

## **EU-Datenschutz-Grundverordnung – BDSG (neu)**

Die Gesetzestexte können unter <https://dsgvo-gesetz.de/> im Internet abgerufen werden. Auch die Erwägungsgründe, welche zur Auslegung des Gesetzes dienen sind dort aufgeführt

**Was muss ich wissen zur EU-Datenschutz Grundverordnung? – bitkom – mit Mustern und Hinweisen** - <https://www.bitkom.org/Presse/Anhaenge-an-Pls/2016/160909-EU-DS-GVO-FAQ-03.pdf>

Die Datenschutz-Grundverordnung (DSGVO), englisch General Data Protection Regulation (GDPR), ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Die Datenschutz-Grundverordnung gilt als EU-Verordnung unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018 ohne dass es einer weiteren gesetzlichen Umsetzung bedarf.

Viele Bereiche des Datenschutzes werden durch die DSGVO nicht neu geregelt und waren auch schon im (alten) Bundesdatenschutzgesetz enthalten. Insbesondere bleibt der Begriff der „personenbezogenen Daten“ im Artikel 4 DSGVO weiterhin weit gefasst:

### **Art 4 DSGVO**

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „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;
  2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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;
- (..)

Weiterhin gilt, dass die Verarbeitung personenbezogener Daten nur aufgrund eines Erlaubnistatbestands zulässig ist. Diese sind im Artikel 6 aufgeführt:

### **Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung**

- (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
  - a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

- b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e) 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;
- f) 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, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. (..)

#### Grundsätze für die Verarbeitung personenbezogener Daten (Art 5 DSGVO)

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)
- Datenminimierung („dem Zweck angemessen und erheblich sowie auf das [...] notwendige Maß beschränkt“)
- Richtigkeit („es sind alle angemessenen Maßnahmen zu treffen, damit [unrichtige] personenbezogene Daten unverzüglich gelöscht oder berichtigt werden“)
- Speicherbegrenzung (Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es [...] erforderlich ist“)
- Integrität und Vertraulichkeit („angemessene Sicherheit der personenbezogenen Daten [...], einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“)

#### Weitere wichtige Grundsätze:

- Transparenz - der Erwägungsgrund (39) hebt den Grundsatz der Transparenz jeglicher Datenverarbeitung für die betroffenen Personen hervor. Mehrere Artikel in der DSGVO verlangen entsprechende Maßnahmen:
  - Nach Artikel 15 hat jede Person das Recht auf Auskunft über alle sie betreffenden Daten.
  - Die Informationen darüber sind laut Artikel 12 in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu liefern.
  - Nach Artikel 13 und 14 muss jeder betroffenen Person bei einer Datenerhebung umfangreich Auskunft u. a. über Zweck, Empfänger und Verantwortliche der Datenverarbeitung, Dauer der Datenspeicherung, Rechte zur Berichtigung, Sperrung und Löschen und Verwendung der Daten für Profiling-Zwecke gegeben werden. Wenn sich der Zweck ändert, ist die betroffene Person aktiv zu informieren.
  - Nach Artikel 16 hat die betroffene Person ein Recht auf Berichtigung falscher Daten sowie laut Artikel 18 ein Recht auf Einschränkung („Sperrung“) der Datenverarbeitung, wenn Richtigkeit oder Grundlage der Datenverarbeitung bestritten werden.

- **Recht auf Vergessenwerden** - Das Recht auf Vergessenwerden (Artikel 17 ausdrücklich so benannt) umfasst einerseits, dass eine betroffene Person das Recht hat, das Löschen aller sie betreffenden Daten zu fordern, wenn die Gründe für die Datenspeicherung entfallen. Andererseits muss aber auch der Verarbeiter selbst aktiv die Daten löschen, sofern es keinen Grund mehr für eine Speicherung und Verarbeitung gibt.
- **Recht auf Datenübertragbarkeit** - Artikel 20 bestimmt, dass eine betroffene Person das Recht hat, sie betreffende Daten in einem „strukturierten, gängigen und maschinenlesbaren Format zu erhalten“, auch und insbesondere für den Zweck, sie anderen „ohne Behinderung durch den Verantwortlichen“ zu übermitteln.
- **Datensparsamkeit/Datenminimierung** - Privacy by Design, Privacy by Default: im Erwägungsgrund (78) werden die Begriffe „data protection by design“ und „data protection by default“ eingeführt, üblicherweise als „Privacy by Design“ und „Privacy by Default“ bezeichnet. Diese Grundsätze bedeuten, dass die Technik („design“) der Datenverarbeitung von vorneherein darauf entworfen und ausgerichtet ist und die Voreinstellungen („defaults“) so ausgewählt sind, dass den Grundsätzen des Datenschutzes Genüge getan wird.

Die DSGVO ändert daher das bisher in Deutschland des geltenden Datenschutzrechts nicht grundlegend. Vielmehr werden vielfach Bestimmungen der EG-Datenschutzrichtlinie 95/46 übernommen, welche die Grundlage des BDSG bilden.

Jedoch gibt es auch zahlreiche neue datenschutzrechtliche Vorgaben sowie bei Verstöße einen deutlich erhöhten Bußgeldrahmen! (bis zu 20 Mio € oder 4 % des weltweiten vorjährigen Gesamtumsatzes).

Das europäische Datenschutzrecht gilt auch für außereuropäische Unternehmen, soweit diese ihre Waren oder Dienstleistungen im europäischen Markt anbieten (Marktortprinzip)

### **Muster und Auslegungen der Datenschutzbehörden zur Umsetzung und Planung einer gesetzeskonformen Datenverarbeitung nach DSGVO**

- **Handreichungen für kleine Unternehmen und Vereine** – Bayerisches Landesamt für Datenschutz (BayLDA) - <https://www.lida.bayern.de/de/kleine-unternehmen.html>
- **Maßnahmenplan** zur Umsetzung der DSGVO (Kurzpapier DSK) - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_8\\_massnahmenplan.pdf](https://www.lida.bayern.de/media/dsk_kpnr_8_massnahmenplan.pdf)
- **Fragebogen** zur Umsetzung der DSGVO - [https://www.lida.bayern.de/media/dsgvo\\_fragebogen.pdf](https://www.lida.bayern.de/media/dsgvo_fragebogen.pdf)
- **Selbsteinschätzung** zur DSGVO – Onlinetool - <https://www.lida.bayern.de/tool/start.html>  
Checkliste Datenschutz-Grundverordnung – vom BVMW - [https://www.bvmw.de/fileadmin/03-Themen/Digitalisierung/checkliste-12-fragen-zum-datenschutz\\_002\\_.pdf](https://www.bvmw.de/fileadmin/03-Themen/Digitalisierung/checkliste-12-fragen-zum-datenschutz_002_.pdf)

## Relevante Kurzpapiere der Datenschutzkonferenz (DSK) – Auslegungshilfen zur DSGVO

- **Einwilligung** nach der DSGVO - [https://www.lida.bayern.de/media/baylda\\_ds-gvo\\_9\\_consent.pdf](https://www.lida.bayern.de/media/baylda_ds-gvo_9_consent.pdf)
- Bedingungen für die **Einwilligung eines Kindes**, Art. 8 DS-GVO - [https://www.lida.bayern.de/media/baylda\\_ds-gvo\\_15\\_childs\\_consent.pdf](https://www.lida.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf)
- **Verzeichnis von Verarbeitungstätigkeiten** Art 30 DSGVO - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_1\\_verzeichnis\\_verarbeitungstaetigkeiten.pdf](https://www.lida.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf)
- **Verarbeitung personenbezogener Daten für Werbung** - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_3\\_werbung.pdf](https://www.lida.bayern.de/media/dsk_kpnr_3_werbung.pdf)
- **Datenschutz-Folgenabschätzung** – Art 35 DSGVO - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_5\\_dsfa.pdf](https://www.lida.bayern.de/media/dsk_kpnr_5_dsfa.pdf)
- **Informationspflichten** bei Dritt- und Direkterhebung von Daten - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_10\\_informationspflichten.pdf](https://www.lida.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf)
- **Recht auf Löschung** / „Recht auf Vergessenwerden“ - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_11\\_vergessenwerden.pdf](https://www.lida.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf)
- **Datenschutzbeauftragter** – Pflicht zur Benennung, Form, Qualifikation, Aufgaben - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_12\\_datenschutzbeauftragter.pdf](https://www.lida.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf)
- **Videoüberwachung** - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_15\\_videoueberwachung.pdf](https://www.lida.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf)
- **Besondere Kategorien personenbezogener Daten** (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, genetische Angaben, biometrische Daten - [https://www.lida.bayern.de/media/dsk\\_kpnr\\_17\\_besondere\\_kategorien.pdf](https://www.lida.bayern.de/media/dsk_kpnr_17_besondere_kategorien.pdf)

## Weitere wichtige Links und Übersichten zum neuen EU-DSGVO

- Was ist **Auftragsverarbeitung**: Übersicht von bitkom - <https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-LF-Auftragsverarbeitung-online.pdf>
- Muster eines Auftragsvertragsvertrags - <https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf>.

**Prüfung einer Webseite auf Verschlüsselung** (SSL-Zertifikat - Pflicht bei eine Verarbeitung von personenbezogenen Daten bzw. jegliche Nutzereingabe auf der Webseite (Kontaktformular, Login, Suchfeld, Unterlagen hochladen, ...) - <https://www.lida.bayern.de/de/httpscheck.html>

Achtung: Bei Nichterfüllung der vorgegebenen Anforderungen an eine HTTPS-Verschlüsselung wird der verantwortliche Webseitenbetreiber zur Anpassung aufgefordert!

**Orientierungshilfe zu den Datenschutzerfordernungen an App-Entwickler und App-Anbieter** (noch nach BDSG! – eventuelle Änderungen nach DSGVO beachten) - [https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH\\_App.pdf?\\_\\_blob=publicationFile&v=3](https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_App.pdf?__blob=publicationFile&v=3)

Stand 08/2018