
LEXWARE
VOR ORT
Wir begrüßen Sie herzlich zu
Lexware vor Ort 2017

8 EU-Datenschutzgrundverordnung (DSGVO) und BDSG neu

Die wichtigsten Fakten in Kürze

Am 25.05.2018 tritt die DS-GVO in Kraft.
→ Ab diesem Datum ist sie unmittelbar geltendes Recht in allen EU-Staaten (Art. 99 DS-GVO).

Zielsetzung: **EU-weiter wirksamer Schutz personenbezogener Daten von natürlichen Personen**

Auswirkungen auf alle Unternehmensbereiche!

Massive Verschärfung des Sanktionsrahmens!

Noch keine Rechtsprechung!

Die Übergangsfrist ist jetzt!

Personenbezogene Daten
Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

Natürliche Person
Jeder lebende Mensch ist eine natürliche Person.

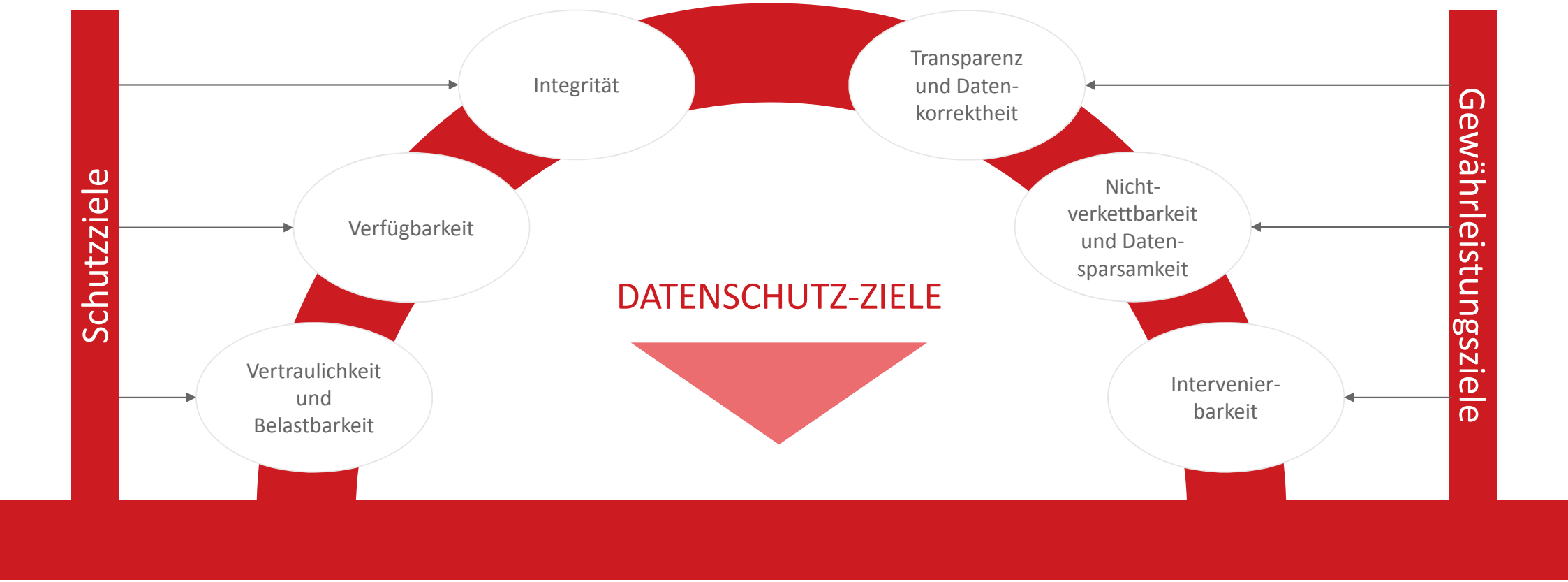
→ Angaben über juristische Personen und Personenmehrheiten (Personengesellschaften, Vereine, Gruppen) sind nicht DS-GVO-relevant.

Inhalte der DS-GVO

- Datenschutz-Ziele

Grundsatz der Datenschutzregelungen

Grundsätzlich ist **verboten, was nicht ausdrücklich erlaubt** wurde ("Verbot mit Erlaubnisvorbehalt").



Anforderungen der DS-GVO
- Gewährleistungsziel: Intervenierbarkeit

Technische Gestaltung von Verfahren zur Ausübung der Betroffenenrechte
Personenbezogene Verfahren benötigen Maßnahmen, die dem Betroffenen die Ausübung der im zustehenden Rechte wirksam ermöglichen.

- **Recht auf Löschung (Recht auf „Vergessen werden“)**
  → ad-hoc Löschfunktion bei berechtigen Anfragen von Betroffenen
- **Recht auf Datenübertragbarkeit**
  → Funktionen zur Bereitstellung der personenbezogenen Daten in maschinenlesbarem Format
- **Einwilligung**
  → Funktionen zur Einholung einer Einwilligung des Nutzers
- **Einwilligungsmanagement**
  → Bei CRM-Systemen: Nachweispflicht von Einwilligungen
- **Kontrollmöglichkeiten (privacy settings)**
- **Recht auf Einschränkung der Verarbeitung**
- **Recht auf Berichtigung**
- **Selbstständige Rechtewahrnehmung**

Anforderungen der DS-GVO
- Gewährleistungsziel: Nicht-Verkettbarkeit

Technische Absicherung der Zweckbindung
Ein Softwareprodukt darf personenbezogene Daten nur für den vorher bestimmten Zweck verarbeiten.

- **Funktionstrennung**
  → Angemessene Trennung von Funktionen im Rollenkonzept der Applikation
- **Mandantentrennung**
  → Trennung von Datenbeständen unterschiedlicher Mandanten
  → Trennung von personenbezogenen Daten unterschiedlicher Verwendungszwecke
  → möglichst bis zur Datenbank-Instanz
- **Profiling und Analytics**
  → Rechtmäßigkeit von Reporting-Funktionen
- **Übermittlung an Dritte**
- **Funktionalitätseinschränkungen**
- **Anonymisierung**

Anforderungen der DS-GVO
- Gewährleistungsziel: Datensparsamkeit

Die Verarbeitung personenbezogener Daten muss dem Zweck entsprechend **angemessen** und **erheblich** sowie auf das für die Zwecke der Verarbeitung **notwendige Maß beschränkt** sein.

- **Privacy by default**
  → Datenschutzfreundliche Voreinstellung des Produkts
- **Löschfristen und regelmäßige Löschung**
  → Definition/Umsetzung nah
- **Kennzeichnung von Pflichtfeldern**
- **Technische Einschränkungen**

Privacy by design	Privacy by default
Die Grundsätze des Datenschutzes sind **bei der Ausgestaltung der technischen Anwendung** bereits zu berücksichtigen. Art. 25 (1) DS-GVO	Bei den **Voreinstellungen der eingesetzten Systeme** sind die Grundsätze des Datenschutzes zu berücksichtigen. Art. 25 (2) DS-GVO

Anforderungen der DS-GVO
- Gewährleistungsziel: Transparenz und Datenkorrektheit

Die datenschutzrechtlichen Anforderungen müssen **für die betroffene Person nachvollziehbar** und **nachprüfbar** erfüllt werden. Die korrekte Eingabe von personenbezogenen Daten sollte unterstützt werden.

- **Informationspflicht**
  → Information zu Umfang und Zweck der Datenverarbeitung. Vor der Installation bzw. der Erhebung personenbezogener Daten
- **Recht auf Auskunft**
  → Funktionen zur Unterstützung von Auskunftsersuchen, insbesondere Identifikation des jeweiligen Datenbestandes
- **Plausibilität**
  → Einrichtung von Plausibilitätsprüfungen für Eingabefelder
- **„Rechtsbehelfsbelehrung“**
  → Transparente Information, Kommunikation und Modalitäten zur Ausübung der Betroffenenrechte
- **Produktbeschreibung**
  → Möglichkeit der Kenntnisnahme der Datenverarbeitung (Funktionsweise, Übermittlung, Speicherorte)

Anforderungen der DS-GVO - Schutzziel: Integrität

Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Das Softwareprodukt stellt über Kontrollen sicher, dass **keine unbefugten Änderungen von personenbezogenen Daten** durchgeführt werden.

- **Rollen- und Rechtekonzept**
  → Softwareseitige Möglichkeit zur Zuweisung spezifischer unwiderruflicher Rechte
- **Authentifizierung**
  → Zugriffskontrollverfahren, Einschränkung von Schreib- und Änderungsrechten
- **Prüfung und Kontrolle**
  → Integritätskontrollen bei Übertragung (Signaturen, Hashes), regelmäßige Integritätsprüfungen/Audits
- **Protokollierung**
  → von schreibenden/änderndern Zugriffen bzw. geänderten Daten

Anforderungen der DS-GVO - Schutzziel: Vertraulichkeit

Das Softwareprodukt stellt sicher, dass **personenbezogene Daten nur befugten Personen zugänglich** sind.

- **Rollen- und Rechtekonzept**
  → Softwareseitige Möglichkeit zur Zuweisung spezifischer unwiderruflicher Rechte
- **Verschlüsselung**
  → möglichst End-to-End-Verschlüsselung
- **Anonymisierung**
  → frühestmöglich
- **Verpflichtung von Mitarbeitern/Dienstleistern**
  → NDA (Vertraulichkeitsvereinbarung)
  → Verpflichtung auf Daten- und Telekommunikationsgeheimnis
- **Datentrennung**

Anforderungen der DS-GVO
- Schutzziel: Verfügbarkeit

Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

- **IT-Infrastruktur**
  → ausreichende Prozessor- und Speicherkapazitäten
  → Redundanz
  → spezielle Maßnahmen gegen Distributed-Denial-of-Service (DDoS) und Denial-of-Service (DoS)
  → Backup/Recovery

- **Ressourcenschonende Programmierung**

To-Dos für den Kunden

~~**Ist die DSGVO für mich relevant?**~~

→ Die DSGVO ist für jeden relevant, der mit personenbezogenen Daten zu tun hat.

To-Do 1: Die richtigen Fragen stellen!

Beispiele für richtige Fragen:

- Bietet unsere Software eine Möglichkeit, um personenbezogene Daten auf Anforderung zu löschen?
- Erlaubt es uns unsere Software, Personen Auskunft über ihre personengebundenen Daten zu geben?
- Speichern wir in unseren Systemen nur die notwendigen Daten und werden diese auch nicht länger als notwendig gespeichert?
- Können wir sicherstellen, dass die Daten nur für einen spezifischen Zweck gespeichert und nicht anderweitig genutzt werden?
- Sind unsere gespeicherten personenbezogenen Daten ausreichend gegen Missbrauch geschützt?
- …

To-Do 2: Prozesse und Tools auf den aktuellen Stand bringen!

Die aktuellen Lexware-Programme unterstützen ab dem Zwischen-Update 2018 datenschutzkonformes Arbeiten nach der DSGVO.

ToDos für den Kunden

ToDo 3: Erste Schritte auf dem Weg zu DSGVO-Konformität

- DSGVO-kompetente Datenschutzbeauftragte einsetzen
- Stammdatenverwaltung auf den neuesten Stand bringen
- Unstrukturierte Daten erfassen und analysieren (E-Mail, Dokumente, etc.)
- Data Mapping zur Identifikation von Datensätzen, ihrer Herkunft und Sensibilität
- Daten in Sicherheitsstufen klassifizieren und dies dokumentieren
- Alle Anwendungen und Ablagen systematisch abarbeiten
- Dokumentation der Verarbeitungsvorgänge anlegen
- Einwilligungserklärungen, AGBs, SLAs, etc. überprüfen
- Software installieren, die Angriffe und Datendiebstahl erkennt und das Notfallmanagement anschiebt
- Notfallmanagement/Desaster Recovery einführen, 72-Stunden-Meldefrist berücksichtigen
- Unerlaubten Datenfluss unterbinden
- Zweckgebundenheit der erhobenen Daten sicherstellen
- Informationsverpflichtung gegenüber den Datengebern nicht vergessen

Interessante Links und Tipps

Haufe-Lexware

- Datenschutzerklärung: https://shop.lexware.de/Datenschutz
- Artikel in Wissen & Tipps: …
- Online-Schulung zum Datenschutz: …

Trainings und Kurse der Haufe Akademie

- Haufe Compliance College – Datenschutz (e-Learning)
- Leitfaden Datenschutzmanagement nach der EU-DatenschutzgrundVO
- Die neue EU-Datenschutz-Grundverordnung und Big Data im Marketing
- Crashkurs Beschäftigtendatenschutz
- Cloud Computing in der Praxis

Externe Links

- Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
- DSK-Kurzpapiere zur DSGVO: https://www.lda.bayern.de/de/datenschutz_eu.html
- …

BDSG-Neu

Am 5. Juni 2017 wurde im Bundesgesetzblatt das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) kurz BDSG-Neu genannt veröffentlicht.

In den §§ 32 – 37 ist das „Recht auf Vergessenwerden“ geregelt.

Laut § 38 gilt: „… benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.“

In den §§ 41 – 43 sind die Bußgeld- und Strafvorschriften geregelt.

BDSG-neu.pdf

Kontaktdaten Ihres Lexware Gold-Partners

Kontaktdaten

Name	Steve Rückwardt
Firma	TAS | LEX-Partner.Net
Adresse	Kohlgartenstr. 24, 04315 Leipzig
Tel.	+49 180 5254210
bevorzugt:	
E-Mail	**info@lex-blog.de**
oder	**lex-blog.de/support**

Blog

lex-blog.de

Community

lex-forum.net

Twitter

twitter.com/lex_blog

YouTube

LexBlogTV.de

Facebook

facebook.com/lexblog


LEXWARE
VOR ORT
Danke für Ihre
Aufmerksamkeit