Der Landesbeauftragte für den

DATENSCHUTZ und die INFORMATIONSFREIHEIT

Rheinland-Pfalz

Die Datenschutz-Grundverordnung: Ein neues Datenschutzrecht in der EU

Gliederung

1. Die DS-GVO: Grundlagen und Systematik
2. Maßnahmen zur Umsetzung
3. Fazit und Ausblick

1. Die DS-GVO: Grundlagen und Systematik

Datenschutzreform

- **Datenschutz-Grundverordnung (DS-GVO)** - Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Engl.: **General Data Protection Regulation (GDPR)**
- **Gilt ab: 25. Mai 2018**
- **Betrifft:** Regelt umfassend den Datenschutz bei privaten und öffentlichen Stellen
- **Außerdem:** EU-Richtlinie für Justiz und Inneres (**JI-Richtlinie**)
  - Gilt für Strafverfolgung und –vollstreckung, Gefahrenabwehr

Regelungsziel und Ansatz

- **Ziel: Harmonisierung** des Datenschutzrechts in der EU

- **Gewähltes Instrument:** Verordnung
  - Im Gegensatz zur bisherigen Datenschutz-RL ohne Umsetzung direkt anwendbar
  - Anwendungsvorrang gegenüber mitgliedstaatlichem Recht

- **Kommissionsentwurf:**
  - Abstrakte Regelungen
  - Konkretisierung durch weitere Rechtsakte der Kommission

- **Rat und Parlament:**
  - Rechtsakte durch Kommission gestrichen
  - Stattdessen Öffnungsklauseln für die Mitgliedstaaten

- **Ergebnis: Komplexes Miteinander** von DS-GVO und nationalem Recht

Wichtige Normbereiche

Art. 2: Sachliche Anwendbarkeit - Private und öff. Stellen (außer Justiz und Inneres)
Art. 3: Räumliche Anwendbarkeit - Marktortprinzip
Art. 5: Grundsätze der Verarbeitung
Art. 6: Erlaubnistatbestände
Art. 7 und 8: Einwilligung
Art. 9: Besondere Kategorien von Daten (z.B. Gesundheitsdaten)
Art. 12 bis 23: Betroffenenrechte
Art. 25: Datenschutz durch Technik
Art. 28: Auftragsverarbeitung
Art. 30: Verzeichnis von Verarbeitungstätigkeiten
Art 32: Sicherheit der Verarbeitung
Art. 35 Datenschutzfolgenabschätzung
Art. 37 bis 39: Datenschutzbeauftragter
Art. 40 und 41: Verhaltensregeln
Art. 42 und 43: Zertifizierung
Art. 44 bis 50: Übermittlung in Drittländer
Art. 51 bis 76: Aufsichtsbehörden und deren Zusammenarbeit in der EU
Art. 77 bis 84: Rechtsbehelfe und Sanktionen
Art. 85 bis 91: Besondere Verarbeitungssituationen

Wichtige Öffnungsklauseln

- Art. 6 Abs. 2 i.V.m. Abs. 1 UAbs. 1 lit. c und e: Öffentliche Stellen → LDSG
- Art. 9 Abs. 2 lit. j: Besondere Kategorien von Daten → § § 27, 28 BDSG
- Art. 23: Beschränkungen von Betroffenenrechten → § 32 BDSG
- Art. 22 Abs. 2 lit. b: Automatisierte Entscheidungen → § 31 BDSG
- Art. 88: Beschäftigtendatenschutz → § 26 BDSG
- Art. 37 Abs. 4: Datenschutzbeauftragte im privaten Bereich → § 38 BDSG

Anpassungen in Deutschland

- Bundesdatenschutzgesetz (neu):
  - gilt ebenfalls ab **25.5.2018**
  - Passt BDSG an DS-GVO an und setzt JI-RL um
- Landesdatenschutzgesetz Rheinland-Pfalz (neu):
  - im Gesetzgebungsprozess, **geplant für 25.5.2018**
- Sozialdatenschutz (insb. SGB X neu):gilt ebenfalls ab **25.5.2018**
- Anpassungen in weiteren Gesetzen zu erwarten
  - Z.B. TMG, TKG

Neues Recht, neues Vokabular

alt		neu
• verantwortliche Stelle	→	• Verantwortlicher
• Betroffener	→	• Betroffene Person
• Auftragsdatenverarbeitung	→	• Auftragsverarbeitung
• Auftragnehmer	→	• Auftragsverarbeiter
• Sperrung	→	• Einschränkung der Verarbeitung
• Datei	→	• Dateisystem
• besondere Arten personenbezogener Daten	→	• besondere Kategorien personenbezogener Daten

2. Maßnahmen zur Umsetzung

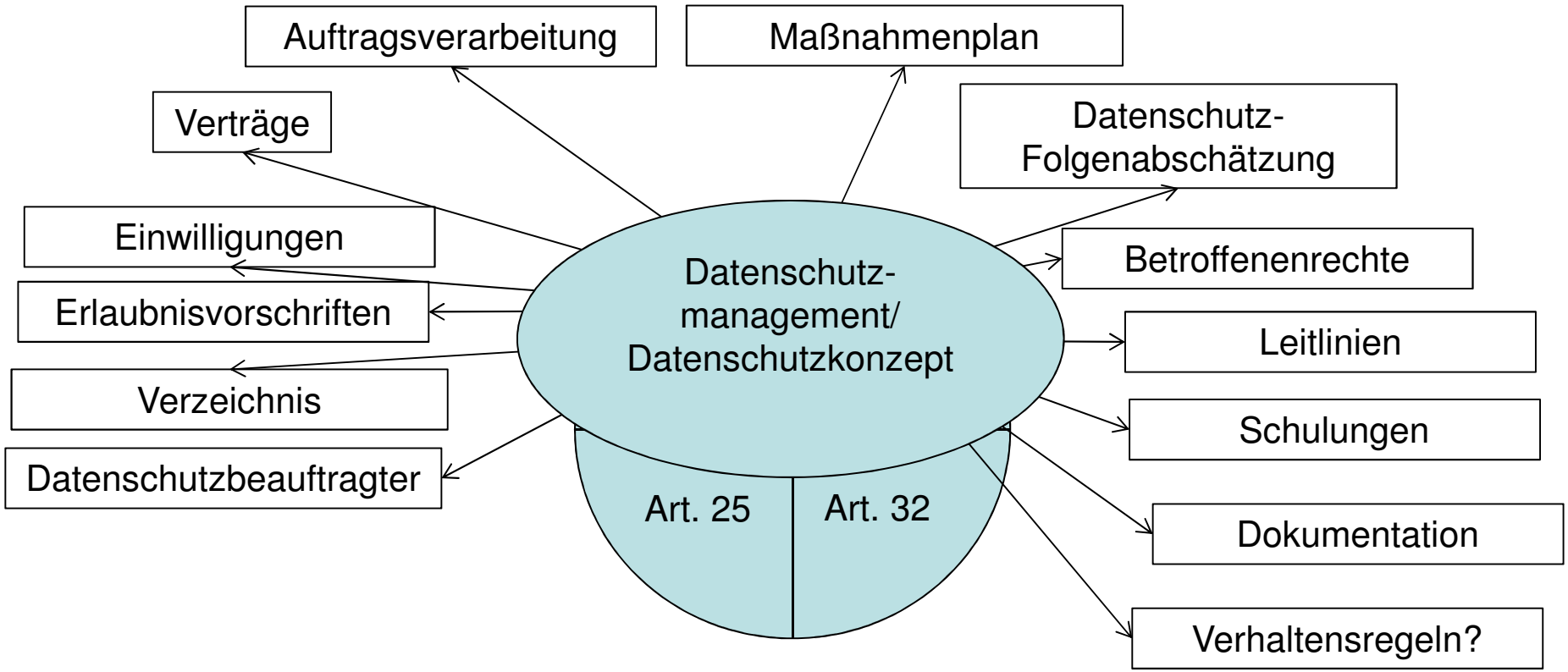
Übersicht: Wichtigste Maßnahmen

- Einrichtung eines Datenschutz-Managements (Art. 24)
- Benennung eines Datenschutzbeauftragten (Art. 37 ff.)
- Einrichtung eines Verfahrensverzeichnisses (Art. 30)
- Anpassung eigener Verarbeitungsvorgänge an Erlaubnistatbestände (insb. Art. 6)
- Anpassung datenschutzrechtlicher Einwilligungen (Art. 7 und 8)
- Umsetzung Pflichten zu Information und Auskunft an betroffene Personen (Art. 12 ff)
- Durchführung Datenschutz-Folgenabschätzungen (Art. 35)
- Umsetzung technischer Datenschutz (Art. 25) und der Datensicherheit (Art. 32)
- Anpassung von Aufträgen im Sinne der Auftragsverarbeitung (Art. 28)
- Schulung der eigenen Mitarbeiter im Hinblick auf die neue Rechtslage.

Art. 24: Datenschutz-Management

- Allgemeine Pflicht zur Implementierung von Maßnahmen, damit Verarbeitung verordnungsgemäß abläuft
- Datenschutz ist Chefsache
- Art. 25 und 32 sind speziellere Ausprägungen desselben Prinzips
- Datenschutzkonzept erarbeiten, umsetzen und nachweisen können
- Risikoanalyse: Art und Umfang der Datenverarbeitung, Wahrscheinlichkeit und Schwere des Eintritts für Rechte der Betroffenen

Art. 24: Datenschutz-Management



Der Datenschutzbeauftragte – Benennung Art. 37

Pflicht zur Bestellung gemäß Art. 37 Abs. 1 Nr. 3 DS-GVO:

- Wenn Kerntätigkeit umfangreiche Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtl. Verurteilungen und Straftaten
  - ➢ Umfangreich: Bsp. Krankenhaus (+), einzelner Arzt i.d.R. (-)

Pflicht besteht auch gemäß § 38 BDSG:

- Wenn mindestens 10 Mitarbeiter ständig mit automatisierter Verarbeitung personenbezogener Daten beschäftigt
  - ➢ Bsp: Zehn Außendienstmitarbeiter verarbeiten bei jedem Termin Daten auf ihrem mobilen Gerät
- **Und:** Wenn Datenschutz-Folgenabschätzung nötig (Positiv-Liste der Aufsichtsbehörden in Arbeit)

Der Datenschutzbeauftragte – Benennung Art. 37

- Auswahl anhand beruflicher Qualifikation und Fachwissen Art. 37 Abs.5
- DSB sowohl intern als auch extern möglich Art. 37 Abs. 6
- Besteller veröffentlicht Kontaktdaten des DSB Art. 37 Abs. 7

Der Datenschutzbeauftragte – Stellung Art. 38

- Frühzeitig einzubinden, wenn Bezug zu Datenschutz Art. 38 Abs.1
- Unterstützungspflicht inkl. Ressourcen Art. 38 Abs. 2
- Keine Anweisungen bzgl. seiner Aufgaben, Art. 38 Abs. 3 S. 1
- Keine Nachteile wg. Erfüllung seiner Aufgaben Art. 38 Abs. 3 S. 2
- Berichtet unmittelbar an oberste „Managementebene“ Art. 38 Abs. 3 S. 3
- Ansprechpartner der Betroffenen Art. 38 Abs. 4
- An Wahrung der Geheimhaltung/Vertraulichkeit gebunden Art: 38 Abs. 5
- Wenn auch andere Aufgaben, Vermeidung von Interessenskonflikten Art. 38 Abs. 6

Der Datenschutzbeauftragte – Aufgaben Art. 39

- Unterrichtung und Beratung des Bestellers und seiner Beschäftigten hinsichtlich DS-GVO u.a. Datenschutzvorschriften (Art. 39 Abs. 1 lit. a)
- Überwachung der Einhaltung der DS-GVO, inkl. Strategien des Bestellers und Schulungen (Art. 39 Abs. 1 lit. b)
- Beratung zur Datenschutz-Folgenabschätzung (Art. 39 Abs. lit. c)
- Zusammenarbeit mit Aufsichtsbehörde und Anlaufstelle für diese (Art. 39 Abs. 1 lit. d und e)

- ABER: Datenschutz bleibt Chefsache!

Verzeichnis von Verarbeitungstätigkeiten: Pflicht und Form

- Zwei Pflichtverzeichnisse:
  - Verantwortliche nach Art. 30 Abs. 1
  - Auftragsverarbeiter nach Art. 30 Abs. 2

- Ausnahme in Art. 30 Abs. 5: klingt weit, ist sie aber nicht, gilt insb. nicht wenn besondere Kategorien verarbeitet werden

- Schriftlich zu führen, inkl. elektronischer Form, Abs. 3

- Auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen

- Aber: keine Verfügbarkeit für jedermann mehr

Verzeichnis von Verarbeitungstätigkeiten: Inhalt

- Verantwortliche
  - Name und Kontaktdaten des Verantwortlichen und seines DSB
  - Zwecke der Verarbeitung
  - Kategorien von Daten und betroffenen Personen
  - Kategorien von Empfängern
  - Übermittlungen in Drittland, evtl. inkl. geeigneter Garantien
  - Löschfristen
  - Technische und organisatorische Maßnahmen nach Art. 32
- Auftragsverarbeiter
  - Name und Kontaktdaten des Auftragsverarbeiters und der Verantwortlichen inkl. der DSB
  - Kategorien von Verarbeitungen
  - Übermittlungen in Drittland, evtl. inkl. geeigneter Garantien
  - Technische und organisatorische Maßnahmen nach Art. 32

Erlaubnistatbestände

Art. 6 Abs. 1 DS-GVO

- Verarbeitung aufgrund von Einwilligungen
- Vertragsdatenverarbeitung
- Verarbeitung aufgrund rechtlicher Verpflichtungen
- Verarbeitung für berechtigte Interessen

Art. 9 Abs. 2

- Regeln für Verarbeitung besonderer Kategorien von Daten

➢ Bei besonderen Kategorien sind Art. 9 und Art. 6 kumulativ anzuwenden

Einwilligung Art. 7, 8 und Art. 9

Alte Rechtslage	DS-GVO
freiwillig	freiwillig
Informiert	Informiert, neue Informationsinhalte
zweckgebunden	Zweckgebunden
schriftlich	Kein Formerfordernis, stattdessen Ausdrücklichkeit
Hervorgehoben	Hervorgehoben
Kopplungsverbot	Ausdrücklich und allgemein geregelt
Widerrufsrecht	Ausdrücklich geregelt, außerdem Hinweispflicht
Ausdrücklichkeit bei besonderen Datenarten	Ausdrücklichkeit bei besonderen Datenkategorien

Bestehende Einwilligungen

- ErwGr. 171: alte Einwilligungen können fortbestehen und müssen nicht neu eingeholt werden, wenn sie den Vorgaben der Verordnung entsprechen

- Beschluss Düsseldorfer Kreis: dies betreffe nicht Informationspflichten nach Art. 13 DS-GVO
  - Mit Vorsicht zu genießen, Einwilligung könnte dann auch schon nach alter Rechtslage unwirksam sein und kann gar nicht fortgelten

- Dringende Empfehlung: Einwilligungen, die nicht Vorgaben der DS-GVO entsprechen neu einholen, wenn möglich

- Erleichterung hierbei: Schriftform nicht mehr notwendig

Betroffenenrechte

- Art. 12: Transparente Information, Modalitäten der Betroffenenrechte
  - Insb.: präzise, transparent, verständlich, leicht zugänglich, insb. für Informationen an Kinder
  - Erleichterung der Ausübung von Art. 15 ff.
  - Informationen möglichst schriftlich, elektronisch und mündlich abrufbar halten

- Art. 13 und 14: Information der betroffenen Personen
- Art. 15: Auskunftsrecht
- Art. 16: Recht auf Berichtigung
- Art. 17: Recht auf Löschung
- Art. 18: Recht auf Einschränkung der Verarbeitung
- Art. 20: Recht auf Datenübertragbarkeit
- Art. 21: Widerspruchsrecht

Art. 35: Datenschutz-Folgenabschätzung

- Formalisierte Risikoanalyse und Maßnahmenplan bei Verarbeitungen, die voraussichtlich mit hohem Risiko für betroffene Personen einhergehen,
- ersetzt Vorabkontrolle nach altem Recht
- Insb. neue Technologien, Profiling, umfangreiche Verarbeitung besonderer Kategorien, systematische Überwachung öffentlich zugänglicher Bereiche
- Prüfen, ob erforderlich nach Art. 35 Abs. 2 oder Abs. 1 (Positiv-Liste der Aufsichtsbehörden in Arbeit)
- Risiko bewerten (kann zu vorheriger Konsultation nach Art. 36 führen)
- Abhilfemaßnahmen planen und treffen
- Bestandsverfahren: Überprüfung nur bei relevanten Änderungen erforderlich

Art. 25: Datenschutz durch Technik

- Abs. 1: Technische und organisatorische Maßnahmen, um Datenschutzgrundsätze technisch umzusetzen
- Faktoren für die Festlegung von Maßnahmen: Stand der Technik, Kosten, Art, Umstände und Zwecke der Datenverarbeitung, Risiken für die betroffenen Personen
- Leitlinien zu Maßnahmen z.B. ENISA, weitere Informationen LfDI
- Abs. 2: Datenschutzfreundliche Voreinstellungen
- Nachweis Abs. 3: Zertifizierung und Verhaltensregeln
- ErwGr. 78: Datenschutz durch Technik ist bei öffentlichen Ausschreibungen zu beachten

Art. 32: Sicherheit der Verarbeitung

- Technische und organisatorische Maßnahmen, um Verarbeitungsverfahren, die personenbezogene Daten verarbeiten, insb. vor Missbrauch zu schützen
- Faktoren für die Festlegung von Maßnahmen: Stand der Technik, Kosten, Art, Umstände und Zwecke der Datenverarbeitung, Risiken für die betroffenen Personen (wie Art. 25)
- Z.B. Verschlüsselung, Zugriffsberechtigungen, etc.
- Neu: ausdrücklich regelmäßige Überprüfungen Art. 32 Abs. 1 lit. d

Auftragsverarbeitung Art. 28 DS-GVO

- Z.B. IT-Wartungsdienstleister, der Zugriff auf personenbezogene Daten hat
- BDSG (neu) enthält keine eigenen Regelungen mehr, im neuen LDSG auch so zu erwarten
- Keine grundsätzliche Neuausrichtung, im Detail aber Unterschiede, insb. bei den Inhalten der Aufträge
- Anpassung bestehender Aufträge an Art. 28 DS-GVO in manchen Punkten notwendig (Unteraufträge, Datenpannen melden)
- In Zukunft für Aufträge auch elektronisches Format möglich

Auftragsverarbeitung

- „Privilegierung“ der Auftragsverarbeitung: noch unklar, ob in der alten Form enthalten,

- LfDI tendiert dazu, Übermittlung an Auftragsverarbeiter als Weiterverarbeitung einzuordnen

- i. E. wird aber Übermittlung zwischen Auftraggeber und Auftragsverarbeiter im Regelfall weiter möglich sein, die DS-GVO bekennt sich klar zur Auftragsverarbeitung

- Verantwortlichkeit: grds. gleichartig wie bisher
  - Auftragsverarbeiter weisungsgebunden und nicht verantwortlich
  - Allerdings neu: eigene Haftung für Verletzung eigener Pflichten (Schadensersatz und Geldbußen
  - DS-GVO nimmt an vielen Stellen den Auftragsverarbeiter selbst in die Pflicht

3. Fazit und Ausblick

Fazit und Ausblick

- DS-GVO stellt Datenschutz nicht völlig auf den Kopf, aber in einigen Bereichen deutlich veränderte Anforderungen
- Empfehlung: Anpassung proaktiv betreiben

Weitere Materialien

Kurzpapier der Datenschutzkonferenz Nr. 8 „Maßnahmenplan“:
https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSK_KPNr_8_Massnahmenplan.pdf

Fragebogen LDA BY zur Vorbereitung auf die DS-GVO:
https://www.lda.bayern.de/media/dsgvo_fragebogen.pdf

BfDI-Broschüre DS-GVO:
https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=21

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Fragen?

Vielen Dank!

Dr. Philipp Richter

Referent

beim Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Postanschrift: Postfach 30 40
55020 Mainz

Büroanschrift: Hintere Bleiche 34
55116 Mainz

Telefon: +49 (6131) 208-2449
Telefax: +49 (6131) 208-2497

E-Mail: p.richter@datenschutz.rlp.de

Web: www.datenschutz.rlp.de