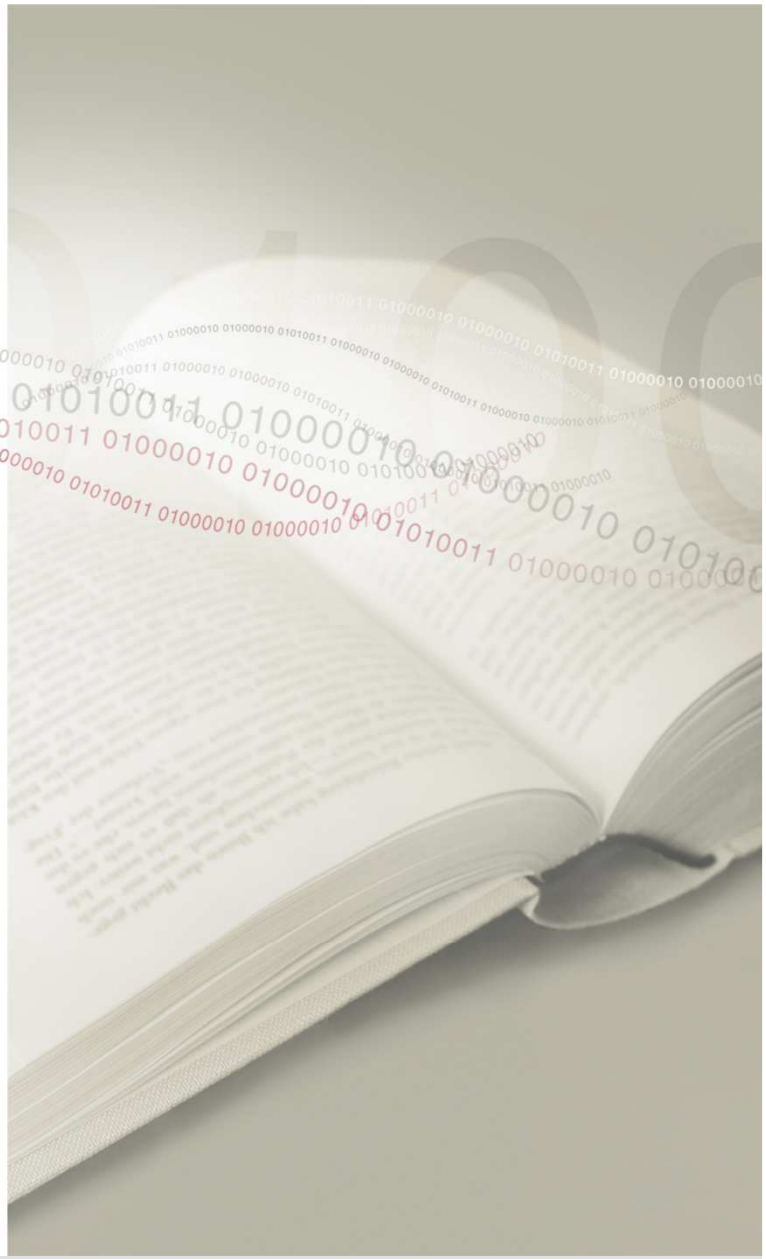
Bayerische StaatsBibliothek
Information in erster Linie



Die EU-Datenschutz-Grundverordnung (DSGVO) von 2016:

Was erwartet uns?

Dr. Stephan Schwarz, MPA
Bayerische Staatsbibliothek
Referatsleiter Informationsdienste und Ortsleihe
Stellv. Leiter Abteilung Benutzungsdienste

31. Mai 2017

„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 Richtlinie 95/46/EG“

kurz: DSGVO

Ziele der DSGVO

1. **Vereinheitlichung** des Datenschutzrechts in der gesamten EU
   - „Vollharmonisierung“
2. **Modernisierung** des Datenschutzrechts; bessere Antworten auf die Herausforderungen durch
   - Globalisierung
   - Technische Innovationen wie Digitalisierung, Internet, „Big Data“, Cloud Computing, Mobile Computing, Standortdatenerhebung etc.
3. **Verbesserung des Grundrechtsschutzes**
   - vgl. z.B. Art. 8 EMRK und Artt. 7 u. 8 GRCh
   - oder: Art. 16 AEUV
   - oder auch : Art 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG („Allgemeines Persönlichkeitsrecht“ / „Recht auf informationelle Selbstbestimmung“)

Andrea Voßhoff
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

„Die Datenschutz-Grundverordnung bietet zudem einen wirksamen Regelungsmechanismus, um auch im **Zeitalter der Digitalisierung und von Big-Data das Grundrecht jedes Einzelnen auf informationelle Selbstbestimmung** im Verhältnis zu den staatlichen und kommerziellen Interessen zu sichern. Dabei lässt sie der deutschen und europäischen Digitalwirtschaft ausreichend Spielraum, innovative und intelligente Geschäftsmodelle zu entwickeln, die das in den vorhandenen enormen Datenmengen liegende Potential ökonomisch verwertbar machen und dabei zugleich die datenschutzrechtlichen Vorgaben beachten. **Guter Datenschutz ist ein Qualitätsmerkmal der europäischen Wirtschaft**.“

BfDI Info 6: Datenschutz-Grundverordnung, Bonn 2017, S. 8.
https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=24

Entwicklung

- 25.01.2012: 1. Entwurf durch EU-Kommission

⋮

- Juni – Dez. 2015: Trilogverfahren (EU-Parlament, Rat, Kommission)
- 08.04.2016: Beschluss im EU-Rat
- 14.04.2016: Annahme durch EU-Parlament
- 04.05.2016: Veröffentlichung im Amtsblatt der EU
- 25.05.2016: DSGVO tritt in Kraft (Übergangsfirst: 2 Jahre)

Fahrplan

- Bis 24.05.2018: Das Recht der Mitgliedstaaten ist an die Vorschriften der DSGVO anzupassen und die Regelungsaufträge sind umzusetzen
- Ab **25.05.2018**: DSGVO ist in allen Mitgliedstaaten unmittelbar und mit **Anwendungsvorrang** anzuwenden

Verhältnis der DSGVO zum nationalen Datenschutzrecht

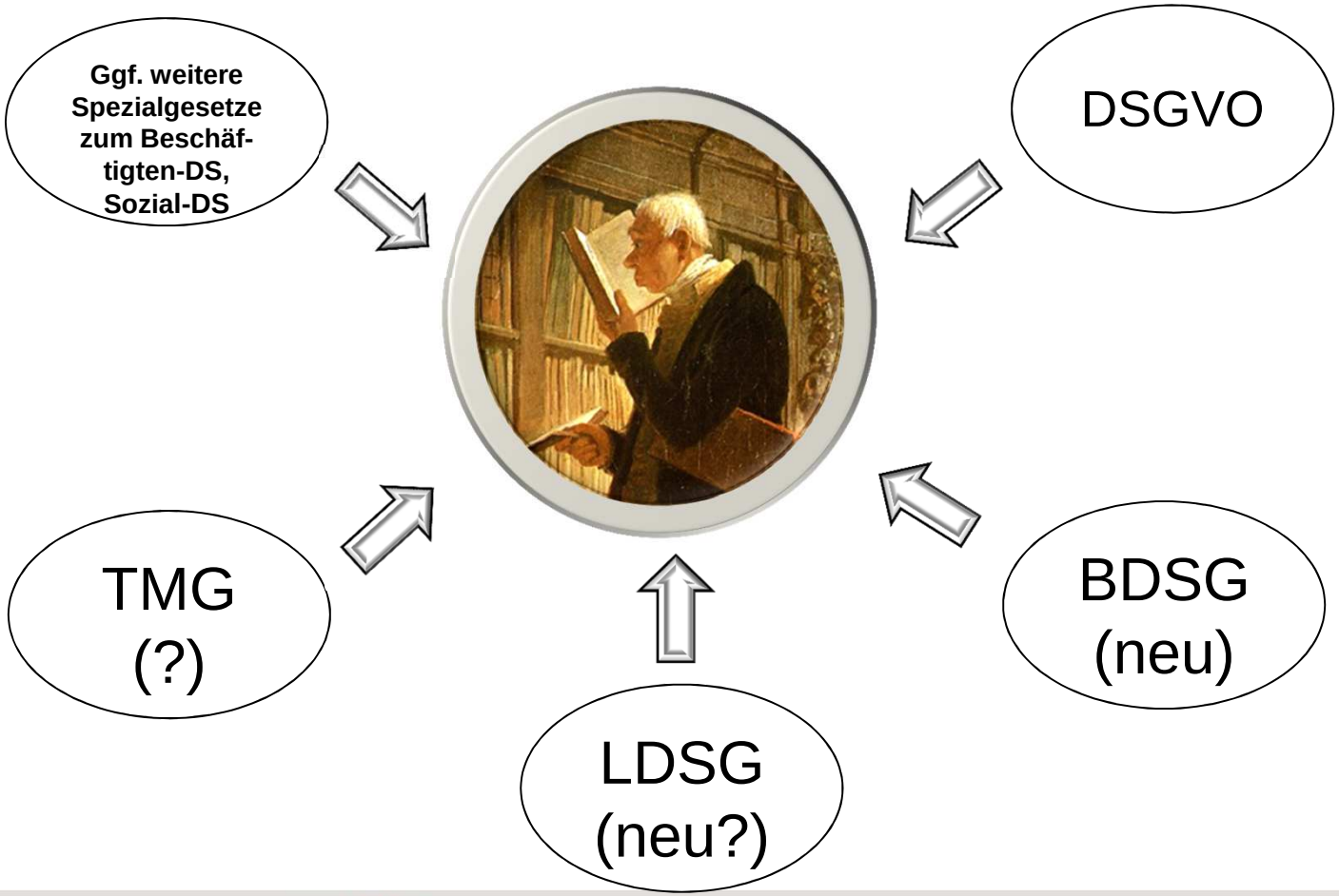
- **Verordnung** der Europäischen Union („*regulation*“): Art. 288 AEUV
  - Allgemeine Geltung (Art. 288 Abs. 1 AEUV)
  - In allen ihren Teilen verbindlich (Art. 288 Abs. 2 AEUV)
- Mit Inkrafttreten ist sie Teil der Rechtsordnung eines jeden Mitgliedsstaates, ohne nationalen Umsetzungsakt wie bei EU-Richtlinien („*directive*“)
- **Anwendungsvorrang** vor den nationalen Rechtsordnungen (entspricht seit über 50 Jahren der Rechtsprechung des EuGH)
- D.h. die DSGVO ist von **allen nationalen Behörden** und **Gerichten** vorrangig anzuwenden
- Problem: ca. **70 (!) Öffnungsklauseln** mit Regelungsaufträgen und Regelungsoptionen für die nationalen Gesetzgeber
- Insgesamt: Erhebliches Maß an **Rechtsunsicherheit**

Prof. Dr. Alexander Roßnagel:

„Aufgrund der Unterkomplexität der Unionsregelungen sind mitgliedstaatliche Präzisierungen, Ausfüllungen und Ergänzungen notwendig, um die Verordnung für die faktischen Probleme, die es zu bewältigen gilt, anwendbar zu machen. Aus diesem Grund ist die Datenschutz-Grundverordnung **kein homogenes, in sich geschlossenes Gesetzeswerk** für den Datenschutz in der Union, sondern gleicht eher einem „**Schweizer Käse**“, der zwar einige strukturierende Elemente aufweist, vor allem aber **durch die Löcher darin auffällt**. Anders als bei einem Schweizer Käse werden diese Löcher aber **unterschiedlich gefüllt**. In der Folge wird kein einheitliches Datenschutzrecht in allen Mitgliedstaaten zur Anwendung kommen. Vielmehr werden vergleichbar viele Unterschiede wie zuvor unter der Datenschutzrichtlinie bestehen – nur an anderen Stellen und mit erheblicher **Rechtsunsicherheit**.“

A. ROßNAGEL, in: DERS. [HRSG.], Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts. Baden-Baden 2017 (NomosPraxis), S. 62.

Was hat der Rechtsanwender in Bibliotheken zu berücksichtigen?



Wie geht es weiter?

Es bleibt ein **knappes** Jahr …

A) Für die nationalen Gesetzgeber

- die jeweiligen nationalen Rechtsordnungen an das neue Recht anzupassen
- d.h. nach Möglichkeit alles streichen, was sich nicht mit der DSGVO in Einklang bringen lässt
- Ziel: Rechtsunsicherheit beseitigen (soweit das möglich ist!)
- Beispiel: BDSG (neu) im Rahmen des DSAnpUG-EG
  - Verabschiedung im Bundestag: 27.04.2017
  - Annahme durch den Bundesrat: 12.05.2017

B) Für Rechtsanwender (z.B. in den Bibliotheken, Hochschulen, etc.)

- Sich auf die Anwendbarkeit der DSGVO vorzubereiten („Awareness“)
- Sich zu informieren und die eigenen datenschutzrechtlich relevanten Prozesse und Strukturen in der Weise zu optimieren, dass sie mit der künftigen Rechtslage übereinstimmten („Compliance“)

Was bleibt gleich?

Die DSGVO schreibt die **bisherigen datenschutzrechtlichen Grundprinzipien** im Wesentlichen fort oder entwickelt sie weiter, z.B.

- Personenbezogene Daten (Art. 4 Nr. 1 DSGVO)
- Rechtmäßigkeit der Datenverarbeitung (Art. 6 DSGVO): „**Verbot mit Erlaubnisvorbehal**t“, d.h.
  a. Einwilligung (**Achtung**: höhere Anforderungen als bisher, vgl. Art. 7 DSGVO)
  b. Eine in der DSGVO normierte Ausnahme (für Bibliotheken v.a. Art. 6 Abs. 1 Buchst. e DSGVO: Handeln im öffentlichen Interesse)
- Datensparsamkeit (Art. 5 Abs. 1 Buchst. c DSGVO)
- Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO)

Grundsätzlich auch vergleichbar wie bisher:

- „Verantwortliche Stelle“ (BDSG) => jetzt: „Verantwortlicher“ (DSGVO)
- „Auftragsdatenverarbeitung“ (BDSG) => jetzt: „Auftragsverarbeitung“ (DSGVO)
- Datentransfer in Drittsaaten (außerhalb EU): „angemessenes Datenschutzniveau“, „EU-US Privacy Shield“, EU-Standardvertragsklauseln, „Binding Corporate Rules“ (BCS), Zertifizierungen

Was ist grundsätzlich neu (in Auswahl)?

- Marktortprinzip
- „One-Stop-Shop“-Verfahren
- Kohärenzverfahren bei der Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden
- Datenportabilität (Art. 20 DSGVO)
- Recht auf Vergessenwerden (Art. 17 Abs. 2 DSGVO)
- Stärkung der Datenschutzaufsichtsbehörden
  - Weitaus höhere Sanktionsmöglichkeiten / Erhöhung des Bußgeldrahmens
  - Gemäß Art. 58 DSGVO auch Anordnungen gegenüber Behörden möglich, z.B. Unterbinden einer rechtswidrigen Datenverarbeitung, Löschung bestimmter Daten oder Verbot einer Datenübermittlung in Drittstaaten

Was ist neu und relevant für Bibliotheken?

- Erweiterung des Transparenzgebots (umfangreiche, proaktive Informationspflichten, Art. 13 u. 14 DSGVO)
  - z.B. Überarbeitung von Datenschutzerklärungen für Bibliothekswebsites
- Hoher Stellenwert des technischen Datenschutzes
  - Privacy-by-Design (Art. 25 Abs. 1 DSGVO)
  - Privacy-by-Default (Art. 25 Abs. 2 DSGVO)
- Datenschutz-Folgeabschätzung (Art. 35 DSGVO)
- Änderungen beim behördlichen Datenschutzbeauftragten
- Neue Gestaltung von Einwilligungen (Art. 7 DSGVO)
- Auskunftspflichten gegenüber den Betroffenen (Art. 15 DSGVO)
- Meldepflichten bei Datenpannen (Art. 33 f. DSGVO)

ToDos und Empfehlungen für Bibliotheken

- Überarbeiten der Einwilligungen (Art. 7 DSGVO)
- Umfassende Rechenschaftspflicht / Dokumentationspflicht des Verantwortlichen beachten: Art. 5 Abs. 2, Art. 24 u. Art. 32 DSGVO („**Accountability**“)
- Entwurf einer **Datenschutz-Policy**: Wie soll der Datenschutz in der Bibliothek geregelt sein?
- Analyse sämtlicher datenschutzrechtlich relevanter Prozesse (**Risikoanalyse**)
- Ggf. Datenschutz-Folgeabschätzungen (Art. 35 DSGVO)
- Führen eines Verfahrensverzeichnisses (Art. 30 DSGVO)
- (Erweiterte) **Informationspflichten** und des **Auskunftsrecht** beachten
- Gewährleistung der **Datensicherheit** (technische und organisatorische Maßnahmen, gemäß Art. 32 DSGVO) und der Prinzipien **Privacy-by-Design** und **Privacy-by-Default** (Art. 25 DSGVO)
- Melde**pflicht** bei Datenpannen und Datenschutzverstößen (Art. 33 DSGVO)
  - innerhalb von 72 Stunden!
- **Empfehlung**: Einführung eins **Datenschutz-Managementsystems**

BSB Bayerische StaatsBibliothek
Information in erster Linie