DATENSCHUTZRECHT

DR. ANSGAR KORENG

GLIEDERUNG

1. Grundbegriffe des Datenschutzrechts
2. Datenschutzrechtliche Grundprinzipien

GRUNDBEGRIFFE

1. Personenbezogene Daten & betroffene Person
2. Anonymisierung
3. Pseudonymisierung
4. Besondere Kategorien personenbezogener Daten
5. Datenverarbeitung
6. Verantwortlicher
7. Auftragsverarbeiter
8. Dritter

ALLGEMEINES ZU DEN GRUNDBEGRIFFEN

- Grundlegende Definitionen finden sich in Art. 4 DS-GVO
- Bei Auslegungsschwierigkeiten oder nicht in Art. 4 definierten Begriffen empfiehlt sich ein Blick in die Erwägungsgründe

PERSONENBEZOGENE DATEN

- Art. 4 Nr. 1 DS-GVO.
- Zentraler Begriff des Datenschutzrechts.
- Datenschutzrecht ist nur anwendbar auf Daten, die Personenbezug aufweisen (Art. 2 Abs. 1 DS-GVO).
- Daten ohne jeden Personenbezug sind vom Datenschutzrecht nicht geschützt.
- Daher ist bei der Bearbeitung einer datenschutzrechtlichen Fragestellung stets an erster Stelle zu prüfen, ob überhaupt personenbezogene Daten vorliegen.

“

Es gibt „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr.“

”

BVerfGE 65, 1 (45)

PERSONENBEZOGENE DATEN

- D.h.: Auch wenn man der Meinung sein mag, dass ein bestimmtes Datum eigentlich unerheblich/uninteressant ist, gilt das Datenschutzrecht mit allen damit verbundenen Folgen.
- Das Datenschutzrecht differenziert nicht zwischen wichtigen und unwichtigen Daten. Die einzigen Daten, die besonders behandelt werden, sind die in Art. 9 und Art. 10 DS-GVO genannten.
- Voraussetzung für das Vorliegen personenbezogener Daten ist **Personenbezug**.

> „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"
>
> Art. 4 Nr. 1 DS-GVO

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

PERSONENBEZUG

- Datum muss einer lebenden (ErwG 27 DS-GVO) natürlichen Person zuzuordnen sein.
- Die Abgrenzung ist häufig schwierig: Vielfach kann ein spezielles Zusatzwissen zur Folge haben, dass ein an sich nicht personenbezogenes Datum doch Personenbezug erhält (relativer/absoluter Personenbezug?).

BEISPIEL IP-ADRESSE

- Beispiel: dynamische IP-Adresse (IPv4).
- Wird bei jeder Internetverbindung neu vergeben. Von außen nicht erkennbar, wer sich dahinter verbirgt.
- Aber: Access-Provider weiß, wem er die Adresse zugeordnet hat (jedenfalls: welchem Anschlussinhaber).
- „Personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG sind unter anderem die IP-Adressen, weil der Access-Provider einen Bezug zwischen den IP-Adressen und der Person des Nutzers herstellen kann “ (BGH, Urt. v. 26. November 2015, Az. I ZR 3/14, noch zum BDSG a.F.).

➢ Personenbezug jedenfalls für den Access-Provider.

RELATIVER/ABSOLUTER PERSONENBEZUG

- Daher besteht ein Meinungsstreit:
- Ist ein Datum allgemein „personenbezogen“, sobald irgendjemand es einer natürlichen Person zuordnen kann („**absoluter** Personenbezug“),
- oder ist es nur für denjenigen, der die Zuordnung vornehmen kann, personenbezogen und sonst nicht („**relativer** Personenbezug“)?

RELATIVER/ABSOLUTER PERSONENBEZUG

- ErwG 26 Satz 4 DS-GVO: Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.
- ErwG 30 DS-GVO: Die Identifizierbarkeit kann sich zudem mittels Zuordnung zu einer Kennnummer, zu Standortdaten zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen ergeben. Zu den Online-Kennungen zählen IP-Adressen und Cookie-Kennungen.

“Zum einen steht nämlich fest, dass die Anordnung, das streitige Filtersystem einzurichten, eine systematische Prüfung aller Inhalte sowie die Sammlung und Identifizierung der IP-Adressen der Nutzer bedeuten würde, die die Sendung unzulässiger Inhalte in diesem Netz veranlasst haben, wobei es sich bei diesen Adressen um personenbezogene Daten handelt, da sie die genaue Identifizierung der Nutzer ermöglichen.”

EuGH, Urteil vom 24.11.2011, Az. C-7/10 – „Scarlet Extended“

“ … dass eine dynamische IP-Adresse … für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen. ”

EuGH, Urt. v. 19. Oktober 2016, Az. C-582/14 – „Breyer“.

RELATIVER/ABSOLUTER PERSONENBEZUG

- Es kommt letztlich darauf an, „ob Mittel existieren, die vom Verantwortlichen nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die bei ihm befindlichen Daten mit den Zusatzinformationen einer anderen Person so zu verknüpfen, dass ihm eine Identifikation der betroffenen Person gelingt.“ (Kühling/Buchner/Klar/Kühling, 3. Aufl. 2020, DS-GVO Art. 4 Abs. 1 Rn. 28)
- i.E.: relativer Personenbezug.
- Also: z.B. IP-Adresse nicht für jedermann personenbezogenes Datum.

ANONYME DATEN

- Daten, die keiner natürlichen Person zugeordnet werden können.
- Solche Daten sind der Natur der Sache nach nicht personenbezogen.
- Auf sie ist die DS-GVO demgemäß nicht anwendbar.
- DS-GVO macht keine Vorgaben zum technischen Verfahren der Anonymisierung.

“Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.”

ErwG 26 DS-GVO.

PSEUDONYMISIERUNG

- Bsp.: Kennziffer in den Examensklausuren: Prüfer kann nicht zuordnen, JPA kann zuordnen.
- Folge: Personenbezug für die Stelle, die die Zuordnungsregel kennt – relativer Personenbezug.
- Letztlich bloße Sicherungsmaßnahme (arg. ex Art. 32 Abs. 1 lit. a DS-GVO).
- Senkung des Risikos für die betroffene Person (vgl. ErwG 28 DS-GVO).

“… 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”

Art. 4 Nr. 5 DS-GVO

BESONDERE KATEGORIEN

- Dies sind personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Art. 9 Abs. 1 DS-GVO; vgl. auch Art. 4 Nr. 13 bis 15 DS-GVO).
- Auch: Sensitive/sensible Daten.
- Solche Daten dürfen nur unter besonderen Bedingungen verarbeitet werden
- Der Gesetzgeber sieht hier ein besonderes Missbrauchsrisiko (nicht ohne jeden Zweifel, man denke an das Foto eines Brillenträgers)
- Die besonderen Bedingungen ergeben sich aus Art. 9 Abs. 2 DS-GVO

“Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.”

ErwG 51 Satz 1 DS-GVO

> Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist.

Art. 10 DS-GVO

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

DATENVERARBEITUNG

- Ebenfalls zentraler Begriff in der DS-GVO, da die DS-GVO die Verarbeitung personenbezogener Daten reguliert.
- Denkbar weit gefasst.

> (Jeder) 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

Art. 4 Nr. 2 DS-GVO

Begriff der „Verarbeitung“

“(Jeder) 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”

Art. 4 Nr. 2 DS-GVO

Begriff der „Verarbeitung“

“

(Jeder) Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten

”

Art. 4 Nr. 2 DS-GVO

Begriff der „Verarbeitung“

VERANTWORTLICHER

- Ist „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“ (Art. 4 Nr. 7 DS-GVO).
- Zentraler Begriff der DS-GVO, weil die Pflichten aus der Verordnung im Wesentlichen den Verantwortlichen treffen.
- Wesentliche Kriterien ergeben sich aus dem Working Paper 169 der Artikel-29-Datenschutzgruppe (noch zur alten Rechtslage, aber im Wesentlichen übertragbar).
- Bestimmung des „Verantwortlichen“ dient dazu, die Verantwortung für die Einhaltung des Datenschutzes zuzuweisen und den Schutz der Rechte der betroffenen Personen sicherzustellen (Artikel-29-Datenschutzgruppe, WP 169, S. 6 f.).

VERANTWORTLICHER: RISIKOBASIERTER ANSATZ

- Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.
- (Art. 24 Abs. 1 DS-GVO)
- Zentrale Norm für die Pflichten des Verantwortlichen.

VERANTWORTLICHER

- Auf die rechtliche Organisationsform kommt es nicht an.
- Zurechnung von Handlungen natürlicher Personen nach den allgemeinen Grundsätzen des Zivil-/Verwaltungs-/Strafrechts.
- Keine Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen in der DS-GVO (aber im BDSG!)
- DS-GVO anerkennt ausdrücklich die Möglichkeit einer gemeinsamen Verantwortlichkeit (siehe auch Art. 26 DS-GVO, sog. „Joint Controllership“).

AUFTRAGSVERARBEITER

- „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“ (Art. 4 Nr. 8 DS-GVO).
- Nähere Ausgestaltung in Art. 28 DS-GVO. Voraussetzung ist insbesondere eine Auftragsverarbeitungsvereinbarung (AVV).
- Wesentliche Aspekte der Auftragsverarbeitung:
  - Auftragsverarbeiter ist nicht Verantwortlicher, er darf nur im Rahmen der Weisungen des Auftraggebers verarbeiten (Art. 29 DS-GVO).
  - Ermöglicht die Auslagerung von Datenverarbeitungsvorgängen an Dienstleister (Rechenzentren etc.).
  - Privilegiert die Datenübermittlung und Datenverarbeitung im Auftragsverarbeitungsverhältnis (keine eigene Rechtsgrundlage für die Übermittlung an Auftragsverarbeiter und für Verarbeitung durch Auftragsverarbeiter erforderlich, wobei das derzeit streitig ist, vgl. im Einzelnen Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 28 Rn. 15-23).

DRITTER

- „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten“ (Art. 4 Nr. 10 DS-GVO).
- Sozusagen jeder, der nicht Verantwortlicher oder Auftragsverarbeiter oder betroffene Person ist (also eigentlich „Vierter“).
- Problematisch in dem Kontext: Stellen innerhalb des Verantwortlichen (Betriebsrat, Personalrat?).

GRUNDPRINZIPIEN

1. Verbot mit Erlaubnisvorbehalt
2. Verarbeitung nach Treu & Glauben
3. Transparenz
4. Zweckbindung
5. Datenminimierung
6. Richtigkeit
7. Speicherbegrenzung
8. Integrität & Vertraulichkeit
9. Rechenschaftspflicht

GRUNDPRINZIPIEN

- Ergeben sich im Wesentlichen aus Art. 5 DS-GVO (und Art. 6 DS-GVO bzgl. Verbot mit Erlaubnisvorbehalt).
- Konkretisieren Art. 16 Abs. 1 AEUV, Art. 8 Abs. 2 GrCh und Art. 8 EMRK.
- werden in zahlreichen Vorschriften der DS-GVO aufgegriffen und konkretisiert.
- Ergänzen die Betroffenenrechte um eine objektive Dimension.
- Näher Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 1.

VERBOT MIT ERLAUBNISVORBEHALT

- Daten müssen „auf rechtmäßige Weise“ verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO).
- Verweist der Sache nach auf Art. 6 DS-GVO.
- Grundlegendes Prinzip des Datenschutzrechts: Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, es besteht ausnahmsweise ein Erlaubnistatbestand.
- Niedergelegt in Art. 6 DS-GVO (bzw. z.B. § 3 Abs. 1 SächsDSUG und vergleichbaren Normen).
- Ergibt sich für öffentliche Stellen letztlich auch schon aus der grundrechtlichen Systematik des Rechts auf informationelle Selbstbestimmung (Eingriffe bedürfen gesetzlicher Grundlage).
- Die Einzelheiten von Art. 6 DS-GVO werden in der nächsten Einheit besprochen.

TREU & GLAUBEN

- Art. 5 Abs. 1 lit. a, 2. Var. DS-GVO (auch: Art. 8 Abs. 2 S. 1 GRCh, früher: Art. 6 Abs. 1 lit. a DSRL).
- Entspricht nicht dem Begriff „Treu und Glauben“ des deutschen Zivilrechts, sondern ist autonom auszulegen.
- Definition fand sich früher in ErwG 38 DSRL: Datenverarbeitung nach Treu und Glauben setzt voraus, „dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei Ihnen erhoben werden.“
- Ist heute allerdings vom Transparenzgebot umfasst. Daher ist der Anwendungsbereich des Grundsatzes von „Treu und Glauben“ heute fraglich („Auffangtatbestand“, Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 17).

TRANSPARENZGEBOT

- Art. 5 Abs. 1 lit. a, 3. Var. DS-GVO.
- Nähere Erläuterungen in den ErwG 39, 58, 60: deckt sich insofern weitestgehend mit den Vorgaben aus Art. 12 bis 14 DS-GVO dazu, in welcher Form und in welchem Umfang betroffene Personen über die Datenverarbeitung aufgeklärt werden müssen.
- Im Ergebnis geht es darum, dass die betroffene Person in die Lage versetzt werden muss, zu wissen, dass, in welcher Form und zu welchem Zweck welche ihrer Daten verarbeitet werden.

ZWECKBINDUNG

- Zweckbindungsgrundsatz folgt aus Art. 5 Abs. 1 lit. b DS-GVO, ergibt sich auch schon aus auch in Art. 8 Abs. 2 S. 1 GrCh.
- „Kernbestandteil des Datenschutzrechts“ (Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 21 m.w.N.)
- Hat zum Inhalt, dass schon bei der Datenerhebung der Zweck der Datenverarbeitung festgelegt sein muss. Der Zweck bildet dann den Maßstab für Art, Umfang und Dauer der Datenverarbeitung.
- Zweckfestlegung muss nicht einer bestimmten Form genügen, aber Rechenschaftspflicht beachten (Art. 5 Abs. 2 DS-GVO, dazu noch später).
- Die Grundsätze der Datenminimierung und der Speicherbegrenzung nehmen insofern Bezug auf den Zweckbindungsgrundsatz.
- Das Datenschutzrecht sieht allerdings punktuelle Durchbrechungen des Zweckbindungsgrundsatzes vor (Art. 5 Abs. 1 lit. b Hs. 2 DS-GVO; Art. 6 Abs. 4 DS-GVO).

DATENMINIMIERUNG

- Ehemals „Datensparsamkeit“.
- Datenminimierung hat den Verarbeitungszweck als Bezugspunkt, es dürfen also nur die Daten erhoben werden, die in Bezug auf den Zweck erforderlich sind.
- Daten dürfen nicht verarbeitet werden, wenn der Verarbeitungszweck auch ohne sie erreicht werden kann (Kühling/Buchner/Herbst, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 57).
- Konkretisierung u.a. in in Art. 25 Abs. 1 DS-GVO und in Art. 89 Abs. 1 DS-GVO.

RICHTIGKEIT

- Art. 5 Abs. 1 lit. d DS-GVO.
- Hat nur bei Tatsachen Relevanz, nicht bei Wertungen (denn die können nicht „richtig“ sein).
- „Richtigkeit“ hat Bezug zum Verarbeitungszweck: Das Protokoll einer Gerichtsverhandlung ist auch richtig, wenn der Zeuge gelogen hat. Die Richtigkeit bezieht sich auf die korrekte Wiedergabe der Zeugenaussage, nicht auf die inhaltliche Richtigkeit dessen, was der Zeuge gesagt hat.
- Grundsatz der Richtigkeit Weist einen engen Bezug zu Art. 16 DS-GVO (Recht auf Berichtigung) auf.

SPEICHERBEGRENZUNG

- Art. 5 Abs. 1 lit. e DS-GVO: Zeitliche Grenze für die Speicherung personenbezogener Daten.
- Weist, wie schon ausgeführt, engen Bezug zum Zweckbindungsgrundsatz auf, weil sich die Speicherdauer auf den Zweck der Verarbeitung bezieht.
- Solange der Zweck der Datenverarbeitung die Speicherung erfordert, steht der Speicherung der Grundsatz der Speicherbegrenzung nicht entgegen.
- Die Einhaltung des Grundsatzes soll auch dadurch sichergestellt werden, dass der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfung der personenbezogenen Daten vorsieht (ErwG 39 DS-GVO).
- Weist engen Bezug zu Art. 17 DS-GVO („Recht auf Löschung“) auf.

INTEGRITÄT & VERTRAULICHKEIT

- Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO) erfordert insbesondere geeignete technische und organisatorische Maßnahmen.
- Findet seine nähere Konkretisierung in Art. 32 DS-GVO und hat auch einen engen Bezug zu Art. 33, 34 DS-GVO („data breach notification“).

RECHENSCHAFTSPFLICHT

- Art. 5 Abs. 2 DS-GVO.
- In der Praxis bedeutender Grundsatz des Datenschutzrechts: Der Verantwortliche muss die Grundsätze des Art. 5 Abs. 1 DS-GVO einhalten und dies nachweisen können.
- Nachweispflicht hat Bedeutung im Hinblick auf Überprüfungen durch die Aufsichtsbehörden, die nach Art. 58 Abs. 1 lit. a auch die Befugnis haben, den Verantwortlichen zur Bereitstellung von Informationen anzuweisen.
- Konkrete Form ist nicht vorgeschrieben.
- Enger Zusammenhang zu Art. 30 DS-GVO (Verzeichnis der Verarbeitungstätigkeiten).
- JI-RL kennt darüber hinausgehend noch die Protokollierung (Art. 25 JI-RL; § 32 SächDSUG), spricht dafür, dass die DS-GVO nicht grundsätzlich eine Protokollierung aller Datenverarbeitungsvorgänge erfordert.

Ende