SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Herausforderung Datenschutzmanagement im Unternehmen – Auswirkungen der EU-Datenschutz-Grundverordnung

Dr. Harald von Bose

Agenda

- Grundlegende Aspekte
- Gliederung der DS-GVO und Anwendungsbereich
- Verbot mit Erlaubnisvorbehalt
- Weitere Prinzipien, Betroffenenrechte und Rechtsschutz
- Dokumentations- und Nachweispflichten
- Technischer Datenschutz
- Der betriebliche Datenschutzbeauftragte
- Datenschutz-Folgenabschätzung
- Besondere Bereiche der Datenverarbeitung
- Bußgelder
- Die neue Datenschutz-Aufsichtsbehörde
- Big Data vs. DS-GVO?
- Datenschutzmanagement - Aufgaben, die jetzt anstehen

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

- Seit dem 25. Mai **2016**: DS-GVO **in Kraft**
- Ab dem 25. Mai **2018**: DS-GVO **anzuwenden**
  - Artikel 99: 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

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-neu aber nicht umgesetzt)

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

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

Weitere Regelungen zur Umsetzung der DS-GVO

- **Europäische** Ebene
  Entwurf einer **Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-Verordnung)**
  (http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010&from=DE)
- **Bundes**ebene
  „Datenschutz-Anpassungs- und Umsetzungsgesetz EU - DSAnpUG-EU“ (BGBl. I Nr. 44 v. 5.7.2017, S. 2097);
  darin enthalten: **BDSG-neu**, Anpassung von zahlreichen **spezialgesetzlichen Regelungen**
- **Länder**ebene
  - Entwicklung neuer **Landesdatenschutzgesetze**
  - Anpassung von zahlreichen **spezialgesetzlichen Regelungen**

Umsetzung in Sachsen-Anhalt

- **Neufassung des DSG LSA in zwei Schritten:**
  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
     Ziel: Inkrafttreten zum 01.01.2018
  2. **Materielle** Regelungen innerhalb des DSG LSA

     Befassung im Ministerium für Inneres und Sport seit Sommer 2017, weiterer Zeitplan hier noch nicht absehbar
- **Anpassung zahlreicher Gesetze des speziellen Datenschutzes durch die zuständigen Ressorts**
  Tätigkeit ist aufgenommen, Zeitplan hier noch nicht absehbar

Konkretisierung der DS-GVO

- **Delegierte Rechtsakte**
  Befugnis der **EU-Kommission**, Rechtsakte mit allgemeiner Geltung zu erlassen (z. B. Festlegung von Anforderungen zu datenschutzspezifischen Zertifizierungen, Art. 43 Abs. 8)

- **Durchführungsrechtsakte**
  Befugnis der **EU-Kommission**, die Durchführung der DS-GVO durch Rechtsakt zu regeln (eigentlich Sache der Mitgliedstaaten; z. B. Festlegung von technischen Standards für Zertifizierungsverfahren, Art. 43 Abs. 9)

- **Leitlinien, Empfehlungen und bewährte Verfahren**
  durch den **Europäischen Datenschutzausschuss**, Art. 70
  (teilweise Übernahme von Dokumenten der Art.-29-Gruppe)

Gliederung der DS-GVO (1)

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

  Es folgen **99 Artikel** mit umfangreichen Regelungen

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

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-neu 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. EG 15, Art. 4 Nr. 6), § 1 Abs. 1 BDSG-neu

- 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 gilt noch: E-Privacy-Richtlinie, TMG, TKG, ab 25. Mai 2018 soll die Verordnung über Privatsphäre und elektronische Kommunikation gelten)

Örtlicher Anwendungsbereich

- Verarbeitung personenbezogener Daten findet im Rahmen der Tätigkeit einer **Niederlassung in der Union** statt, Art. 3 Abs. 1

- **Marktortprinzip**, Art. 3 Abs. 2
  - DS-GVO gilt auch für Unternehmen, die keine Niederlassung in der EU haben, aber
    - Waren oder Dienstleistungen in der EU anbieten oder
    - das Verhalten betroffener Personen beobachten, soweit ihr Verhalten in der EU erfolgt

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 DS-GVO: Verarbeitung ist nur rechtmäßig, wenn eine Einwilligung vorliegt oder eine andere in der Vorschrift genannte Fallgruppe erfüllt ist. Ansonsten ist sie verboten!
- Hier **kein risikobasierter** Ansatz!
- Einfache und komplexe Datenverarbeitungen werden hier 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
- Interessenabwägung: berechtigtes Interesse ./. schutzwürdiges Interesse (unter besonderer Berücksichtigung der Rechte des Kindes)

Einwilligung, Art. 7, EG 32, 33, 42, 43

Freiwilligkeit

- Einwilligung ist „**keine gültige Rechtsgrundlage**“ für die Verarbeitung, wenn „**ein klares Ungleichgewicht besteht**“ und es deshalb unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben werden würde (EG 43) – dies kann z. B. in Beschäftigungs- und Mietverhältnissen vorliegen oder auch im Verhältnis Verbraucher / marktbeherrschendes Unternehmen (Microsoft, Facebook…)

- Einwilligung gilt i. d. R. nicht als erteilt, wenn die **Erfüllung eines Vertrages**, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist (**Koppelungsverbot**)

Einwilligung (Fortsetzung)

- Wenn Einwilligung im Zusammenhang mit anderen schriftlichen Erklärungen erfolgt, muss das Ersuchen um Einwilligung in **verständlicher und leicht zugänglicher Form**, in **klarer und einfacher Sprache erfolgen**, sodass es von anderen Sachverhalten klar zu unterscheiden ist.
- Einwilligung ist **jederzeit widerrufbar**, betroffene Person wird vor der Abgabe der Einwilligung hiervon **in Kenntnis gesetzt**
- Form: **formfrei**, muss aber **nachgewiesen** werden

Empfehlung bei Alteinwilligungen:

1. Prüfung, ob Alteinwilligung durch Zeitablauf **unwirksam geworden** ist - wenn nicht und sie weiterhin genutzt werden soll:
2. **Nachträgliche Belehrung** über den Widerruf

Weitere Prinzipien

Art. 5, 12 ff, 25, 32, 51 ff

- **Erforderlichkeit, Angemessenheit, Datenminimierung**

  Beschränkung der Verarbeitung auf das **erforderliche Maß**, jetzt ausdrücklich in DS-GVO: data protection by design/ by default = Möglichkeit, mit Technik datenminimierend umzugehen

- **Zweckbindung**

  Verarbeitung nur für **festgelegte, eindeutige Zwecke**; Zweckänderung ohne Einwilligung nur wenn diese mit Ursprungszweck vereinbar (Privilegierung für im öffentlichen Interesse liegende Archiv-, wissenschaftliche oder historische Forschungs- und Statistikzwecke, Art. 89)

- **Transparenz**
  Informationspflichten und Auskunfts-, Berichtigungs-, Löschungsrechte
- **Datensicherheit**
- **Unabhängige Datenschutzaufsicht** mit Abhilfebefugnissen, jetzt auch gegenüber Behörden, inkl. Kammern (Art. 58 Abs. 2)

Betroffenenrechte - Überblick (1)

- **Erweiterte Informationspflichten, Art. 13, 14**
  Z. B. über Betroffenenrechte und Beschwerderecht bei Aufsichtsbehörde
- **Recht auf Auskunft, Art. 15 -** auf Antrag
- **Recht auf Berichtigung, Art. 16**
- **Recht auf Löschung, Art. 17 Abs. 1**
  Daten sind **unverzüglich zu löschen**, wenn sie z. B. für den Zweck der Erhebung nicht mehr notwendig sind oder unrechtmäßig verarbeitet wurden
- **Neues Recht auf Vergessenwerden, Art. 17 Abs. 2**
  Hat der Verantwortliche zu löschende Daten zuvor **öffentlich bekannt gemacht**, trifft er **angemessene Maßnahmen**, um die Verantwortlichen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person Löschung verlangt hat
- **Recht auf Einschränkung der Verarbeitung, Art. 18**

Betroffenenrechte - Überblick (2)

- **Neues Recht auf Datenübertragbarkeit, Art. 20**
  Daten müssen in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden, wenn Verarbeitung automatisiert erfolgt und auf Einwilligung oder Vertrag nach Art. 6 Abs. 1b) beruht
  Arbeitspapier der Art.-29-Gruppe unter
  http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- **Widerspruchsrecht, Art. 21**
  Recht besteht in besonderen Situationen (z. B. Gefahr für Leib oder Vermögen) bei Datenverarbeitungen, die auf Interessensabwägung beruhen (auch Profiling); Folge des Widerspruchs: keine Weiterverarbeitung,
  Ausnahme: zwingende Gründe o. Rechtsverteidigung

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** darstellt, 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

Jetzt in **§§ 32 – 37 BDSG-neu** geregelt

Informationspflichten bei der Erhebung bei betroffener Person, Art. 12, 13, EG 58 ff

- **Neue Informationsinhalte**: z. B. Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten, Rechtsgrundlage der Datenverarbeitung, Interessenabwägung, Drittstaatentransfer, Dauer der Speicherung oder Kriterien der Festlegung der Dauer, bestimmte Betroffenenrechte, Recht auf Widerruf der Einwilligung, automatisierte Entscheidungsfindung einschließlich Profiling; Art. 13 Abs. 1 u. 2
- Information muss **auch** erfolgen, wenn Daten aus **öffentlichen Quellen** stammen
- Zeitpunkt: bei Erhebung
- **Form:** schriftlich, elektronisch, mündlich (wenn Identität nachgewiesen)
- Pflicht **entfällt**
  - wenn Betroffener über Information verfügt, Art. 13 Abs. 3
  - bei Weiterverarbeitung
    - analog gespeicherter Daten, wenn Interesse der betroffenen Person gering ist
    - Information würde öffentliche Sicherheit, Ordnung, Rechtsverteidigung oder vertrauliche Übermittlung an öffentliche Stellen gefährden, § 32 Abs. 1 BDSG-neu

  Entfällt die Pflicht, sind gemäß § 32 Abs. 2 BDSG-neu Schutzmaßnahmen zu treffen (z. B. öffentliche Information) und ist der Grund zu dokumentieren

Informationspflichten bei Dritterhebung, Art. 12, 14, EG 58 ff

- **Neue Informationsinhalte:** ähnlich Art. 13 Abs. 1 u. 2
- Information muss **auch** erfolgen, wenn Daten aus **öffentlichen Quellen** stammen
- Zeitpunkt: spätestens nach einem Monat, Art. 14 Abs. 3
- Form: wie bei Art. 13
- Pflicht entfällt z. B. wenn:
  - Betroffener über Information verfügt, bei unverhältnismäßigem Aufwand, Berufsgeheimnis (Art. 14 Abs. 3)
  - durch Information Rechtsverteidigung (§ 33 Abs. 1 Nr. 2a BDSG-neu) oder
  - öffentliche Sicherheit oder Ordnung gefährdet wäre - hier Feststellung einer öffentlichen Stelle erforderlich (§ 33 Abs. 1 Nr. 2b BDSG-neu)

  Entfällt die Pflicht nach § 33 BDSG-neu, sind Schutzmaßnahmen zu treffen (z. B. öffentliche Information) und es ist der Grund zu dokumentieren

Auskunftsrecht, Art. 12, 15

- Beinhaltet die Pflicht, **auf Verlangen** die in Art. 15 Abs. 1 genannten Informationen zu erteilen (ähnlich Art. 13 u. 14)
- Frist:
  unverzüglich, spätestens innerhalb eines Monats, Art. 12 Abs. 3
- Form
  schriftlich, elektronisch (Kopie), auch über sicheren Fernzugriff
- Auskunft entfällt gemäß § 34 Abs. 1 BDSG-neu, wenn
  - Voraussetzungen des § 33 Abs 1 Nr. 2b BDSG-neu vorliegen, oder
  - Daten aufgrund Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder sie nur der Datensicherheit / Datenschutzkontrolle dienen,

  und Auskunft unverhältnismäßigen Aufwand erfordern würde und Verarbeitung zu anderen Zwecken ausgeschlossen ist
- Auskunftsverweigerung nach § 34 Abs. 1 BDSG-neu ist zu dokumentieren und regelmäßig zu begründen, § 34 Abs. 2 BDSG-neu

Recht auf Löschung, Art. 17

- Pflicht entfällt
  nach Art. 17 Abs. 3 DS-GVO, wenn Verarbeitung erforderlich ist
  - zur Ausübung von Meinungsäußerungsfreiheit und Information
  - zur Erfüllung einer rechtlichen Verpflichtung (z. B. Steuerrecht)
  - aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
  - für Archiv-, historische oder statistische Zwecke
  - zur Rechtsverteidigung

  nach § 35 Abs. 1 BDSG-neu
  - im Falle nicht automatisierter Datenverarbeitung, wenn Aufwand unverhältnismäßig hoch und Interesse der betroffenen Person gering ist
  - wenn Interessen der betroffenen Person entgegenstehen

  Wenn Daten aufgrund von § 35 Abs. 1 BDSG-neu nicht gelöscht werden können, dürfen sie nur eingeschränkt verarbeitet werden

Rechtsschutz

- **Beschwerde bei der Aufsichtsbehörde**, Art. 77
  Beschwerderecht für Betroffene **bei „einer Aufsichtsbehörde“**,
  („insbesondere“ am Ort ihres gewöhnlichen Aufenthaltsortes im Mitgliedstaat, ihres Arbeitsplatzes oder des mutmaßlichen 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

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

  - kein Verzeichnis erforderlich bei Unternehmen, die **weniger als 250 Mitarbeiter** beschäftigen, **sofern** die Verarbeitung
    1.) **nicht ein 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

  - Vordruck demnächst auf Homepage des LfD

Dokumentations- und Nachweispflichten (2)

- **Einhaltung der Grundsätze** der Verarbeitung
  = Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit (**Rechenschaftspflicht**), Art. 5 Abs. 2
- **Einwilligung**, Art. 7 Abs. 1 (kein zwingendes Schriftformerfordernis, muss aber nachgewiesen werden)
- **Datenschutz-Organisation**, Art. 24 Abs. 1,
  einschließlich technischer Maßnahmen, Art. 25 und 32
- Nachweispflicht bei **Auftragsverarbeitung**, Art. 28
- Dokumentationspflicht bei **Verletzungen** des Datenschutzes, Art. 33 Abs. 5
- Einhaltung der DS-GVO bei erforderlicher **Datenschutz-Folgenabschätzung**, Art. 35 Abs. 7 Buchst. d)
- Garantien bei **Drittstaatenübermittlungen**, Art. 46 ff.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Artikel 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, z. B. Datenminimierung, frühestmögliche Pseudonymisierung, Transparenz
- **Maßstab:** Stand der Technik, Implementierungskosten, mit der Verarbeitung verbundene Risiken (Senkung des Risikos bei Nutzung europäischer Dienstleister – „europäische Cloud“?), Zertifizierung möglich
- **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

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

Diese Maßnahmen schließen **unter anderem** Folgendes ein:

a) die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten

b) **Sicherstellung** der **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste

c) (rasche) Wiederherstellung der **Verfügbarkeit** und den **Zugang** zu personenbezogenen Daten bei einem **physischen** oder **technischen** Zwischenfall

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

Betrieblicher Datenschutzbeauftragter (bDSB), Benennung, Art. 37

- Ist gemäß **Art. 37** zu benennen, wenn **Kerntätigkeit**
  - aus Verarbeitungsvorgängen besteht, die eine **regelmäßige und systematische Überwachung** erforderlich machen,
  - in der umfangreichen Verarbeitung **besonderer Kategorien** von personenbezogenen Daten (Art. 9) oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

- **§ 38 Abs. 1 BDSG-neu** sieht zusätzlich vor:
  Benennung bDSB erforderlich, wenn
  - in der Regel **mindestens 10 Personen** ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind
  - oder eine **Datenschutz-Folgenabschätzung** (DSFA) erforderlich ist. DSFA ist erforderlich, wenn Verarbeitung voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 35).

Stellung des bDSB, Art. 38

Der bDSB

- 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
- kann nach §§ 38 Abs. 2, 6 Abs. 4 BGSG-neu nur bei Vorliegen eines **wichtigen Grundes** i. S. v. § 626 BGB **abberufen und gekündigt** werden

Aufgaben des bDSB, Art. 39

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

- **Aufgabe des Verantwortlichen und des Auftragsverarbeiters**
  Veröffentlichung der Kontaktdaten des bDSB und Mitteilung an die Aufsichtsbehörde, Art. 37 Abs. 7

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

Es handelt sich um eine **risikobezogene Pflicht** des für die Verarbeitung Verantwortlichen

- Durchführung erforderlich, wenn Art, Umfang, Umstände und Zweck der Verarbeitung **voraussichtlich ein hohes Risiko** für die persönlichen Rechte und Freiheiten zur Folge haben, Art. 35 Abs. 1
- Art. 35 Abs. 3 nennt Situationen, die eine DSFA erfordern (z. B. Abs. 3 Buchst. c): „**systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche**“)
- Die Aufzählung ist nicht abschließend („insbesondere“)
- Art. 35 Abs. 7 gibt Mindestinhalte der DSFA vor (ähnlich wie bisherige Vorabkontrolle)
- Aufsichtsbehörde erstellt Liste für DSFA-Vorgänge, Art. 35 Abs. 4

Datenschutz-Folgenabschätzung, Art. 35 (2)

Weitere mögliche Verpflichtungen für den Verarbeiter

- **Standpunkt der betroffenen Personen** oder ihrer Vertreter zur beabsichtigten Verarbeitung einholen (Art. 35 Abs. 9)
- **Überprüfung** der tatsächlichen Verarbeitung gemäß der DSFA insb. bei einer Änderung des Risikos durchführen (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
- Verstöße sind bußgeldbewehrt (Art. 83 Abs. 4 Buchst. a))

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

(gilt für alle Datenarten)

- **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))

Auftragsverarbeitung, Art. 28

- **Vertrag** zwischen dem Verantwortlichen und dem Auftragnehmer, Art. 28 Abs. 3
- EU-Kommission oder Aufsichtsbehörden können **Standardvertragsklauseln** für die Auftragsverarbeitung genehmigen, Art. 28 Abs. 7, 8
- **Verhaltensregeln und Zertifizierungen** können Bestandteil ausreichender Garantien des Auftragsverarbeiters für die Einhaltung der DS-GVO und für den Schutz von Rechten der Betroffenen sein, Art. 28 Abs. 1, 5
- Bei Pflichtverletzung **haftet** jetzt auch der **Auftragsverarbeiter für Schadensersatz**, Art. 82 Abs. 1, 2, 4

Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9, EG 51-56 (1)

- Besondere Kategorien personenbezogener Daten sind:

  personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen; Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung **sowie genetische Daten**, **biometrische Daten** (**neu**) zur eindeutigen Identifizierung einer natürlichen Person

- Genetische, biometrische und Gesundheitsdaten sind legaldefiniert in Art. 4 Nr. 13- 15

Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9, EG 51-56 (2)

- **Verarbeitung u. a. zulässig** (Art. 9 Abs. 2):
  - bei **ausdrücklicher** Einwilligung, Abs. 2a
  - zur Ausübung von Rechten und Pflichten aus dem **Arbeitsrecht** oder des **Sozialschutzes**, Abs. 2b
  - zum Schutz **lebenswichtiger Interessen**, wenn Einwilligung nicht einholbar, Abs. 2c
  - zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** (Abrechnung), Abs. 2f
  - für Zwecke der **Gesundheitsvorsorge, Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit, med. Diagnostik** (eigentl. Patientenbehandlung), Abs. 2h
  - bei öffentlichem Interesse im Bereich öffentlicher Gesundheit (**Gesundheitsgefahren**), Abs. 2i
  - …
- **Person des Verarbeitenden**
  im Falle des **Art. 9 Abs. 2h** muss Verarbeitung erfolgen durch **Fachpersonal**, welches dem **Berufsgeheimnis** unterliegt (§ 203 StGB) oder unter dessen Verantwortung

Beschäftigtendatenschutz (1) - Verarbeitung aufgrund Gesetz, Art. 88, § 26 BDSG-neu

- Personenbezogene Daten von Beschäftigten dürfen für **Zwecke des Beschäftigtenverhältnisses** verarbeitet werden, wenn dies **erforderlich** ist:
  - für die **Begründung, Durchführung oder Beendigung des Beschäftigten-verhältnisses**
  - auch auf der Grundlage von **Kollektivvereinbarungen** (einschließlich besonderer Kategorien personenbezogener Daten)
- Zur Ausübung oder Erfüllung der sich aus einem **Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung** (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten
- Zur **Aufdeckung von Straftaten**, wenn zu dokumentierende tatsächliche Anhaltspunkte auf eine Straftat des Beschäftigten vorliegen, die Verarbeitung zur Aufklärung erforderlich ist und keine schutzwürdigen Interessen überwiegen
- § 26 BDSG-neu gilt auch, wenn Daten nicht in einem Dateisystem gespeichert werden, § 26 Abs. 7 BDSG-neu (wie bisher § 32 BDSG)

Die Grundsätze der Datenverarbeitung aus Art. 5 sind einzuhalten.

Beschäftigtendatenschutz (2) - Einwilligung

Die Verarbeitung personenbezogener Daten von Beschäftigten ist grundsätzlich aufgrund einer Einwilligung möglich, soweit sie freiwillig erfolgt. Dies ist nicht gegeben, wenn infolge von Abhängigkeit ein **klares Ungleichgewicht** besteht und es deshalb in Anbetracht aller Umstände unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben werden würde, EG 43.

Voraussetzungen nach **§ 26 Abs. 2 BDSG-neu**:

- **Freiwilligkeit** kann insbes. vorliegen,
  - wenn für die beschäftige Person ein rechtlicher und wirtschaftlicher **Vorteil** erreicht wird, oder
  - Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen, oder
  - dem Beschäftigten nachteilsfreie Alternativen zur Verfügung stehen
- **Schriftform** ist erforderlich, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (Nachweispflicht beachten!)
- **Aufklärung** des Beschäftigten in Textform über den **Zweck** der Datenverarbeitung und das Recht, die Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3).

Beschäftigtendatenschutz (3) - Verarbeitung besonderer Kategorien personenbezogener Daten

1) § 26 Abs. 3 BDSG-neu:

Verarbeitung ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsverhältnis erforderlich ist und kein Grund zur Annahme besteht, dass schutzwürdiges Interesse des Betroffenen überwiegt

2) Nach § 22 Abs. 1 Nr. 1 b BDSG-neu ist die Verarbeitung besonderer Kategorien personenbezogenen Daten abweichend von Art. 9 der EU DS-GVO zulässig **für die Beurteilung der Arbeitsfähigkeit der Beschäftigten**.

Nach der Begründung des BDSG-neu erfasst die Vorschrift die Verarbeitung besonderer personenbezogener Daten des Beschäftigten im Rahmen der **Arbeitsmedizin**.

Kundendatenschutz

- Die Verarbeitung von personenbezogenen Kundendaten kann zulässig sein aufgrund:
- **Einwilligung**, Art. 6 Abs. 1 Nr. 1 a, Art. 7
- **Weitere Fallgruppen**
  - Art. 6 Abs. 1b: Verarbeitung ist zulässig, wenn sie **zur Erfüllung eines Vertrages erforderlich** ist (nicht: Werbung, Problem: Geburtsdaten?)
  - Art. 6 Abs. 1f: **Interessenabwägung**
  - Weitere Alternativen des Art. 6 Abs. 1 (Folie 17)
- **Zweckänderung** (bei Weiterverarbeitung), Art. 6 Abs. 4
  Weiterverarbeitung muss hier mit Zweck der Erhebung **vereinbar** sein

Werbung

- **Wegfall** des sog. „**Listenprivilegs**“ (z. B. Anschriften)
- Werbung ist nur dann zulässig, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten** erfordern, die **berechtigten Interessen des Werbenden** überwiegen (Art. 6 Abs. 1f)
  Problem: Ist Werbung **absehbar** (EG 47)? Art und Weise, Intensität…
  Direktwerbung kann zulässig sein.
- Besonderer Schutz für **Kinder** erforderlich, EG 38
  „Kind“ nach DS-GVO meint alle nach deutschem Recht **Minderjährigen**
- Beschränkungen des **UWG** sind weiterhin zu beachten, soweit ePrivacy Richtlinie noch gilt
  aber: Entwicklung der **Verordnung über Privatsphäre und elektronische Kommunikation beachten** (Folie 8)
- Nach **Werbewiderspruch** keine Verarbeitung mehr für Werbung zulässig, Art. 21 Abs. 3

Höhere Bußgelder

- 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

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)

Was ist bei Wirtschaft 4.0 und Big Data zu berücksichtigen?

- **"Big Data„:** große Datenmengen, die u.a. aus Bereichen wie Internet und Mobilfunk, Finanzindustrie, Energiewirtschaft, Gesundheitswesen und Verkehr und aus Quellen wie intelligenten Agenten, sozialen Medien, Kredit- und Kundenkarten, Smart-Metering-Systemen, Assistenzgeräten, Überwachungskameras sowie Flug- und Fahrzeugen stammen und die mit speziellen Lösungen gespeichert, verarbeitet und ausgewertet werden.
- **„Wirtschaft 4.0“:** intelligente, internetgestützte Herstellung von Produkten mit branchenübergreifendem Datenaustausch
- **Wann ist die DS-GVO bei Big Data und Wirtschaft 4.0 zu beachten?** Immer dann, wenn sich die **Daten auf eine identifizierte oder identifizierbare Person beziehen** – dies gilt auch, wenn der Personenbezug erst durch Verknüpfung von Daten hergestellt wird.

Können personenbezogene Daten zu Big Data/ Wirtschaft 4.0 Zwecken verarbeitet werden? (1)

Ja, wenn

- die betroffene Person freiwillig, informiert und unmissverständlich in die Anwendung **eingewilligt** hat (Art. 7, EG 32)
  Problem: ggf. umfangreiche Erklärungen notwendig bei Vielzahl von Zwecken, Zweck zum Zeitpunkt der Erhebung noch nicht bestimmt, nicht Einwilligende sind ausgeschlossen, derzeitige Praxis verwendet Daten auch ohne Einwilligung (z. B. WhatsApp)
- **oder** die Anwendung zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person** überwiegen (Art. 6 Abs 1f)
  Problem: Interessen der betroffenen Person können überwiegen (insbes. bei Minderjährigen, Beschäftigten, Profiling (vgl. Art. 22))

Können personenbezogene Daten zu Zwecken der Wirtschaft 4.0/ des Big Data verarbeitet werden? (2)

- **oder** im Falle der Weiterverarbeitung deren Zweck **mit dem ursprünglichen Zweck vereinbar** ist (Art. 5 Abs. 1b, 6 Abs. 4)
  Die Weiterverarbeitung für im öff. Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt nicht als unvereinbar mit dem ursprünglichen Zweck
  Problem: Vereinbarkeit dürfte in der Praxis oft nur begrenzte Big Data-Anwendungen ermöglichen
- **und** die Verarbeitung personenbezogener Daten für den Zweck **erforderlich** ist
  Problem: Verarbeitung muss auf das notwendige Maß beschränkt sein (Art. 5 Abs. 1c); reichen sachbezogene Daten? Wenn nicht, ist frühzeitig zu anonymisieren bzw. pseudonymisieren
- **und** die Voraussetzungen **nachgewiesen** und **dokumentiert** werden (Art. 5 Abs. 2)
- **und** die **Betroffenenrechte** gewährleistet werden (Art. 12 – 20)

Missachtet die DS-GVO die neuen Geschäftsmodelle?

- **These**: DS-GVO missachtet die neuen Geschäftsmodelle:
  Big Data i. V. m. Künstlicher Intelligenz und Wirtschaft 4.0:
  - Wie passen Erfordernisse der Einwilligung, Datensparsamkeit, und Zweckbindung mit Wirtschaft 4.0/Big Data zusammen?
  - Datenschatz statt Datenschutz!
  - Neue „Datensouveränität“!
  - Maschine und Algorithmen anstelle des Menschen?

- **Gegenthese/Lösungen**: Datenschatz **mit** Datenschutz!
  - sachbezogene Informationen (Logistik) – aber: Informationssicherheit beachten
  - Eigentumsrecht an Daten? Ökonomisierung der Daten?

- Ergänzend: Wettbewerbsrecht; Haftungsrecht
- Verbindung von Recht und Technik in der Datenschutz-Folgenabschätzung gemäß DS-GVO
- i. V. m. Data Protection by Design (Datenminimierung, Anonymisierung, Pseudonymisierung) (Marktchance)
  Problem bei Anonymisierung: Re-Identifizierung!
- Künstliche Intelligenz (intelligente Privatsphäre-Assistenten; Verbraucher-Datenportale) (Marktchance)
- Transparenz der Algorithmen

- **Verfassungsrechtlicher Einwand**: Verbot der zwangsweisen Registrierung des Menschen in seiner ganzen Persönlichkeit auch mittels anonymer Daten und Verbot der Totalüberwachung (Menschenwürde und Freiheit der Persönlichkeit)

Aufgaben aus der DS-GVO, die jetzt anstehen

- Sensibilisierung derjenigen, die personenbezogene Daten verarbeiten, auf die DS-GVO und das BDSG-neu
- 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 – Beratungsangebote nutzen!**

Weitere Informationen und Beratungen

- Im Unternehmen: Datenschutzbeauftragte
- https://datenschutz.sachsen-anhalt.de/datenschutz-sachsen-anhalt/
  insbesondere: Kurzpapiere der DSK zu wesentlichen Themen
- https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html
- Kammern
- Branchenverbände (z. B. Deutsche Kreditwirtschaft, Gesamtverband der Deutschen Versicherungswirtschaft e. V.)
- https://www.gdd.de/
- https://www.bvdnet.de/
- https://www.datenschutzverein.de/

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

- Datenschutz wird komplexer, komplizierter und strenger, daher:

- **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 Unternehmensleitung)

- Anpassung an die DS-GVO **jetzt!**

- 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
Freecall: 0800 9153190 (nur über Festnetz)
Telefax: 0391 81803-33