



# DATENSCHUTZRECHT AKTUELL

INFORMATIONEN, EMPFEHLUNGEN und PRAXISTIPPS für Chorverbände und Chöre

## NEUE RECHTSLAGE AB 25. MAI 2018

Aufgrund der EU-Datenschutzgrundverordnung (kurz: DSGVO) werden alle Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen EU-weit vereinheitlicht. Die DSGVO und das daraus resultierende österreichische Datenschutz-Anpassungsgesetz 2018 verschärfen bzw. verändern somit den Umgang mit personenbezogenen Daten.

## GRUNDSÄTZLICHE INFORMATIONEN<sup>1</sup>

### REGELUNGSINHALT UND DEFINITIONEN:

Es geht um die Verarbeitung von „personenbezogenen Daten“ (z.B. durch Chorverbände oder Chöre), wobei Pflichten für die Verantwortlichen festgelegt sind sowie Rechte der Personen, deren Daten verarbeitet werden, eingeräumt werden. Gesetzlich werden folgende Begriffe bzw. Funktionen unterschieden:

#### Verantwortlicher

ist eine Person oder Institution, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet – z.B. *Präsident/in eines Chorverbands, Obmann/frau eines Chors.*

#### Auftragsverarbeiter

ist eine Person oder Einrichtung, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet – z.B. *Assistent/in im Büro des Chorverbands, Schriftführer/in eines Chors.*

#### Betroffener

ist jene Person, deren Daten erhoben bzw. verarbeitet werden – z.B. *Obmann eines Mitgliedschors im Chorverband, Sänger/in im Chor.*

### Personenbezogene Daten

sind jene Daten, die sich eindeutig auf eine bestimmte Person beziehen oder die einer Person zugeordnet werden können – z.B. *Name, Geburtsdatum, Geschlecht, Adresse, email-Adresse, Sozialversicherungsnummer, Telefonnummer, Bankdaten, Bild- oder Tonaufnahmen, technische Daten wie IP-Adresse / Geräteerkennung / Standortdaten.*

### Sensible Daten

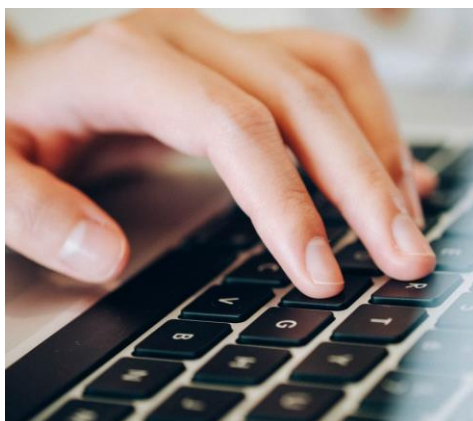
sind besondere personenbezogene Daten, die einem höheren Schutz unterliegen – z.B. *Religionszugehörigkeit, politische Überzeugung, Gewerkschaftszugehörigkeit, Krankengeschichte.*

### Verarbeitung von Daten

ist jeder (mit oder ohne Hilfe automatisierter Verfahren, d.h. digital und analog) ausgeführter Vorgang, der mit personenbezogenen Daten zu tun hat – z.B. *Erheben, Erfassen, Organisieren, Ordnen, Speichern, Verändern, Abfragen, Offenlegen, Verbreiten, Verknüpfen, Löschen und Vernichtung von Daten.*

**Ausnahme:** Die Verarbeitung sensibler Daten (als Sonderform personenbezogener Daten) ist untersagt und bedarf in der Regel immer der Einwilligung der/des Betroffenen.

<sup>1</sup> Dies ist eine spezifische Zusammenstellung für Chorverbände und Chöre, die folgende Informationsquellen einbezieht: anwaltliche Auskünfte, juristische Fachartikel, spezifische Websites und dem Autor aus Fachgesprächen bekannte Informationen.



Quelle: <https://pxhere.com/de/photo/714530> [23.04.2018]

## Rechte der Betroffenen:

Die betroffenen Personen haben Recht auf

- Auskunft
- Berichtigung
- Löschung und Vergessenwerden
- Widerspruch
- Einschränkung der Verarbeitung
- Datenübertragbarkeit

## GRUNDSÄTZE BEI DER DATENVERARBEITUNG:

Personenbezogene Daten dürfen nur verarbeitet werden, wenn folgende Grundsätze eingehalten werden:

### **Rechtmäßigkeit:**

Eine Verarbeitung ist rechtmäßig, wenn insbesondere

- eine rechtliche Verpflichtung vorliegt (z.B. Vereinsstatuten, Meldung an Vereinsbehörde),
- dies für die Erfüllung eines Vertrags notwendig ist (z.B. AKM-Vertrag, mündlich abgeschlossene Verträge),
- die betroffene Person in die Verarbeitung eingewilligt (in Form einer Erklärung oder bestätigenden Handlung, nachweislich, für einen bestimmten Fall) hat.

### **Zweckbindung:**

Die Datenverarbeitung darf nur für festgelegte, eindeutige und legitime Zwecke erfolgen, die bereits bei der Erhebung von Daten anzugeben sind.

### **Datenminimierung:**

Anzahl und Umfang der Daten muss auf das für den Zweck notwendige Maß beschränkt sein – „Weniger ist mehr!“

### **Richtigkeit:**

Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein, d.h. unrichtige Daten müssen gelöscht werden.

### **Speicherbegrenzung:**

Die Identifizierung einer Person darf nur so lange möglich sein, als es der Zweck der Datenverarbeitung erfordert. Werden Daten nicht mehr benötigt, sind diese zu löschen.

### **Transparenz:**

Für jede betroffene Person soll nachvollziehbar sein, ob und welche personenbezogenen Daten über sie erhoben wurden.

### **Integrität und Vertraulichkeit:**

Personenbezogene Daten müssen auf sichere Weise verarbeitet werden, sodass unbefugte oder unrechtmäßige Verarbeitung, Manipulation oder Schädigung verhindert wird.



## EMPFEHLUNGEN zur UMSETZUNG

Zur Umsetzung werden folgende Maßnahmen empfohlen, wobei zu berücksichtigen ist, dass jeder Chorverband bzw. jeder Chor bereits Datenverarbeitungen betreibt.

### 1. Evaluierung des Ist-Zustands

- 1.1. Werden alle Daten rechtmäßig verarbeitet? -> **Rechtmäßigkeit, Einwilligung**
- 1.2. Sind alle Daten notwendig, um einen berechtigten Zweck zu erfüllen? -> **Datenminimierung**
- 1.3. Sind alle Verarbeitungsvorgänge notwendig? -> **Zweckbindung**
- 1.4. Sind alle Daten richtig? -> **Richtigkeit, Speicherbegrenzung**
- 1.5. Sind alle notwendigen Sicherungsmaßnahmen verwirklicht? -> **Integrität**

### 2. Umsetzung der DSGVO

Dabei gelten für die Verantwortlichen folgende Pflichten:

#### a. Prinzip der Selbstverantwortlichkeit:

- Die Verantwortlichen sind für die Einhaltung selbst verantwortlich!
- Es gibt keine (Vorab-)Genehmigungen durch staatliche Stellen.
- Bei Nichteinhaltung drohen gravierende finanzielle Sanktionen.

#### b. Prinzip der Rechenschaftspflicht („Accountability“):

Die Verantwortlichen müssen die Erfüllung der datenschutzrechtlichen Pflichten nachweisen können.

#### 2.1. Festlegung der Verantwortlichkeit für Datenschutz:

Konkrete Zuständigkeit klären und nachweislich festlegen, Funktionär/innen und Mitarbeiter/innen sensibilisieren.

- ▶ *Welche/r Funktionär/in ist Verantwortliche/r?*
- ▶ *Wer ist interner Auftragsverarbeiter?*

#### 2.2. Erarbeitung eines detaillierten Verarbeitungsverzeichnisses:

Folgende Informationen sind für jeden Verarbeitungsprozess einheitlich und nachvollziehbar zu erfassen: Art der Daten, Verarbeitungszwecke, Gruppe betroffener Personen, Art und Ort der Datenverarbeitung, Beginn der Datenverarbeitung, Rechtsgrundlage für die Rechtmäßigkeit, Speicherort, Sicherheitsmaßnahmen, Zugriffsrecht welcher Personen, Datenweitergabe, (vorgesehene) Löschrufen.

- ▶ *Anlegen in einer Excel-Tabelle oder in einer speziellen Software.*



### 2.3. Sicherung der Rechtmäßigkeit der Datenverarbeitung:

Umfangreiche Information an die Betroffenen über die Datenverarbeitung (vgl. 2.2.), allfällig fehlende Einwilligungen einholen.

- ▶ *Mail mit Informationen über die Datenverarbeitung an die Betroffenen.*
- ▶ *Die Einwilligung der jeweiligen Person muss im Anlassfall vom Verantwortlichen nachgewiesen werden.*
- ▶ *Liegt bereits eine (rechtmäßige) Einwilligung vor, ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt.*
- ▶ *Wenn es bisher jedoch keine Einwilligung der betroffenen Person gegeben hat, so ist diese nachzuholen. Es bedarf einer e-mail-Bestätigung, einer anzukreuzenden Check- bzw. Tickbox oder einer anderen nachweislichen Bestätigung der Betroffenen. Schweigen als Zustimmung ist zu wenig.*
- ▶ *Für die Verwendung der Daten im üblichen Umfang des Vereinszwecks eines Chors (Proben, Konzerte, Aktivitäten...) gilt der Beitritt mit der Abgabe der Daten als Einwilligung.*
- ▶ *Für Kinder und Jugendliche bis inkl. 16 Jahre müssen die Erziehungsberechtigten die Einwilligung geben.*

### 2.4. Sicherstellung der Datensicherheit:

IT-Systeme überprüfen (Berechtigungen, Sicherheitslücken, Protokollierung, Aktualität, Backup etc.), Websites überprüfen (Impressum, Cookies-Zustimmung, etc.).

- ▶ *Die Daten müssen am Computer geschützt werden mittels Verschlüsselung, Passwortsicherung, regelmäßiger Änderung der Passwörter, Sperre des Computers bei (auch kurzer) Abwesenheit vom Platz etc.*

### 2.5. Festlegung der Löschfristen:

Technische Einrichtung und organisatorische Maßnahmen vorsehen, um nicht benötigte Daten immer wieder zu löschen.

- ▶ *Es muss regelmäßig evaluiert werden, ob der Umfang der gespeicherten Daten für die jeweiligen Tätigkeiten noch erforderlich ist.*

### 2.6. Abschluss von Verträgen mit externen Auftragsverarbeitern:

Vertrag zur Nutzung der Daten bzw. Datenverarbeitung mit externen Auftragsverarbeitern abschließen.

- ▶ *Für die Weitergabe der Daten an Dachverbände (z.B. Landeschorverband) muss ein Datenverarbeitungsvertrag für die Weitergabe gewisser Daten vereinbart werden, wenn nicht die jeweiligen Statuten die Rechtmäßigkeit absichern.*

### 2.7. Einrichtung eines Prozesses zur Wahrung der Rechte der Betroffenen:

Sichere und effiziente Möglichkeit der Datenauskunft/Berichtigung/Löschung/Übertragbarkeit...

- ▶ *Betroffene Personen können u. a. Auskunft über ihre Daten verlangen, was innerhalb eines Monats erfolgen muss.*

### 2.8. Einrichtung eines Prozesses im Falle einer Verletzung des Datenschutzes:

Umfassende und zeitgerechte (innerhalb 72 Stunden!) Meldung an die Behörde und die Betroffenen.



## PRAXISTIPPS

- ▶ Es wird empfohlen, nur solche personenbezogene Daten zu verarbeiten, die zur Mitgliederbetreuung und -verwaltung sowie zum Verfolgen des Vereinsziels laut Statuten notwendig sind.
- ▶ Die DSGVO normiert, dass bereits bestehende Datenverarbeitungen ab dem 25. Mai 2018 „DSGVO-konform“ zu sein haben. Wenn somit Daten vor dem 25. Mai 2018 rechtmäßig erhoben wurden, müssen sie nach dem 25. Mai 2018 nicht gelöscht werden, sie dürfen aber nur nach Maßgabe der neuen Bestimmungen verarbeitet werden.
- ▶ Die bisherige DVR-Nummer, die mit der Registrierung eines Vereins vergeben wurde, ist ab 25. Mai 2018 gegenstandslos. Daher ist die DVR-Nummer bei Sendungen nicht mehr anzuführen.
- ▶ Beim Versenden von E-Mails ist stets auf die richtigen Empfänger/innen zu achten. Bei Massenmails, wie z. B. Konzert- oder Veranstaltungseinladungen, ist das BC-Feld für die konkreten Adressen zu verwenden.
- ▶ Die Verarbeitung funktionsbezogener Daten – z.B. Name oder vereinsbezogene email-Adresse einer Funktionärin/eines Funktionärs – bedarf keiner gesonderten Einwilligung, da sie unmittelbar mit dem Vereinszweck zusammenhängen. Dies gilt auch für Ergebnisse von Wahlen.
- ▶ Die Veröffentlichung von personenbezogenen Daten auf Websites oder facebook setzt eine explizite Einwilligung der betroffenen Personen voraus. Dies gilt nicht für funktionsbezogene Daten oder Ergebnisse von Wahlen.
- ▶ Fotos oder Videos aus dem Vereinsleben dürfen erst nach Einwilligung der abgebildeten Personen auf Websites oder in Zeitungen veröffentlicht werden. Dies gilt nicht, wenn lediglich Menschenansammlungen abgebildet sind, bei denen keine Einzelpersonen erkennbar sind.
- ▶ Es ist zu beachten, dass durch die Inanspruchnahme von Cloud-Services eine Datenübermittlung in ein Drittland stattfinden kann, für die es eine gesonderte Rechtsgrundlage für den abzuschließenden Datenverarbeitungsvertrag braucht (z.B. Standardvertragsklauseln der EU).
- ▶ Wenn eine Website Cookies auf dem Computer der Benutzer/innen speichert (was bei fast allen Websites der Fall ist), müssen Benutzer/innen beim Einstieg auf die Website explizit darauf hingewiesen werden.
- ▶ Für die Löschung von personenbezogenen Daten in digitaler Form reicht die gängige Löschfunktion von Betriebssystemen meist nicht aus, da die Daten lediglich als gelöscht markiert werden. Für die vollständige Datenlöschung wird meistens eine eigene Software benötigt.
- ▶ Dokumente in Papierform, die personenbezogene Daten enthalten, sollten keinesfalls mit dem normalen Papiermüll entsorgt werden – diese gehören unbedingt geschreddert.

## WEITERFÜHRENDE LINKS

*„Je weniger Daten und je kürzer man sie speichert, desto geringer ist das Risiko, den Datenschutz zu verletzen. Datenschutz muss von allen Personen im Alltag gelebt werden!“*

*DDr. Karl-Gerhard Straßl MAS  
Präsident  
Chorverband Österreich*



Quelle: <https://pxhere.com/de/photo/536212> [23.04.2018]

Unter folgenden Links sind empfehlenswerte Materialien und Erläuterungen zur Datenschutzgrundverordnung (Stand: 16.04.2018) zu finden:

### **Datenschutzgrundverordnung:**

[http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L\\_.2016.119.01.0001.01.DE.U&toc=OJ%3AL%3A2016%3A119%3ATOC](http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DE.U&toc=OJ%3AL%3A2016%3A119%3ATOC)

### **Leitfaden Datenschutzbehörde:**

<https://www.dsb.gv.at/documents/22758/116802/DSGVO-2016-Leitfaden.pdf/93d6cb80-8d8e-433d-a492-a827e3ed81a2>

### **Informationen der Bundessportorganisation:**

<http://www.bso.or.at/de/schwerpunkte/mitgliederservice/information-und-download/rechtsinformationen/datenschutzgrundverordnung/>

### **Informationen der WKO:**

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html>

### **Empfohlener Experte für datenschutzrechtliche Spezial- und Haftungsfragen:**

<http://www.rechtsmanufaktur.at/>

Erstellt von: DDr. Karl-Gerhard Straßl MAS, Stand: 20. April 2018