

# Keine Angst vorm Datenschutz

– DSGVO, ePrivacy, KunstUrhG, NetzDG –

08.06.2018 tim.schrock@dbjr.de

# »Datenschutz«

Worum geht's nochmal?

<b>Was wird geschützt</b>	bestimmte Daten, alle personenbezogen
<b>vor wem</b>	böse Hacker, Firmen, eigenes Umfeld
<b>für wen</b>	Teilnehmende, Organisation
<b>und warum</b>	Bloßstellung, Missbrauch für Anderes
<b>wie sicher</b>	zu sicher macht Freiheit kaputt
<b>und wie lange?</b>	wann wird's gelöscht?

# Aktuelle Situation: DSGVO

Datenschutz 3x anders: 2018/2019

- DSGVO: Seit 25. Mai europaweit einheitlich, ersetzt vorherige Regelungen und bisheriges nationales Recht (z.B. bisheriges Bundesdatenschutzgesetz)
- Es geht um Erfassung, Verarbeitung und Speicherung personenbezogener Daten
- Faustregel: Alles immer zustimmungspflichtig
- Relevant für uns: Besonderheit der Anforderungen für Unter-16-Jährige ([ErwG 38](#) und [Art. 8](#))

# Prinzipien der DSGVO (I)

Worauf zielt die DSGVO?

- **Transparenz der Datenverarbeitung:** Was wird damit gemacht, wo geht's hin? Verständlich darstellen!  
Dokumentieren!
- **Recht auf Vergessenwerden und auf Berichtigung:**  
Aktives Löschen & Löschen lassen
- **Recht auf Datenübertragbarkeit:** Dienst wechseln können
- **Privacy by Design, Privacy by Default:** Dokumentierte gute Voreinstellungen

# Prinzipien der DSGVO (II)

Worauf zielt die DSGVO?

- **Kopplungsverbot:** Einwilligung muss freiwillig sein und darf nicht mit anderen Aspekten verbunden werden (Gewinnspiele, Werbung, etc.) (ErwG 43)
- **Datenminimierung:** Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke; Abrücken von „Datensparsamkeit“ (Big Data ↔ BDSG-alt)
- **Verpflichtung zur Bestellung von Datenschutzbeauftragten:** ab 10 Personen (ErwG 97; Art. 37; § 38 BDSG-neu)
- **Meldepflicht** für Verletzungen binnen 72 Std (Art. 33)

# Personenbezogene Daten

Definition (Art. 4)

- Alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen;
- Identifizierbar: direkt oder indirekt, insbesondere bei Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen (physisch, physiologisch, genetisch, psychisch, wirtschaftlich, kulturell oder sozial)
- Besonderer Schutz sensibler Daten (ErwG 51, Art. 9)
- **Möglicher Schaden:** Diskriminierung, Rufschädigung, Identitätsdiebstahl, finanzieller Verlust (ErwG 75)

# Sensible Daten

Besondere Kategorien personenbezogener Daten (Art. 9)

- Rassistische und ethnische Herkunft,
- politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit,
- genetische oder biometrische Daten zur eindeutigen Identifizierung,
- Gesundheitsdaten,
- Daten zum Sexualleben oder der sexuellen Orientierung.
- Strafrechtliche Daten nur unter behördlicher Aufsicht.

# Einwilligung

## Anforderungen und Beweislast (Art. 7)

- Anforderungen an wirksame Einwilligung gegenüber bisherigem BDSG reduziert: **Schriftform nicht mehr die Regel** (ErwG 32)
- Stillschweigende Einwilligungserklärung ist zulässig, sofern Wille eindeutig
- Aber: Verarbeitende müssen das **nachweisen** → daher doch Schriftform
- Generell ist Schriftform vorgeschrieben für besondere personenbezogene Daten
- In **verständlicher und leicht zugänglicher Form** sowie in einer klaren und einfachen Sprache, so dass andere Sachverhalten klar zu unterscheiden sind
- Einwilligung kann **jederzeit widerrufen werden**, Verarbeitung bis dahin gültig



# Kinder, Jugendliche, Minderjährige?

Die DSGVO und ihre besonderen Regelungen für Kinder

- Erstmals wird in DSGVO anerkannt, dass Minderjährige **IT-Dienste** nutzen
- Dienste, die sich (auch) an Kinder richten
- Rechtmäßige Einwilligung **ab 16** (in manchen Staaten schon ab 13) (Art. 8)
- Angemessene Anstrengung unter Berücksichtigung verfügbarer Technik, Einwilligung ist zu dokumentieren (Art. 8 (2))
- Präventions- und Beratungsdienste für Kinder: Einwilligung auch ohne Erziehungsberechtigte (ErwG 38)
- Kein Profiling

# Das Recht am eigenen Bild

Exkurs: KUG vor DSGVO und BDSG-neu! ([§§ 22, 23 KunstUrhG](#))

- Recht am eigenen Bild als besondere Ausprägung des allgemeinen Persönlichkeitsrechts im Kunsturhebergesetz: Abbildungen einer (erkennbaren) Person nur weitergeben, wenn Einwilligung
- **Ausnahmen:** Zeitgeschichte, Personen als Beiwerke, Menschenansammlungen
- Keine Verletzung berechtigter Interessen
- Bei Entlohnung gilt Einwilligung als erteilt
- Nach Tod noch 10 Jahre die Einwilligung der Angehörigen
- **Beweislast** liegt bei Verwender\_in

# Betroffenenrechte

Welche Rechte auf Auskunft und Veränderung habe ich? (Art. 15 – 19)

- › Welche Daten werden verarbeitet (Art 15 Abs 1)
- › Was sind Verarbeitungszwecke
- › Konkret genutzte Kategorien personenbezogener Daten neu
- › Ggf. Empfänger der Daten
- › Geplante Speicherdauer neu
- › Hinweis auf Rechte zur Berichtigung, Einschränkung, Löschung sowie zum Widerspruch (Art 21) neu
- › Hinweis auf Beschwerderecht bei Aufsichtsbehörde neu
- › Herkunft der Daten, soweit nicht von Betroffenen selbst erhoben
- › Ggf. Bestehen von automatisierter Entscheidungsfindung oder Profiling neu
- › Bringschuld: Info bei Verletzung des Schutzes personenbezogener Daten mit hohem Risiko (Art. 34)

# Wen betrifft's?

DSGVO gilt nicht für Alle(s) gleichermaßen

- DSGVO **unterscheidet** (im Gegensatz zum BDSG) nicht zwischen öffentlichen und nicht-öffentlichen Stellen, aber Gefahrenabwehr, Strafverfolgung und Rechtfertigung bei öffentlichem Interesse und Ausübung öffentlicher Gewalt
- DSGVO **greift nicht** bei ausschließlich persönlicher oder familiärer Tätigkeit (ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit), z.B. bei privatem Adressbuch oder Nutzung sozialer Netze und Online-Tätigkeiten.
- DSGVO **gilt jedoch** für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.
- **Auftrags(daten)verarbeitung** (Art. 28), Empfänger und Dritte
- **Marktortprinzip:** in EU angebotene Tätigkeit/Leistung

# Wie weit betrifft es uns?

## Einschränkungen und Begrenzungen

- Pflicht zu **Verzeichnis der Verarbeitungstätigkeiten**: gilt nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeitende beschäftigen, außer ([Art. 30 Abs 5; ErwG 13](#))
  - die Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen
  - die Verarbeitung erfolgt nicht nur gelegentlich oder
  - es erfolgt eine Verarbeitung besonderer Datenkategorien
- Erforderlichkeit einer **Datenschutz-Folgenabschätzung** bei großer Zahl möglicher Betroffener, auch bereits regional ([ErwG 91](#))
- **Pseudonymisierung** hilft ([ErwG 28](#))
- **Stand der Technik** (IT-Sicherheitsrichtlinie) ([Art. 32](#))

# Konkrete Maßnahmen

Beim Sichtbarsten beginnen & Transparenz herstellen

- Datenschutzkontakt datenschutz@... für Websites, Anmeldeformulare und Bewerbungsverfahren (Außenvertretungen)
- Datenschutzerklärungen für Websites, Social Media und Online-Tools
- (Erneutes) Abschließen von Vereinbarungen zur Auftragsverarbeitung
- Gemeinsames Verzeichnis von Verarbeitungstätigkeiten ([Art. 30 DSGVO](#))
- Fragebogen zur Selbstauskunft
- Löschen, löschen, löschen ... ! Oder doch nicht?
- Ungeklärt: Teilnehmendenlisten bei z.B. KJP-Förderung

# Grenzen des Datenschutzes

Der Schutz franst aus – Beispiele für weitere Regeln

- **Öffentliches Interesse zur Archivierung; wissenschaftliche und historische Forschungs- und Statistikzwecke:** [Art. 89](#)
- **EU-US Privacy Shield:** EuGH erklärt 2015 das Safe-Harbor-Abkommen für ungültig. Seit Februar 2016 Regelungspaket, u.a. können sich US-Unternehmen in Selbstverpflichtungsliste eintragen lassen. Beschwerdestelle für EU-Bürger\_innen. Weiter umstritten.
- **Netzwerkdurchsetzungsgesetz:** Betreiber sozialer Netzwerke ab 2 Mio. Nutzenden müssen „offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden“ nach Eingang einer Beschwerde löschen oder sperren. ([NetzDG verschärft § 14 Abs 2 TMG](#))

# Das Cookie-Problem

In Deutschland anders als in der EU

- **2002: ePrivacy-Richtlinie**

Umgang mit Daten durch Netzanbieter, damit Inhalte und Metadaten vertraulich bleiben.

- **2009: Cookie-Richtlinie**

Anbieter dürfen Nutzer\*innen nur mit deren Einwilligung verfolgen. Und nun auch Social Media, Messenger, Vereinswebsites, Online-Spiele: Explizite Zustimmung erforderlich (Button „Cookies akzeptieren“). In DE nie in nationales Recht überführt, daher gilt der Stand der ePrivacy-Richtlinie von 2002.



# Ab 2019: ePrivacy-Verordnung?

Ergänzung zur DSGVO: Fokus auf Kommunikation

- **Tracking:** In DE gilt noch die Opt-out-Lösung
- **Erforderlichkeit:** Nur noch zwingend erforderliche Cookies
- **Aussperren:** Bei Cookie-Ablehnung nicht zulässig
- **Datenerhebung durch Drittfirmen:** Nur mit expliziter Zustimmung

Die ePrivacy-Verordnung ist noch in Verhandlung. Inkrafttreten nicht vor Frühjahr 2019 zu erwarten.

# Weitere Informationen

Hilfreiche und zielgruppen-genaue Unterstützung

- **DSGVO:** <https://dsgvo-gesetz.de>  
Mit hilfreichen Verlinkungen zu Erwägungsgründen und BDSG-neu
- **Artikelreihe zur DSGVO:** <https://tooldoku.dbjr.de>
- **Umfassendes Infoportal der Datenschutzbehörden:**  
[https://www.lda.bayern.de/de/datenschutz\\_eu.html](https://www.lda.bayern.de/de/datenschutz_eu.html)  
mit Kurzanleitungen, interaktivem Selbsttest, Vorlagen
- **Hilfestellung für kleine Unternehmen und Vereine:**  
<https://www.lda.bayern.de/de/kleine-unternehmen.html>