutzverletzungen (Art. 33 DSGVO)
- Allergie-Ambulanz konnte auf Nachfrage der DSB keine ausreichenden Auskünfte geben
- DSB leitet amtswegiges Prüfverfahren ein
Entscheidung (2018/11/16)
- Verstoß gegen die Bestellverpflichtungen zum Datenschutzbeauftragten (Art. 37 DSGVO)
- Einwilligungserklärung intransparent (ungeeignete Trennung zwischen einwilligungspflichtigen und nicht pflichtigen Teilen, ua Art. 6 DSGVO)
- nicht erfüllen der Informationspflicht (Art. 14 DSGVO)
- fehlende Datenschutzfolgenabschätzung (Art. 35 DSGVO)
zusätzlich: 50.000,- Euro Strafe (Rechtskraft?, BVwG anhängig?)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-

DSGVO / DSG - Strafbestimmungen

Strafpraxis AT (RIS-Veröffentlichungen)

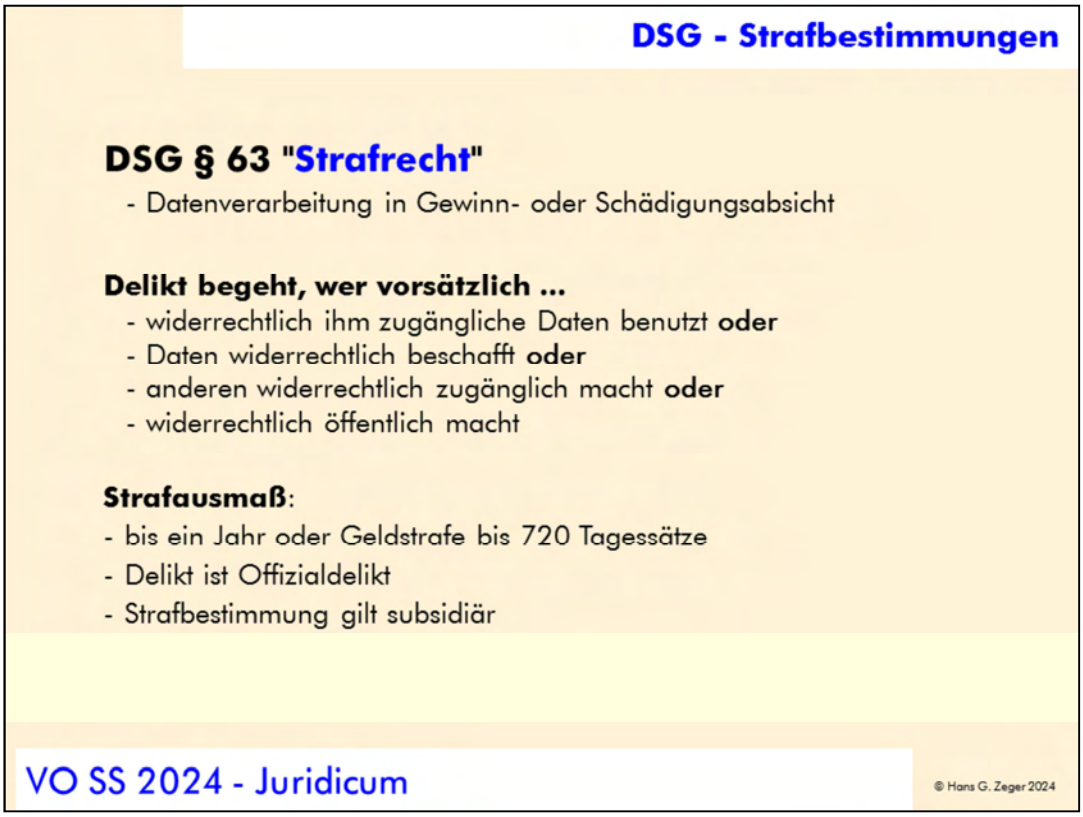
GZ	Jahr	Thema	Branche	Höhe (Euro)	Rechtskraft
2023-0.603.142	2023	Meldepflicht Datenschutzverletzung	Tourismusbetrieb	5.900,-	rk
2023-0.789.858	2023	Verletzung Auskunftspflicht	Bank	9.500,-	rk
2023-0.583.644	2023	Videoüberwachung Arbeitnehmer	Gaststätte	20.000,-	rk
2023-0.637.760	2023	Mangelnde Mitwirkung Verfahren	Wohnbaugesellschaft	10.000,-	rk
2023-0.420.407	2023	Veröffentlichung Gesundheitsdaten	Arzt	10.000,-	tw rk
2023-0.404.421	2023	politische Werbung mit Kundendaten	Politiker	1.000,-	rk
2022-0.585.764	2022	Videoüberwachung Toiletten	Privatperson	25.000,-	rk
2021-0.518.795	2021	Weitergabe Gerichtsdaten	Privatperson	600,-	rk
2020-0.582.166	2021	Mangelnde Mitwirkung Verfahren	Unternehmen	3.000,-	rk
2020-0.111.488	2020	Veröffentlichung Gesundheitsdaten	Arzt	600,-	rk
2020-0.550.322	2020	Videoüberwachung Toiletten w	Privatperson	150,-	rk
DSB-D550.185	2019	Videoüberwachung Umkleidekabine w	Fußballklub	10.000,-	rk
DSB-D550.037	2018	Videoüberwachung Wohnhausanlage	Privatperson	2.200,-	rk
DSB-D550.015	2018	Videoüberwachung Verkehr	Verein	Ermahnung	rk
DSB-D550.084	2018	Videoüberwachung Dashcam	Privatperson	300,-	rk

VO SS 2024 - Juridicum

-

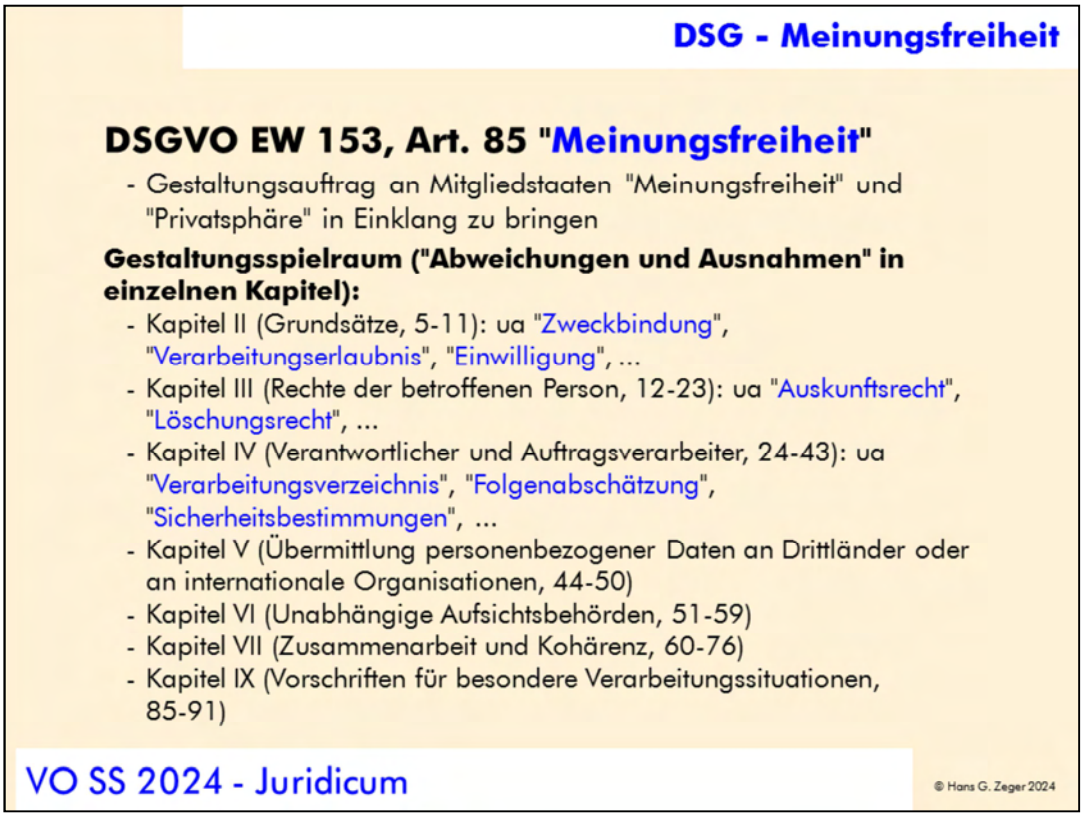

DSGVO / DSG - Strafbestimmungen
Strafbestimmungen im europäischen Vergleich
große Unterschiede in der Publikation von Entscheidungen
- sehr restriktive Auslegung der Publikationspflicht: LU, IR
- weitreichende Publikationen zu Verfahren: FR, NO, ES
- Mittelfeld: AT, DE
große Unterschiede in Strafen und Strafhöhen
- sehr restriktiv: IR
- tendenziell hohe Strafen: FR, NO, LU
- geringe Strafen: AT
viele Strafen nur bekannt, weil Unternehmen auf Grund der großen Höhe Rückstellungen in den veröffentlichten Bilanzen ausweisen (Amazon/LU/746 Mio Euro, Post/AT/18 Mio Euro)
große Unterschiede zwischen publizierten und tatsächlich verhängten Strafen
generell werden Strafen erst nach langjährigen Rechtsverfahren verhängt
DSGVO-Strafen mögen emotional befriedigen, werden das Phänomen des immer stärkeren Ungleichgewichts in der Informationsgesellschaft zwischen USA und Europa nicht lösen
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



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.

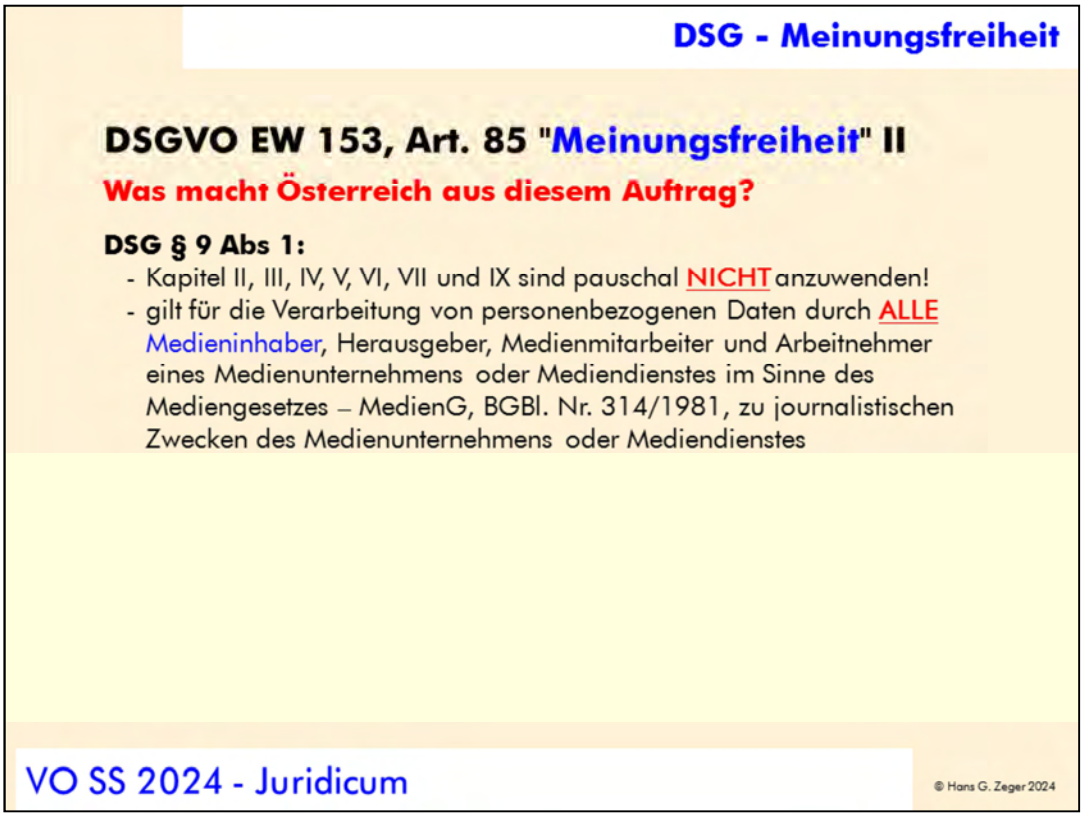


DSGVO Art 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

(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.



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.

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;

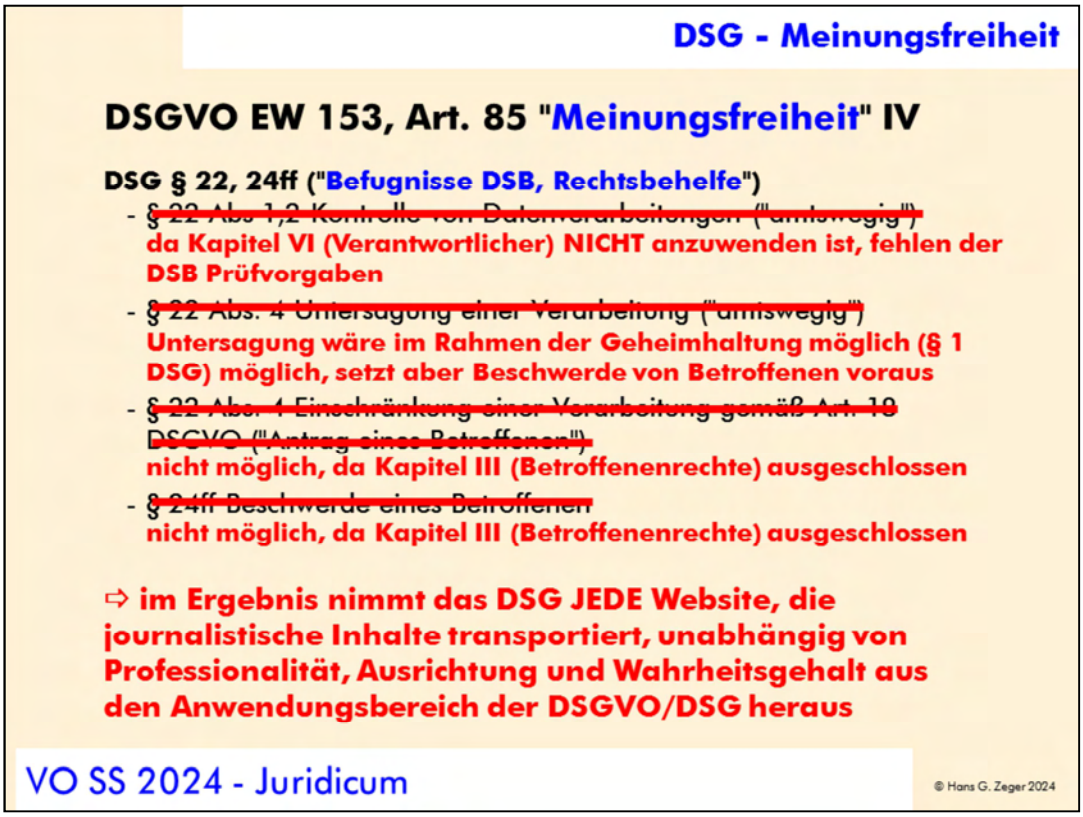
9. „Herausgeber“: wer die grundlegende Richtung des periodischen Mediums bestimmt;

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.

DSB-D123.768/0004-DSB/2019

...
3. Zum Vorliegen einer gesetzlichen Grundlage

Darüber hinaus ist festzuhalten, dass angesichts der Definition einer politischen Partei in (der Verfassungsbestimmung des) § 1 Abs. 2 PartG deutlich wird, dass der Zweck von politischen Parteien vom Gesetzgeber primär in der kontinuierlichen „umfassenden Beeinflussung der staatlichen Willensbildung“ gesehen wird.

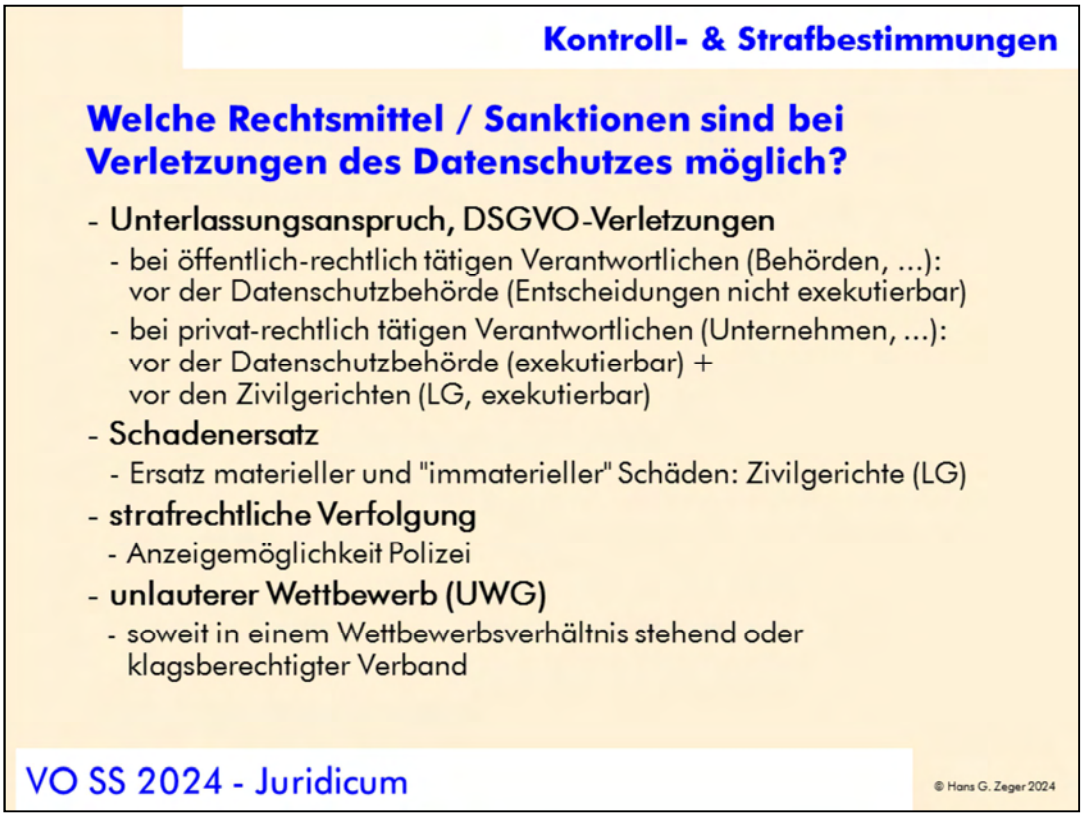
Nach der Rechtsprechung des Verfassungsgerichtshofes sind das Vorhandensein politischer Parteien und die Möglichkeit der Änderung der Mehrheitsverhältnisse Auswirkungen des dem B-VG zugrundeliegenden demokratischen Prinzips. Zu den wesentlichen Zielen politischer Parteien gehört die Verwirklichung ihrer politischen Vorstellungen im Wege der Ausübung staatlicher Funktionen durch ihre Beauftragten und Vertrauensträger in den verschiedenen Gremien der Gesetzgebung und staatlichen Verwaltung, ganz besonders in den allgemeinen Vertretungskörpern (siehe dazu VfSlg. 14.803/1997 und VfSlg. 20.128/2016 mwN).

Hiervon umfasst wird auch die Einflussnahme auf die Gestaltung der öffentlichen Meinung zu politischen Mitbewerbern sein. Die verfahrensgegenständliche Verwendung der Daten des Beschwerdeführers durch die Beschwerdegegnerin ist somit auch durch das PartG gedeckt.

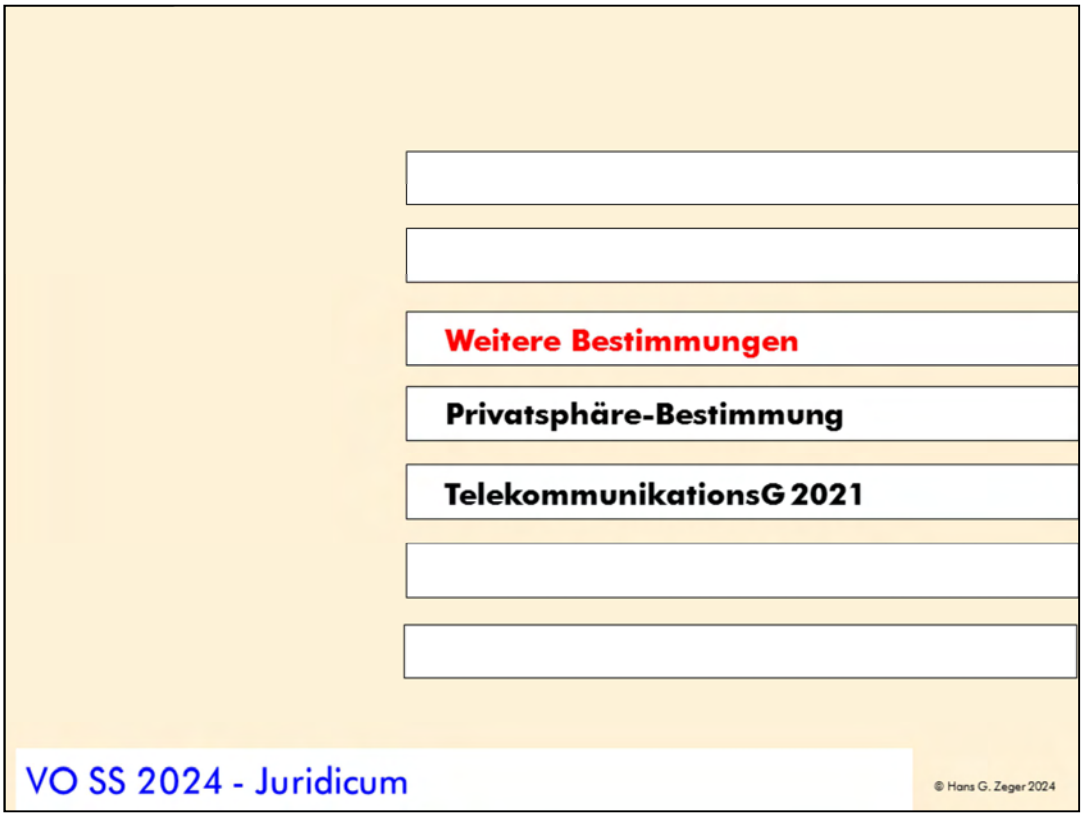
DSB-D124.1342 2020-0.303.727

...
3. Ergebnis

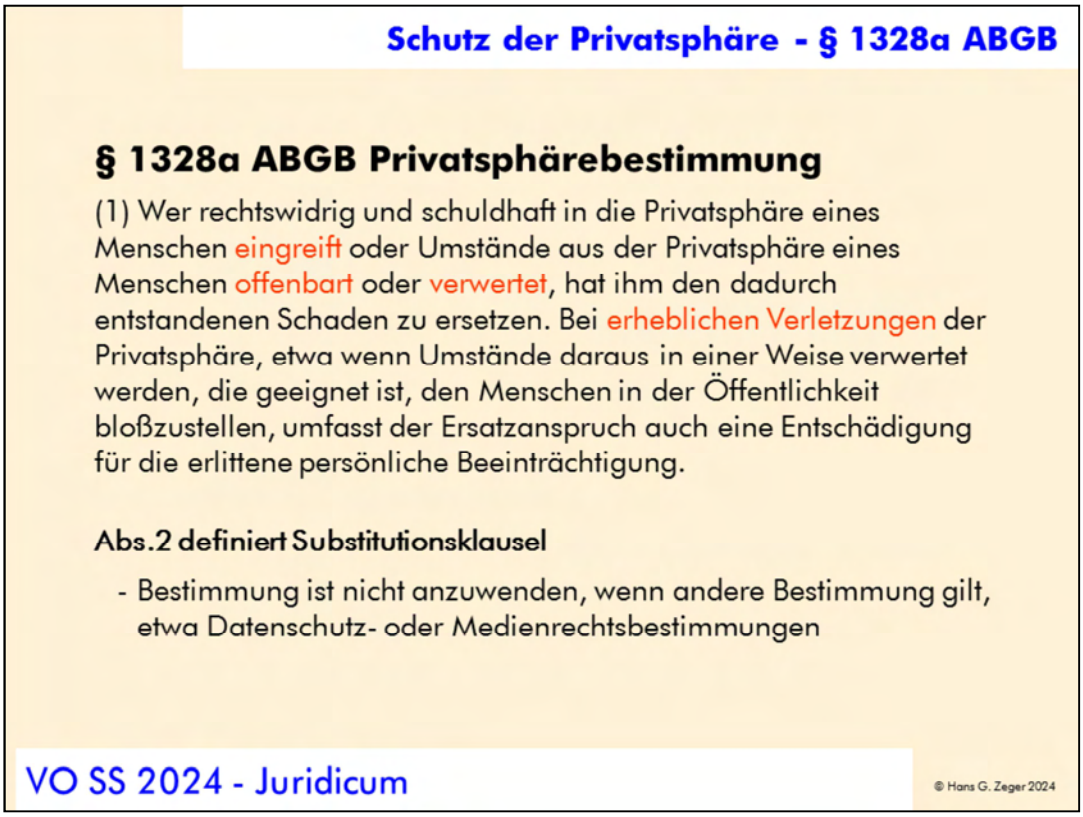
Im Ergebnis ist festzuhalten, dass es sich beim Beschwerdegegner
i) jedenfalls im Rahmen des Betriebs des Newsbereichs unter https://verein-n***.at/presse/news/ um ein Medienunternehmen gemäß § 1 Abs. 1 Z 6 MedienG handelt und dass
ii) die gegenständlich relevante Veröffentlichung der personenbezogenen Daten der Beschwerdeführerin im Newsbereich unter https://verein-n***.at/presse/news/201*/berichteneu*3*1*8*.php zu journalistischen Zwecken erfolgte.
Die Voraussetzungen des § 9 Abs. 1 DSG sind daher erfüllt.
Wie oben ausgeführt ist die Datenschutzbehörde im Anwendungsbereich des § 9 Abs. 1 DSG für die Behandlung von Beschwerden unzuständig.
Die Beschwerde war daher spruchgemäß zurückzuweisen.


Kontroll- & Strafbestimmungen
Welche Rechtsmittel / Sanktionen sind bei Verletzungen des Datenschutzes möglich?
- Unterlassungsanspruch, DSGVO-Verletzungen
- bei öffentlich-rechtlich tätigen Verantwortlichen (Behörden, ...): vor der Datenschutzbehörde (Entscheidungen nicht exekutierbar)
- bei privat-rechtlich tätigen Verantwortlichen (Unternehmen, ...): vor der Datenschutzbehörde (exekutierbar) + vor den Zivilgerichten (LG, exekutierbar)
- Schadenersatz
- Ersatz materieller und "immaterieller" Schäden: Zivilgerichte (LG)
- strafrechtliche Verfolgung
- Anzeigemöglichkeit Polizei
- unlauterer Wettbewerb (UWG)
- soweit in einem Wettbewerbsverhältnis stehend oder klagsberechtigter Verband
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-

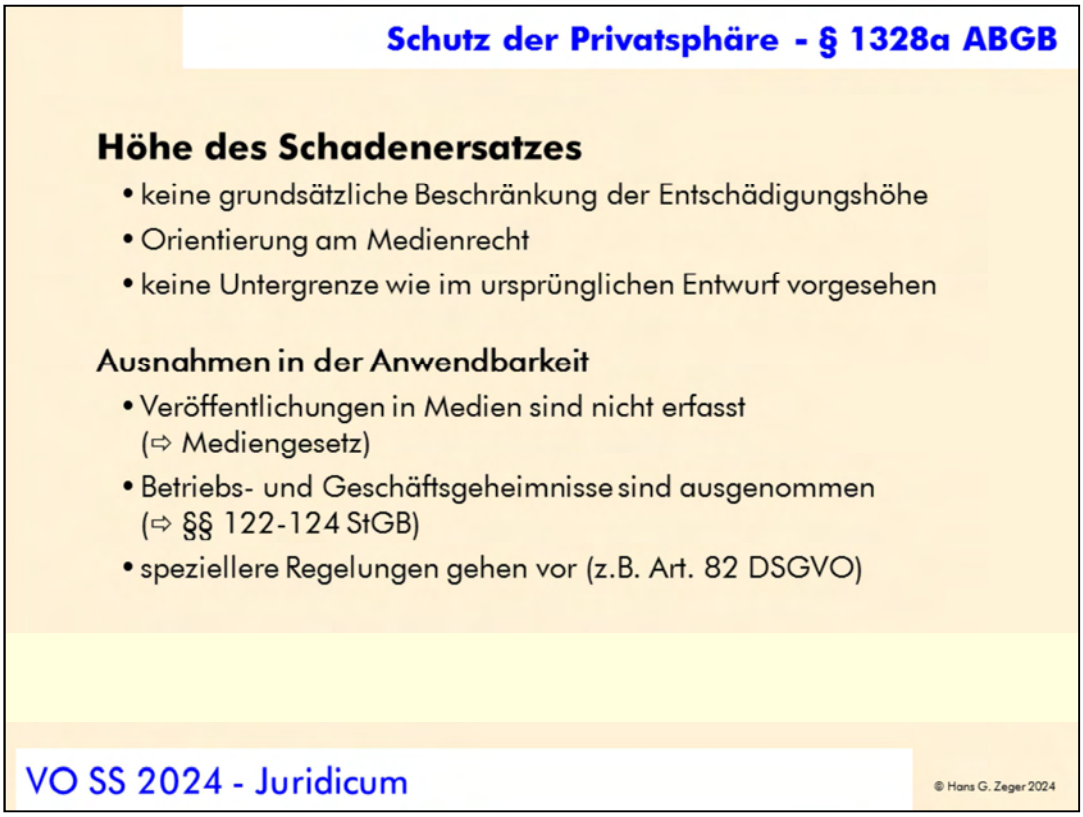

Weitere Bestimmungen
Privatsphäre-Bestimmung
TelekommunikationsG 2021
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



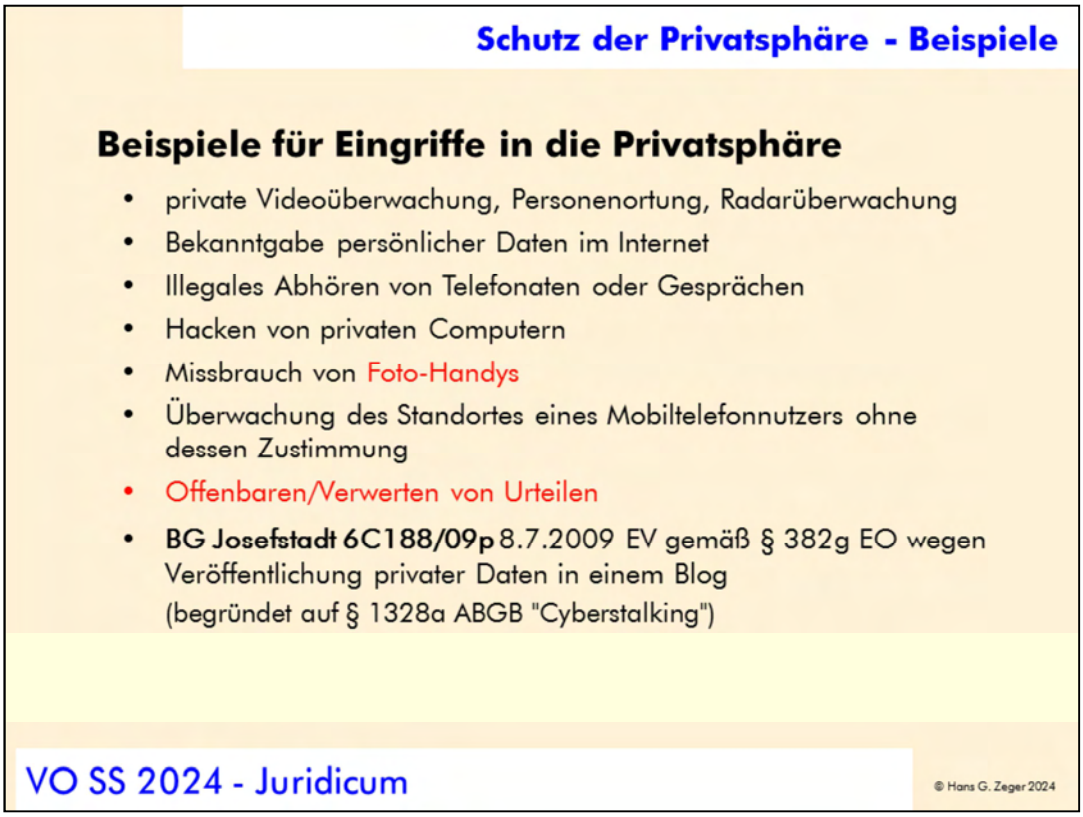
§ 1328a Abs. 2 ABGB:

"(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."



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.



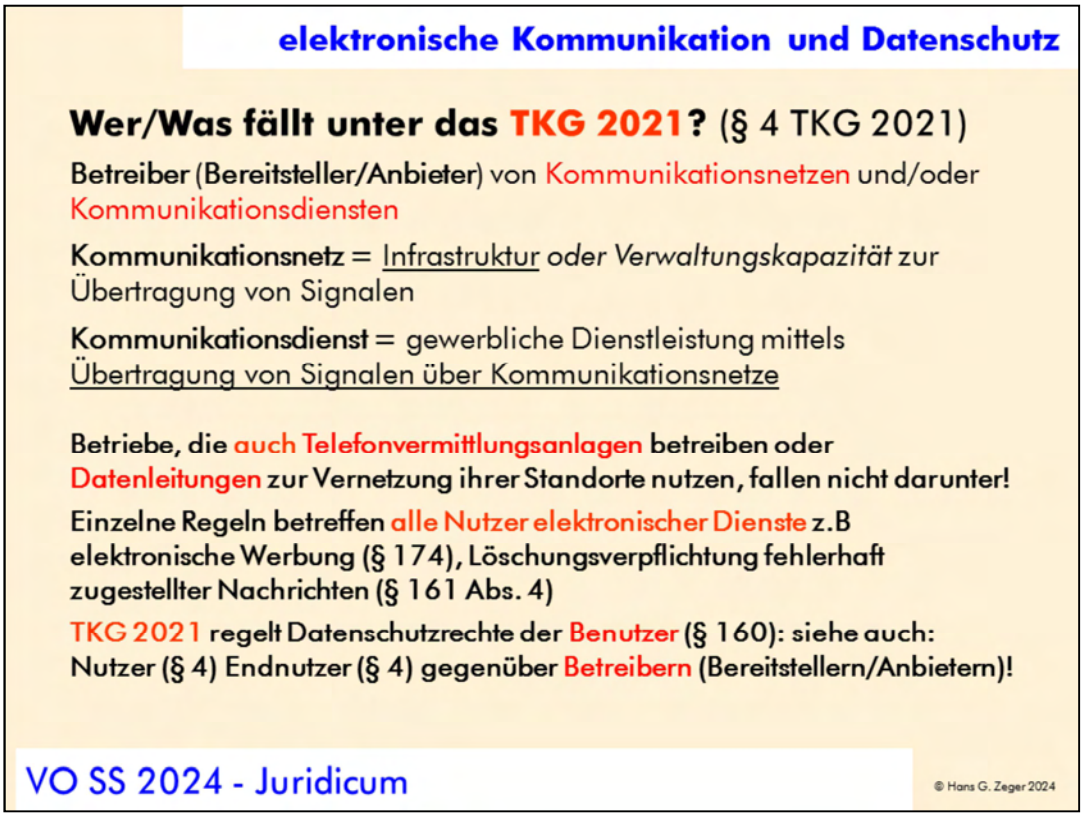
Die oben genannten Beispiele sind teilweise auch in den erläuternden Bemerkungen zum Entwurf angeführt.

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, seither zahlreiche Änderungen
- 2018/1972/EU (berichtigt ABl. Nr. L 334 27.12.2019
- in AT durch TKG 2021 (BGBl. I 190/2021) umgesetzt
- wir beschränken uns auf 2002/58/EG ("ePrivacy"-Richtlinie, Kommunikations-Datenschutz-RL) bzw. 14. Abschnitt des TKG 2021
Ziel ist die Regelung spezifischer Kommunikations-Datenschutzanforderungen und -situationen
ergänzend:
Fernmeldegeheimnis (Art. 10a StGG)
seit 1.1.1975 als Gegenstück zum Briefgeheimnis (Art. 10 StGG)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



TKG 2021 § 4 ausgewählte Begriffe

4. „**Kommunikationsdienste**" unabhängig vom Sitz des Anbieters im räumlichen Geltungsbereich dieses Bundesgesetzes gewöhnlich gegen Entgelt über Kommunikationsnetze erbrachte elektronische Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen, es sei denn, es handelt sich um eine geringfügige Nebendienstleistung:

a) „Internetzugangsdienste" im Sinne der Begriffsbestimmung des Artikels 2 Abs. 2 Nummer 2 der Verordnung (EU) 2015/2120,

b) interpersonelle Kommunikationsdienste und

c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden;

13. „**Nutzer**" eine natürliche oder juristische Person, die einen öffentlich zugänglichen Kommunikationsdienst vertraglich in Anspruch nimmt oder beantragt;

14. „**Endnutzer**" ein Nutzer, der keine öffentlichen Kommunikationsnetze oder öffentlich zugänglichen Kommunikationsdienste bereitstellt;

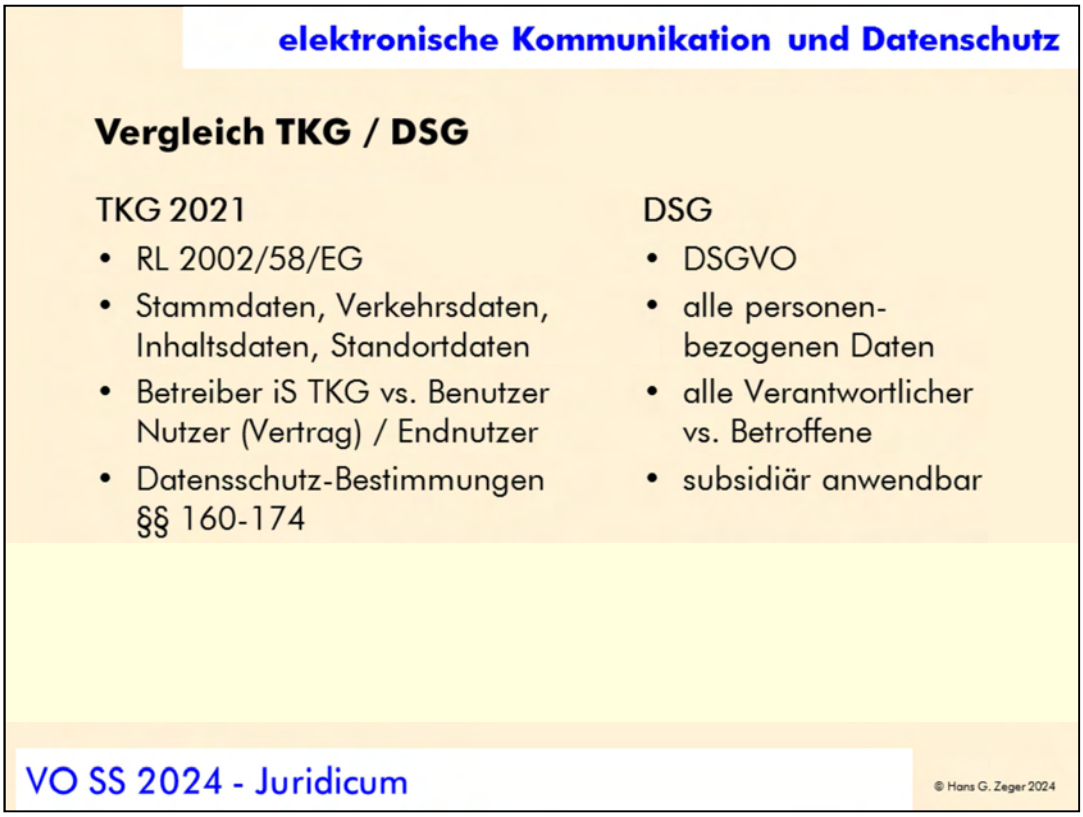
15. „Verbraucher" jede natürliche Person, die einen öffentlich zugänglichen Kommunikationsdienst zu anderen als gewerblichen, geschäftlichen, handwerklichen oder beruflichen Zwecken nutzt oder beantragt (Verbraucher gemäß § 1 des Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz – KSchG), BGBl. Nr. 140/1979);

16. „**Bereitsteller**" jeder, der ein Kommunikationsnetz errichtet, betreibt, kontrolliert oder zur Verfügung stellt;

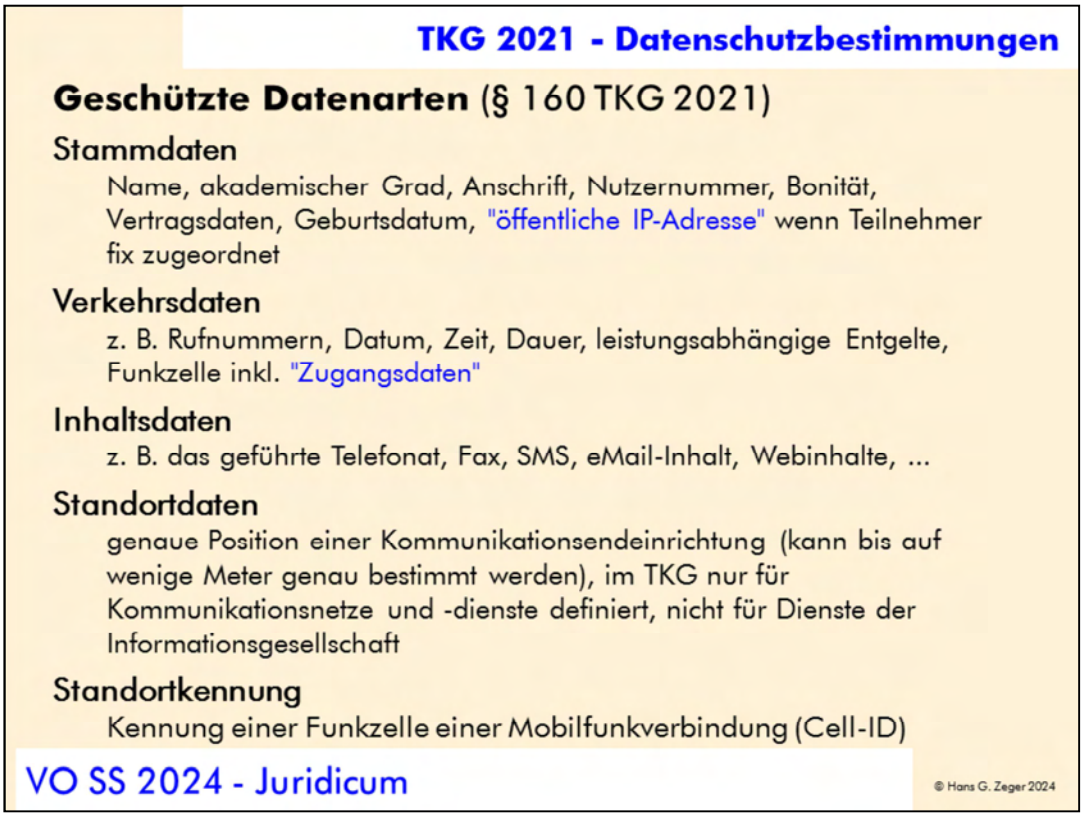
TKG 2021 § 160 Abs 3 Definitionen zum Abschnitt "Kommunikationsgeheimnis, Datenschutz" (§§ 160-174)

1. "**Anbieter**" Betreiber von öffentlichen Kommunikationsdiensten;

2. "**Benutzer**" eine 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 2021
• RL 2002/58/EG
• Stammdaten, Verkehrsdaten, Inhaltsdaten, Standortdaten
• Betreiber iS TKG vs. Benutzer Nutzer (Vertrag) / Endnutzer
• Datensschutz-Bestimmungen §§ 160-174
DSG
• DSGVO
• alle personen-bezogenen Daten
• alle Verantwortlicher vs. Betroffene
• subsidiär anwendbar
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



TKG 2021 § 160 Abs 2 ...

5. „**Stammdaten**"alle Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Nutzerverzeichnissen erforderlich sind; dies sind:

a) Name (Familienname und Vorname bei natürlichen Personen, Name oder Bezeichnung bei juristischen Personen),

b) akademischer Grad bei natürlichen Personen,

c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz oder Rechnungsadresse bei juristischen Personen),

d) Nutzernummer und sonstige Kontaktinformation für die Nachricht,

e) Information über Art und Inhalt des Vertragsverhältnisses,

f) Bonität;

g) Geburtsdatum

6. „**Verkehrsdaten**"Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

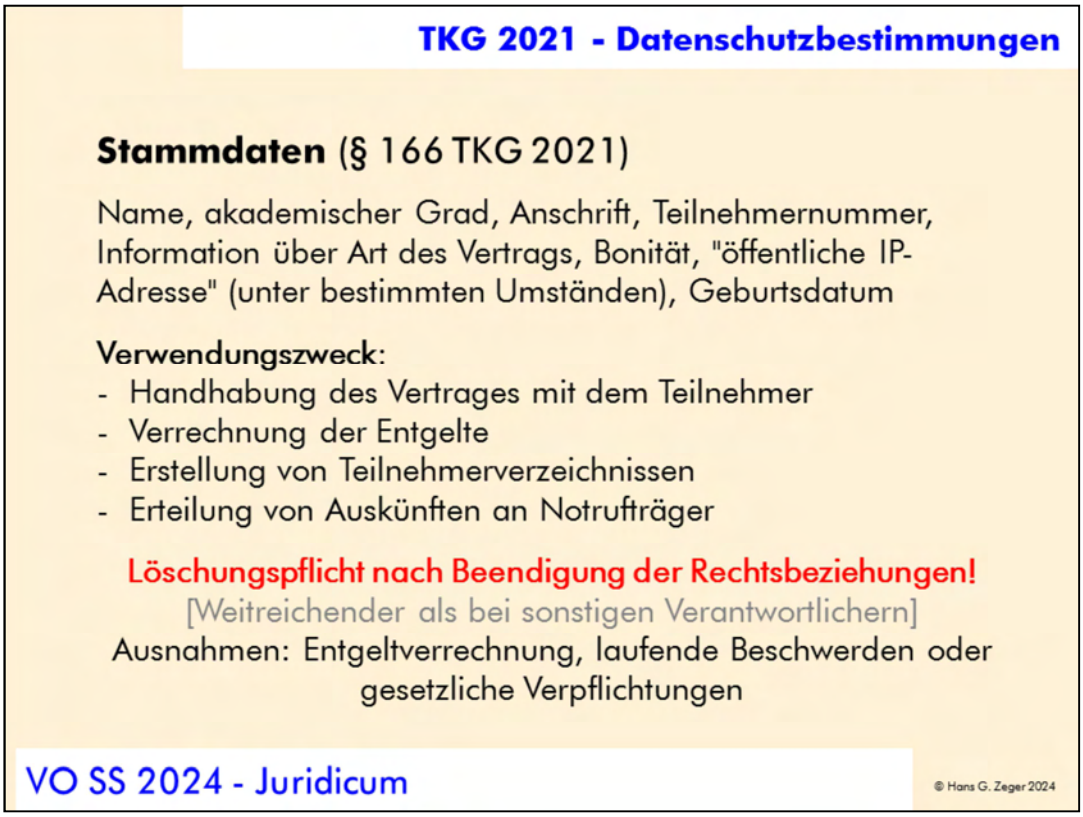
7. „**Zugangsdaten**"jene Verkehrsdaten, die beim Zugang eines Nutzers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Nutzer notwendig sind;

8. „**Inhaltsdaten**" die Inhalte übertragener Nachrichten (Z 11);

9. „**Standortdaten**"Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Endeinrichtung eines Benutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Endeinrichtungen sind Standortdaten die Adresse der Einrichtung;

10. „**Standortkennung**" die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-ID); ...

15.„**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 § 160 Abs. 3 Z 7. Wenn eine konkrete öffentliche IP-Adresse einem Nutzer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 160 Abs. 3 Z 5;



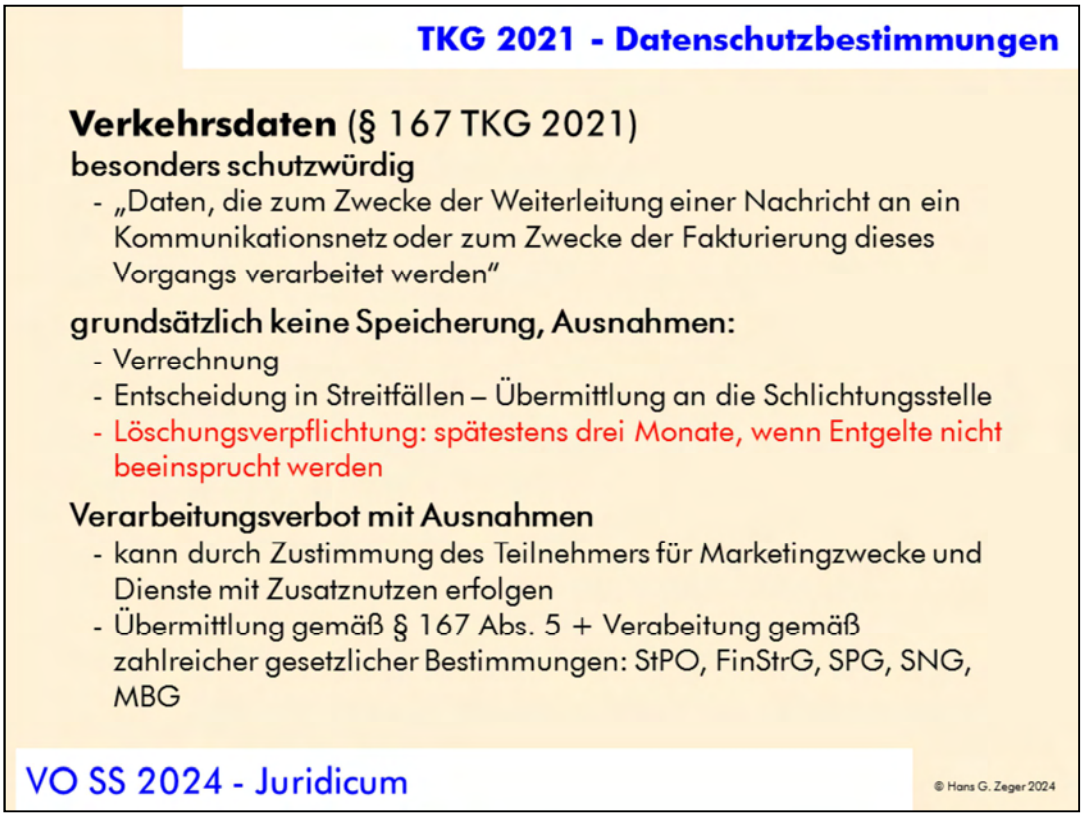
TKG 2021 § 166

(1) Stammdaten dürfen unbeschadet der § 165 Abs. 1 und 2 sowie § 181 Abs. 8 und 9 von Anbietern nur für folgende Zwecke verarbeitet werden:

1. Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Nutzer;
2. Verrechnung der Entgelte;
3. Erstellung von Nutzerverzeichnissen, gemäß § 126 und
4. Erteilung von Auskünften an Betreiber von Notdiensten, gemäß § 124.

(2) Vor Durchführung des Vertrages sowie vor der erstmaligen Wiederaufladung nach dem 1. September 2019 ist durch oder für den Anbieter die Identität des Nutzers zu erheben und sind die zur Identifizierung des Nutzers erforderlichen Stammdaten (§ 160 Abs. 3 Z 5 lit. a, b und g) anhand geeigneter Identifizierungsverfahren zu registrieren. Die Festlegung geeigneter Identifizierungsverfahren erfolgt durch Verordnung der Bundesministerin für Landwirtschaft, Regionen und Tourismus im Einvernehmen mit dem Bundesminister für Inneres. Die Abgeltung unbedingt erforderlicher Investitionen erfolgt nach den Regeln des § 162 Abs. 1.

(3) Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Nutzer 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 2021 § 167

(1) Verkehrsdaten dürfen außer in den in diesem Gesetz ausdrücklich 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, des SNG sowie des MBG. ...

(3) Die Verarbeitung mit Ausnahme der Übermittlung von Verkehrsdaten darf nur durch solche Personen erfolgen, die für die Entgeltverrechnung oder Verkehrsabwicklung, Behebung von Störungen, Kundenanfragen, Betrugsermittlung oder Vermarktung der Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen zuständig sind oder die von diesen Personen beauftragt wurden. Der Umfang der verarbeiteten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(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 Nutzernummer auszuwerten. Mit Zustimmung des Nutzers 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

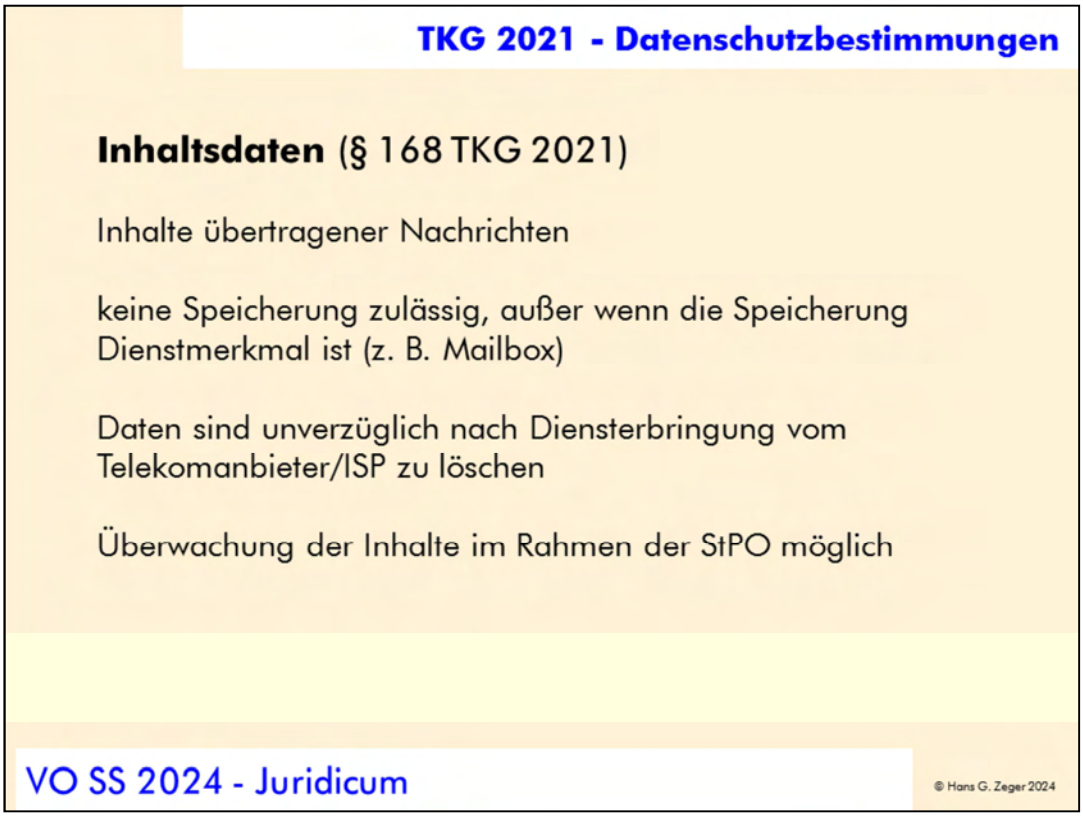
1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;

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, § 11 Abs. 1 Z 5 SNG sowie § 22 Abs. 2b MBG. 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, des § 11 Abs. 1 Z 5 SNG, des § 99 Abs. 3a FinStrG sowie des § 22 Abs. 2b MBG;

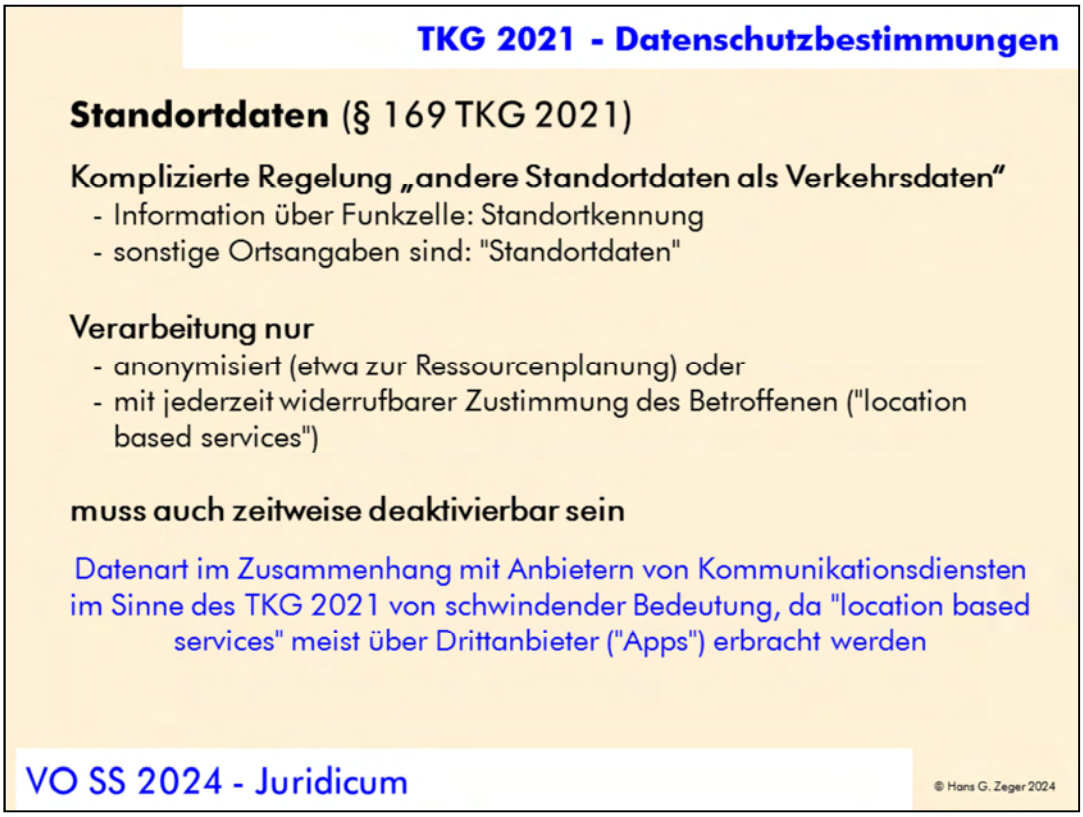
5. Verkehrsdaten, Zugangsdaten und Standortdaten nach Maßgabe des § 11 Abs. 1 Z 7 SNG sowie des § 22 Abs. 2b MBG.Abs. 2b MBG.



TKG 2021 § 168

(1) Inhaltsdaten dürfen außer in den in diesem Gesetz geregelten Fällen und 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 2021 § 169

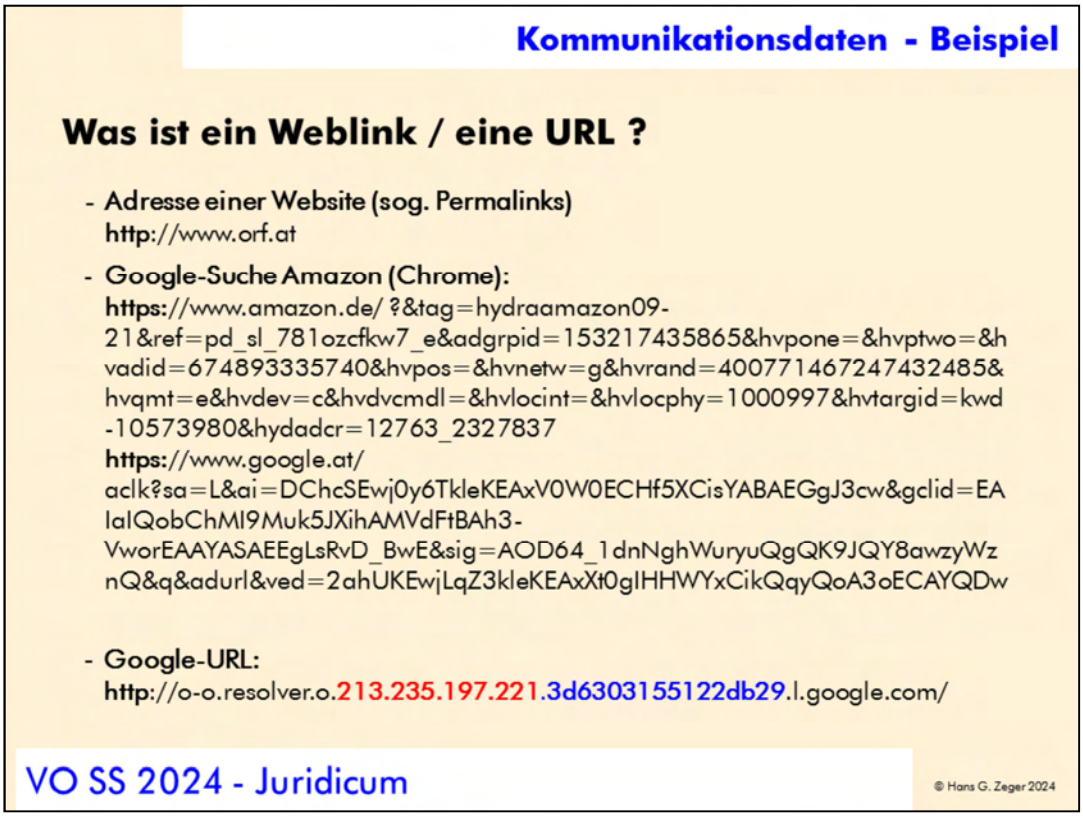
(1) Andere Standortdaten als Verkehrsdaten dürfen unbeschadet des § 124 nur verarbeitet werden, wenn sie

1. anonymisiert werden oder

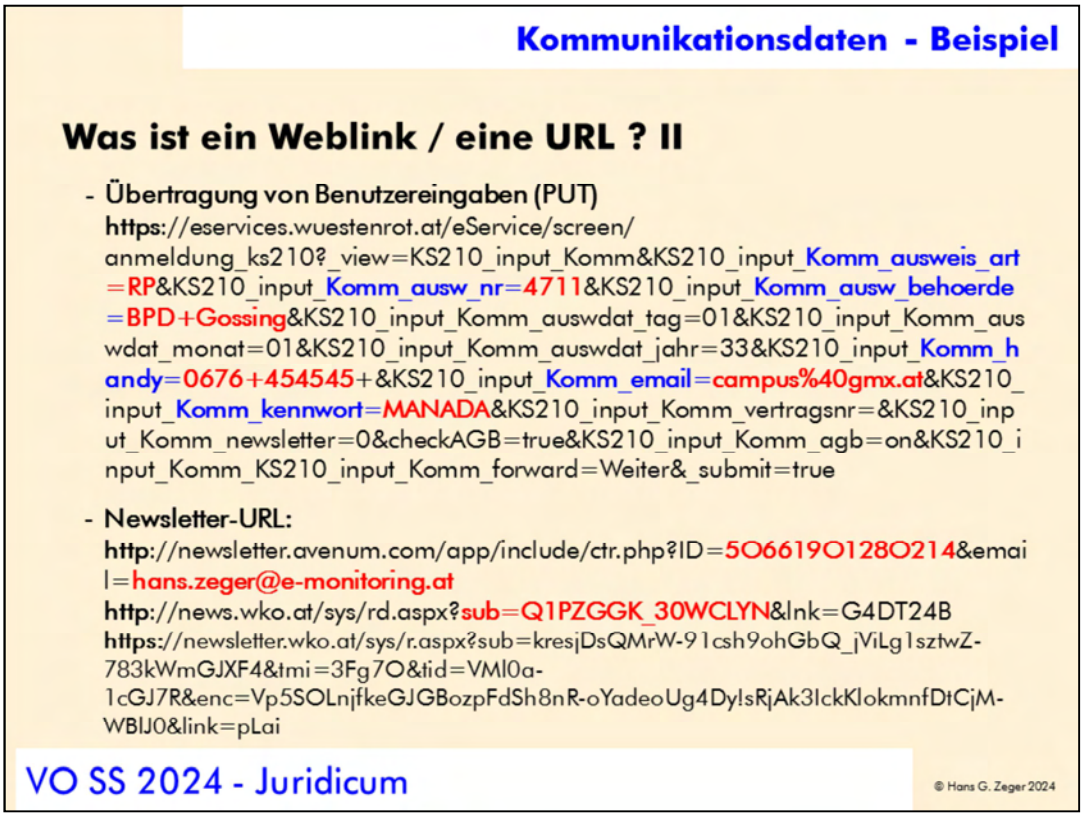
2. die Benutzer oder Nutzer eine jederzeit widerrufbare Einwilligung gegeben haben.

(2) Selbst im Falle einer Einwilligung zur Verarbeitung von Daten gemäß Abs. 1 müssen die Benutzer oder Nutzer die Möglichkeit haben, diese Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu untersagen.

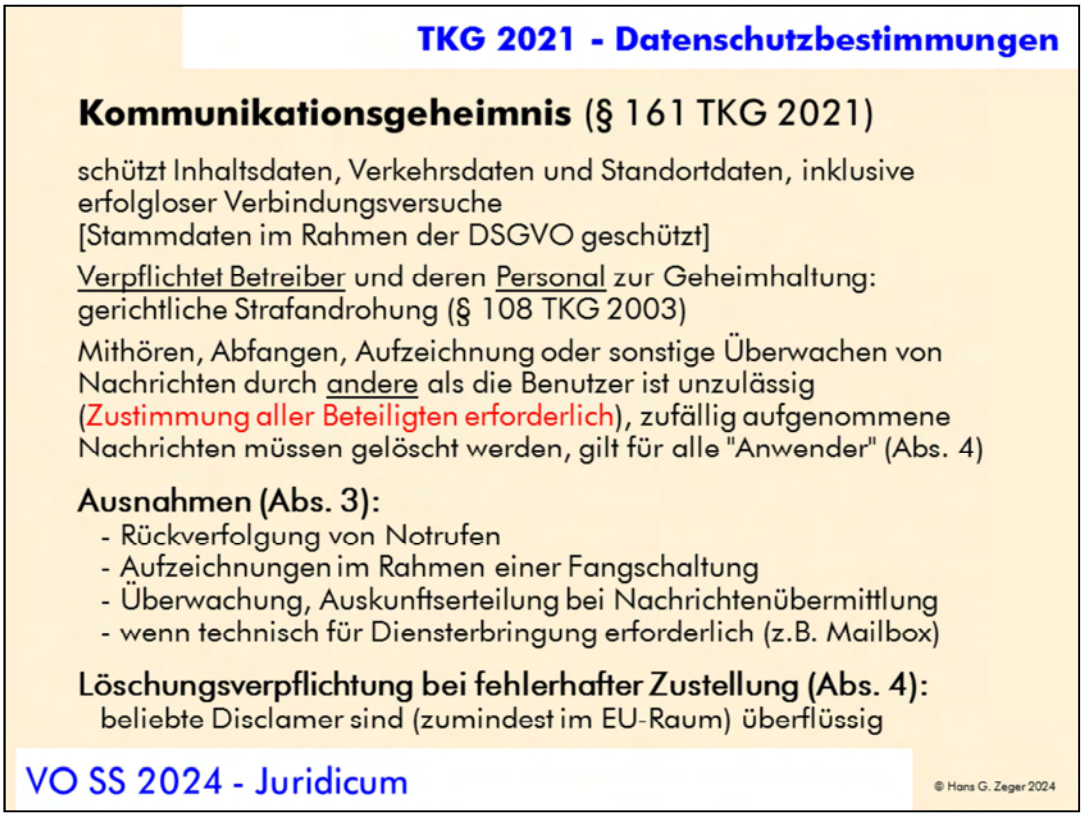
(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß Abs. 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln. Unbeschadet des § 161 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 ?
- Adresse einer Website (sog. Permalinks)
http://www.orf.at
- Google-Suche Amazon (Chrome):
https://www.amazon.de/ ?&tag=hydraamazon09-21&ref=pd_sl_781ozcfkw7_e&adgrpid=153217435865&hvpone=&hvptwo=&hvadid=674893335740&hvpos=&hvnetw=g&hvrand=4007714672474324 85&hvqmt=e&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1000997&hvtargid=kwd-10573980&hydadcr=12763_2327837
https://www.google.at/aclk?sa=L&ai=DChcSEwj0y6TkleKEAxV0W0ECHf5XCisYABAEGgJ3cw&gclid=EAIaIQobChMI9Muk5JXihAMVdFtBAh3-VworEAAYASAEEgLsRvD_BwE&sig=AOD64_1dnNghWuryuQgQK9JQY8awzyWznQ&q&adurl&ved=2ahUKEwjLqZ3kleKEAxXt0gIHHWYxCikQqyQoA3oECAYQDw
- Google-URL:
http://o-o.resolver.o.213.235.197.221.3d6303155122db29.l.google.com/
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Kommunikationsdaten - Beispiel
Was ist ein Weblink / eine URL ? II
- Übertragung von Benutzereingaben (PUT)
https://eservices.wuestenrot.at/eService/screen/anmeldung_ks210?_view=KS210_input_Komm&KS210_input_Komm_ausweis_art=RP&KS210_input_Komm_ausw_nr=4711&KS210_input_Komm_ausw_behoerde=BPD+Gossing&KS210_input_Komm_auswdat_tag=01&KS210_input_Komm_auswdat_monat=01&KS210_input_Komm_auswdat_jahr=33&KS210_input_Komm_handy=0676+454545+&KS210_input_Komm_email=campus%40gmx.at&KS210_input_Komm_kennwort=MANADA&KS210_input_Komm_vertragsnr=&KS210_input_Komm_newsletter=0&checkAGB=true&KS210_input_Komm_agb=on&KS210_input_Komm_KS210_input_Komm_forward=Weiter&_submit=true
- 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
https://newsletter.wko.at/sys/r.aspx?sub=kresjDsQMrW-91csh9ohGbQ_jViLg1sztwZ-783kWmGJXF4&tmi=3Fg7O&tid=VMl0a-1cGJ7R&enc=Vp5SOLnjfkeGJGBozpFdSh8nR-oYadeoUg4DyIsRjAk3IckKlokmnfDtCjM-WBlJ0&link=pLai
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



TKG 2021 § 161

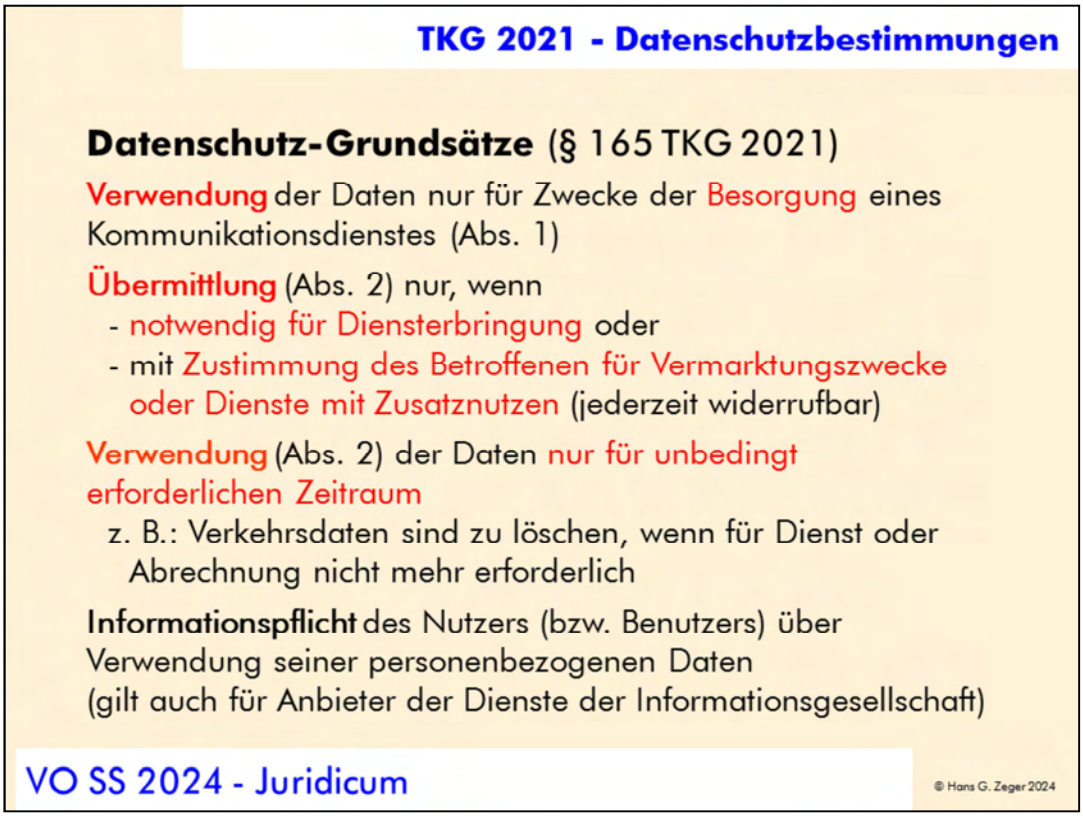
(1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber oder Anbieter eines öffentlichen Kommunikationsnetzes oder -dienstes und alle Personen, die an der Tätigkeit des Betreibers oder Anbieters 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 und Abwicklung von Notrufen und die Fälle der **Fangschaltung**, der Überwachung von Nachrichten nach § 135 Abs. 3 StPO, der Auskunft über Daten einer Nachrichtenübermittlung nach § 135 Abs. 2 StPO, der Auskunft über Daten nach § 99 Abs. 3a des Bundesgesetzes vom 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (FinStrG), BGBl. Nr. 129/1958 idF BGBl. Nr. 21/1959 (DFB), der Auskunft über Daten nach § 11 Abs. 1 Z 7 des Bundesgesetzes über die Organisation, Aufgaben und Befugnisse des Verfassungsschutzes (SNG), BGBl. I Nr. 5/2016, und der Auskunft über Daten nach § 22 Abs. 2a und 2b des Militärbefugnisgesetzes (MBG), BGBl. I Nr. 86/2001, sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

(4) Werden mittels einer Funkanlage, einer Endeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Endeinrichtung 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.

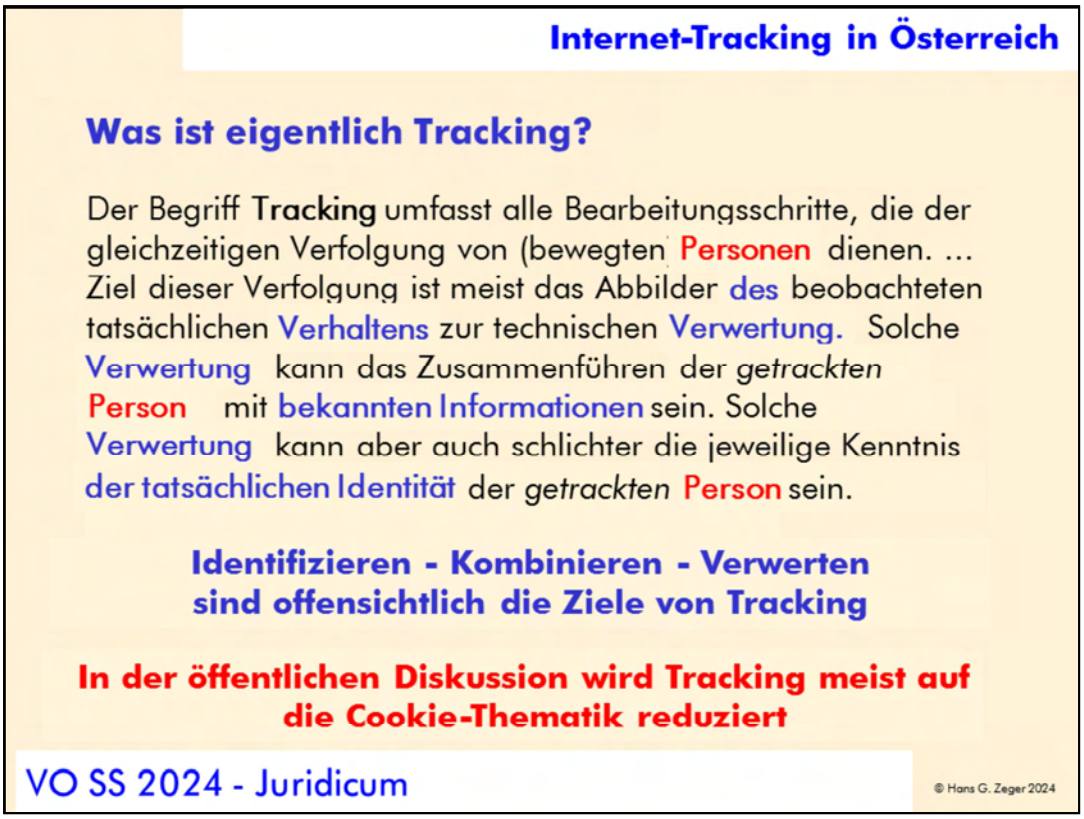


TKG 2021 § 165

(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.

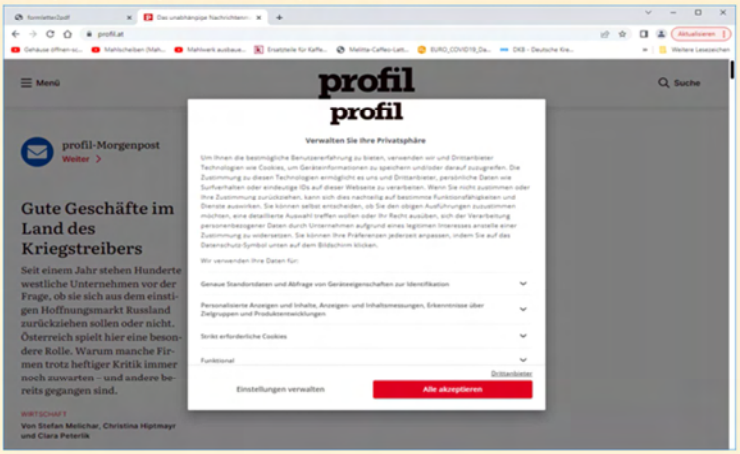

Internet-Tracking in Österreich
Was ist eigentlich Tracking?
Der Begriff Tracking umfasst alle Bearbeitungsschritte, die der gleichzeitigen Verfolgung von (bewegten Personen dienen. ... Ziel dieser Verfolgung ist meist das Abbilder des beobachteten tatsächlichen Verhaltens zur technischen Verwertung. 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
In der öffentlichen Diskussion wird Tracking meist auf die Cookie-Thematik reduziert
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-

Demobeispiel Onlinetracking

Was passiert bei Aufruf einer Website? (VERSION 2023)

Beispiel: https://www.profil.at



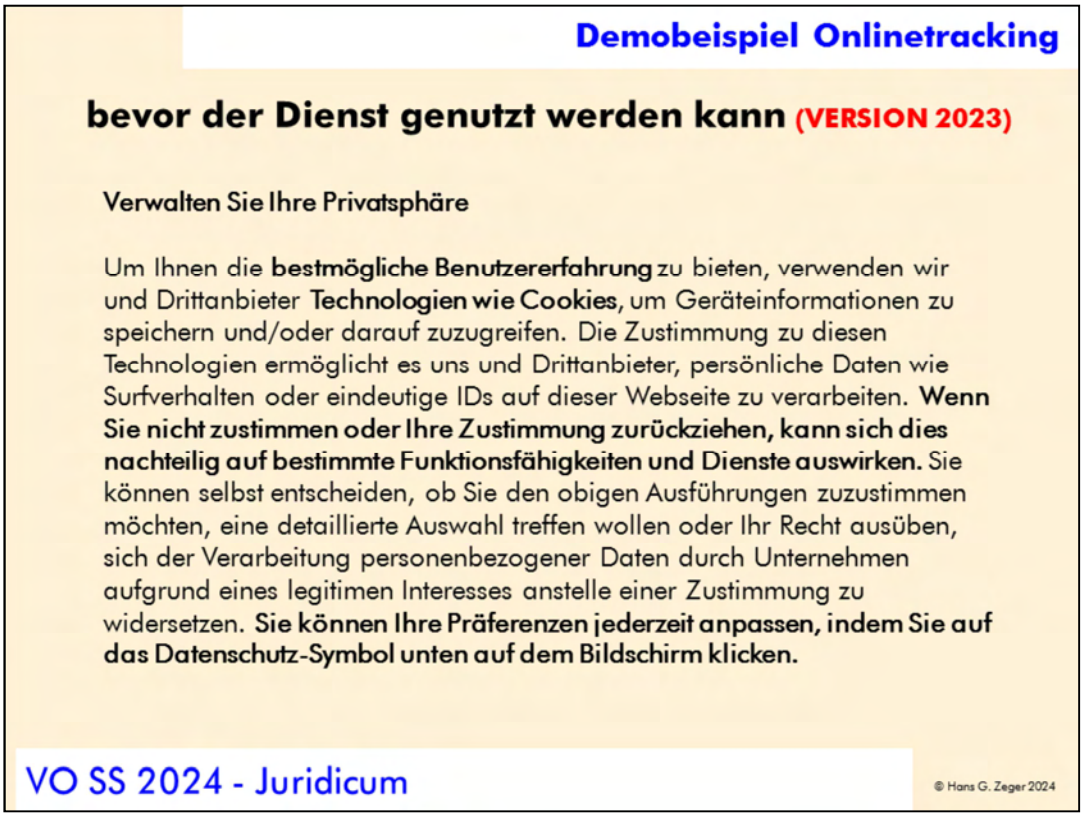
Was erwartet sich Nutzer?

- Informationen von profil und er akzeptiert, dass profil sein Interesse registriert

Was passiert 2023 tatsächlich?

VO SS 2024 - Juridicum

-

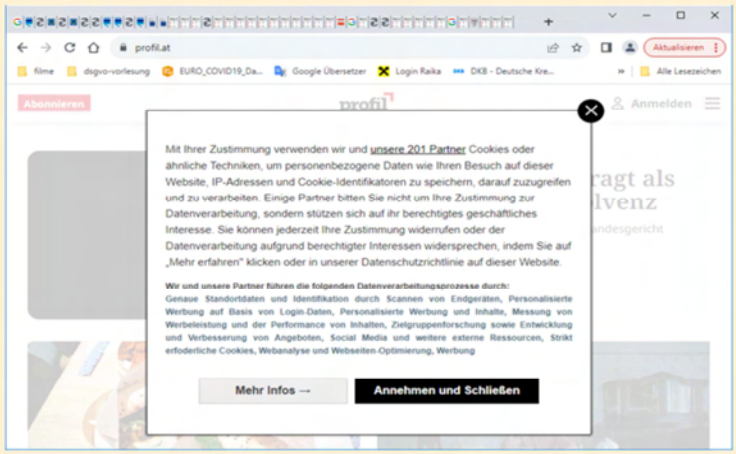

Demobeispiel Onlinetracking
bevor der Dienst genutzt werden kann (VERSION 2023)
Verwalten Sie Ihre Privatsphäre
Um Ihnen die bestmögliche Benutzererfahrung zu bieten, verwenden wir und Drittanbieter Technologien wie Cookies, um Geräteinformationen zu speichern und/oder darauf zuzugreifen. Die Zustimmung zu diesen Technologien ermöglicht es uns und Drittanbieter, persönliche Daten wie Surfverhalten oder eindeutige IDs auf dieser Webseite zu verarbeiten. Wenn Sie nicht zustimmen oder Ihre Zustimmung zurückziehen, kann sich dies nachteilig auf bestimmte Funktionsfähigkeiten und Dienste auswirken. Sie können selbst entscheiden, ob Sie den obigen Ausführungen zuzustimmen möchten, eine detaillierte Auswahl treffen wollen oder Ihr Recht ausüben, sich der Verarbeitung personenbezogener Daten durch Unternehmen aufgrund eines legitimen Interesses anstelle einer Zustimmung zu widersetzen. Sie können Ihre Präferenzen jederzeit anpassen, indem Sie auf das Datenschutz-Symbol unten auf dem Bildschirm klicken.
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-

Demobeispiel Onlinetracking

Was passiert bei Aufruf einer Website? (VERSION 2024)

Beispiel: https://www.profil.at



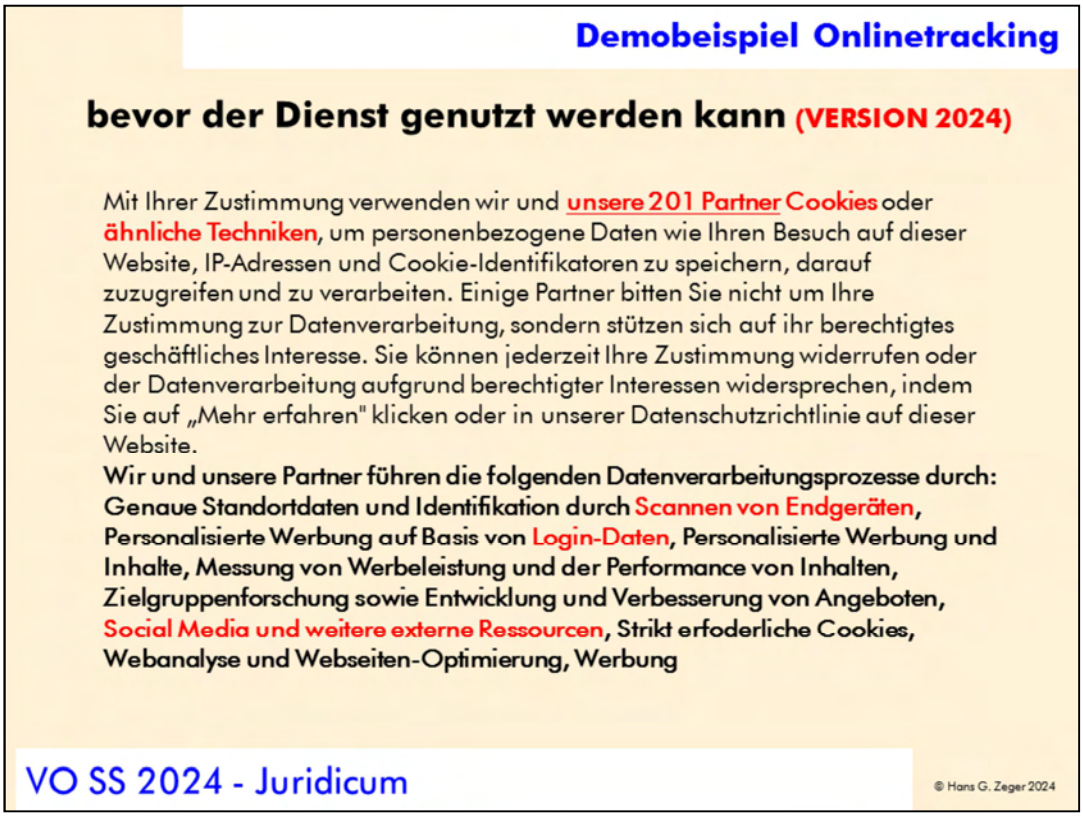
Was erwartet sich der Nutzer?

- Informationen von profil und er akzeptiert, dass profil sein Interesse registriert

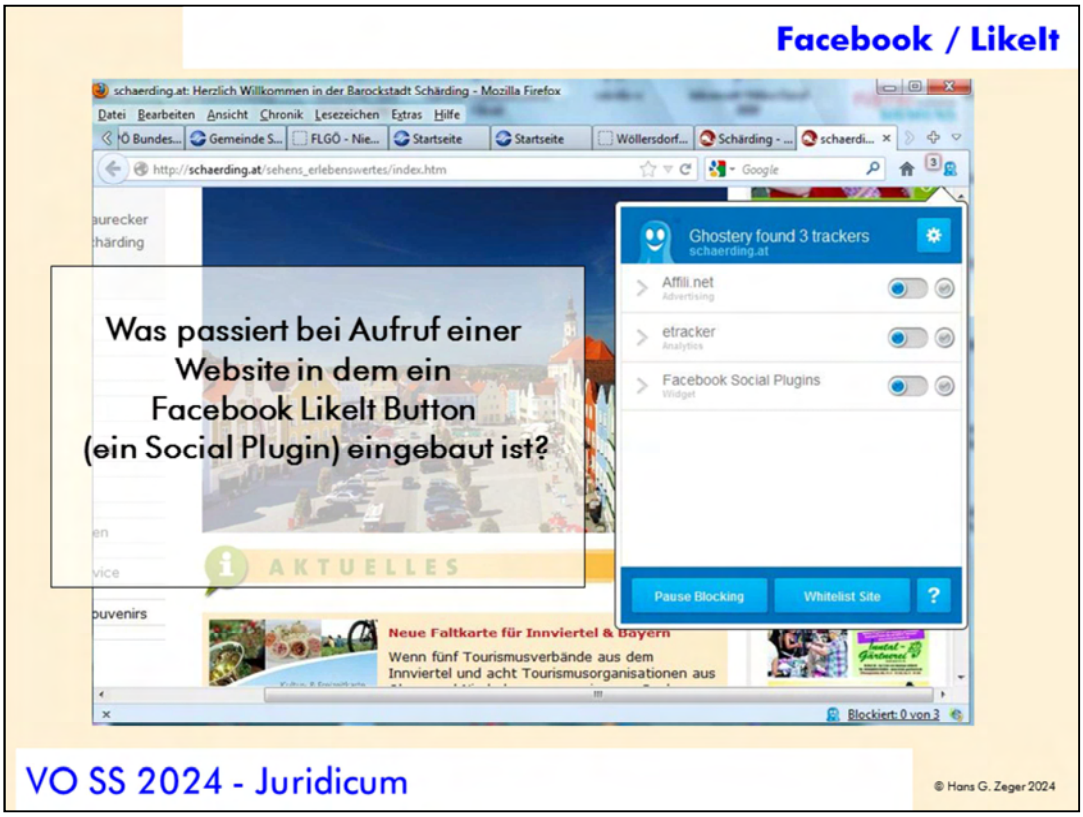
Was passiert 2024 tatsächlich?

VO SS 2024 - Juridicum

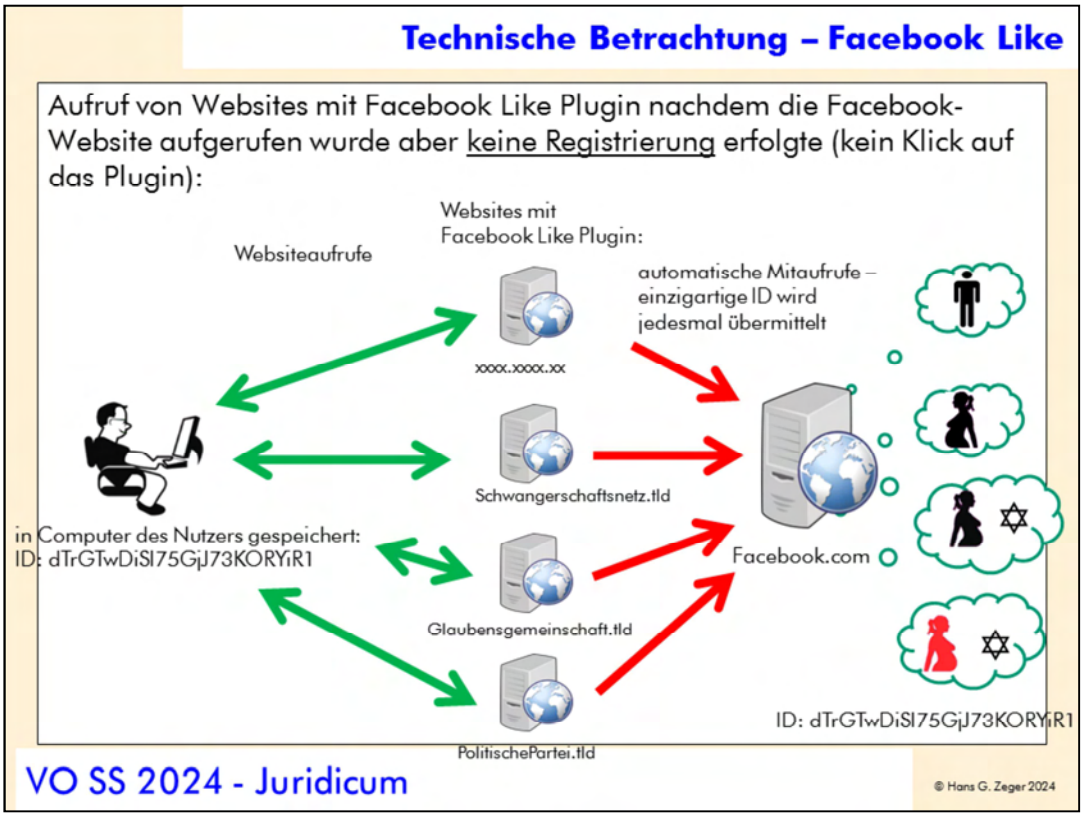
-


Demobeispiel Onlinetracking
bevor der Dienst genutzt werden kann (VERSION 2024)
Mit Ihrer Zustimmung verwenden wir und unsere 201 Partner Cookies oder ähnliche Techniken, um personenbezogene Daten wie Ihren Besuch auf dieser Website, IP-Adressen und Cookie-Identifikatoren zu speichern, darauf zuzugreifen und zu verarbeiten. Einige Partner bitten Sie nicht um Ihre Zustimmung zur Datenverarbeitung, sondern stützen sich auf ihr berechtigtes geschäftliches Interesse. Sie können jederzeit Ihre Zustimmung widerrufen oder der Datenverarbeitung aufgrund berechtigter Interessen widersprechen, indem Sie auf „Mehr erfahren" klicken oder in unserer Datenschutzrichtlinie auf dieser Website.
Wir und unsere Partner führen die folgenden Datenverarbeitungsprozesse durch: Genaue Standortdaten und Identifikation durch Scannen von Endgeräten, Personalisierte Werbung auf Basis von Login-Daten, Personalisierte Werbung und Inhalte, Messung von Werbeleistung und der Performance von Inhalten, Zielgruppenforschung sowie Entwicklung und Verbesserung von Angeboten, Social Media und weitere externe Ressourcen, Strikt erfoderliche Cookies, Webanalyse und Webseiten-Optimierung, Werbung
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Facebook / LikeIt
schaerding.at: Herzlich Willkommen in der Barockstadt Schärding - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://schaerding.at/sehens_erlebenswertes/index.htm
Was passiert bei Aufruf einer Website in dem ein Facebook Likelt Button (ein Social Plugin) eingebaut ist?
Ghostery found 3 trackers
schaerding.at
Affili.net
Advertising
etracker
Analytics
Facebook Social Plugins
Widget
Pause Blocking
Whitelist Site
AKTUELLES
Neue Faltkarte für Innviertel & Bayern
Wenn fünf Tourismusverbände aus dem Innviertel und acht Tourismusorganisationen aus
Blockiert: 0 von 3
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



Graphik: Michael Löffler, e-commerce monitoring Gmbh

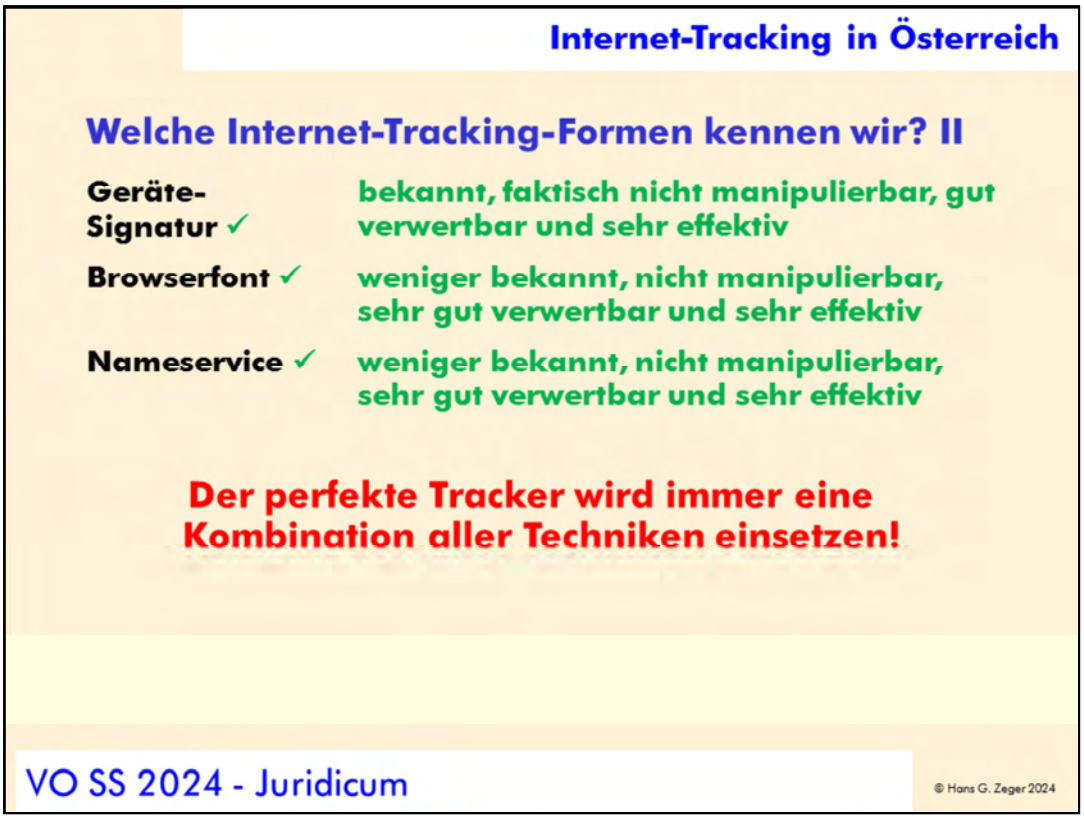
Internet-Tracking in Österreich

Welche Internet-Tracking-Formen kennen wir?

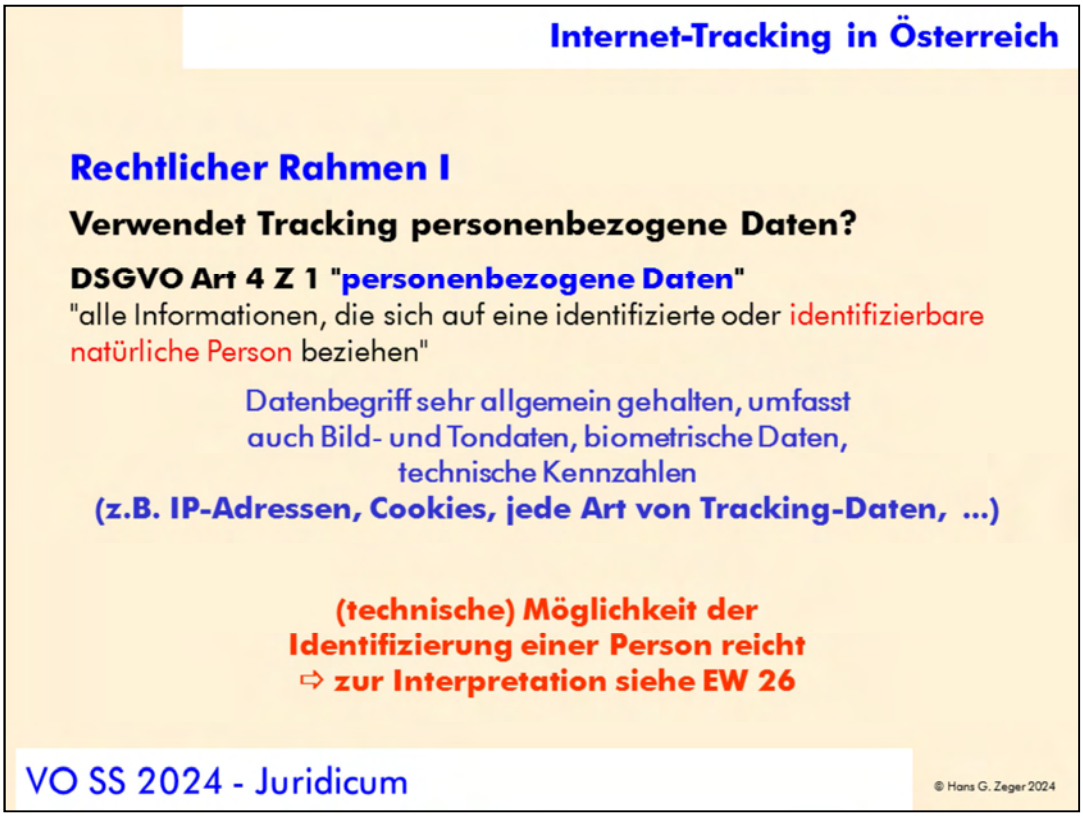
Cookies ✓	**bekannt, leicht zu unterbinden, schwach**
IP-Adresse ✓	**bekannt, oft irreführend (z.B. Internet-Cafes)**
MAC-Adressen ✓	**weniger bekannt, leicht zu manipulieren gut verwertbar**
Zählpixel ✓	**bekannt, vom Benutzer kaum abwehrbar, gut verwertbar**
Skripts, Plugins ✓	**bekannt, theoretisch 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 SS 2024 - Juridicum

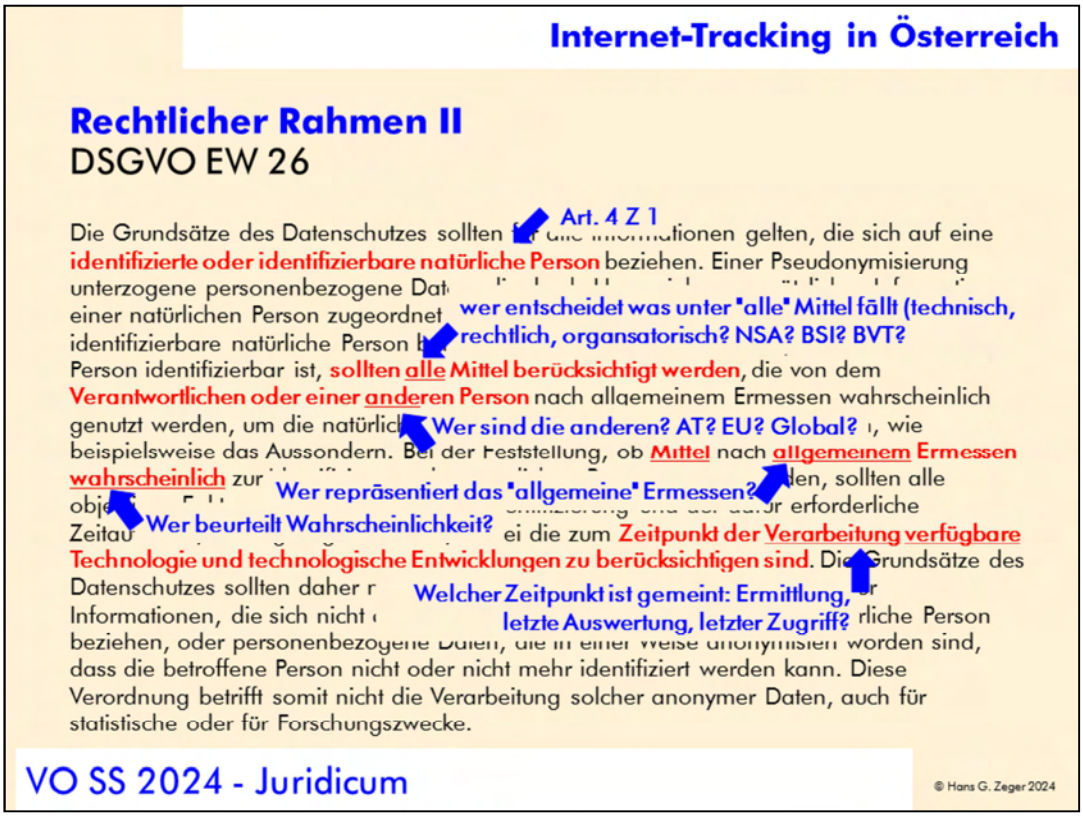
-


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
Nameservice ✓
weniger bekannt, nicht manipulierbar, sehr gut verwertbar und sehr effektiv
Der perfekte Tracker wird immer eine Kombination aller Techniken einsetzen!
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

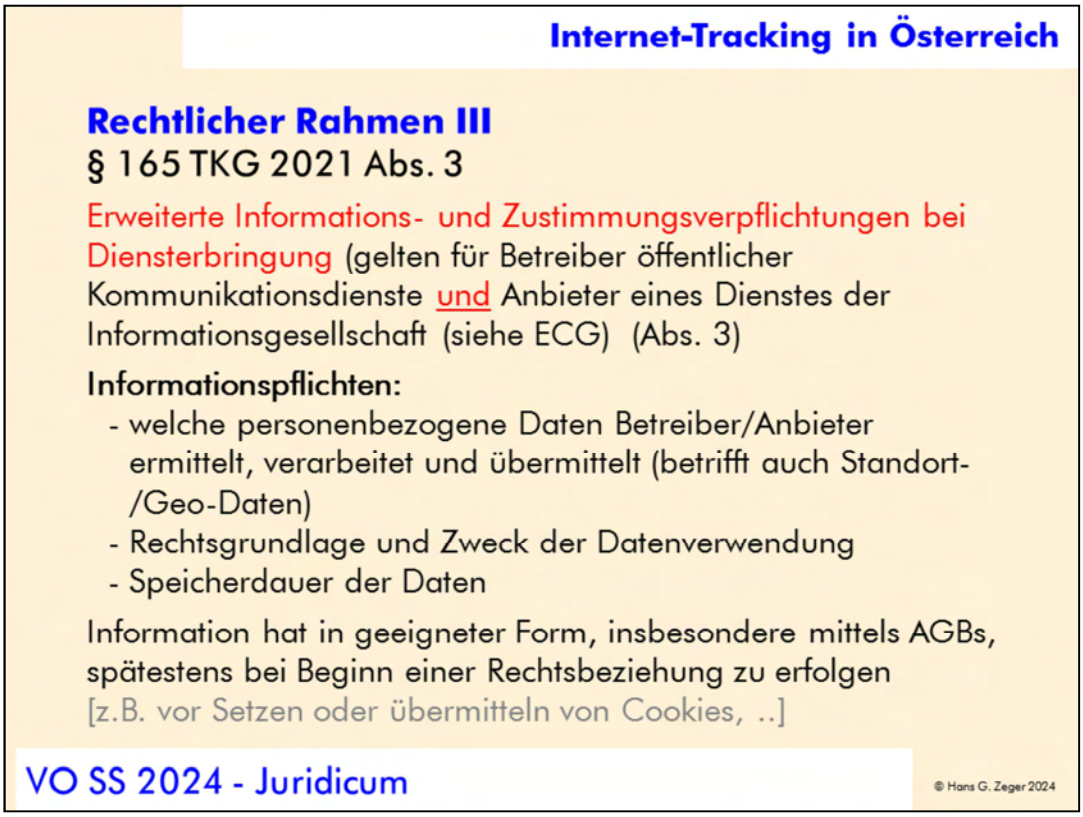
-


Internet-Tracking in Österreich
Rechtlicher Rahmen I
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
⇨ zur Interpretation siehe EW 26
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

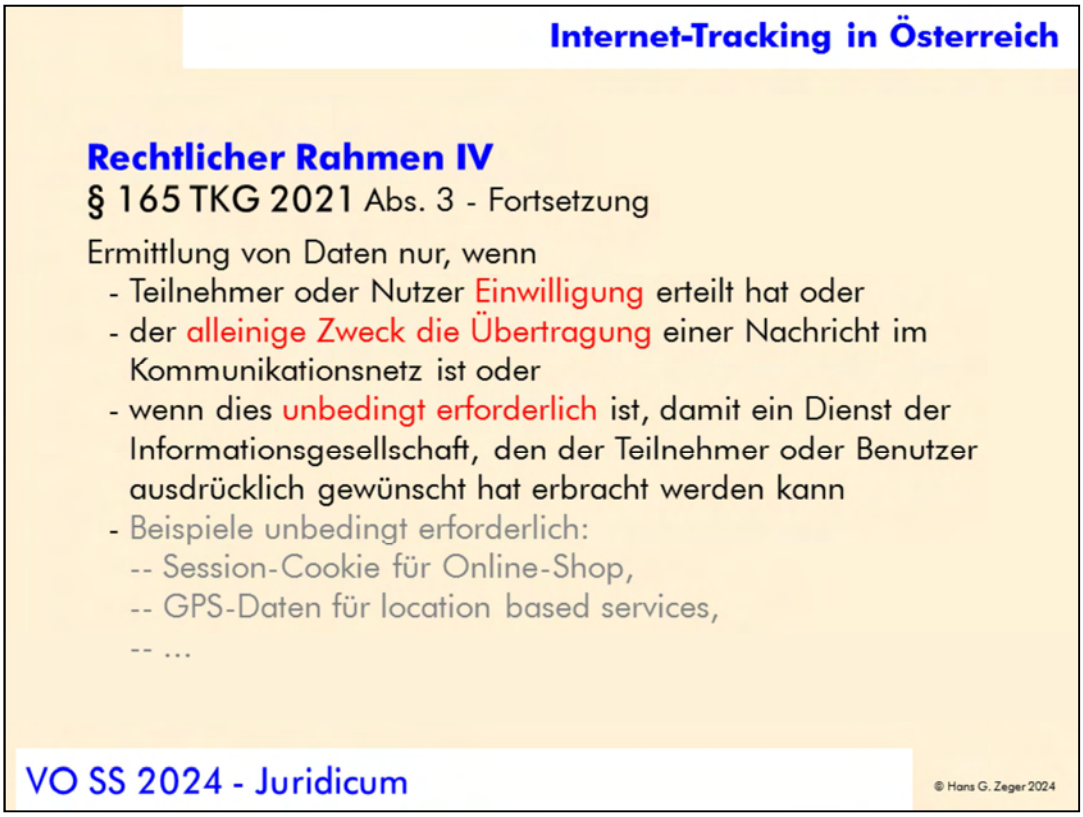
-


Internet-Tracking in Österreich
Rechtlicher Rahmen II
DSGVO EW 26
Art. 4 Z 1
Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Dat
einer natürlichen Person zugeordnet
identifizierbare natürliche Person b
Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürlich
beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur
obje
Zeitau
Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher n
Informationen, die sich nicht
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.
wer entscheidet was unter "alle" Mittel fällt (technisch, rechtlich, organsatorisch? NSA? BSI? BVT?
Wer sind die anderen? AT? EU? Global?
Wer repräsentiert das "allgemeine" Ermessen?
Wer beurteilt Wahrscheinlichkeit?
ei die zum Zeitpunkt der Verarbeitung verfügbare
Welcher Zeitpunkt ist gemeint: Ermittlung, letzte Auswertung, letzter Zugriff?
rliche Person
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

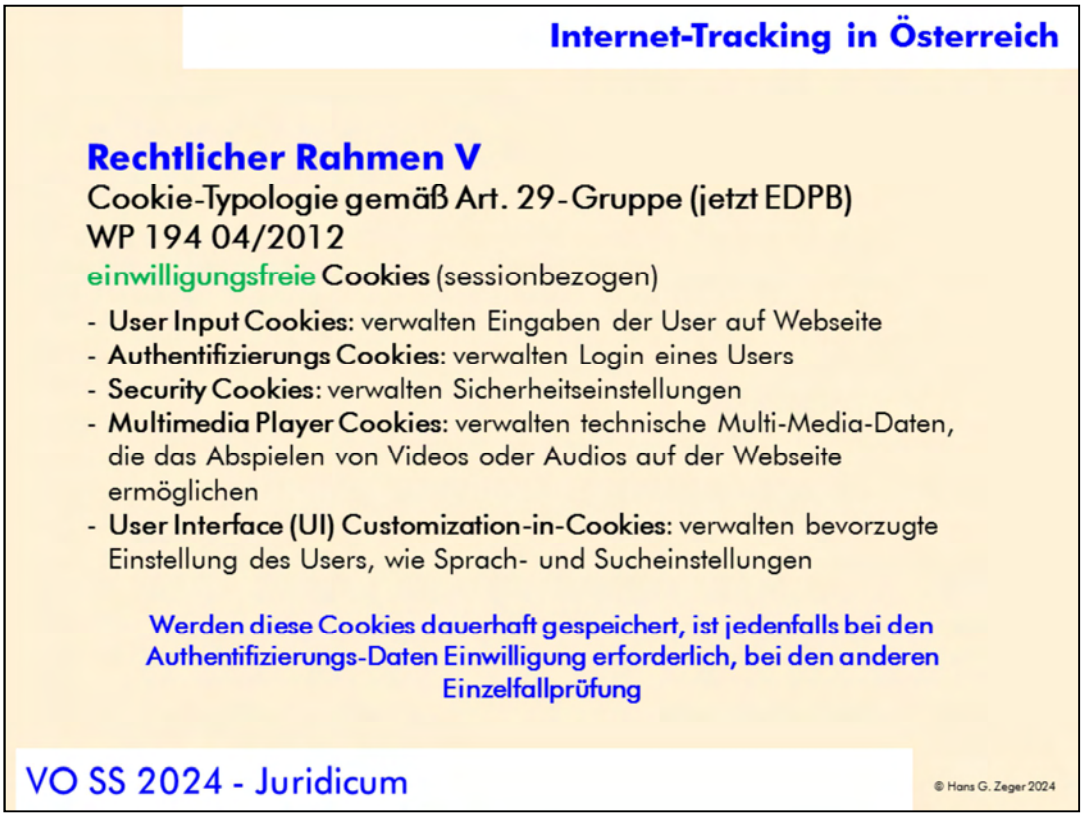
-


Internet-Tracking in Österreich
Rechtlicher Rahmen III
§ 165 TKG 2021 Abs. 3
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 hat in geeigneter Form, insbesondere mittels AGBs, spätestens bei Beginn einer Rechtsbeziehung zu erfolgen
[z.B. vor Setzen oder übermitteln von Cookies, ..]
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

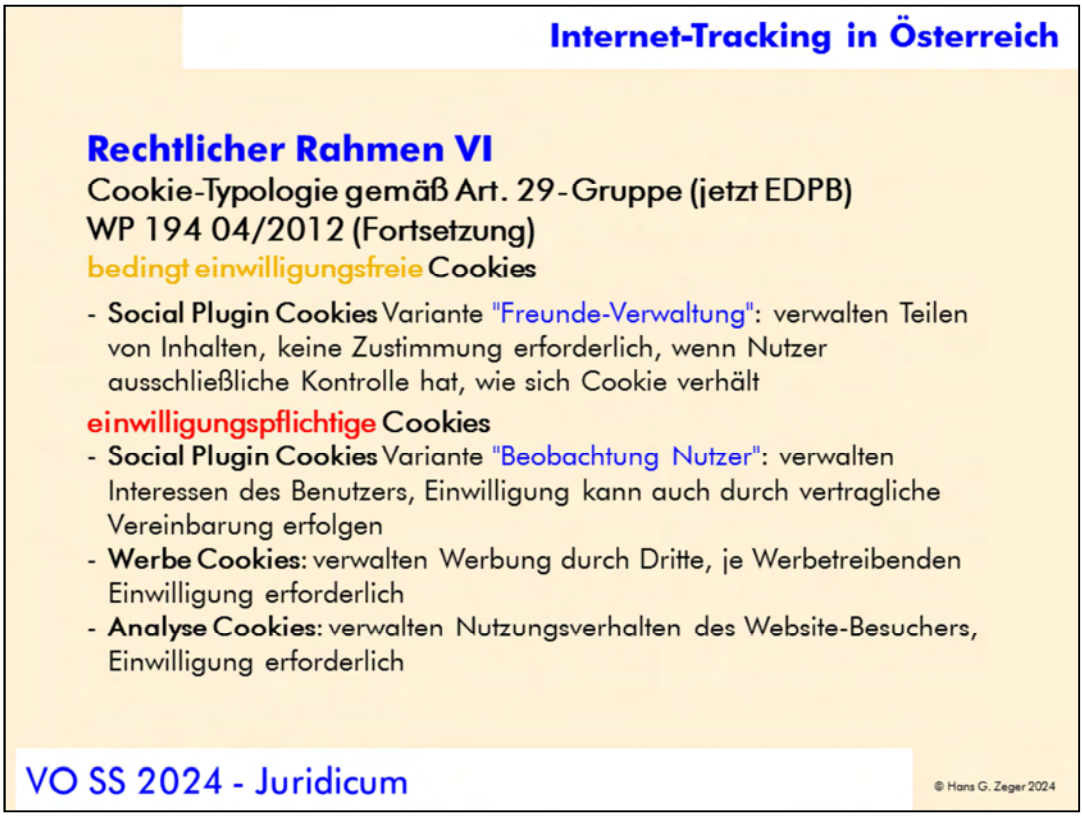
-


Internet-Tracking in Österreich
Rechtlicher Rahmen IV
§ 165 TKG 2021 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
- Beispiele unbedingt erforderlich:
-- Session-Cookie für Online-Shop,
-- GPS-Daten für location based services,
-- ...
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Internet-Tracking in Österreich
Rechtlicher Rahmen V
Cookie-Typologie gemäß Art. 29-Gruppe (jetzt EDPB)
WP 194 04/2012
einwilligungsfreie Cookies (sessionbezogen)
- User Input Cookies: verwalten Eingaben der User auf Webseite
- Authentifizierungs Cookies: verwalten Login eines Users
- Security Cookies: verwalten Sicherheitseinstellungen
- Multimedia Player Cookies: verwalten technische Multi-Media-Daten, die das Abspielen von Videos oder Audios auf der Webseite ermöglichen
- User Interface (UI) Customization-in-Cookies: verwalten bevorzugte Einstellung des Users, wie Sprach- und Sucheinstellungen
Werden diese Cookies dauerhaft gespeichert, ist jedenfalls bei den Authentifizierungs-Daten Einwilligung erforderlich, bei den anderen Einzelfallprüfung
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Internet-Tracking in Österreich
Rechtlicher Rahmen VI
Cookie-Typologie gemäß Art. 29-Gruppe (jetzt EDPB)
WP 194 04/2012 (Fortsetzung)
bedingt einwilligungsfreie Cookies
- Social Plugin Cookies Variante "Freunde-Verwaltung": verwalten Teilen von Inhalten, keine Zustimmung erforderlich, wenn Nutzer ausschließliche Kontrolle hat, wie sich Cookie verhält
einwilligungspflichtige Cookies
- Social Plugin Cookies Variante "Beobachtung Nutzer": verwalten Interessen des Benutzers, Einwilligung kann auch durch vertragliche Vereinbarung erfolgen
- Werbe Cookies: verwalten Werbung durch Dritte, je Werbetreibenden Einwilligung erforderlich
- Analyse Cookies: verwalten Nutzungsverhalten des Website-Besuchers, Einwilligung erforderlich
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-

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.

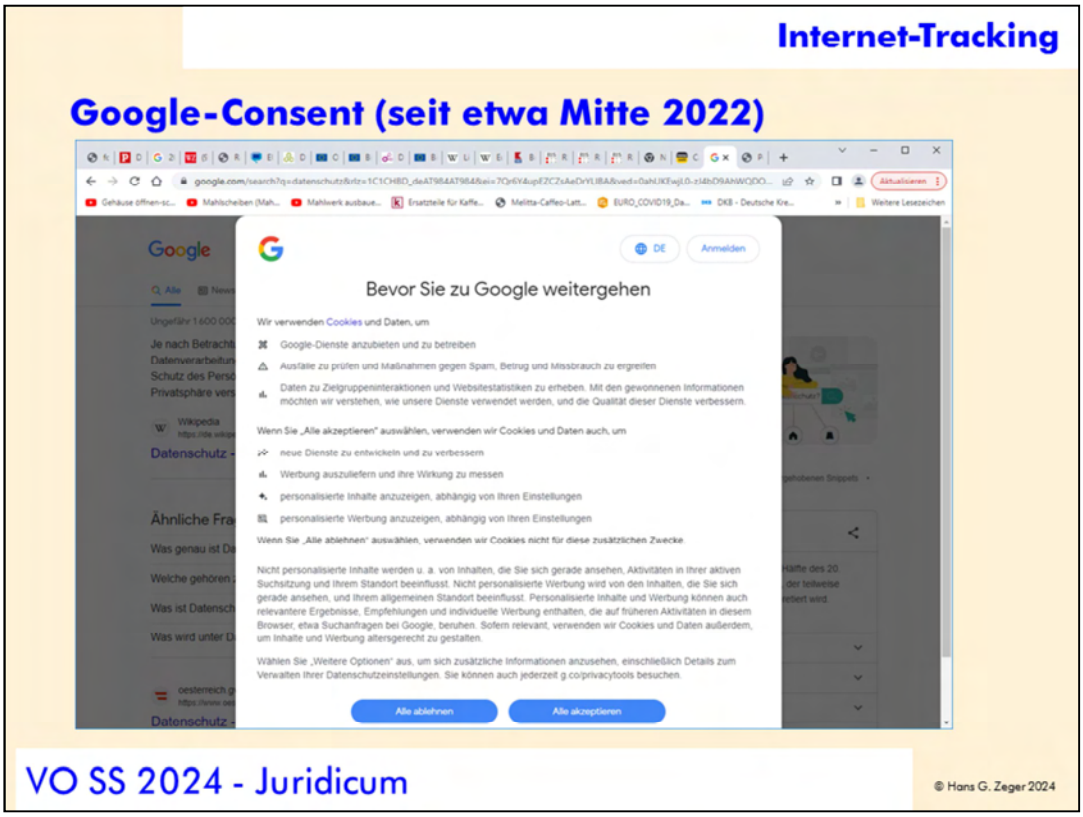
Despite the measures implemented by GOOGLE (documentation and configuration tools), the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life since they are based on a huge amount of data, a wide variety 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.


Internet-Tracking
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
⇨ wird Google die Entscheidung beeindrucken ?
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



Google-Statement

Wir verwenden Cookies und Daten, umGoogle-Dienste anzubieten und zu betreiben

Ausfälle zu prüfen und Maßnahmen gegen Spam, Betrug und Missbrauch zu ergreifen

Daten zu Zielgruppeninteraktionen und Websitestatistiken zu erheben. Mit den gewonnenen Informationen möchten wir verstehen, wie unsere Dienste verwendet werden, und die Qualität dieser Dienste verbessern.
Wenn Sie „Alle akzeptieren" auswählen, verwenden wir Cookies und Daten auch, umneue Dienste zu entwickeln und zu verbessern
Werbung auszuliefern und ihre Wirkung zu messen
personalisierte Inhalte anzuzeigen, abhängig von Ihren Einstellungen
personalisierte Werbung anzuzeigen, abhängig von Ihren Einstellungen

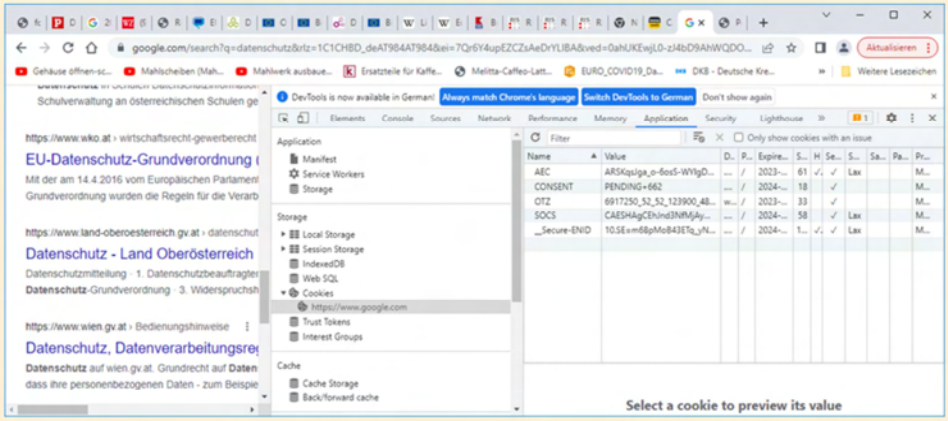
Wenn Sie „Alle ablehnen" auswählen, verwenden wir Cookies nicht für diese zusätzlichen Zwecke.

Nicht personalisierte Inhalte werden u. a. von Inhalten, die Sie sich gerade ansehen, Aktivitäten in Ihrer aktiven Suchsitzung und Ihrem Standort beeinflusst. Nicht personalisierte Werbung wird von den Inhalten, die Sie sich gerade ansehen, und Ihrem allgemeinen Standort beeinflusst. Personalisierte Inhalte und Werbung können auch relevantere Ergebnisse, Empfehlungen und individuelle Werbung enthalten, die auf früheren Aktivitäten in diesem Browser, etwa Suchanfragen bei Google, beruhen. Sofern relevant, verwenden wir Cookies und Daten außerdem, um Inhalte und Werbung altersgerecht zu gestalten.

Wählen Sie „Weitere Optionen" aus, um sich zusätzliche Informationen anzusehen, einschließlich Details zum Verwalten Ihrer Datenschutzeinstellungen. Sie können auch jederzeit g.co/privacytools besuchen.

Internet-Tracking

Google-Consent II



bei "alles ablehnen"

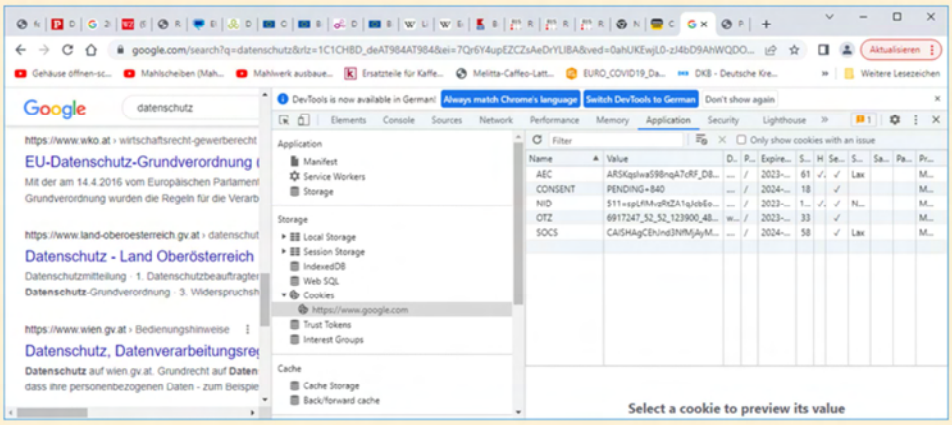
- Google setzt 5 "Cookies": AEC, CONSENT, OTZ, SOCS, _Secure-ENID

VO SS 2024 - Juridicum

-

Internet-Tracking

Google-Consent III



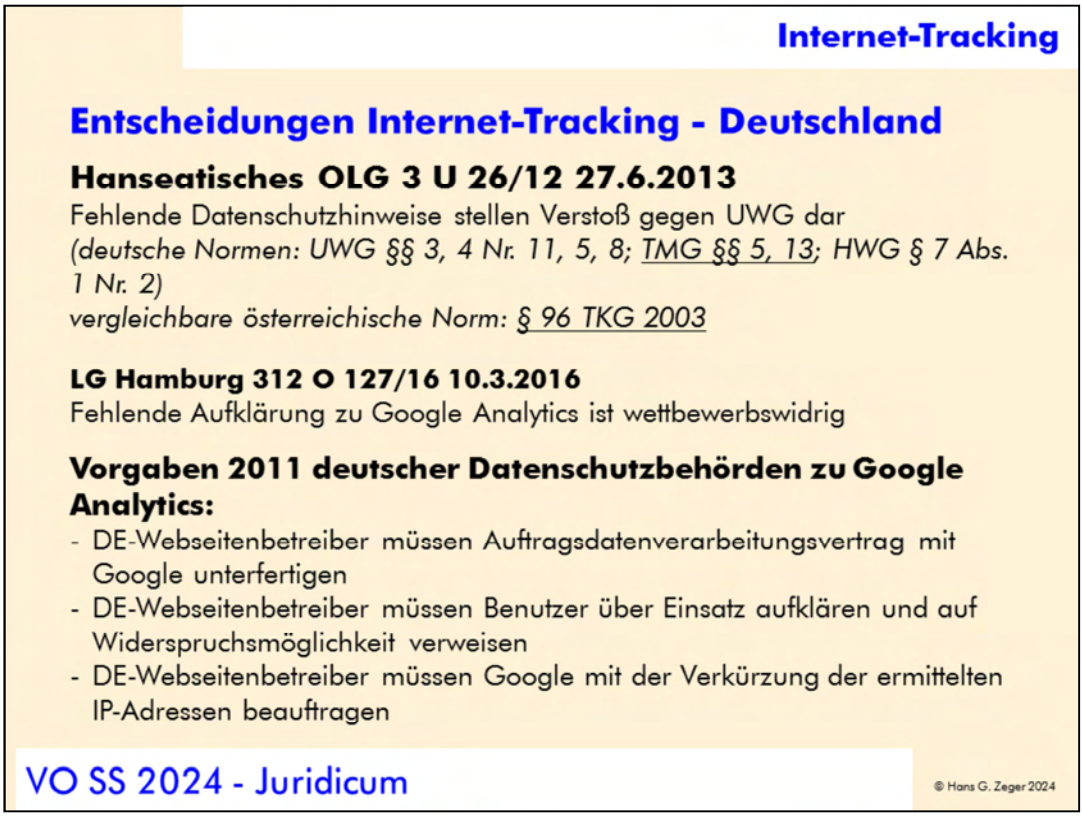
bei "alle akzeptieren"

- Google setzt 5 "Cookies": AEC, CONSENT, NID, OTZ, SOCS

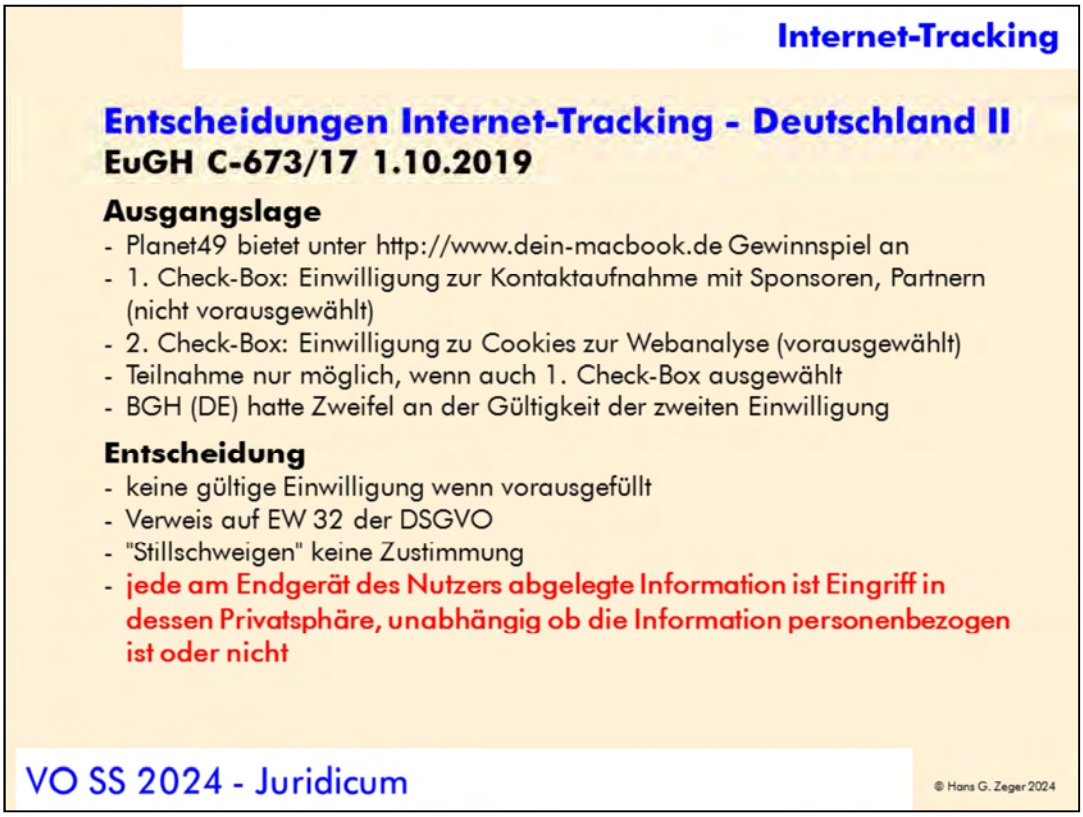
Unterschied liegt in den Inhalten, die jedoch nicht transparent ausgewiesen sind

VO SS 2024 - Juridicum

-


Internet-Tracking
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
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

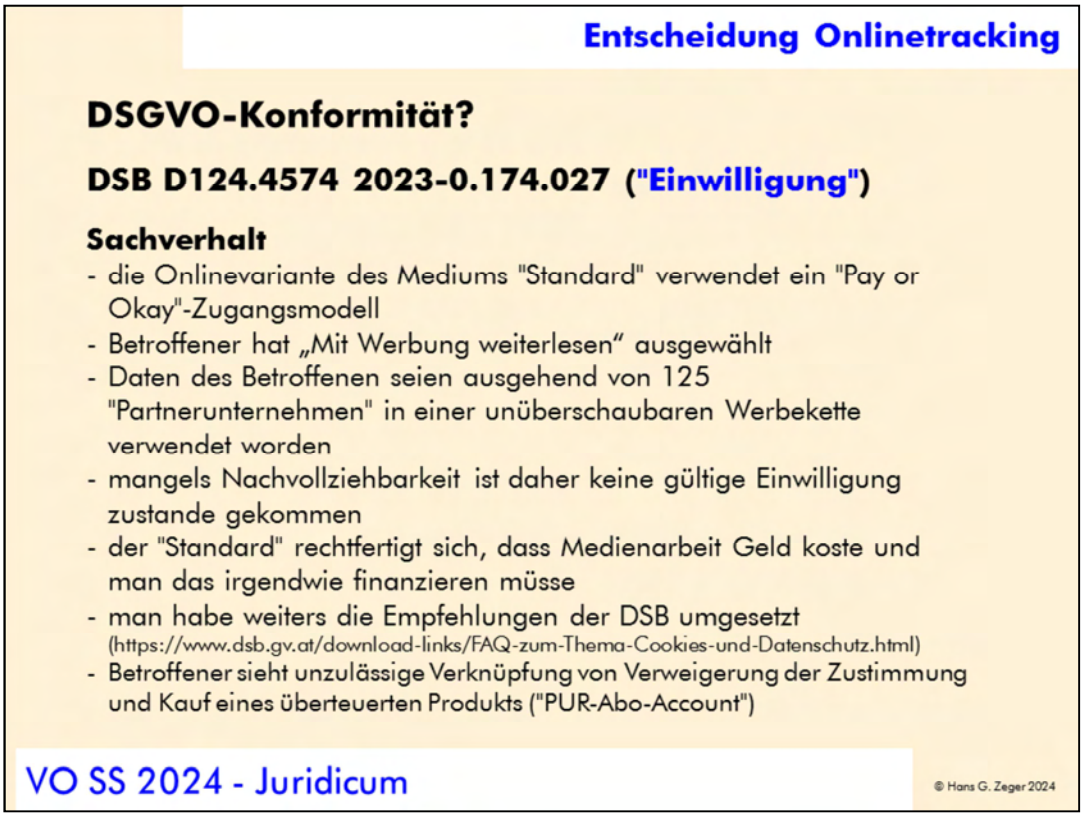
-


Internet-Tracking
Entscheidungen Internet-Tracking - Deutschland II
EuGH C-673/17 1.10.2019
Ausgangslage
- Planet49 bietet unter http://www.dein-macbook.de Gewinnspiel an
- 1. Check-Box: Einwilligung zur Kontaktaufnahme mit Sponsoren, Partnern (nicht vorausgewählt)
- 2. Check-Box: Einwilligung zu Cookies zur Webanalyse (vorausgewählt)
- Teilnahme nur möglich, wenn auch 1. Check-Box ausgewählt
- BGH (DE) hatte Zweifel an der Gültigkeit der zweiten Einwilligung
Entscheidung
- keine gültige Einwilligung wenn vorausgefüllt
- Verweis auf EW 32 der DSGVO
- "Stillschweigen" keine Zustimmung
- jede am Endgerät des Nutzers abgelegte Information ist Eingriff in dessen Privatsphäre, unabhängig ob die Information personenbezogen ist oder nicht
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Internet-Tracking
Internet-Tracking - Österreich
Beschwerden
- allein Max Schrems (nyob) hat mehrere hundert Beschwerden wegen DSGVO-widriger Cookie-Banner eingebracht (Frühjahr 2023: 700+)
- weitere 101 Beschwerden wegen der Verwendung von Google Analytics
Entscheidung
- bisher eine Teilentscheidung der DSB (D155.027 2021-0.586.257) zur Unzulässigkeit von Google Analytics
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



DSB D124.4574 2023-0.174.027

...

B. Beschwerdegegenstand

B.1. Ausgehend vom Vorbringen des Beschwerdeführers, insbesondere aufgrund seines (ausdrücklichen) Antrags vom 2. September 2021 und seiner Aussage im Rahmen der mündlichen Verhandlung vom 3. Februar 2023 (S. 15 der Niederschrift), ergibt sich als Beschwerdegegenstand die Frage, ob die Beschwerdegegner den Beschwerdeführer im

A) Recht auf Geheimhaltung gemäß § 1 Abs. 1 DSG verletzt und (dadurch auch) gegen den

B) Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 lit. a iVm Art. 6 Abs. 1 DSGVO verstoßen haben, indem beim Besuch des Nachrichtenportals www.derstandard.at zumindest am 12. August 2021 personenbezogene Daten des Beschwerdeführers (diese sind, jedenfalls in Kombination, einzigartige Nutzer-Identifikations-Nummern, IP-Adresse und Browserparameter) unrechtmäßig verarbeitet wurden.

...

C. Sachverhaltsfeststellungen

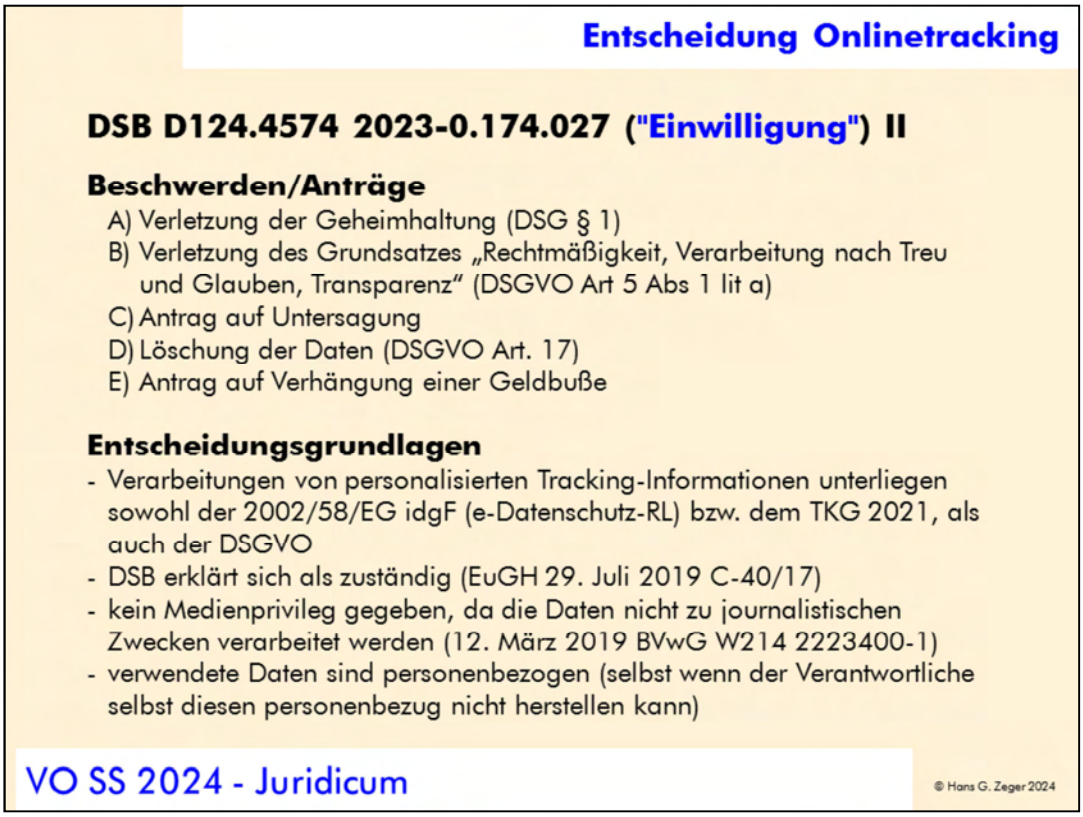
[Anm. ident zu Schlussanträgen des Generalanwalts in der Rechtssache C-673/17 Rz 36-39]

C.1. Mittels Cookies lassen sich Informationen sammeln, die von einer Website generiert und über den Browser eines Internetnutzers gespeichert wurden. Es handelt sich um eine kleine Datei oder Textinformation (in der Regel kleiner als ein Kbyte), die von einer Website über den Browser eines Internetnutzers auf der Festplatte seines Computers oder mobilen Endgeräts platziert wird.

Ein Cookie erlaubt es der Website, sich an die Aktionen oder Vorlieben des Nutzers zu „erinnern“. Die meisten Webbrowser unterstützen Cookies, aber die Nutzer können ihre Browser so einstellen, dass sie die Cookies abweisen. Sie können die Cookies auch jederzeit löschen.

Websites nutzen Cookies, um Nutzer zu identifizieren, sich die Vorlieben ihrer Kunden zu merken und es den Nutzern zu ermöglichen, Aufgaben abzuschließen, ohne Informationen neu eingeben zu müssen, wenn sie zu einer anderen Seite wechseln oder die Website später erneut besuchen.

Cookies können auch genutzt werden, um anhand des Online-Verhaltens Informationen für gezielte Werbung und Vermarktung zu sammeln. Unternehmen verwenden zum Beispiel Software, um das Nutzerverhalten nachzuverfolgen und persönliche Profile zu erstellen, die es ermöglichen, den Nutzern Werbung zu zeigen, die auf ihre zuvor durchgeführten Suchvorgänge zugeschnitten ist. ...



DSB D124.4574 2023-0.174.027 (Fortsetzung)

...

D.2. Verarbeitung personenbezogener Daten

a) Zu Art. 4 Z 1 DSGVO

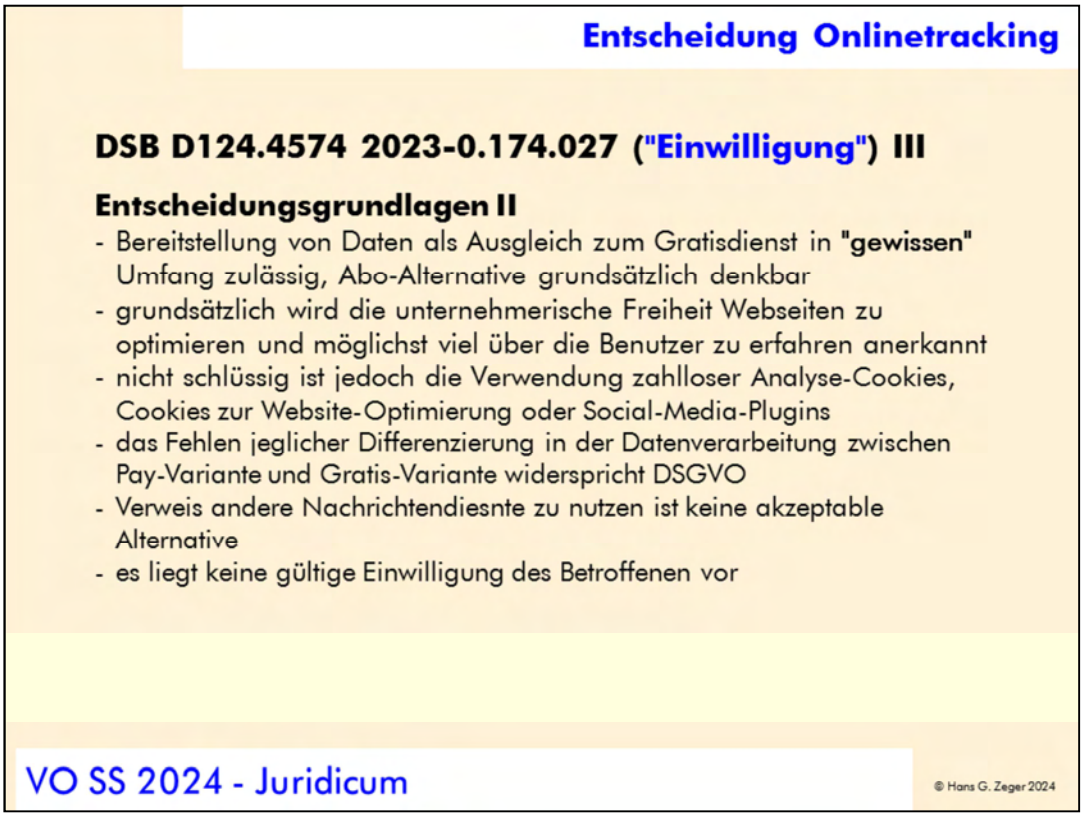
Die Datenschutzbehörde hat im Fall Google Analytics – im Einklang mit der Judikatur des Europäischen Datenschutzbeauftragten (EDSB) – bereits ausgesprochen, dass Cookies, die einen einzigartigen, zufallsgenerierten Wert (random number) beinhalten und die mit dem Zweck gesetzt werden, Personen zu individualisieren und auszusondern, die Definition des Art. 4 Z 1 DSGVO erfüllen. Insbesondere kann nie ausgeschlossen werden, dass die Cookie-Werte und die IP-Adresse des Endgeräts einer Person an irgendeiner Stelle der Verarbeitungskette mit Zusatzinformationen verknüpft werden, z.B. wenn sich die betroffene Person auf einer Website mit ihrer Email-Adresse oder dem Klarnamen registriert, oder durch eine Verknüpfung durch ein soziales Netzwerk (vgl. zur näheren Begründung den Bescheid vom 22. April 2022, GZ: 2022-0.298.191, abrufbar unter https://www.dsb.gv.at/downloadlinks/bekanntmachungen.html; vgl. zur Einordnung von zB. Google Analytics Cookies als personenbezogene Daten auch die Entscheidung des EDSB gegen das Europäische Parlament vom 5. Jänner 2022, GZ: 2020-1013, S. 13).

...

Im gegenständlichen Fall haben die Beschwerdegegner – entgegen den Vorgaben von Art. 5 Abs. 2, Art. 24 Abs. 1 sowie Art. 25 Abs. 1 DSGVO, der bereits an einem Zeitpunkt vor Beginn der Datenverarbeitung anknüpft – keinen Nachweis erbracht, dass technische Schutzmaßnahmen implementiert wurden, um eine Verknüpfung dieser Daten mit weiteren Zusatzinformationen zu verhindern (vgl. den Rechenschafts- und Compliancepflichten eines Verantwortlichen das Urteil des EuGH vom 27. Oktober 2022, C-129/21 Rz 81).

Nicht erforderlich ist es, dass die Beschwerdegegner selbst einen Personenbezug herstellen können müssen (vgl. das Urteil des EuGH vom 29. Juli 2019, C-40/17, Rz 66 ff und die dort angeführten weiteren Nachweise).

Schließlich spricht für eine weite Auslegung von Art. 4 Z 1 DSGVO auch der Schutzzweck der Verordnung. Dieser liegt darin, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten (vgl. das Urteil des EuGH vom 1. August 2022, C-184/20 Rz 61).



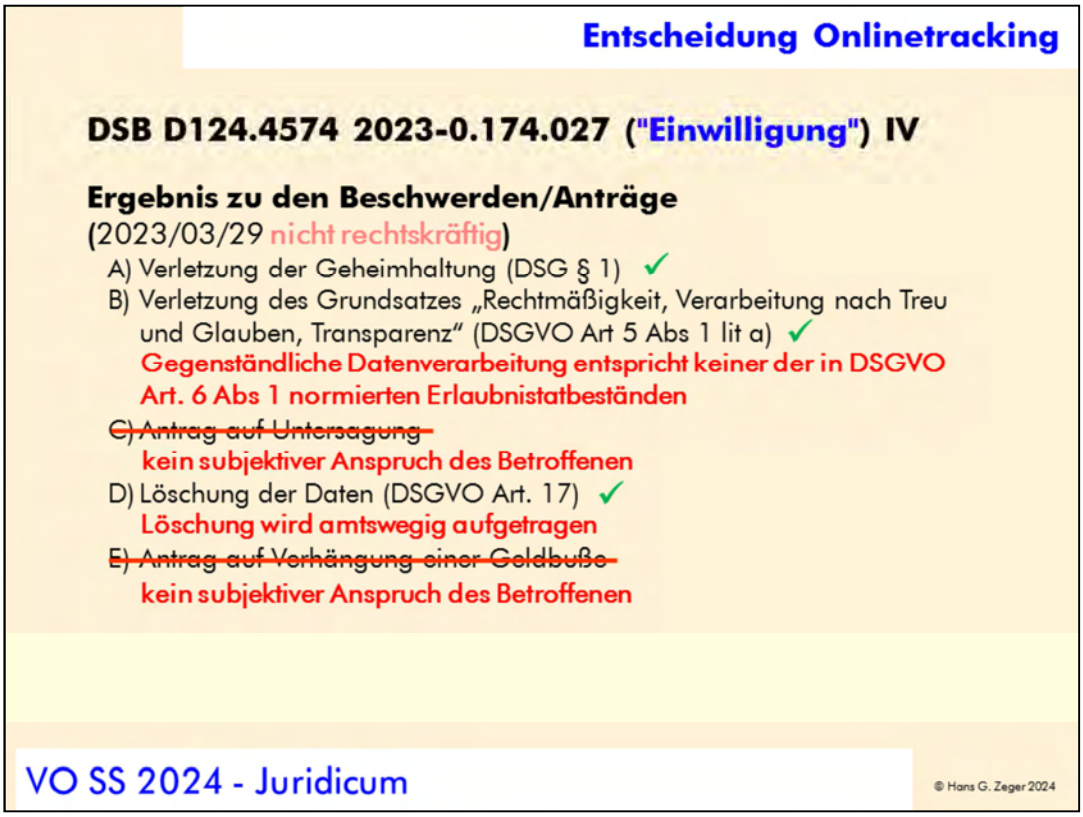
DSB D124.4574 2023-0.174.027 (Fortsetzung)

b) Gültigkeit der Einwilligung im konkreten Fall

Dem Grunde nach kann ein kostenpflichtiges Abonnement weiterhin eine tragfähige Alternative für eine Einwilligung sein (vgl. Frage 9 der FAQ der Datenschutzbehörde, abrufbar unter https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html). Mit der Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen bringt der europäische Gesetzgeber nämlich seinen Willen zum Ausdruck, dass Verbraucher – zumindest im gewissen Ausmaß – im Austausch für digitale Dienstleistungen ihre Daten bereitstellen können.

Fraglich ist jedoch, in welchem konkreten Ausmaß dies möglich ist. Bei dieser Beurteilung spielt im gegebenen Fall die sogenannte „Granularität einer Einwilligung" – als Aspekt der Freiwilligkeit – eine wesentliche Rolle. ...
Im gegenständlichen Fall haben die Beschwerdegegner unstrittig eine Einwilligung für zahlreiche, in ihrer Datenschutzerklärung angeführten Verarbeitungszwecke eingeholt (vgl. Sachverhaltsfeststellung C.5.).
Aus Sicht der Datenschutzbehörde konnten die Beschwerdegegner nicht schlüssig erklären, inwiefern es – neben der Einwilligung zum Zweck der Anzeige (personalisierter) Werbung und der Messung des Werbeerfolgs – angemessen ist, dass die Einwilligung auch weitere Verarbeitungsvorgänge umfasst, die mit dem Einsatz von vielen unterschiedlichen Analyse-Cookies, Cookies zur Website-Optimierung oder Social-Media-Plugins in Verbindung steht.
...
Ein Vorgehen, bei dem jedoch nicht einmal versucht wird, die oben angeführten Vorgaben hinsichtlich der Granularität einzuhalten, und bei dem eine „Pauschaleinwilligung" einer Abonnement-Variante gegenübergestellt wird, kann kein angemessener Ausgleich zwischen dem Grundrecht auf Datenschutz nach Art. 8 EU-GRC und Art. 16 EU-GRC sein.
Mit anderen Worten: Ein wirtschaftliches Interesse kann nicht dazu führen, dass es – iSd ErwGr 43 DSGVO – angemessen ist, für unterschiedliche Verarbeitungsvorgänge keine gesonderte Einwilligung einzuholen.

So hat auch der EuGH wiederholt ausgesprochen, dass sich Eingriffe in das Grundrecht auf Datenschutz auf das absolut Notwendige beschränken müssen und dass ein hoher Maßstab an die oben dargestellten Voraussetzungen für eine gültige Einwilligung zu setzen ist (vgl. die Urteile vom 14. Februar 2019, C-345/17 Rz 64 sowie vom 1. Oktober 2019, C-673/17 Rz 51 ff).



DSB D124.4574 2023-0.174.027 (Fortsetzung)

1. Der Beschwerde wird teilweise stattgegeben und es wird festgestellt, dass die Beschwerdegegner B) gegen den Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 lit. a iVm Art. 6 Abs. 1 DSGVO verstoßen und den Beschwerdeführer damit auch A) im Recht auf Geheimhaltung gemäß § 1 Abs. 1 DSG verletzt haben, indem diese beim Besuch des Nachrichtenportals www.derstandard.at zumindest am 12. August 2021 personenbezogene Daten des Beschwerdeführers (diese sind, jedenfalls in Kombination, einzigartige Nutzer-Identifikations-Nummern, IP-Adresse und Browserparameter) unrechtmäßig verarbeitet haben.

2. Betreffend Beschwerdepunkt D) werden die Beschwerdegegner angewiesen, innerhalb einer Frist von vier Wochen ihren Datenbestand dahingehend zu überprüfen, ob die in Sachverhaltsfeststellung C.8. genannten Cookie-Werte (value) und Browserdaten zum aktuellen Zeitpunkt noch verarbeitet werden und, sofern dies bejaht wird, diese Daten unverzüglich bei sonstiger Exekution zu löschen.

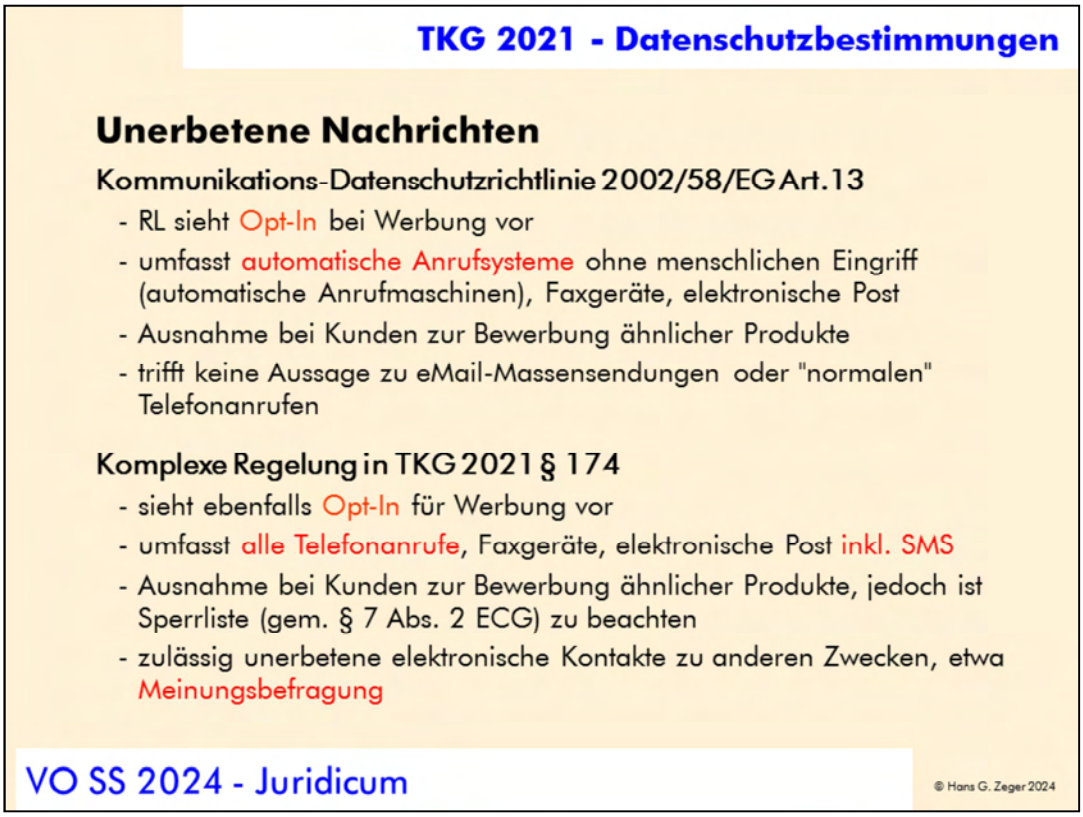
3. Die Anträge zu C) (Untersagung der relevanten Verarbeitungsvorgänge) und E) (Antrag auf Verhängung einer Geldbuße) werden zurückgewiesen.

f) Ergebnis für Spruchpunkt 1
Die gegenständliche Datenverarbeitung kann durch keinen Tatbestand des Art. 6 Abs. 1 DSGVO und § 1 Abs. 2 DSG gerechtfertigt werden und erweist sich daher als unrechtmäßig. ...

D.4. Zu Spruchpunkt 2
Spruchpunkt 2 stützt sich auf die in Art. 58 Abs. 2 lit. d DSGVO normierter Abhilfebefugnis. Nach Judikatur des Bundesverwaltungsgerichts ist es nämlich zulässig, dass die Datenschutzbehörde auch im Beschwerdeverfahren von ihren in Art. 58 Abs. 2 DSGVO normierten Befugnissen amtswegig Gebrauch macht (vgl. das Erkenntnis vom 16. November 2022, GZ: W274 2237056-1/8E). ...

a) Antrag auf Untersagung der relevanten Verarbeitungsvorgänge
Darüber hinaus ist über den Antrag des Beschwerdeführers, gemäß Art. 58 Abs. 2 lit. f DSGVO ein Verarbeitungsverbot gegen die Beschwerdegegner zu verhängen, abzusprechen. Aus dem Wortlaut von Art. 58 Abs. 2 lit. f DSGVO kann nicht abgeleitet werden, dass einer betroffenen Person ein subjektives Recht zukommt, dass eine Aufsichtsbehörde ein ganz konkretes Verarbeitungsverbot verhängt. ...

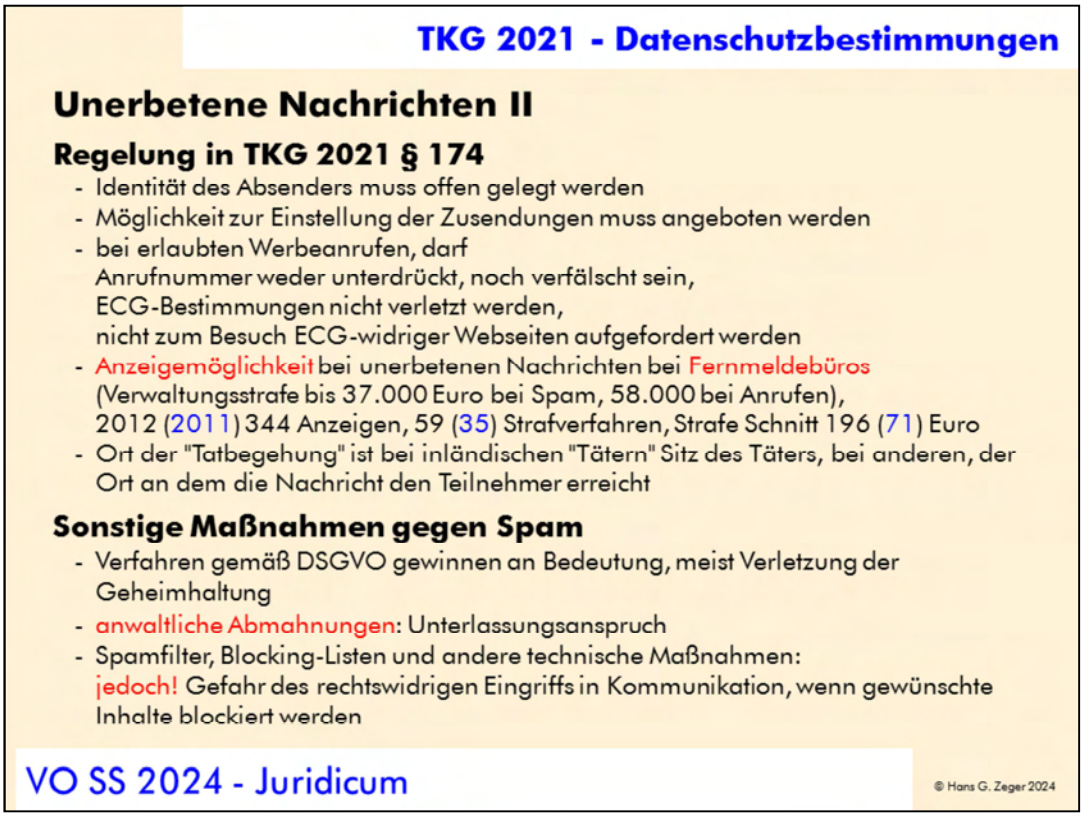
b) Antrag auf Verhängung einer Geldbuße ...
Ein subjektives Recht auf Einleitung eines Strafverfahrens gegen einen gewissen Verantwortlichen oder Auftragsverarbeiter kann aus Art. 77 Abs. 1 bzw. § 24 Abs. 1 und 5 DSG nicht abgeleitet werden.



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 2021 § 174

(1) Anrufe – einschließlich das Senden von Fernkopien – zu Werbezwecken ohne vorherige Einwilligung des Nutzers sind unzulässig. Der Einwilligung des Nutzers steht die Einwilligung einer Person, die vom Endnutzer 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.

(2) 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.

(3) Die Zusendung einer elektronischen Post – einschließlich SMS – ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt.

(4) Eine vorherige Einwilligung für die Zusendung elektronischer Post gemäß Abs. 3 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.

(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, 3 oder 5 nicht im Inland begangen, gelten sie als an jenem Ort begangen, an dem die unerbetene Nachricht den Anschluss des Nutzers erreicht.

Datensicherheitsmaßnahmen

TKG 2021 § 163. (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 Nutzer 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 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

TKG 2021 § 164. (1) Im Fall einer Verletzung des Schutzes personenbezogener Daten oder der nicht öffentlich zugänglichen Daten einer juristischen Person hat unbeschadet des § 44 sowie unbeschadet der Bestimmungen des DSG 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 (Data-Breach-Verordnung), ABl. Nr. L 173 vom 26.06.2013 S. 2, 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.

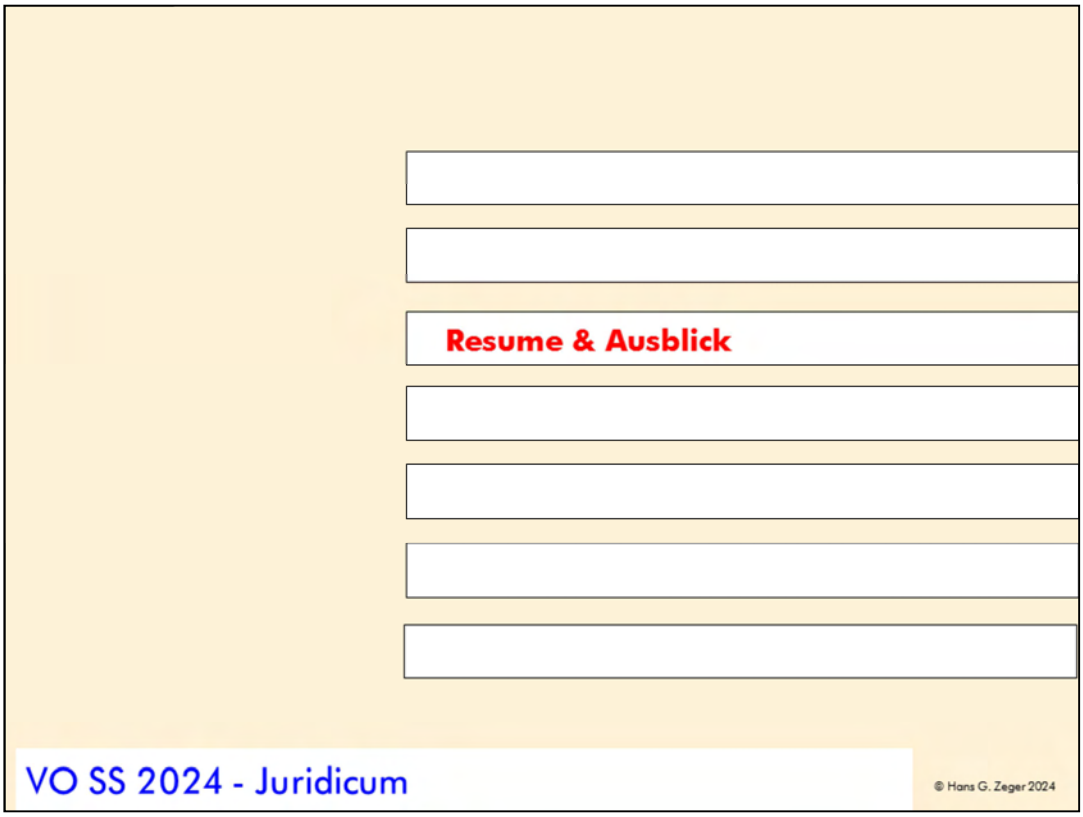
(3) Unbeschadet der Verpflichtung des Betreibers nach Abs. 1 zweiter Satz kann die Datenschutzbehörde den Betreiber öffentlicher Kommunikationsdienste – nach Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung – auch auffordern, eine Benachrichtigung durchzuführen.

(4) Der Inhalt der Benachrichtigung der betroffenen Personen hat Art. 3 der Data-Breach-Verordnung zu entsprechen.

(5) 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 oder der nicht öffentlich zugänglichen Daten einer juristischen Person 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 § 44 übertragenen Aufgaben notwendig sind.


Resume & Ausblick
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

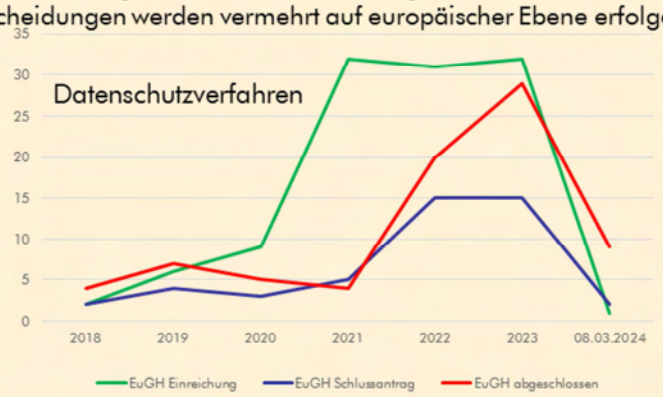
-

Datenschutz & Internet

Wohin geht die Datenschutzreise im Internet?

Status

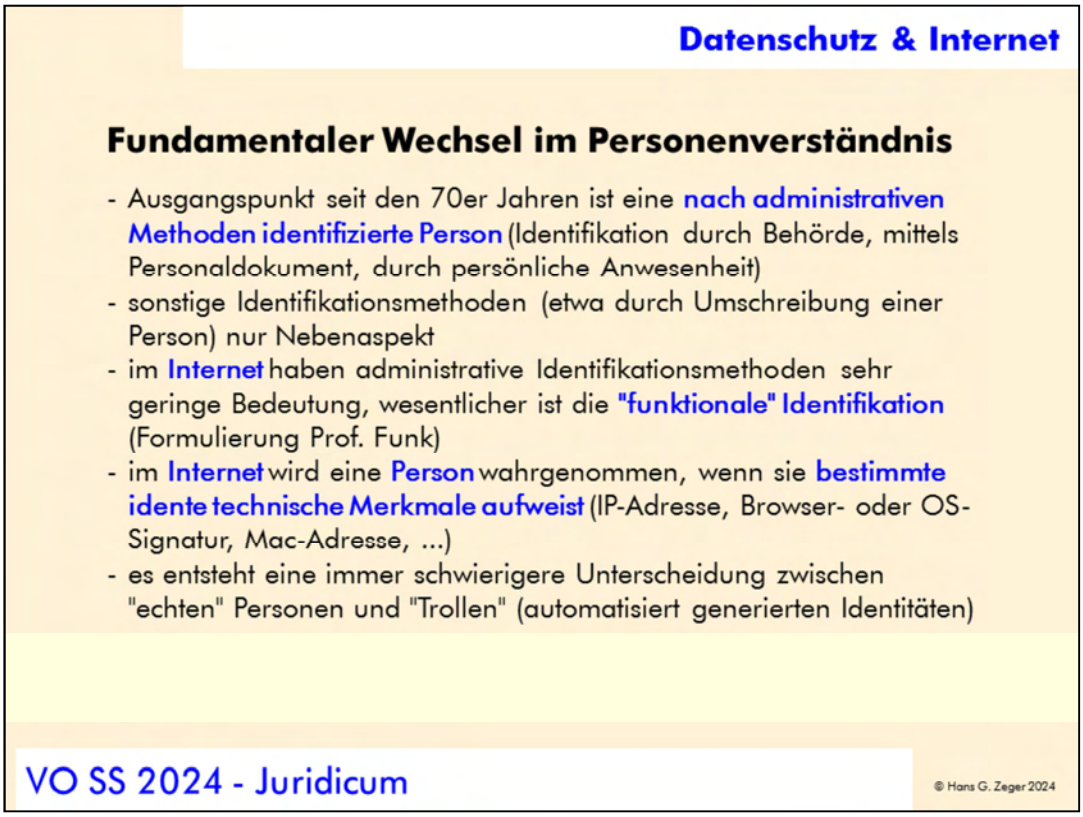
- Datenschutzfragen werden kasuistisch abgehandelt
- Entscheidungen werden vermehrt auf europäischer Ebene erfolgen



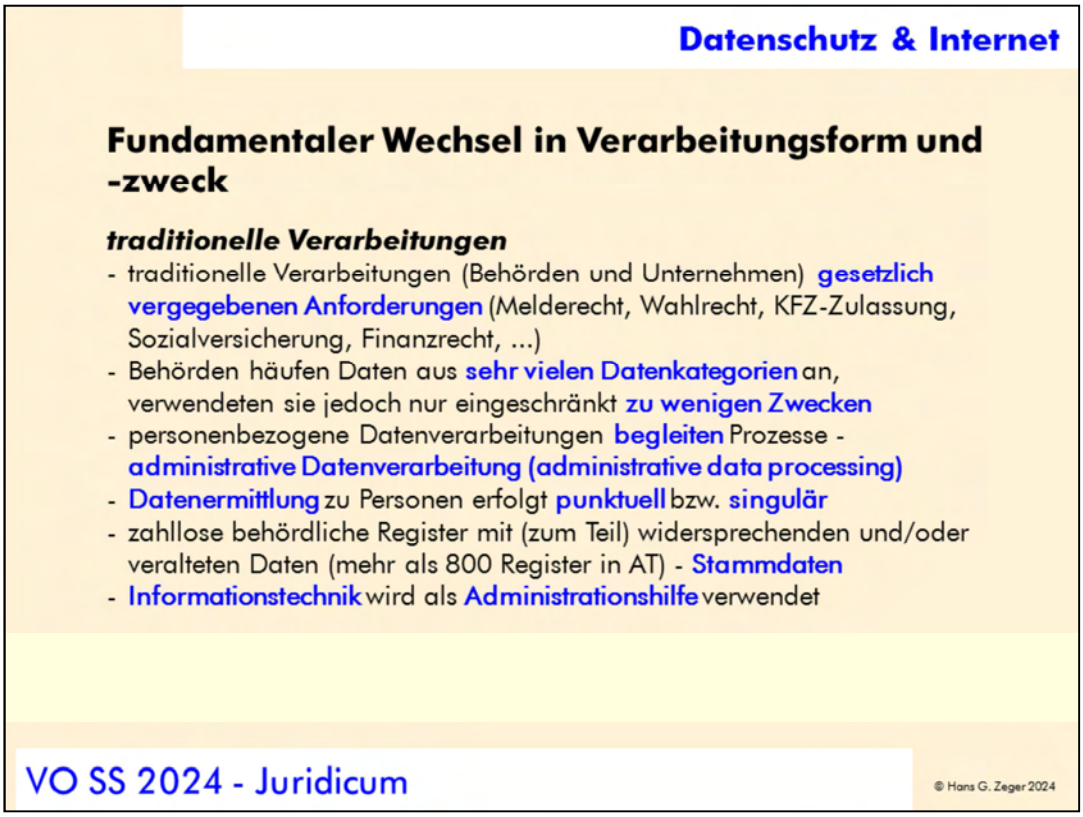
- Koordination und Zusammenarbeit der nationalen DSBs wird an Bedeutung gewinnen
- wesentliche Unterschiede zwischen klassischen Datenschutzfragen und Datenschutzfragen im Internet unterschätzt

VO SS 2024 - Juridicum

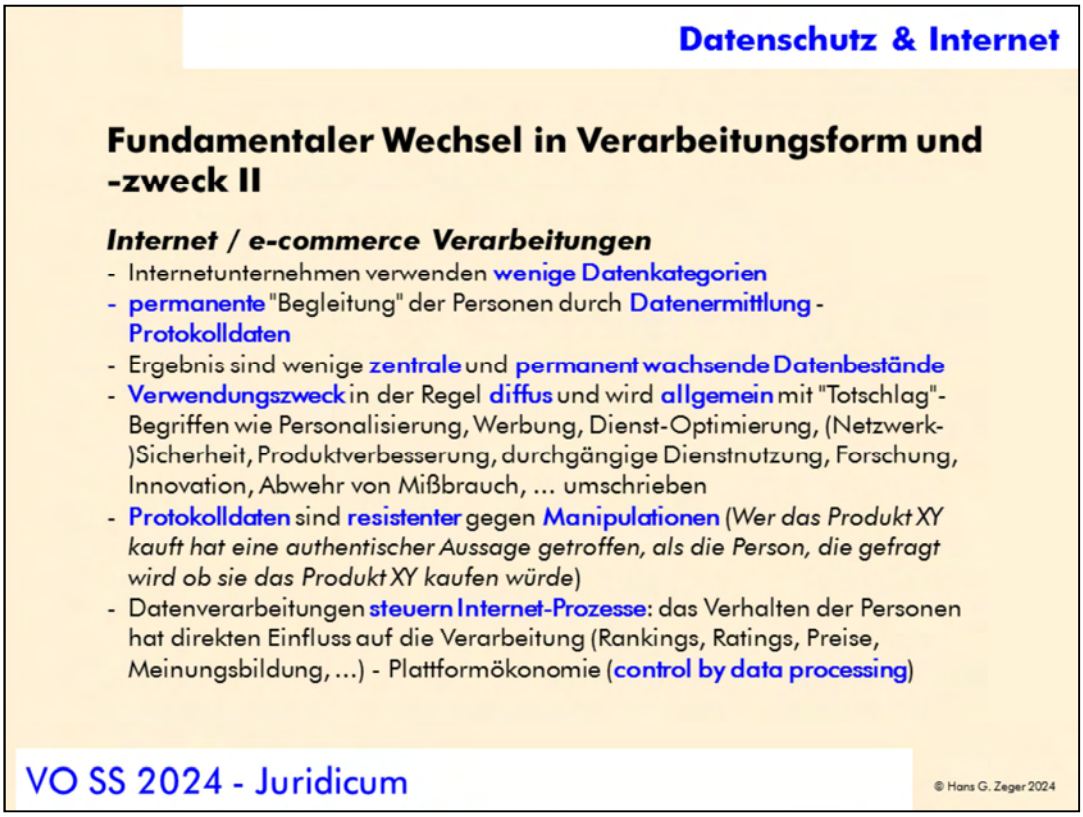
-


Datenschutz & Internet
Fundamentaler Wechsel im Personenverständnis
- Ausgangspunkt seit den 70er Jahren ist eine nach administrativen Methoden identifizierte Person (Identifikation durch Behörde, mittels Personaldokument, durch persönliche Anwesenheit)
- sonstige Identifikationsmethoden (etwa durch Umschreibung einer Person) nur Nebenaspekt
- im Internet haben administrative Identifikationsmethoden sehr geringe Bedeutung, wesentlicher ist die "funktionale" Identifikation (Formulierung Prof. Funk)
- im Internet wird eine Person wahrgenommen, wenn sie bestimmte idente technische Merkmale aufweist (IP-Adresse, Browser- oder OS-Signatur, Mac-Adresse, ...)
- es entsteht eine immer schwierigere Unterscheidung zwischen "echten" Personen und "Trollen" (automatisiert generierten Identitäten)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

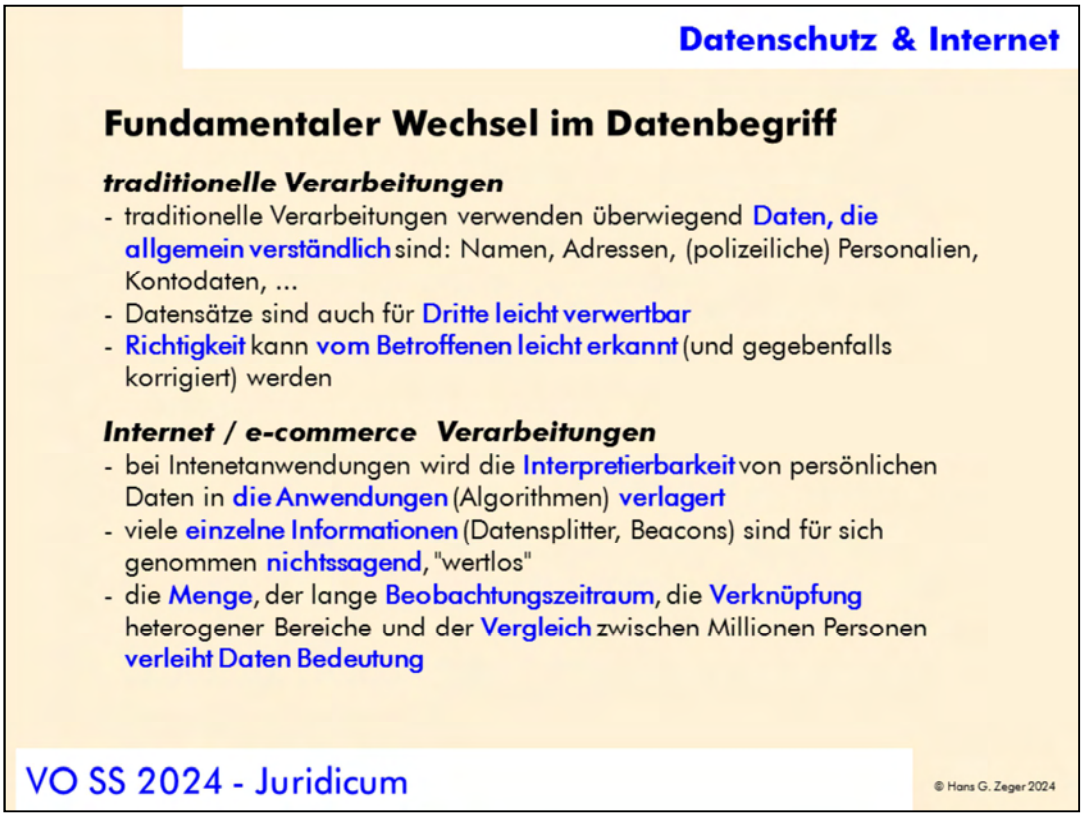
-


Datenschutz & Internet
Fundamentaler Wechsel in Verarbeitungsform und -zweck
traditionelle Verarbeitungen
- traditionelle Verarbeitungen (Behörden und Unternehmen) gesetzlich vergegebenen Anforderungen (Melderecht, Wahlrecht, KFZ-Zulassung, Sozialversicherung, Finanzrecht, ...)
- Behörden häufen Daten aus sehr vielen Datenkategorien an, verwendeten sie jedoch nur eingeschränkt zu wenigen Zwecken
- personenbezogene Datenverarbeitungen begleiten Prozesse - administrative Datenverarbeitung (administrative data processing)
- Datenermittlung zu Personen erfolgt punktuell bzw. singulär
- zahllose behördliche Register mit (zum Teil) widersprechenden und/oder veralteten Daten (mehr als 800 Register in AT) - Stammdaten
- Informationstechnik wird als Administrationshilfe verwendet
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Datenschutz & Internet
Fundamentaler Wechsel in Verarbeitungsform und -zweck II
Internet / e-commerce Verarbeitungen
- Internetunternehmen verwenden wenige Datenkategorien
- permanente "Begleitung" der Personen durch Datenermittlung - Protokolldaten
- Ergebnis sind wenige zentrale und permanent wachsende Datenbestände
- Verwendungszweck in der Regel diffus und wird allgemein mit "Totschlag"-Begriffen wie Personalisierung, Werbung, Dienst-Optimierung, (Netzwerk-)Sicherheit, Produktverbesserung, durchgängige Dienstnutzung, Forschung, Innovation, Abwehr von Mißbrauch, ... umschrieben
- Protokolldaten sind resistenter gegen Manipulationen (Wer das Produkt XY kauft hat eine authentischer Aussage getroffen, als die Person, die gefragt wird ob sie das Produkt XY kaufen würde)
- Datenverarbeitungen steuern Internet-Prozesse: das Verhalten der Personen hat direkten Einfluss auf die Verarbeitung (Rankings, Ratings, Preise, Meinungsbildung, ...) - Plattformökonomie (control by data processing)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

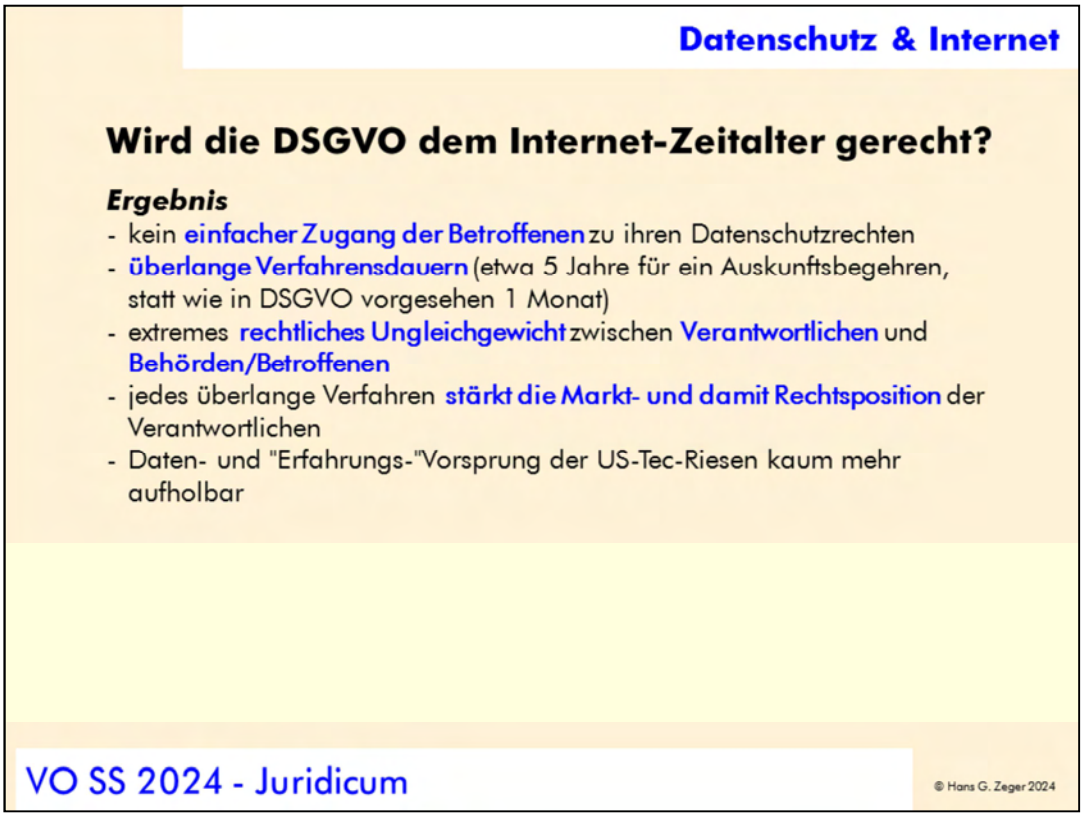
-


Datenschutz & Internet
Fundamentaler Wechsel im Datenbegriff
traditionelle Verarbeitungen
- traditionelle Verarbeitungen verwenden überwiegend Daten, die allgemein verständlich sind: Namen, Adressen, (polizeiliche) Personalien, Kontodaten, ...
- Datensätze sind auch für Dritte leicht verwertbar
- Richtigkeit kann vom Betroffenen leicht erkannt (und gegebenfalls korrigiert) werden
Internet / e-commerce Verarbeitungen
- bei Intenetanwendungen wird die Interpretierbarkeit von persönlichen Daten in die Anwendungen (Algorithmen) verlagert
- viele einzelne Informationen (Datensplitter, Beacons) sind für sich genommen nichtssagend, "wertlos"
- die Menge, der lange Beobachtungszeitraum, die Verknüpfung heterogener Bereiche und der Vergleich zwischen Millionen Personen verleiht Daten Bedeutung
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

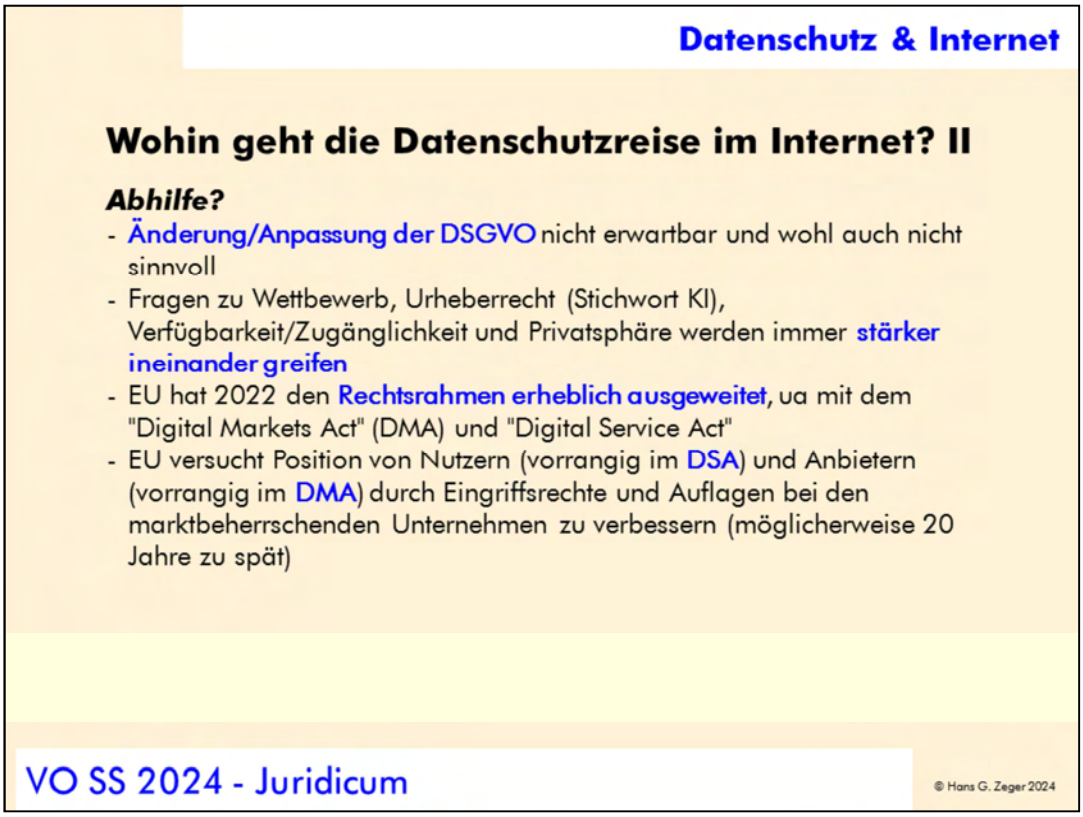
-


Datenschutz & Internet
Wird die DSGVO dem Internet-Zeitalter gerecht?
DSGVO Grundlagen
- im Kern verwendet die DSGVO die Begriffe der 70er-Jahre
- geht von einzelnen, schutzwürdigen Subjekten aus
- geht von festgefügten, klar definierten Zwecken aus
- Menge der Daten dieser Subjekte ist überschaubar, nur langsam veränderlich und jede Information für sich genommen interpretierbar
- Daten werden nach klar definierter (nationaler) Rechtslage verarbeitet
- zwischen Verantwortlichen und Betroffenen bestehen klare Rechtsbeziehungen
Wo liegen die Schwachstellen der DSGVO?
- Betroffenenrechte bei sehr großen, weit verteilten und nur kurzfristig existierenden Datenmengen de facto nicht umsetzbar
- unzureichende Eingriffsmöglichkeiten bei Verarbeitungen die erst in Verbindung mit einer großen Benutzerzahlen bedeutsam werden
- unzureichende Handhabe die Interpretierbarkeit der Daten für Betroffene sicher zu stellen
- Fokus liegt zusehr auf den Daten statt den Verarbeitungen (Algorithmen)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

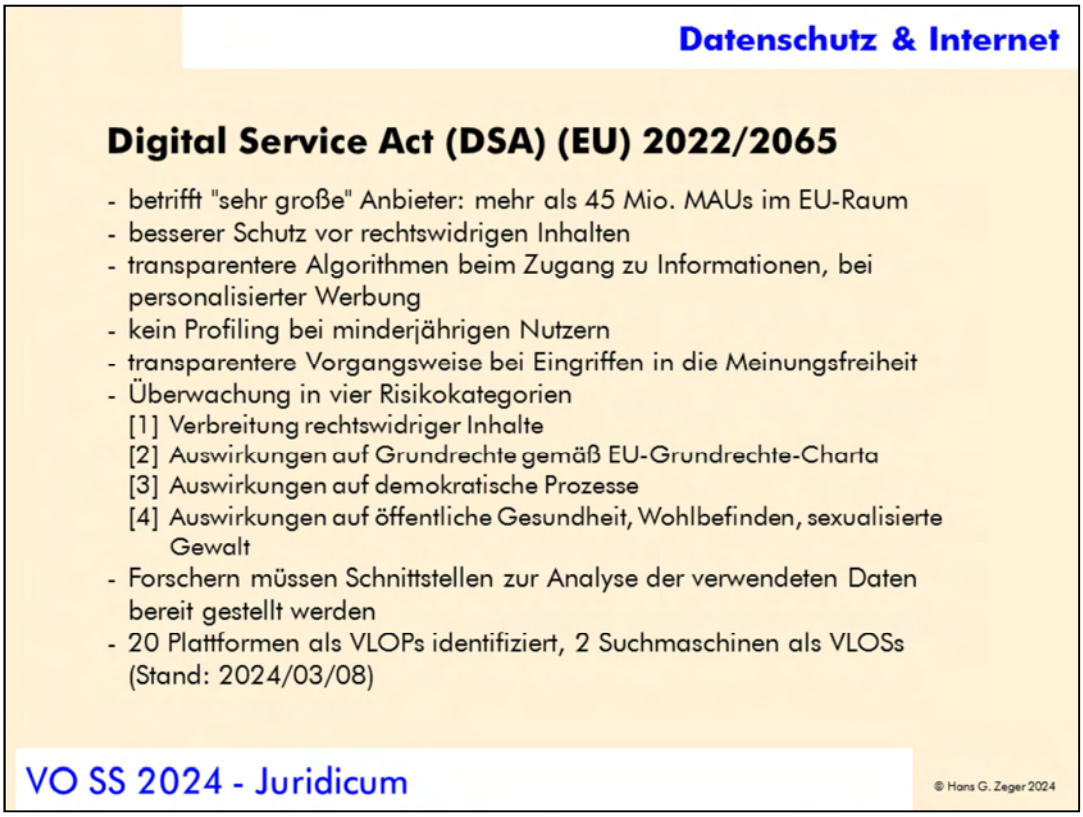
-


Datenschutz & Internet
Wird die DSGVO dem Internet-Zeitalter gerecht?
Ergebnis
- kein einfacher Zugang der Betroffenen zu ihren Datenschutzrechten
- überlange Verfahrensdauern (etwa 5 Jahre für ein Auskunftsbegehren, statt wie in DSGVO vorgesehen 1 Monat)
- extremes rechtliches Ungleichgewicht zwischen Verantwortlichen und Behörden/Betroffenen
- jedes überlange Verfahren stärkt die Markt- und damit Rechtsposition der Verantwortlichen
- Daten- und "Erfahrungs-"Vorsprung der US-Tec-Riesen kaum mehr aufholbar
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Datenschutz & Internet
Wohin geht die Datenschutzreise im Internet? II
Abhilfe?
- Änderung/Anpassung der DSGVO nicht erwartbar und wohl auch nicht sinnvoll
- Fragen zu Wettbewerb, Urheberrecht (Stichwort KI), Verfügbarkeit/Zugänglichkeit und Privatsphäre werden immer stärker ineinander greifen
- EU hat 2022 den Rechtsrahmen erheblich ausgeweitet, ua mit dem "Digital Markets Act" (DMA) und "Digital Service Act"
- EU versucht Position von Nutzern (vorrangig im DSA) und Anbietern (vorrangig im DMA) durch Eingriffsrechte und Auflagen bei den marktbeherrschenden Unternehmen zu verbessern (möglicherweise 20 Jahre zu spät)
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



Very Large Online Platforms: 25. April 2023

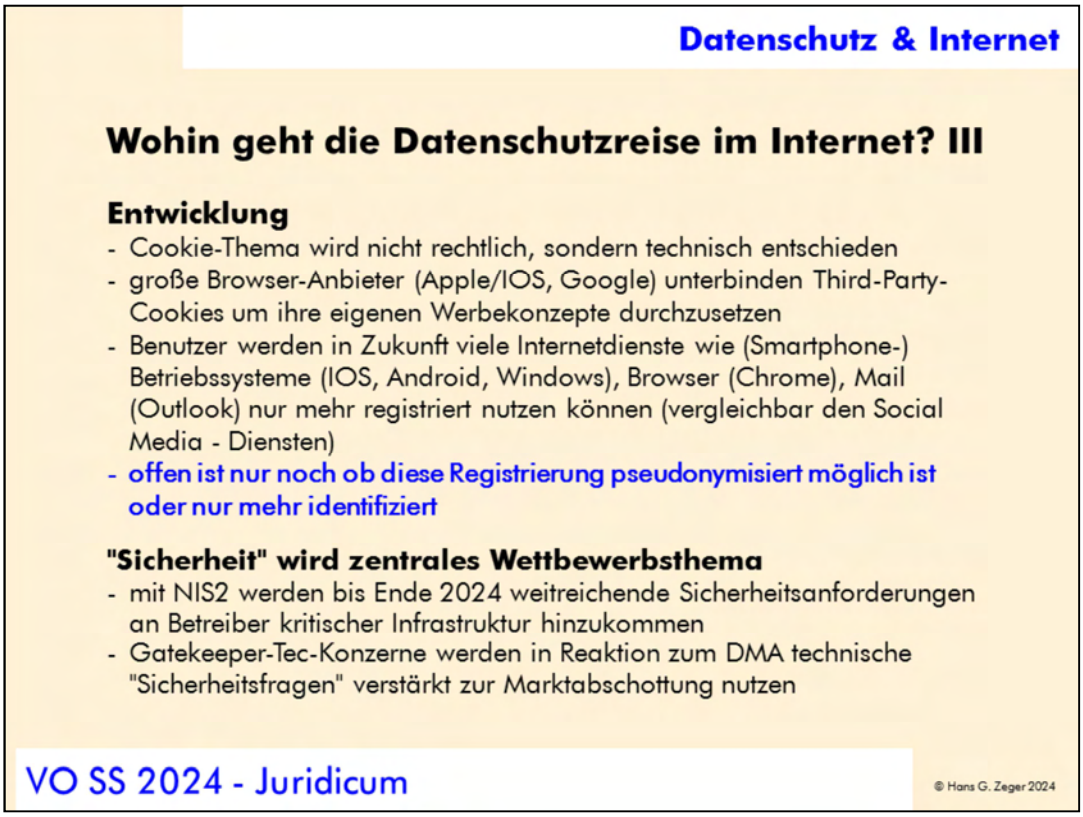
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413
Alibaba AliExpress
Amazon Store
Apple AppStore
Booking.com
Facebook
Google Play
Google Maps
Google Shopping
Instagram
LinkedIn
Pinterest
Snapchat
TikTok
Twitter
Wikipedia
YouTube
Zalando

Very Large Online Search Engines: 25. April 2023

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413
Bing
Google Search

Very Large Online Platforms: 20. Dezember 2023

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6763
Pornhub
Stripchat
XVideos


Datenschutz & Internet
Wohin geht die Datenschutzreise im Internet? III
Entwicklung
- Cookie-Thema wird nicht rechtlich, sondern technisch entschieden
- große Browser-Anbieter (Apple/IOS, Google) unterbinden Third-Party-Cookies um ihre eigenen Werbekonzepte durchzusetzen
- Benutzer werden in Zukunft viele Internetdienste wie (Smartphone-) Betriebssysteme (IOS, Android, Windows), Browser (Chrome), Mail (Outlook) nur mehr registriert nutzen können (vergleichbar den Social Media - Diensten)
- offen ist nur noch ob diese Registrierung pseudonymisiert möglich ist oder nur mehr identifiziert
"Sicherheit" wird zentrales Wettbewerbsthema
- mit NIS2 werden bis Ende 2024 weitreichende Sicherheitsanforderungen an Betreiber kritischer Infrastruktur hinzukommen
- Gatekeeper-Tec-Konzerne werden in Reaktion zum DMA technische "Sicherheitsfragen" verstärkt zur Marktabschottung nutzen
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

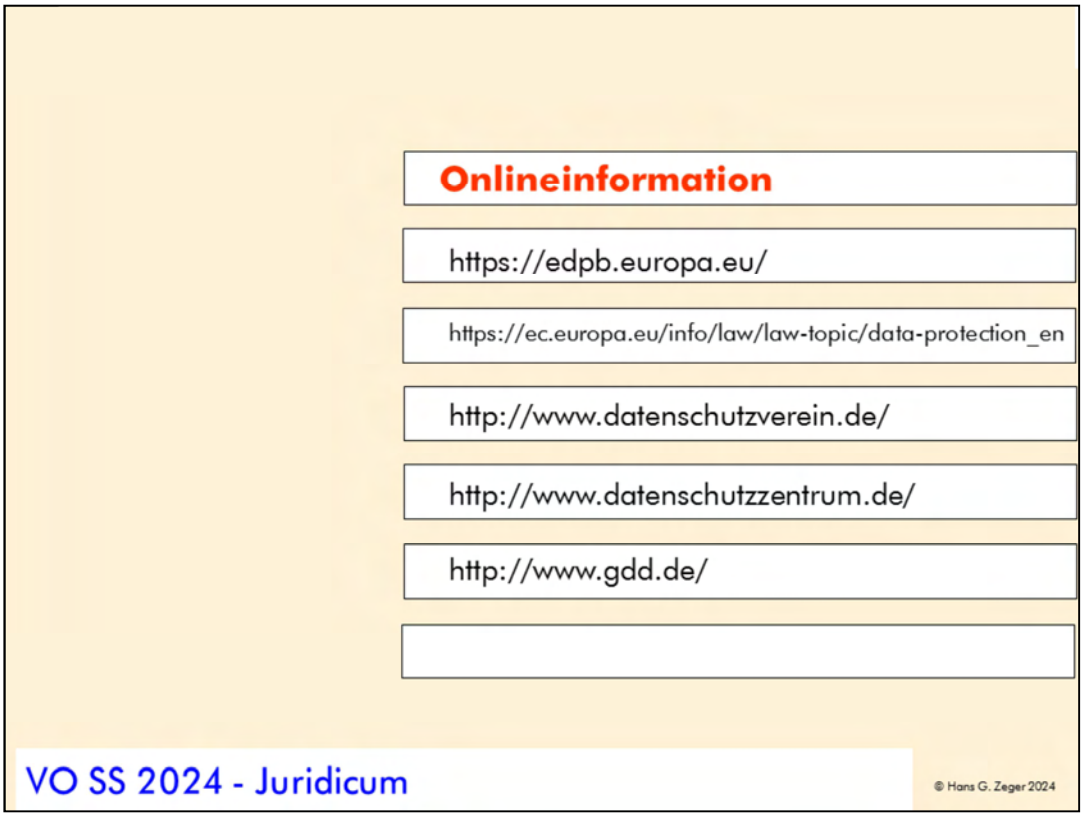
-


Ich danke für Ihre Aufmerksamkeit
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-


Kontaktinformationen
Dr. Hans G. Zeger
A-1160 Wien, Redtenbachergasse 20
Mail persönlich: hans@zeger.at
VO SS 2024 - Juridicum
© Hans G. Zeger 2024

-



Entscheidungen finden sich im RIS:

- http://www.ris.bka.gv.at/dsb/ (Datenschutzbehörde)
- http://www.ris.bka.gv.at/jus/ (OGH-Entscheidungen)

Sonstige Informationen

- Bundesamt fuer Sicherheit in der Informationstechnik (BSI) http://www.bsi.bund.de/
- EUGH http://curia.europa.eu/juris/recherche.jsf?pro=&nat=or&oqp=&dates=&lg=&language=de
- Datenschutzbehörde Österreich https://www.dsb.gv.at/bekanntmachungen
- DFN Cert http://www.cert.dfn.de/
- BITKOM DSGVO https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html