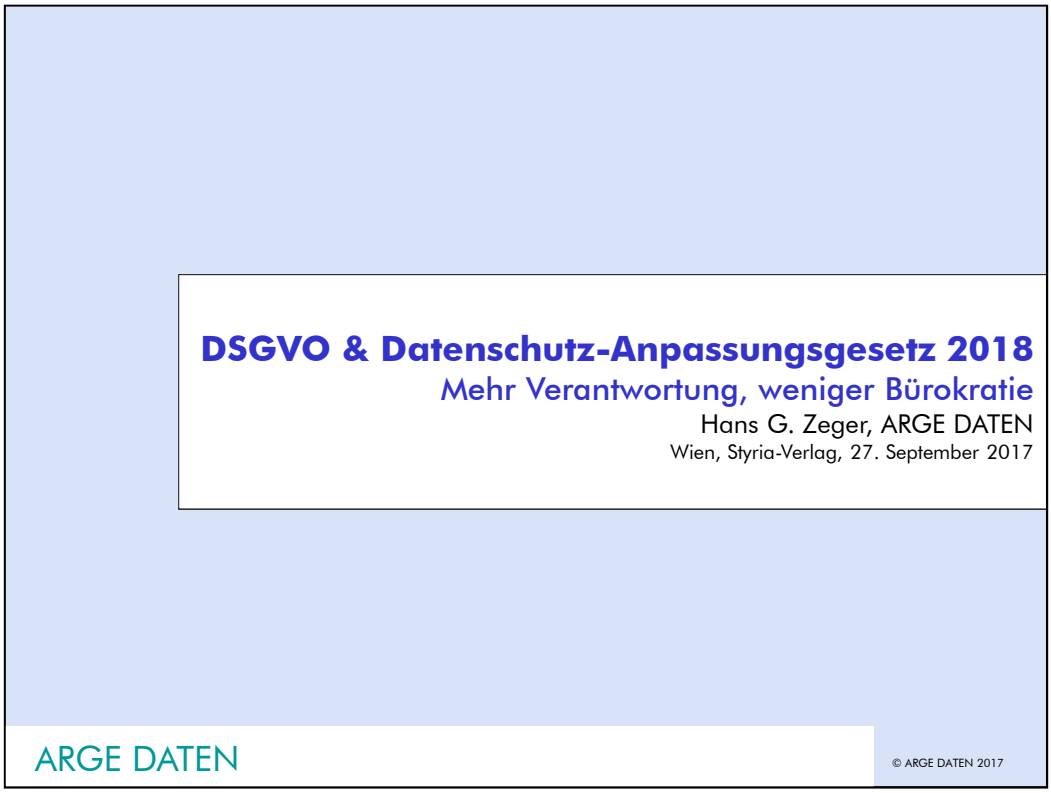


ARGE DATEN - Österreichische Gesellschaft für Datenschutz
A-1160 Wien, Redtenbachergasse 20

Tel.:	+43 0676 / 9107032
Fax.:	+43 01 / 53 20 974
Mail Verein:	info@argedaten.at
Mail persönlich:	hans.zeger@argedaten.at

WWW-Verein:	http://www.argedaten.at
Zertifizierung:	http://www.globaltrust.eu
WWW-DSG2000:	http://www.argedaten.at/dsg2000
DSG-Volltext:	ftp://ftp.freenet.at/privacy/ds-at/dsg2000-aktuell.pdf
EU DSGVO-Volltext:	ftp://ftp.freenet.at/privacy/ds-at/eu-DSGVO-aktuell.pdf
DSG-StMV:	ftp://ftp.freenet.at/privacy/ds-eu/stmv-2004.pdf
diverse Muster:	http://www.argedaten.at/muster/

Die ARGE DATEN als PRIVACY-Organisation

Aktivitäten der ARGE DATEN

Öffentlichkeitsarbeit, Informationsdienst:
- Web-Service: +80.000 Besucher/Monat
- Newsletter: rund 5.200 Abonnenten

Mitgliederbetreuung Datenschutzfragen
- 2016: ca. 500 Datenschutz-Anfragen

Rechtsschutz, PRIVACY-Services
- 2016: in ca. 80 Fällen Mitglieder in Verfahren vertreten

Studien- und Beratungsprojekte
- Sichere Tickets
- Onlinebanking
- Smartmeter
- Onlineapotheken

ARGE DATEN

Diese Datenschutzthemen bewegen die Österreicher:

- Gesundheit und Soziales:	20%	⇧
- Finanzdienstleister und Privatversicherungen/ Wirtschaftsauskunftsdienste:	17%	⇨
- Beruf / Ausbildung:	11%	⇗
- Persönliches und Privatleben:	10%	⇗
- Behörden und Verwaltung:	8%	⇨
- Konsumentendaten/Adressenverlage:	8%	⇘
- Internet und Telekombetreiber:	7%	⇘
- Bildung und Ausbildung:	4%	⇘
- sonstige Themen, wie Statistik, Politik, Herkunft, öffentliche und private Sicherheit:	15%	⇗

Ausgewertet wurden rund 500 Datenschutzfälle der letzten fünf Jahre
⇧,⇗,⇨,⇘,⇩: Tendenzangaben, Entwicklungen gegenüber Vorjahre

(Statistik F-6a, Stand Dezember 2016)


Geplanter Ablauf
Überblick DSGVO / DSAG 2018
DSGVO Neukonzeption Datenschutz
Datenschutz Management
DSAG 2018 Österreichs Lösungen
sonstige Spezial-Regelungen
ToDo für Österreichs Betriebe
ARGE DATEN
© ARGE DATEN 2017

-

Entwicklung des Datenschutzes in Österreich

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

Änderungen zum DSG 2000

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

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

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

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

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

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

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

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

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

EU Datenschutz-Grundverordnung

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

EU-Neuregelung des Datenschutzes

Fahrplan zur EU DSGVO

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

ARGE DATEN

Informationen zur weiteren Entwicklung der EU-Verordnung:

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

EU-Neuregelung des Datenschutzes

Was ist die Datenschutz-Grundverordnung?

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

ARGE DATEN

-

DSGVO Grundlagen

Eckpfeiler der neuen DSGVO

- verpflichtender Datenschutzbeauftragter (Art. 37)
  - ✓ alle öffentlichen Einrichtungen
  - ✓ Kerntätigkeit erfordert umfangreiche regelmäßige und systematische Beobachtung der Betroffenen
  - ✓ Kerntätigkeit ist die Verarbeitung besonderer Kategorien von Daten
  - ✓ Kerntätigkeit ist die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten
- 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

ARGE DATEN

-

DSGVO Grundlagen

Eckpfeiler der neuen DSGVO II

- 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
- 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

ARGE DATEN

-

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 "Vergessenwerden": Löschen + Verständigungspflicht (Art. 17 + 19)
  ✓ Förderung technischer Datenschutzmaßnahmen ("data protection by design") (EW 61)
  ✓ Privatsphäreeinstellungen sollen Standard werden ("data protection by default") (EW 61)
- neue "besondere Kategorien" von Daten (Art. 9)
  ✓ genetische Daten, biometrische Daten

ARGE DATEN

-

Datenschutz-Anpassungsgesetz DSAG 2018

DSAG 2018 Aufbau

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

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

ARGE DATEN

-

DSGVO - Grundlagen

EU-Verordnung DSGVO (2016)

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

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

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

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

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

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

ARGE DATEN

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)

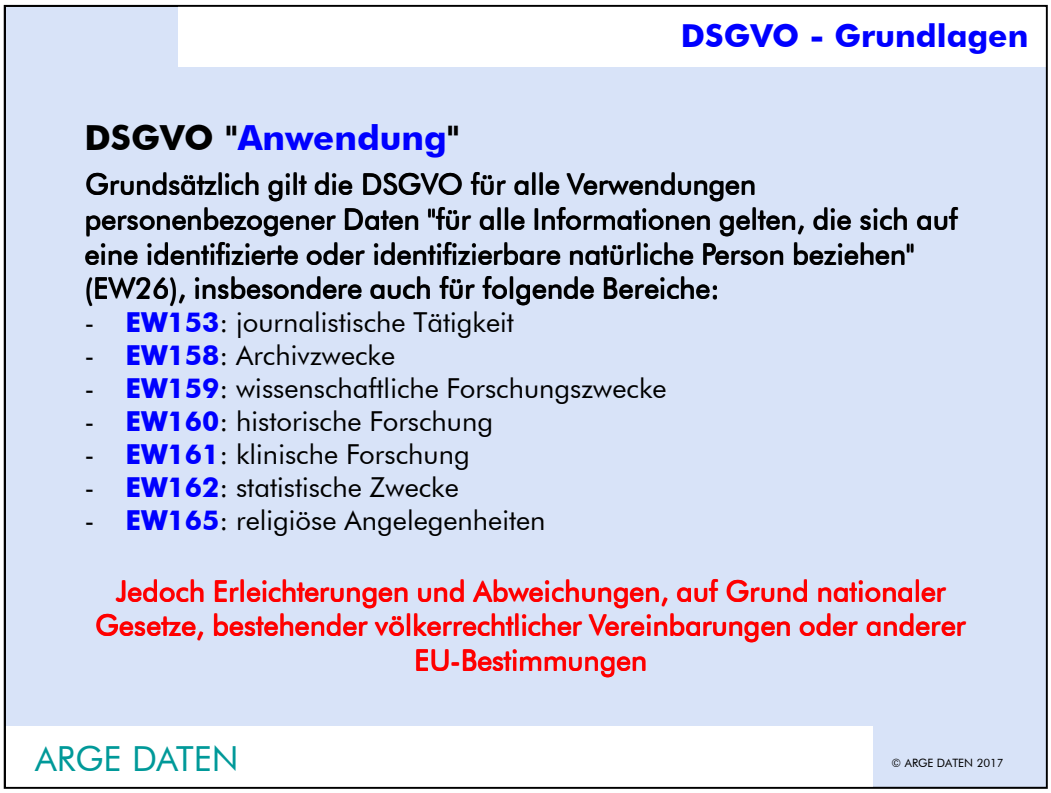
Die Richtlinie soll gleichermaßen den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung
personenbezogener Daten und den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten sichern

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 - Grundlagen

DSGVO Art. 2 Abs. 2 "Keine Anwendung"

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

weiters keine Anwendung:

- Verstorbene (EW27, EW160)

ARGE DATEN

DSGVO Art. 2 Sachlicher Anwendungsbereich

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

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

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

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

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

DSGVO EW27

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

DSGVO EW160

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

DSGVO Art. 3 Räumlicher Anwendungsbereich

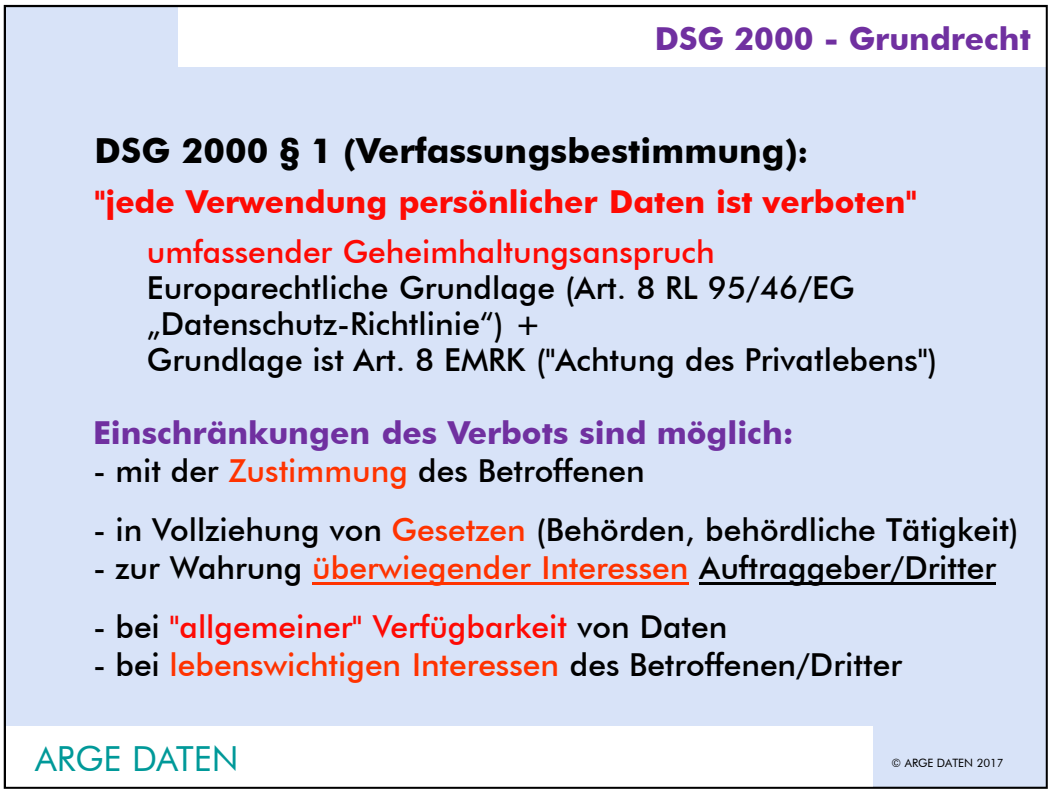
(2)Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

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.


Geplanter Ablauf
Überblick DSGVO / DSAG 2018
DSGVO Neukonzeption Datenschutz
Datenschutz Management
DSAG 2018 Österreichs Lösungen
sonstige Spezial-Regelungen
ToDo für Österreichs Betriebe
ARGE DATEN
© ARGE DATEN 2017

-



DSG 2000 § 1 Verfassungsbestimmung

"(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."

Einschränkung dieser Rechte nur mit Zustimmung des Betroffenen, zur Wahrung lebenswichtiger Interessen des Betroffenen oder laut Art. 8 Abs. 2 der europäischen Menschenrechtskonvention aufgrund von Gesetzen.

Weitere Verarbeitungsbeschränkungen für den öffentlichen Bereich ("Wahrung wichtiger öffentlicher Interessen") bei "besonders schutzwürdigen Daten" ("sensible Daten")

Festlegung der subjektiven Rechte: Auskunfts-, Richtigstellungs- und Löschungsrecht

Festlegung der Rechtsdurchsetzung / Zivilrechtsweg

Datenschutzkonzept neu

Neu

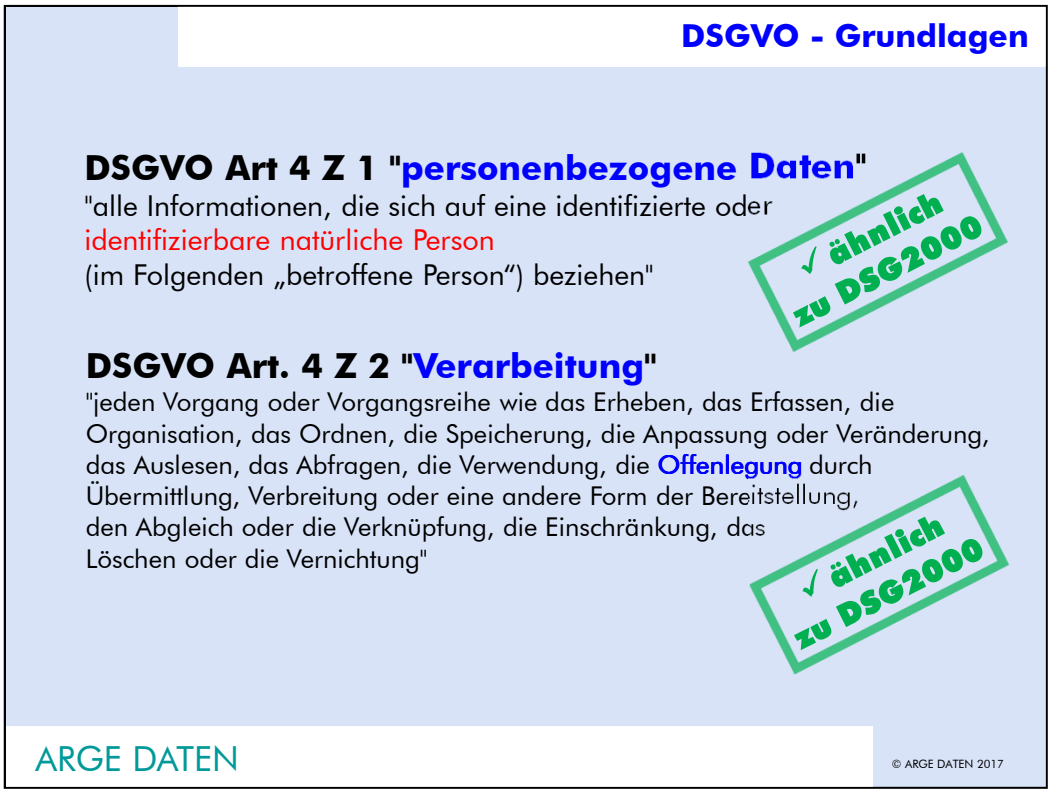
Datenschutz wird von den Betrieben eingehalten, wenn
[a] den umfangreichen internen Dokumnetationspflichten nachgekommen wird,
[b] die Risken der Datenverarbeitung korrekt bewertet werden
[c] sich Betroffene nicht beschweren
[d] die Datenschutzbehörde auf den Betrieb nicht aufmerksam wird

Damit wird Datenschutz zu einer permanenten Herausforderung, jede Lösung ist nur vorläufig gültig - zurücklehnen ist, auch angesichts der hohen Strafdrohung, nicht mehr möglich

Weniger Bürokratie wird durch mehr Verantwortung und mehr Unsicherheit im Einzelfall ersetzt

ARGE DATEN

-



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 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;

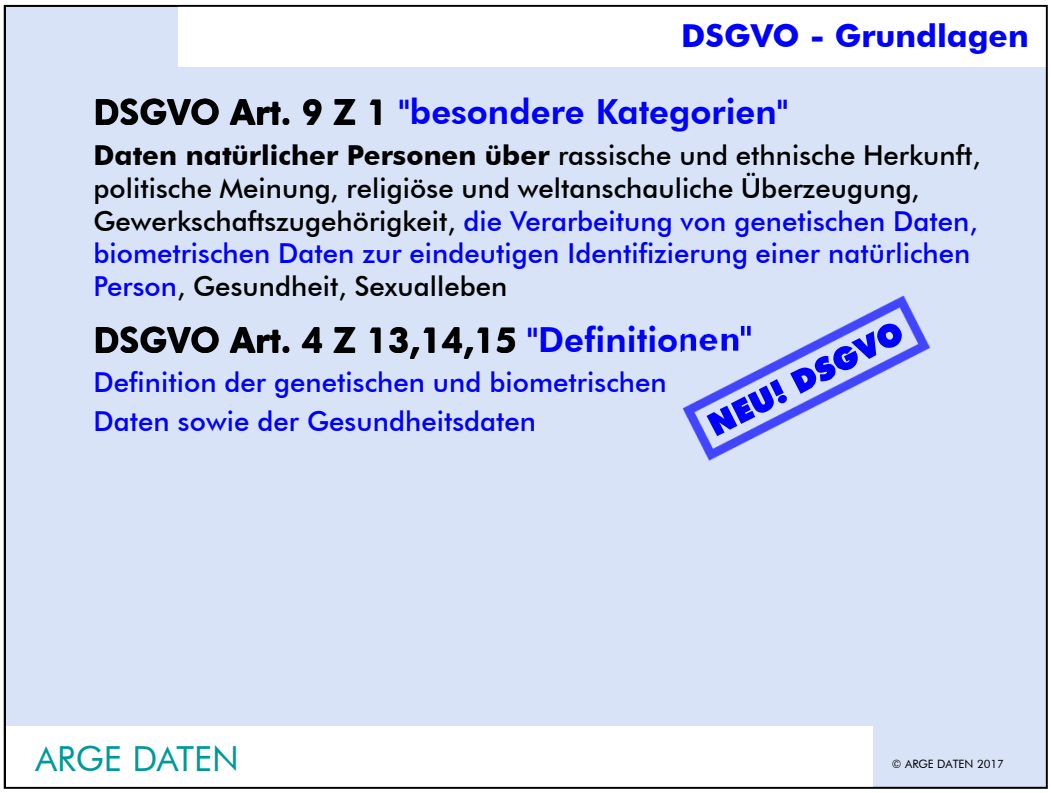
8.„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

DSG 2000 § 4 Z 4 "Auftraggeber"

4. "Auftraggeber": natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, **Daten zu verwenden** (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. **Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt** oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;"

DSG 2000 § 4 Z 5 "Dienstleister"

„5. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie **Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden** (Z 8);“



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

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

DSGVO Art. 4 Begriffsbestimmungen

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

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

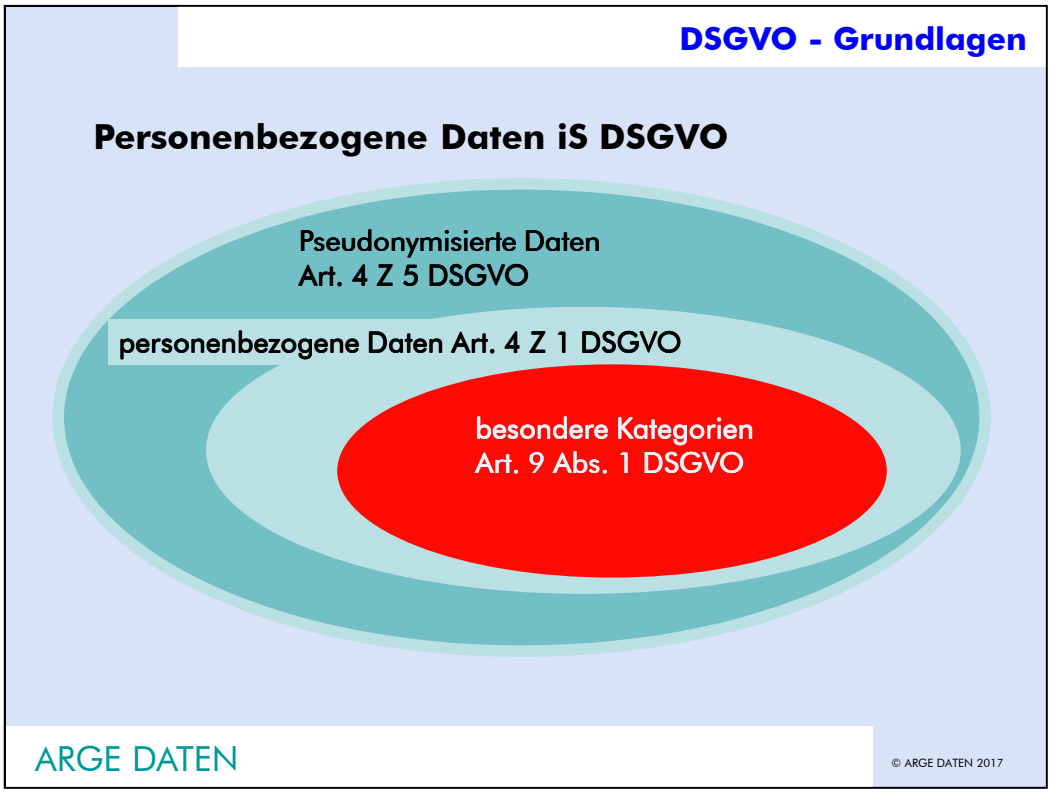
15. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

DSGVO Art. 4 Begriffsbestimmungen

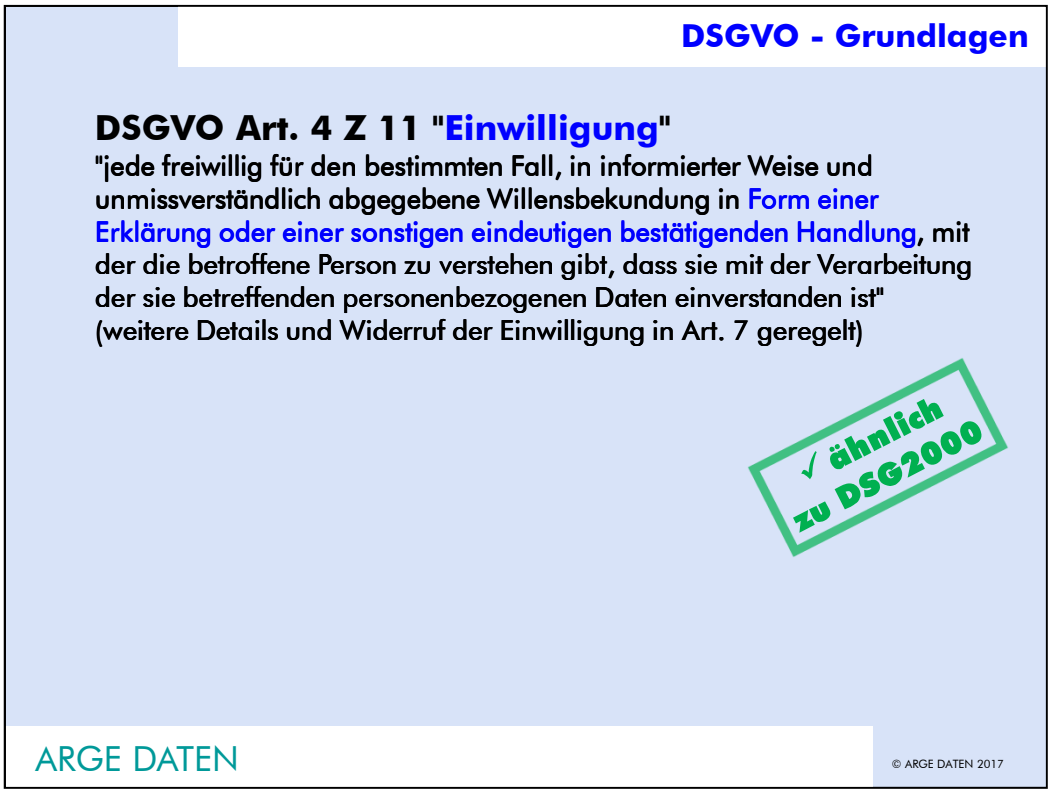
3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

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

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

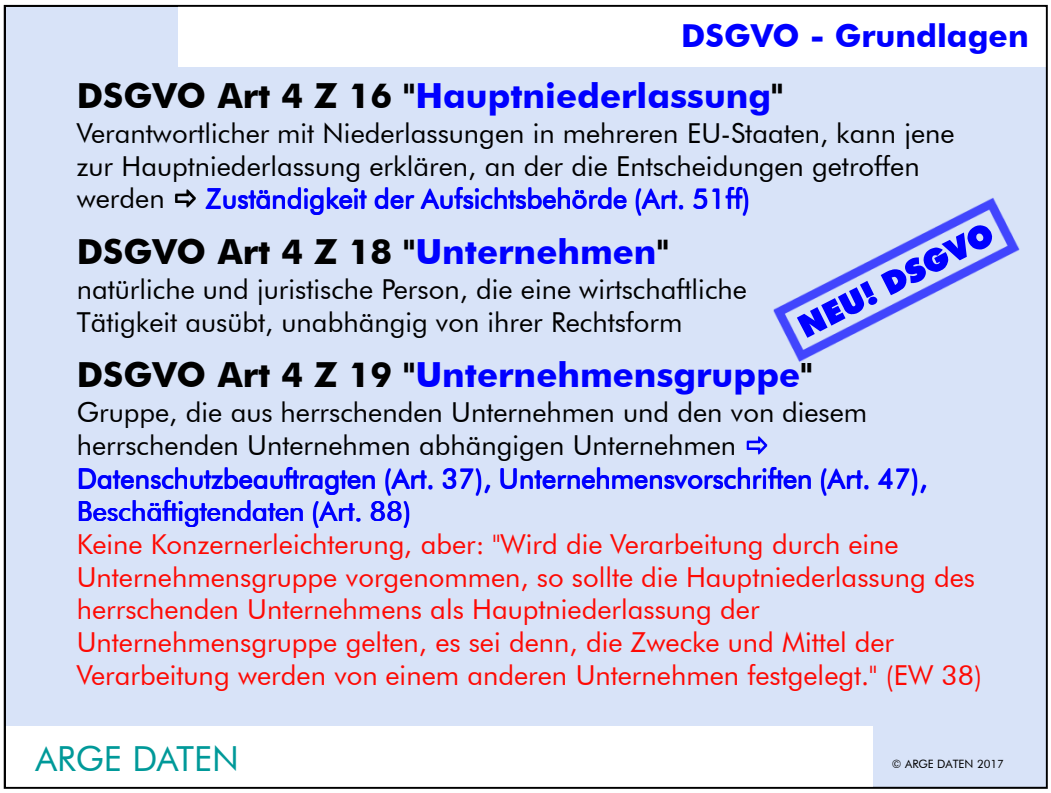

DSGVO - Grundlagen
Personenbezogene Daten iS DSGVO
Pseudonymisierte Daten
Art. 4 Z 5 DSGVO
personenbezogene Daten Art. 4 Z 1 DSGVO
besondere Kategorien
Art. 9 Abs. 1 DSGVO
ARGE DATEN
© ARGE DATEN 2017

-



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“

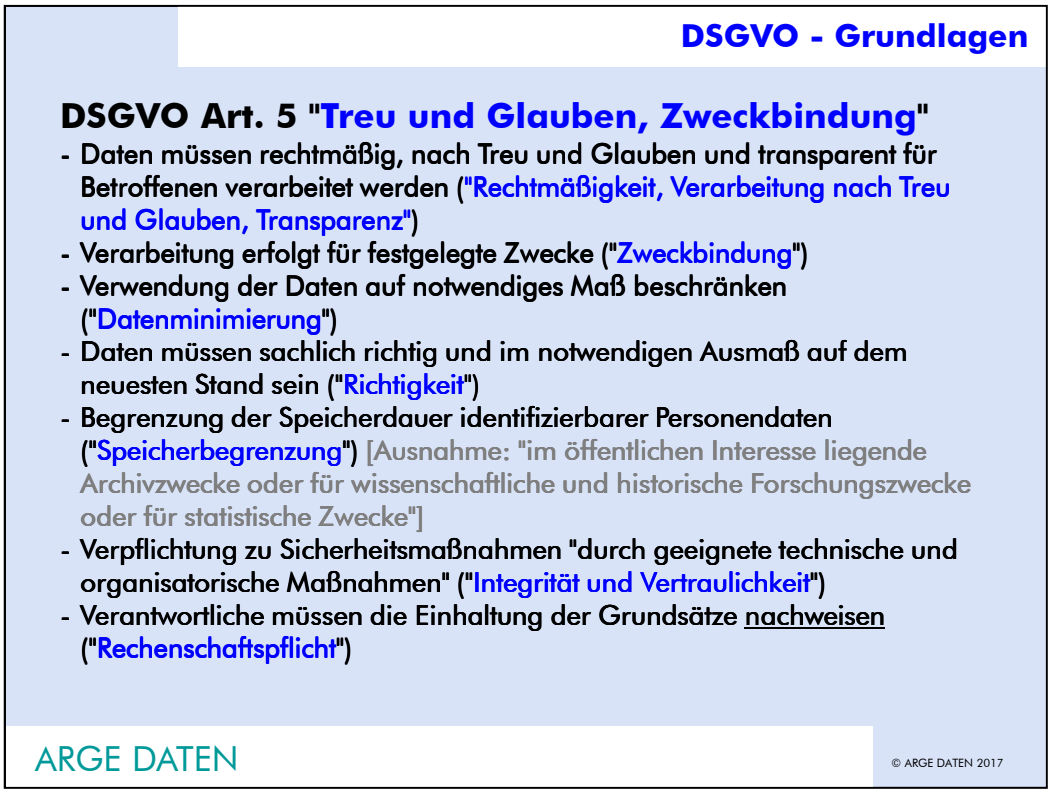
a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in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

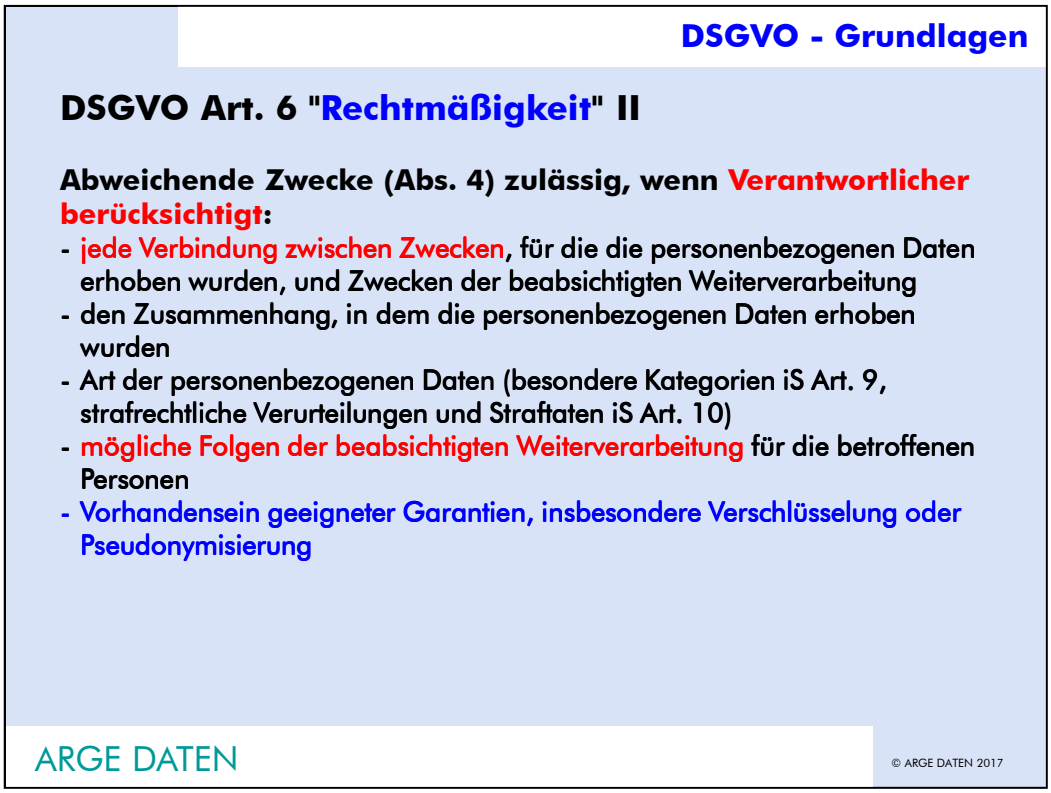
Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(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.

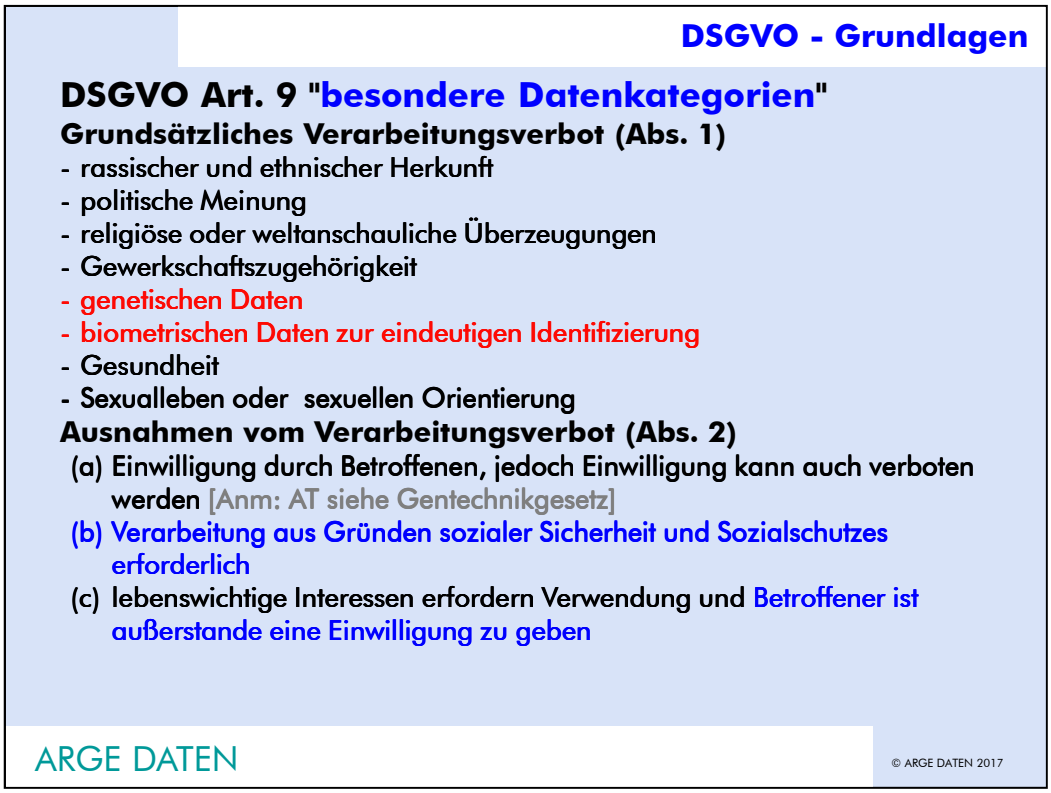
(4)Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige 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.



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.

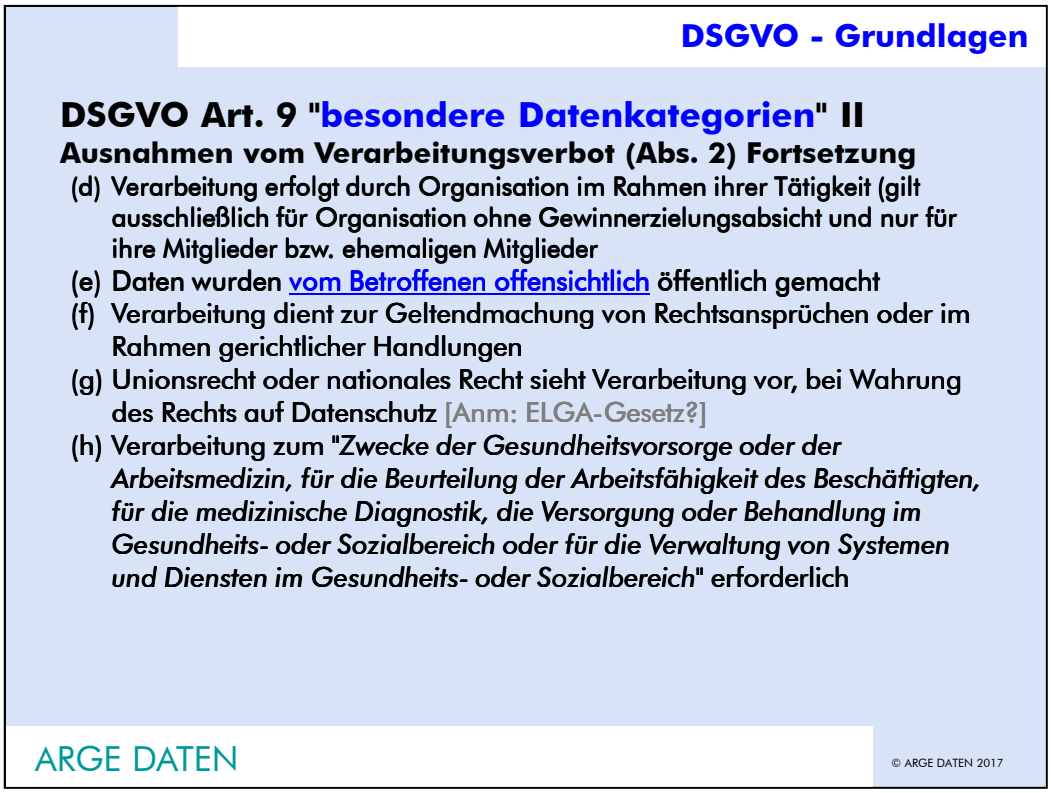
(2)Absatz 1 gilt nicht in folgenden Fällen:

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)

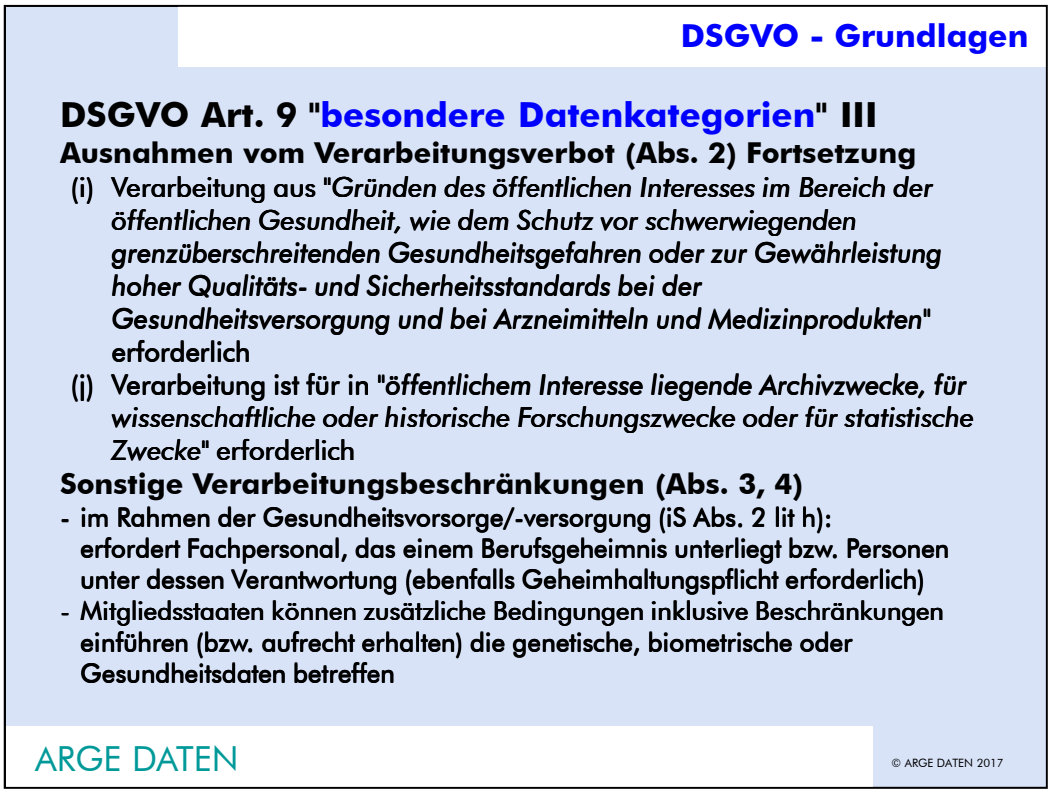
e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

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.

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.

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

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

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

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

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

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

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

DSGVO Art. 26 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 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.

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.


Geplanter Ablauf
Überblick DSGVO / DSAG 2018
DSGVO Neukonzeption Datenschutz
Datenschutz Management
DSAG 2018 Österreichs Lösungen
sonstige Spezial-Regelungen
ToDo für Österreichs Betriebe
ARGE DATEN
© ARGE DATEN 2017

-

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.

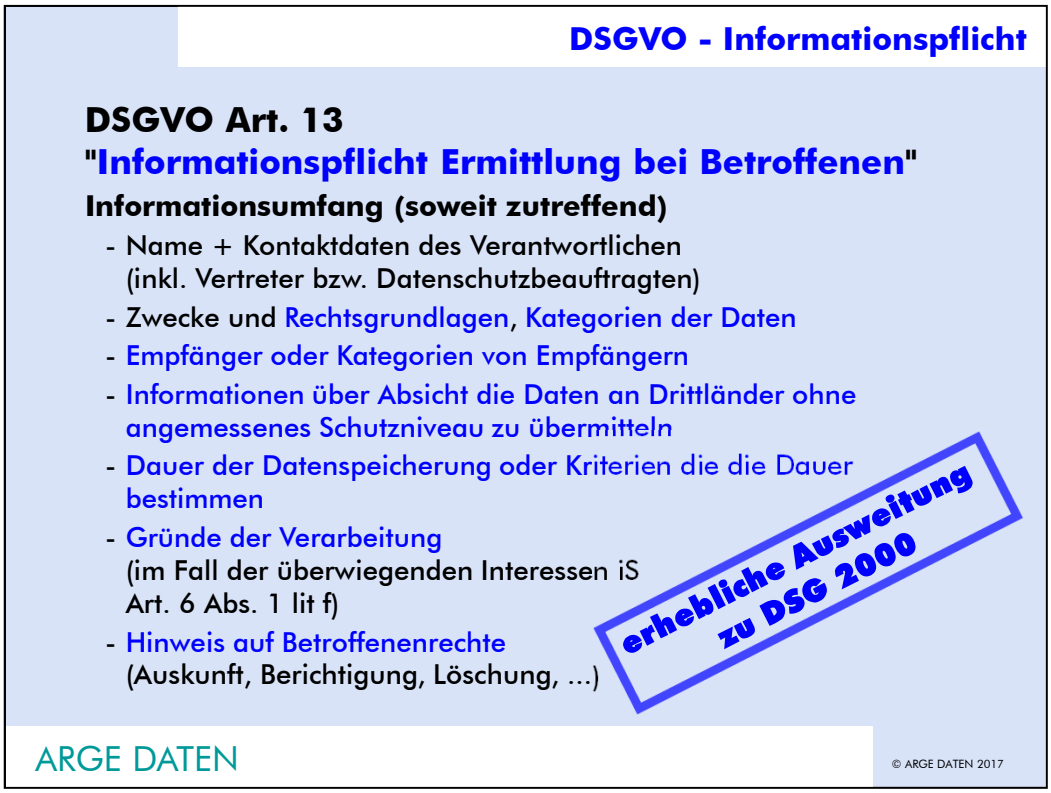
(4)Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen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

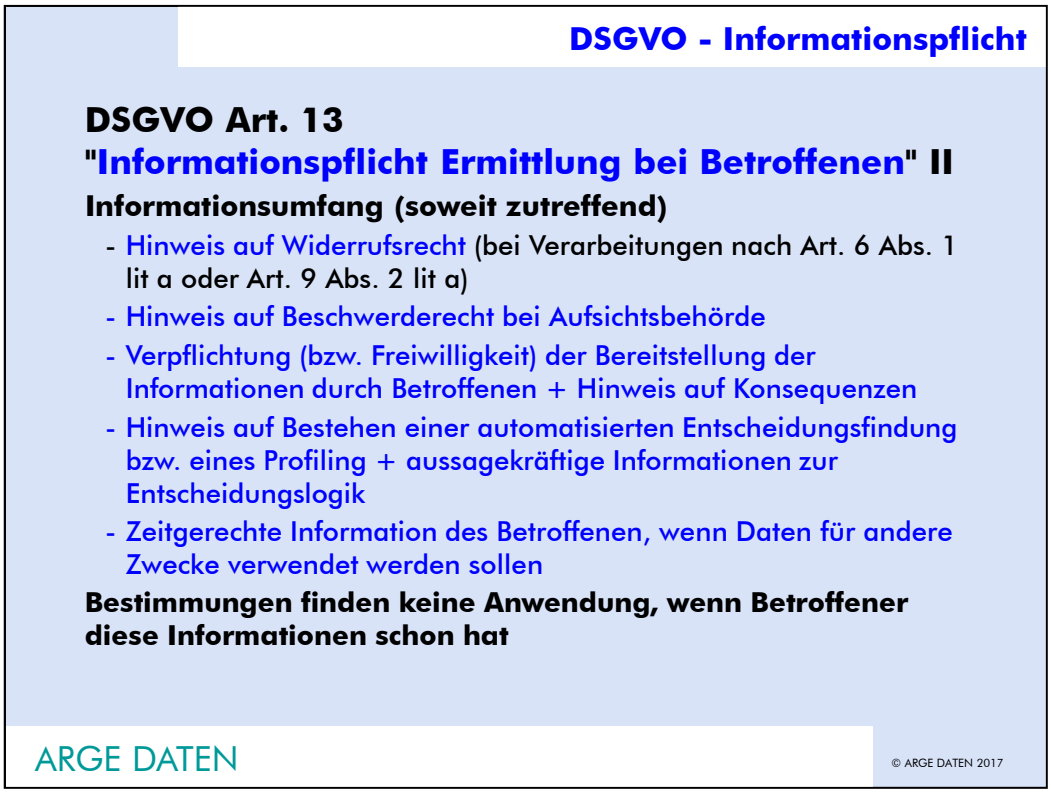
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

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:

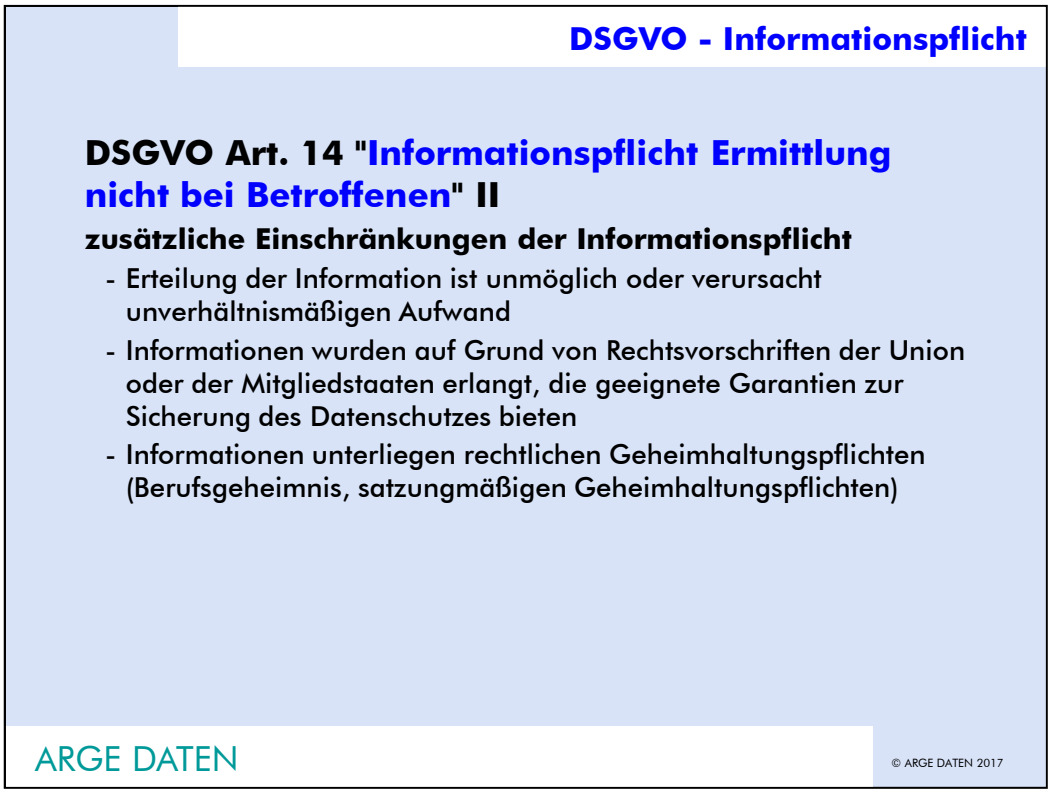
a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

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;

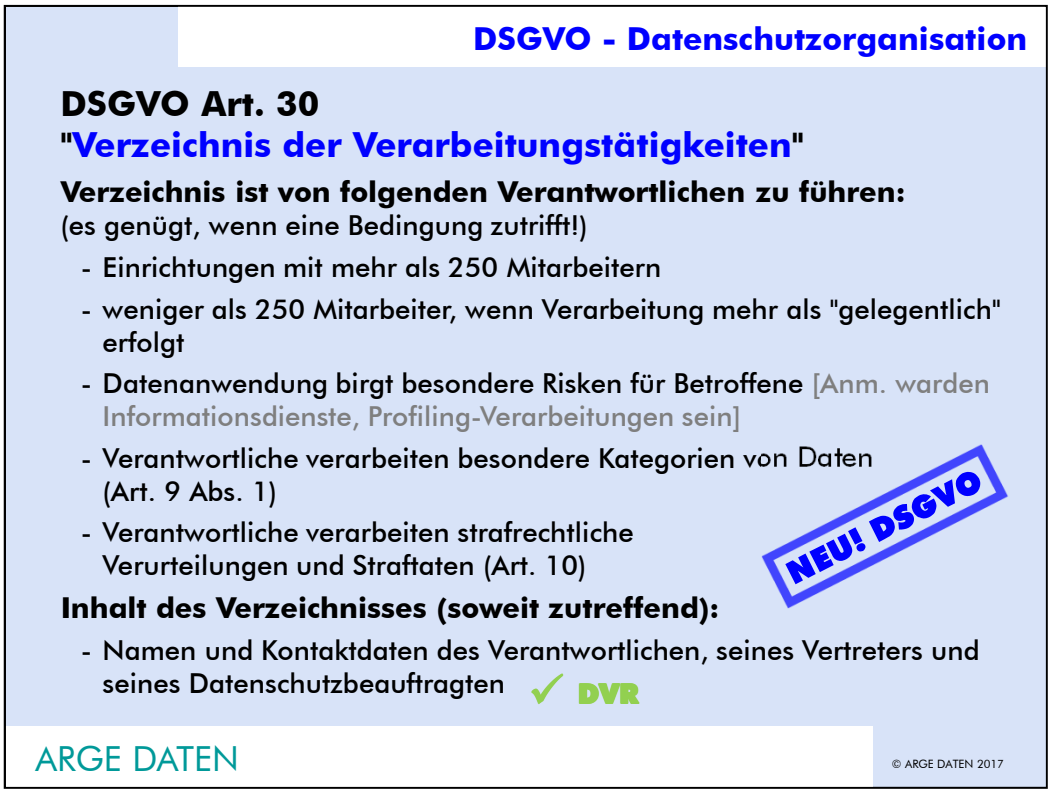
b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

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

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



DSGVO Art. 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;

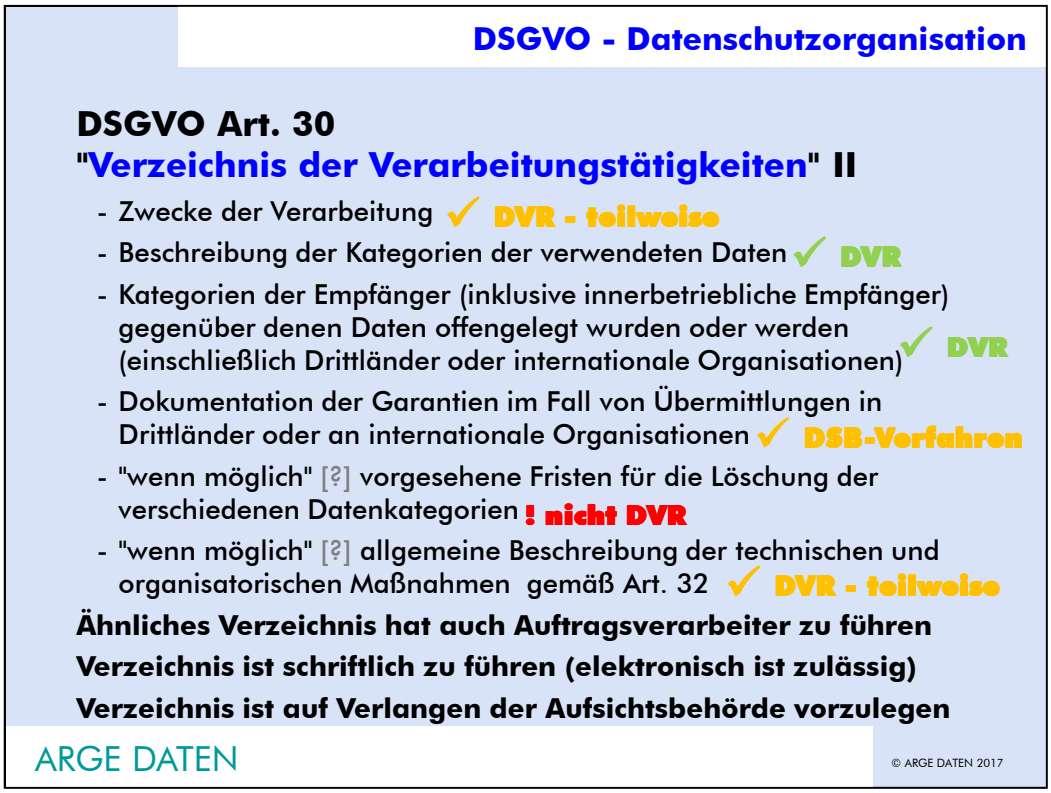
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

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

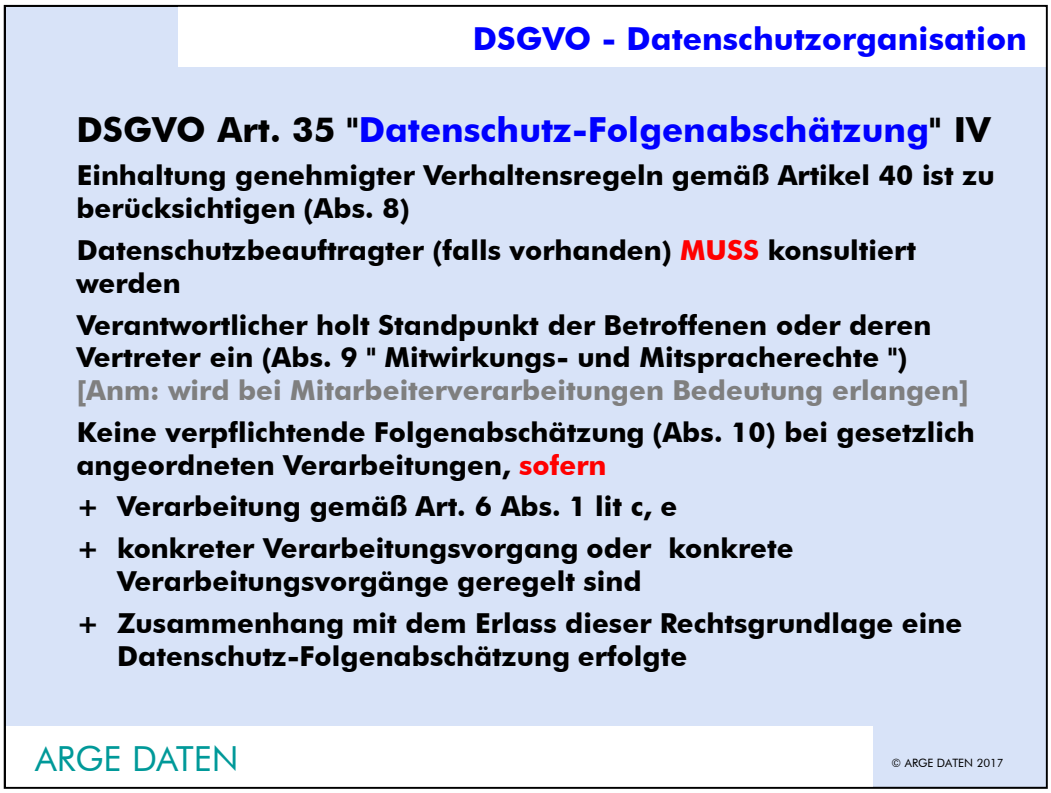
Listen müssen im "Kohärenzverfahren" mit den anderen EU-Staaten abgestimmt werden

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

ARGE DATEN

-



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**

ARGE DATEN

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Erforderlichkeit II

- **systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche**
  Videoüberwachung
  Kundentracking
  Mitarbeitertracking (etwa bei Fuhrpark, ...)
- **sonstige Risiken**

ARGE DATEN

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Schäden

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

fehlerhafte Datenverarbeitungen führen zu:

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

ARGE DATEN

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, ...)*

ARGE DATEN

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Schadensklassen I

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

ARGE DATEN

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Schadensklassen III

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

ARGE DATEN

-

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

ARGE DATEN

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Risikomatrix

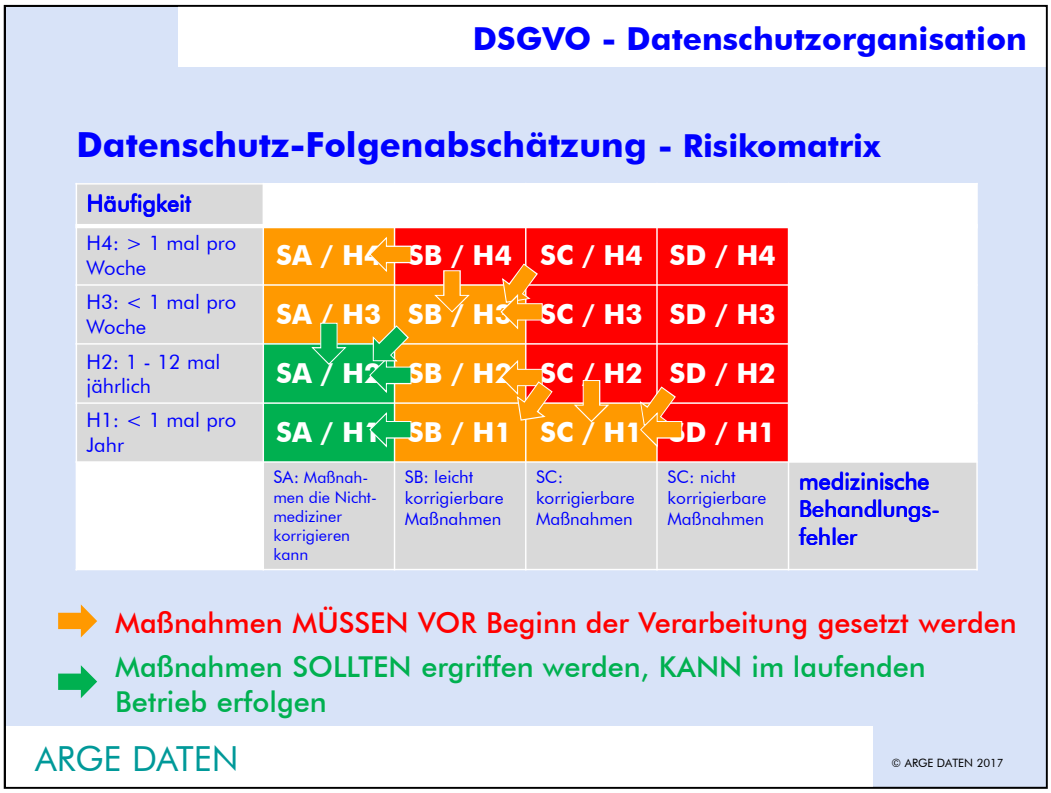
Häufigkeit					
H4: > 1 mal pro Woche	SA / H4	SB / H4	SC / H4	SD / H4	
H3: < 1 mal pro Woche	SA / H3	SB / H3	SC / H3	SD / H3	
H2: 1 - 12 mal jährlich	SA / H2	SB / H2	SC / H2	SD / H2	
H1: < 1 mal pro Jahr	SA / H1	SB / H1	SC / H1	SD / H1	
	SA: < 100 Euro	SB: 100 bis 1.000,- Euro	SC: 1.000 - 100.000,- Euro	SC: > 100.000 Euro bzw. nicht bezifferbar	**Finanzieller Schaden für Betroffenen**

➡ Maßnahmen MÜSSEN VOR Beginn der Verarbeitung gesetzt werden

➡ Maßnahmen SOLLTEN ergriffen werden, KANN im laufenden Betrieb erfolgen

ARGE DATEN

-


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
SB / H1
SC / H1
SA: Maßnahmen die Nichtmediziner korrigieren kann
SB: leicht korrigierbare Maßnahmen
SC: korrigierbare Maßnahmen
SC: nicht korrigierbare Maßnahmen
medizinische Behandlungsfehler
Maßnahmen MÜSSEN VOR Beginn der Verarbeitung gesetzt werden
Maßnahmen SOLLTEN ergriffen werden, KANN im laufenden Betrieb erfolgen
ARGE DATEN
© ARGE DATEN 2017

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Auslöser

- ☐ **Betriebsinterner unberechtigter Zugriff**
- ☐ **Unberechtigter Zugriff durch Dritte**
- ☐ **Veröffentlichung von Daten**
- ☐ **Fehlerhafte Etikettierung**
- ☐ **Fehlerhafter Restoremechanismus**
- ☐ **Unbeabsichtigtes Löschen von Daten**
- ☐ **Fehlerhafte Datenerfassung**
- ☐ **Fehlerhafte Datenkorrektur**
- ☐ **Fehlerhaftes Berechnungsverfahren**
- ☐ **Fehlerhafte Auswertung**

ARGE DATEN

-

DSGVO - Datenschutzorganisation

Datenschutz-Folgenabschätzung - Fallbeispiel

- **Verarbeitung:** Kreditvergabe
- **Verarbeitungsschritt:** Online-Kreditantrag
- **Auslöser:** Fehlerhafte/unvollständige Datenerfassung
- **Schadensklasse:** Mehrkosten Kredit / Kreditablehnung

Potentielle Bedrohung	Basis Eintrittshäufigkeit und Schadenshöhe je Ereignis	getroffene Maßnahmen	Behandlung Restrisiko
Mögliche Schwachstelle	**Bewertung Basisrisiko**	**Bewertung Restrisiko**	
Es erfolgt auf Basis der Onlineangaben des Betroffenen im Hintergrund ein Geoscoring	Jederzeit, kann zu Kreditablehnung führen und dem Betroffenen Mehrkosten > 1.000,- Euro verursachen	Geoscoring führt nicht zu einer automatisierten Kreditbewertung sondern nur zu einem Hinweis, dass Betroffener Daten korrigieren soll bzw. sich direkt an eine Filiale wenden soll	Vor Berechnung der Kreditkonditionen wird das vorliegende Scoringergebnis auch inhaltlich geprüft.
Antragsteller gibt jedoch unvollständige Adressdaten bekannt	SC / H4	SA / H2	

ARGE DATEN

-

DSGVO - Datenschutzorganisation

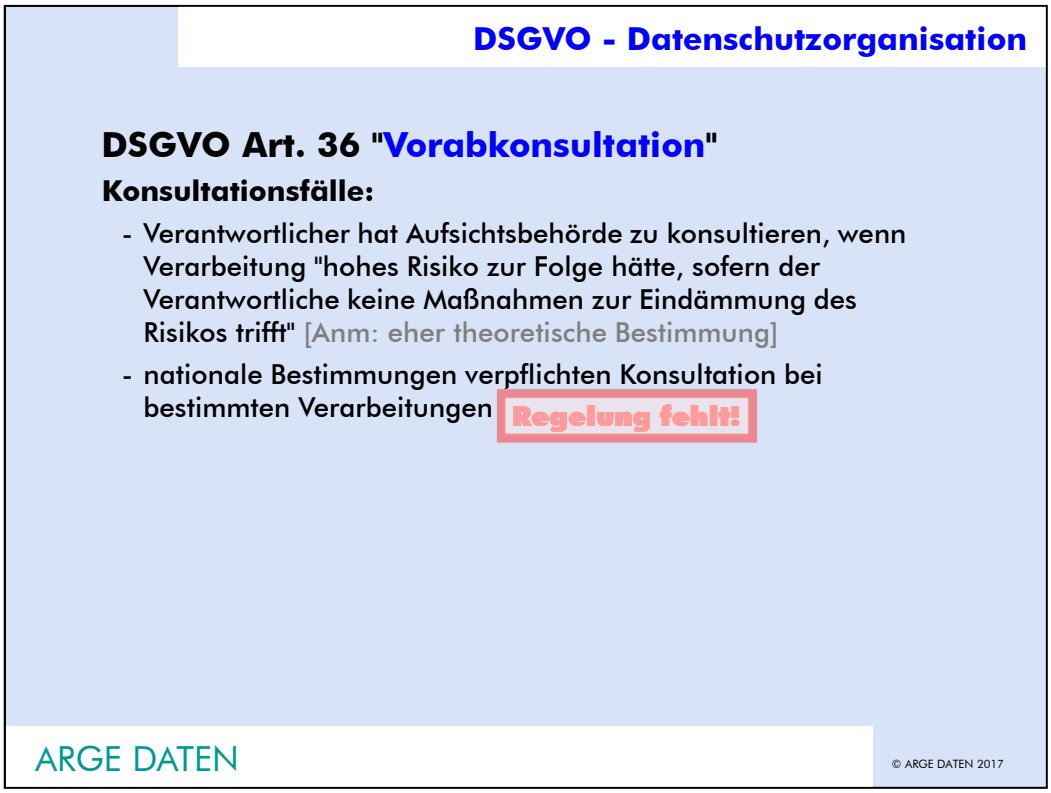
Datenschutz-Folgenabschätzung - Fallbeispiel II

- **Verarbeitung:** Patientenverwaltung
- **Verarbeitungsschritt:** Erst-Anamnese Spital
- **Auslöser:** Fehlerhafte Datenerfassung
- **Schadensklasse:** Fehltherapie

Potentielle Bedrohung	Basis Eintrittshäufigkeit und Schadenshöhe je Ereignis	getroffene Maßnahmen	Behandlung Restrisiko
Mögliche Schwachstelle	**Bewertung Basisrisiko**	**Bewertung Restrisiko**	
Es werden in der Erhebung Allergien und Medikamentenunverträglich-keiten übersehen	Jederzeit, maximales Risiko bis letalem Ausgang einer Behandlung	Nur Fachpersonal macht Anamnese, es existiert eine Checkliste, zumindest einmal jährlich Schulung, Patient muss Erhebung nach Aufklärung abzeichnen	Vor Verwendung der Anamnesedaten erfolgt Plausibilitätscheck der Daten, kritische Daten werden ein zweites Mal gecheckt, stichprobenhafte anlassunabhängige Prüfung der Erhebungsdaten
Unübersichtliches Formular, Zeitnot in der Erhebung, mangelnde Erfahrung des Erhebungspersonals	SD / H4	SA / H2	

ARGE DATEN

-



DSGVO Art. 36 Vorherige Konsultation

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

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

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

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

b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;

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

d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

e) die Datenschutz-Folgenabschätzung gemäß Artikel 35 und

f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

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

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

DSGVO - Datenschutzorganisation

DSGVO Art. 13 & 14 iV mit Art. 30, 33+34 und 19 ersetzen und erweitern:

DSG 2000 § 24 "Informationspflicht bei Ermittlung"

- Zweck und Auftraggeber
- spätestens zum Zeitpunkt der Übermittlung

Entfällt,

- bei Datenanwendungen, die durch **Gesetz/Verordnung eingerichtet** sind **oder**
- bei **mangelnder Erreichbarkeit** der Betroffenen **oder**
- bei **Unwahrscheinlichkeit der Beeinträchtigung der Betroffenenrechte** und Höhe der Kosten der Information

DSG 2000 §§ 16ff "Registrierungspflicht"

Das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 iVm den Informationsverpflichtungen gemäß Art. 13 & 14, 33+34, 19 und der Folgenabschätzung gemäß Art. 35 kann als Kernstück des neuen Datenschutzmanagements angesehen werden

ARGE DATEN

Bisherige Informations-Bestimmung gemäß DSG 2000

Betroffene sind aus Anlass der Ermittlung zu informieren über

Zweck der DA

Namen/Adresse des Auftraggebers

Notwendige weitere Informationen sind in geeigneter Weise zu geben:

Widerspruchsrechte gegen Übermittlungen

rechtliche Verpflichtung zur Beantwortung von Fragen

Verarbeitung in einem Informationsverbundsystem, ohne gesetzlichen Auftrag

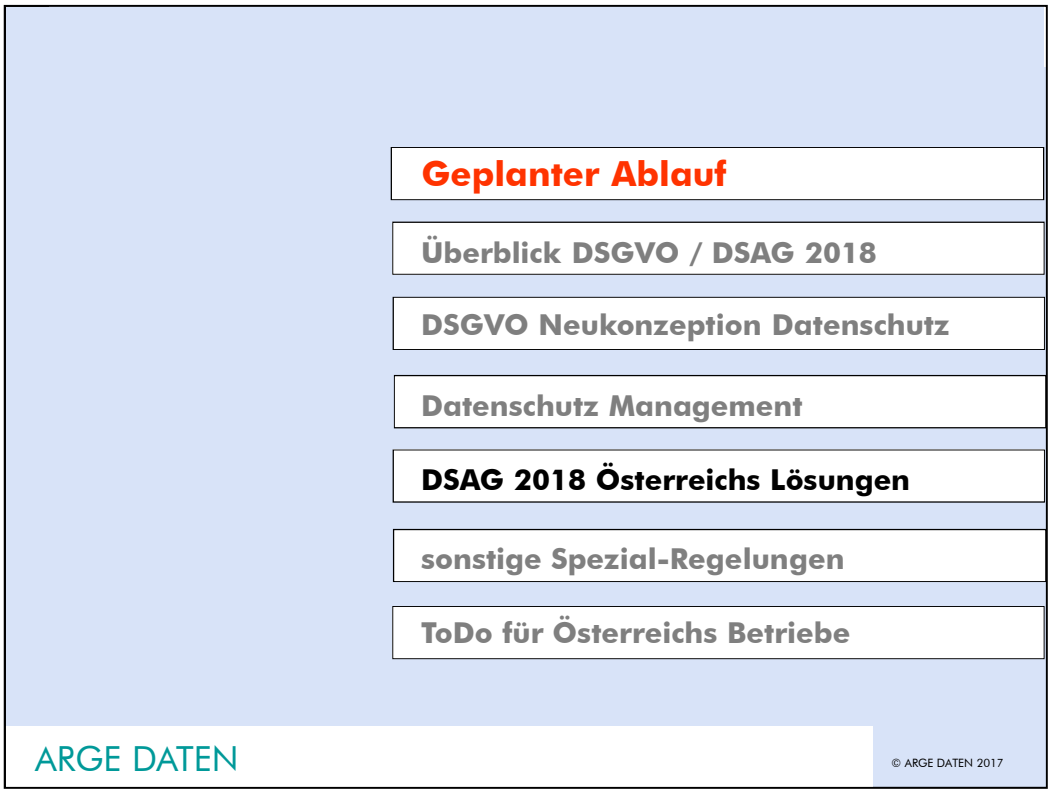
Werden Daten nicht direkt beim Betroffenen ermittelt, entfällt die Informationspflicht:

bei Datenanwendungen, die durch **Gesetz/Verordnung eingerichtet** sind **oder**

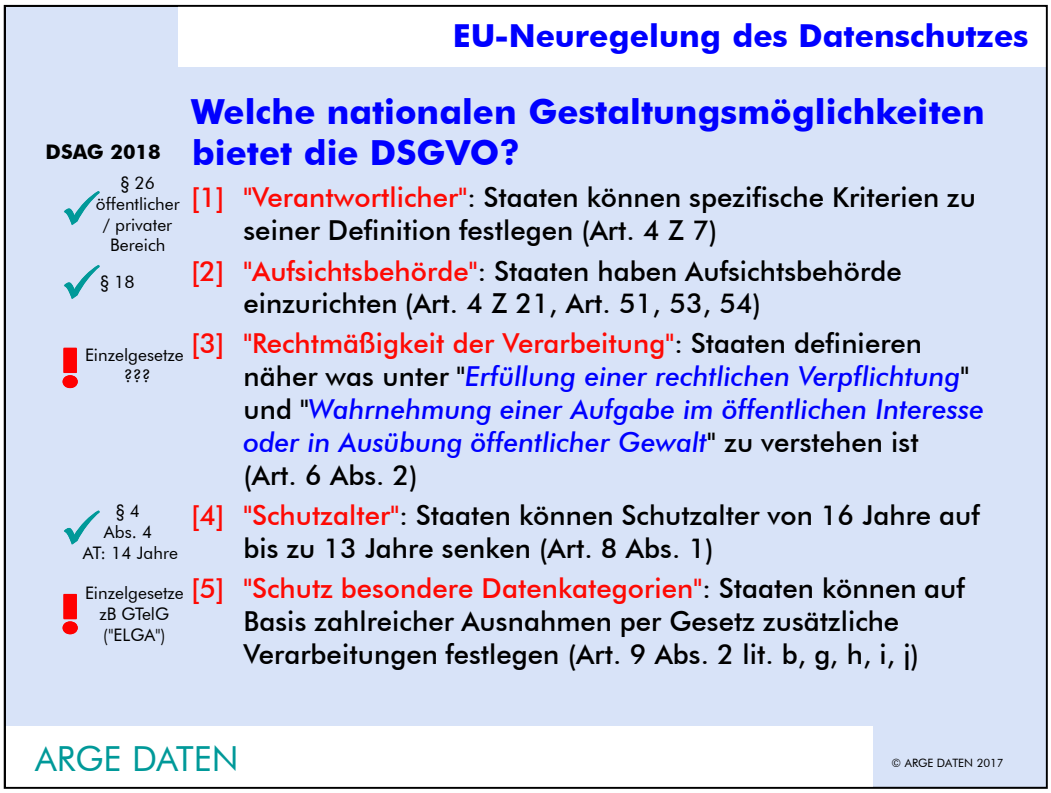
bei **mangelnder Erreichbarkeit** der Betroffenen **oder**

bei **Unwahrscheinlichkeit der Beeinträchtigung der Betroffenenrechte** und Höhe der Kosten der Information

Keine Informationspflicht besteht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind [persönliche DA, publizistische DA, indirekt pesonenbezogene Daten, DA zum Schutz der Verfassung/Einsatzbereitschaft/Landesverteidigung/Strafverfolgung]


Geplanter Ablauf
Überblick DSGVO / DSAG 2018
DSGVO Neukonzeption Datenschutz
Datenschutz Management
DSAG 2018 Österreichs Lösungen
sonstige Spezial-Regelungen
ToDo für Österreichs Betriebe
ARGE DATEN
© ARGE DATEN 2017

-



Verantwortliche des öffentlichen und des privaten Bereichs

DSAG 2018 § 26. (1) Verantwortliche des öffentlichen Bereichs sind alle Verantwortliche,
1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.
(2) Verantwortliche des öffentlichen Bereichs sind Partei in Verfahren vor der Datenschutzbehörde.
(3) Verantwortliche des öffentlichen Bereichs können Beschwerde an das Bundesverwaltungsgericht und Revision beim Verwaltungsgerichtshof erheben.
(4) Die dem Abs. 1 nicht unterliegenden Verantwortlichen gelten als Verantwortliche des privaten Bereichs im Sinne dieses Bundesgesetzes.

Einrichtung

DSAG 2018 § 18. (1) Die Datenschutzbehörde wird als nationale Aufsichtsbehörde gemäß Art. 51 DSGVO eingerichtet.
(2) Der Datenschutzbehörde steht ein Leiter vor. In seiner Abwesenheit leitet sein Stellvertreter die Datenschutzbehörde. Auf ihn finden die Regelungen hinsichtlich des Leiters der Datenschutzbehörde Anwendung.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

DSAG 2018 § 8. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adressdaten eines bestimmten Kreises von betroffenen Personen zum Zweck ihrer Benachrichtigung oder Befragung der Einwilligung der betroffenen Personen.

Anwendungsbereich und Durchführungsbestimmung

DSAG 2018 § 4. (1) ...

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

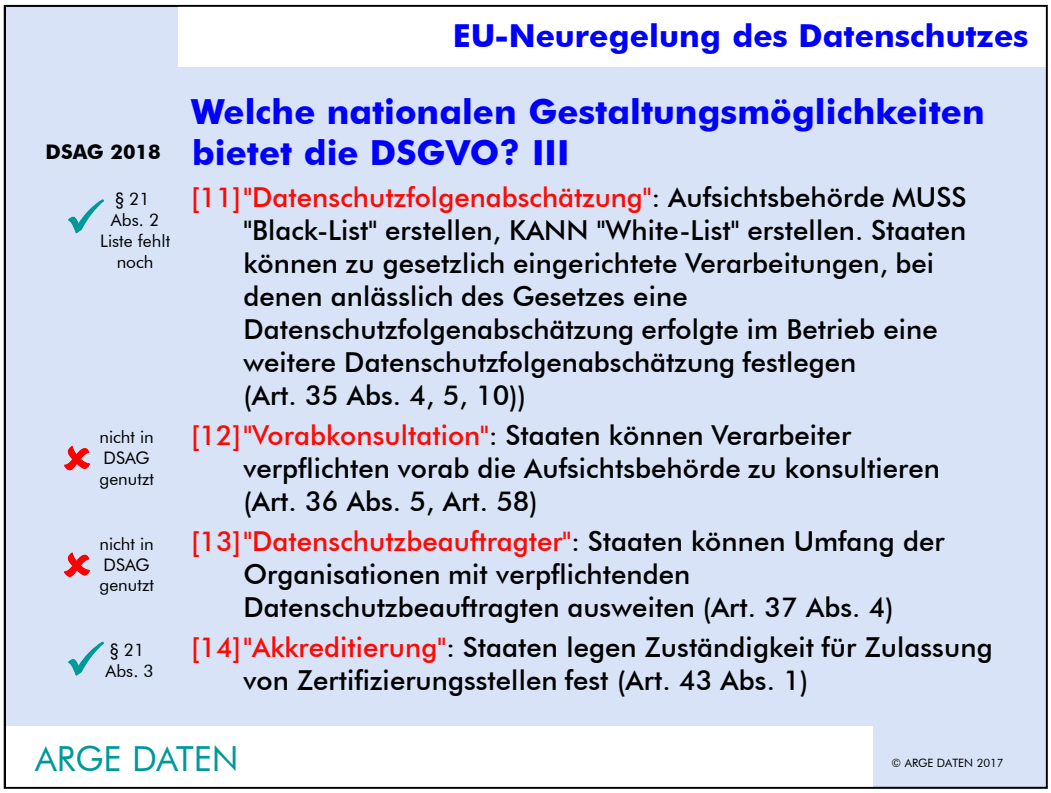
(3) Die Verarbeitung von personenbezogenen Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen ist unter Einhaltung der Vorgaben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

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

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

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

-

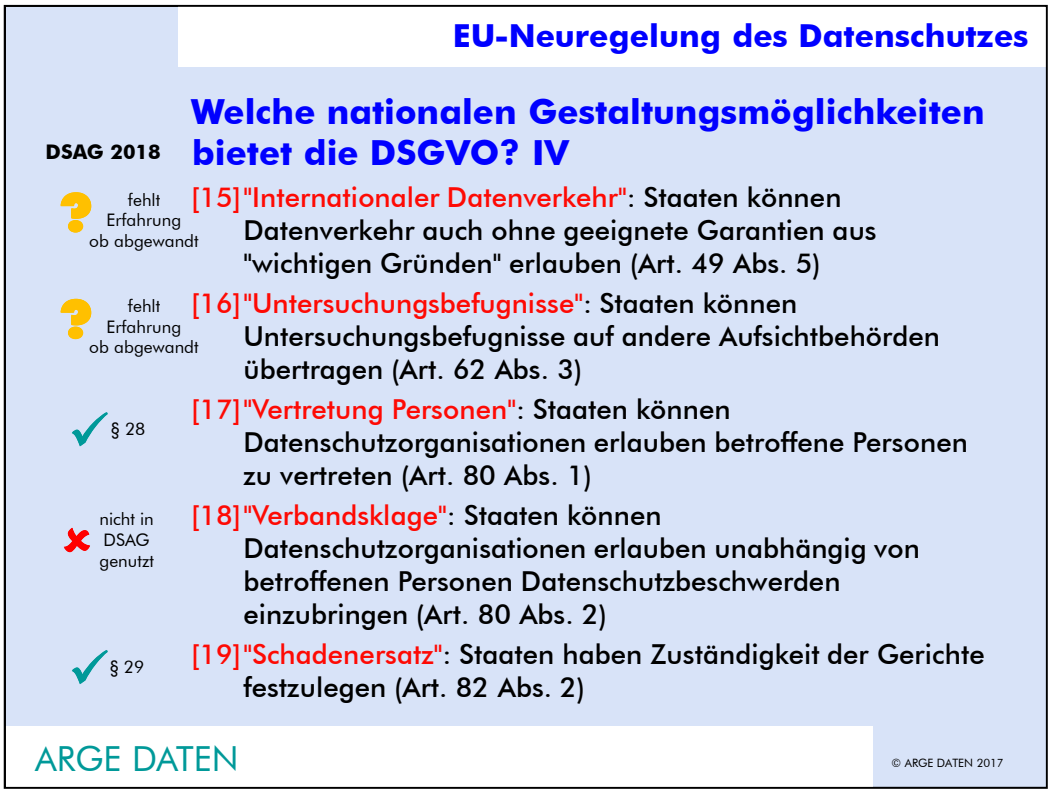


Aufgaben

DSAG 2018 § 21. (1) Die Datenschutzbehörde berät die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen. Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

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

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



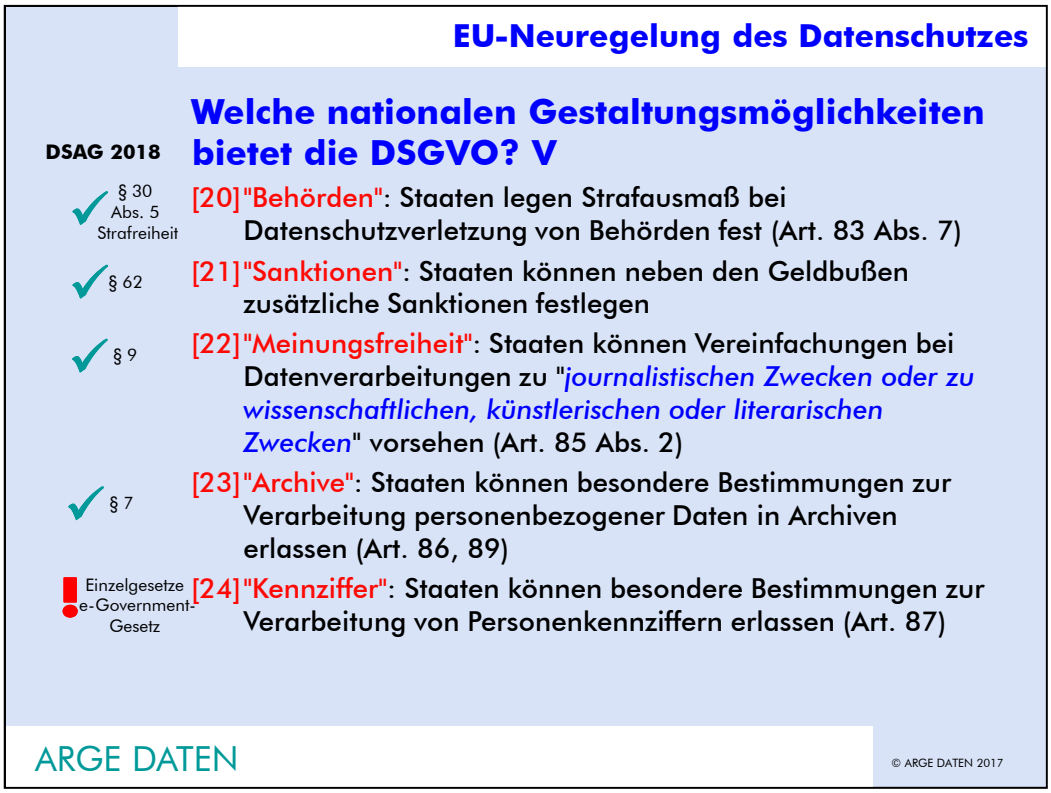
Vertretung von betroffenen Personen

DSAG 2018 § 28. Die betroffene Person hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den §§ 24 bis 27 genannten Rechte wahrzunehmen und das Recht auf Schadenersatz gemäß § 29 in Anspruch zu nehmen.

Haftung und Recht auf Schadenersatz

DSAG 2018 § 29. (1) Jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen § 1 oder Artikel 2 1. Hauptstück ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter nach Art. 82 DSGVO. Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts.

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



Allgemeine Bedingungen für die Verhängung von Geldbußen

DSAG 2018 § 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

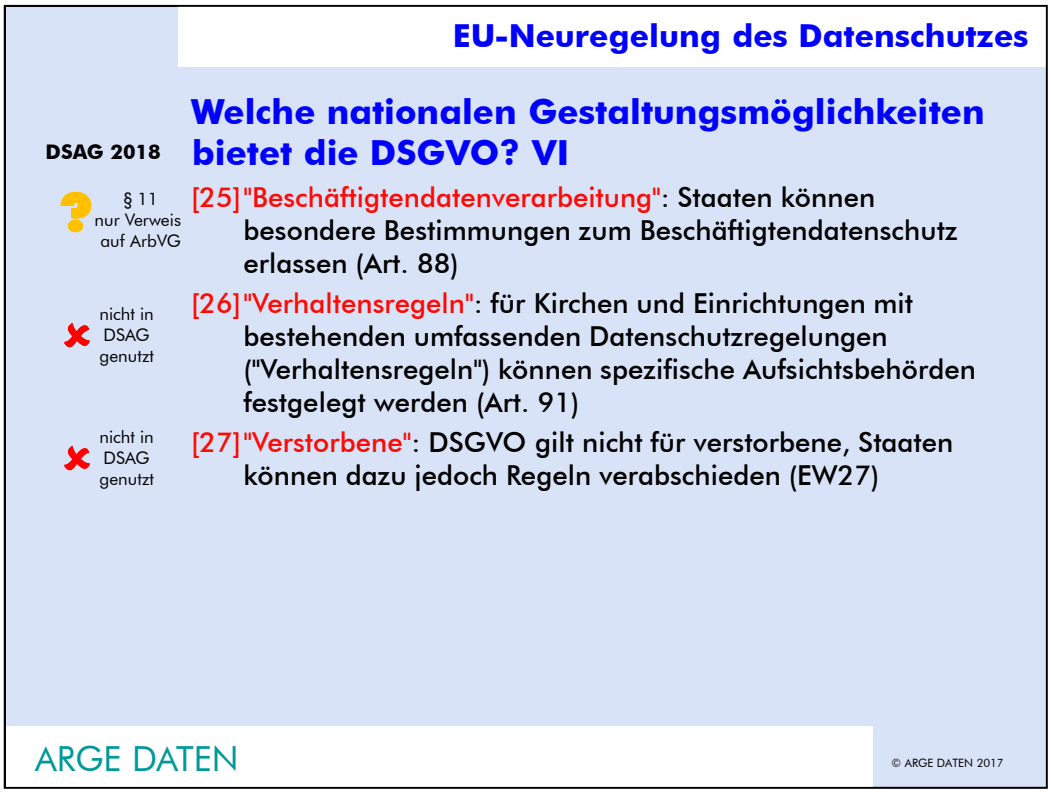
innehaben.

(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 und keine besonderen Umstände vorliegen, die einem Absehen von der Bestrafung entgegenstehen.

(4) ...

(5) Gegen Behörden und öffentliche Stellen können keine Geldbußen verhängt werden.



Verwaltungsstrafbestimmung

DSAG 2018 § 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.

Datenschutz-Anpassungsgesetz 2018

DSAG 2018 - Anpassungen auf Grund der DSGVO

- ✓ Aufsichtsbehörde festgelegt (§ 18 DSAG 2018)
- ✗ Schutzalter gesenkt (§ 4 Abs. 4 DSAG 2018)
- ✓ private Einrichtungen dürfen notwendige Daten zu Straftaten verarbeiten [Whistleblowing, Strafregisterauszug MA] (§ 4 Abs. 3 DSAG 2018)
- ? Zuständigkeit für Akkreditierung geregelt (§ 21 Abs. 3 DSAG 2018)
- ✓ Datenschutzorganisationen dürfen Personen vertreten (§§ 23, 28 DSAG 2018)
- ✗ Behörden von Geldstrafen "befreit" (§ 30 Abs. 5 DSAG 2018)
- ? Informationsfreiheit und Archive geregelt (§§ 7, 9 DSAG 2018)

DSAG 2018 - verpasste Chancen

- ✗ keine Regelung zum Arbeitnehmer-Datenschutz (Art. 88 DSGVO)
- ✗ keine Verbandsklagebefugnisse (Art. 80 DSGVO)
- ✗ keine Profiling-Regelungen (Art. 22 DSGVO)
- ✗ keine sinnvollen Sanktionen bei Behörden (Art. 83 DSGVO)
- ✗ keine generellen Vorgaben für Auftragsverarbeiter (Art. 28 DSGVO)

ARGE DATEN

-

Datenschutz-Anpassungsgesetz 2018

DSAG 2018 - sonstige Regelungen

- ✓ Datenverwendung zu Verständigungszwecken (§ 8 DSAG 2018)
- ✓ Bildverarbeitung (§§ 12-13 DSAG 2018)

DSAG 2018 - vermutlich DSGVO/EU-widrig

- ✖ weiterhin existierender § 1 des DSG 2000
- ✖ Verarbeitungsbeschränkung statt Löschung (§ 4 Abs. 2 DSAG 2018)
- ✖ Erlaubnis der Tonaufnahmen als Teil der Bildaufzeichnung (§ 12 Abs. 1 DSAG 2018)
- ✖ Fristsetzung bei Beschwerden (§ 24 Abs. 4 DSAG 2018)

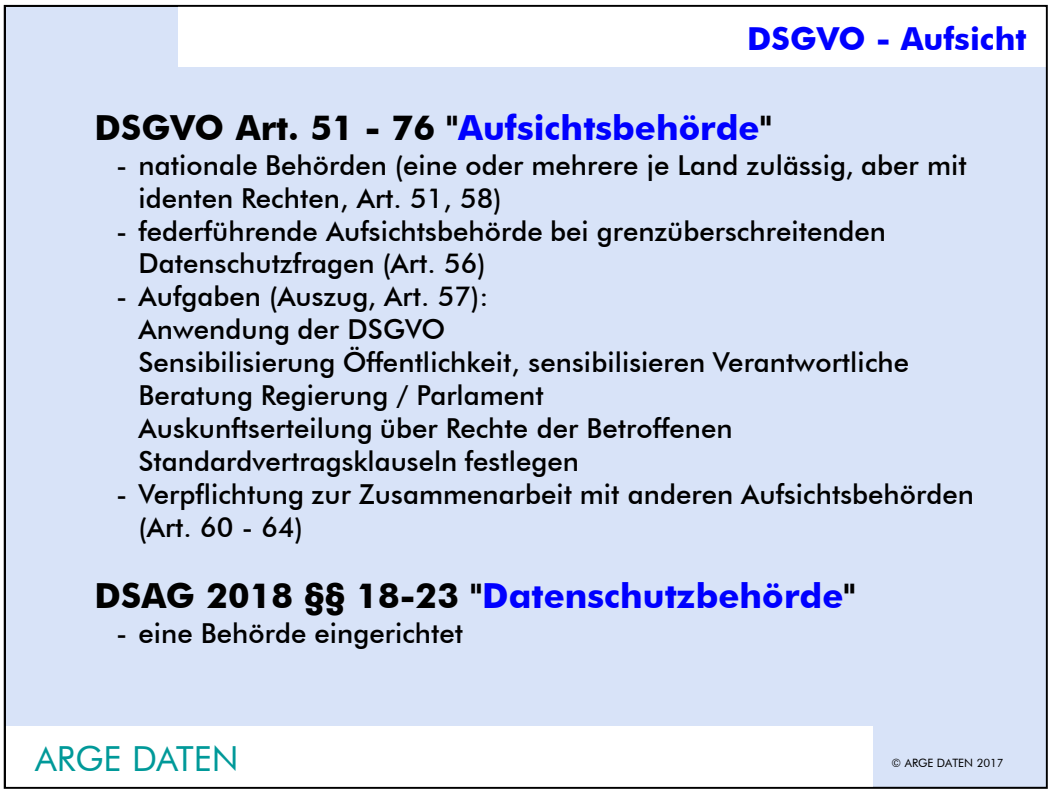
DSAG 2018 - Datenschutzfolklore

- ? Datenverarbeitung im Katastrophenfall (§ 10 DSAG 2018)
- ? Datenschutzrat (§§ 14-17 DSAG 2018)
- ? Strafbestimmung (§ 63 DSAG 2018)

DSAG 2018 präsentiert sich als Sammelsurium von Ergänzungen zur DSGVO, verpassten Chancen und bewahren "liebgewordener" Datenschutzfolklore

ARGE DATEN

-



Aufgaben

DSAG 2018 § 21. (1) Die Datenschutzbehörde berät die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen. Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

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

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

Befugnisse

DSAG 2018 § 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.

...

DSGVO - zuständige Stellen

Einrichtungen / Zuständigkeiten zum Datenschutz

- **Datenschutzbehörde *(formlos)***
  - Beschwerdestelle für Betroffene in allen Fällen
  - Aufsichtsstelle für alle Verantwortliche und Auftragsverarbeiter, die ihre Hauptniederlassung in AT haben
  - Strafbehörde bei Datenschutzverletzungen nach DSGVO und DSAG 2018
  - Kontroll-, Beratungs- und Informationsbefugnisse
  - Ansprechstelle in EU-Koheränzverfahren
- **Bundesverwaltungsgericht *(formlos)***
  - Beschwerdeinstanz gegen Entscheidungen der Datenschutzbehörde
- **Zivilgericht *(Anwaltspflicht)***
  - bei Schadenersatzklagen
- **Staatsanwaltschaft / Polizei (formlos)**
  Anzeigen gem. § 63 DSAG 2018

Zivilgerichte - 16 Landesgerichte zuständig:

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

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


Geplanter Ablauf
Überblick DSGVO / DSAG 2018
DSGVO Neukonzeption Datenschutz
Datenschutz Management
DSAG 2018 Österreichs Lösungen
sonstige Spezial-Regelungen
ToDo für Österreichs Betriebe
ARGE DATEN
© ARGE DATEN 2017

-

DSGVO Art. 37 Benennung eines Datenschutzbeauftragten

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

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

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

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

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

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

DSGVO - Datenschutzorganisation

DSGVO Art. 37
"Benennung Datenschutzbeauftragter" II

Organisationsbestimmungen:

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

ARGE DATEN

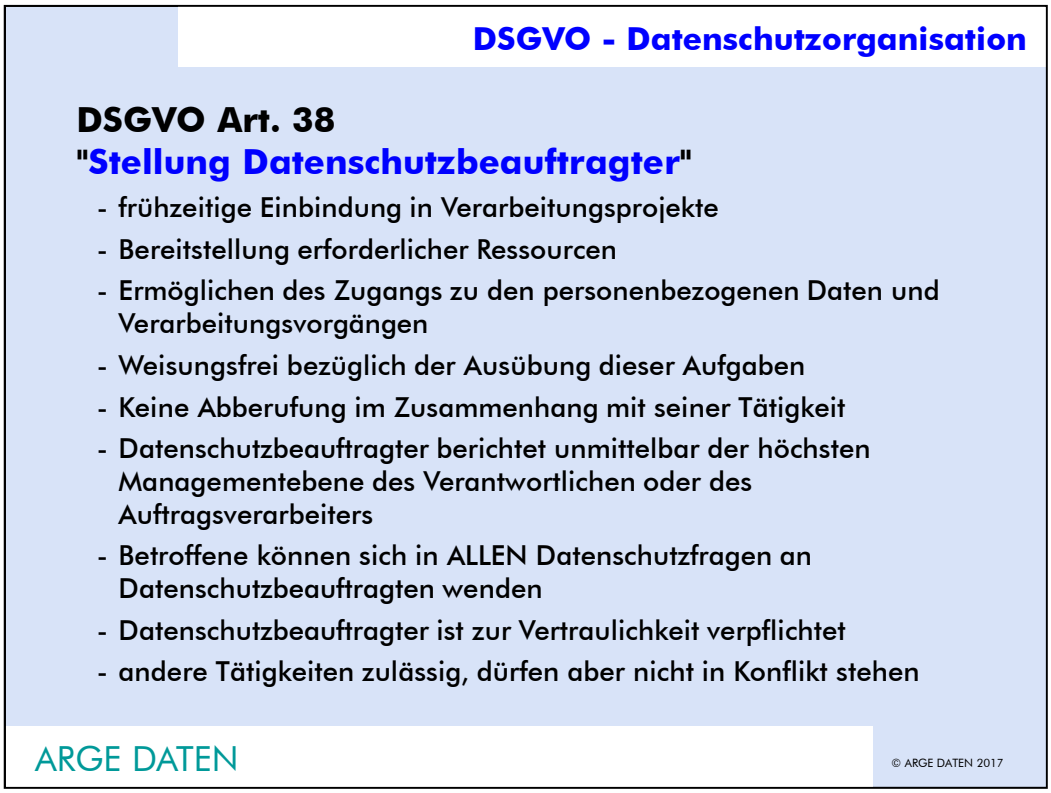
DSGVO Art. 37 Benennung eines Datenschutzbeauftragten

(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.

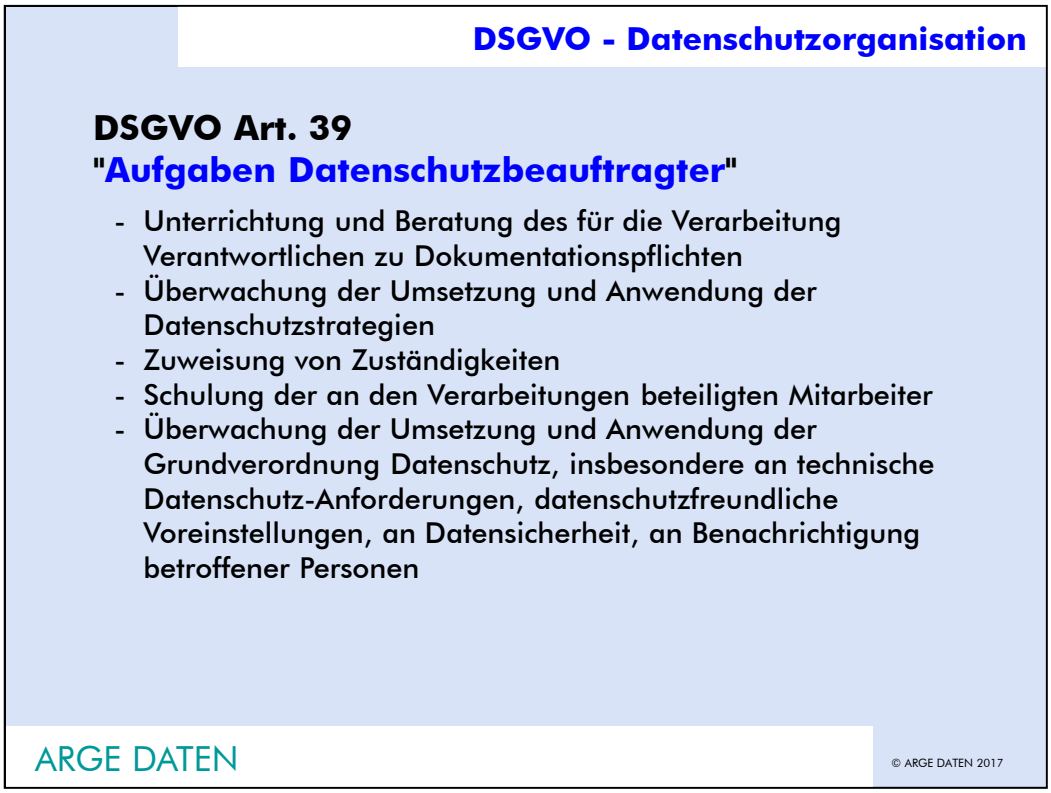
(2)Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur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

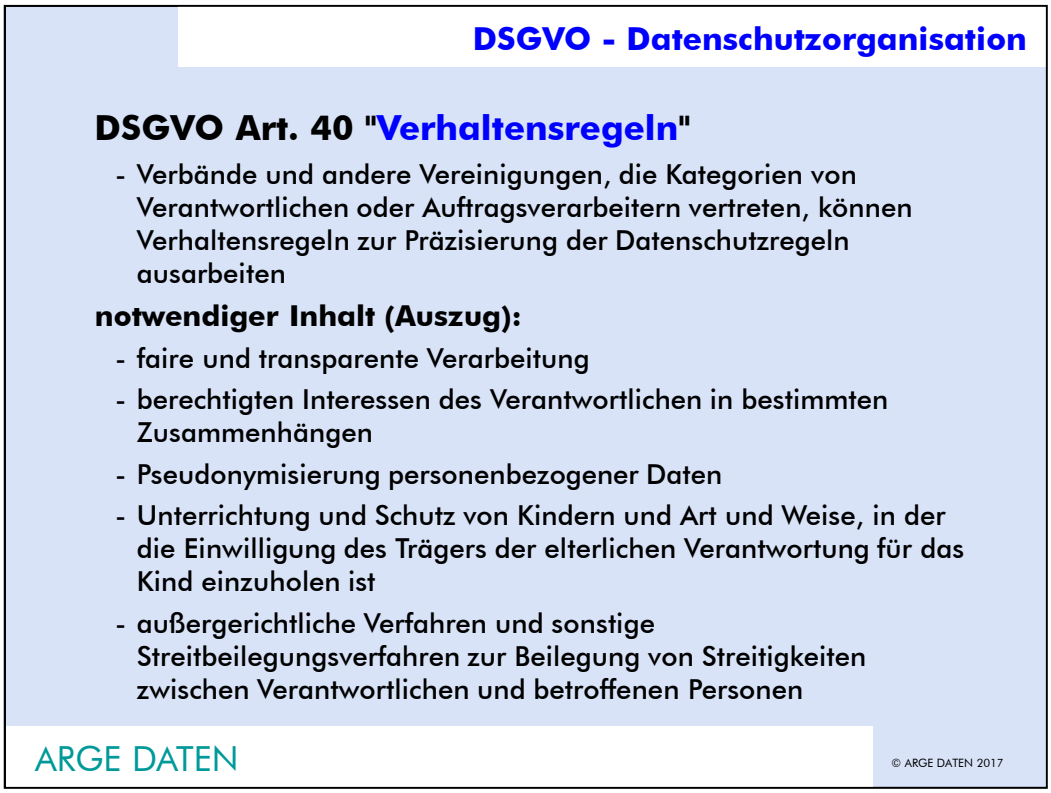
DSGVO - Datenschutzorganisation

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

ARGE DATEN

-



DSGVO Art. 28 Verhaltensregeln

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

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

a) faire und transparente Verarbeitung;

b) die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;

c) Erhebung personenbezogener Daten;

d) Pseudonymisierung personenbezogener Daten;

e) Unterrichtung der Öffentlichkeit und der betroffenen Personen;

f) Ausübung der Rechte betroffener Personen;

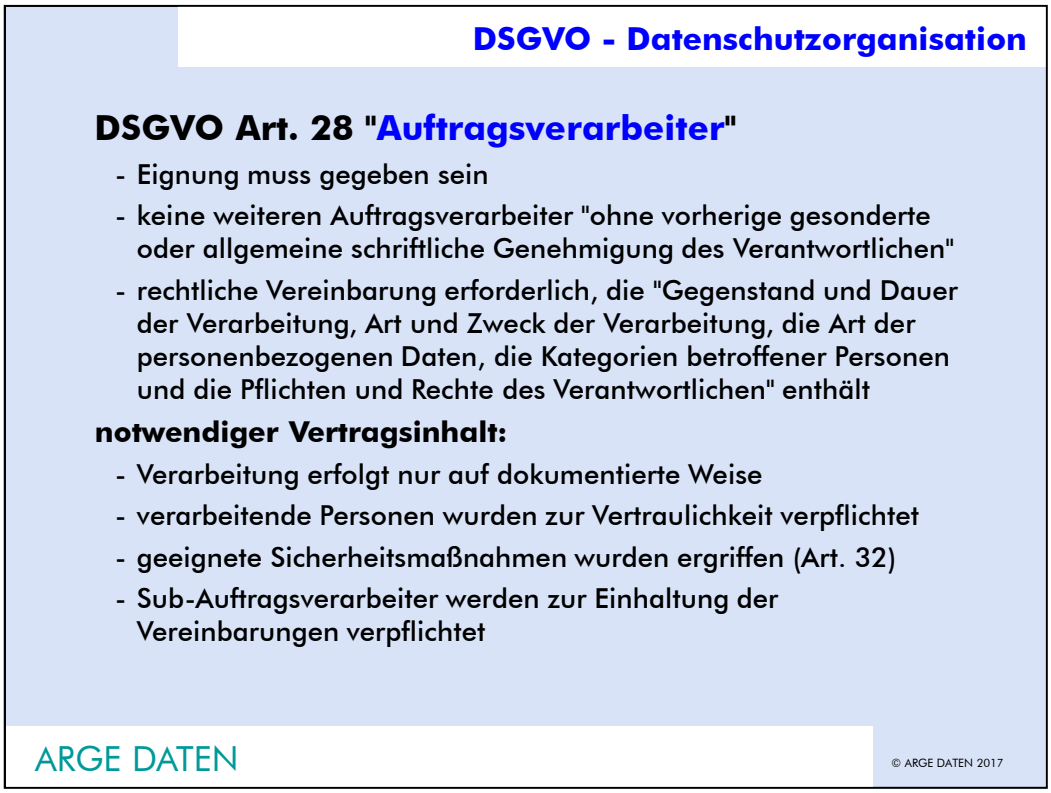
g) Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;

h) die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;

i) die Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes personenbezogener Daten;

j) die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder

k) außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Artikeln 77 und 79.



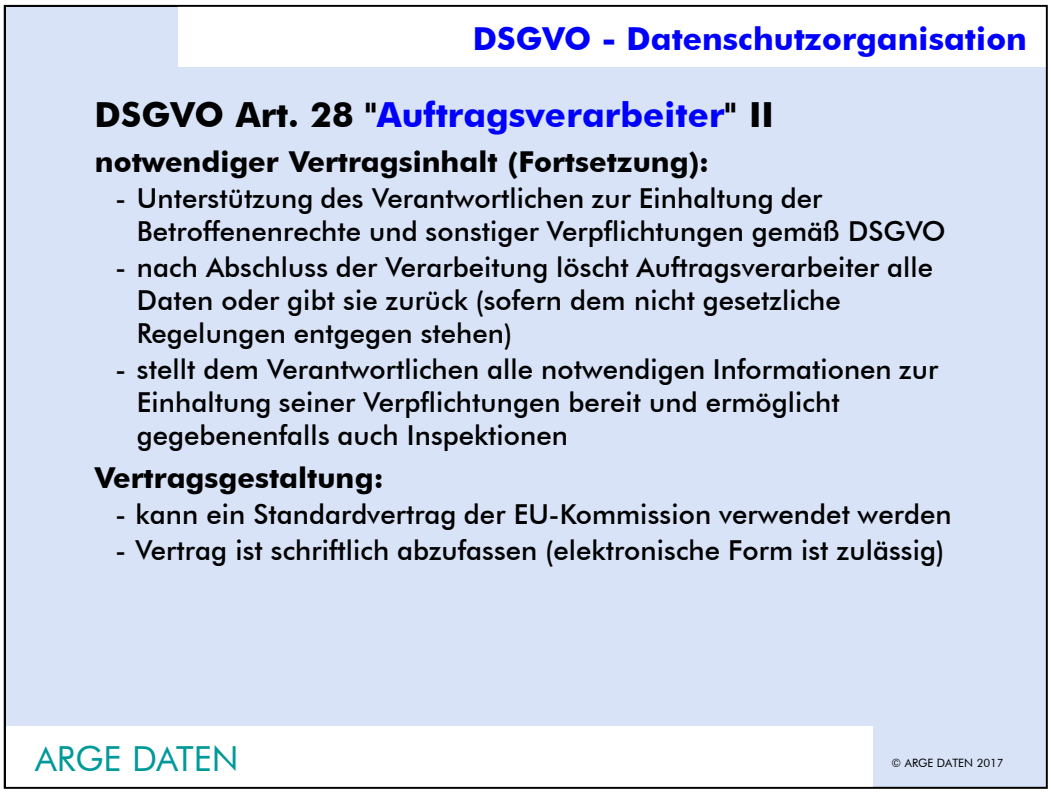
DSGVO Art. 28 Auftragsverarbeiter

(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;

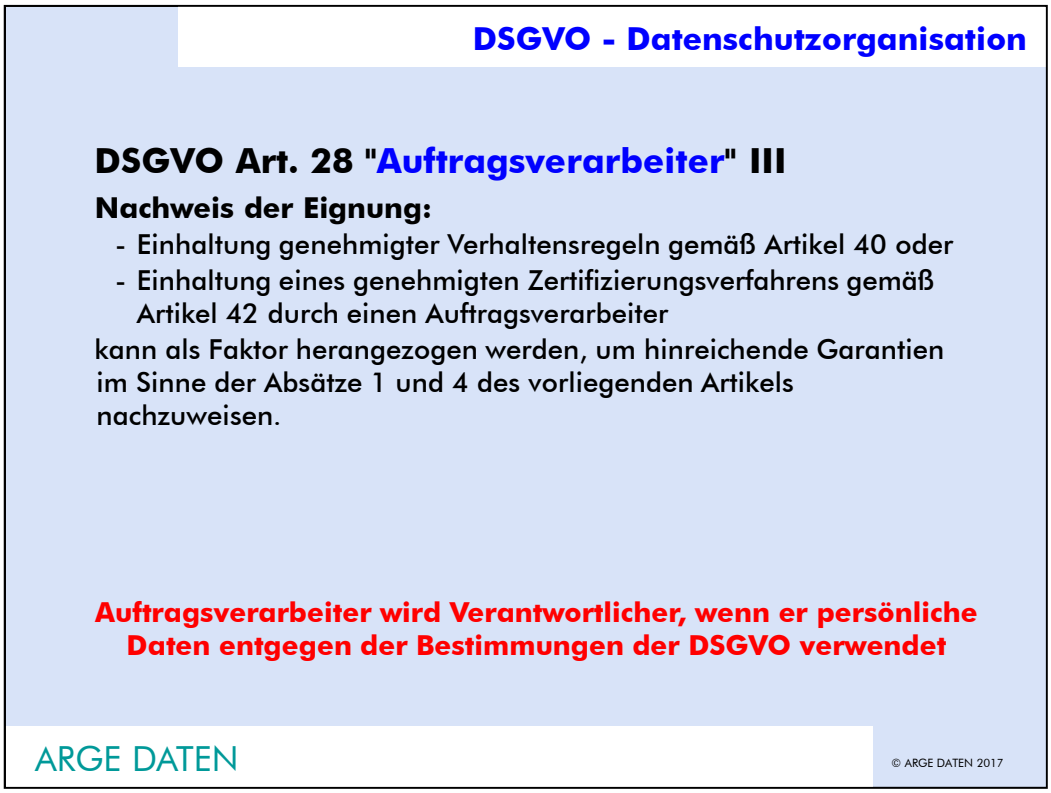
e)angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

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.

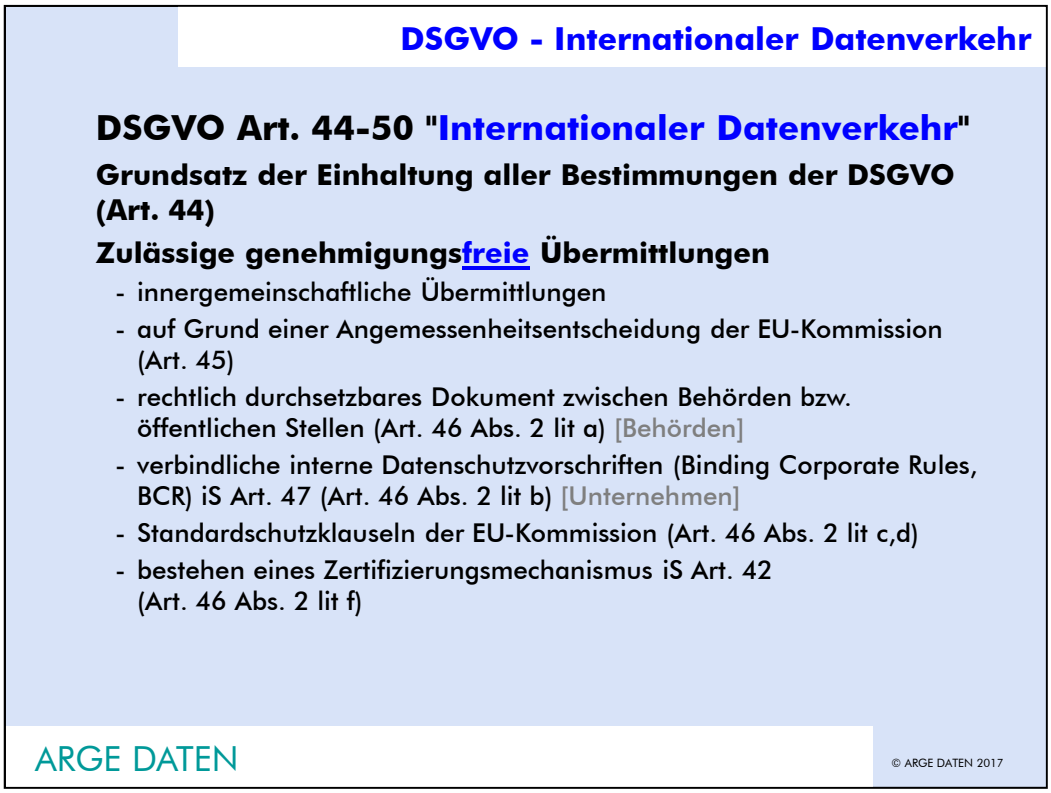
(6)Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln 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.



DSGVO Art. 44 Allgemeine Grundsätze der Datenübermittlung

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

DSGVO Art. 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

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

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

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

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

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

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

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

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

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

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

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

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

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

DSGVO 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;

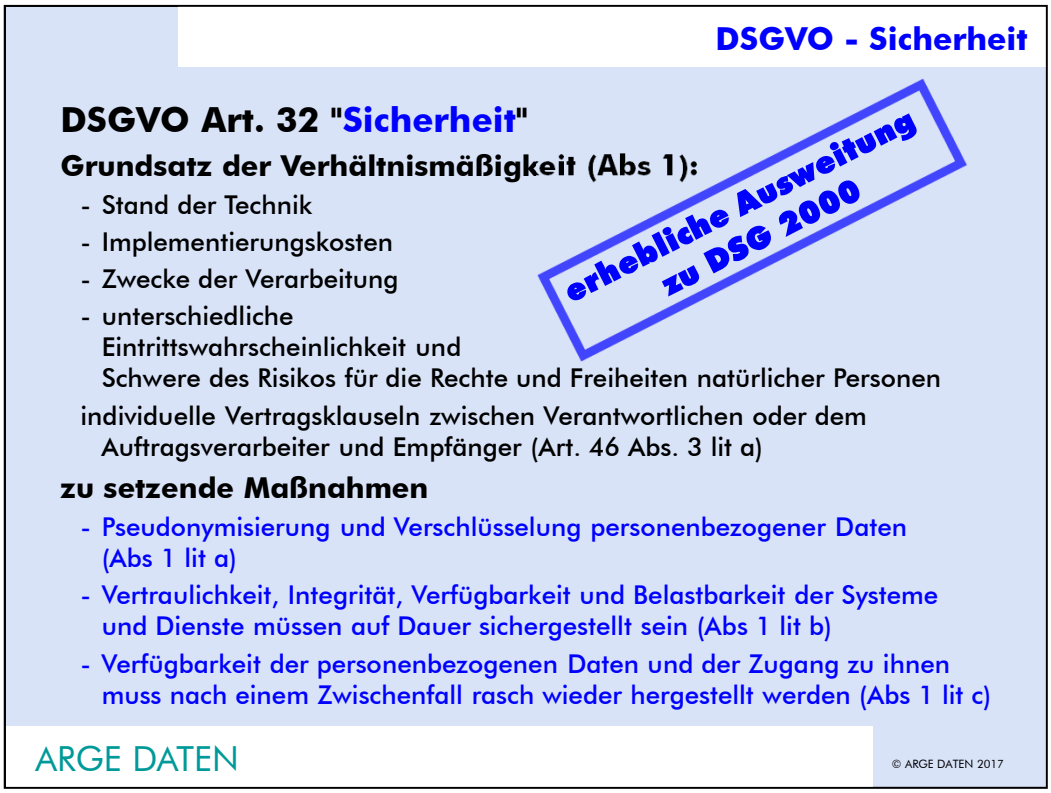
k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

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.



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;

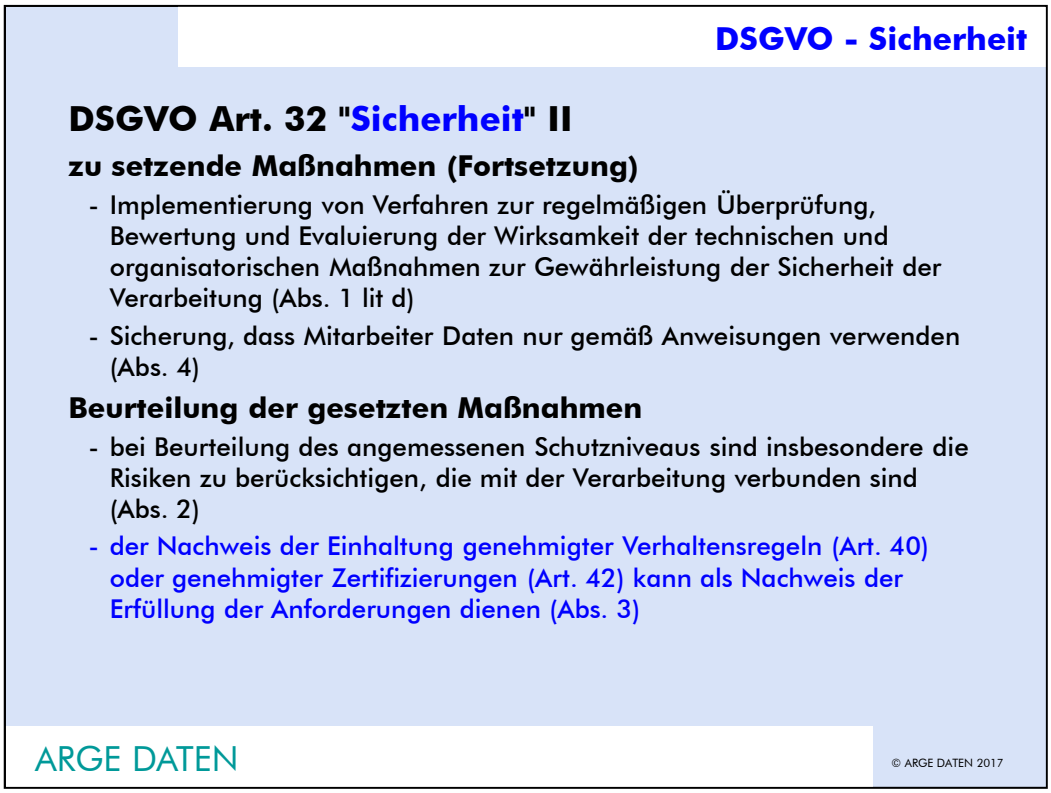
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

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 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;

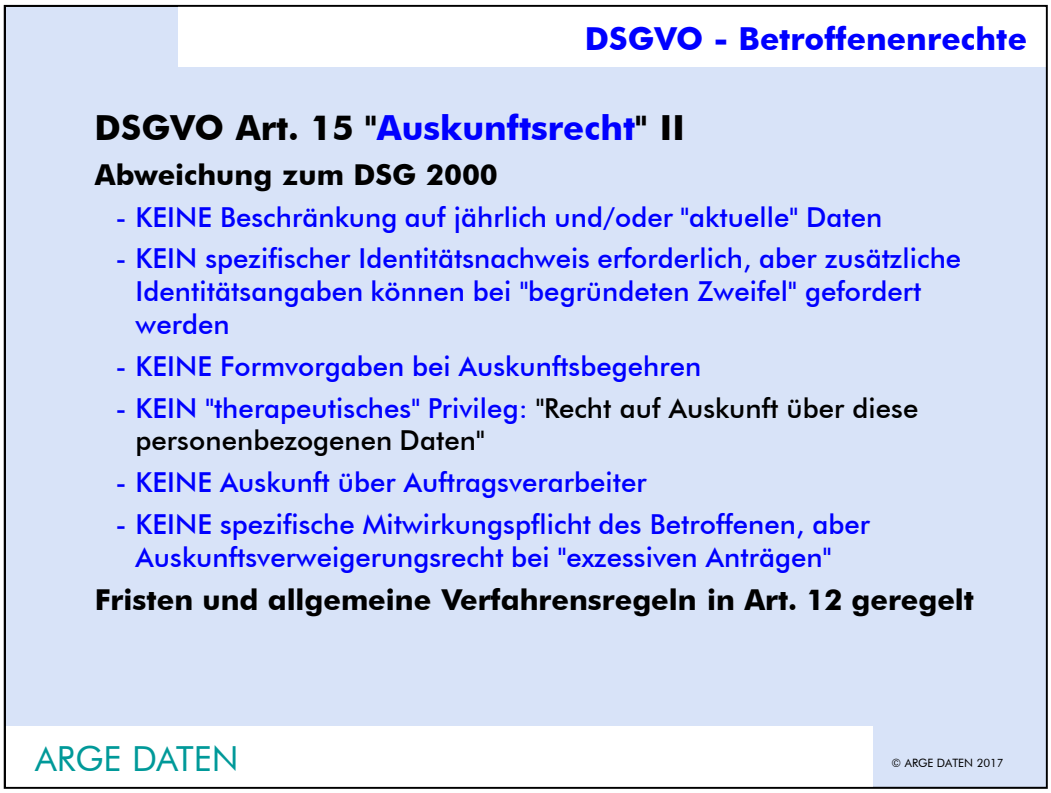
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

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.

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

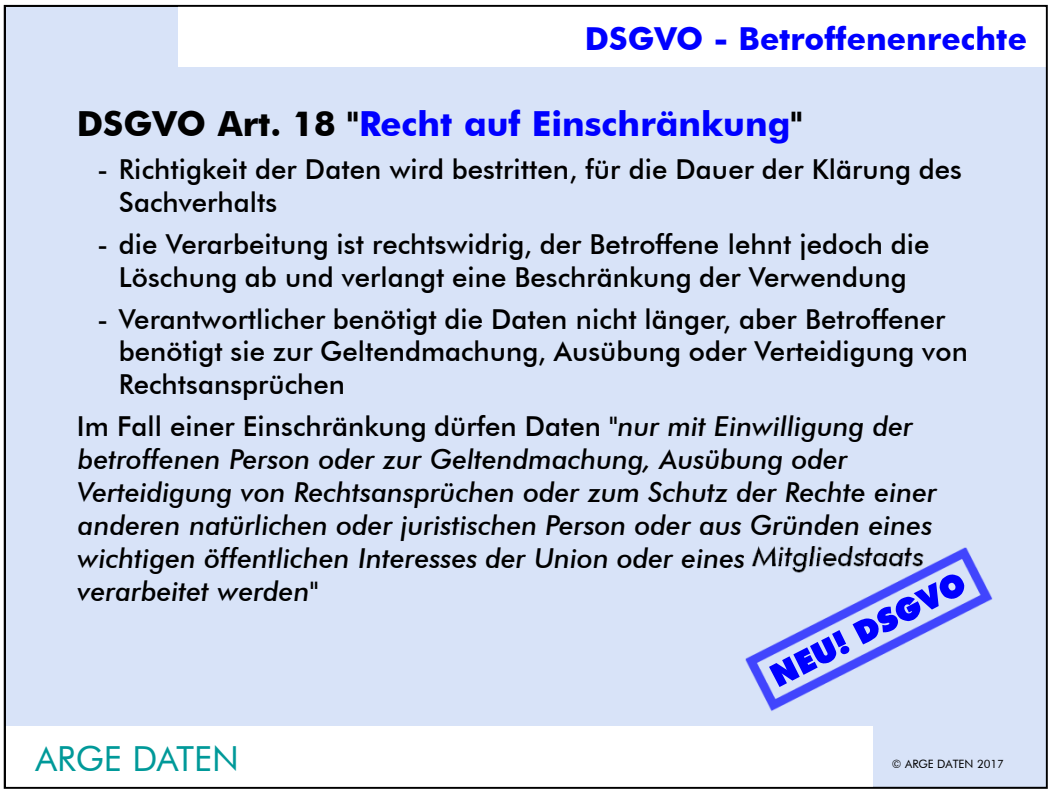
a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

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.



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,

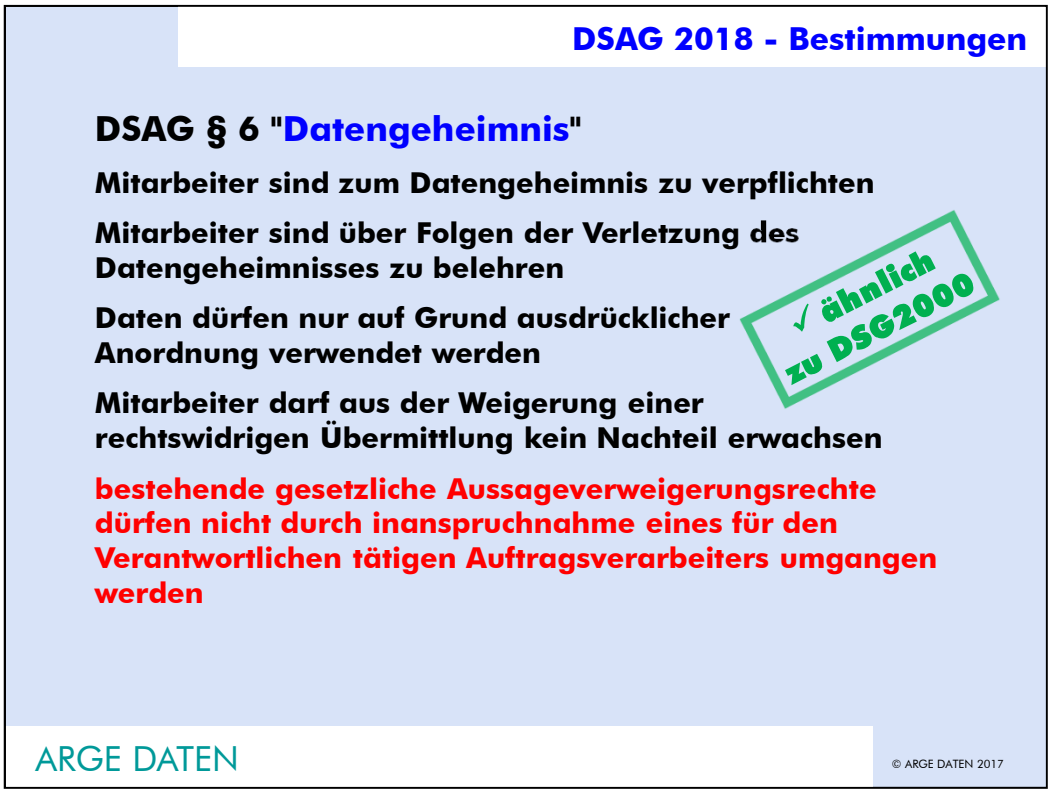
b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

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.



Datengeheimnis

DSAG 2018 § 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.

Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke

DSAG 2018 § 7 (1) Für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Verantwortliche alle personenbezogenen Daten verarbeiten, die

1. öffentlich zugänglich sind,

2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder

3. für ihn pseudonymisierte personenbezogene Daten sind und der Verantwortliche die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen kann.

(2) Bei Datenverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke, die nicht unter Abs. 1 fallen, dürfen personenbezogene Daten nur

1. gemäß besonderen gesetzlichen Vorschriften,

2. mit Einwilligung der betroffenen Person oder

3. mit Genehmigung der Datenschutzbehörde gemäß Abs. 3

verarbeitet werden.

(3) Eine Genehmigung der Datenschutzbehörde für die Verarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke ist auf Antrag des Verantwortlichen der Untersuchung zu erteilen, wenn

1. die Einholung der Einwilligung der betroffenen Person mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet,

2. ein öffentliches Interesse an der beantragten Verarbeitung besteht und

3. die fachliche Eignung des Verantwortlichen glaubhaft gemacht wird.

Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke (Fortsetzung

DSAG 2018 § 7...

Sollen besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) ermittelt werden, muss ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muss gewährleistet sein, dass die personenbezogenen Daten beim Verantwortlichen der Untersuchung nur von Personen verarbeitet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Person notwendig ist.

(4) Einem Antrag nach Abs. 3 ist jedenfalls eine vom Verfügungsbefugten über die Datenbestände, aus denen die personenbezogenen Daten ermittelt werden sollen, unterfertigte Erklärung anzuschließen, dass er dem Verantwortlichen die Datenbestände für die Untersuchung zur Verfügung stellt. Anstelle dieser Erklärung kann auch ein diese Erklärung ersetzender Exekutionstitel (§ 367 Abs. 1 der Exekutionsordnung – EO, RGBl. Nr. 79/1896) vorgelegt werden.

(5) Auch in jenen Fällen, in welchen die Verarbeitung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, ist der Personenbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit personenbezogenen Daten gemäß Abs. 1 Z 3 das Auslangen gefunden werden kann. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, ist der Personenbezug der Daten gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist.

(6) Rechtliche Beschränkungen der Zulässigkeit der Benützung von personenbezogenen Daten aus anderen, insbesondere urheberrechtlichen Gründen, bleiben unberührt.

Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

DSAG 2018 § 8. (1) Soweit gesetzlich nicht ausdrücklich anderes bestimmt ist, bedarf die Übermittlung von Adressdaten eines bestimmten Kreises von betroffenen Personen zum Zweck ihrer Benachrichtigung oder Befragung der Einwilligung der betroffenen Personen.

(2) Wenn allerdings eine Beeinträchtigung der Geheimhaltungsinteressen der betroffenen Personen angesichts der Auswahlkriterien für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung unwahrscheinlich ist, bedarf es keiner Einwilligung, wenn

1. Daten desselben Verantwortlichen verarbeitet werden oder

2. bei einer beabsichtigten Übermittlung der Adressdaten an Dritte

a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder

b) keiner der betroffenen Personen nach entsprechender Information über Anlass und Inhalt der Übermittlung innerhalb angemessener Frist Widerspruch gegen die Übermittlung erhoben hat.

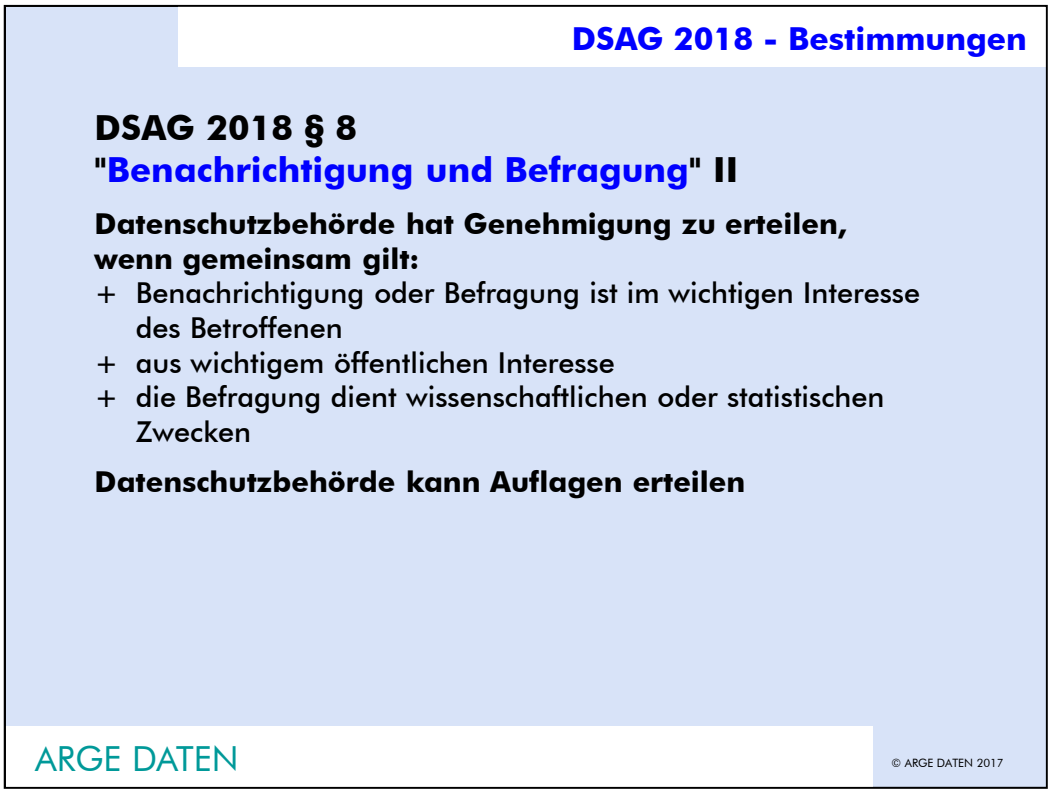
(3) Liegen die Voraussetzungen des Abs. 2 nicht vor und würde die Einholung der Einwilligung der betroffenen Personen gemäß Abs. 1 einen unverhältnismäßigen Aufwand erfordern, ist die Übermittlung der Adressdaten mit Genehmigung der Datenschutzbehörde gemäß Abs. 4 zulässig, falls die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst,

2. aus einem wichtigen öffentlichen Benachrichtigungs- oder Befragungsinteresse oder

3. zur Befragung der betroffenen Personen für wissenschaftliche oder statistische Zwecke

erfolgen soll.



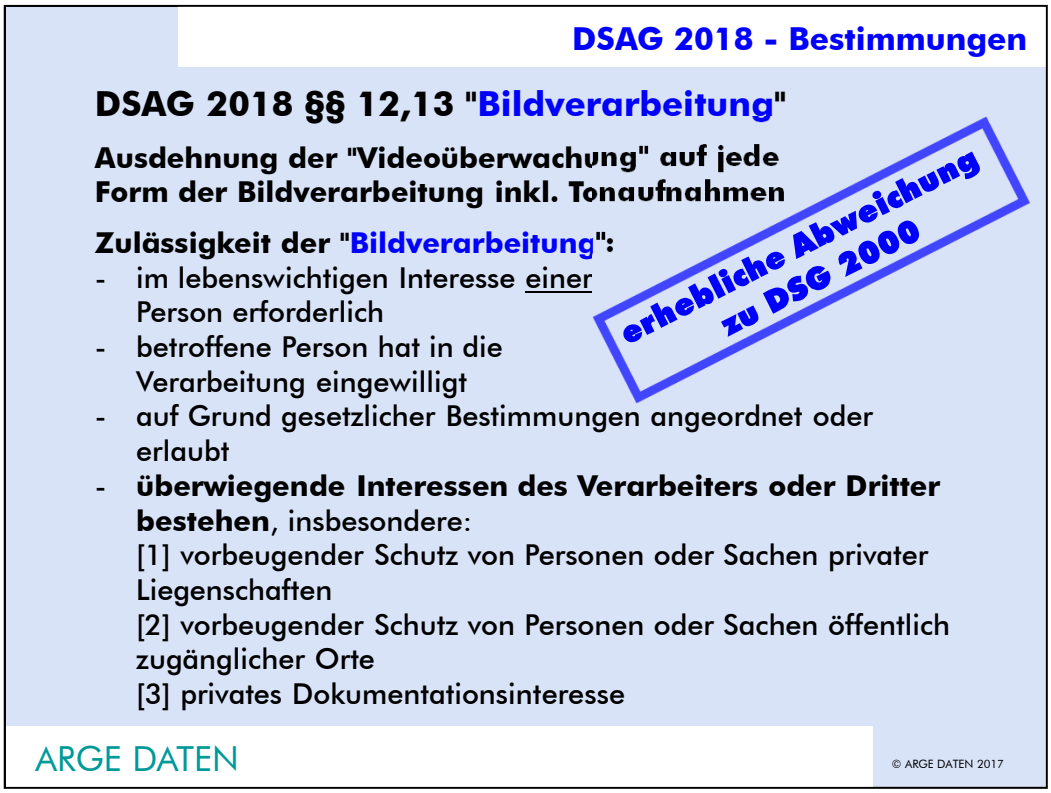
Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen (Fortsetzung)

DSAG 2018 § 8. ...

(4) Die Datenschutzbehörde hat auf Antrag eines Verantwortlichen, der Adressdaten verarbeitet, die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der betroffenen Personen der Übermittlung nicht entgegenstehen. Die Datenschutzbehörde hat die Genehmigung an die Erfüllung von Bedingungen und Auflagen zu knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der betroffenen Personen notwendig ist.

(5) Die übermittelten Adressdaten dürfen ausschließlich für den genehmigten Zweck verarbeitet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

(6) Sofern es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, dürfen auch die zum Zweck der Auswahl der zu übermittelnden Adressdaten notwendigen Verarbeitungen vorgenommen werden.



Zulässigkeit der Bildaufnahme

DSAG 2018 § 12. (1) Eine Bildaufnahme im Sinne dieses Abschnittes bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen. Für eine derartige Bildaufnahme gilt dieser Abschnitt, soweit nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Eine Bildaufnahme ist unter Berücksichtigung der Vorgaben gemäß § 13 zulässig, wenn

1. sie im lebenswichtigen Interesse einer Person erforderlich ist,

2. die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,

3. sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder

4. im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

(3) Eine Bildaufnahme ist gemäß Abs. 2 Z 4 insbesondere dann zulässig, wenn

1. sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen,

2. sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist und kein gelinderes geeignetes Mittel zur Verfügung steht, oder

3. sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.

DSAG 2018 - Bestimmungen

DSAG 2018 §§ 12,13 "Bildverarbeitung" II

[1] Bildverarbeitung privat genutzter Liegenschaft:
- Liegenschaft ausschließlich vom Verantwortlichen genutzt
- Aufzeichnung erfolgt innerhalb der Liegenschaft
- öffentliche Verkehrsflächen dürfen im Umfang der Zielerreichung erfasst warden

[2] Bildverarbeitung öffentlich zugänglicher Orte:
- Ort unterliegt dem Hausrecht des Verantwortlichen
- vorherige Rechtsverletzungen oder besonderes Gefährdungspotential erfordert Überwachung

[3] Bildverarbeitung aus privatem Dokumentationsinteresse:
- keine identifizierende Erfassung von Personen angestrebt
- keine Erfassung von Objekten, die zur mittelbaren Identifikation von Personen geeignet ist wird angestrebt

ARGE DATEN

Zulässigkeit der Bildaufnahme

DSAG 2018 § 12. ...

(4) Unzulässig ist

1. eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich,

2. eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,

3. der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten oder

4. die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

(5) Im Wege einer zulässigen Bildaufnahme ermittelte personenbezogene Daten dürfen im erforderlichen Ausmaß übermittelt werden, wenn für die Übermittlung eine der Voraussetzungen des Abs. 2 Z 1 bis 4 gegeben ist. Abs. 4 gilt sinngemäß.

DSAG 2018 - Bestimmungen

DSAG 2018 §§ 12,13 "Bildverarbeitung" III

Verarbeitungsverbote:

- Bildaufnahme ohne Einwilligung des Betroffenen in seinem höchstpersönlichen Lebensbereich
- zur Kontrolle der Mitarbeiter
- automationsunterstützter Abgleich der Daten der Bildaufnahme mit anderen personenbezogenen Daten
- Auswertung der Daten der Bildaufnahmen mit besonderen Kategorien von Daten

Sicherheitsmaßnahmen:

- Verhinderung nachträglicher Änderungen durch Unbefugte
- jede Verwendung ist zu protokollieren (Ausnahme: Echtzeitüberwachung)
- Löschung, wenn nicht mehr benötigt, eine Aufbewahrung länger als 72 Stunden ist zu begründen und dokumentieren

Sicherheitsmaßnahmen sind nicht im Fall [3] privates Dokumentationsinteresse anzuwenden!

ARGE DATEN

Besondere Datensicherheitsmaßnahmen und Kennzeichnung

DSAG 2018 § 13. (1) Der Verantwortliche hat dem Risiko des Eingriffs angepasste geeignete Datensicherheitsmaßnahmen zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist.

(2) Der Verantwortliche hat – außer in den Fällen einer Echtzeitüberwachung – jeden Verarbeitungsvorgang zu protokollieren.

(3) Aufgenommene personenbezogene Daten sind vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen.

(4) Die Abs. 1 bis 3 finden keine Anwendung auf Bildaufnahmen nach § 12 Abs. 3 Z 3.

(5) Der Verantwortliche einer Bildaufnahme hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt.

(6) Die Kennzeichnungspflicht gilt nicht in den Fällen des § 12 Abs. 3 Z 3 und für zeitlich strikt zu begrenzende Verarbeitungen im Einzelfall, deren Zweck ausschließlich mittels einer verdeckten Ermittlung erreicht werden kann, unter der Bedingung, dass der Verantwortliche ausreichende Garantien zur Wahrung der Betroffeneninteressen vorsieht, insbesondere durch eine nachträgliche Information der betroffenen Personen.

(7) Werden entgegen Abs. 5 keine ausreichenden Informationen bereitgestellt, kann jeder von einer Verarbeitung potenziell Betroffene vom Eigentümer oder Nutzungsberechtigten einer Liegenschaft oder eines Gebäudes oder sonstigen Objekts, von dem aus eine solche Verarbeitung augenscheinlich ausgeht, Auskunft über die Identität des Verantwortlichen begehren. Die unbegründete Nichterteilung einer derartigen Auskunft ist einer Verweigerung der Auskunft nach Art. 15 DSGVO gleichzuhalten.

DSAG 2018 - Bestimmungen

DSAG 2018 §§ 12,13 "Bildverarbeitung" IV

Kennzeichnungspflicht:

- Bildaufnahmen sind zu kennzeichnen
- keine Kennzeichnung im Fall [3] privates Dokumentationsinteresse
- keine Kennzeichnung bei zeitlich strikt begrenzten Verarbeitungen, wenn Zweck nur durch verdeckte Ermittlung erreicht werden kann

ARGE DATEN

-

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.

DSGVO - Strafbestimmungen

DSGVO Art. 58, 83, 84 "Sanktionen"

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

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

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

ARGE DATEN

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;

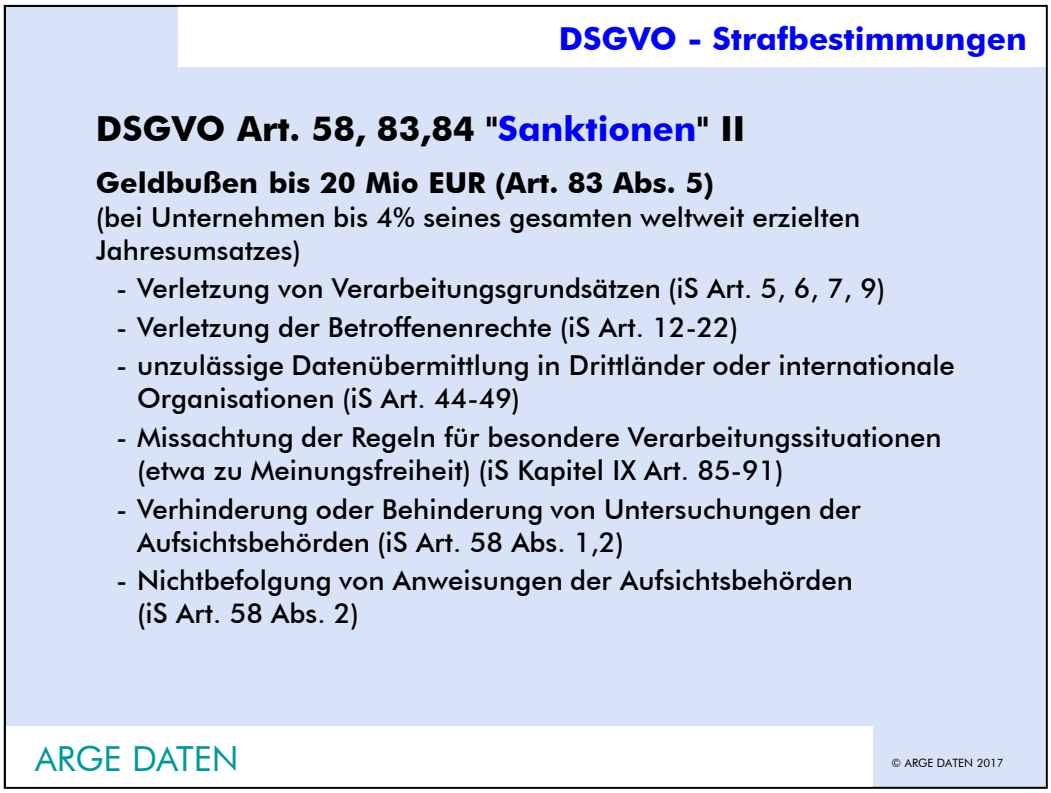
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

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.

DSGVO / DSAG 2018 - Strafbestimmungen

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

Mitgliedsstaaten können Geldbußen gegen Behörden abweichend regeln!

DSAG 2018 § 30 Abs. 4 "Behördensanktion"

- KEINE Strafen bei Datenschutzverletzungen durch Behörden

DSAG 2018 § 62 "ergänzende Sanktionen"

Verwaltungsstrafe bis 50.000,- Euro

- vorsätzliches Verschaffen eines Zugangs zu einer Datenverarbeitung
- vorsätzliches aufrecht Erhalten eines Zugangs
- Übermittlung unter vorsätzlicher Verletzung des Datengeheimnisses
- Verschaffen von personenbezogenen Daten unter Vortäuschung falscher Tatsachen
- Bildverarbeitung entgegen den Bestimmungen

! neu zu DSG 2000

ARGE DATEN

-

DSGVO / DSAG 2018 - Strafbestimmungen

DSAG 2018 § 62 "ergänzende Sanktionen" II

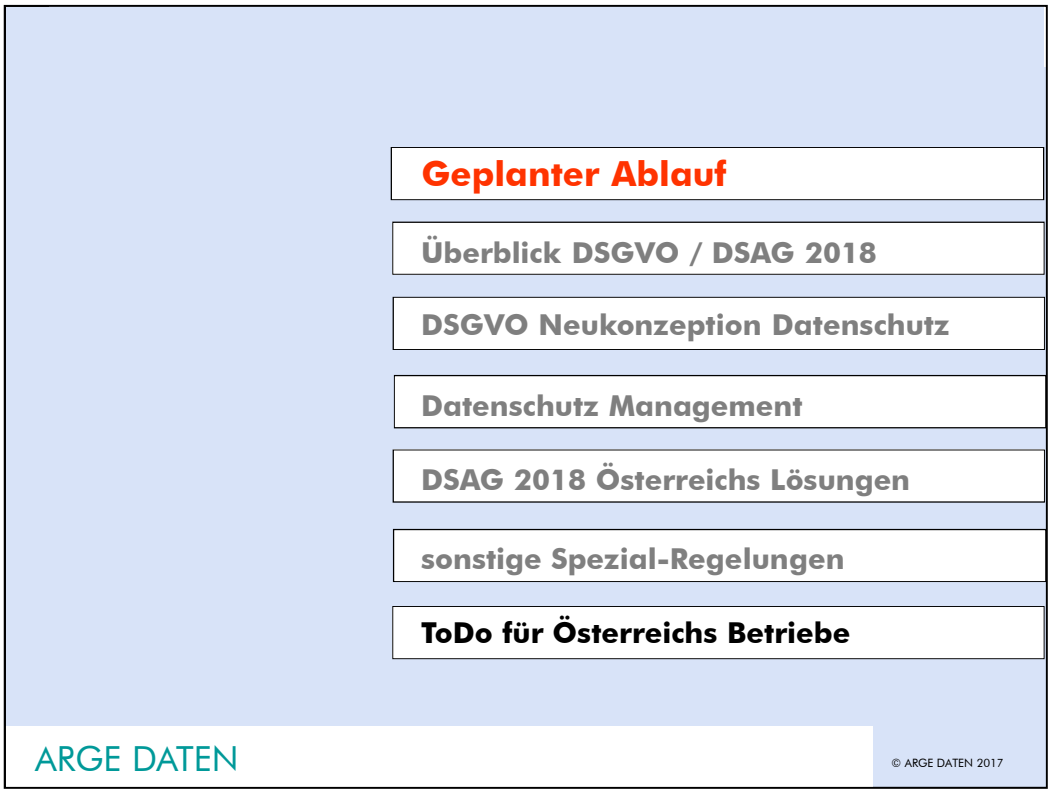
- Verweigerung der Einschau durch die Datenschutzbehörde
- Versuch ist strafbar
- Verfall von Datenträgern und Programmen kann ausgesprochen werden, wenn diese im Zusammenhang mit der Verwaltungsübertretung stehen
- verschaffen von personenbezogenen Daten unter Vortäuschung falscher Tatsachen
- Datenschutzbehörde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

ARGE DATEN

-

Datenverarbeitung in Gewinn- oder Schädigungsabsicht

DSAG 2018 § 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.


Geplanter Ablauf
Überblick DSGVO / DSAG 2018
DSGVO Neukonzeption Datenschutz
Datenschutz Management
DSAG 2018 Österreichs Lösungen
sonstige Spezial-Regelungen
ToDo für Österreichs Betriebe
ARGE DATEN
© ARGE DATEN 2017

-

DSGVO - Ready

Wie auf die DSGVO reagieren?

Sind alle innerbetrieblichen Verarbeitungstätigkeiten bekannt? Sind für alle Verarbeitungstätigkeiten dokumentiert?

Ist die Hauptniederlassung definiert? Welche Aufsichtsstelle wird in Zukunft zuständig sein?

Ist Unternehmen Teil einer Unternehmensgruppe? Wenn ja, sind in der Unternehmensgruppe BCR geplant?

Gibt es in der eigenen Branche / im eigenen Verband bestrebungen zu eigenen Verhaltensregeln? Wer wird sich an der Ausarbeitung beteiligen?

Ist internationaler Datenverkehr mit Dritt-Staaten vorhanden/geplant? Auf welcher Grundlage soll er stattfinden?

Sind die erforderlichen Informationsunterlagen für die Betroffenen vorbereitet? Sind sie leicht zugänglich?

ARGE DATEN

-

DSGVO - Ready

Wie auf die DSGVO reagieren? II

Können die Betroffenendaten in einem "technisch üblichen Format" bereit gestellt werden?

Ist ein verpflichtender Datenschutzbeauftragter erforderlich? Wenn nein, soll ein freiwilliger Datenschutz-beauftragter eingesetzt werden? Soll ein interner Mitarbeiter oder eine externe Stelle Datenschutzbeauftragter sein?

Wer wird für die Datenschutzfolgenabschätzung zuständig sein?

Wer wird Ansprechstelle für die Aufsichtsbehörde?

Sind die Meldeverfahren im Falle von Datenschutzverletzungen vorbereitet?

Ist zum Datenschutzmanagement eine Zertifizierung geplant?

ARGE DATEN

-

DSGVO - Ready

Wie auf die DSGVO reagieren? III

Ist die Vorbereitung auf Löschungswünsche ausreichend (inklusive der Verständigung früherer Empfänger)?

Sind Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sichergestellt?

Ist für die Umsetzung der DSGVO ausreichendes Budget bewilligt?

Oder werden lieber für zu erwartende Strafen Rückstellungen gemacht?

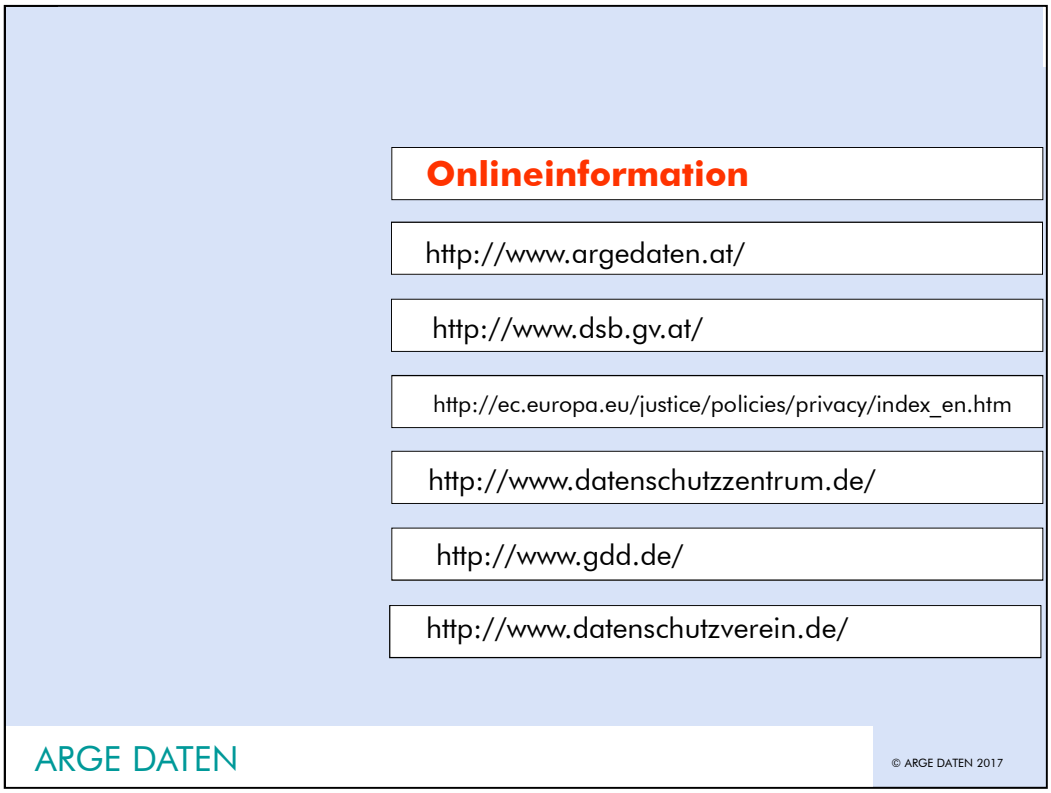
Wenn Sie auf alle diese Fragen eine klare Antwort haben, dann sind Sie für den

25. Mai 2018

bestens vorbereitet

ARGE DATEN

-



Weitere Datenschutzeinrichtungen

- http://www.argedaten.at/php/cms_monitor.php?q=ORG-DATENSCHUTZ

Weitere Rechtsinformationen

- http://www.argedaten.at/php/cms_monitor.php?q=RECHTS-LINKS

Entscheidungen finden sich im RIS:

- http://www.ris.bka.gv.at/dsk/ (Datenschutzkommission)
- http://www.ris.bka.gv.at/jus/ (OGH-Entscheidungen)

Technische Informationen

- Bundesamt fuer Sicherheit in der Informationstechnik (BSI) http://www.bsi.bund.de/
- CERT http://www.cert.org/
- Online-Sicherheitsstatus http://www.netcraft.com
- DFN Cert http://www.cert.dfn.de/
- Security-Server http://www.infoserversecurity.org
- Informationstechnik-Koordination (BKA Wien) http://www.cio.gv.at/


Ich danke für Ihre Aufmerksamkeit
ARGE DATEN
© ARGE DATEN 2017

-