Vorgaben der DS-GVO mit Relevanz für die Wissenschaft

Katrin Schaar

HU Berlin und ScientificData Strategies

RDA-Workshop 2017, 28.11.16, Berlin

Outline

Geltung

- Gilt seit 24.5.2016 (bereits in Kraft)
- Wird umgesetzt 25.5.2018 (dazwischen Übergangszeit)
- Nationale Regelungsmöglichkeiten für eine Reihe von Fragen (insgesamt 70 Spezifizierungsklauseln)
- Löst Datenschutzrichtlinie 95/46/EG von 1995 ab (Unterschied zwischen Richtlinie und Verordnung: Verordung gilt direkt in allen Mitgliedsländern)
- Löst Bundesdatenschutzgesetz (BDSG) und Landesdatenschutzgesetze (LDGS) ab

Bezugsrahmen

- Europäische Grundrechte Charta (GRCh)
  - Die Würde des Menschen ist unantastbar (Art.1)
  - Recht auf Achtung d. Privat- und Familienlebens (Art.7)
  - Recht auf Schutz personenbezogener Daten (Art.8 Abs.1).
    - Verarbeitung nach "Treu und Glauben für festgelegte Zwecke und mit Einwilligung" ... oder auf sonstiger gesetzlicher Grundlage.
    - Recht auf Auskunft über erhobene Daten und Berichtigung (Art. 2)
  - Aber auch: Freiheit der Kunst und Wissenschaft (Art. 13)

Sinn und Zweck

- Grundlage für das Funktionieren der Demokratie
- Abwehrrechte des Einzelnen
- Teilweise muss es einen Ausgleich geben

Anwendbarkeit der DS-GVO

- Gilt nur für personenbezogene Daten, d.h. Daten, die einer bestimmten oder bestimmbaren Person zugeordnet werden können (Art. 4 Abs. 1)
  - d.h. nicht für anonymisierte Daten (Erw-Gr. 26) und nicht für Daten von Verstorbenen (Erw-Gr. 27)
  - Allerdings: Bei Übermittlung kommt es darauf an, ob die Stelle, an die Daten übermittelt werden, eine Person wieder identifizieren kann. Dann ist Person wieder bestimmbar (Gola, Schomeres §3 Rn. 5 ff)

Zulässigkeit der Verarbeitung

- Verbot mit Erlaubnisvorbehalt: Verarbeitung personenbezogener Daten ist verboten, es sei denn es liegen Ausnahmetatbestände vor z.B.
  - Einwilligung zur Verarbeitung von pers. bez. Daten "für einen oder mehrere bestimmte Zwecke erteilt" (Art. 6 Abs. 1 lit a) sowie
  - Andere Erlaubnistatbest. (z.B. gesetzl. Regelungen, Verpflichtungen) (vgl. BDSG §4 Abs. 1 und DS-GVO Art.6 lit b-f)

Zulässigkeit der Verarbeitung

- Höherer Schutz bei Verarbeitung besonderer Kategorien personenbezogenener Daten, "aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person" (Neu: Verarb. genet. und biometrischer Daten) (Art. 9)

Geregelt sind . . .

- Verantwortlichkeit: Natürliche oder juristische Person, die über Zwecke und Mittel der Verarbeitung entscheidet (z.B. Forschungseinrichtung, vertreten durch Leiter) (Art. 5 Abs. 2, Art. 4 Abs. 7)
  - DS-Beauftragter (Art. 37-39):
    - Muss u.a. benannt werden sofern sensible Daten verarb. werden und von öffentlichen Stellen (Art. 37 Abs. 1)
    - Muss die Einhaltung der Vorschriften kontrollieren und sicherstellen und Datenschutz-Folgeabschätzung kontrollieren (Art. 39 Abs. 1 lit a-c)
- Strafen: 10 bis 20 Mio EUR bzw. 2-4 Prozent des Jahreseinkommens (Art. 83 Abs. 4)

Gefordert ist . . .

- Datenschutzfolgeabschätzung (Neu)
  - Pflicht, wenn neue Technologien Verwendung finden (Big Data) oder sensible Daten (besondere Kategorien) verarbeitet werden (Art. 23) - Relevant für medizinische, sozialwissenschaftliche Forschung
  - Dazu: Heranziehung DS-Beauftagter (Art. 35 Abs. 2)
  - Zweck und Weise der Datenverarb., Notwendigkeit, Verhältnismäßigkeit, Risiken und Sicherheitsmaßnahmen müssen beschrieben werden (Art. 35 Abs. 7)

Gefordert ist . . .

- Einwilligung (Art. 4 und 13)
  - Freiwillig, informiert, widerruflich
  - Explizit, d.h. aktive Zustimmung (Erw.Gr. 32)
  - Neu: Broad Consent (Einwilligung in "bestimmte Bereiche wissenschaftlicher Forschung" möglich)

(Erw.Gr. 33)

- Opt-in - opt-out (Erw.Gr. 33)
- Informationen über Zwecke, Kontaktdaten, Datenweitergabe, Rechte (Widerruf, Auskunft, Bereitstellung, Beschwerde, Löschung) (Art. 13 Abs. 1-2)

Gefordert ist dabei . . .

- Transparenz: Informationen sollen “in präziser, transparenter, verständlicher und leicht zugänglicher Form” dargeboten werden (Art. 12 Abs. 1)

"Spezifizierungssklauseln"

- Garantien und Ausnahmen für im öffentl. Interesse liegenden Archiv-, zu wissenschaftlichen oder historischen Forschungs- und statistischen Zwecken können durch Mitgliedsstaaten erlassen werden (Art. 89)

Artikel 89 Abs. 1

- Beschränkt sich auf genannte Zwecke; definiert Mindeststanforderungen (Paal 2017, Art. 89 Rn.1), dazu gehört
  - Unterliegt "geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person (. . .)." (Abs.1)
  - Sicherstellung, "dass technische und organisatorische Maßnahmen bestehen" (insb. Datenminimierung)
  - Neben Anonymisierung auch Pseudonymisierung möglich

Exkurs Definition pseudonymisierte Daten

- Pseudonymisiert sind Daten, (Art. 4 Abs. 5)
  - die ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.
  - Zusätzliche Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, so dass die personenbezogenen Daten nicht zugewiesen werden können
  - Schwierigkeit: Genetische Daten, Biobanken

Artikel 89 Abs.1

- Evt. zulässig: ggf. andere Maßnahmen möglich (Verschlüsselung, Verpflichtung auf Geheimhaltung) (Pauly 2017, Rn. 12)

Artikel 89 Abs. 2

- Es können nationalstaatl. "Ausnahmen von den Rechten vorgesehen werden, wenn die Zwecke sonst nicht erreicht werden können."
  - Ausnahmen betreffen Art. 15 (Auskunftsrechte), Art. 16 (Recht auf Berichtigung), Art. 18 (Einschr. der Verarb.) und Art. 21. (Widerspruchsrecht)" (Art. 89 Abs. 2)
  - Zusätzlich für im öff. Interesse liegenden Archivzwecke auch Art. 19 (Mitteilungspflicht hinsichtl. Löschung, Einschränkung, Bearb.) und 20 (Recht auf Datenübertragbarkeit an anderen Verantwortlichen)
  - **Einschränkungen danach nicht zulässig** Informationspflichten bei Erhebung (Art. 13)

Artikel 9 Abs. 4

- Zusätzliche Bedingungen und Beschränkungen können für die Verarb. von genetischen, biologischen und Gesundheitsdaten erlassen werden (Art. 9 Abs. 4)

Weitere Ausnahmen

- Weniger strenge Anforderungen bei der Speicherung/Verarbeitung wiss. Daten (für Sammlung vorhandener Daten, nicht bei Neuerhebung) (Pauly 2017, Rn. 4) bei
  - Zweckbindung. Weiterverarbeitung zu wiss. Zwecken gilt nicht als unvereinbar zu ursprünglichen Zwecken (Art. 5 Abs. 1 lit b DS-GVO)
  - Begrenzung der Speicherdauer. Im wissenschaftl. Kontext können Daten länger gespeichert werden, sofern Garantien (s.o.) eingehalten werden (Art. 5 Abs. 1 lit e DS-GVO)

Weitere Ausnahmen

- Besonderen Kateg. personenbez. Daten unter best. Voraussetzung (Angemessenh., Wahrung Rechte, TOMs) (Art. 9 Abs. 2 lit j DS-GVO)
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 Abs. 5 lit b DS-GVO)
- Recht auf Löschung ("Recht auf Vergessenwerden") (Art. 17 Abs. 3 lit d)
- Widerspruchsrecht (Art. 21 Abs. 6 DS-GVO) (nur bei Vorliegen eines (festgestellten) öffentlichen Interesses)

Konsequenzen

- Verfahren für Datenschutzfolgeabschätzung bei Verarb. sensibler Daten erarbeiten
  - Datenschutzbeauftragten frühzeitig einbeziehen
- Einwilligungserklärungen anpassen
- Opt-In Opt-Out Möglichkeiten gewähren, aber auch in Datenbanken abbilden
- Widerrufmöglichkeiten technisch in Datenbanken umsetzen

Konsequenzen

- Größerer Stellenwert von Anonymisierungsverfahren/Pseudonymisierungverfahren
- Dokumentation erforderlich, z.B. über Datenweitergabe und verarb. Kategorien von Daten erforderlich
- Nutzungsseite prüfen:
  - Über welche Referenzinformationen verfügt ein Datennutzer
  - Zweck der Nutzung prüfen (Achtung bei: Kommerziellem Nutzer, wobei "Wissenschaftliche Nutzung" weit ausgelegt wird (auch private Forschung), Erwäg.Gr. 159)

Fragen

- Ausgestaltung der nationalen Gesetzgebung wesentlich, aber momentan offen (z.B. Art. 89 und 9)
- Ersterhebung - Weiterverarbeitung (es gelten u.U. andere Regeln)
- Grauzone Biobanken, verknüpfte Daten, insb. Gesundheitsdaten und genetische Daten - sind bei der weiteren Verarbeitung dieser Daten die geforderten Garantien (Art. 89) erfüllbar? (Stichw. Anonymisierung)
- Grenzen der Open-data-Nutzung (Realisierbarkeit der Vorgaben, Aspekt z.B. Vertrauen von Forschugnssubjekten)

Fragen

- Schwierigkeit bei der Einwilligung (Broad Consent)
  - Was ist informiert?
  - Wie weit darf eine Einwilligung gehen, ohne Wesensgehalt von Grundrechten/Primärrecht zu beeinträchtigen?

Dank

Vielen Dank für Ihre Aufmerksamkeit!

Literatur

Gola, Peter; Klug, Christoph; Körffer, Barbara; Schomerus, Rudolf (2015): Bundesdatenschutzgesetz. BDSG ; Kommentar. 12., überarb. und erg. Aufl. München: Beck.

Monlnár-Gábor, Fruzsina; Korbel, Jan (2016): Verarbeitung von Patientendaten in der Cloud. Die Freiheit transnationaler Forschung und der Datenschutz in Europa. In: Zeitschrift für Datenschutz (ZD) 6 (6), S. 274–281.

Pauly, Daniel A. (2017): Art. 89. In: Boris P. Paal und Daniel A. Pauly: Datenschutz-Grundverordnung. München, München: C.H.Beck (Beck'sche Kompakt-Kommentare).

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. EUR-Lex 23.11.1995.

Schaar, Katrin (2016): DS-GVO: Geänderte Vorgaben für die Wissenschaft. Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen? In: Zeitschrift für Datenschutz (ZD) (05), S. 224–226.

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) 04.05.2016.

+++

Technisch-Organisatorische Maßnahmen

- Technische Maßnahmen
  - z.B. Umzäunung Gebäude
  - Sicherung Fenster
  - Bauliche Maßnahmen
  - Alarmanlagen
  - Benutzerkonto
  - Passworterzwingung
  - Log-In
  - Benutzeridentifikation

Technisch-Organisatorische Maßnahmen

- Organisatorische Maßnahmen
  - Besucheranmeldung
  - Arbeitsanweisungen
  - Vier-Augen-Prinzip
  - Stichprobenprüfung

TOMs nach BDSG § 9

- Zutrittskontrolle (Gebäudesicherung, Sicherung der Räume)
- Zugangskontrolle (Zugang zu Rechnern/Systemen, Firewall)
- Zugriffskontrolle (Berechtigungskonzepte, Paßwortschutz etc.)
- Weitergabekontrolle (Sicherung bei elektr. Weitergabe, Protokolle, bei Transport etc.)
- Eingabekontrolle (Benutzeridentifikation, Protokollierung)
- Verfügbarkeitskontrolle (Stromversorgung, Backupkonzept, Schutz vor Diebstahl)
- Trennungsgebot (getrennte Ordnerstrukturen, separate Tables in DB)