EU-Datenschutz-Grundverordnung

- Hinweise zur Umsetzung in den Hochschulen -

Stand: 06.09.2017

Roswitha Iburg, RL`in 2

Die Landesbeauftragte für den Datenschutz Niedersachsen

Rechtsgrundlagen

Verordnung (EU) 2016/679
des Europäischen Parlaments und des Rates vom 27.04.2016
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG
(DSGVO)

- **Geltung** ab 25.05.2018
- **Ziel**: Harmonisierung des Datenschutzrechts in der EU
- **Unmittelbar** geltendes Recht in allen Mitgliedstaaten
- Aber: **Öffnungsklauseln** und Regelungsaufträge für den nationalen Gesetzgeber

  - Art. 6 Abs. 2 und 3: Wahrnehmung einer im öff. Interesse liegenden Aufgabe
  - Art. 23: Beschränkungen der Betroffenenrechte
  - Art. 88: DV im Beschäftigungskontext
  - Art. 51 ff, 83: Aufsichtsbehörden, Rechtsschutz

  → z.B.: BDSG neu, Änderung SGB X zum 25.05.2018

  → Problem: zeitnahe Anpassung des niedersächsischen Rechts ?

Anwendungsbereich

Persönlicher Schutzbereich (Art. 1 Abs. 1 und 2)

- natürliche Personen
- unabhängig von Staatsangehörigkeit und Aufenthalt

Sachlicher Anwendungsbereich (Art. 2)

Personenbezogene Daten, wenn

- ganz oder teilweise automatisierte Verarbeitung (Def. s. Art. 4 Nr. 2)
- nicht-automatisierte Verarbeitung, soweit in Dateisystem (Def. s. Art. 4 Nr. 6) gespeichert
- Ausnahmen in Abs. 2 → z. B. Buchst. c : „ausschließlich persönliche oder familiäre Tätigkeit"

Räumlicher Anwendungsbereich (Art. 3)

- Niederlassungsprinzip (Abs. 1)
- Marktortprinzip (Abs. 2) → vgl. DSK-Kurzpapier Nr. 7

Begriffsbestimmungen

Art. 4 Begriffsbestimmungen

- Keine wesentlichen Änderungen gegenüber der EU-DatenschutzRili 95/46/EG

- Zentrale Definitionen:
  - Personenbezogene Daten (Nr. 1)
  - Verarbeitung (Nr. 2) → weiter Begriff
  - Verantwortlicher (Nr. 7)
  - Auftragsverarbeiter (Nr. 8)
  - Dritter (Nr. 10)
  - Einwilligung (Nr. 11)

- Neu:
  - Profiling (Nr. 4)
  - genetische Daten (Nr. 13)
  - biometrische Daten (Nr. 14)
  - Gesundheitsdaten (Nr. 15)
  - Unternehmen (Nr. 18)
  - verbindliche unternehmensinterne Datenschutzvorschriften (Nr. 20)

Verarbeitungsgrundsätze

Art. 5 Abs. 1: Verarbeitungsgrundsätze:

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

Art. 5 Abs. 2: Rechenschaftspflicht des Verantwortlichen

→ Nachweis- und Dokumentationspflichten

Bei Verstößen:

- Aufsichtsbehördliche Maßnahmen nach Art. 58 Abs. 2
- Ggf. Sanktionen (Art. 83 Abs. 7)

Art. 6

Grundsatz: Verbot mit Erlaubnisvorbehalt

Rechtsgrundlagen für die Datenverarbeitung:

- Einwilligung (Art. 6 Abs. 1 Buchst. a)
  - Definition in Art. 4 Nr. 11 (informiert und unmissverständlich)
  - Bedingungen in Art. 7 und 8 (insbes. widerruflich)
  - Problematisch bei Ungleichgewicht, insbes. Behörde (vgl. EG 43)
- Erfüllung eines Vertrages (Art. 6 Abs. 1 Buchst. b)
- Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchst. c)
  → **Rechtsvorschrift** (vgl. Art. 6 Abs. 2 und 3)
- Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 Buchst. d)
- Wahrnehmung e. im öff. Interesse liegenden Aufgabe (Art. 6 Abs. 1 Buchst. e)
  → **Rechtsvorschrift** (vgl. Art. 6 Abs. 2 und 3)
- Wahrung überwiegender berechtigter Interessen (Art. 6 Abs. 1 Buchst. f)
  → gilt nicht für Aufgabenerfüllung durch Behörde

Verarbeitung besonderer Kategorien personenbezogener Daten

Art. 9

- Abs. 1: Definition der bes. Datenkategorien:
  - Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen und Gewerkschaftszugehörigkeit hervorgehen
  - Genetische Daten, biometrische Daten, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung

- Grundsatz: Verarbeitungsverbot

- Ausnahmen gem. Abs. 2:
  - Ausdrückliche Einwilligung (Buchst. a)
  - Erforderlich zum Schutz lebenswichtiger Interessen (Buchst. c)
  - Zweckgebundene interne Verarbeitung durch best. Organisationen (Buchst. d)
  - Von der Person offensichtlich veröffentlichte Daten (Buchst. e)
  - Verfolgung rechtlicher Ansprüche (Buchst. f)
  - Bei Vorliegen einer **Rechtsgrundlage**:
    - Wahrnehmung von arbeits- und sozialrechtlichen Rechten und Pflichten (Buchst. b)
    - Erhebliches öffentliches Interesse (Buchst. g)
    - Maßnahmen für die individuelle Gesundheit (Buchst. h)
    - Öffentliche Gesundheit (Buchst. i)
    - Archivzwecke, wiss. oder histor. Forschungszwecke, statistische Zwecke (Buchst. j)

- Weitergehende normative Bedingungen und Beschränkungen gemäß Absatz 4 möglich

Auftragsverarbeitung

- **Art. 4 Nr. 8:** Definition des Auftragsverarbeiters (AV)
- Abgrenzung zur Funktionsübertragung: Weisungsgebundenheit (vgl. Art. 29)
- AV ist kein „Dritter" iSd Art. 4 Nr. 10 → Privilegierung der AVerarb. bleibt

- **Art. 28:**
- Abs. 1: Eignung des AV
- Abs. 3: Vertragliche Regelung nötig
  → Mindestinhalt: Gegenstand, Dauer, Art und Zweck der DV, Art der pb Daten, betroffene Personen, Rechte und Pflichten des Verantwortlichen, Pflichten des AV (insbes. Weisungsgebundenheit, Vertraulichkeit, toMs, Maßnahmen nach Art. 32)
- Abs. 2: Subunternehmer-Einsatz nur mit schriftlicher Genehmigung
- Wichtig: bestehende ADV-Verträge anpassen !

- **Neue Verantwortlichkeiten und Pflichten des AV**:
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 Abs. 2)
- Zusammenarbeit mit Behörden (Art. 31)
- Unverzügliche Meldung von Datenpannen an den Verantwortlichen (Art. 33 Abs. 2)
- Benennung eines eigenen DSB (Art. 37 ff)
- Bei Verstoß gegen weisungsgebundene DV: Einstandspflicht des AV (Art. 28 Abs. 10)
- AV als Adressat behördlicher AnO (Art. 58)
- Haftung gem. Art. 82, 83 bei Datenschutzverletzungen (Schadenersatz, Geldbuße)

Betroffenenrechte

- Transparenzgebot, Art. 12
- Informationspflichten, Art. 13 und 14 → vgl. DSK-Kurzpapier Nr. 10
  → umfassender als nach geltendem Recht
- Auskunftsrecht des Betroffenen, Art. 15 → vgl. DSK-Kurzpapier Nr. 6
- Recht auf Berichtigung, Art. 16
- Recht auf Löschung, Art. 17 (neu: Abs. 2) → vgl. DSK-Kurzpapier Nr. 11
- Recht auf Einschränkung der Verarbeitung („Sperrung"), Art. 18
- Recht auf Datenübertragbarkeit, Art. 20
- Widerspruchsrecht, Art. 21
- Automatisierte Entscheidungen im Einzelfall (einschl. Profiling, Art. 22)

→ Art. 23: Möglichkeit der gesetzlichen Beschränkung von Betroffenenrechten zur Sicherstellung best. wichtiger Rechtsgüter, wie z.B. wichtiger Ziele des allgemeinen öff. Interesses

→ Art. 89 Abs. 2 und 3: Möglichkeit der gesetzlichen Beschränkung best. Betroffenenrechte zu Forschungs-, Statistik- oder Archivzwecken

toM I

Art. 24: Technisch-organisatorische Maßnahmen des Verantwortlichen

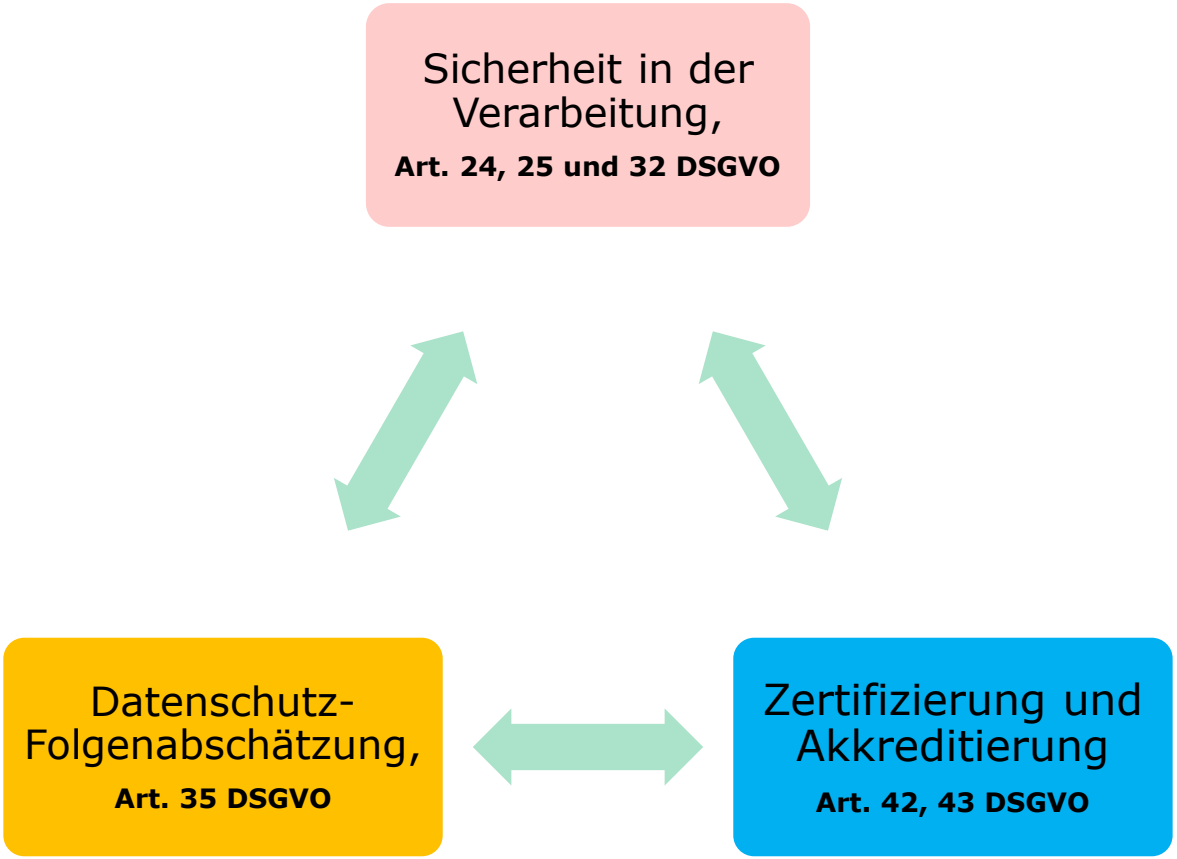
- zur Sicherstellung und Erbringung des Nachweises, dass die Verarbeitung gemäß der DSGVO erfolgt
- Maßnahmen „geeignet" unter Berücksichtigung von Art, Umfang, Umständen und Verarbeitungszweck
- sowie der Eintrittswahrscheinlichkeit und der Schwere der Risiken für die Rechte und Freiheiten der betroffenen Person
- Pflicht zur regelmäßigen Überprüfung und Aktualisierung (Abs. 1 Satz 2)

Art. 25: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Art. 32: Sicherheit der Verarbeitung

- Gerichtet an Verantwortlichen und Auftragsverarbeiter
- Ziel: Gewährleistung eines dem Risiko angemessenen Schutzniveaus durch toMs
- Bestehende IT-Systeme: Anpassung an DSGVO-Vorgaben
- Neue IT-Systeme: Art. 25 berücksichtigen
- Ggf. Durchführung e. DSFA (Art. 35)

toM II


Sicherheit in der Verarbeitung,
Art. 24, 25 und 32 DSGVO
Datenschutz-Folgenabschätzung,
Art. 35 DSGVO
Zertifizierung und Akkreditierung
Art. 42, 43 DSGVO

Dokumentation

Art. 30 - Verzeichnis von Verarbeitungstätigkeiten

- **Abs. 1: Mindestinhalt des Verzeichnisses für Verantwortliche**
  - neu: erfasst „alle" und somit auch nicht-automatisierte Verarbeitungstätigkeiten
  - insbes.: Kontaktdaten des Verantwortlichen und des DSB, Zweck der DV, Beschreibung der Kategorien betroffener Personen, pb Daten und Empfänger, Löschfristen, Beschreibung der toMs
- **Abs. 2: Verzeichnis für AV** (neu)
- **Abs. 3**: Schriftform (auch elektronisch)
- **Abs. 5 Ausnahmen:** Einrichtungen mit weniger als 250 Mitarbeitern, es sei denn
  - Risikogeneigte DV (z.B. Überwachungsmaßnahmen),
  - nicht nur gelegentliche DV (z.B. regelmäßige Verarbeitung von Beschäftigtendaten) oder
  - Verarbeitung bes. Daten gem. Art. 9 Abs. 1 (z.B. Gesundheitsdaten) oder gem. Art. 10
- Neu: Verzeichnis ist nicht öffentlich
- Verzeichnis als ein Baustein einer strukturierten Datenschutzdokumentation
- Ggf. sinnvoller Einsatz für weitere Zwecke, wie
  - Erfüllung der Rechenschafts- und Dokumentationspflichten (Art. 5 Abs. 2, Art. 24 und Art. 32)
  - Maßnahme zur Erfüllung der Betroffenenrechte (Art. 12 Abs. 1)
  - Prüfung des Erfordernisses einer Datenschutzfolgeabschätzung (Art. 35)

→ vgl. DSK-Kurzpapier Nr. 1 und Hinweise der Aufsichtsbehörden

Meldung von Datenschutzverstößen

Art. 33 Abs. 1: Meldepflicht des **Verantwortlichen** an die Aufsichtsbehörde

- Zeitpunkt: Unverzüglich, möglichst binnen 72 Std. ab Bekanntwerden
- Abs. 3: Inhalt der Meldung: Beschreibung der Datenschutzverletzung und ungefähre Zahl der betr. Datensätze, Name und Kontaktdaten des DSB, Folgenbeschreibung, Beschreibung ergriffener oder vorgeschlagener Maßnahmen
- Ausnahme: voraussichtlich kein Risiko für Rechte und Freiheiten
- Dokumentationspflicht, Abs. 5

Art. 33 Abs. 2: Meldepflicht des **Auftragsverarbeiters** an den Verantwortlichen
(Empfehlung: entspr. Hinweis in AV-Vertrag aufnehmen)

Art. 34: Benachrichtigungspflicht des Verantwortlichen an die **betroffene Person**

- Vorauss. gem. Abs. 1: hohes Risiko für Rechte und Freiheiten
- Zeitpunkt: unverzüglich
- Inhalt gem. Abs. 2
- Ausnahmen gem. Abs. 3: z.B. techn.-org. Sicherheitsvorkehrungen getroffen

Datenschutz-Folgeabschätzung, Art. 35

- **Abs. 1: Voraussetzungen**
  - Verarbeitungsform, die ein hohes Risiko für Rechte und Freiheiten nat. Personen darstellt (insbes. bei der Verwendung neuer Technologien) → „vorabkontrollähnlich"
  - Zu beurteilen nach Art, Umfang, Umständen, Zwecken
  - Regelbeispiele in Abs. 3
    - system. und umfangreiche Bewertung persönlicher Aspekte (Profiling)
    - Umfangreiche Verarbeitung bes. Kategorien pb Daten (Krankenhausinformationssysteme)
    - system. und umfangreiche Überwachung öff. zugänglicher Bereiche
  - Vorab zu erstellen, an Veränderungen anzupassen

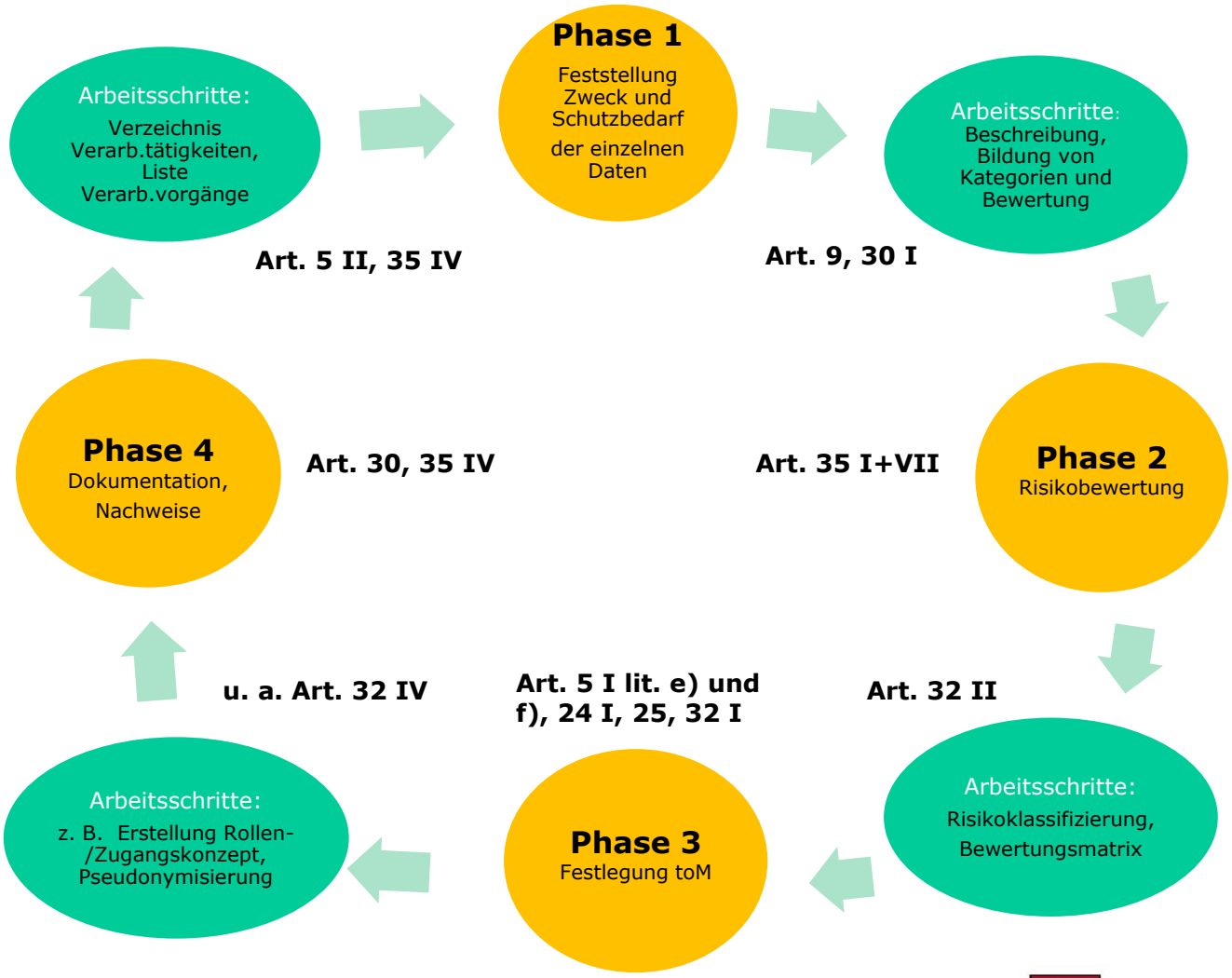
- **Abs. 7: Mindestinhalt**
  - Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit sowie der Risiken
  - Abhilfemaßnahmen zur Eindämmung der Risiken (insbes. toMs)
  - Ggf. vorherige Konsultation der Aufsichtsbehörde (Art. 36)

- **Pflicht des Verantwortlichen**
  - Einbindung des DSB (Abs. 2)
  - ggf. Einholung Standpunkt Betroffener (Abs. 9)
  - DSFA-Bericht als Baustein der Dokumentationspflicht gem. Art. 5 Abs. 2

→ vgl. DSK-Kurzpapier Nr. 5

→ Positivliste der Aufsichtsbehörden in Vorbereitung

Risikobasierter Ansatz; Phasenmodell



Risikobasierter Ansatz I

Die DSGVO verfolgt an vielen Stellen einen risikobasierten Ansatz, d.h. die **Maßnahmen müssen risikoangemessen** sein.

Was ist seitens der Verantwortlichen (s. Art. 24 DSGVO) zu tun?

Checkliste /Phasenmodell

(vgl. frühere Hinweise der LfD zur „Vorabkontrolle" nach § 7 Abs. 3 NDSG)

Mit dem sog. „Standarddatenschutzmodell"(SDM) kann der Verantwortliche die erforderlichen Funktionen und Schutzmaßnahmen systematisch planen, umsetzen und kontinuierlich überwachen. Zugleich bietet dieses Modell den Datenschutzbehörden die Möglichkeit, mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren Gesamturteil über ein Verfahren und dessen Komponenten zu gelangen.

Risikobasierter Ansatz II

daten schutz

Phase 1:

Feststellung Schutzbedarf der zu verarbeitenden personenbezogenen Daten

- Erfassung der einzelnen Daten,
- Bewertung der einzelnen Daten: Der Schutzbedarf der Daten ist festzulegen (s. „Schutzstufenkonzept LfD“)

Phase 2:

Risikobewertung vornehmen: Erstellung einer Bewertungsmatrix sinnvoll.

- Festlegung
  - der Risiken,
  - deren Eintrittswahrscheinlichkeit und
  - Eintrittsauswirkungen.
- Bildung sog. „Risikoklassen“ für die einzelnen Daten.

Phase 3:

Festlegung der aufgrund der Risikobewertung zu ergreifenden technisch-organisatorischen Maßnahmen.

Phase 4:

Erforderliche Nachweise für die Maßnahmenumsetzung beibringen.

Behördliche Datenschutzbeauftragte

Art. 37: Benennung

- Abs. 1: Benennungspflicht bei DV durch Behörde oder öff. Stelle
- Anforderungen gem. Abs. 5: Qualifikation, Fähigkeit, Fachwissen
- Abs. 7: Mitteilung und Veröffentlichung der Kontaktdaten des DSB

Art. 38: Stellung

- Frühzeitige Einbindung, Unterstützung, Ressourcen
- Weisungsfreiheit, Berichtsrecht an Geschäftsleitung (Präsidium), Benachteiligungsverbot
- Verschwiegenheitspflicht, Vermeidung von Interessenkollisionen

Art. 39: Aufgaben

- Unterrichtung und Beratung des Verantwortlichen bzw. des AV und der Beschäftigten hinsichtl. der Pflichten nach DSGVO und sonstiger DS-Vorschriften
- Überwachung der Einhaltung der DSGVO und sonstiger DS-Vorschriften einschließlich der Sensibilisierungen und Schulungen der MA und der Prüfung interner Datenschutzstrategien
- auf Anfrage: Beratung im Zusammenhang mit DSFA; Überwachung ihrer Durchführung
- Zusammenarbeit mit Aufsichtsbehörde, Anlaufstelle für Aufsichtsbehörde
- weitere Aufgabenübertragungen möglich, sofern keine Interessenkollision mit Kontrollpflicht

→ Zentrale Aufgabe liegt in Kontrolle und Beratung; Umsetzungspflicht bei der Geschäftsleitung

→ Erläuterungen im WP 243 der Art. 29-Datenschutzgruppe

Internationaler Datenverkehr I

daten schutz

Allgemeine Grundsätze, Art. 44

- Verbot mit Erlaubnisvorbehalt
- Drittländer: alle Nicht-EU-Staaten
- Übermittlung als solche muss erlaubt sein,
  sog. „2-Stufen-Prüfung“:

1. Stufe: Die allgemeinen Bestimmungen der DSGVO sind einzuhalten.
2. Stufe: Darüber hinaus sind die besonderen und zusätzlichen Anforderungen der Art. 44 ff DSGVO zu beachten.

Internationaler Datenverkehr II

Erlaubnis-Tatbestände gem. Art. 45, 46:

→ insbes.

- Angemessenheitsbeschluss der KOM, Art. 45 (auch EU-US-Privacy Shield)
- Rechtlich bindende und durchsetzbare Dokumente zw. Behörden, Art. 46 Abs. 2 Buchst. a)
- Genehmigte Vertragsklauseln, Art. 46 Abs. 3 Buchst. a)
- Genehmigte VwV zw. Behörden, Art. 46 Abs. 3 Buchst. b)

Für Behörden geltende **AusnahmeTB** gem. Art. 49 Abs.1 Buchst. d) bis g)

→ vgl. DSK-Kurzpapier Nr. 4

Aufsichtsbehörden

Befugnisse, Art. 58

Ausübung der Befugnisse unparteiisch, gerecht, innerhalb angemessener Frist; klare und eindeutige Maßnahmen, die schriftlich zu erlassen sind.

Abs. 1 Untersuchungsbefugnisse	Abs. 2 Abhilfebefugnisse	Abs. 3 Genehmigungsbefugnisse und beratende Befugnisse
•Datenschutzüberprüfungen •Anweisung zur Bereitstellung von Informationen •Zugang zu Daten und Informationen •Zugang zu Geschäftsräumen •Überprüfung von Zertifizierungen •Hinweis auf Verstoß	•Verwarnen •Anweisungen, Anordnungen •Geldbuße verhängen	•Stellungnahmen zu Datenschutzfragen an Parlamente und Öffentlichkeit •Zertifizierung erteilen •Genehmigungen nach Art. 46, 47

- Unmittelbar geltendes Recht, nicht abschließender Katalog
- Abs. 4: Ausübung der Befugnisse richtet sich nach nationalem Recht, das Vf-Regelungen und gerichtl. Rechtsbehelfe vorsehen muss → VwVfG, VwGO, OWiG

Rechtsbehelfe

Rechtsbehelfe der betroffenen Person Art. 77 – 82

- Beschwerde bei einer Aufsichtsbehörde, Art. 77
- Gerichtlicher Rechtsbehelf gegen die Aufsichtsbehörde, Art. 78
- Gerichtlicher Rechtsbehelf gegen den Verantwortlichen oder AV, Art. 79
- Schadenersatz, Art. 82

Nach Maßgabe nationalen Rechts:

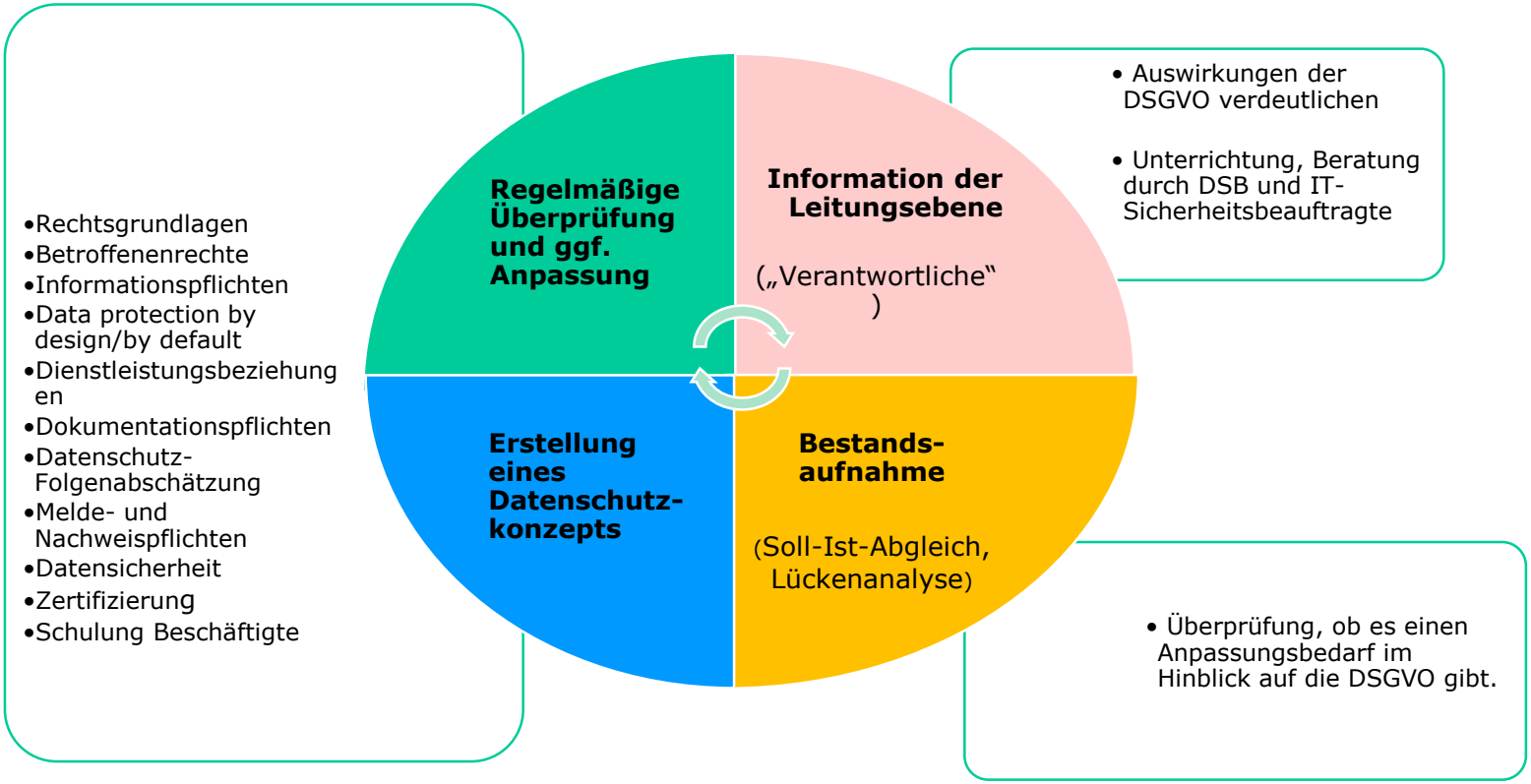
- Gewillkürte Verfahrens- und Prozessvertretung, Art. 80 Abs. 1
- Verbandsbeschwerde oder Verbandsklagerecht, Art. 80 Abs. 2

Besondere Verarbeitungssituationen

- Meinungsfreiheit, Presse- und Informationsfreiheit, Wissenschaft, Kunst und Literatur, Art. 85
- Informationsfreiheit, Art. 86
- Nationale Kennziffern, Art. 87
- Beschäftigtendatenschutz, Art. 88
- Archiv, Wissenschaft, Forschung und Statistik, Art. 89
- Zuständigkeit LfD für Berufsgeheimnisträger, Art. 90

→ Möglichkeit der Schaffung spez. Normen durch nationales Recht

Maßnahmenplan zur Umsetzung der DSGVO



→ vgl. DSK- Kurzpapier Nr. 8