

Die Datenschutz-Grundverordnung in der Tätigkeit des Sachverständigen

Vortrag bei der AKNW am Sachverständigentag 2019
Referentin: RAin Janina Winz

Hinweis: Die Architektenkammern der Länder bieten gemeinsam praktische Hinweise und Muster zur DS-GVO unter <https://www.bak.de/architekten/datenschutz/> an.

© Kapellmann und Partner Rechtsanwälte mbB

Fakten zur DS-GVO



- Inkrafttreten der Europäischen Datenschutz-Grundverordnung (DS-GVO) am 24. Mai 2016
- nach zweijähriger Umsetzungsfrist Geltung seit dem **25. Mai 2018**
- Unmittelbare Anwendung in allen EU-Mitgliedstaaten
- „Vereinzelte „Öffnungsklauseln“ für nationale Spezialregelungen
 - ▶ In Deutschland: ergänzende Regelungen für die Privatwirtschaft im Bundesdatenschutzgesetz (BDSG) und in Spezialgesetzen
- Bußgeldrahmen bis zu 20 Mio. EUR oder 4 % des gesamten weltweit erzielten Vorjahresumsatzes einer Unternehmensgruppe
- Hohe Schadensersatzrisiken, Abmahnrisiko, Reputationsverlust
- Zuständige Aufsichtsbehörde: Landesdatenschutzbeauftragte



Welchen Zweck verfolgt sie?



Schutz natürlicher Personen bei Verarbeitung ihrer personenbezogenen Daten

- **Natürliche Personen**

idR keine „Unternehmensinformationen“, sondern Informationen zu Einzelpersonen, z.B. Verbraucher, (Privat-) Eigentümer, Mieter, Mitarbeiter und Ansprechpartner von Unternehmen, Behörden, Gerichten etc.

- **Personenbezogene Daten (pbD)**

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“ oder „Betroffene“) beziehen

- ▶ z.B. Stamm- und Kontaktdaten, aber auch Sachdaten, die sich auf eine natürliche Person beziehen (z.B. Kommunikationsdaten, Bildaufnahmen von Personen, Sachverhaltsangaben im Gutachten z.B. zu Vermögenssituation, Vertragsverhältnissen, Mieterlisten oder sonstige Angaben zu Dritten, die Gegenstand der Begutachtung sind)
- ▶ Ausreichend, dass betroffene Person indirekt, z.B. mittels einer Kennnummer identifiziert werden kann (z.B. IP-Adresse, Pseudonym)

3

Auf welche Sachverhalte findet sie Anwendung?



Primäre Adressaten: „Verantwortliche“

- Jede Person oder Stelle, die über die „Zwecke und Mittel der Verarbeitung“ entscheidet
- Pflichten der DS-GVO gelten nicht nur für datenintensive Unternehmen und Großunternehmen, sondern auch für Kleinstunternehmen bzw. Einzelunternehmer, ggf. Privatpersonen

Anwendungsbereich

- Automatisierte und dateibezogene Verarbeitungen
 - ▶ Verarbeitung: Jegliche Form von der Erhebung, Speicherung, Änderung, Verknüpfung, Auswertung, Übermittlung bis hin zur Löschung
 - ▶ Dateibezug: z.B. papiergeführte Akten, strukturierte Sammlungen
 - ▶ Ausnahme: DV durch natürliche Person für persönliche oder familiäre Zwecke
- Verarbeitung im Rahmen der Tätigkeit einer Niederlassung in der EU; ggf. Verarbeitung durch außereuropäische Unternehmen/ Stellen (Art. 3 Abs. 2)

4

Welche Grundregeln gelten?

Verarbeitungsgrundsätze (Art. 5)

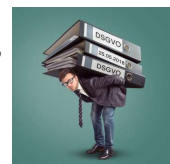
- **Rechtmäßigkeit und Verarbeitung nach Treu und Glauben**
- **Transparenz** (insb. strengere Informations- und Auskunftspflichten)
- **Zweckbindung** (Verarbeitung nur für festgelegte, eindeutige, rechtmäßige Zwecke)
- **Datenminimierung** (Beschränkung der Verarbeitung auf das für die Zweckerreichung notwendige Maß)
- **Richtigkeit und Aktualität der Daten**
- **Speicherbegrenzungsprinzip** (Speicherdauer, Löschpflichten!)
- **Integrität und Vertraulichkeit** (Datensicherheit durch technische und organisatorische Maßnahmen)
 - Ausrichtung jeder Verarbeitung an diesen Datenschutzprinzipien
 - **Rechenschafts- und Dokumentationspflichten:** Einhaltung muss nachgewiesen werden können!

5

Wann ist die Verarbeitung rechtmäßig?

Verbot mit Erlaubnisvorbehalt

- Jede Verarbeitung personenbezogener Daten ist verboten, soweit keine ausdrückliche Erlaubnis vorliegt
- Art. 6 DS-GVO: Verarbeitung pbD ist u.a. erlaubt, soweit
 - ▶ eine ausdrückliche **Einwilligung** des Betroffenen vorliegt
 - ▶ sie für die **Vertragserfüllung** oder Durchführung von vorvertraglichen Maßnahmen erforderlich ist
 - ▶ sie für die Erfüllung einer **gesetzlichen Verpflichtung** erforderlich ist
 - ▶ sie für die Wahrnehmung einer im **öffentlichen Interesse** liegenden oder in **Ausübung öffentlicher Gewalt** erfolgenden Aufgabe erforderlich ist, die auf Verantwortlichen übertragen wurde
 - ▶ sie zur Wahrung **berechtigter Interessen** erforderlich ist und keine schutzwürdigen Interessen der Betroffenen überwiegen
- Ggf. spezielle Erlaubnisnormen in DS-GVO, BDSG, Spezialgesetzen
- Bei Datentransfer in Länder außerhalb EU oder EWR: Art. 44 ff. beachten!



6

Wann ist die Verarbeitung rechtmäßig?



Rechtsgrundlagen i.R.d. Sachverständigentätigkeit

• Gerichtsgutachten

- ▶ Einwilligung eignet sich i.d.R. nicht, da widerruflich; zudem schriftliche Einholung aufwendig und konkludente Einwilligung schwer nachweisbar
- ▶ **e.A.:** zur Erfüllung einer gesetzlichen Verpflichtung erforderlich (Art. 6 Abs. 1 S. 1 lit. c) DS-GVO i.V.m. § 407 ZPO)
- ▶ **a.A.:** berechtigtes Interesse (Art. 6 Abs. 1 S. 1 lit. f), da zur Erfüllung der Pflichten aus §§ 407 f. ZPO notwendig; idR keine überwiegenden Interessen der Betroffenen, da Verwendung nur iRd Gerichtsverfahren/keine Veröffentlichung

• Privatgutachten

- ▶ Einwilligung eignet sich i.d.R. auch hier nicht (s.o.)
- ▶ **Daten des Auftraggebers:** zur Vertragserfüllung einschl. vorvertraglicher Maßnahmen erforderlich (Art. 6 Abs. 1 S. 1 lit. b), jedenfalls aber berechtigtes Interesse (Art. 6 Abs. 1 S. 1 lit. f)
- ▶ **Daten Dritter:** berechtigtes Interesse des Auftraggebers, aber im Einzelfall Interessenabwägung (Art. 6 Abs. 1 S. 1 lit. f); ggf. vertragliche Vereinbarung mit AG zum Schutz der Daten Dritter

7

Wann ist die Verarbeitung rechtmäßig?



Rechtsgrundlagen i.R.d. Sachverständigentätigkeit

• Beachte: **Datenminimierung!**

- ▶ zwar keine Schwärzung/Pseudonymisierung von Daten Dritter notwendig, da Nachvollziehbarkeit des Gutachtens an oberster Stelle steht, aber nicht mehr pbD erheben und verarbeiten als unbedingt notwendig
- ▶ nur für Vertragsabwicklung bzw. Durchführung der Begutachtung und Abwicklung des Auftrags erforderliche pbD erheben, speichern und sonst verarbeiten
- ▶ Empfänger/Zugriffsberechtigte und Speicherfristen auf das notwendige Maß reduzieren

• Beachte: **Informationspflichten** bestehen unabhängig von der Rechtmäßigkeit!

- ▶ Datenschutzzinformation gemäß Art. 13, 14 DS-GVO, auch im B2B-Bereich!

8



Information ist alles!

9

Erfüllung der Informationspflichten

Die Betroffenen sind bei Erhebung ihrer Daten über bestimmte Umstände der Verarbeitung zu informieren:



- **Adressat:**
Betroffen sind z.B. Auftraggeber/Vertragspartner bzw. deren Ansprechpartner, Eigentümer, Mieter, Ansprechpartner bei Behörden, Gerichten etc., eigene Mitarbeiter, Bewerber, Homepage-User
- **Informationsgehalt:**
Katalog in Art. 13 Abs. 1 und 2 DS-GVO (i.F.d. Datenerhebung direkt beim Betroffenen) und Art. 14 Abs. 1 und 2 DS-GVO (i.F.d. Erhebung aus einer anderen Quelle)
- **Zeitpunkt der Information**
 - ▶ Direkterhebung: **im Zeitpunkt der Erhebung** beim Betroffenen
 - ▶ Andere Quelle: „innerhalb angemessener Frist“ nach Erlangung bzw. zum Zeitpunkt der ersten Kommunikation bzw. bei beabsichtigter Weitergabe an andere Stelle zum Zeitpunkt der ersten Offenlegung; **spätestens nach 1 Monat**

10

Informationspflichten des Sachverständigen

- Datenschutzhinweise für Auftraggeber und andere Betroffene im Rahmen der Sachverständigentätigkeit (z.B. Mieter, Mitarbeiter von Gerichten, Behörden)
 - ▶ **öffentlich bestellte und vereidigte Sachverständige:**
 - Datenschutzhinweise für alle Verfahrensbeteiligten erstellen
 - mit Bestätigungsschreiben über Gutachtenannahme bereitstellen
 - ▶ **private Sachverständige:**
 - Datenschutzhinweise für Auftraggeber/ sonstige beteiligte Personen erstellen
 - bei erster Kontaktaufnahme und/oder bei Vertragsschluss bereitstellen
 - ▶ **P: Informationspflicht gegenüber Dritten (z.B. Mietern, Zeugen)?**
 - Direkterhebung: grds. ja (z.B. Hinweise an Mieter bei Wohnungsbesichtigung)
 - Erhebung aus anderer Quelle: grds. ja, soweit keine Ausnahme (z.B. Unmöglichkeit, unverhältnismäßiger Aufwand, Geheimhaltungspflicht)
- Datenschutzhinweise für eigene Mitarbeiter und Bewerber
- Datenschutzhinweise („Datenschutzerklärung“) auf Homepage

11

Gewährleistung der Betroffenenrechte

- **Auskunftsrecht**, Art. 15:
 - ▶ unentgeltlich, Beantwortung „unverzüglich“ und spätestens nach 1 Monat
 - ▶ Recht auf unentgeltliche Zurverfügungstellung einer Kopie der pbD
 - ▶ Ausnahmen: insb. Geschäftsgeheimnisse, geheimhaltungspflichtige bzw. -bedürftige Informationen (§§ 29, 34)
- **Recht auf Löschung** („Recht auf Vergessenwerden“), Art. 17
 - ▶ Grds.: Aufbewahrung von pbD nur solange, wie für jeweiligen Zweck erforderlich
 - ▶ Ausnahme: insb. wenn weitere Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder Durchsetzung von Rechtsansprüchen erforderlich ist
- **Weitere Betroffenenrechte:**
Recht auf Berichtigung (Art. 16), Recht auf Einschränkung (Art. 18), „Recht auf Datenportabilität“ (Art. 20), Widerspruchsrecht (Art. 21)
- Schaffung von Standardprozessen für die Beantwortung von Auskunfts-/ Löschbegehren oder sonstigen Anträgen von Betroffenen

12

Informationspflichten und Betroffenenrechte



Besonderheiten im Rahmen der Sachverständigentätigkeit

- **Auskunftsrecht: Pflicht zur Herausgabe des Gutachtens?**
 - ▶ Betroffene haben (nur) Anspruch auf Auskunft über die sie betreffenden Daten
 - ▶ aber Datenkopie: Daten sind so herauszugeben, wie sie vorliegen (also grds. in Form des Gutachtens)
 - ▶ Ausnahme: u.a. bei geheimhaltungspflichtigen bzw. -bedürftigen Daten und – im Falle der Kopie – Beeinträchtigung Rechte Dritter (z.B. des Auftraggebers)
- **Berichtigungsrecht:**
 - ▶ Betrifft nur „falsche“ Daten betreffend eine Person, nicht Werturteile oder z.B. Ergebnis von Wertgutachten etc.
- **Ausnahmen von den Löschpflichten, insb.**
 - ▶ i.F. gesetzlicher Aufbewahrungspflichten (z.B. § 13 Abs. 2 SVO AKNW, § 257 HGB, § 147 AO) oder sonstiger Rechtspflichten
 - ▶ für Geltendmachung, Ausübung, Verteidigung von Rechtsansprüchen
 - ▶ ggf. für im öffentliche Archivzwecke, für Forschungs- oder statistische Zwecke

13

Vertragsbeziehungen zu Dritten



Auftragsverarbeitung

bei Einbindung von Dienstleistern, die im Auftrag pbD verarbeiten oder im Rahmen ihrer Tätigkeit auf solche Zugriff haben

- Voraussetzung: Weisungsgebundenheit bei der Verarbeitung, keine wesentlichen Entscheidungsbefugnisse des Auftragnehmers
- Vertrag nach Art. 28 Abs. 3 DS-GVO erforderlich
- Beispiel: IT-Dienstleister, Cloud-Betreiber, externe Lohnbuchhaltung, externe E-Mail-Verwaltung, Website-Dienste, ggf. externe Datenerfassung/-konvertierung/Einscannen von Dokumenten/Copyshops
- **Folge:** Nur Auftraggeber „Verantwortlicher“ i.S.d. DS-GVO; Auftragnehmer selbst nicht für Rechtmäßigkeit der Verarbeitung, Informationspflichten etc. verantwortlich; keine gesonderte Rechtsgrundlage für Datenaustausch zwischen Auftraggeber und Auftragnehmer erforderlich

14

Verträge mit Dritten



Joint Controllershship (gemeinsame Verantwortlichkeit)

- Voraussetzung: gemeinsame Zweck- und Mittelfestlegung
- Vertrag nach Art. 26 Abs. 1, 2 DS-GVO erforderlich
- Beispiel: gemeinsamer Betrieb einer Internetplattform / Website
- **Folge:** gemeinschaftliche Haftung für gesamten Schaden, soweit fehlendes Verschulden nicht nachgewiesen

„Bloße“ Inanspruchnahme fremder Fachleistungen

bei eigenständig handelnden Verantwortlichen

- Keine Pflicht zum Abschluss eines speziellen Vertrags, aber ggf. sinnvoll
- Beispiel: Berufsgeheimnisträger, Inkassobüro mit Forderungsübertragung, Postdienst, Bankinstitut für Geldtransfer
- **Folge:** Jede Vertragspartei selbst „Verantwortlicher“ i.S.d. DS-GVO

15

Verträge mit Dritten



Einordnung des Sachverständigen

- **Private Sachverständige:**
 - ▶ e.A.: Privatbegutachtung (z.B. Immobilienbewertung) sei Auftragsverarbeitung, da Sachverständige nach Weisung des Auftraggebers tätig werde
 - ▶ h.M.: keine Auftragsverarbeitung, SV ist **eigenständig Verantwortlicher**
 - SV steht aufgrund fachlicher Kompetenz wesentlicher Entscheidungs- und Beurteilungsspielraum zu, welche Daten für Begutachtung erforderlich sind
 - Schwerpunkt liegt in Inanspruchnahme fremder fachlich-intellektueller Leistung des SV als Spezialist auf seinem Gebiet
- **öffentlich bestellte und vereidigte Sachverständige:**
 - ▶ e.A.: SV seien jedenfalls im Rahmen eines gerichtlichen Gutachtenauftrags Auftragsverarbeiter des verfahrensführenden Gerichts, da ihre Tätigkeit als Teil der justiziellen Tätigkeit der Gerichte anzusehen sei
 - ▶ h.M.: keine Auftragsverarbeitung, SV ist **eigenständig Verantwortlicher**
 - Grundpflichten eines öbvS (Objektivität, Unparteilichkeit, Weisungsfreiheit) widersprechen der Weisungsgebundenheit einer Auftragsverarbeiters

16

Organisations- und Rechenschaftspflichten



- **Vertraulichkeitserklärung** der Beschäftigten
- Ggf. Pflicht zur Benennung eines **Datenschutzbeauftragten**
- Pflicht zur Vorhaltung eines **Verarbeitungsverzeichnisses**
- **Rechenschaftspflichten**: Laufende Überwachung und Dokumentation zu Zwecken der Nachweisbarkeit!
- **Datenschutz-Folgenabschätzung** bei Verarbeitungsprozessen, die vsstl. ein hohes Risiko für Betroffenen haben (z.B. bei Einsatz neuer Technologien)
- **Datensicherheit**, insb. technisch-organisatorische Maßnahmen - risikobasierter Ansatz (z.B. ISO/EC 27001, Standard-Datenschutzmodell)
- **Privacy by Design** und **Privacy by Default**
- **Löschkonzept**
- **Meldepflicht bei Datenverstößen**
- **Interne Datenschutzrichtlinien** (insb. bei großen Sachverständigenbüros)



17

Der Datenschutzbeauftragte (DSB)



- **Pflicht zur Bestellung eines DSB (intern oder extern)**
 - ▶ Behörden oder öffentlichen Stellen: grds. ja
 - ▶ nicht-öffentliche Stellen:
 - wenn in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung von pbD beschäftigt sind (z.B. PC-Arbeitsplatz)
 - wenn Kerntätigkeit in besonders risikoreichen und umfangreichen Datenverarbeitungsvorgängen (z.B. in der Verarbeitung besonders sensibler Daten oder in umfangreichen systematischen Überwachungen) liegt
- **Aufgaben des DSB**
 - ▶ Unterrichtung und Beratung der Geschäftsführung und Beschäftigten
 - ▶ Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben und Datenschutzstrategien
 - ▶ Zusammenarbeit mit und Ansprechpartner der Aufsichtsbehörden

18

Der Datenschutzbeauftragte (DSB)

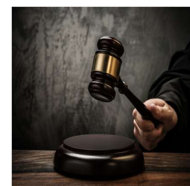
- **Bestellungspflicht des Sachverständigen?**
 - ▶ **Private Sachverständige:**
 - idR nur, wenn 10-Personen-Grenze erreicht ist
 - ▶ **öffentlich bestellte und vereidigte Sachverständige:**
 - Bestellungspflicht als „öffentliche Stelle“?
 - i.d.R. keine öffentliche Stelle, da öffentliche Bestellung zum öbvS nach § 36 GewO, § 91 Nr. 8 HWO sowie den Landesarchitekten-/Ingenieur-/Baukammergesetzen kein Beleihungsakt, d.h. keine Übertragung hoheitlicher Befugnisse
 - „nur“ öffentlich-rechtliche Anerkennung einer besonderen beruflichen Qualifikation
 - Bestellungspflicht daher ebf. idR nur, wenn 10-Personen-Grenze erreicht ist
 - anders bei Beleihung (z.B. öffentlich bestellter Vermessungsingenieur)
 - so auch Auffassung des LfD Niedersachsen (www.lfd.niedersachsen.de)

19

Was droht im Falle eines Verstoßes?

Hohe Bußgelder

- **Bußgeld** bis zu 20 Mio. EUR oder 4 % des weltweiten Vorjahresumsatzes durch Aufsichtsbehörde
- Daneben: **Strafbarkeitsrisiken!**



Zivilrechtliche Haftung

- Insb. **Schadensersatz** für materielle und immaterielle Schäden
- u.U. können auch Geschäftsführer, verantwortliche Führungskräfte oder Datenschutzbeauftragte haftbar gemacht werden
- **Abmahnung** seitens Wettbewerber (OLG Hamburg v. 25.10.2018, 3 U 66/17)

Maßnahmen der Datenschutzaufsichtsbehörden

- Neben Bußgeldverhängung z.B. Untersuchungen, (Ver-) Warnungen, Verhängung von Verarbeitungsverböten oder sonstige Anweisungen

Enormer Imageschaden

20

Aus der Bußgeldpraxis der Aufsichtsbehörden



- Derzeit über 200.000 behördliche Verfahren nach DS-GVO in der EU bekannt
- Höchstes bislang verhängtes Bußgeld i.H.v. 50 Mio. EUR gegen Google seitens französischer Aufsichtsbehörde (CNIL)
 - ▶ Datenschutzhinweise schwer zugänglich, zu abstrakt, ungenau und unverständlich; ungültige Einwilligung für personalisierte Werbung
- Deutsche Aufsichtsbehörden bislang eher zurückhaltend
 - ▶ bislang 64 Bußgeldbescheide u.a. auch gegen kleinere Unternehmen
 - ▶ Höchstes Bußgeld in Deutschland: 80.000 EUR wegen unzulässiger Veröffentlichung von Gesundheitsdaten im Internet infolge mangelhafter Datensicherheit
 - ▶ Weitere Fälle: weitere Fälle mangelnder Datensicherheit (z.B. Abhandenkomme von Kundendaten iRe Hackerangriffs); unzulässiger Versand von Werbe-E-Mails; unzulässiger Einsatz von Videoüberwachungssystemen; unzulässige Datenweitergabe an Geschäftsnachfolger; offene E-Mail-Verteiler, kein AVV
- Weitere Bußgeldverfahren anhängig
- Weitere anlassbezogene und stichprobenartige Überprüfungen angekündigt

21

Daraus folgt



Hohe Haftungsrisiken drohen bei

völligem Untätigbleiben in Zeiten der DS-GVO, aber auch bei

- Verletzung der Informations- und Transparenzpflichten und Missachtung deren Rechte
 - ▶ Keine Datenschutzhinweise auf Internetseite
 - ▶ Keine bzw. keine vollständigen, transparenten oder hinreichend bestimmten Datenschutzhinweise für Kunden, Mitarbeiter etc.
 - ▶ Ignorieren von Auskunftsbegehren, Löschanfragen
- Unzureichende Datensicherheitsmaßnahmen
- fehlerhafte Einwilligungserklärungen
- unzulässiger Einsatz neuer Technologien / Videoüberwachung
- unzulässige Mitarbeiterüberwachungen
- fehlender Abschluss von Auftragsverarbeitungsverträgen
- Keine Meldung von Datenpannen trotz entsprechender Pflicht
- Werbliche Ansprache ohne erforderliche (nachweisbare) Einwilligung des Betroffenen
- Kein Löschkonzept, kein Verarbeitungsverzeichnis, keine Dokumentation



22

Vielen Dank für Ihre Aufmerksamkeit!

Ihre Fragen?



Janina Winz
Rechtsanwältin

Rechtsanwälte Kapellmann und Partner mbB
Stadttor 1
40219 Düsseldorf
Tel.: 02 11 - 600 500 431
janina.winz@kapellmann.de

Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers. Die Präsentation stellt keine Rechtsberatung dar. Diese muss individuell unter Berücksichtigung der Umstände des Einzelfalls erfolgen.

© Kapellmann und Partner Rechtsanwälte mbB