

Die EU-Datenschutz- grundverordnung (DSGVO) und das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO

**Diplom Informatiker
Werner Hülsmann
Datenschutzexperte**

Dipl. Informatiker Werner Hülsmann

- 1982 – 1988 Studium der Informatik an der TU Darmstadt
Schwerpunkt Datenschutzrecht
- 1988 – 1991 Softwareentwickler bei der Telenorma GmbH, Frankfurt (Main)
- 1992 – 1999 Wissenschaftlicher Mitarbeiter und Referatsleiter Technik beim Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen
- 1999 – 2001 Datenschutz- und Technologieberatung bei ForBIT e.V. in Hamburg
- Seit 1999 selbständiger Datenschutzberater (Datenschutzconsulting.info)
- 2001 – 2003 Projektmanager Dataprotection bei der Telegate AG (Martinsried)
- 2003 – 2009 Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz (DVD) e.V., Bonn - www.datenschutzverein.de
- Seit 2004 Kooperationspartner des virtuellen Datenschutzbüros
- 2004 Gründung von Datenschutzwissen.de – Organisation und Leitung von Datenschutzseminaren
- Seit 2004 beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich/technisch)
- Seit 2010 Expert for legal and technical evaluations for the European Privacy Seal (EuroPrise <http://www.european-privacy-seal.eu/>)
- Seit 09/2017 Member of the Commission Multistakeholder expert group to support the application of Regulation (EU) 2016/679 (GDPR)

Platz für
Ihre Notizen

Gliederung

- Datenschutz?!
- Überblick über die Europäische Datenschutz-
Grundverordnung (DSGVO)
 - Ziel der DSGVO
 - Wesentliche Inhalte der DSGVO
- Das Verzeichnis von Verarbeitungstätigkeiten

Datenschutz?!

Datenschutz – was ist das?

- Datenschutz schützt nicht die Daten, sondern dient dem Schutz der **Privatsphäre** sowie der **Grundrechte und Grundfreiheiten** der betroffenen Personen.
- Datenschutz ist keine moderne Erfindung, sondern gibt es bereits seit der Antike (z.B. im Hippokratischen Eid).
- Datenschutz ist ein **Menschenrecht**.
- Der Datenschutz – das Recht auf informationelle Selbstbestimmung – wurde 1983 vom BVerfG aus den **Grundrechten** der Art. 1 und 2 des Grundgesetzes abgeleitet.
- Datenschutz ist seit 2009 auch in der **Europäischen Grundrechtecharta** verankert.

Was sind personenbezogene Daten?

- Einige Beispiele für personenbezogene Daten:

Name Anschrift
Steuerklasse Versicherungsnr.
E-Mail-Adresse KFZ-Kennzeichen
Kontonr. Gehalt
IP-Nummer Telefonnummer Geburtsdatum
usw.

- Personenbezogene Daten können unterschiedlich sensibel sein



Was sind personenbezogene Daten?

Personenbezogene Daten sind gemäß Art. 4 Ziff. 1 DSGVO

- „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 identifiziert werden kann, 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;“

Datenschutzentwicklung in D und der EU

- 1977: Erstes Bundesdatenschutzgesetz
- 1980: OECD: Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten
- 1981: Europarat: Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten
- 1983: Volkszählungsurteil des BVerfG: Recht auf Informationelle Selbstbestimmung
- 1995: EG-Datenschutz-Richtlinie 95/46/EG (umzusetzen bis Oktober 1998, in D 2001 umgesetzt)
- 2009: Europäischen Grundrechtecharta
- 2016: EU-Datenschutzgrundverordnung (DSGVO)
- 2017: Bundesdatenschutzgesetz (BDSG-neu)

Grundgesetz für die Bundesrepublik Deutschland

Artikel 1 – Absatz 1

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Artikel 2 – Absatz 1

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Europäische Grundrechtecharta (EuGRCh)

Artikel 7 - Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8 - Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht

Überblick über die Europäische Datenschutz- Grundverordnung (DSGVO)

Entstehung der Europäischen Datenschutzgrundverordnung

- Im Januar 2012 hat die Europäische Kommission ein umfassendes Paket zur Neuregelung des Datenschutzes in Europa vorgestellt.
- Ein Teil dieses Pakets war der Vorschlag für die EU-DSGVO, die mit ihrem Wirksamwerden die bisherige EU-DS-Richtlinie ersetzen wird.
- Im März 2014 hat das Europäische Parlament seinen Standpunkt zum Entwurf der EU-DSGVO beschlossen.
- Der Ministerrat brauchte wesentlich länger und hat seinen Standpunkt im Juni 2015 festgelegt.
- Die Trilogverhandlungen (zwischen Parlament, Rat und Kommission) kamen im Dezember 2015 zum Abschluss.
- Die EU-DSGVO wurde am 04. Mai 2016 im EU-Amtsblatt veröffentlicht und wird am **25. Mai 2018 direkt und unmittelbar** in der gesamten EU gültig.

Erwägungsgründe und Artikel

- Der eigentlichen Regelungen des Verordnungstextes finden sich in den 99 Artikeln der EU-DSGVO.
- Davor finden sich die sogenannten Erwägungsgründe.
- Diese Erwägungsgründe stellen zwar selbst keine rechtlichen Regelungen dar, beinhalten aber die Motive zur und Gründe für die Einführung der entsprechenden Artikel.
- Die Erwägungsgründe helfen bei der Auslegung und z.T. beim Verstehen der Regelungen der Artikel.
- Viele Erwägungsgründe beziehen sich dabei auf konkrete Artikel
- **Hinweis:** Oft ist es für das Verständnis hilfreich, die englische Originalfassung hinzuzunehmen, da es in der deutschen Fassung Übersetzungsungenauigkeiten und redaktionelle Fehler gibt, einige wenige davon wurden inzwischen korrigiert.

Wesentliche Inhalte der DSGVO

Wichtige Regelungen für den betrieblichen Datenschutz

- Art. 2: Sachlicher Anwendungsbereich (S.109)
- Art. 3: Räumlicher Anwendungsbereich (S. 111)
- Art. 4: Begriffsbestimmungen (S. 104 ff, vgl. § 3 BDSG)
- Kapitel 2: Grundsätze (Art. 5 – 11, S.118)
- Kapitel 3: Rechte der betroffenen Person (Art. 12 – 23, S. 130 ff)
- Kapitel 4: Verantwortlicher* und Auftragsverarbeiter (Art. 24 – 43, S. 151 ff)
- Kapitel 5: Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen (Art. 44 – 50, S. 186 ff)
- Kapitel 8: Rechtsbehelfe, Haftung und Sanktionen (Art. 77 – 84, S. 239 ff)
- Artikel 88: Datenverarbeitung im Beschäftigungskontext

*) gemeint ist mit „Verantwortlicher“ (Englisch: Controller) die bisherige „verantwortliche Stelle“ aus dem BDSG-alt

Grundsätze der Daten- verarbeitung in der DSGVO

Art. 5 Abs. 1 DSGVO fordert, dass personenbezogene Daten nach den folgenden Grundsätzen verarbeitet werden müssen:

- „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“
- „Zweckbindung“
- „Datenminimierung“
- „Richtigkeit“
- „Speicherbegrenzung“
- „Integrität und Vertraulichkeit“

Art. 5 Abs. 2 DSGVO regelt:

- „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)

Die Verarbeitung personenbezogener Daten ist „nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist“:

- die wirksame Einwilligung der betroffenen Person liegt vor
- die Verarbeitung dient der Erfüllung eines Vertrags mit der betroffenen Person oder vorvertraglicher Maßnahmen auf Initiative der betroffenen Person
- die Verarbeitung ist zur Erfüllung gesetzlicher Verpflichtungen erforderlich
- „die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen“
- „die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“
- „die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“

Was ändert sich?

- Die Dokumentationspflichten erhöhen sich
- Die Rechte der Betroffenen werden ausgeweitet
- Es werden neue Bußgeldtatbestände eingeführt
- Die möglichen Bußgelder werden drastisch erhöht (vgl. Art. 83 ff EU-DSGVO)
 - „Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** ist.“ (Art. 83, Abs.1)
 - Höhe der Geldbußen für Unternehmen je nach Verstoß bis zu 10 bzw. 20 Mio. Euro oder 2 bzw. 4 % „gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs“, je nach dem, was der höhere Betrag ist.

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätig- keiten nach der EU-DSGVO

Rechtsgrundlage

- Bisher: § 4e i.V.m. § 4g Abs. 2 und 2a BDSG
- Künftig: Art. 30 EU-DSGVO
- Ab 25. Mai 2018 ist ein fehlendes, unvollständiges oder nicht aktuelles Verzeichnis von Verarbeitungstätigkeiten ein Bußgeldtatbestand, der mit bis zu 10 Mio. Euro oder 2 % des Jahresumsatzes (je nach dem, welcher Betrag höher ist) geahndet werden kann.



Verzeichnis von Verarbeitungstätigkeiten nach der EU-DSGVO

- Das Verzeichnis von Verarbeitungstätigkeiten dient nicht nur der Erfüllung der gesetzlichen Verpflichtung aus Art. 30 DSGVO.
- Es dient vielmehr insbesondere
 - der effizienten Umsetzung des Datenschutzes im Unternehmen
 - der Umsetzung der vielfältigen Dokumentationspflichten aus der DSGVO
- Ein aktuelles Verzeichnis von Verarbeitungstätigkeiten hilft **Risiken zu vermeiden**
 - Bußgeldrisiken für das Unternehmen
 - Risiken für die Grundfreiheiten und Grundrechte der betroffenen Personen

Verzeichnis von Verarbeitungstätigkeiten nach der EU-DSGVO

- Das „öffentliche Verfahrensverzeichnis“ fällt durch die EU-DSGVO weg.
- Das vorhandene Verfahrensverzeichnis ist um die neuen Pflichtangaben
 - Kontaktdaten der Verantwortlichen (inkl. E-Mail-Adresse und Telefonnummer) und
 - Angaben zum/zur Datenschutzbeauftragten zu ergänzen
- Die Angaben zu zugriffsberechtigten Personen sollten entfernt werden, Angaben zu zugriffsberechtigten Personen**gruppen** sind weiterhin sinnvoll, aber nicht vorgeschrieben.

Verzeichnis von Verarbeitungstätigkeiten nach der EU-DSGVO

- Nach Art. 30 Abs. 5 DSGVO gibt es für Unternehmen mit weniger als 250 MitarbeiterInnen Ausnahmen von der Pflicht das Verzeichnis zu führen.
 - Diese Ausnahmen gilt aber nur für Verarbeitungen, die nur gelegentlich erfolgen und weder besondere Risiken (wie z.B. durch Videoüberwachung oder Leistungs- und Verhaltenskontrolle) bedingen noch eine Verarbeitung besonderer Datenarten beinhalten.
 - Diese Ausnahme ist mit Vorsicht zu genießen!
- Auftragsverarbeiter haben nach Art. 30 Abs. 2 DSGVO ein Verzeichnis der „Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung“ zu führen.

Das Verzeichnis von Verarbeitungstätigkeiten der Verantwortlichen enthält

- den Namen und die Kontaktdaten des Verantwortlichen und (...) eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

Das Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche enthält weiterhin

- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation(...);
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Das Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter enthält

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, (...) und eines etwaigen Datenschutzbeauftragten;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, (...)terabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Platz für
Ihre Notizen

Wie kann das Verzeichnis von Verarbeitungstätigkeiten geführt werden

- Es ist schriftlich zu führen, dies kann auch elektronisch erfolgen (sic!)
- Möglichkeiten des Führens sind
 - Nutzung von Formularen mittels einer Textverarbeitung (z.B. Word)
 - Nutzung von entsprechenden Tabellen (z.B. in Excel)
 - Nutzung einer Software speziell für dieses Verzeichnis
 - Nutzung einer Datenschutzmanagementsoftware, die ein entsprechendes Modul für dieses Verzeichnis enthält
- Beispielformulare (siehe Anlage)

Zum Schluss

Weitere Informationen

- <https://dsgvo.expert> - Meine Website zur EU-DSGVO mit Informationen und weiteren Links, insbesondere
 - <https://dsgvo.expert/MatV3T> - Materialien zum Verzeichnis von Verarbeitungstätigkeiten
- Synopse mit Artikeln der DSGVO, den dazugehörigen Erwägungsgründen und den entsprechenden Regelungen des am 25. Mai 2018 in Kraft tretenden Bundesdatenschutzgesetz (BDSG-neu):
<https://efweha-verlag.de/bd41>

Noch Fragen?

- **Diplom-Informatiker Werner Hülsmann**
 - Münchener Str. 101 ■ NL Berlin/Brandenburg:
Gebäude 01 / 1. OG Pappelhof 12
D-85737 Ismaning D-14478 Potsdam
Tel.: 089 / 51 30 569-7 Tel.: 0331 / 58 50 39 31
- E-Mail: wh@datenschutzwissen.de
- <http://www.datenschutzwissen.de>
- <https://dsgvo.expert> – Blog: <http://extdsb.info>