

# EU – Datenschutz-Grundverordnung



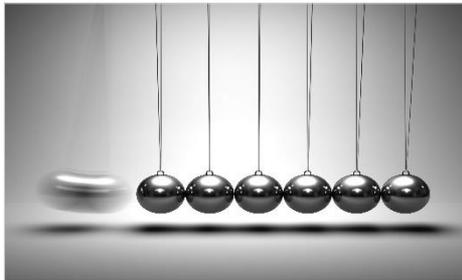
Überblick



Rechte der betroffenen Person



Pflichten der Organisation



Verfahrensverzeichnis



Datenschutzbeauftragter



Umsetzung im Verein

# EU-Datenschutzgrundverordnung (EU-DSGVO)

## Zeitplan



Die [Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr](#) ist eine 1995 erlassene Richtlinie der Europäischen Gemeinschaft zum Schutz der Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten.

Sie wird durch die am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlichte [Datenschutz-Grundverordnung \(EU-DSGVO\)](#) (offizielle Bezeichnung: "Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG") am 25. Mai 2018 abgelöst werden.

**Die Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.** (Art. 1 DSGVO Abs. 1)

# Grundsätze der Datenverarbeitung

## Nach Artikel 5 DSGVO



- **Rechtmäßigkeit, Treu und Glauben, Transparenz** in einer für die betroffene Person nachvollziehbaren Weise
- **Zweckbindung** für festgelegte, eindeutige und legitime Zwecke (auch für statistische oder wissenschaftliche Zwecke)
- **Datenminimierung** auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt
- **Richtigkeit** sachlich richtig und erforderlichenfalls auf dem neuesten Stand, unrichtige Daten sind zu löschen oder zu berichtigen
- **Speicherbegrenzung** Speicherung nur so lange, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist
- **Integrität und Vertraulichkeit** Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung
- **Rechenschaftspflicht** über die Einhaltung der Vorschriften

# Rechtmäßigkeit der Verarbeitung

## Nach Artikel 6 DSGVO



- **Einwilligung der betroffenen Person** für einen oder mehrere bestimmte Zwecke
- **Vertragliche Vereinbarung** zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen
- **Rechtliche Verpflichtungen**
- **Lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person
- **Öffentliche Interessen** oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde
- **Berechtigte Interessen des Verantwortlichen**, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere, wenn es sich um ein Kind handelt.
- **EU-Mitgliedstaaten** können spezifischere Bestimmungen erlassen

# Bedingungen für die Einwilligung

Nach Artikel 7 und 8 DSGVO



- **Einwilligung einer Person** muss nachgewiesen werden können
- **Einwilligung durch eine schriftliche Erklärung** muss „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ erfolgen, andernfalls sind diese Teile der Einwilligung nicht verbindlich!
- **Recht auf Widerruf**, der jederzeit erfolgen kann und so einfach wie die Erteilung der Einwilligung formuliert sein muss. Bis zum Zeitpunkt des Widerrufs bleibt die Rechtmäßigkeit der Einwilligung erhalten
- **Kinder** die das sechzehnte Lebensjahr vollendet haben, können ihre Einwilligung selbst erteilen. Bei Kindern, die das sechzehnte Lebensjahr nicht vollendet haben, muss die Einwilligung durch den Träger der elterlichen Verantwortung erfolgen. EU-Mitgliedstaaten können die Altersgrenze maximal bis auf 13 Jahre senken. Es sollen „angemessene Anstrengungen“ unternommen werden, um sich zu vergewissern, dass die Einwilligung mit der Zustimmung des Kindes erteilt wurde.

# Rechte der betroffenen Person

## Nach Artikel 12 bis 23 DSGVO



- **Transparente Information** über alle personenbezogene Daten in präziser, transparenter und leicht zugänglicher Form [Art. 12]
- **Informationspflicht** bei Datenerhebung mit Ansprechpartner, Datenschutzbeauftragter, Zweck, Rechtsgrundlage etc. [Art. 13]
- **Auskunftsrecht** über gespeicherte Daten, Verarbeitungszwecke, Datenempfänger, Dauer der Speicherung etc. [Art. 16]
- **Recht auf Berichtigung** [Art. 16]
- **Recht auf Löschung** („Recht auf Vergessenwerden“) [Art. 17]
- **Recht auf Einschränkung der Verarbeitung** bei Zweifel an der Korrektheit für die Dauer der Überprüfung [Art. 18]
- **Mitteilungspflicht** nach Löschung oder Einschränkung [Art. 19]
- **Recht auf Datenübertragbarkeit** sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt [Art. 20]

# Pflichten der Organisation

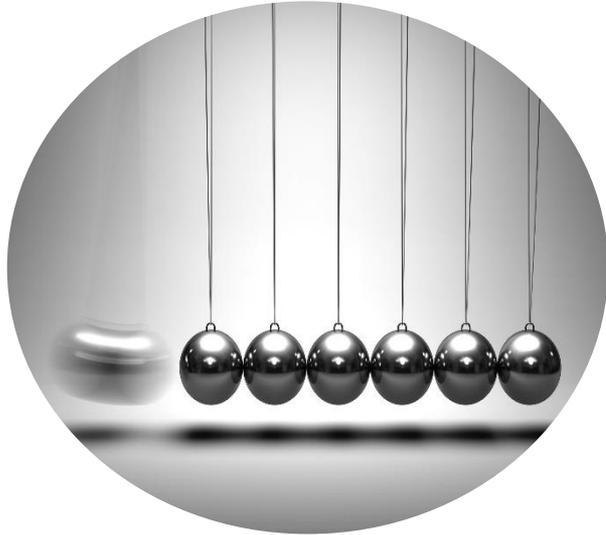
## Nach Artikel 24 bis 43 DSGVO



- **Verantwortlicher Umgang mit den Daten** [Art. 24-25]
- **Mehrere Verantwortliche** müssen in einer Vereinbarung in transparenter Form festlegen, wer welche Verpflichtung erfüllt [Art. 26]
- **Datenverarbeitung durch Auftragsverarbeiter** müssen Garantien für geeignete technische und organisatorische Maßnahmen bieten, dass die Rechte der betroffenen Personen gewährleistet sind [Art. 28]
- **Verzeichnis von Verarbeitungstätigkeiten** u.a. mit Kontaktperson, Zweck, Kategorien von Personendaten, Empfänger etc. **bei mehr als 250 Mitarbeitern oder „nicht nur gelegentlicher Verarbeitung“** [Art. 30]
- **Sicherheit der Verarbeitung** durch geeignete Techniken und Vorgehensweisen hinsichtlich Verschlüsselung, Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Recovery etc. [Art. 32]
- **Meldung von Verletzungen** an die Aufsichtsbehörde [Art. 33]
- **Benennung eines Datenschutzbeauftragten** [Art. 34]

# Verfahrensverzeichnis

## Dokumentation von Verarbeitungstätigkeiten



- **Verfahrensverzeichnis** Jeder Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen.
  - Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten
  - die Zwecke der Verarbeitung
  - Beschreibung der Kategorien betroffener Personen
  - Beschreibung der Kategorien personenbezogener Daten
  - Kategorien von Empfängern, denen personenbezogene Daten offengelegt werden
  - vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
  - technische und organisatorische Maßnahmen zur Datensicherheit nach Art. 32
  - Risiken bei Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung

# Der Datenschutzbeauftragte

## Vermittler im Innenverhältnis und nach außen



Wenn mindestens 10 Personen im Verein ständig mit der Verarbeitung von Daten betraut sind, muss ein Datenschutzbeauftragter benannt werden.

- Beratung der Verantwortlichen
- Überwachung der Einhaltung der Verordnung
- Sensibilisierung und Schulung
- Dokumentation des Umgangs mit Daten
- Zusammenarbeit mit der Aufsichtsbehörde

# Maßnahmen für der Verein (1)

## Verbindlich oder freiwillig



- **Ergreifen technischer und organisatorischer Maßnahmen** um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, z. Bsp. durch Regelungen der Zugangskontrolle und des Passwortschutzes bis hin zu Anweisungen bezüglich der Löschung von Daten.
- **Erstellen von Verarbeitungsverzeichnissen** Es kann sinnvoll sein, freiwillig ein Verzeichnis der Verarbeitungstätigkeiten anzulegen, um die Datenverarbeitung innerhalb des Vereins transparent zu machen.
- **Benennung eines Datenschutzbeauftragten** der nicht nur die Einhaltung der datenschutzrechtlichen Bestimmungen kontrolliert, sondern den Vorstand und die Mitarbeiter/innen im Umgang mit personenbezogenen Daten unterstützt und berät.
- **Aufnahme einer Datenschutzklausel in die Satzung** des Vereins um den Informationspflichten gemäß Artikel 13 der DS-GVO – zumindest teilweise – zu entsprechen.

# Maßnahmen für der Verein (2)

## Verbindlich oder freiwillig



- **Erstellen einer Datenschutzordnung** in der festgeschrieben wird, welche Daten erhoben und verarbeitet werden, wer Zugriff auf welche Daten hat und welche technischen Maßnahmen ergriffen werden. (Die Regelungen sollten sich an das Verzeichnis anlehnen.)
- **Verpflichtung der Mitarbeiter auf das Datengeheimnis** Die Verpflichtungserklärung sensibilisiert die Mitarbeiter im Umgang mit den personenbezogenen Daten und gewährleistet die Regressmöglichkeit, wenn Mitarbeiter das Datengeheimnis verletzen.
- **Erstellen von Datenschutzerklärungen** Bei Besuch von Internetseiten sind sie bereits vertraut, aber auch in der analogen Welt halten sie Einzug, um den Informationspflichten bei der Erhebung und Verarbeitung von Daten gerecht zu werden.
- **Informationspflichten** Personen, deren Daten Sie verarbeiten, müssen umfangreich informiert werden. Sofern diese Informationen noch nicht zur Verfügung gestellt wurden, muss dies aktiv durch den Verein vor dem 25.5.2018 erfolgen.

# Maßnahmen für der Verein (3)

## Verbindlich oder freiwillig



- **Einwilligungserklärungen** Die DSGVO gibt detaillierte Regelungen zu Einwilligungserklärungen der Personen vor, deren Daten Sie verarbeiten. Insbesondere muss dies eine „unmissverständlich abgegebene Willensbekundung“, bzw. „eine eindeutig bestätigende Handlung“ sein. Die Formulierung muss „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ erfolgen. Auch bereits vorliegende Einwilligungserklärungen müssen geprüft werden, ob sie noch den neuen Anforderungen entsprechen.
- **Meldepflicht bei Datenschutzpannen** Kommt es zu Verletzungen des Schutzes personenbezogener Daten und ist dies mit einem Risiko für die Rechte und Freiheiten von Betroffenen verbunden, dann hat der Verantwortliche unverzüglich möglichst binnen 72 Stunden die Aufsichtsbehörde und unter Umständen auch die betroffene Person zu benachrichtigen. Jeder Verein sollte im Vorfeld einen Prozess, ein Muster für die Meldung und die zuständige Person bestimmen. Mindestinhalte der Meldung sind in Art 33 Abs. 3 DSGVO geregelt.

# EU – Datenschutz- Grundverordnung (EU-DSGVO)

## Quellenangaben

- Internet

<https://dsgvo-gesetz.de/>

<https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/>

<http://www.vibss.de/vereinsmanagement/recht/datenschutz-und-internetrecht/eu-datenschutz-grundverordnung-dsgvo/>

<https://www.bdolegal.de/de-de/einblicke/aktuelles/2018/auch-fur-vereine-lauft-die-umsetzungsfrist-fur-die-eu-datenschutz-grundverordnung>

- Fortbildungsseminar des LSVS

Die neue Datenschutz Grundverordnung  
Referent: Patrick Nessler

28.4.2018

9:00 – 13:00 Uhr