EU-Datenschutzgrundverordnung

6. DFN-Konferenz Datenschutz

RA Dr. Jan K. Köcher

Datenschutzauditor, DFN-CERT

koecher@dfn-cert.de

Personenbezug

Nur Schutz personenbezogener Daten

Alle Informationen mit Bezug zu:

Identifizierte Person:

z.B.: *Hans Meier ist verheiratet*

Identifizierbare Person:

Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung 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

z.B.: *Personalnummer 12345 verdient 50000€ p.a.*

Datenverarbeitung

Bisher im BDSG/LDSG: Erheben, **Verarbeiten** (*Speichern, Verändern, Übermitteln, Sperren, Löschen),* **Nutzen**

Jetzt in Art. 4 Nr. 2 DSGVO, Verarbeitung:

- **Erheben, Erfassen,**
- **Organisation, Ordnen, Speicherung,**
- **Anpassung, Veränderung,**
- **Auslesen, Abfragen, die Verwendung,**
- **Bereitstellung: Offenlegung durch Übermittlung, Verbreitung oder eine andere Form Bereitstellung**
- **Abgleich oder der Verknüpfung**
- **Einschränkung, Löschen oder die Vernichtung**

Relevante Erlaubnisnormen

Art. 6 Abs. 1 a): Einwilligung der betroffenen Person

Art. 6 Abs. 1 b): Zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich / Vorvertragliche Maßnahmen auf Anfrage der betroffenen Person

Art. 6 Abs. 1 c): Zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich

Art. 6 Abs. 1 e): Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

- **Hochschulen:** Art. 6 Abs. 1 e) i.V.m Art. 6 Abs. 3 i.V.m. Hochschulgesetz, -zulassungsgesetz, Satzungen, VOen
- **Forschung:** Wann im öffentlichen Interesse?

Art. 6 Abs. 1 f): Berechtigtes Interesse, nicht bei überwiegendem Interesse des Betroffenen

- Nicht für Behörden in Erfüllung ihrer Aufgaben!

Einwilligung

Art. 4 Nr. 11, 6 Abs. 1 a), 7:

- Freiwillig, informiert, unmissverständlich
- Hinweis auf den Zweck und ggf. Folgen der Verweigerung /Kopplung: Nachw. Freiwilligkeit!
- Von anderen Sachverhalten klar zu unterscheiden
- Besondere Kategorien: Art. 9 Abs. 2 a)

Neu:

- Eindeutige bestätigende Handlung reicht
- Keine Formvorgabe mehr / **Widerruf muss in derselben Form möglich sein**
- **Informationspflicht, dass bei Widerruf die Verarbeitung bis Widerruf zulässig**

Datenminimierung

Neu:

Art. 25 Abs. 1 Privacy by design

- **Verpflichtet: Verantwortlicher (nicht Hersteller)**
- Festlegung der Mittel (z.B. Produktauswahl)
- Eigentlichen Verarbeitung (Customizing, Gestaltung)
- **Kriterien: Stand der Technik, Kosten, Art, Umfang, Umstände, Zwecke, Eintrittswahrscheinlichkeiten**

Art. 25 Abs. 2 Privacy by default

- **Verpflichtet: Verantwortlicher (nicht Hersteller)**
- **Voreinstellung nur erforderliche Daten**
- Menge, Umfang der Verarbeitung, Speicherfrist, Zugänglichkeit
- **Zugänglichkeit für Allgemeinheit nicht ohne Eingreifen des Betroffenen**

Zweckbindung/-trennung

Grundsätzliche Begrenzung auf den Zweck, der der Erhebung zugrundelag (Art. 5 I b):

„Die Daten dürfen bis auf die Fälle einer gesetzlichen Erlaubnis oder Einwilligung des Betroffenen nicht in einer mit den Erhebungs-zwecken ***nicht zu vereinbarenden*** *Weise weiterverarbeitet werden.“*

- ***Art. 6 Abs. 4: Anleitung zur Prüfung, ob eine Vereinbarkeit mit dem Ursprungszweck vorliegt***

Zwecktrennung (Teilaspekt Art. 25 II):

Verschiedenen Zwecken dienende Datenverarbeitungen müssen ***technisch*** *und/oder organisatorisch getrennt werden*

Verfahrensverzeichnis

Gibt es als solches nicht mehr:

Nach Außen, Art. 13 - 15:

- **Erweiterte Informationspflichten**
- Inhaltlich ähnlich wie bisher Verfahrensverzeichnis
- Anforderungen an Form ähnlich wie bisher Datenschutzerklärungen auf Webseiten

Nach Innen, Art. 30:

- **Verzeichnis von Verarbeitungstätigkeiten**
- **Verpflichtet:** Verantwortlicher und Auftragsverarbeiter
- **Einsicht:** Aufsichtsbehörde auf Anfrage
- **Form:** Schriftlich, kann auch im elektronischen Format erfolgen
- **Ausnahme:** Unter 250 Beschäftigte + weitere unklare Voraussetzungen

Informationspflichten

Art. 12 Abs. 1: Transparente Information

- Art. 13: Erhebung beim Betroffenen
- Art. 14: Erlangung nicht vom Betroffenen
- Art. 15-22: Betroffenenrechte
- Art. 34: Betroffener Datenschutzverletzung

Anforderungen:

- Präzise, transparent, verständlich und leicht zugänglich in einer klaren und einfachen Sprache
- Schriftlich oder in anderer Form, ggf. auch elektronisch

Informationspflichten

Art. 13 Erhebung beim Betroffenen

Vergleichbar dem bisherigen Verfahrensverzeichnis:

Allgemeine Informationen:

- *Name und Kontaktdaten des Verantwortlichen (VV)*
- *Kontaktdaten des Datenschutzbeauftragten (VV)*
- *Zwecke der Verarbeitung und Rechtsgrundlage (VV)*
- *Wenn Art. 6 Abs. 1 f), dann das berechtigte Interesse* ***(Neu)***
- *Empfänger oder Kategorien von Empfängern (VV)*
- *Absicht der Übermittlung in ein Drittland (VV)*

Zusätzliche Informationen

- *Dauer Speicherung oder Kriterien der Festlegung (VV)*
- *Hinweis auf die Betroffenenrechte* ***(Neu)***
- *Hinweis auf Widerrufsoption und Folgen bei Einwilligung* ***(Neu)***
- *Hinweis auf Beschwerderecht Aufsichtsbehörde* ***(Neu)***
- *Information über die Erforderlichkeit und welche Konsequenzen eine Nichtbereitstellung von Daten hätte* ***(teils neu)***
- *Automatisierte Entscheidungsfindung einschließlich Profiling* ***(Neu)***
- *Zweckänderung: Zweck und erforderliche Informationen* ***(Neu)***

Informationspflichten

Ausnahmen

Art. 12 Abs. 4 EU-DSGVO

- Betroffene Person hat die Daten bereits (EG 62)
- Speicherung und Offenlegung ausdrücklich durch Rechtsvorschrift
- Unterrichtung der Person unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich
- Beispiel (EG 62): Forschungsprojekte mit vielen Beteiligten

Recht auf Auskunft

Art. 15 Recht auf Auskunft

- **Auskunft ob personenb. Daten verarbeitet werden**
- **Anspruch auf kostenlose Kopie eigener Daten**
- **Weitere Informationen zur Verarbeitung:** Zwecke, Empfänger, Speicherdauer, Betroffenenrechte, Ggf. Auskunft zur Datenquelle, Ggf. automatisierte Entscheidungen, Ggf. Übermittlung Drittland

Datenportabilität

NEU: Art. 20

- **Bereitstellung der personenbezogenen Daten in strukturiertem, gängigem und maschinenlesbarem Format**
- **Ungehinderte Übertragung an neuen Anbieter/ bzw. direkte Übermittlung**

Ausnahmen:

- Gilt nur bei Verarbeitung mit Einwilligung oder Verarbeitung aufgrund Vertrags
- Gilt nicht bei Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

Damit: Nicht bei Ausübung der Aufgaben nach dem Hochschulgesetz

Schadenersatz

Art. 82:

- **Materielle und immaterielle Schäden durch Verletzung EU-DSGVO**
- **Ersatzpflichtig:**
- Verantwortliche
- Auftragsverarbeiter
- **Abs. 3: Nachweis fehlender Verantwortlichkeit möglich**
- **Außenverhältnis: Gesamtschuldnerische Haftung jedes Verantwortlichen/ Auftragsverarbeiters**

Sicherheit personenbezogener Daten

Art. 32 Sicherheit der Verarbeitung

- Geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:
- Berücksichtigung Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung

Wer: Verantwortlicher und Auftragsverarbeiter

Code of Conduct, Zertifizierung

- **Code of Conduct, Art. 40**
- Gemeinsame Verhaltensregeln durch Verbände und Vereinigungen
- Inhaltlich insbesondere:
- Berechtigte Interessen in bestimmten Zusammenhängen
- Privacy by Design / Privacy by Default
- Maßnahmen zur Datensicherheit
- Meldung bei Datenschutzverletzungen
- Übermittlung personenbezogener Daten in Drittländer
- Genehmigung durch Aufsichtsbehörden
- **Vorteil:** Einhaltung CoC begründet gesetzliche Vermutung für die Einhaltung der EU-DSGVO
- **Zertifizierung, Art. 42**
- Genehmigtes und formalisiertes Verfahren für Prüfsiegel
- **Vorteil:** Gesetzliche Vermutung wie bei CoC

Datenschutz-Folgeabschätzung

Art. 35 und 36:

- **Hohes Risiko** einer Verarbeitung aufgrund Art, Umfang, Umstände und Zwecke
- **Zuständig:** Verantwortlicher/bDSB nur beratend!
- **Positiv-Liste:** LDSB erstellen und veröffentlichen eine Liste mit Verarbeitungsvorgängen
- **Inhaltliche Anforderungen in Art. 35 Abs. 7:**
  Systematische Beschreibung Verarbeitung und Zwecke
  Bewertung Notwendigkeit und Verhältnismäßigkeit
  Bewertung Risiken für Rechte und Freiheiten Betroffener
  Geplante Abhilfemaßnahmen und Nachweise
- **Konsultationspflicht:**
- Bei hohem Risiko, wenn keine Maßnahmen zur Eindämmung getroffen werden

Meldepflicht Art. 33 EU-DSGVO

- **Innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde**
- Auftragsverarbeiter hat eine Verletzung unverzüglich an den Verantwortlichen zu melden
- **Ausnahme:** Verletzung führt voraussichtlich nicht zu einem Risiko für Rechte und Freiheiten natürlicher Personen

Inhalt:

- Beschreibung Art der Verletzung, Kategorien, ungefähre Anzahl Betroffener, ungefähre Zahl betroffener Datensätze
- Name und Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung

Übermittlung in ein Drittland

Art. 44: Grundsätze

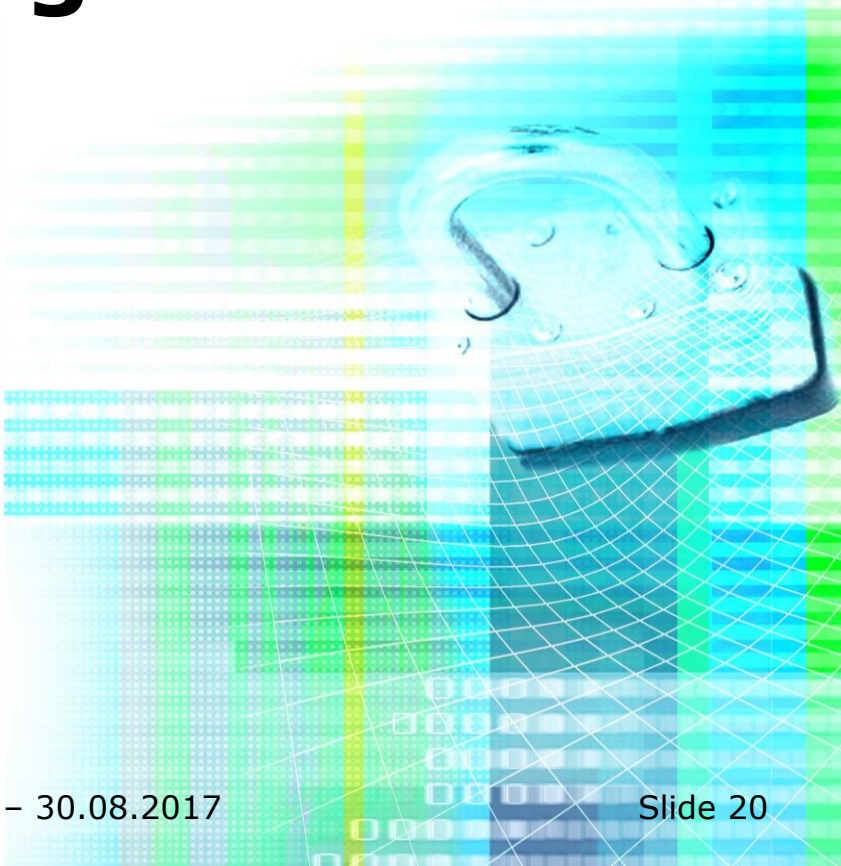
- **Daten:** Werden bereits verarbeitet oder werden für eine Verarbeitung in das Drittland übermittelt
- **Bestimmungen:** Einhaltung der EU-DSGVO auch bei Weiterübermittlung innerhalb/anderes Drittland
- **ErwG 102:** Int. Abkommen zwischen EU und Drittländern über die Übermittlung einschließlich geeigneter Garantien, werden von der EU-DSGVO nicht berührt!(Lex TTIP, CETA)

Gestufte Zulässigkeit

- **Art. 45 Angemessenheitsbeschluss**
- **Art. 46: Datenübermittlung vorbehaltlich geeigneter Garantien**
- **Art. 49 Ausnahmen für bestimmte Fälle**

Rechenschaftspflicht und daraus erwachsende Anforderungen an das Datenschutz-Management

RA Dr. Jan K. Köcher
Datenschutzauditor, DFN-CERT
koecher@dfn-cert.de



Rechenschaftspflicht

Neu:

Art. 5 Abs. 2: „Der Verantwortliche ist für die Einhaltung des Absatzes 1 [Datenschutzgrundsätze] verantwortlich und muss dessen Einhaltung nachweisen können."

Art. 24 Abs. 1: „Der Verantwortliche setzt … geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt."

Datenschutzmanagement erforderlich!
Dokumentation von Maßnahmen!

Verantwortlichkeiten

- **Verantwortlicher / Auftragsverarbeiter**
- Muss alle Anforderungen aus der EU-DSGVO erfüllen
- Grundsätzlich keine Option zur Übertragung der Umsetzung an bDSB
- **Behördlicher Datenschutzbeauftragter**
- Rein überwachende Aufgabe
- Unterstützung auf Anfrage
- Ansprechpartner für die Aufsichtsbehörden
- Keine Schulungsverpflichtung!
- **Fachbereiche**
- Unterstützung der Hochschulleitung
- Ggf. Stellung von Datenschutzkoordinatoren zur Unterstützung des bDSB

Datenschutzmanagement (1)

Datenschutzorganisation

- Bekenntnis der Leitungsebene zum Datenschutz, Förderung einer Datenschutz- und Sicherheitskultur
- Strukturelle Gewährleistung der Anforderungen
- Effektive Datenschutzkontrolle
- Datenschutzbeauftragte(r) (DSB)
- Einbindung DSB in die Geschäftsprozesse und IT-Strategie / Vorabkontrolle
- IT-SiBe/DSB: Abgestimmte Sicherheitsstrategie
- Durchsetzung in den Fachbereichen
- Gewährleistung einer Grundsicherheit
- Strukturelle Gewährleistung der Betroffenenrechte
- Strukturelle Gewährleistung der Meldepflichten
- Information und Schulung der Mitarbeiter

Datenschutzmanagement (2)

Verarbeitungsbezogen:

- Verarbeitungsverzeichnis
- Dokumentierte Maßnahmen zur Datensicherheit
- Dokumentierte Beurteilung neuer Verarbeitungen und wesentlicher Änderungen (Vorabkontrolle)
- Rechtmäßigkeit, Datensparsamkeit, Zweckbindung, Informationspflichten, Betroffenenrechte, besondere Umstände
- Gegebenenfalls: Ergänzende Maßnahmen zur Gewährleistung des Datenschutzes.
- Gegebenenfalls: Durchführung eine Datenschutz-Folgeabschätzung
- Gewährleistung der regelmäßigen/anlassbezogenen Überprüfung (Audits) von Maßnahmen auf ihre Wirksamkeit, ggf. Anpassung und Dokumentation (Plan, Do, Check, Act)

Informationssicherheit und Datenschutz

Datenschutz

- **Schutz personenbezogener Daten**
- Vertraulichkeit
- Verfügbarkeit
- Integrität

Informationssicherheit

- **Schutz personenbezogener Daten**
- **Schutz aller weiteren geschäftskritischen Informationen**
- Vertraulichkeit
- Verfügbarkeit
- Integrität

Maßnahmen

Reine Informationssicherheit Maßnahmen ohne direkte Relevanz für den Datenschutz (z.B. Einhaltung DIN-Normen, Blitzschutz)	**Reiner Datenschutz** Spezifische Maßnahmen zum Datenschutz (Meldepflichten, Führen von Verfahrensverzeichnissen)
Informationssicherheit mit gleichzeitiger Datenschutzrelevanz (z.B. Passwortsicherheit, Protokollierung, Sicherheitsbereiche, zutrittsbeschränkende Maßnahmen, Verschlüsselung)	

DFN CERT®

DFN Deutsches Forschungsnetz

Vielen Dank
für die Aufmerksamkeit

RA Dr. Jan K. Köcher
koecher@dfn-cert.de