

# Startschuss DSGVO: Die wichtigsten Neuerungen für Unternehmen auf einen Blick

Dr. Sven Polenz  
Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein



[www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

## Übersicht

### I. Allgemeine Grundsätze

### II. Spezielle Punkte (Auswahl)

1. Einwilligung und Informationspflichten
2. Fristen bei der Gewährleistung von Rechten betroffener Personen sowie Eskalationsfälle
3. Erweitertes Auskunftsrecht
4. Gestaltung der Verarbeitung
5. Verarbeitungsverzeichnisse
6. Anforderungen bei Auftragsverarbeitung
7. Meldepflichten
8. Benennung von Datenschutzbeauftragten
9. Beschäftigtendatenschutz
10. Anwendung der DSGVO im internationalen Kontext

### III. Zusammenfassung

# Datenschutz-Grundverordnung

- Konstrukt „Verordnung“: **unmittelbar anwendbar**
- Anwendungsvorrang gegenüber nationalem Recht
- 70 **Öffnungsklauseln** (Regelungsaufträge und Regelungsoptionen) für nationalen Gesetzgeber
- Geltung ab **25.05.2018**

- **Marktortprinzip**
- **One-Stop-Shop:**  
einfacher für Verbraucher(innen)
- **Kohärenzmechanismus:**  
Einigung der Aufsichtsbehörden



# DSGVO als „Game Changer“



 Bild: Astryd\_MAD via Pixabay

**Mächtige Toolbox,**  
wenn entsprechend  
verwendet

- **Marktortprinzip** (Art. 3 DSGVO)
- **Verantwortung** (Art. 24 DSGVO)
- **Datenschutz „by design“** (Art. 25(1) DSGVO)
- **Datenschutz „by default“** (Art. 25(2) DSGVO)
- **Sicherheit** (Art. 32 DSGVO)
- **Datenschutz-Folgenabschätzung**  
(Art. 35 DSGVO – „Rechte und Freiheiten natürlicher Personen“)
- **Zertifizierung** (Art. 42+43 DSGVO)
- **Bußgelder & Sanktionen** (Art. 83+84 DSGVO)
- **Gerichte**

**Vorab:**  
Zulässigkeits-  
prüfung

# I. Allgemeine Grundsätze, Art. 5 DSGVO

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz** (→ Rechtsgrundlagen, Nachvollziehbarkeit)
- **Zweckbindung** (→ festgelegte, eindeutige und legitime Zwecke)
- **Datenminimierung** (→ Begrenzung durch Zwecksetzung)
- **Richtigkeit** (→ Berichtigung/Löschung personenbezogener Daten)
- **Speicherbegrenzung** (→ Erforderlichkeit)
- **Integrität und Vertraulichkeit** (→ technisch-organisatorische Maßnahmen)
- **Rechenschaftspflicht** (→ Dokumentationspflicht)

# II. Spezielle Punkte

## 1. Einwilligung und Informationspflichten

- Willensbekundung für den bestimmten Fall, **in informierter Weise** und in unmissverständlicher Form (Information über Verantwortliche und Zwecke), EG 43 DSGVO
- **Nachweis der Erteilung** einer wirksamen Einwilligung (Implementierung von Mechanismen), Art. 7 Abs. 1 DSGVO
- **„opt-in“**, nicht „opt-out“, EG 32 DSGVO

## II. Spezielle Punkte

### 1. Einwilligung und Informationspflichten

- Belehrung über **Widerrufsrecht** vor Abgabe der Erklärung, Art. 7 Abs. 3 Satz 3 DSGVO
- **Freiwilligkeit der Erklärung** (insbesondere: Ist die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung personenbezogener Daten **abhängig**, die für die Erfüllung des Vertrags nicht erforderlich sind?), Art. 7 Abs. 4 DSGVO
- zusätzlich: **Erfüllung von Informationspflichten** nach Art. 13 DSGVO (z.B. Kontaktdaten des Datenschutzbeauftragten, beabsichtigte Datenübermittlung in Drittland, Speicherdauer, Belehrung über Rechte betroffener Personen)

## II. Spezielle Punkte

### 1. Einwilligung?

- a) Anton kauft einen Rasenmäher auf Rechnung. Der Verkäufer erhebt die Rechnungsadresse.
- b) Abwandlung 1: Der Rasenmäher wird nur dann geliefert, wenn Anton drei weitere technische Geräte zur Pflege seines Gartens benennt, an denen er Interesse hätte.
- c) Abwandlung 2: Der Rasenmäher wird geliefert. Anton wird vom Verkäufer gebeten, drei weitere technische Geräte zur Pflege seines Gartens zu benennen, an denen er Interesse hätte.
- d) Abwandlung 3: Der Verkäufer bietet Anton einen Rabatt auf den Kaufpreis, wenn er drei weitere Geräte zur Gartenpflege benennt, an denen Interesse besteht.

## II. Spezielle Punkte

### 1. Einwilligung

- e) Ein Unternehmen möchte seine Einwilligungsklauseln über den 25. Mai 2018 hinaus verwenden. Informationen nach Art. 13 DSGVO sind im Text nicht vorhanden. Es fehlt auch ein Hinweis auf ein bestehendes Widerrufsrecht.

Vgl. EG 171 Satz 2 DSGVO

- (171) Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.

08.01.2018

9

## II. Spezielle Punkte

### 2. Fristen bei der Gewährleistung von Rechten betroffener Personen sowie Eskalationsfälle, Art. 12 Abs. 3-5 DSGVO

- Die Ergreifung von Maßnahmen nach den Art. 15-22 DSGVO (z.B. Auskunft, Löschung, Berichtigung, Einschränkung der Verarbeitung, Widerspruch) muss durch den Verantwortlichen unverzüglich, längstens jedoch **innerhalb eines Monats** nach Eingang eines Antrages auf Auskunft durch die betroffene Person erfolgen (Art. 15 Abs. 3 DSGVO).
- Eine Fristverlängerung um **bis zu weitere 2 Monate** kann zulässig sein (→ Benachrichtigungs- und Begründungspflicht beachten).
- Sollte der Verantwortliche nicht tätig werden, hat er die betroffene Person ohne Verzögerung über die Gründe hierfür und seine rechtlichen Möglichkeiten zu informieren.
- Bei **offenkundig unbegründetem oder exzessivem Charakter** des Antrages kann der Verantwortliche ein Entgelt verlangen oder sich weigern, aufgrund des Antrags tätig zu werden (→ Nachweispflichten beachten).

## II. Spezielle Punkte

### 3. Erweitertes Auskunftsrecht, Art. 15 DSGVO

- Art. 15 DSGVO enthält das Recht der betroffenen Person, von dem Verantwortlichen einen ausführlichen Katalog an Informationen zu erhalten.
- Die betroffene Person hat das Recht auf **Erhalt einer kostenfreien Kopie** über die personenbezogenen Daten, die verarbeitet werden.
- Wird der Antrag auf Auskunft **elektronisch** gestellt, so sind die Informationen grundsätzlich auch elektronisch zur Verfügung zu stellen.
- Es sind die allgemeinen Grundsätze nach Art. 12 DSGVO zu beachten, insbesondere Vorgaben zu **Fristen, Kosten und Identitätsnachweise**.

## II. Spezielle Punkte

### 4. Verarbeitungsverzeichnis, Art. 30 DSGVO

- Der Verantwortliche hat die **Pflicht, ein Verzeichnis zu führen**.
- Art. 30 enthält einen ausführlichen Katalog über die im Verzeichnis erforderlichen Angaben.
- Auftragsverarbeiter müssen künftig ein **separates Verzeichnis** über die von Ihnen erbrachten, weisungsgebundenen Tätigkeiten führen.
- Es ist nicht mehr öffentlich zur Verfügung zu stellen.
- Es bestehen Ausnahmen für Betriebe bis 250 Mitarbeiter, sofern keine kritische Datenverarbeitung erfolgt, keine Daten besonderer Kategorien verarbeitet werden, kein Risiko für Rechte und Freiheiten betroffener Personen besteht und die Verarbeitung nicht nur gelegentlich erfolgt.

## II. Spezielle Punkte

### 5. Gestaltung der Verarbeitung

- a) Art. 32 DSGVO: **eingebaute Sicherheit**  
[Abwägung Zweck, Risiken für betroffene Personen, Stand der Technik, Kosten]
- b) Art. 25 Abs. 1 DSGVO: **eingebauter Datenschutz** – von Anfang an  
[Abwägung Zweck, Risiken für betroffene Personen, Stand der Technik, Kosten]
- c) Art. 25 Abs. 2 DSGVO: **datenschutzfreundliche Vorsteinstellungen**  
[ohne Abwägung: Umsetzung der Erforderlichkeit]
- d) Art. 35 DSGVO: **Datenschutz-Folgenabschätzung**  
[bei voraussichtlich hohem Risiko]

## II. Spezielle Punkte

### 6. Anforderungen bei Auftragsverarbeitung

- Der Verantwortliche hat die Verpflichtung, nur mit solchen Auftragsverarbeitern zusammenzuarbeiten, die **hinreichende Garantien** für geeignete technisch-organisatorische Maßnahmen bieten.
- **Unterbeauftragungen** müssen vom Verantwortlichen schriftlich autorisiert sein.
- Bei allgemeinen schriftlichen Genehmigungen stehen dem Verantwortlichen **Einspruchsrechte** gegen den Auftragsverarbeiter zu.
- Für den Vertrag über die Auftragsverarbeitung gilt die **Schriftform**.
- Dem Unterauftragnehmer müssen **die gleichen Datenschutzverpflichtungen** auferlegt werden wie dem Hauptauftragnehmer.
- Bestimmt der Auftragsverarbeiter ordnungswidrig Zwecke und Mittel der Verarbeitung, wird er **wie ein Verantwortlicher** behandelt (Art. 28 Abs. 10 DSGVO).

## II. Spezielle Punkte

### 6. Anforderungen bei Auftragsverarbeitung

Verpflichtende Vertragsinhalte (Auswahl):

- Datenübermittlungen (auch in Drittstaaten) bedürfen einer **dokumentierten Weisung** des Verantwortlichen.
- Befugte Personen des Auftragsverarbeiters müssen einer vertraglichen oder gesetzlichen **Verschwiegenheitspflicht** unterliegen.
- Es besteht eine **Pflicht zur Unterstützung des Verantwortlichen** bezüglich der Meldepflichten gegenüber der Aufsichtsbehörde bei Datenschutzverstößen (Art. 33 DSGVO), bei der Benachrichtigung betroffener Personen bei Datenschutzverletzungen (Art. 34 DSGVO), bei der Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und bei Konsultationsverfahren nach Art. 36 DSGVO.

## II. Spezielle Punkte – 7. Meldepflichten

### Derzeit: Meldepflichten nach § 42a BDSG

- Begrenzt auf bestimmte Datenkategorien (§ 42a Satz 1 BDSG)
- Unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt
- Es drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen
- Unverzügliche Meldung an Aufsichtsbehörde/Betroffene

### Künftig: Meldepflichten nach Art. 33 und 34 DSGVO

- **Keine Begrenzung auf bestimmte Datenkategorien** („Verletzung des Schutzes personenbezogener Daten“)
- Meldepflicht an Aufsichtsbehörde entfällt, wenn Verletzung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“
- **Meldung an Aufsichtsbehörde unverzüglich** (möglichst binnen 72 Std.)
- **Benachrichtigung** der betroffenen Personen kann in bestimmten Fällen entfallen

## II. Spezielle Punkte

### 8. Benennung von Datenschutzbeauftragten

- a) **Verpflichtung** zur Benennung für
- öffentliche Stellen,
  - nichtöffentliche Stellen (10-Personen-Grenze)
  - Verantwortliche wie Auftragsverarbeiter
  - bei bestimmten Kerntätigkeiten (umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen / Verarbeitung von Datenkategorien nach Art. 9 u. 10 DSGVO)
- b) Auswahl anhand beruflicher Qualifikation und Fachkunde/Datenschutzpraxis
- c) **Pflicht zur Mitteilung der Kontaktdaten an Aufsichtsbehörde** + Veröffentlichungspflicht (Art. 37 Abs. 7 DSGVO)

## II. Spezielle Punkte

### 8. Benennung von Datenschutzbeauftragten

- d) Pflicht des Verantwortlichen/Auftragsverarbeiters, den Datenschutzbeauftragten **ordnungsgemäß und frühzeitig** einzubinden (Art. 38 Abs. 1 DSGVO)
- e) Pflicht des Verantwortlichen/Auftragsverarbeiters zur Bereitstellung von Ressourcen/keine Erteilung von Weisungen
- f) **Aufgaben des Datenschutzbeauftragten:**
- Unterrichtung und Beratung des Verantwortlichen/Auftragsverarbeiters
  - Überwachung der Einhaltung von Datenschutzvorschriften
  - Sensibilisierung und Schulung der Mitarbeiter überwachen
  - Beratung/Überwachung bei Datenschutz-Folgenabschätzungen
  - Kontaktstelle für Aufsichtsbehörde

## II. Spezielle Punkte

### 8. Benennung von Datenschutzbeauftragten

- g) Interne und externe Benennung grundsätzlich möglich
- h) Interessenkonflikte vermeiden (insbesondere keine Benennung von Personen mit Leitungsaufgaben im eigenen Unternehmen)
- i) Arbeitsrechtliche Vorgaben beachten (besonderer Kündigungsschutz)
- j) Benennung von Mitgliedern des Betriebsrats?

## II. Spezielle Punkte

### 9. Beschäftigtendatenschutz

Insbesondere **Betriebsvereinbarungen** müssen angemessene und besondere Maßnahmen umfassen zur Wahrung der

- menschlichen **Würde**
- berechtigten Interessen und Grundrechte der betroffenen Personen (vor allem bzgl. **Transparenz** der Verarbeitung/Datenübermittlung innerhalb Unternehmensgruppe)
- **Überwachungssysteme am Arbeitsplatz**

## II. Spezielle Punkte

### 9. Beschäftigtendatenschutz

- Es besteht **kein Konzernprivileg** (vgl. auch EG 48 DSGVO). Für Datenübermittlungen zwischen Konzernunternehmen müssen daher die Anforderungen der Art. 6 ff. DSGVO beachtet werden.
- **Einwilligungen** Beschäftigter im Arbeitsverhältnis sind grundsätzlich möglich, aber an hohe Anforderungen geknüpft (Information über Zwecke, Freiwilligkeit, Belehrung über Widerruflichkeit, Schriftform, vgl. auch § 26 Abs. 2 BDSG n.F.).

## II. Spezielle Punkte

### 9. Beschäftigtendatenschutz

§ 26 Abs. 1 Satz 1 BDSG-neu

„Personenbezogene Daten eines 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“.

## II. Spezielle Punkte

### 9. Beschäftigtendatenschutz

§ 26 Abs. 1 Satz 2 BDSG-neu

„Zur **Aufdeckung von Straftaten** dürfen personenbezogene Daten eines Beschäftigten nur dann verarbeitet werden, wenn **zu dokumentierende tatsächliche Anhaltspunkte** den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung **erforderlich** ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass **nicht unverhältnismäßig** sind.“

## II. Spezielle Punkte

### 10. Anwendung der DSGVO im internationalen Kontext

Die DSGVO wird angewendet auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen **nicht in der Union niedergelassenen** Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht,

- a) betroffenen Personen **in der Union Waren oder Dienstleistungen anbieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist,
- b) das **Verhalten betroffener Personen zu beobachten**, soweit ihr Verhalten in der Union erfolgt.

## III. Zusammenfassung

Ab 25.05.2018 gelten die DSGVO und das **BDSG-neu**.

Beachten Sie insbesondere folgende Fragestellungen:

- a) Werden die Grundsätze der Datenverarbeitung eingehalten und wird die **Rechenschaftspflicht** (Art. 5 Abs. 2 DSGVO) erfüllt?
- b) Können die **Rechte betroffener Personen** nach internen Mechanismen fristgemäß (Art. 12 Abs. 3 DSGVO) erfüllt werden?
- c) Wurden **Verträge zur Auftragsverarbeitung, Betriebsvereinbarungen sowie Einwilligungserklärungen** auf ihre Konformität mit den Anforderungen der DSGVO geprüft und ggf. angepasst?
- d) Werden die Anforderungen von **Sicherheit und Datenschutz technisch und organisatorisch** umgesetzt (Art. 32 und 25 DSGVO)?
- e) Gibt es interne Prozesse zur fristgemäßen **Erfüllung der Meldepflichten** bei Datenschutzverstößen (Art. 33 und 34 DSGVO)?

## Weitere Informationen

- Kurzpapiere zu vielen Themen der DSGVO
  - Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
  - Aufsichtsbefugnisse/Sanktionen
  - Verarbeitung personenbezogener Daten für Werbung
  - Datenübermittlung in Drittländer
  - Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
  - Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
  - Marktortprinzip – Regelungen für außereuropäische Unternehmen
  - Maßnahmenplan „DS-GVO“ für Unternehmen
  - Zertifizierung nach Art. 42 DS-GVO
  - Informationspflichten bei Dritt- und Direkterhebung
  - Recht auf Löschung / „Recht auf Vergessenwerden“
  - Datenschutzbeauftragter
  - Auftragsverarbeitung, Art. 28 DS-GVO
  - Beschäftigtendatenschutz
  - Videoüberwachung
  - Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO

• <https://www.datenschutzzentrum.de/dsgvo/>

• <https://www.datenschutzzentrum.de/plugin/tag/dsgvo>

• DSGVO+BDSG: <https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf>

