udis

Ulmer Akademie für Datenschutz
und IT-Sicherheit
gemeinnützige Gesellschaft mbH

Neue Regeln für den Datenschutz in Europa

Die 10 wichtigsten Fragen zur Europäischen Datenschutz-grundverordnung (EU-DSGVO)

Rechtsanwalt Ivo Gönner und Prof. Dr. Gerhard Kongehl

Unsere Dozenten

RA Ivo Gönner
Oberbürgermeister der Stadt Ulm a.D.

- 1978 Erstes Juristisches Staatsexamen
- 1981 Zweites Juristisches Staatsexamen
- 1981 - 1992 Selbstständiger Rechtsanwalt in Ulm, eigene Rechtsanwaltskanzlei
- 1985 - 1991 Fraktionsvorsitzender der SPD-Gemeinderatsfraktion im Ulmer Gemeinderat
- 1992 - 2016 Oberbürgermeister der Stadt Ulm
- 2005 - 2010 Präsident des Städtetags Baden-Württemberg
- 2009 - 2016 Präsident des Rats der Donaustädte und -regionen
- 2012 - 2015 Präsident des Verbandes kommunaler Unternehmen (VKU)
- 2016 Verleihung des Verdienstordens des Landes Baden-Württemberg
- seit 2016 Ehrenbürger der Stadt Ulm
- seit 2017 Ehrensenator der Universität Ulm
- seit 2017 Rechtsanwalt in der Kanzlei Derra, Meyer & Partner in Ulm

Prof. Dr. Gerhard Kongehl
Geschäftsführer und wissenschaftlicher Leiter der udis Ulmer Akademie für Datenschutz und IT-Sicherheit gemeinnützige Gesellschaft mbH

- Leiter der Ausbildung zum Datenschutzbeauftragten nach dem Ulmer Modell
- Diplom in Physik, Doktorarbeit in der Hirnforschung
- Zunächst Professor im Bereich Wahrnehmungstheorie mit Schwerpunkt Mensch - Computerkommunikation, dann Professor für Datenschutz, Datensicherheit und Technologiefolgenabschätzung an der FH-Ulm-Hochschule für Technik
- Erster Datenschutzbeauftragter in Baden-Württemberg (Universität und Universitätsklinikum Ulm)
- Ehrenmitglied des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.
- Lehrbeauftragter für Datenschutz der Hochschule Neu-Ulm (HNU)
- Träger des Verdienstkreuzes am Bande des Verdienstordens der Bundesrepublik Deutschland

Die Europäische Datenschutzgrundverordnung – Was ist das eigentlich?

Verordnungen, Richtlinien und nationales Recht

Wir unterscheiden auf EU-Ebene **Richtlinien** und **Verordnungen**.

Eine Richtlinie
der Europäischen Union ist für alle **Mitgliedsstaaten verbindlich nur in Bezug auf ihre Zielsetzung**.

Eine Verordnung
der Europäischen Union ist für alle **Mitgliedsstaaten verbindlich sowohl in Bezug auf ihre Zielsetzung als auch** hinsichtlich der zu ergreifenden **Formen** und **Mittel**.

Verordnungen, Richtlinien und nationales Recht

Eine Verordnung

- ist **Teil der Rechtsordnung** eines jeden Mitgliedstaats der Europäischen Union
- ist unmittelbar **für alle Bürger**,
  für alle öffentlichen Stellen und
  für alle nichtöffentlichen Stellen

  in der Europäischen Union **verbindliches Recht**.

Verordnungen, Richtlinien und nationales Recht

Die Länder der Europäischen Union müssen deshalb ihr **nationales Recht so anpassen**, dass es dem Unionsrecht nicht widerspricht.

Es darf **nichts abgeschwächt oder gestrichen** werden und auch **nur dort etwas hinzugefügt** werden, wo eine Verordnung der EU einen Sachverhalt **nicht abschließend regelt**.

Andernfalls *„verstoßen sie damit gegen ihre Verpflichtung aus dem europäischen Primärrecht zur loyalen Zusammenarbeit (Art. 4 Abs. 3 EUV).“*

Die Öffnungsklauseln der EU-DSGVO

Durch so genannte Öffnungsklauseln im EU-Recht soll den Mitgliedstaaten der EU die **Möglichkeit gegeben werden, nationale Regelungen in das EU-Recht einzubinden.**

Aber nur an den Stellen eines EU-Gesetzes, an welcher eine Öffnungsklausel steht, **kann der nationale Gesetzgeber tätig werden.**

Eine solche Regelung **darf aber nicht im Widerspruch** zu den entsprechenden Regelungen des EU-Rechts stehen.

EU-Datenschutz-Grundverordnung (EU-DSGVO)

173 Erwägungsgründe

99 Artikel in 11 Kapiteln

Sie tritt am 25. Mai 2018 in Kraft
und löst das bisherige Datenschutzrecht in Deutschland ab

Definitionen (Begriffsbestimmungen) 1

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Personenbezogene Daten

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 … Identität dieser natürlichen Person sind;

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Personenbezogene Daten

Merke:

Nur für personenbezogene Daten in diesem Sinne gilt die EU-Datenschutzgrundverordnung!

Bei Verwendung von Daten, die in diesem Sinne keine Personenbezogenen Daten sind, muss man sich um die Datenschutzgesetze nicht kümmern!

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Einwilligung

Einwilligung der betroffenen Person:

jede **freiwillig für den bestimmten Fall,**
in **informierter Weise** und **unmissverständlich**
abgegebene Willensbekundung

in Form einer Erklärung
oder einer **sonstigen eindeutigen bestätigenden Handlung**,

mit der die betroffene Person zu verstehen gibt, dass sie **mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;**

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Verantwortlicher

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,

die allein oder gemeinsam mit anderen

über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

Der Verantwortliche (bzw. die Verantwortlichen) ist (sind) allein für die Einhaltung des Datenschutzes im Betrieb verantwortlich und beweispflichtig!

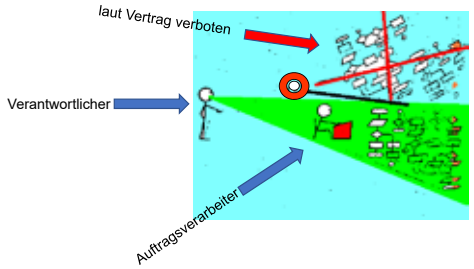
Definitionen (Begriffsbestimmungen) 2

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Auftragsverarbeiter

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,

die personenbezogene Daten **im Auftrag des Verantwortlichen verarbeitet**;



Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Dritter

Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,

außer der betroffenen Person,

dem Verantwortlichen,

dem Auftragsverarbeiter und

den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters **befugt sind, die personenbezogenen Daten zu verarbeiten;**

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Empfänger

Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,

denen personenbezogene Daten

offengelegt werden,

unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Verarbeitung

jeder **mit oder ohne Hilfe automatisierter Verfahren** ausgeführter **Vorgang** oder jede solche **Vorgangsreihe** im Zusammenhang mit personenbezogenen Daten

wie das **Erheben**,
das **Erfassen**,
die **Organisation**,
das **Ordnen**,
die **Speicherung**,
die **Anpassung** oder **Veränderung**,
das **Auslesen**,
das **Abfragen**,
die **Verwendung**,
die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung,
den **Abgleich** oder die **Verknüpfung**,
die **Einschränkung**,
das **Löschen** oder
die **Vernichtung**;

Definitionen (Begriffsbestimmungen) 3

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Verletzung des Schutzes personenbezogener Daten

Verletzung des Schutzes personenbezogener Daten ist
eine **Verletzung der Sicherheit,**

die zur **Vernichtung**, zum **Verlust** oder zur **Veränderung**,
ob unbeabsichtigt oder unrechtmäßig, oder

zur **unbefugten Offenlegung …** beziehungsweise

zum **unbefugten Zugang** zu personenbezogenen Daten führt,

die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Gesundheitsdaten

Gesundheitsdaten sind personenbezogene Daten,

die sich auf die **körperliche oder geistige Gesundheit**

einer natürlichen Person,

einschließlich der **Erbringung von Gesundheitsdienstleistungen**,
beziehen und

aus denen **Informationen über deren Gesundheitszustand hervorgehen**;

Die Verarbeitung von Gesundheitsdaten ist nur unter bestimmten Gegebenheiten erlaubt (Artikel 9)

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Dateisystem

Dateisystem ist jede **strukturierte Sammlung**
personenbezogener Daten,
die nach bestimmten Kriterien zugänglich sind,
unabhängig davon, ob diese Sammlung
zentral, dezentral
oder nach **funktionalen** oder **geografischen**
Gesichtspunkten **geordnet** geführt wird;

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Biometrische Daten

biometrische Daten sind mit speziellen technischen Verfahren
gewonnene personenbezogene Daten zu den

physischen,

physiologischen oder

verhaltenstypischen Merkmalen

einer natürlichen Person,

die **die eindeutige Identifizierung** dieser natürlichen Person
ermöglichen oder bestätigen,

wie **Gesichtsbilder**

oder **daktyloskopische Daten**;

Frage 1: Wann gilt die EU-DSGVO für privatwirtschaftliche Unternehmen?

Artikel 2 EU-DSGVO Sachlicher Anwendungsbereich

Diese Verordnung gilt für die **ganz oder teilweise automatisierte Verarbeitung** **Personenbezogener Daten** sowie für die **nichtautomatisierte Verarbeitung** personenbezogener Daten, die **in einem Dateisystem gespeichert sind** oder gespeichert werden sollen.

Artikel 2 Abs. 1

Sie gilt nicht für unstrukturierte Sammlungen von Unterlagen auf Papier z.B. in Leitz-Ordnern!

Begriffsbestimmungen nach Artikel 4 EU-DSGVO

Personenbezogene Daten

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 … Identität dieser natürlichen Person sind;

Artikel 2 EU-DSGVO Sachlicher Anwendungsbereich

(2) Diese Verordnung **findet keine Anwendung** auf die Verarbeitung personenbezogener Daten

im Rahmen einer Tätigkeit, **die nicht in den Anwendungsbereich des Unionsrechts** fällt,

d. h. sie gilt für alle Unternehmen und Behörden in der EU

Artikel 2 EU-DSGVO Sachlicher Anwendungsbereich

(2) Diese Verordnung **findet keine Anwendung** auf die Verarbeitung personenbezogener Daten

durch natürliche Personen zur Ausübung **ausschließlich persönlicher oder familiärer** Tätigkeiten,

Frage 2: In welchen geographischen Bereichen gilt die EU-DSGVO?

Artikel 3 EU-DSGVO Räumlicher Anwendungsbereich

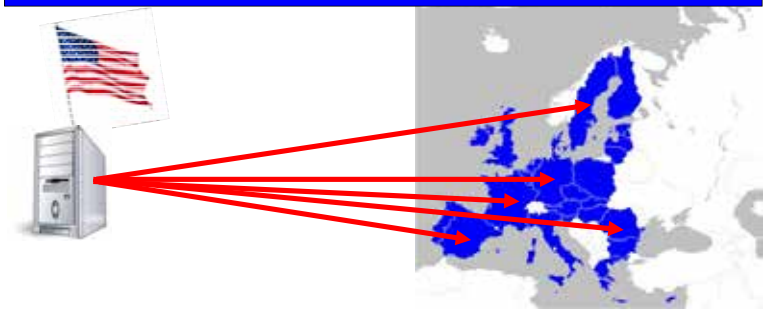
Gilt auch für den EWR
(Europäischen Wirtschaftsraum)

Diese Verordnung findet **Anwendung auf die Verarbeitung** personenbezogener Daten, soweit diese **im Rahmen der Tätigkeiten** … **in der Union erfolgt**

unabhängig davon, ob die Verarbeitung in der Union stattfindet

Artikel 3 Abs. 1

Artikel 3 EU-DSGVO Räumlicher Anwendungsbereich

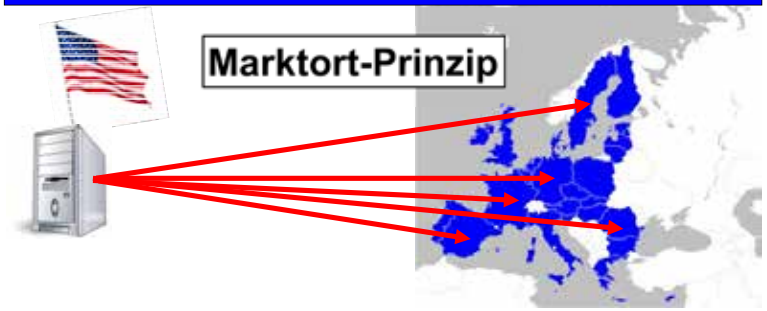


Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen **Personen, die sich in der Union befinden**,

durch einen **nicht in der Union niedergelassenen** Verantwortlichen oder Auftragsverarbeiter,

Artikel 3 Abs. 2

Artikel 3 EU-DSGVO Räumlicher Anwendungsbereich



wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen **in der Union Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

Artikel 3 Abs. 2

EU-DSGVO Räumlicher Anwendungsbereich

wenn die Datenverarbeitung im Zusammenhang damit steht

b) das **Verhalten** betroffener Personen zu **beobachten**, soweit ihr **Verhalten in der Union** erfolgt.

Artikel 3 Abs. 2

Frage 3: Welches sind die wesentlichen Regelungen zur Datensicherheit?

IT-Sicherheit:

Schutz **von Hardware, Software und Daten**

vor Gefährdung der

Vertraulichkeit,
Integrität,
Verfügbarkeit
Datensparsamkeit
Transparenz,
Nichtverkettbarkeit
Intervenierbarkeit

Wesentliche Regelungen zur Datensicherheit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die **eine angemessene Sicherheit** dieser Daten gewährleiste, einschließlich Schutz vor

- unbefugter oder unrechtmäßiger **Verarbeitung** und vor
- unbeabsichtigtem **Verlust**
- unbeabsichtigter **Zerstörung**
- unbeabsichtigter **Schädigung**

durch **geeignete technische und organisatorische Maßnahmen**

Artikel 5 Abs. 1 lit. f

Wesentliche Regelungen zur Datensicherheit

Geeignete technische und organisatorische Maßnahmen unter Berücksichtigung

- der **Eintrittswahrscheinlichkeit der Risiken**
- der **Schwere der Risiken**
- des **Zwecks** der Verarbeitung

für die **Rechte und Freiheiten** natürlicher Personen

Artikel 24 Abs. 1

Der Verantwortliche hat eine **Rechenschaftspflicht** für die **Umsetzung angemessener Sicherheitsmaßnahmen**

Artikel 5 Abs. 2

Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung … **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge,** so führt der Verantwortliche **vorab eine Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Artikel 35 Abs. 1

Der Verantwortliche **konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung …hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte**…

Artikel 36 Abs. 1

Frage 4: Welche neuen Informationspflichten gibt es gegenüber den Betroffenen?

Informationspflichten des Verantwortlichen

1. Werden personenbezogene Daten bei einer betroffenen Person erhoben, so hat der Verantwortliche gegenüber der betroffenen Person **bestimmte Informationspflichten** (siehe Punkt 5) und zwar **schon zum Zeitpunkt der Erhebung** dieser Daten.

Artikel 13 Abs. 1

2. Wenn personenbezogene Daten **nicht bei einer betroffenen Person erhoben**, so hat der Verantwortliche gegenüber der betroffenen Person **ebenfalls Informationspflichten** (siehe Punkt 5)

Artikel 14 Abs. 1

3. Jede betroffene Person hat das Recht, vom Verantwortlichen **eine Bestätigung zu verlangen**, ob Daten verarbeitet werden, die diese Person betreffen.

Artikel 15 Abs. 1

Informationspflichten des Verantwortlichen

4. Trifft Punkt 3 zu, hat die betroffene Person **Recht auf Auskunft** über diese Daten und die unter Punkt 5 aufgelisteten Informationen

Artikel 15 Abs. 1

5. Die oben angesprochenen **Informationspflichten** des Verantwortlichen umfassen u.a. das folgende:

- Verarbeitungszwecke
- Art der Daten, die verarbeitet werden
- Herkunft der Daten
- Empfänger der Daten
- Dauer der Speicherung bzw. Kriterien zur Festlegung der Speicherdauer
- Bestehen einer automatisierten Entscheidungsfindung
- Bei Übermittlung in Drittland, Unterrichtung über entsprechende Garantien zum Datenschutz
- Hinweis auf **Recht der Berichtigung oder Löschung** der Daten
- Hinweis auf **Beschwerderecht bei einer Aufsichtsbehörde**

Informationspflichten des Verantwortlichen

6. Hat die Verletzung des **Schutzes personenbezogener Daten einer betroffenen Person** (siehe Definitionen (Begriffsbestimmungen 3) voraussichtlich **ein hohes Risiko für die persönlichen Rechte und Freiheiten** natürlicher Personen zur Folge, so **benachrichtigt der** Verantwortliche (unter Berücksichtigung bestimmter Ausnahmen – siehe Artikel 34 Abs. 3) die betroffene Person **unverzüglich** von der Verletzung. Dabei teilt er u.a. mit:

- den Namen und die **Kontaktdaten des Datenschutzbeauftragten** oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der **wahrscheinlichen Folgen der Verletzung** des Schutzes personenbezogener Daten
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen **Maßnahmen zur Behebung der Verletzung** des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Artikel 34 Abs. 1

Informationspflichten des Verantwortlichen

7. Die Information der betroffenen Person und die Kommunikation mit ihr hat in

- **präziser**,
- **transparenter**,
- **verständlicher** und
- **leicht zugänglicher Form**

zu erfolgen und in einer

- **klaren** und
- **einfachen Sprache**

Artikel 12 Abs. 1

Frage 5: Bedarf es nach der Verordnung jetzt für jegliche Datenverarbeitung der Einwilligung des Betroffenen?

DV-Verbot mit Erlaubnisvorbehalt

Nein!

Nach Artikel 6 gibt es insgesamt sechs Bedingungen für die Rechtmäßigkeit der Verarbeitung, wenn mindestens eine davon erfüllt ist. Diese sind:

1. Die betroffene Person hat ihre **Einwilligung** zur Verarbeitung der sie betreffenden personenbezogenen Daten **für einen oder mehrere festgelegte Zwecke gegeben**;

Artikel 6 Abs. 1 lit. a

DV-Verbot mit Erlaubnisvorbehalt

2. Die Verarbeitung ist **für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist**, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Antrag der betroffenen Person erfolgen;

Artikel 6 Abs. 1 lit. b

3. Die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

Artikel 6 Abs. 1 lit. c

DV-Verbot mit Erlaubnisvorbehalt

4. Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

Artikel 6 Abs. 1 lit. d

5. 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;

Artikel 6 Abs. 1 lit. e

DV-Verbot mit Erlaubnisvorbehalt

6. Die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person … überwiegen;

Artikel 6 Abs. 1 lit. f

Frage 6: Was ist im Zusammenhang mit der Einholung einer Einwilligung des Betroffenen zu beachten?

Einwilligung der betroffenen Person

Einwilligung

Einwilligung der betroffenen Person ist jede

freiwillig für den bestimmten Fall,
in informierter Weise und
unmissverständlich

abgegebene Willensbekundung

in Form einer Erklärung
oder einer sonstigen eindeutigen bestätigenden Handlung,

mit der die betroffene Person zu verstehen gibt, dass sie
mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Artikel 4 Nr. 11

Einwilligung der betroffenen Person

Bedingungen für die Einwilligung

1. Beruht die Verarbeitung auf einer Einwilligung, **muss der Verantwortliche nachweisen können**, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten **eingewilligt hat**.

Artikel 7 Abs. 1

2. Die betroffene Person hat das Recht, **ihre Einwilligung jederzeit zu widerrufen.** Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. **Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.**

Artikel 7 Abs. 3

Einwilligung der betroffenen Person

Bedingungen für die Einwilligung

3. Erfolgt die **Einwilligung** der betroffenen Person durch eine schriftliche Erklärung, **die noch andere Sachverhalte betrifft,** so muss das Ersuchen um Einwilligung **in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache** so erfolgen, dass es **von den anderen Sachverhalten klar zu unterscheiden** ist.

Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

Artikel 7 Abs. 2

Einwilligung der betroffenen Person

Bedingungen für die Einwilligung

4. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem **die Erfüllung eines Vertrags** einschließlich der Erbringung einer Dienstleistung**, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist**, die für die Erfüllung des Vertrags nicht erforderlich sind.

Artikel 7 Abs. 4

5. Bei einem Angebot, das **einem Kind direkt** gemacht wird, ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind **das 16. Lebensjahr vollendet** hat. Andernfalls ist diese Verarbeitung nur rechtmäßig, soweit diese **Einwilligung durch den Träger der elterlichen Verantwortung** für das Kind erteilt wird.

Artikel 8 Abs. 1

Frage 7: Bedarf es nach der Verordnung einer neuen Einwilligung?

Bestehende Einwilligungen können weiter gelten, wenn die Einwilligungserklärung

- **unmissverständlich formuliert** wurde und sich nicht allgemein auf die Datenverarbeitung, sondern **konkret auf einen oder mehrere bestimmte Zwecke bezieht**
  (Artikel 6 Abs. 1 lit. a)
- zwar **zusammen mit anderen Sachverhalten** eingeholt wurde in Bezug auf die Einwilligung jedoch in einer **einfachen und klaren Sprache von den anderen Sachverhalten unterschieden** wurde
  (Artikel 7 Abs. 2)
- zwar **mit dem Zustandekommen eines Vertrags oder einer Dienstleistung zusammenhängt**, der Freiwilligkeit der Einwilligung aber in größtmöglichem Umfang Rechnung getragen wurde
  (Artikel 7 Abs. 4)

Bestehende Einwilligungen können weiter gelten, wenn die betroffenen Personen:

- vor dem Einholen der Einwilligung auf die **Möglichkeit des Widerspruchs** hingewiesen und dies **auch dokumentiert** wurde (Artikel 7 Abs. 3)
- darauf hingewiesen wurden, dass **bis zum Zeitpunkt des Widerrufs** die Verarbeitung ihrer Daten **rechtmäßig** ist und das dies **auch dokumentiert** wurde (Artikel 7 Abs. 3)
- vor dem Einholen der Einwilligung auf **den Zweck für den die Daten verwendet werden** sollen, hingewiesen wurde und dies **auch dokumentiert** wurde (Artikel 7 Abs. 3)
- Zum **Zeitpunkt der Einwilligung mindestens 16 Jahre alt** waren und andernfalls die Einwilligung durch den Träger der elterlichen Verantwortung erteilt wurde (Artikel 8 Abs.1)

Eine Einwilligung muss **dann nicht erneut eingeholt werden, wenn die hier aufgeführten Punkte bereits berücksichtigt worden sind.** Deswegen müssen **alle bisherigen Einwilligungen daraufhin überprüft werden**. **Wichtig ist, dass entsprechend den neuen Vorschriften auch alles dokumentiert wird. Es besteht Rechenschaftspflicht!**

Frage 8: Muss jedes Unternehmen eine(n) Datenschutzbeauftragte(n) benennen?
Kann auch ein(e) externe(r) statt eines/einer internen Datenschutzbeauftragten benannt werden?

Betriebliche Datenschutzbeauftragte
nach neuem Recht

Verantwortliche und der Auftragsverarbeiter haben eine(n) Datenschutzbeauftragte(n) zu benennen, **soweit sie in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.**

§38 BDSG neu

Betriebliche Datenschutzbeauftragte
nach neuem Recht

Auch **Unternehmen, die weniger als 10 Personen** in diesem Bereich beschäftigen, haben eine(n) Datenschutzbeauftragte(n) zu benennen, wenn

- die Kerntätigkeit in der umfangreichen Verarbeitung **besonderer Arten von Daten** (z.B. Gesundheitsdaten) besteht,
- Daten verarbeitet werden, die eine **Datenschutz-Folgenabschätzung** erforderlich machen,
- es **Adresshändler, Auskunfteien, Detekteien, Markt-** und **Meinungsforscher** betrifft.

§38 BDSG neu

Auch **Unternehmen, die keine(n) Datenschutzbeauftragte(n) benennen müssen haben die Einhaltung der Datenschutzvorschriften zu gewährleisten.** Auch hier ist der Verantwortliche voll für den Datenschutz verantwortlich

Betriebliche Datenschutzbeauftragte
nach neuem Recht

Der Datenschutzbeauftragte kann **Beschäftigter** des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der **Grundlage eines Dienstleistungsvertrags** erfüllen.

Artikel 37 Abs. 6

Der Verantwortliche oder der Auftragsverarbeiter **veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit**.

Artikel 37 Abs. 7

Betriebliche Datenschutzbeauftragte
nach neuem Recht

(3) Die oder der Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner **beruflichen Qualifikation und insbesondere ihres oder seines Fachwissens** benannt, das sie oder er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in Artikel 39 (§7 BDSG neu) genannten Aufgaben.

Artikel 37 Abs. 5
BDSG neu §5 Abs. 3

Frage 9: Was ist für Unternehmen wichtig?

Beschäftigten-Datenschutz

Was der Chef **nicht unbedingt wissen muss**, **darf er auch nicht wissen**:

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies **für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung** oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

§ 26 Abs. 1 BDSG (neu)

Hausrecht

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) **ist nur zulässig, soweit sie** … zur Wahrnehmung des **Hausrechts** … erforderlich ist und **keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.**

§ 4 Abs. 1 BDSG (neu)

Zum Zwecke der **Gefahrenabwehr** und zur **Verfolgung von Straftaten** ist eine Überwachung ebenso möglich, wie zur

- **Geltendmachung,**
- **Ausübung oder**
- **Verteidigung**

zivilrechtlicher Ansprüche

Besondere Berufe / Tätigkeiten

- Für Unternehmen im Gesundheitswesen sind weiterhin Möglichkeiten gegeben, **Patientendaten** zu verarbeiten. Einsatz und Verwendung muss aber anhand der neuen rechtlichen Bestimmungen überprüft werden. **Insbesondere müssen auch professionelle Maßnahmen des technischen Datenschutzes** realisiert werden. Hier sind Versäumnisse jetzt mit Bußgeld bedroht.
- Spezielle Regelungen gelten vor allem auch für die **Kreditwirtschaft** im Hinblick auf Bonitätsauskünfte oder Scoring-Verfahren. **Schutzwürdige Interessen der Betroffenen** müssen mit den **Interessen der datenverarbeitenden Stelle** abgewogen werden. Insbesondere besteht die Pflicht zur Dokumentation. Dies muss in einem **Verzeichnis der Verarbeitungstätigkeiten** verbunden mit einer Risikobewertung dargestellt werden.
- **Datenpannen** sind jetzt **spätestens 72 Stunden nach Bekanntwerden** bei der Datenschutzbehörde anzuzeigen.

Bußgeldregelungen

Bei einfachen Verstößen gegen Bestimmungen der Verordnung werden **Geldbußen von bis zu 10 000 000 EUR** oder im Fall eines Unternehmens von bis zu **2% seines gesamten weltweit erzielten Jahresumsatzes** des vorvergangenen Geschäftsjahr verhängt, je nachdem, **welcher der Beträge höher ist.**

Artikel 83 Abs. 4

Bei bestimmten besonders schwerwiegenden Verstößen gegen Bestimmungen der Verordnung werden **Geldbußen von bis zu 20 000 000 EUR** oder im Fall eines Unternehmens von bis zu **4% seines gesamten weltweit erzielten Jahresumsatzes** des vorvergangenen Geschäftsjahr verhängt, je nachdem, **welcher der Beträge höher ist:**

Artikel 83 Abs. 5

Grundsatz: Geldbußen sollen in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** sein

Artikel 83 Abs. 1

Frage 10: Was muss getan werden, um Bußgelder zu vermeiden?

Überprüfung und Anpassung der Organisations-struktur des eigenen Unternehmens in der Weise, dass diese den besonderen technischen und organisatorischen Anforderungen der EU-Datenschutz-Grundverordnung gerecht wird:

- **Benennung eines Datenschutzexperten** für das Unternehmen (ggf. einen Datenschutzbeauftragten, wenn mehr als 9 Menschen mit personenbezogenen Daten umgehen – siehe Frage 8),
- **Proaktive Organisation der Betroffenenrechte** einschließlich Dokumentation, um der Rechenschaftspflicht (siehe unten) zu genügen,
- **Überprüfung und Anpassung von Verträgen** in Bezug auf die Anforderungen der Verordnung (Compliance!), insbesondere auch bei der Auftragsverarbeitung (siehe Definitionen 3),
- **Schaffung von Awareness für mögliche Datenpannen** durch Schulungsmaßnahmen (Pannen müssen innerhalb von 72 Stunden der Aufsichtsbehörde mitgeteilt werden!),

Überprüfung und Anpassung der Organisations-struktur des eigenen Unternehmens in der Weise, dass diese den besonderen technischen und organisatorischen Anforderungen der EU-Datenschutz-Grundverordnung gerecht wird:

- **Organisation und Dokumentation der technischen Sicherheit** entsprechend der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die von der DV betroffenen (siehe Frage 3),
- **Abstimmung mit der Aufsichtsbehörde** wegen möglicherweise erforderlichen Folgenabschätzungen in Bezug auf die Risiken der personenbezogenen Datenverarbeitung (Artikel 35 und 36),
- **Dokumentation aller Verarbeitungstätigkeiten** in Bezug auf Rechtmäßigkeit, Transparenz, Zweckbindung, Datensparsamkeit, Richtigkeit, Zugriffsmöglichkeit, Integrität und Vertraulichkeit, um der Rechenschaftspflicht (siehe unten) zu genügen,
- Darüber hinaus in größeren Unternehmen(>249 Mitarbeiter): **Überprüfung und Anpassung des Verzeichnisses aller Verarbeitungstätigkeiten** in Bezug auf den Umgang mit personenbezogenen Daten nach Artikel 30.

Man sollte bei der Umsetzung der EU-Datenschutzgrundverordnung sein **Augenmerk nicht nur auf die Bußgelder richten**. **Viel wichtiger ist möglicherweise die Rechenschaftspflicht.** Hier handelt es sich gegenüber der bisherigen Datenschutz-gesetzgebung um eine Beweislastumkehr: Der Verantwortliche muss beweisen, dass er die Datenschutzvorschriften korrekt umgesetzt hat. **Hierdurch wird der Datenschutz weit mehr als bisher zum Wettbewerbsfaktor**. Man lässt z.B. den Mit-bewerber abmahnen, wenn man der Auffassung ist, dass er die Vorschriften der Verordnung nicht so rechtskonform umgesetzt hat, wie man selbst (siehe hierzu auch Artikel 80 der Verordnung).

Zusammenfassende Empfehlungen

Die bereits jetzt stattfindenden Datenverarbeitungen müssen anhand der neuen EU-Datenschutzverordnung und des neuen Datenschutzrechts in Deutschland **auf ihre weitere Zulässigkeit hin überprüft und ggf. angepasst werden**.

Anstehende und neu zu gestaltende Datenverarbeitungen müssen bereits jetzt an die Vorgaben des neuen Datenschutzrechts ausgerichtet werden. Aufgrund der umfassenden Erweiterungen der Informationspflichten gegenüber den Betroffenen **müssen bestehende und zukünftige Datenerhebungen und Datenverarbeitungen schon von Anfang an die Erfüllung künftiger Informationspflichten berücksichtigen. Sie müssen in die Prozesse mit eingebunden werden**.

Ab dem **25.05.2018** ist nur noch die Verarbeitung personenbezogener Daten zulässig, die der neuen und überall in der Europäischen Union geltenden Datenschutzgrundverordnung entspricht.

udis

Ulmer Akademie für Datenschutz
und IT-Sicherheit
gemeinnützige Gesellschaft mbH

Sedanstraße 14
89077 Ulm

Geschäftsstelle und Postanschrift:
udis gGmbH
Marlene-Dietrich-Straße 5
89231 Neu-Ulm

Kontaktmöglichkeiten

E-Mail: info@udis.de
Webseite: www.udis.de

Bei Fragen können Sie direkt unser Kontaktformular verwenden:
https://www.udis.de/kontakt/formular.php

Wenn Sie sich für ein Seminar anmelden wollen, können Sie unmittelbar unser Anmeldeformular verwenden:
https://www.udis.de/kontakt/anmeldung.php

Telefon: (0731) 985 885 60
Telefax: (0731) 985 885 64

Geschäftszeiten Büro: Montag bis Freitag von 8:30 Uhr bis 12:00 Uhr
Ansprechpartner:
Prof. Dr. Gerhard Kongehl
Geschäftsführender Gesellschafter und wissenschaftlicher Leiter der udis Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH

Redaktion und Text: Prof. Dr. Gerhard Kongehl, Ivo Gönner

Titelgestaltung, Layout: Bert Neumann, Büro für Gestaltung, Nürtingen

udis

Ulmer Akademie für Datenschutz und IT-Sicherheit
gemeinnützige Gesellschaft mbH