JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

Datenschutz an der Hochschule
Informationsveranstaltung zur EU-Datenschutzgrundverordnung

Dr. Matthias Stenke
Dr. Robert Pfeffer
Axel P. Globuschütz

1. Allgemeine datenschutzrechtliche Grundlagen

2. Neuerungen durch die EU-DSGVO

3. Technische Aspekte

1.1 Grundsätze des Schutzes personenbezogener Daten

1.2 Normative Grundlagen

1.3 Abgrenzungsfragen

Was sind personenbezogene Daten?

- Personenbezogene Daten sind Einzelangaben zu persönlichen oder sachlichen Verhältnissen einer bestimmten oder (ggfs. mit Zusatzwissen) bestimmbaren natürlichen Person

- Beispiele: Name, Adresse, Geburtsdatum, Staatsangehörigkeit, Beruf, Titel, akademischer Grad, Zugehörigkeit zu einer Religionsgemeinschaft, Identifikationsnummern, wie z.B. Personal-, Matrikel-, Sozialversicherungsnummer, Semesterzugehörigkeit

Die datenschutzrechtlichen Regelungen beziehen sich auf den Umgang mit personenbezogenen Daten (Art. 1 (1) EUDSGVO, § 1 Abs. 1 HDSG, § 1 Abs. 1 E-HDSIG), andere Daten unterliegen ggfs. eigenen Regelungen (Betriebs- und Geschäftsgeheimnisse, Amtsverschwiegenheit, vertraglich vereinbarte Verschwiegenheitspflichten – z.B. Forschungsverträge)

Ausgangspunkt des modernen Datenschutzes:

Volkszählungsurteil des Bundesverfassungsgerichtes (BVerfG, Urteil vom 15. Dezember 1983 - Az. 1 BvR 209/83, BVerfGE 65, 1 ff.)

- **Es gibt kein belangloses Datum**
  - Unter den Bedingungen der elektronischen Datenverarbeitung kommt es entscheidend auf den möglichen Verwendungszusammenhang an.
- **Grundrecht auf informationelle Selbstbestimmung**
  - Herleitung aus dem allgemeinen Persönlichkeitsrecht (Art. 1 GG) und dem Recht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG), damit zunächst individualrechtliche Ausprägung des Datenschutzes, Weiterentwicklung zum Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350).

Zulässigkeit der Datenverarbeitung

- **Grundsatz**: Verbot mit Erlaubnisvorbehalt, Art. 6 EU-DSGVO
  - => die Verarbeitung personenbezogener Daten setzt eine ausdrückliche Berechtigung/Erlaubnis voraus. Diese kann sich ergeben aus:
  - Rechtsvorschriften
    - EU-DSGVO
    - Hessisches Datenschutzgesetz
    - Anderen Rechtsvorschriften (Gesetze, Verordnungen, Satzungen)
  - Einwilligung
    - Anforderungen aus § 7 HDSG, Art. 7 EU-DSGVO: i.d.R. Schriftform, Aufklärung über Verwendungszweck der Daten, Hinweis auf Widerrufsmöglichkeit, Freiwilligkeit, besondere Hinweispflichten, wenn die E. zusammen mit anderen Erklärungen abgegeben wird.

- **Transparenz (Art. 5 Abs. 1 lit. a EU-DSGVO)**
  Datenverarbeitung muss in einer für die Betroffenen nachvollziehbaren Weise erfolgen

- **Zweckbindung (Art. 5 Abs. 1 lit. b EU-DSGVO)**
  Festlegung eindeutiger und legitimer Zwecke, Erhebung und Weiterverarbeitung müssen mit diesen Zwecken vereinbar sein (Auflösung der Bindung für besondere Zwecke, Art. 89 Abs. 1 EU-DSGVO)

- **Datensparsamkeit (Datenminimierung Art. 5 Abs. 1 lit. c EU-DSGVO)**
  Die personenbezogenen Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke notwendige Maß beschränkt sein

- **Datensicherheit (Art. 5 Abs. 1 lit. f EU-DSGVO)**
  Angemessenes Sicherheitsniveau; Schutz vor unbefugter Verarbeitung, unbeabsichtigtem Verlust; unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen

Maßgebliche datenschutzrechtliche Grundlagen

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 – **EU-DSGVO** –

Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) – **BDSG** –

Hessisches Datenschutzgesetz in der Fassung vom 7. Januar 1999 (GVBl. I S. 98) zuletzt geändert durch Artikel 5 des Gesetzes vom 14. Juli 2016 (GVBl. S. 121) **– HDSG –**

Hessisches Datenschutz- und Informationsfreiheitsgesetz, gegenwärtig nur als Entwurf, Drucksache des Hessischen Landtags 19/5728 – **HDSIG** –

Bereichsspezifische Datenschutzregelungen, z.B.:

- **Hochschulstatistikgesetz**
- **§ 12 Abs.7 HHG (Alumnidaten)**
- **§ 55 HHG i.V.m. § 15 HImmatrikulationsVO (Bewerbungsdaten, Studierendendaten)**
- **Verordnung über den Betrieb von Forschungsinformationssystemen**

EU-DSGVO

- Verordnung oder Richtlinie? Zum Großteil direkte Geltung aber zugleich ca. 30 Regelungsaufträge an den nationalen Gesetzgeber, bzw. dessen Behörden
- Europaweite Geltung
- Für privaten und öffentlichen Bereich

BDSG

- Nationale Geltung
- Für private und öffentliche Stellen, aber nur für Bundesbehörden, Landesbehörden nur wenn sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden (d.h. keine Geltung für die JLU, ggfs. für ihre Vertragspartner)

HDSG (zukünftig HDSIG)

- Geltung in Hessen
- Für öffentliche Stellen (d.h. ggfs. nicht für Vertragspartner der JLU)
- Enthält Ausführungen zur **EU-DSGVO**

Bereichsspezifische Regelungen

- Anwendung entsprechend ihres definierten Anwendungsbereichs

Teil 2

Neuerungen aufgrund der EU-DSGVO

Dr. Robert Pfeffer

2. Neuerungen aufgrund der EU-DSGVO

2.1. Rechenschaftspflicht

2.2. Meldepflicht

2.3. Bußgelder

2.4. Verarbeitungsverzeichnis

2.5. Informations- und Auskunftspflichten

2.6. sonstige Betroffenenrechte

2.1. Rechenschaftspflicht (Art. 5 Abs. 2)

insbes. ggü. Aufsichtsbehörde (Hess. DSB), aber auch vor Gericht

Verantwortlicher muss nachweisen können:

- **Rechtmäßigkeit, Transparenz und Sicherheit der Verarbeitung,**
- **Einhaltung d. Zweckbindung,**
- **Richtigkeit der Daten,**
- **Datenminimierung auf erforderliches Maß und**
- **Speicherbegrenzung auf erforderliche Dauer**

→ Beweislast beim Verantwortlichen

2.2. Meldepflichten bei Verletzungen:

2.2.1 Pflicht zur Meldung an die Aufsichtsbehörde (Art. 33):

im Falle einer Verletzung des Schutzes personenbezogener Daten

(= Verlust, Veränderung oder Offenlegung von Daten)

… es sei denn, es kommt voraussichtlich zu keinem Risiko

für Rechte u. Freiheiten nat. Personen!

→ in diesem Fall dennoch Pflicht zur Dokumentation

2.2.2. Pflicht zur Mitteilung an die betroffene Person (Art. 34)

bei voraussichtlich hohem Risiko für deren Rechte und Freiheiten

2.3. Bußgelder (Art. 83):
bis zu 10–20 Mio. Euro Geldbuße für fast jeden Verstoß

- **z. B. für Verstöße gegen Grundsätze gem. Art. 5, wie z. B. die Pflicht, Daten „in einer für die betroffene Person nachvollziehbaren Weise“ zu verarbeiten**
- **Beweislast: Verantwortlicher muss Einhaltung der Verordnung nachweisen**
- **Meldepflicht (s. o.): Verantwortlicher muss sich selbst bezichtigen**
- **teilw. vertreten: kein Ermessen der Aufsichtsbehörde hinsichtlich Verhängung**

→öffentl. Verwaltung wird ausgenommen, Bußgeld trifft nur Private (Art. 83 Abs. 7, § 36 Abs. 2 HDSIG)

Strafvorschriften nach Hess. Datenschutzgesetz werden wohl im Wesentlichen gleich bleiben (entgeltliche, unerlaubte Datenverarbeitung, um sich oder andere zu bereichern oder Dritte zu schädigen)

2.4. Verarbeitungsverzeichnis (Art. 30):

statt „Verfahrensverzeichnis“ (§ 6 HDSG a.F.) nun
„Verzeichnis aller Verarbeitungstätigkeiten“ (Art. 30)

wie bisher je ein Verzeichnis für jedes Verfahren, plus ein Gesamtverzeichnis, welches sich aus den Einzelverzeichnissen zusammensetzt

Inhalt des einzelnen Verzeichnisses:

- **Verantwortlicher und Datenschutzbeauftragter**
- **Zwecke der Verarbeitung**
- **betroffene Personen (Kategorien)**
- **betroffene Daten (Kategorien)**
- **ggf. geplante Empfänger (Kategorien)**
- **ggf. geplante Übermittlung ins Ausland**
- **technische und organisatorische Maßnahmen zum Datenschutz**
- **Speicherdauer, Löschfristen**

→ also im Wesentlichen alles wie bisher (einige inhaltliche und redaktionelle Anpassungen werden erfolgen, neues Muster wird ausgegeben)

Neuerungen bzgl. Verarbeitungsverzeichnis:

- **bisherige Vorabkontrolle (§ 7 Abs. 6 HDSG a. F.) für jedes Verfahren entfällt!**
  nur noch „Datenschutz-Folgenabschätzung“ (Art. 35) bei solchen Verfahren, die voraussichtlich mit besonders hohem Risiko verbunden sind
  (z. B. Profiling mit verbindlichen Rechtswirkungen oder umfangreiche Videoüberwachung öffentlicher Räume)
  → Verarbeitungsvorgänge nebst Schutzmaßnahmen beschreiben, Risiko für Betroffene und Verhältnismäßigkeit bewerten

- **Verzeichnis ist nicht mehr öffentlich – dafür haben Betroffene div. Auskunftsrechte**

2.5. Informations- und Auskunftspflichten (Artt. 13–15)

bei Erhebung der Daten sowie jederzeit auf Anfrage Auskunft insbes. über:

- **Kontaktdaten d. Verantwortlichen u. d. Datenschutzbeauftragten,**
- **Rechtsgrundlage und Zweck der Verarbeitung,**
- **Kategorien verarbeiteter Daten,**
- **Herkunft der Daten (sofern nicht vom Betroffenen),**
- **etwaige Empfänger, insbes. in Drittländern,**
- **Speicherdauer, Löschfristen**
- **Bestehen von Auskunfts-, Berichtigungs-, Löschungsanspruch, Anspruch auf Einschränkung der Verarbeitung, Widerrufs-, Widerspruchs- u. Beschwerderecht**

→ Recht auf Kopie der Daten

gem. § 33 Abs. 1 Nr. 2 a) HDSIG nicht bei Daten, die nur noch wegen Aufbewahrungsvorschriften gespeichert sind:

→ also i.d.R. nicht mehr nach Exma., wenn Prüfungsunterlagen etc. nur noch aufgrund § 21 ImmaVO gespeichert sind

2.6. sonstige Betroffenenrechte:

2.6.1. Berichtigungsanspruch (Art. 16)

2.6.2. Löschungsanspruch „Recht auf Vergessenwerden“ (Art. 17):

z. B. wenn

- **Daten für Zwecke nicht länger nötig sind**
- **Daten rechtswidrig erhoben wurden**
- **Einwilligung widerrufen wurde**

→ gilt gem. Abs. 3 b nicht, soweit Datenverarbeitung erforderlich ist, um rechtlichen Verpflichtungen zu genügen, insbesondere bei Wahrnehmung einer Aufgabe im öffentlichen Interesse, und/oder in Ausübung öffentlicher Gewalt

2.6.3. Anspruch auf Einschränkung d. Verarbeitung (Art. 18):

z. B. wenn

- **Richtigkeit der Daten strittig ist oder**
- **Daten rechtswidrig erhoben oder für Zwecke nicht länger nötig sind,**

der Betroffene aber keine Löschung will (z. B. zwecks Rechtsverfolgung)

→ Daten werden markiert und dürfen nur noch verarbeitet werden

- **mit Einwilligung d. Betroffenen,**
- **zur Rechtsverfolgung oder**
- **zum Schutze Dritter oder wichtiger öffentlicher Interessen**

2.6.4. Widerspruchsrecht (Art. 21):

wenn Rechtsgrundlage

- **Aufgabenwahrnehmung im öfftl. Interesse**
  oder in Ausübung öfftl. Gewalt (Art. 6 Abs. 1 e) oder
- **Wahrnehmung berechtigter privater Interessen (Art. 6 Abs. 1 f)**

→ **dann bei Widerspruch: Interessenabwägung …**

→ **nicht einschlägig, wenn Rechtsgrundlage Erfüllung rechtlicher Verpflichtung!**
(Art. 6 Abs. 1 c)

2.6.5. Beschwerderecht bei Aufsichtsbehörde (Art. 77)

Teil 3

Technische Aspekte

Dr. Matthias Stenke

Was hat IT-Sicherheit mit Datenschutz zu tun?

Hauptziele der IT-Sicherheit:

- Verfügbarkeit
- Vertraulichkeit
- Integrität

→ IT-Sicherheit ist eine Voraussetzung für effektiven Datenschutz

Was ist bei der Verarbeitung personenbezogener Daten zu beachten?

- Umsetzung von technischen und organisatorischen Maßnahmen zur Gewährleistung der Einhaltung der Gesetze und Vorschriften erforderlich

Technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten (bisheriger §10 HDSG):

- Zutrittskontrolle
  - Schutz von Datenverarbeitungsanlagen vor dem Zutritt Unbefugter
  - Physische Sicherung Gebäude, Räume
- Benutzerkontrolle
  - Schutz von Datenverarbeitungsanlagen vor der Nutzung durch Unbefugte
  - Zugangssicherung durch Authentifizierung, z.B. Kennung/Passwort
- Zugriffskontrolle
  - Kontrolle des Zugriffs berechtigter Nutzer
  - Berechtigungskonzept

- Datenverarbeitungskontrolle
  - Schutz vor unbefugter/zufälliger Veränderung, Kopie, Löschung, Kenntnisnahme, Übermittlung,…
- Verantwortlichkeitskontrolle
  - Wer hat welche Daten zu welcher Zeit verarbeitet, wohin wurden/sollten diese übermittelt werden
- Auftragskontrolle (bei Auftragsdatenverarbeitung)
  - Verarbeitung nur nach Weisung des Auftraggebers
- Dokumentationskontrolle
  - Überprüfbarkeit der Datenverarbeitungsanlage und -Verfahren durch Dokumentation aller wesentlichen Verarbeitungsschritte
- Organisationskontrolle
  - Organisation muss den Anforderungen des Datenschutzes gerecht werden

Sicherheit der Verarbeitung (Art. 32 EU-DSGVO)

- Treffen von geeigneten technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
- Dabei zu berücksichtigen: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände, Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für Rechte und Freiheiten natürlicher Personen
- Konkret genannte Maßnahmen:
  - Pseudonymisierung, Verschlüsselung
  - Fähigkeit zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit von Systemen und Diensten
  - Fähigkeit zur raschen Wiederherstellung der Daten und des Zugangs bei Zwischenfällen
  - Sowie regelmäßige Prüfung der Wirksamkeit der Maßnahmen

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 EU-DSGVO)

„privacy by design“:

- Treffen geeigneter technischer und organisatorischer Maßnahmen zur
  - Umsetzung von Datenschutzgrundsätzen wie Datenminimierung
  - Einhaltung der Anforderungen der EU-DSGVO und zum Schutz der Rechte der Betroffenen
- Dabei zu berücksichtigen: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände, Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für Rechte und Freiheiten natürlicher Personen
- Bereits bei der Konzeption der Verarbeitung personenbezogener Daten mit berücksichtigen

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 EU-DSGVO)

„privacy by default“:

- Per Voreinstellung nur die personenbezogenen Daten verarbeiten, die für den jeweiligen Zweck erforderlich sind.
- Dabei zu berücksichtigen: Menge der erhobenen Daten, Umfang der Verarbeitung, Speicherfrist, Zugänglichkeit.
- Voreinstellungen müssen so sein, dass Zugänglichkeit personenbezogener Daten für die Allgemeinheit nicht ohne Eingreifen des Betroffenen möglich ist.

Anforderungen an neue (und bestehende) Systeme/Software:

- Grundsätze „privacy by design“ und „privacy by default“ beachten
- Informationspflichten beachten – lassen sich diese im System (z.B. bei Nutzer-Erstanmeldung) umsetzen?
- Auskunftspflichten beachten – können die in einem System/einer Software gespeicherten personenbezogenen Daten einer Person ermittelt werden?
- Risiko bewerten und technische und organisatorische Maßnahmen planen und umsetzen

Auskunft über die Verarbeitung personenbezogener Daten

- Auf Anfrage von Betroffenen: Auskunft, ob und welche personenbezogenen Daten verarbeitet werden und Erstellung einer Kopie dieser Daten
- Aufgabe für Verantwortliche: Konzeption und Umsetzung von Verfahren hierfür
- Noch festzulegen: Prozess zur JLU-weiten Bearbeitung von Auskünften

Unterstützungsangebote HRZ

- Beratung bei der Beschaffung von Software
- Bei Nutzung von Servern, Datenspeichersystemen und anderer Infrastruktur des HRZs in einer gesicherten Rechenzentrumsumgebung: Unterstützung bei der Beschreibung von technischen und organisatorischen Maßnahmen (Zutrittskontrolle, Zugangskontrolle) für Verfahrens-/Verarbeitungsverzeichnisse
- Beratung in Fragen der IT-Sicherheit

Diskussion/Fragen