



EDV-Unternehmensberatung  
**Floß** GmbH

# EU Datenschutz- Grundverordnung

Das sollten Sie wissen!



# EU Datenschutz-Grundverordnung

Die EU Datenschutz-Grundverordnung (DS-GVO) ist bereits in Kraft getreten. Sie gilt ab dem 25.05.2018 in allen EU-Mitgliedstaaten. Ihre Ziele sind der einheitliche Schutz personenbezogener Daten und der freie Datenverkehr innerhalb des Europäischen Binnenmarktes. Die Einführung der DS-GVO verpflichtet Unternehmen, die bestehende Struktur in Bezug auf Datenschutz und Datensicherheit kritisch zu untersuchen und an

die Vorgaben der DS-GVO anzupassen. Das bringt für das Unternehmen neben vielen Pflichten auch große Vorteile. In der heutigen Zeit sind die gespeicherten Daten und die eingesetzte Informationstechnik äußerst wertvolle Teile des Unternehmens, die vor dem Zugriff Fremder oder internen Komplikationen geschützt werden müssen.



## Betroffenen-Rechte

### Herausforderung

**Die DS-GVO stärkt die Betroffenenrechte. Als Betroffene sind die Personen anzusehen, deren personenbezogene Daten (Name, Geburtsdatum, Kontodaten etc.) verarbeitet werden. Zum Zeitpunkt der Datenerhebung, spätestens aber nach einem Monat der Datenerhebung, ist dem Betroffenen schriftlich unter anderem mitzuteilen:**

- \* Zweck und Rechtsgrundlage der Verarbeitung
- \* Bestehen eines Rechts auf Widerspruch der Einwilligung
- \* Unterrichtung bei Übermittlung in ein Drittland

Weiterhin genießen die personenbezogenen Daten von Kindern und Jugendlichen einen besonderen Schutz.

### Umsetzung

**Sie haben Informationspflichten dem Betroffenen gegenüber: zum Beispiel, wenn Sie Daten des Betroffenen erfassen und über den Zweck der Erfassung. Des Weiteren ist zu beachten, dass der Betroffene z.B. Auskunfts- oder Widerspruchsrechte hat, auf die Sie eingehen müssen.**

**Um die Rechte der Betroffenen einzuhalten, sind z.B. folgende Schritte notwendig:**

- \* Umsetzung des Auskunftsrechts der Betroffenen
- \* Einrichtung von Werbesperren
- \* Etablierung von Prozessen zur Meldung von Verstößen





# Einwilligung

## Herausforderung

**Es ist grundsätzlich verboten, personenbezogene Daten ohne Rechtsgrundlage oder Erlaubnis des Betroffenen zu verarbeiten. Durch die DS-GVO verschärfen sich die Anforderungen an eine wirksame Einwilligungserklärung, die im Wesentlichen aus drei Voraussetzungen bestehen:**

- \* Beachtung formaler Vorgaben
- \* Informiertheit des Betroffenen
- \* Freiwilligkeit der Einwilligungen des Betroffenen

**Die wichtigsten Anforderungen an eine rechtsgültige Einwilligung sind:**

- \* die freie Entscheidung des Betroffenen
- \* klare und eindeutige Zweckangabe der Verarbeitung
- \* Nachweis der Einwilligungserklärung
- \* Widerruflichkeit der Einwilligungserklärung

## Umsetzung

**Um alle Einwilligungen korrekt vorliegen zu haben, sind folgende Schritte erforderlich:**

- \* Überprüfung der zu verarbeitenden Daten & Prozesse
- \* Überprüfung sämtlicher bestehender Einwilligungen (inkl. online eingeholter Einwilligungen) und ggf. Neueinholung

**Die Erhebung personenbezogener Daten von Minderjährigen bei Onlinebestellungen unterliegt besonderen Prozessen. Hier ist insbesondere zu prüfen/sicherzustellen:**

- \* ob die Einwilligung der/des Erziehungsberechtigten vorliegt
- \* dass die Einwilligung der/des Erziehungsberechtigten unter Berücksichtigung der verfügbaren Technik (z.B. Postident) eingeholt wird



# Datenschutz-Folgenabschätzung

**Bei einem hohen Datenschutzrisiko muss eine Folgenabschätzung durchgeführt werden. Dies gilt z.B. IMMER bei:**

- \* Scoring
- \* Profiling
- \* Videoüberwachung

Um mögliche Risiken für den Betroffenen erkennen zu können, müsse alle Verfahren und Prozesse mit personenbezogenen Daten betrachtet werden. Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung immer den Rat des Datenschutzbeauftragten ein.



## \*\*\*\* Technik

### Herausforderung

„Privacy by Design“ („Datenschutz durch Technikgestaltung“) und „Privacy by Default“ („Datenschutz durch Voreinstellung“) sollen sicherstellen, dass Datenschutz und Privatsphäre schon in der Entwicklung von Technik beachtet werden.

- \* die gesamte Technik ist auf einem entsprechenden Stand zu halten bzw. zu bringen
- \* Ziel ist das Erreichen eines möglichst hohen Schutzniveaus

### Umsetzung

Datenschutz muss künftig schon beim Design und bei der Implementierung eines Systems berücksichtigt werden. Folgende Aspekte müssen dabei von den verantwortlichen Stellen umgesetzt werden:

- \* regelmäßige Durchführung von Audits
- \* Stichprobenkontrollen
- \* Risikoanalysen
- \* Schulung der Mitarbeiter
- \* Dokumentation aller Vorgänge
- \* regelmäßige Penetration-Tests



## Auftragsverarbeitung

### Herausforderung

Einige Dinge ändern sich bei den Verträgen zur Auftragsverarbeitung (früher: Auftragsdatenverarbeitung). Besonders zu beachten sind:

- \* gemeinsame Haftung für Auftraggeber und Auftragnehmer
- \* Datenverarbeitung außerhalb der EU
- \* Pflicht zur Führung von Verzeichnissen

### Umsetzung

Zur Umsetzung der neuen Auftragsverarbeitungsrichtlinien sind folgende Schritte notwendig:

- \* Prüfung von vorhandenen Auftragsverarbeitungs-Verträgen bzw.
- \* Auftragsverarbeitungs-Verträge abschließen, wenn noch keine vorhanden sind
- \* mit neuen Dienstleistern rechtzeitig Auftragsverarbeitungs-Verträge abschließen und die Verarbeitung überprüfen



## Onlinepräsenz

### Herausforderung

Eine Website ist nicht nur Ihre Visitenkarte im Internet. Ein unvollständiges Impressum oder eine fehlerhafte Datenschutzerklärung können aufgrund der DS-GVO künftig hohe Bußgelder nach sich ziehen.

### Umsetzung

Folgende Schritte sind erforderlich, um Ihre Onlinepräsenz auf Vordermann zu bringen:

- \* Überprüfen der Datenschutzerklärung bzw. des Impressums hinsichtlich der Vorgaben der DS-GVO
- \* Überprüfen aller Einwilligungen und eventuell neue Einholung
- \* verschlüsselter Datenverkehr (https)



## Sanktionen

**Bei Verstößen gegen die DS-GVO bzw. das neue BDSG-E können von den Landes-Aufsichtsbehörden empfindliche Geldstrafen festgesetzt werden.**

\* Erhöhung der Bußgelder auf bis zu 20 Mio. € bzw. 4 % des Jahresumsatzes

Gemäß dem Wortlaut der DS-GVO müssen die Sanktionen „wirksam, verhältnismäßig und abschreckend“ sein.

\* **Vorstellbar sind Strafen in Höhe von bis zu drei Jahresgewinnen!**



## Betrieblicher Datenschutzbeauftragter

### Herausforderung

**Laut derzeitigem Entwurf für das neue BDSG, das durch die Öffnungsklauseln als Ergänzung der DS-GVO möglich ist, wird folgende Regelung beibehalten:**

**Ab 10 Personen, die Zugang zu personenbezogenen Daten haben, ist ein fachkundiger Datenschutzbeauftragter intern oder extern zu bestellen.**

Doch auch diejenigen, die von dieser Regelung nicht betroffen sind, sind selbstverständlich nicht davon befreit, einen gesetzeskonformen Datenschutz einzuführen.

### Umsetzung

**Gerne sind wir in diesem Bereich für Sie tätig!**

Wir bieten Ihnen:

- \* fachgerechte Unterstützung bei der Umsetzung der DS-GVO
- \* Bestellung als externer Datenschutzbeauftragter
- \* Schulung und Sensibilisierung von Management und Mitarbeitern
- \* Bestandsaufnahme des Ist-Zustands in den Bereichen Datenschutz und Datensicherheit und Erstellung eines Maßnahmenplans
- \* Unterstützung bei der Erfassung von Verzeichnissen
- \* Durchführung von Penetration-Tests
- \* Datenschutz-Audits

**Fordern Sie Ihr individuelles Angebot bei uns an!**



EDV-Unternehmensberatung  
**Floß GmbH**

## Risk-Management für IT & Daten

**Die EDV-Unternehmensberatung Floß GmbH ist eine Spezialdienstleisterin für das Risikomanagement im Bereich der IT/Elektronischen Datenverarbeitung. Wir arbeiten für Unternehmen und Institutionen aller Art und Größe, für Gerichte und Staatsanwaltschaften ebenso wie für Versicherungen.**

Hierzu zählen Einsätze als externer respektive unabhängiger

- ✦ EDV-Sachverständiger und Forensiker (punktuell)
- ✦ Datenschutzbeauftragter (extern)
- ✦ IT-Compliance Manager (extern)
- ✦ IT-Sicherheitsbeauftragter (dauerhaft und punktuell)
- ✦ IT-Supervisor (Projekt- oder Unternehmensbezogen)

[www.floss-consult.de](http://www.floss-consult.de)

EDV-Unternehmensberatung Floß GmbH  
Parkstr. 1a · 33775 Versmold  
Telefon 05423 964900 · [info@floss-consult.de](mailto:info@floss-consult.de)