SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Überblick zur Europäischen Datenschutz-Grundverordnung

Agenda

Teil I

- Grundlegende Aspekte
- Umsetzung der DS-GVO
- Die neue Datenschutz-Aufsichtsbehörde
- Gliederung der DS-GVO und Anwendungsbereich
- Grundlagen
- Grundsätze der Datenverarbeitung
- Rechtsgrundlagen der Datenverarbeitung
- Betroffenenrechte und Rechtsschutz
- Haftung und Bußgeld

Ausgangslage (1)

Richtlinie 95/46 EG

- Problematische Aspekte laut Europäischer Kommission (Mitteilung vom 04.11.2010) u. a. in den Bereichen:
  - Beherrschung der Auswirkungen neuer Technologien (1998 ging Google online, seit 2004 gibt es Facebook)
  - Binnenmarktdimension des Datenschutzes: uneinheitliches Niveau
  - Globalisierung und internationale Datentransfers
  - institutioneller Rahmen zur Rechtsdurchsetzung

Ausgangslage (2)

Lösung:

„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)“

Ziele der DS-GVO

- Harmonisierung, gleichmäßig hohes Datenschutzniveau
  - ein **einheitliches Datenschutzrecht** für in der EU tätige Unternehmen (inkl. Marktortprinzip)
  - kein „Forum-Shopping“ möglich (Datenverarbeitung in Mitgliedstaat mit geringstem Datenschutzniveau)
  - „One-Stop-Shop“; **konzentrierte Zuständigkeit** der Aufsichtsbehörden (federführende Aufsichtsbehörde am Hauptsitz von Unternehmen)
  - EU-Kommissarin Jourova: Unternehmen sparen jährlich 2,3 Mrd. €
  - Stärkung des Binnenmarktes
- Modernisierung (Berücksichtigung Globalisierung/ Internet/ Big Data, Wirtschaft 4.0)

Anwendung der DS-GVO Art. 99

- Seit dem 25. Mai **2016**: DS-GVO **in Kraft**
- Ab dem 25. Mai **2018**: DS-GVO **anzuwenden**
  - in **allen Teilen verbindlich** und **unmittelbare Geltung** in **jedem** Mitgliedstaat (anders als Richtlinie von 1995)
  - bis dahin Fortgeltung jetziger Vorschriften und Anpassungszeitraum, auch für bereits begonnene Verarbeitungen
  - ab 25. Mai 2018 besteht ggf. ein Anwendungsvorrang der DS-GVO

Geltung der DS-GVO

- Viele **Regelungsspielräume** zugunsten der Mitgliedstaaten
  - teilweise zwingend umzusetzen (z. B. zu Zertifizierungen, Art. 42, 43)
  - oder nur Optionen (z. B. kann das Alter für die Einwilligungsfähigkeit von 16 auf bis zu 13 Jahre herabgesetzt werden, im BDSG 2018 aber nicht umgesetzt)

- Besondere Regelungsspielräume im Bereich der klassischen Staatsaufgaben nach Art. 6 Abs. 1 lit. e), Abs. 2 und 3
  Gesetze **beibehalten** oder **einführen**
  Spezielle Befugnisse u. a. für Medien, Presse, Beschäftigte, Forschung

- Regelungsspielräume beschränken die Harmonisierung (**Grund**-Verordnung)!

- DS-GVO ist insgesamt im nicht-öffentlichen Bereich wesentlich verbindlicher als im öffentlichen Bereich

Weitere EU-Regelungen

- Entwurf einer Verordnung über Privatsphäre und elektronische Kommunikation (**ePrivacy-Verordnung**)

- **Delegierte Rechtsakte** (Art. 92)
  Befugnis der **EU-Kommission**, Rechtsakte mit allgemeiner Geltung zu erlassen (z. B. Anforderungen zu spezif. Zertifizierungen, Art. 43 Abs. 8, Bildsymbole im Rahmen der Informationspflicht, Art. 12 Abs. 8)

- **Durchführungsrechtsakte** (Art. 92)
  Befugnis der **EU-Kommission**, die Durchführung der DS-GVO durch Rechtsakt zu regeln (z. B. technische Standards für Zertifizierungsverfahren, Art. 43 Abs. 9, Beschluss zu angemessenem Schutzniveau im Drittstaat, Art. 45 Abs. 3)

- **Leitlinien und Empfehlungen** (Art. 70 Abs. 1 lit. f))
  durch den **Europäischen Datenschutzausschuss**, (teilweise Übernahme von Dokumenten der Art.-29-Gruppe)

Regelungen zur Ergänzung der DS-GVO

- **Länderebene**
  - Entwicklung neuer **Landesdatenschutzgesetze**
  - Anpassung von zahlreichen **spezialgesetzlichen Regelungen**

- **Bundesebene**
  „Datenschutz-Anpassungs- und Umsetzungsgesetz EU - DSAnpUG-EU“ (BGBl. I Nr. 44 v. 5.7.2017, S. 2097);
  darin enthalten: **BDSG 2018**,
  -Anpassung von **spezialgesetzlichen Regelungen** (u.a. SGB)

Umsetzung in Sachsen-Anhalt

- **Neufassung des allgemeinen Datenschutzrechts :**

  1. Regelungen zur Organisationsfortentwicklung des Landesbeauftragten für den Datenschutz (LfD)
     darin: Konkretisierung der „völligen Unabhängigkeit“, z. B. eigener Einzelplan und Personalhoheit, LfD bleibt Teil der unmittelbaren Landesverwaltung; LfD erhält **Anordnungsbefugnis** gegenüber Behörden (Inkrafttreten am 06.05.2018)

  2. Gesetz zur Ausfüllung der DS-GVO (DSAG LSA, Ende 2018)
     bis dahin: DSG-LSA i. d. F. vom 6. Mai 2018 (soweit kein Anwendungsvorrang der DS GVO)

  3. Gesetz zur Umsetzung der JI-Richtlinie (DSUG LSA, Herbst 2018)

- Anpassung **Fachgesetze** des bereichsspezifischen Datenschutzes durch die zuständigen Ressorts

Erforderliche Anpassungen in Bundesgesetzen

Betrifft über 100 Einzelgesetze (BT.-Drs. 18/13581, S. 10 ff), z. B.:

- Bundesmeldegesetz
- Bürgerliches Gesetzbuch
- Einkommensteuergesetz
- Gendiagnostikgesetz
- Gewerbeordnung
- Informationsfreiheitsgesetz
- SGB III, V, VIII, IX und XI
- Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern
- Handwerksordnung
- Kreditwesengesetz

Die neue Datenschutz-Aufsichtsbehörde

- Völlige **Unabhängigkeit**, Art. 52 Abs. 1
  Mitgliedstaat **muss** Ressourcen **gewährleisten**, Art. 52 Abs. 4
  - Personalhoheit, Art. 52 Abs. 5
  - Eigener, jährlicher, öffentlicher Haushaltsplan, Art. 52 Abs. 6

- Neue **zusätzliche Pflichtaufgaben**, Art. 57, 58, insbesondere
  - Anordnungsbefugnis auch gegenüber Behörden
  - Weitere Beratungspflichten gegenüber **Behörden und Unternehmen** (z. B. bei der Datenschutz-Folgenabschätzung)
  - Europaweite Zusammenarbeit mit **kurzen Fristen**
  - Räumlich **erweiterter Tätigkeitsbereich** (Marktortprinzip)

Gliederung der DS-GVO (1)

- Text beginnt mit **173 Erwägungsgründen** (EG)
  diese enthalten vereinzelt verbindliche Regelungen, dienen aber insbesondere der **Auslegung** der folgenden Artikel

  Es folgen **99 Artikel** mit umfangreichen Regelungen

  Bsp.: **Art. 6 Abs. 1 lit. f)** gestattet die Verarbeitung personenbezogener Daten, wenn ein berechtigtes Interesse vorliegt. **EG 47** erläutert das berechtigte Interesse.

Gliederung der DS-GVO (2)

Kapitel I:	Allgemeine Bestimmungen
Kapitel II:	Grundsätze
Kapitel III:	Rechte der betroffenen Person
Kapitel IV:	Verantwortlicher und Auftragsverarbeiter
Kapitel V:	Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen
Kapitel VI:	Unabhängige Aufsichtsbehörden
Kapitel VII:	Zusammenarbeit und Kohärenz
Kapitel VIII:	Rechtsbehelfe, Haftung und Sanktionen
Kapitel IX:	Vorschriften für besondere Verarbeitungssituationen
Kapitel X:	Delegierte Rechtsakte und Durchführungsrechtsakte
Kapitel XI:	Schlussbestimmungen

Sachlicher Anwendungsbereich, Art. 2

- Die DS-GVO und das BDSG 2018 gelten für die:
  - ganz/teilweise automatisierte Verarbeitung **personenbezogener Daten**
  - nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen (inkl. Akten, soweit sie nach bestimmten Kriterien geordnet sind; vgl. Art. 4 Nr. 6, EG 15, § 1 Abs. 1 BDSG 2018)

- Keine Geltung bei Datenverarbeitungen, die
  - vom **EU-Recht ausgenommen** sind (z. B. Nachrichtendienste)
  - unter die gemeinsame **Außen- und Sicherheitspolitik** fallen
  - ausschließlich **persönliche / familiäre Tätigkeit** von natürlichen Personen sind
  - unter die **JI-Richtlinie** fallen (Strafverfolgung, polizeiliche Gefahrenabwehr)
  - die Bereitstellung öffentlicher elektronischer **Kommunikationsdienste** in öffentlichen Netzen betreffen, Art. 95 (hier gelten noch: E-Privacy-Richtlinie, TMG, TKG; die Verordnung über Privatsphäre und elektronische Kommunikation E-Privacy-Verordnung steht noch aus)

Grundlagen

- Europarecht: Art. 16 AEUV
  -Abs. 1: Anspruch auf Schutz personenbezogener Daten
  -Abs. 2: Rechtsgrundlage für den Erlass der EU-Regelungen

- Völkerrechtliche Basis: Art. 8 EMRK
  Recht auf Achtung des Privat- und Familienlebens

- Grundrechtlicher Hintergrund
  Art. 7 EU GRCh (Familienleben)
  Art. 8 EU GRCh (Schutz personenbezogener Daten)

Grundsätze, Art. 5

- Rechtmäßigkeit
- Treu und Glauben
- Transparenz
- Richtigkeit
- Zweckbindung
- Datenminimierung
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Verbot mit Erlaubnisvorbehalt (1)

EU-Grundrechtecharta, Art. 8 Abs. 2:

Personenbezogene Daten „dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“.

Daraus folgt: weiterhin **Verbot mit Erlaubnisvorbehalt**

- Art. 6 Abs. 1 : Verarbeitung ist **nur rechtmäßig**, **wenn**

  -eine Einwilligung vorliegt oder

  -eine andere in der Vorschrift genannte Fallgruppe erfüllt ist.

  Ansonsten ist die Verarbeitung verboten!

- Einfache und komplexe Datenverarbeitungen werden gleich behandelt.

Verbot mit Erlaubnisvorbehalt (2)

Verarbeitung nur zulässig, wenn eine der **folgenden Fallgruppen** nach Art. 6 Abs. 1 erfüllt ist:

- Einwilligung
- Vertrag
- Rechtliche Verpflichtung
- Lebenswichtige Interessen
- Öffentliches Interesse/hoheitliche Aufgaben
- Verarbeitung zur Wahrung berechtigter Interessen, unter Interessenabwägung mit schutzwürdigen Interessen und Grundrechten der Betroffenen (insbes. b. Kindern)

Weitere Prinzipien

- **Datenminimierung** (Art. 5 Abs. 1 lit. c))
  dem Zweck angemessen, notwendiges Maß
  Umsetzung durch angemessene technisch-organisatorische Maßnahmen: Technikgestaltung / Voreinstellungen (Art. 25), data protection by design/by default

- **Speicherbegrenzung**, Art. 5 Abs. 1 lit. e))
  Speicherung nur so lange, wie es für die Zwecke, für die verarbeitet wird, erforderlich ist

  Diese Vorgaben sind Ausdruck der **Erforderlichkeit**.

  Umsetzung: Verhältnismäßigkeitsgrundsatz

Weitere Prinzipien

- **Zweckbindung** (Art. 5 Abs. 1 lit. b))
  Verarbeitung nur für festgelegte, eindeutige Zwecke;
  Zweckänderung ohne Einwilligung nur wenn diese mit Ursprungszweck vereinbar (Privilegierung für im öffentlichen Interesse liegende Archiv-, Forschungs- und Statistikzwecke, Art. 89)
  Zweckänderung ggf. möglich nach Art. 6 Abs. 4 :
  Verantwortlicher prüft die Vereinbarkeit mit dem Erhebungszweck

- **Richtigkeit** (Art. 5 Abs. 1 lit. d))
  Berichtigungsrecht (Art. 16) und Löschungsrecht (Recht auf „Vergessenwerden“, Art. 17)
  Pflicht des Verantwortlichen, alle angemessenen Maßnahmen zu treffen, damit die Daten sachlich richtig und aktuell sind

Weitere Prinzipien

- **Verantwortlichkeit des Verantwortlichen** (Art. 24)
  Ausdrückliche Verpflichtung des Verantwortlichen zu Maßnahmen zur Umsetzung der Grundsätze aus Art. 5 DS-GVO und zum Nachweis unter Berücksichtigung von Eintrittswahrscheinlichkeit und Schwere des Risikos (risikobasierter Ansatz der DS GVO, s. EG 74 und 76)
  Hinweise zu Risiken in EG 75:
  u. a. Diskriminierung, finanzieller Verlust,
  Die Verantwortung gebietet ein **Datenschutzmanagement**

- **Integrität und Vertraulichkeit** (Art. 5 Abs. 1 lit. f))
  Geeignete techn.-organisator. Maßnahmen gegen Verlust, unbefugte oder unrechtmäßige Verarbeitung

- **Datensicherheit** (Art. 32, EG 78)
  angemessene Maßnahmen unter Berücksichtigung von
  --Stand der Technik, Implementierungskosten
  --Art, und Umfang der Verarbeitung,
  --Eintrittswahrscheinlichkeit und Schwere des Risikos
  für die Rechte und Freiheiten des Betroffenen

Weitere Prinzipien

- **Rechenschaftspflicht** (Art. 5 Abs. 2)
  Der Verantwortliche muss die Grundsätze des Art. 5 einhalten
  (verstärkt durch Bußgelddrohung in Art. 83 Abs. 5 lit. a))
  Er muss die Einhaltung nachweisen
  Maßnahmen und Strategien sind zu dokumentieren

- **Treu und Glauben und Transparenz**
  -Treu und Glauben als Vorgabe aus Art. 8 Abs. 2 EU GRCh
  -Informationspflichten und Auskunftsrechte (Art. 12 ff)

Einwilligung, Art. 7, EG 32, 33, 42, 43 (1)

Anforderungen an die Einwilligung (Art. 7)

- Einwilligung muss unmissverständlich sein
- in einfacher Sprache, verständlich und leicht zugänglich
- hervorgehoben (von anderen Sachverhalten getrennt)
- nicht notwendig schriftlich, auch elektronisch oder mündlich, aber nachzuweisen
- „opt out“ (Widerspruchslösung) ist out! (eindeutige bestätigende Handlung, EG 32)
- jederzeit einfach widerrufbar (vorheriger Hinweis nötig)
- über Verarbeiter und Zwecke der Verarbeitung ist zu informieren
- In Bezug auf Kinder ist ggf. Art. 8 zu beachten

Einwilligung, Art. 7, EG 32, 33, 42, 43 (2)

Freiwilligkeit

- Einwilligung gilt i. d. R. nicht als erteilt, wenn die Erfüllung eines Vertrages, einschließlich einer Dienstleistung, von der Einwilligung in eine hierfür nicht erforderliche Datenverarbeitung abhängig ist (**Koppelungsverbot**)
- Freie Wahl / nachteilsfreie Verweigerungsmöglichkeit notwendig
- Einwilligung ist „**keine gültige Rechtsgrundlage**“, wenn „**ein klares Ungleichgewicht besteht**“ und es deshalb unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben würde (EG 43) (z. B. **Behörde**, Beschäftigungs-, Miet-, oder Versicherungsverhältnis)
- Alte Einwilligungen gelten grundsätzlich weiter (EG 171). Sie sollten aber den neuen Bedingungen entsprechen (informiert, auch über Widerruf). (ggf. prüfen)

Betroffenenrechte - Überblick

- Erweiterte **Informationspflichten**, Art. 13, 14
- Recht auf **Auskunft**, Art. 15 - auf Antrag
- Recht auf **Berichtigung**, Art. 16
- Recht auf **Löschung**, Art. 17 Abs. 1
  Neues Recht auf Vergessenwerden, Art. 17 Abs. 2
- Recht auf **Einschränkung** der Verarbeitung, Art. 18
- Neues Recht auf **Datenübertragbarkeit**, Art. 20
- **Widerspruchsrecht**, Art. 21

Beschränkung der Betroffenenrechte, Art. 23

…ist möglich aufgrund **mitgliedstaatlicher Rechtsvorschriften,** sofern **Wesensgehalt** der Grundrechte und Grundfreiheiten geachtet wird und sie eine notwendige und **verhältnismäßige Maßnahme** darstellen, die unter anderem Folgendes sicherstellt:

a) nationale Sicherheit
c) öffentliche Sicherheit
d) Strafverfolgung
e) wichtige Ziele allgemeinen öffentlichen Interesses
i) Rechte und Freiheiten anderer Personen
j) Durchsetzung zivilrechtlicher Ansprüche

ist in **§§ 32 – 37 BDSG-2018** geregelt. Landesregeln sind im DSAG zu erwarten.

Rechtsschutz

- **Beschwerde bei der Aufsichtsbehörde**, Art. 77
  Beschwerderecht für Betroffene **bei „einer Aufsichtsbehörde“**,
  („insbesondere“ am gewöhnlichen Aufenthaltsort oder Arbeitsplatzort oder am Platz des Verstoßes)
- **Klagerecht gegen die Aufsichtsbehörde**, Art. 78
- **Direktes Klagerecht**, Art. 79
  gegen die für die Verarbeitung Verantwortlichen oder gegen deren Auftragsverarbeiter
- **Vertretung betroffener Personen durch Verbände möglich**, Art. 80 Abs. 1
- **Verbandsklagerecht** , Art. 80 Abs. 2
  Fortgeltung § 2 Abs. 2 Nr. 11 UKlaG

Haftung und höhere Bußgelder

- **Haftung** auf Schadensersatz mit Beweislastumkehr nach Art. 82
- Verstöße gegen organisatorische Regelungen, Art. 83 Abs. 4
  - Geldbußen von bis zu **10.000.000 EUR**
  - im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs
- Verstöße gegen Grundsätze und Betroffenenrechte etc., Art. 83 Abs. 5
  - Geldbußen von bis zu **20.000.000 EUR**
  - im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres
- Höhe der Geldbuße muss im Einzelfall **wirksam, verhältnismäßig und abschreckend** sein, Art. 83 Abs. 1
- Keine Geldbußen gegenüber öffentlichen Stellen (Ausn.: Wettbewerbsunternehmen)

Agenda

Teil II

- Terminologie
- Besondere Kategorien von Daten
- Informationspflichten
- Dokumentation und Nachweis
- Meldepflichten
- Datenschutz-Folgeabschätzung
- Datenschutzbeauftragte
- Auftragsverarbeiter
- Technisch-organisatorische Maßnahmen

Terminologie, Art. 4 DS-GVO

- **Personenbezogene Daten**
  Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, Maßstab: **Identifizierbarkeit**
  direkt oder indirekt mittels Kennung (Name, Nummer, Merkmale)
  irgendein Dritter kann Identifizierung wahrscheinlich durchführen
- **Verantwortlicher**
  …ist, wer allein oder gemeinsam mit anderen über die Zwecke und die Mittel der Verarbeitung entscheidet
  Auftragsverarbeiter ist, wer im Auftrag des Verantwortlichen agiert
  Verarbeitung
  umfasst sind u.a.: Erheben, Speichern, Verändern, Abfragen, Verwenden, Übermitteln, Bereitstellen, Verknüpfen, Löschen
- **Pseudonymisierung**
  Zuordnung durch Hinzuziehen zusätzlicher Informationen
  Zuordnungsfunktion ist gesondert aufbewahrt („file Trennung“)
- Insgesamt 26 Begriffsdefinitionen

Besondere Kategorien personenbezogener Daten, Art. 9 DS-GVO

- **Besondere Kategorien:**
  Rassische u. ethnische Herkunft, politische Meinung, Religion, Weltanschauung, Gewerkschaft, Sexualleben, genetische oder biometrische Daten, Gesundheitsdaten

- **Art. 9 Abs. 1** : Verarbeitung grundsätzlich verboten.

- **Ausnahmen: Art. 9 Abs. 2 :**
  Einwilligung, Arbeitsrecht, soziale Sicherheit, lebenswichtige Interessen, Gesundheits- und Sozialbereich

- **Art. 9 Abs. 4**
  Mitgliedsstaat kann zusätzlich Bedingungen und Beschränkungen regeln (u. a. InfSchG, SGB V, MVollzG, KRG, GDG)

Art. 9 Abs. 2 DS-GVO

Ausnahmen nach Art. 9 Abs. 2: (u.a.)

- **Einwilligung:**
  nicht konkludent, sondern ausdrücklich
  gesondert: Entbindung von beruflicher Schweigepflicht (2 Schranken)
- zur Ausübung von Rechten und Pflichten aus dem **Arbeitsrecht** und der **sozialen Sicherheit**
  z. B. Religion für Kirchensteuer, Arbeitsschutz
- zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**
- **Schutz lebenswichtiger Interessen** (Notfälle)
- **offensichtlich vom Betroffenen öffentlich gemacht**
- **Erhebliches öffentliches Interesse**
  Gesetz im Gemeinschaftsinteresse (z. B. Gefahrenabwehr)
- **Gesundheitsvorsorge und –versorgung**
  Gesundheits- und Sozialbereich (u. a. Patientenbehandlung)
  Art. 9 Abs. 3: Fachpersonal (berufl. schweigeverpflichtet) verarbeitet bzw. ist verantwortlich
- **Öffentliche Gesundheit**

Transparente Information, Art. 12 DS-GVO

- **Art. 12** verpflichtet den Verantwortlichen zu Information und Kommunikation
  Maßnahmen geboten, alle Informationen
  leicht zugänglich, in klarer und verständlicher Sprache,
  grundsätzlich unentgeltlich bereitzustellen, für:

- **Datenerhebung beim Betroffenen**, Art. 13
- **Datenerhebung bei Dritten**, Art. 14
- **Auskunftsrecht**, Art. 15
- **Weitere Rechte** aus Art. 16 bis 22 und 34 (Berichtigung, Löschung, Datenübertragbarkeit, Widerspruchsrecht, Benachrichtigung von der Verletzung des Datenschutzes)

Informationspflichten bei der Erhebung beim Betroffenen Art. 13, EG 58 ff (1)

- **Informationsinhalte (Abs. 1)**:
  -Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
  -Zweck und Rechtsgrundlage der Verarbeitung,
  -Interessenabwägung (bei Verarbeitung nach Art. 6 Abs. 1 lit. f))
  -(ggf. Kategorien von) Empfänger
  -ggf. Drittstaatentransfer
- **Infos für faire und transparente Verarbeitung (Abs. 2)**
  -Dauer der Speicherung oder Kriterien der Festlegung der Dauer
  -Hinweis auf Betroffenenrechte: (u. a.)
  --Auskunftsrecht
  --Recht auf Widerruf der Einwilligung
  --Beschwerderecht bei der Aufsichtsbehörde
  --Info, ob Betroffener verpflichtet ist, Daten bereit zu stellen
  --Info über Folgen der Nichtbereitstellung
  --automatisierte Entscheidungsfindung oder Profiling
- **Info zur Absicht, Daten für einen anderen Zweck weiterzuverarbeiten** (Abs. 3)

Informationspflichten bei der Erhebung bei betroffener Person, Art. 13, EG 58 ff (2)

- **Informationspflicht entfällt**,
  -wenn und soweit der Betroffene schon darüber verfügt , Art. 13 Abs. 4
  (Betroffener hat Informationen im gebotenen Umfang)

- **Fakultative Beschränkungen nach Art. 23**
  nach Art. 23 können gesetzliche Regelungen Beschränkungen vorsehen, u. a. wenn
  -öffentliche Interessen od.
  -private Interessen beeinträchtigt würden
  (Beispiel § 32 BDSG 2018, künftig: auch im DSAG LSA)

- **Zeitpunkt**: bei Erhebung

- **Form:**
  schriftlich, elektronisch, auf Verlangen mündlich (wenn Identität nachgewiesen)
  Ein Medienbruch ist nicht grundsätzlich ausgeschlossen
  Maßgeblich: leichte und rechtzeitige Zugänglichkeit;
  Genauigkeit und Verständlichkeit, kein information overload

Information des Betroffenen bei der Erhebung bei Dritten Art. 14

- **Informationsinhalte (Abs. 1):**
  -Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten, Zweck und Rechtsgrundlage der Verarbeitung, ggf. (Kategorien von) Empfänger
  -ggf. Drittstaatentransfer
  -Kategorien von verarbeiteten Daten
- **Infos für faire und transparente Verarbeitung (Abs. 2)**
  -Dauer der Speicherung (oder Kriterien der Festlegung)
  -Interessenabwägung (bei Verarbeitung nach Art. 6 Abs. 1 lit. f))
  -die Quelle der Daten
  -Hinweis auf Betroffenenrechte: (u. a.)
  Auskunftsrecht, Recht auf Widerruf der Einwilligung, Beschwerderecht bei der Aufsichtsbehörde, automatisierte Entscheidungsfindung oder Profiling
- **Info zur Absicht, Daten für einen anderen Zweck weiterzuverarbeiten (Abs. 4)**
- **Zeitpunkt**: in angemessener Frist (max. ein Monat, ggf. Sonderregelung)
- **Pflicht entfällt**: Betroffener verfügt über die Info, Offenlegung durch Rechtsvorschrift, unverhältnismäßiger Aufwand, Berufsgeheimnis

➔ zu den Infopflichten siehe auch Kurzpapier der DSK

Auskunftsrecht Art. 15

- **Auskunftsumfang:**
  -welche Daten verarbeitet werden (Kategorien)
  -nicht über Daten die verarbeitet wurden
  -Verarbeitungszwecke
  -(ggf. Kategorien von) Empfängern
  -geplante Dauer der Speicherung
  -Beschwerde- (Aufsichtsbeh.) und Betroffenenrechte (Löschung, Widerspr., etc.)
  -alle Informationen zur Herkunft
  -automatisierte Entscheidungsfindung, Profiling
  Form: schriftlich, elektronisch, auf Verlangen mündlich
- **Fakultative Beschränkungen** (Art. 23), Rechte Dritter
- **Recht auf Datenkopie**
  vollständig, wie vorliegend, aber keine umfassende Aktenkopie

Löschung, Art. 17

- **Löschung:** (Abs. 1)
  geboten bzw. auf Antrag notwendig, wenn:
  -die Daten für den Verarbeitungszweck nicht mehr notwendig sind
  -unrechtmäßig verarbeitet wurden
  -die Einwilligung widerrufen wurde und bei
  -erfolgreichem Widerspruch nach Art. 21 erfolgt

- **Umfang**: Unkenntlichmachen

- **Zeitpunkt**: unverzüglich

- **Entfallen**, u. a.: -ges. Aufbewahrungsvorgabe, -Forschungszwecke

Vergessenwerden Art. 17

- **Vergessenwerden:** (Abs. 2)

  Voraussetzung: Öffentlichmachen, keine Ausnahme von der Löschpflicht
  Pflicht zur Information anderer Verarbeiter über das Löschungsverlangen

- **Einschränkungen**: keine Löschpflicht bei Erforderlichkeit für

  -freie Meinungsäußerung -Erfüllung rechtlicher Verpflichtungen
  -öffentliche Interessen im Bereich öffentlicher Gesundheit
  -Archiv-, Forschungs- und statistische Zwecke
  -Geltendmachung von Rechtsansprüchen

Einschränkung Art. 18

- **Einschränkung der Verarbeitung**

kann der Betroffenen verlangen, wenn

-die Richtigkeit bestritten ist, -die Verarbeitung unrechtmäßig ist,

-der Verantwortliche die Daten nicht mehr benötigt, aber die betroffene Person sie noch zur Geltendmachung von Rechtsansprüchen braucht,

-bei Widerspruch

- Verarbeitung dann nur mit Einwilligung oder zur Geltendmachung von Rechtsansprüchen

Datenübertragbarkeit Art. 20

Bei Datenverarbeitung auf Basis von Einwilligung und Vertrag:

Anspruch auf Übertragung im strukturierten maschinenlesbaren Format

Widerspruch Art. 21

Aus einer besonderen Situation heraus ist ein Widerspruch möglich. Demgegenüber kann der Verantwortliche auf zwingende schutzwürdige Gründe verweisen.

Dokumentations- und Nachweispflichten (1)

- **Verzeichnis von Verarbeitungstätigkeiten, Art. 30**

  Pflicht für Verantwortlichen (Abs. 1) und Auftragsverarbeiter (Abs. 2) mit jeweils unterschiedlichen Inhalten

  - gilt für **alle Verarbeitungen** nach DS GVO
  - muss **nicht mehr jedermann verfügbar gemacht** werden, aber
  - auf Anforderung der **Aufsichtsbehörde zur Verfügung gestellt** werden
  - Form: schriftlich oder elektronisch

  - **nicht** erforderlich bei Unternehmen, die **weniger als 250 Mitarbeiter** beschäftigen, **sofern** die Verarbeitung
    1.) **kein Risiko** für die Rechte und Freiheiten der betroffenen Person birgt,
    2.) **nur gelegentlich** erfolgt und
    3.) **nicht besondere Kategorien** personenbezogener Daten oder Daten über **Straftaten** einschließt

  - Hinweise und Muster auf Homepage des LfD

Dokumentations- und Nachweispflichten (2)

- **Einhaltung der Grundsätze** der Verarbeitung, Art. 5 Abs. 2 Rechtmäßigkeit,, Zweckbindung, Datenminimierung, Speicher-begrenzung, Integrität und Vertraulichkeit etc. sind nachzuweisen (**Rechenschaftspflicht**)
- **Einwilligung**, Art. 7 Abs. 1 (kein zwingendes Schriftformerfordernis, muss aber nachgewiesen werden)
- **Datenschutz-Organisation**, Art. 24 Abs. 1, Technische und organisatorische Maßnahmen zum Nachweis der Verarbeitung nach der DS GVO
- Nachweispflicht bei **Auftragsverarbeitung**, Art. 28 Abs. 5
- Dokumentationspflicht bei **Verletzungen** des Datenschutzes, Art. 33 Abs. 5
- Einhaltung der DS-GVO bei erforderlicher **Datenschutz-Folgenabschätzung**, Art. 35 Abs. 7 lit. d)

Meldepflicht des Verantwortlichen bei Datenschutzverletzungen an Aufsichtsbehörde, Art. 33, 34

- **Auftragsverarbeiter** meldet dem Verantwortlichen
- Erfolgt Meldung nicht binnen **72 Stunden**, ist deren Verzögerung zu begründen
- **Inhalt**: Art der Verletzung, Kategorien und Zahlen der betroffenen Personen und Datensätze, bDSB, wahrscheinliche Folgen, Abwehrmaßnahmen
- Meldepflicht **entfällt**, wenn Verletzung „**nicht zu einem Risiko** für die Rechte und Freiheiten einer natürlichen Person führt."
- Besteht ein **hohes Risiko**, so ist unverzüglich die **betroffene Person zu benachrichtigen**
  (Ausnahme: Daten mittlerweile für Unbefugte unzugänglich, Risiko besteht nicht mehr, Benachrichtigung unzumutbar (dann aber öffentliche Bekanntmachung))

Datenschutz-Folgenabschätzung (DSFA), Art. 35 (1)

Risikobezogene Pflicht des Verantwortlichen

- wenn aus Art, Umfang, Umständen und Zweck der Verarbeitung **voraussichtlich ein hohes Risiko** für die persönlichen Rechte folgt
- Beispiele nach Art. 35 Abs. 3:
  -**systematische umfangreiche Überwachung öff. zugänglicher Bereiche**
  -umfangreiche Verarbeitung besonderer Kategorien von Daten
  -systematische und umfassende Bewertung persönlicher Aspekte
- Die Aufzählung ist nicht abschließend („insbesondere“)
- Aufsichtsbehörde erstellt Liste für DSFA-Vorgänge, Art. 35 Abs. 4
- Schwellwertanalyse -eigenverantwortliche Prognoseentscheidung (Technologierisiko statt Meldebürokratie)
- Ggf. gemeinsame DSFA
- Ggf. eine DSFA für mehrere Verfahren
- **DSFA entfällt**, wenn schon durch Gesetzgeber erfolgt

Datenschutz-Folgenabschätzung, Art. 35 (2)

Verfahren

- **Art. 35 Abs. 7** gibt Mindestinhalte der DSFA vor (ähnlich wie bisherige Vorabkontrolle)

- **Umfassende Beschreibung der Verarbeitungsvorgänge**
- **Beschreibung der konkreten Zwecke**
- **Bewertung der Notwendigkeit und Verhältnismäßigkeit**
- **Risikobewertung** (s. hierzu EG 75 u. 76)
  -Analyse (Eintrittswahrscheinlichkeit, Schwere), -Schutzbedarfsfeststellung, -Sicherheitsziele
  (s. Standard-Datenschutzmodell der Aufsichtsbehörden)
- **Auswahl von Maßnahmen**
- **Dokumentation**

Datenschutz-Folgenabschätzung, Art. 35 (3)

Weitere mögliche Verpflichtungen für den Verantwortlichen

- **Standpunkt der betroffenen Personen** oder ihrer Vertreter zur beabsichtigten Verarbeitung einholen (Art. 35 Abs. 9)
- **Überprüfung** der tatsächlichen Verarbeitung, ob sie gemäß DSFA läuft, insb. bei einer Änderung des Risikos (Art. 35 Abs. 11)
- Kommt die DSFA zu dem Ergebnis, dass bei der Datenverarbeitung ein **hohes Risiko** für Betroffene besteht, ist vor der Verarbeitung die **Aufsichtsbehörde zu konsultieren**, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, Art. 36 Abs. 1 (**nur dann, wenn Risikominimierung nicht gelingt**)
- Verstöße sind bußgeldbewehrt (Art. 83 Abs. 4 Buchst. a))
- Siehe DSK-Kurzpapier; WP 248 Rev. 01 der Art.-29-Gruppe

Datenschutzbeauftragter (DSB) Art. 37 bis 39

Benennung des DSB

- auf jeden Fall:
  -bei **Behörden** oder öffentlichen Stellen
  (Ausn. teilw.: Gericht)

  -Kerntätigkeit mit umfangreicher oder systematischer **Überwachung** von Personen

  -Kerntätigkeit mit umfangreicher Verarbeitung **besonders sensibler Daten**
- I. d. R. nicht bei einzeln tätigem Berufsgeheimnisträger
- Benennung gemeinsamer DSB möglich
- Benennung externer DSB möglich
- Maßgeblich berufliche Qualifikation und Fachwissen
- Schriftform zu empfehlen

Stellung des Datenschutzbeauftragten (DSB), Art. 38

Der DSB

- ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen **eingebunden**
- ist durch Ressourcen und Zugang zu Verarbeitungsvorgängen **zu unterstützen**
- ist **weisungsfrei**, darf wegen der Erfüllung seiner Aufgabe nicht abberufen oder benachteiligt werden, berichtet unmittelbar der höchsten Managementebene
- kann von betroffenen Personen **zu Rate gezogen** werden
- ist an **Geheimhaltung und Vertraulichkeit** gebunden
- kann **andere Aufgaben** wahrnehmen, sofern **kein Interessenkonflikt** vorliegt
- Gesetzliche Ausgestaltung in §§ 6 u. 38 BGSG 2018 , DSAG LSA: Eingeschränkte Abberufung und Kündigung, Zeugnisverweigerung

Aufgaben des DSB, Art. 39

- **Unterrichtung und Beratung** der Verantwortlichen, Auftragsverarbeiter und Beschäftigten
- **Überwachung** der Einhaltung der Datenschutzvorschriften (DSB führt die Datenverarbeitung nicht durch!)
- Beratung im Zusammenhang mit der **Datenschutz-Folgenabschätzung**
- **Zusammenarbeit** mit der **Aufsichtsbehörde**
- **Anlaufstelle** für Betroffene und Aufsichtsbehörde
- Es entfällt: Verfügbarmachen des Verfahrensverzeichnisses für Jedermann

- **Aufgabe des Verantwortlichen und des Auftragsverarbeiters** Veröffentlichung der Kontaktdaten des DSB und Mitteilung an die Aufsichtsbehörde, Art. 37 Abs. 7
- siehe zum DSB auch Leitlinie der Art.-29-Gruppe (WP 243 rev.01)

Auftragsverarbeitung, Art. 28 (1)

- Basis: **Vertrag** zwischen dem Verantwortlichen und dem Auftragnehmer, Art. 28 Abs. 3
- **Keine** gesonderte **Rechtsgrundlage** erforderlich
- Keine **„Funktionsübertragung“**: Auftragsverarbeiter ohne Entscheidungskompetenz und Eigeninteresse
- Auftragsverarbeiter bietet hinreichende **Datenschutz-garantien**, (Nachweis: ggf. Verhaltensregel oder Zertifizierung)
- Vertragsgestaltung entspricht bisherigen Vorgaben, u. A.:
  Gegenstand und Dauer, Weisungen, Art und Zweck, techn.-organisator. Maßnahmen, Verpflichtung der Mitarbeiter, Löschungen, Inspektionen
  Bestehende Verträge sollten überprüft werden
- **Subunternehmer** sind vorher zu genehmigen

Auftragsverarbeitung, Art. 28 (2)

- Geheimhaltungspflichten, Berufs-/Amtsgeheimnisse bleiben grundsätzlich unberührt
- Berufsgeheimnisträger nach § 203 Abs. 1 und 2 StGB: „Mitwirkende“ Dienstleister möglich (§ 203 Abs. 3 u. 4 StGB)
- Nachweispflicht und Informationspflichten des Verantwortlichen umfassen die Auftragsverarbeitung
- Auch der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten
- Bei Verstößen kann der Auftragsverarbeiter zum Verantwortlichen werden, bei Pflichtverletzung haftet er ggf. auch auf Schadensersatz, Art. 82 Abs. 1, 2, 4

➔ Umfängliches Kurzpapier der DSK

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25

- **Ziel:** Gestaltung von Systemen & Diensten von Anfang an durch technischen Datenschutz **(Data Protection by Design)** und mit möglichst datenschutzkonformen Voreinstellungen **(Data Protection by Default)** (Art. 25, EG 78)
- **Inhalt:** Pflicht zur Implementierung techn. und org. Maßnahmen zur Umsetzung der DS-GVO-Ziele (Datenminimierung): Pseudonymisierung, Transparenz
- **Maßstab:** Umstände des Einzelfalls, Wahrscheinlichkeit und Schwere der Risiken, Stand der Technik, Verhältnismäßigkeit der Implementierungskosten
  Nachweis ggf. durch Zertifizierung
- Schützende Voreinstellungen von Produkten und Diensten
- **Zielgruppe: Verantwortlicher** und **Auftragsverarbeiter**, indirekt aber auch **Hersteller** von IT-Systemen (Marktchance!)

Sicherheit der Verarbeitung, Art. 32 Abs. 1 (1)

Unter Berücksichtigung

- des **Stands der Technik**
- der (Implementierungs-)**Kosten**,
- der **Art**, des **Umfangs**, der **Umstände** und des **Zwecks** der Verarbeitung
- der **Eintrittswahrscheinlichkeit** und **Schwere** des **Risikos** für Rechte und Freiheiten natürlicher Personen

treffen der Verantwortliche und der Auftragsverarbeiter **technische und organisatorische Maßnahmen**, die dem **Risiko** angepasstes **Schutzniveau** gewährleisten

Maßstab ist die Betroffenensicht

Ziel: Schutz des Persönlichkeitsrechts

Sicherheit der Verarbeitung, Art. 32 Abs. 1 (2)

Technisch-organisatorische Maßnahmen

a) **Angemessen** im Verhältnis zum Risiko

b) Am **Schutzbedarf** des Betroffenen orientiert

c) **Risikobewertung** unter Berücksichtigung von Eintrittswahrscheinlichkeit und Schwere

d) **Sicherstellung** der Ziele (u. a.) der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste durch entsprechende Maßnahme (Pseudonymisierung, Zugriffsautorisierung, Verschlüsselung etc.)

e) Verfahren zur **Überprüfung** und **Dokumentation**

(siehe SDM)

Einzelthemen

Verpflichtung auf das Datengeheimnis

nicht mehr in § 5 BDSG, wohl aber im DSAG
Die Verantwortung macht eine Verpflichtungen sinnvoll (Sensibilisierung, Nachweis, s. auch Art. 29)

Direkterhebungsgrundsatz

Personenbezogenen Daten sind **vorrangig** beim Betroffenen zu erheben. Dies gebietet das Grundrecht auf informationelle Selbstbestimmung (Transparenz, Steuerung der Angaben, kein Hinweis über Verwaltungsverfahren an Dritte).

Videoüberwachung

Eine behördliche Videoüberwachung kann im öffentlichen Interesse aufgrund einer gesetzlichen Grundlage erfolgen.
Im n.-öff. Bereich gilt § 4 BDSG 2018 (Anwendungsvorrang)

Drängende Aufgaben aus der DS-GVO

- Sensibilisierung derjenigen, die personenbezogene Daten verarbeiten, auf die DS-GVO und das Anpassungsrecht
- Bestandsaufnahme der Datenverarbeitungen durchführen
- Rechtsgrundlagen prüfen
- Data Protection by Design und by Default umsetzen
- Bestehende Verträge, inkl. Verträge zur Auftragsverarbeitung, prüfen
- Datenschutz-Folgenabschätzung implementieren
- Melde- und Konsultationspflichten gegenüber der Aufsichtsbehörde organisieren
- Betroffenenrechte und Informationspflichten umsetzen
- Dokumentationspflichten organisieren

➔ **Datenschutzmanagement anpassen**

Ausblick

- Europäische und nationale Gesetzgebung zur **Konkretisierung der DS-GVO** muss beobachtet werden, insbesondere
  - die ePrivacy-Verordnung
  - die weitere Entwicklung des speziellen Datenschutzes auf Bundes- und Landesebene

- Hilfestellung bieten die Veröffentlichungen der Aufsichtsbehörden und der Fachverbände
  s. z. B. Kurzpapiere der Datenschutzkonferenz

- **Datenschutz bleibt Chefsache**, gerade in der Phase der Anpassung an die DS-GVO und danach (Verantwortlicher i. S. v. Art. 4 Nr. 7 ist die Behörde, vertreten durch die Leitung)

- Anpassung an die DS-GVO, der count-down läuft**!**

- Datenschutz bleibt **„Wettbewerbsvorteil“**

Vielen Dank für Ihre Aufmerksamkeit!

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Geschäftsstelle und Besucheradresse: Leiterstraße 9, 39104 Magdeburg
Postadresse: Postfach 1947, 39009 Magdeburg

poststelle@lfd.sachsen-anhalt.de

Telefon: 0391 81803-0
Telefax: 0391 81803-33