vogel—partner
RECHTSANWÄLTE

Alles neu macht der Mai – Überblick über die DS-GVO und die geplante ePrivacy-VO

RA Dr. Oliver Meyer-van Raay

Hochschule der Medien, Stuttgart

1. Dezember 2017

RA Dr. Oliver Meyer-van Raay

Rechtsanwalt, Fachanwalt für IT-Recht, Betriebl. Datenschutzbeauftragter, Dozent für Vertragsgestaltung und -verhandlung

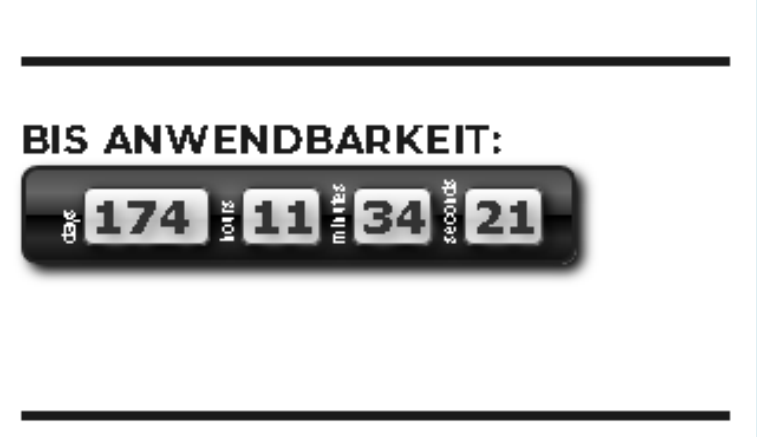
Studium und Referendariat in Münster; Promotion an der Universität Karlsruhe/ Freiburg im Softwarevertragsrecht

von 2007 bis 2009 Rechtsanwalt in einer Stuttgarter Großkanzlei (IT-Recht, Vertrags- und AGB-Gestaltung, Commercial)

von 2009 bis 2011 Rechtsanwalt bei Bartsch und Partner, Karlsruhe (UrhR, IT-Recht)

seit Januar 2011 Partner bei Vogel & Partner in Karlsruhe

Der Countdown läuft …



Entwicklung des Datenschutzes

- Geburtsstunde: **BVerfG Volkszählungsurteil** von 1983
  - Grundecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts
  - Befugnis des Einzelnen, grds. selbst bestimmen zu können, wem welche Daten für welchen Zweck preisgegeben werden.
- **Anwendungsbereich** des Datenschutzrechts: Personenbezogene Daten (weites Verständnis, vgl. z.B. IP-Adressen)
- Vielzahl **unbestimmter Rechtsbegriffe** (z.T. unklare und widersprüchliche Auslegung unter den Landes-Aufsichtsbehörden)
- **Europäisches Datenschutzrecht**:
  - bislang teilharmonisiert durch EU-Richtlinien
  - DS-GVO und BDSG (neu) verabschiedet → Inkrafttreten 25. Mai 2018
  - ePrivacy-Verordnung → Inkrafttreten 25. Mai 2018 ???

Abgrenzung Datenschutz und Datensicherheit

- **Datenschutz**
  - Datenschutz ist der Schutz des Menschen und seiner persönlichen Daten vor Missbrauch durch Andere
  - Nicht Schutz der Daten, sondern Schutz der Personen, über die die Daten etwas aussagen (Betroffene)
  - bislang insb. Bundesdatenschutzgesetz, EU-Richtlinien
- **Datensicherheit**
  - Datensicherheit ist der Schutz aller Daten eines Unternehmens vor unbefugten und unberechtigten Zugriffen
  - Betrifft die Sicherheit der Daten, also beispielsweise Schutz vor
    - nachträglichen Manipulationen (etwa durch Signaturen)
    - Datenverlust (durch geeignete Backup-Strategien)
    - unberechtigten Zugriffen oder Kenntnisnahmen (z.B. durch Verschlüsselung)

Wichtige datenschutzrechtliche Grundsätze (Status Quo)

- Gebot der **Datensparsamkeit** und **Datenvermeidung**
- **Zweckbindungsgebot**
  - keine zweckfreie Datenspeicherung auf Vorrat
  - Daten dürfen grds. nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden
  - über die Zweckerfüllung hinausgehende Speicherung unzulässig
- **Erforderlichkeitsprinzip**: Umgang nur mit den für einen bestimmten Zweck erforderlichen Daten
- **Präventives Verbot mit Erlaubnisvorbehalt**
  - Gesetzlicher Erlaubnistatbestand, z.B. wenn zur Vertragserfüllung erforderlich
  - Betriebsvereinbarungen
  - Einwilligung des Betroffenen: freiwillig, informiert, schriftlich, opt-in versus opt-out; in AGB schwierig (Bestimmtheit & Transparenz)

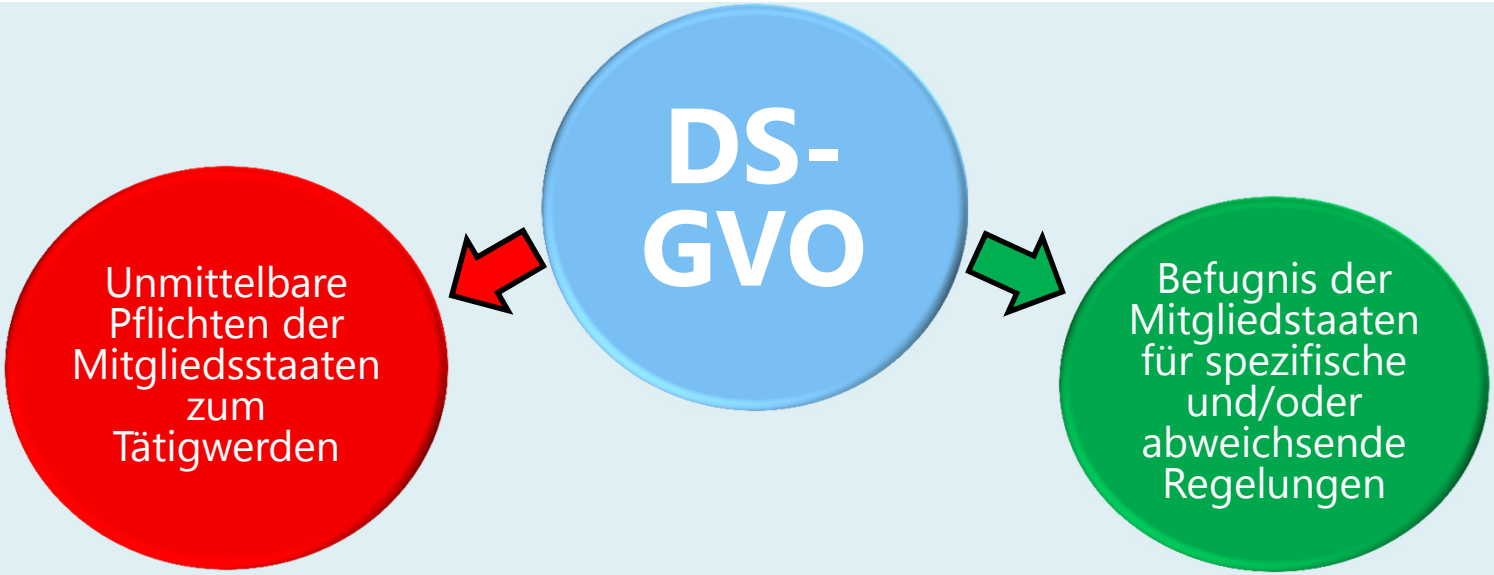
Die EU-Datenschutz-Grundverordnung (DS-GVO)

Ziel	Einheitliches Datenschutzrecht in der gesamten Europäischen Union (EU)
Nationales Recht	Wird weitgehend ersetzt, z.B. deutsches BDSG
In Kraft treten	Übergansfrist bis 25. Mai 2018 (2 Jahre) Gleichzeitig tritt neues, schlankes BDSG in Kraft (bereits verabschiedet)
Durchsetzung	Empfindliche Bußgelder (bis mind. 20 Mio. €) Ausgeweitete Haftung

Ziele der DS-GVO

- Betroffene erhalten mehr **Kontrolle** über ihre Daten
- **Europaweit gültige Standards** für Datenschutz werden gesetzt
- Datenschutzregeln **passend für den digitalen Binnenmarkt**
  - **Harmonisierung**:
    - » Grds. Vollharmonisierung angestrebt
    - » Ersetzt nationales Datenschutzrecht, führt also grds. zur Unanwendbarkeit abweichender nationaler Regelungen
  - **Kein „Forum-Shopping“**: Datenverarbeitung in Mitgliedstaat mit weniger strengem Datenschutzrecht
  - **„One-Stop-Shop“**: Eine zuständige Aufsichtsbehörde für Unternehmen in der Europäischen Union
  - Effiziente **Kooperation** der Datenschutzaufsichtsbehörden
  - Mehr **Konsistenz** der Anwendung des Datenschutzrechts

Vielzahl von Öffnungsklauseln in der DS-GVO



ca. 50-60 Öffnungsklauseln:

- bei Rechtsgrundlagen der Datenverarbeitung
- für spezifischere nationale Regelungen
- für Ausnahmen von Betroffenenrechten
- für sonstige Fälle

→ **Beispiel: Beschäftigtendatenschutz!**

Die wichtigsten Neuerungen der DS-GVO

… und ihre Folgen für Unternehmen:

- Haftung auch für immaterielle Schäden
- Anhebung des Bußgeldrahmens
- Erweiterte Dokumentations- und Nachweispflichten
- Erweiterte Informationspflichten bei Datenerhebungen
- Datenschutz-Folgenabschätzung (löst Vorabkontrolle ab)
- Löschpflichten und Recht auf Vergessenwerden
- Privacy by design und Privacy by default
- Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten
- Ausweitung der Betroffenenrechte

→ **Evolution statt Revolution: Die Struktur ähnelt stark der des BDSG, aber: Auf Unternehmen kommt trotzdem viel Arbeit zu!**

Interpretation / Auslegung der DS-GVO

Keine gefestigte Interpretations- bzw. Auslegungshilfen:

- EuGH-Rechtsprechung bezieht sich auf Richtlinie 95/46/EG
- Stellungnahmen/Orientierungshilfen des Europäischen Datenschutzausschusses müssen erst noch formuliert werden
- Stellungnahmen/ Orientierungshilfen der nationalen Aufsichtsbehörden und der Verbände kommen (allerdings teilweise Uneinigkeit unter den Aufsichtsbehörden):
  - „Kurzpapiere“ der Aufsichtsbehörden z.B. abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/dokumente-der-datenschutzkonferenz/
  - Praxishilfen der GDD: https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- Unternehmen werden sich anfangs einer großen Rechtsunsicherheit bei der Auslegung der DS-GVO stellen müssen.

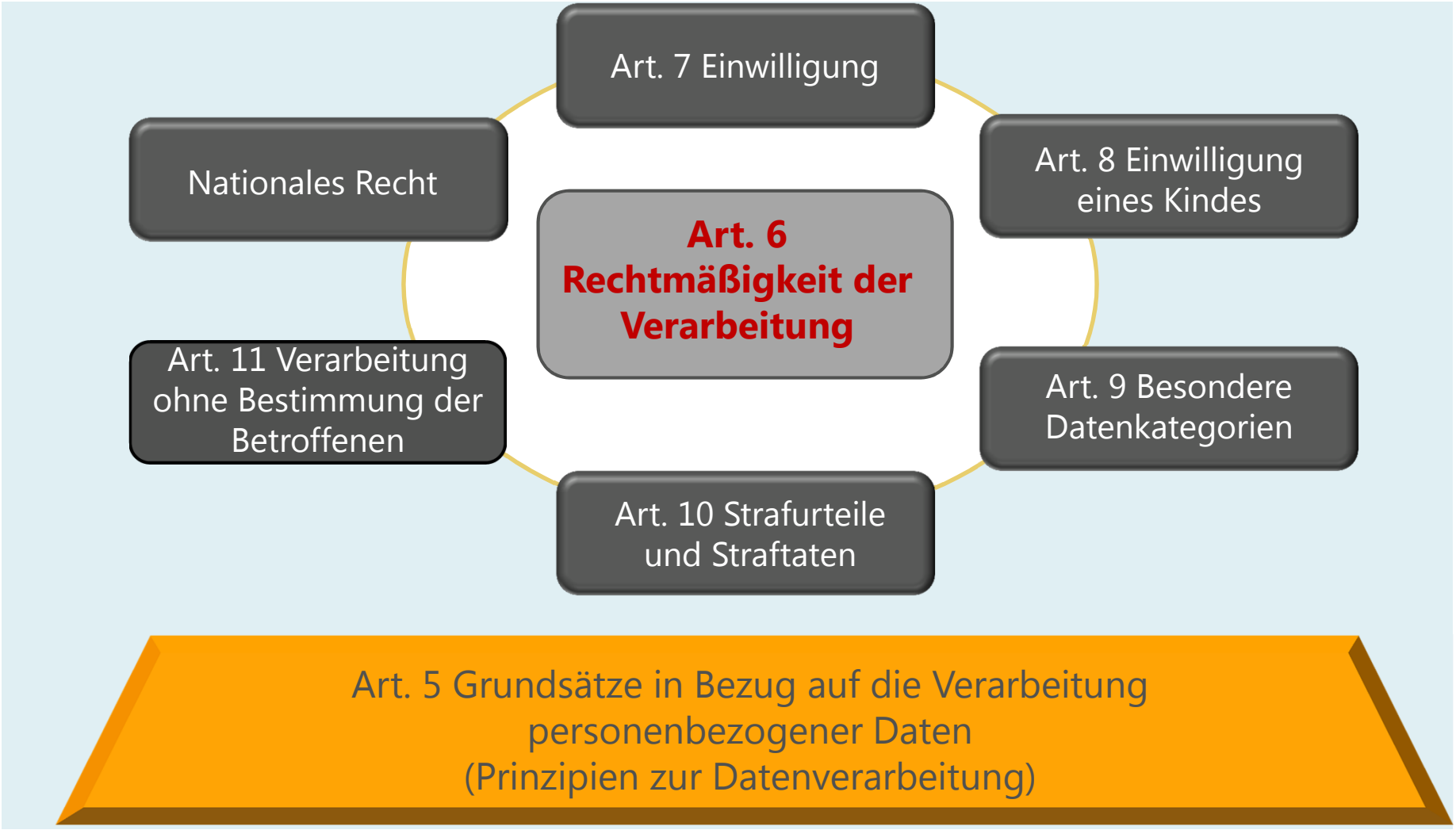
Personenbezogene Daten gemäß DS-GVO

Art. 4 DS-GVO Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

„personenbezogene Daten“ alle Informationen, die sich auf eine **identifizierte oder identifizierbare** natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die **direkt oder indirekt**, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Rechtsgrundlagen – Art. 6 ff. DS-GVO



Zentrale Themen der DS-GVO: Überblick

Zentrale Themen der DS-GVO

§

1. Rechtsgrundlagen reduziert auf

- Vertragserfüllung
- Einwilligung
- Gesetzliche Verpflichtung
- Interessensabwägung

Neu zu bewerten sind insbesondere Werbung und Videoüberwachung

Zentrale Themen der DS-GVO

2. Betroffenenrechte

- Umfangreiche Informationspflichten bei Erhebung, Datenbeschaffung und Zweckänderung
- Recht auf Datenmitnahme
- Recht auf Einschränkung der Verarbeitung (Sperrung)
- Enge Zeit- und Verfahrensvorgaben bei erweiterten Interventionsrechten

Zentrale Themen der DS-GVO

3. Dokumentationspflichten

Grundsatz: Nachweispflicht für datenschutz-konformes Handeln

- Explizite oder implizierte Dokumentationspflichten (ca. 20 Vorschriften)
- Nachweis einer wirksamen Datenschutzorganisation
- Nachweis des rechtmäßigen Datenumgangs (Accountability)

Zentrale Themen der DS-GVO

4. IT-Sicherheit

- Implizite Pflicht zum Sicherheitskonzept/ IT-Sicherheitsmanagement
- Pflicht zum Testen der Wirksamkeit
- Sicherstellung der Verhinderung unbefugter Datenverarbeitung
- Informations-/Dokumentationspflichten bei Sicherheitsvorfällen

Zentrale Themen der DS-GVO

5. Outsourcing (Auftragsdatenverarbeitung)

- Grundsätze bleiben
- Aktuelle Verträge müssen geprüft und gegebenenfalls angepasst werden
- Auftraggeber und Auftragnehmer müssen selbstständig die Vorgaben der DS-GVO einhalten
- Explizite Kontrollpflichten entfallen (aus Haftungsgründen aber empfohlen)
- Gesamtschuldnerische Haftung Auftraggeber und Auftragnehmer

Zentrale Themen der DS-GVO

6. Beschäftigtendaten

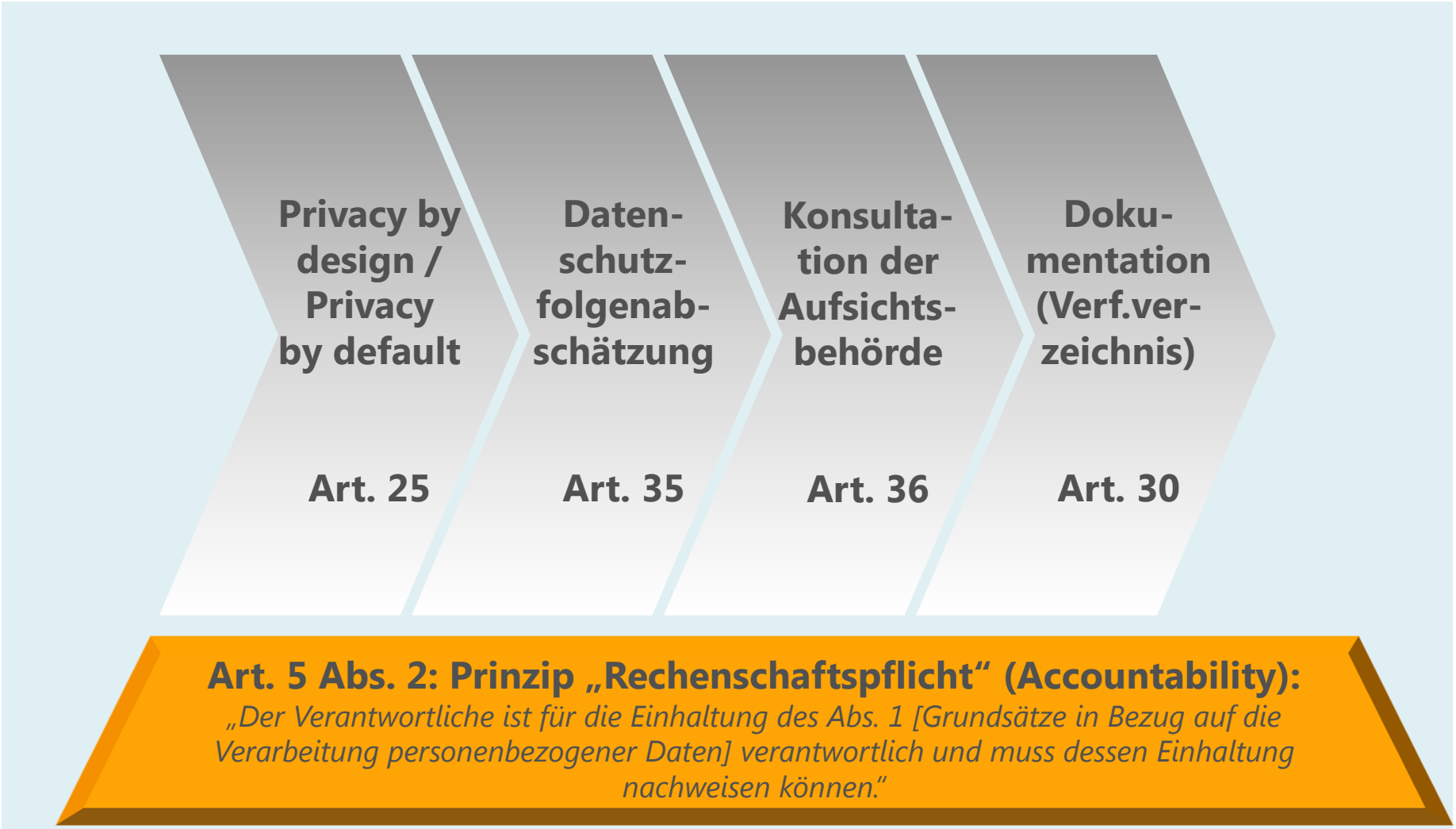
- Befugnis der Mitgliedsstaaten zur Regelung des Beschäftigtendatenschutzes. Deutschland hat von der Öffnungsklausel bereits Gebrauch gemacht (§ 26 BDSG – neu)
- Tarifverträge/Betriebsvereinbarungen können weiterhin Datenschutzregeln enthalten
- Die Inhalte von Datenschutzregeln in Tarifverträgen/ Betriebsvereinbarungen müssen mit der DS-GVO konform sein
- Bestehende Betriebsvereinbarungen müssen überprüft werden

Zentrale Themen der DS-GVO

7. Haftung und Bußgelder

- Empfindliche Bußgelder für fast alle Vorschriften: 10/20 Mio. Euro oder 2/4% des weltweiten Jahres-umsatzes (jeweils höherer Betrag)
- Ausgeweitete – gesamtschuldnerische Haftung – auch für immaterielle Schäden

Die DS-GVO ist vor allem ein Prozessthema …



Privacy by design / Privacy by default – Art. 25

Privacy by design

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten … geeignete technische und organis. Maßnahmen …, mit denen die **wirksame Umsetzung der Daten-schutzgrundsätze** wie etwa Datenminimierung und die **Aufnahme der notwendigen Garantien** in die Verarbeitung erreicht werden sollen.

Privacy by default

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass **durch Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung **für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist,** verarbeitet werden.

Möglichkeiten müssen im Produkt implementiert sein!
Produkt-Zertifizierung als Nachweis ist möglich.

Datenschutz-Folgenabschätzung – Art. 35

Indizien für Erforderlichkeit

- Neue Technologien
- Neue Verarbeitungsvorgänge
- Verarbeitung großer Datenmengen, große Anzahl Betroffener
- Sensibilität der Daten, Profiling
- usw.

Durchführung der Datenschutz-Folgenabschätzung

- Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
- Bewertung der Verhältnismäßigkeit, Maßnahmen zur Risikoverringerung
- Abstimmung mit Betroffenen
- Abschließende Risikobewertung → ggf. Konsultation der Aufsichtsbeh.

Ausreichende Dokumentationen hierzu müssen vorhanden sein!

Verzeichnis von Verarbeitungstätigkeiten – Art. 30

- Verantwortlicher führt „Verzeichnis aller Verarbeitungstätigkeiten“
- Auftragsverarbeiter: kundenbezogene Aufzeichnung der „durchgeführten Tätigkeiten …“
- Nicht öffentlich, aber Einsicht für Aufsichtsbehörden auf Anfrage
- Dokumentation ähnlich Verfahrensverzeichnis
- Zusätzlich aufzunehmen: Beurteilung und Garantien bei Datenübermittlung in Drittland
- Ausnahmen für Unternehmen unter 250 Mitarbeiter – aber aufgrund Gegenausnahmen häufig nicht einschlägig
- **Achtung**: Daneben bestehen weitere Dokumentationspflichten

Auswirkungen auf Organisation und Compliance-Systeme

Haupt-Aufgaben des **Unternehmens** 	**Etablierung:** ▪ Datenschutz-Management (insbes. im Hinblick auf „Accountability“/Nachweise) ▪ IT-Sicherheitsmanagement
Haupt-Aufgaben der **Fachabteilung, Mitarbeiter** 	**Umsetzung:** ▪ Prozessgestaltung (Privacy by design/default) ▪ Datenschutzfolgenabschätzung/PIA ▪ Dokumentationen/Nachweise/Meldepflichten ▪ Prozesse für Rechte der Betroffenen
Datenschutz-beauftragter (DSB) Haupt-Aufgaben des **DSB** 	▪ Bestellpflicht bleibt nach deutschem Recht ▪ Jeder „Verantwortliche“ (= Legaleinheit) ▪ Bestandteil des Datenschutz-Managements **Beratung:** ▪ Abstimmung bei „Strategien“ und – vorgegebenen – Einzelfällen **Überwachung:** ▪ Umsetzung, risikoorientiert

Die wichtigsten Herausforderungen

Verarbeitung:
Insbes. Anpassung von Verträgen und Einwilligungen

Zielsetzung:
Nachweisbar datenschutz-konformer Datenumgang

Organisation:
Insbes. Etablierung von Nachweisen und Dokumentationen

Bay. Landesdatenschutzaufsicht: DS-GVO-Fragebogen

Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018

Unternehmen/Verantwortliche Stelle	Eingangsstempel BayLDA

I. Struktur und Verantwortlichkeit im Unternehmen	
1.	▪ Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch ▪ Vorhandensein einer Datenschutzleitlinie ▪ Beschreibung der Datenschutzziele ▪ Regelung der Verantwortlichkeiten ▪ Bewusstsein über Datenschutzrisiken ▪ Transparenz über Zielkonflikte (z.B. zwischen Marketing- und Rechtsabteilung)
2.	▪ Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten? ▪ Wenn nein, warum nicht? ▪ Wenn ja, ist geklärt, wann er von wem einzubeziehen ist? ▪ Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?

II. Übersicht über Verarbeitungen	
1.	▪ Haben Sie ein Verzeichnis Ihrer Verarbeitungstäti ▪ Wenn nein, warum nicht? Ist das dokumentier

Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?

IV. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte	
1.	▪ Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst? ▪ Wenn nein, warum nicht?
2.	▪ Haben Sie insbes. folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten: ▪ Kontaktdaten des Datenschutzbeauftragten ▪ Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten ▪ Falls Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen: die berechtigten Interessen ▪ Falls Sie Daten in Drittländer übermitteln: die von Ihnen zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (z.B. Standarddatenschutzklauseln) ▪ Dauer der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer ▪ Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität

Webtracking über Cookies – bisherige Rechtslage

Zulässige Verwendung von Nutzungsprofilen

- Erstellung zu Werbezwecken nur zulässig bei Verwendung von Pseudonymen und soweit der User der Erstellung nicht widerspricht (opt-out), vgl. § 15 Abs. 3 TMG!
  - User muss Widerspruchsrecht und -möglichkeit haben
  - Abbildung in Datenschutzhinweisen gem. § 13 Abs. 1 TMG erforderlich

Einschränkung durch ePrivacy-Richtlinie (sog. Cookie-Richtlinie)?

- In Deutschland nicht umgesetzt (Umsetzungsfrist bis Ende 2011!) – jedenfalls nach Ansicht der dt. Datenschutzaufsichtsbehörden (andere Ansicht Bundesregierung und EU-Kommission …)
- Kernfrage: Opt-out für „Einwilligung“ gemäß Cookie-Richtlinie ausreichend?

… bald überholt durch ePrivacy-Verordnung …

Entwurf der neuen EU-ePrivacy-Verordnung

Grundlagen

- Gegenstand: Datenschutz in der elektronischen Kommunikation
- Geplantes Inkrafttreten am 25. Mai 2018 – zeitgleich mit DS-GVO
  - aber: massive „Lobbyschlacht“ und 800 Änderungsvorschläge abzuarbeiten …
- Ziel: Ersetzung der bisherige ePrivacy-Richtlinie 2002/58/EC
- Gründe für Neuregelung
  - Übereinstimmung mit DS-GVO (*lex specialis* zur DS-GVO)
  - EU-weite Harmonisierung
  - Neue technische Entwicklungen
- Auch neue digitale Dienste umfasst, z.B. M2M-Kommunikation, Smart Home Anwendungen, Connected Cars
- Änderungen am TKG, TMG u.a. Gesetzen werden erforderlich

Entwurf der neuen EU-ePrivacy-Verordnung

Umgang mit Cookies

- **Personenbezug**, je nachdem, was der Cookie sammelt (insb. IP-Adresse)
- **Notwendige Cookies**, z.B. Warenkorbfunktion → Gesetzliche Erlaubnis
- **Nicht notwendige Cookies**, z.B. zu Zwecken des Retargeting
  - Einwilligung zwar erforderlich (Verweis auf DS-GVO)
  - aber: Erklärung über **Browser-Einstellungen** möglich (nach Kommissionsentwurf)
    - *„Consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet."*
    - *„Upon installation, the software shall inform … and, to continue with the installation, require the end-user to consent to a setting."*

Daneben: Neue Pflichten für **Softwareanbieter** (privacy by design/ default, z.B. do-not-track voreingestellt); Recht auf **verschlüsselte Kommunikation** u.v.m.

vogel—partner
RECHTSANWÄLTE

Noch Fragen?

Vogel & Partner Rechtsanwälte mbB
Technologiepark Karlsruhe
Emmy-Noether-Straße 17
76131 Karlsruhe

www.vogel-partner.eu
om@vogel-partner.eu
Tel. +49 721 782027-22
Fax +49 721 782027-27