**Datenschutz-Konzept
(Ausbildungs-) Verein für Psychotherapeuten**
gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

Logo/Schriftzug

Verein
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
ZVR-Zahl des Vereins gemäß § 18 Abs. 3 VG: ……………...

 **Verantwortliche gemäß DSGVO
Titel/Name
Obfrau/mann
gemäß Statuten**

Adresse
Tel
Email

**Wenn fertig, bitte** **Inhaltsverzeichnis neu erstellen.**

Inhaltsverzeichnis

[1 Allgemeine Angaben 4](#__RefHeading___Toc25509_501753674)

[1.1 Datenschutz-Konzept 4](#__RefHeading___Toc12320_3966647769)

[1.2 Sachliche und räumliche Tätigkeit 4](#__RefHeading___Toc12322_3966647769)

[1.3 Datenschutzbeauftragter (DSB) 4](#__RefHeading___Toc12324_3966647769)

[1.4 Verantwortliche (Stammdaten) 4](#__RefHeading___Toc12326_3966647769)

[1.5 Weiterbildung und Stand der Technik 5](#__RefHeading___Toc12330_3966647769)

[1.6 Datenschutz-Info-Veranstaltung für alle Mitarbeiter und Funktionäre 5](#__RefHeading___Toc25511_501753674)

[2 Datenverarbeitungen/Datenverarbeitungszwecke 6](#__RefHeading___Toc12332_3966647769)

[2.1 Zwecke und Beschreibung der Datenverarbeitung: 6](#__RefHeading___Toc12334_3966647769)

[2.2 Wurde eine Datenschutz-Folgenabschätzung durchgeführt? 6](#__RefHeading___Toc12342_3966647769)

[3 Verarbeitungsverzeichnisse 7](#__RefHeading___Toc12344_3966647769)

[3.1 Mitgliederverwaltung 7](#__RefHeading___Toc12346_3966647769)

[3.2 Ausbildung 13](#__RefHeading___Toc26949_2260806127)

[3.3 Kommunikation 18](#__RefHeading___Toc12366_3966647769)

[3.4 Personalwesen 21](#__RefHeading___Toc26951_2260806127)

[4 Auftragsverarbeitungsvereinbarungen 30](#__RefHeading___Toc26953_2260806127)

[5 Impressum und Statuten 30](#__RefHeading___Toc12390_3966647769)

[6 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs) 31](#__RefHeading___Toc12392_3966647769)

[6.1 Kontaktaufnahme 31](#__RefHeading___Toc75634_1065443354)

[6.2 Fotos bei Vereinsveranstaltungen 31](#__RefHeading___Toc25513_501753674)

[6.3 Selbstschutz 31](#__RefHeading___Toc25515_501753674)

[6.4 Clear Desk Policy 31](#__RefHeading___Toc26955_2260806127)

[6.5 Umgang mit mobilen IT-Geräten 32](#__RefHeading___Toc10749_980896830)

[6.6 Emails 32](#__RefHeading___Toc10751_980896830)

[6.7 Datengeheimnis 32](#__RefHeading___Toc75638_1065443354)

[6.8 Zutrittskontrolle 32](#__RefHeading___Toc75640_1065443354)

[6.9 Zugangskontrolle 33](#__RefHeading___Toc25517_501753674)

[6.10 Zugriffskontrolle 33](#__RefHeading___Toc12470_39666477691)

[6.11 Weitergabekontrolle 34](#__RefHeading___Toc12472_39666477691)

[6.12 Eingabekontrolle 34](#__RefHeading___Toc12474_39666477691)

[6.13 Auftragskontrolle 35](#__RefHeading___Toc12476_39666477691)

[6.14 Verfügbarkeitskontrolle 35](#__RefHeading___Toc12478_39666477691)

[6.15 Trennungsgebot 35](#__RefHeading___Toc12480_39666477691)

[6.16 Regelmäßigen Überprüfung, Bewertung und Evaluierung 36](#__RefHeading___Toc12404_3966647769)

[6.17 Auftragskontrolle: 36](#__RefHeading___Toc10753_980896830)

[7 Betroffenenrechte wahren 37](#__RefHeading___Toc12406_39666477691)

[7.1 Prozess betreffs Betroffenenrechte 37](#__RefHeading___Toc10755_980896830)

[7.2 Dokumentation 42](#__RefHeading___Toc47919_274173113)

[8 Profiling light 42](#__RefHeading___Toc75644_1065443354)

[9 E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO) 42](#__RefHeading___Toc12412_39666477691)

[10 Risikoanalyse 43](#__RefHeading___Toc12416_39666477691)

[10.1 Risikoanalyse ohne Maßnahmen 43](#__RefHeading___Toc12420_39666477691)

[10.2 Risiko-Matrix mit Maßnahmen 45](#__RefHeading___Toc12432_39666477691)

[11 Zusammenfassung und GV-/Vorstands-Beschluss 45](#__RefHeading___Toc12436_3966647769)

[12 Anhang 47](#__RefHeading___Toc12446_3966647769)

[12.1 Einwilligung für Newsletter (Homepage) 47](#__RefHeading___Toc26959_2260806127)

[12.2 Kontaktformular (Homepage) 47](#__RefHeading___Toc47921_274173113)

[12.3 Vorlage für Messen 48](#__RefHeading___Toc47923_274173113)

[12.4 Auskunftsbegehren 49](#__RefHeading___Toc27162_4014249856)

[12.5 Muster Datenschutzverletzung (WKO) 50](#__RefHeading___Toc27166_4014249856)

[12.6 Mustervertrag Auftragsverarbeitung (WKO) 52](#__RefHeading___Toc27168_4014249856)

[12.7 Muster: Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO) 55](#__RefHeading___Toc27170_4014249856)

**DISCLAIMER**

Sämtliche zur Verfügung gestellten Inhalte wurden mit der größtmöglichen Sorgfalt erstellt. Die Autoren, Christopher Temt und Michael Werzowa übernehmen jedoch keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der bereitgestellten Informationen (einschließlich des Verweises auf externe Quellen wie Wirtschaftskammer, Ärztekammer). Die korrekte Datenschutzdokumentation und die TOMs erfordert stets eine konkrete Prüfung im Einzelfall, und meist auch Änderungen in den eigenen Prozessen, weshalb die Beiziehung eines Datenschutzberaters (z.B. [https://www.dataprivacydoctors.at/](https://www.dataprivacydoctors.at/vorlagen/%22%20%5Cl%20%22Newsletter) ) sowie eines Rechtsanwaltes, insbesondere bei der Erstellung oder Überprüfung von Verträgen, dringend empfohlen wird. Die zur Verfügung gestellten Inhalte stellen keine Beratungsleistung welcher Art auch immer dar und können eine Beratung auch nicht ersetzen.

Haftungsansprüche gegen den Christopher Temt, und/oder Michael Werzowa welche sich auf Schäden materieller oder ideeller Art, einschließlich entgangenen Gewinn oder sonstige direkte oder indirekte Folgeschäden, beziehen, die durch die Nutzung oder Nichtnutzung der zur Verfügung gestellten Informationen verursacht wurden, sind ausgeschlossen. Die Autoren behalten es sich ausdrücklich vor, Teile der zur Verfügung gestellten Information oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

Ein Danke an die Wirtschaftskammer, die Ärztekammer, dem Datenschutzguru und viele andere, die ausgezeichnete Vorlagen und Muster kostenlos im Internet zur Verfügung stellen!

# Allgemeine Angaben

## Datenschutz-Konzept

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSGVO geforderte Einhaltung der Verordnungskonformität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte ( Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1 ).

## Sachliche und räumliche Tätigkeit

Unser Verein Name und ZVR-Zahl verarbeitet personenbezogene Daten von natürlichen Personen ganz oder teilweise automatisiert und hat seine Niederlassung in der EU, in der Vereinsadresse.

Referenzen: Art 2 + 3 + 4 DSGVO, EuGH Entscheidung Weltimmo v. NAIH (C-230/34)

## Datenschutzbeauftragter (DSB)

Trifft einer der nachfolgenden Kriterien zu, ist ein externer oder interner DSB notwendig und zu bestellen:

|  |  |  |
| --- | --- | --- |
| **Kriterium** | **Ja** | **Nein** |
| Verarbeitung der Daten durch eine Behörde oder eine öffentliche Stelle, mit Ausnahme der Gerichte |  | **X** |
| Verarbeitung der personenbezogenen Daten stellt eine Kerntätigkeit der Organisation dar und/oder erfordert eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person |  | **X** |
| Verarbeitung besonders schutzwürdige Kategorien personenbezogenen Daten (Art 9 Z 1 DSGVO wie zB Gesundheitsdaten, ethische Herkunft, genetische bzw. biometrische Daten, Gewerkschaftszugehörigkeit, usw.) stellt eine Kerntätigkeit bzw Vereinszweck der Organisation dar |  | **X** |

 Referenzen: Art 37 DSGVO, Erwägungsgründe 97

Da für unseren Verein keiner der obigen Kriterien zutrifft, wird kein DSB bestellt.

## Verantwortliche (Stammdaten)

|  |
| --- |
| **Verantwortliche** |
| Titel/NameObfrau/Mannbzw. gemäß StatutenAdresseEmailTelefon |

Referenzen: Art 4 Z 7 DSGVO

## Weiterbildung und Stand der Technik

Betreffs Weiterbildung und Stand der Technik setze wir folgende Aktivität:

|  |  |  |
| --- | --- | --- |
| **Aktivitäten** | **Veranstalter** | **sonstiges** |
| Info- u. Weiterbildungsveranstaltungen | WKO-Wien |  |
| Homepages bzw. Newsletter | <https://www.dataprivacydoctors.at/vorlagen/> |  |
|  |  |  |
| Update und Aktualisierung | [https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung](https://www.dataprivacydoctors.at/vorlagen/%22%20%5Cl%20%22NewsletterAnmeldung)- | **Newsletter** |
| Ausbildung der Mitarbeiter und Funktionäre | <https://www.dataprivacydoctors.at/angebot/>  | Workshops |
|  |  |  |

Referenzen: Art 4, 5-11 DSGVO

## Datenschutz-Info-Veranstaltung für alle Mitarbeiter und Funktionäre

Am ……….. fand in ………………………... eine x-stündige Datenschutz-Info-Veranstaltung für alle Mitarbeiter und Funktionären statt, wobei alle gebeten wurden, betreffs Sensibilisierung-Datensicherheit den Online-Fragebogen <https://itsafe.wkoratgeber.at/> auch vorher auszufüllen und dann mitzubringen.

Die „Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen“ wurde von allen Mitarbeiter und Funktionären dort unterschrieben und im Archiv abgelegt.

Alle Mitarbeiter und Funktionären wurden ebenso gebeten, dass sie folgende Basis-Webinare mit grundlegenden Informationen zur DSGVO durcharbeiten:

**[Datenschutzschulung: Video für Beschäftigte](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/webinare-dsgvo.html%22%20%5Cl%20%22heading_Basis_Webinar__Datenschutz_jetzt_neu_angehen_) (Datenschutz-guru)**
<https://www.datenschutz-guru.de/datenschutzschulung-video-fuer-beschaeftigte/>

**Handbuch für die Praxis im Betrieb**
<https://consulio.at/it-richtlinien-mitarbeiter-dsgvo/>

 **["Datenschutz jetzt neu angehen"](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/webinare-dsgvo.html%22%20%5Cl%20%22heading_Basis_Webinar__Datenschutz_jetzt_neu_angehen_)**
Mag. Ursula Illibauer / WKÖ BSIC

**["Was ist zulässig, online und offline"](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/webinare-dsgvo.html%22%20%5Cl%20%22heading_Vertiefungs_Webinar__Datenverarbeitung__Was_ist_zulaessig__online_und_offline_)**
Mag Regina Hauser-Boulanger / WKW

**["Grundlagen des Datenschutzes im Arbeitsverhältnis"](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/webinare-dsgvo.html%22%20%5Cl%20%22heading_Vertiefungs_Webinar___Grundlagen_des_Datenschutzes_im_Arbeitsverhaeltnis_)**Mag. Wolfram Hitz / WKÖ BSIC

**["Datensicherheit im eigenen Unternehmen und beim Auftragsverarbeiter"](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/webinare-dsgvo.html%22%20%5Cl%20%22heading_Vertiefungs_Webinar__Datensicherheit_im_eigenen_Unternehmen_und_beim_Auftragsverarbeiter_)**
Mag. Verena Becker / WKÖ BSIC

# Datenverarbeitungen/Datenverarbeitungszwecke

## Zwecke und Beschreibung der Datenverarbeitung:

### Mitgliederverwaltung

Führung, Verarbeitung und Übermittlung von Mitgliederverzeichnissen, Evidenz der Mitglieds- und Förderungsbeiträge, Verkehr mit Mitgliedern oder Förderern von Körperschaften des öffentlichen und privaten Rechts, insbesondere Vereinen, und Personengemeinschaften, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten.

Verarbeitung und Übermittlung von Daten im Rahmen des Vereinszweckes, hier Vereinszweck eintragen …………. ……………….……………………………………………….
sowie Geschäftsbeziehungen mit Lieferanten, sowie an den Vereinsaktivitäten mitwirkende Dritte inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

### Ausbildungen

Wir verarbeiten die Daten von Bewerber-/Auszubildenden-und Lehrbeauftragte/Vortragende nur zum Zweck und im Rahmen des Ausbildungsverfahrens, zur Information und Betreuung bei Veranstaltungen wie zB Workshops, Seminare, Referate, … im Einklang mit unseren Statuten bzw. den gesetzlichen Vorgaben, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Rechnungen, Korrespondenzen oder Verträge, Schulungsunterlagen, Bewerberunterlagen, Zeugnisse, Anwesenheitslisten, ...) in diesen Angelegenheiten.

### Kommunikation

Vereinszweck-orientierte Information und Betreuung von kategorisierten Mitglieder, Lieferanten, Auszubildende, Förderern und an den Vereinsaktivitäten mitwirkende Dritte inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter und Informationsmaterial.

### Personalwesen

Verarbeitung und Übermittlung von Daten für Lohn-, Gehalts-, Entgeltverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten

Verarbeitung und Übermittlung von personenbezogenen Daten von Bewerbern als Mitarbeiter, soweit diese Daten vom Betroffenen angegeben wurden.

## Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

**Ja  Nein X**

**Wenn Ja, wann?**

**Wenn Nein, aus welchem Grund nicht?**

Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, da. sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht – siehe Risikobewertung und Maßnahmen -, da keine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und da keine umfangreiche [Verarbeitung](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Grundsaetze-und-Rechtmaes.html) sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt. Es gibt auch keine Überwachung öffentlich zugänglicher Bereiche durch Video.

Darüber hinaus hat die österr. Datenschutzbehörde in Ihrer Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018 festgehalten, dass alle unsere Verarbeitungen Standard- und Muster-Verarbeitungen sind und somit keine Folgeabschätzungen notwendig sind.

Referenzen: Art 35 Z1-3 DSGVO

# Verarbeitungsverzeichnisse

Referenzen: Art 30, Art 31 DSGVO, Erwägungsgründe 13, 75, 76, 82, 89

## Mitgliederverwaltung

### Verantwortliche

|  |
| --- |
| **Verantwortliche** |
| **Titel/ Name**Obfrau/mannAdresseEmailTelefon |

### Zweck

Führung, Verarbeitung und Übermittlung von Mitgliederverzeichnissen, Evidenz der Mitglieds- und Förderungs­beiträge, Verkehr mit Mitgliedern oder Förderern von Körperschaften des öffentlichen und privaten Rechts, insbesondere Vereinen, und Personengemeinschaften, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten.

Verarbeitung und Übermittlung von Daten im Rahmen des Vereinszweckes, hier Vereinszweck eintragen

………………...…...……………..…. sowie Geschäftsbeziehungen mit Lieferanten, sowie an den Vereinsaktivitäten mitwirkende Schule sowie Dritte inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

### Kategorien der betroffenen Personen

|  |  |
| --- | --- |
| **Lfd.Nr.** | **Beschreibung der Kategorien betroffener Personen** |
| 1 | Vereinsmitglieder |
| 2 | Funktionäre |
| 3 | Förderer inkl. Kontaktpersonen |
| 4 | An den Vereinsaktivitäten mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen |

### Rechtsgrundlagen (in geltender Fassung)

* Art 6 Z 1 lit a (Einwilligung der Betroffenen) Fotos, SMS
* Art 6 Z 1 lit b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen) DSGVO
* § 132 BAO
* §§ 190, 212 UGB
* EStG, UStG
* Standard- und Musteranwendungen nach Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018
* Vereinsgesetz 2002
* (Statuten)
* möglicherweise Gewerberecht

### Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen zu aufrechten Vereinstätigkeit, Geschäftsabwicklungen, Mitgliedsbeiträge, Rechnungen, erledigte Geschäftsfälle, Unterlagen und Zustimmungserklärungen sowie Verträge mit Auftragsverarbeitern sind im Archiv abgelegt.

### Kategorien der verarbeiteten Daten

|  |  |  |  |
| --- | --- | --- | --- |
| **Betroffene Personen­gruppen:** | **Nr.:** | **Datenkategorie:** | **Empfänger­kategorie** |
| Alle | 01 | Einwilligung nach Art 4 abgelegt(insbesondere Newsletter und Fotos) | 2-4 |
| Mitglieder | 02 | Mitgliedsnummer / Ordnungsnummer | 1, 3, 4, 5 |
| 03 | Name oder Bezeichnung der Organisation, Firma | 1, 3, 4, 5 |
| 04 | Anrede / Geschlecht | 1, 3, 4, 5 |
| 05 | Geburtsdatum | 3, 4 |
| 06 | Anschrift | 1, 3, 4, 5 |
| 07 | Telefon-, Faxnummer Email und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | 1, 3, 4, 5 |
| 08 | Beruf oder Branche (nach Angabe des Betroffenen) | 3, 4, 5 |
| 09 | Mitgliederkategorie, z.B. ordentliches/außerordentliches/unterstützendes Mitglied, Ehrenmitglied usw. | 3, 4, 5 |
| 10a | Fotos (ausdrückliche Einwilligung) | 2 -4 |
| 10b |  Foto im Vereinsausweis gemäß Statuten | 2 - 4 |
| 11 | Eintritts-, Austrittsdaten | 3, 4, 5 |
| 12 | Beiträge | 1, 3, 4, 5 |
| 13 | Auszeichnungen und Ehrungen | 3 |
| 14 | Anwesenheits-Liste bzw Bestätigungen,  | 2, 3, 4 |
| 15 | Vom Betroffenen bekannt gegebene Interessen und Spezialgebiete | 3 |
| 16 | Vereinszweckrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen, Workshops, Seminaren, …. | 3 |
| 17 | Angaben betreffend die Inanspruchnahme von Leistungen des Auftraggebers (zB siehe 16) mit Zahlungsverpflichtungen des Betroffenen an den Auftraggeber | 1, 4, 5 |
| 18  | Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen | 1, 4, 5 |
| 19 | Bankverbindung | 1, 4, 5 |
| 20 | Newsletter-Sperre | 1, 3, 4 |
| Funktionäre: | 21 | Ordnungsnummerwie zB Mitgliedernummer, ... | 2 - 4, 5 |
| 22 | Name | 1 - 4, 5 |
| 23 | Anrede / Geschlecht | 1 - 4, 5 |
| 24 | Geburtsdatum (Volljährigkeit) | 2 |
| 25 | Zustellanschrift im Rahmen der Funktion | 1 - 4, 5 |
| 26 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben, beim Auftraggeber | 1 - 4, 5 |
| 27 | Funktion beim Auftraggeber | 1 - 4, |
|  28 | Beginn und Ende der Funktion | 1 - 4, 5 |
| 29 | Zahlungsverpflichtungen des Betroffenen an den Auftraggeber | 1 - 4, 5 |
| 30 | Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen | 1, 3, 5 |
| 31 | Auszeichnungen und Ehrungen | 3 |
| 32 | Newsletter-Sperre | 1, 3, 4 |
| Fördererinklusive Kontaktpersonen | 33 | Ordnungsnummer |  3, 4 |
| 34 | Name oder Bezeichnung der Organisation und Firmenbuch- und andere Kennzahlen (UID-Nummer, ...) | 1, 3, 4, 5 |
| 35 | Anrede/Geschlecht | 3, 4, 5 |
| 36 | Anschrift | 3, 4, 5 |
| 37 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben |  3, 4, 5 |
| 38 | Spenden und sonstige Leistungen des Betroffenen | 3, 4, 5 |
| 39 | Angaben betreffend die Inanspruchnahme von Leistungen des Auftraggebers | 3, 4, 5 |
| 40 | Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen | 1, 3, 4, 5 |
| 41 | Kontaktperson | 1, 3-5 |
| 42 | Deren Adresse sowie Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergebende Kontaktdaten der Kontaktperson | 3, 4, 5 |
| 43 | Newsletter-Sperre  | 2 -4 |
| mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen | 44 | OrdnungsnummerLieferantennummer, ... | 2 - 4, 5 |
| 45 | Name oder Bezeichnung der Organisation und Firmenbuch- und andere Kennzahlen (UID-Nummer, ...) | 1 - 4, 5 |
| 46 | Anrede/Geschlecht | 2 - 4, 5 |
| 47 | Anschrift | 2 - 4, 5 |
| 48 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | 2 - 4, 5 |
| 49 | Vereinszweckrelevante Aktivitäten bzw. Veranstaltungen | 2 - 4, 5 |
| 50 | Bankverbindungen | 1 -4, 5 |
| 51 | Namen Kontaktpersonen | 1 - 4, 5 |
| 52 | Zuordnung zu einer bestimmten Kategorie (einschließlich regionale Zuordnung, usw.) |  |
| 53 | Vertragstext und Geschäftskorrespondenzen, Rechnungen,.. | 2 - 4, 5 |
| 54 | Besondere Rabatte bzw. Vergünstigungen, …  | 2 - 4 |
| 55 | Gegenstand der Lieferung oder Leistung | 2 - 4, 5 |
| 56 | Rechnungsbetrag | 1 - 4, 5 |
| 57 | Newslettersperre | 2 -4 |
| Alle | 58 | Auftragssperre= Recht auf Einschränkung geltend gemacht |  |

### Löschungs- und Aufbewahrungsfristen

|  |  |
| --- | --- |
| **Daten** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** |
| 1 - 18, 20 – 30, | Bis zur Beendigung der Mitgliedschaft des Betroffenen und Ablauf der für den Auftraggeber geltenden Verjährungs- und gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. |
| 32 – 42 | Bei Förderern: Bis zum Ablauf des dritten Jahres nach dem letzten Kontakt mit dem Auftraggeber. |
| 43 – 55 | Bis zur Beendigung der Geschäftstätigkeit mit Betroffenen und Ablauf der für den Auftraggeber geltenden Verjährungs- und gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. |
| 19, 31, 42, 56 + 10 | Newsletter und Fotos: Recht auf jederzeitigen Widerspruch (Art 21 DSGVO) |

### Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Empfängerkategorien** | **Drittstaat außerhalb der EU** | **Internationale Organisation** |
| 1 | Banken | Nein | Nein |
| 2 | Behörden und sonstige Institutionen auf Grund gesetzlicher Melde- oder Berichtspflichten wie, insbesondere Vereinsbehörden, Veranstaltungsbehörden usw.; | Nein | Nein |
| 3 | Personen und Institutionen auf Grund einer Ermächtigung oder Verpflichtung zur Datenübermittlung in den Statuten oder auf Grund ausdrücklicher Zustimmung des Betroffenen; | Nein | Nein |
| 4 | Rechtsanwälte, Gerichte und sonstige Stellen, zum Zweck der Rechtsdurchsetzung. | Nein | Nein |
| 5 | Steuerberater, Bilanzbuchhalter | *Nein* | *Nein* |
| 6 | Provider Homepage/IT-Dienstleister | *?* | *Nein* |
| *7* | *Software-Anbieter mit Fernwartung* | *?* | *Nein* |
| *8* | …… | *?* | *Nein* |
| *9* |  |  |  |
|  |  |  |  |

### Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten *?*

## Ausbildung

### Verantwortliche

|  |
| --- |
| **Verantwortliche** |
| **Titel/ Name**Obfrau/mannAdresseEmailTelefon |

### Zweck

Wir verarbeiten die Daten von Bewerber-/Auszubildenden-und Lehrbeauftragte/Vortragende nur zum Zweck und im Rahmen des Ausbildungsverfahrens, zur Information und Betreuung bei Veranstaltungen wie zB Workshops, Seminare, Referate, … im Einklang mit unseren Statuten bzw. den gesetzlichen Vorgaben, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Rechnungen, Korrespondenzen oder Verträge, Schulungsunterlagen, Bewerberunterlagen, Zeugnisse, Anwesenheitslisten, ...) in diesen Angelegenheiten.

### Kategorien der betroffenen Personen

|  |  |
| --- | --- |
| **Lfd.Nr.** | **Beschreibung der Kategorien betroffener Personen** |
| 1 | Bewerber für Ausbildung bzw Auszubildende |
| 2 | Lehrkraft, Vortragende |
| 3 | Dritte |

### Rechtsgrundlagen (in geltender Fassung)

* Art 6 Z 1 lit a (Einwilligung der Betroffenen) Newsletter, Fotos. SMS
* Art 6 Z 1 lit b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen) DSGVO
* § 132 BAO
* §§ 190, 212 UGB
* EStG, UStG
* Standard- und Musteranwendungen nach Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018
* Vereinsgesetz 2002
* Vereinsstatuten
* Mit der Übermittlung der Bewerbung für eine Ausbildung an uns, erklären sich die Bewerber mit der Verarbeitung ihrer Daten zu Zwecken des Bewerbungsverfahrens entsprechend der in dieser Datenschutzerklärung dargelegten Art und Umfang einverstanden.

### Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen zu Bewerbungen, Lebenslauf, Leumund, …., Schulungsunterlagen, Verschwiegenheit, Geschäftsabwicklungen, Rechnungen, erledigte Geschäftsfälle, Unterlagen und Zustimmungserklärungen sowie Verträge mit Auftragsverarbeitern bzw Lehrbeauftragten sind im Archiv abgelegt.

### Kategorien der verarbeiteten Daten

Das Bewerbungsverfahren setzt voraus, dass Bewerber uns die Bewerberdaten zwecks Ausbildung mitteilen. Die notwendigen Bewerberdaten ergeben sich aus den Schulungsbeschreibungen und grundsätzlich gehören dazu die Angaben zur Person, Post- und Kontaktadressen und die zur Bewerbung gehörenden Unterlagen, wie Anschreiben, Lebenslauf, Leumund und die Zeugnisse. Daneben können uns Bewerber freiwillig zusätzliche Informationen mitteilen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Betroffene Personen­gruppen:** | **Nr.:** | **Datenkategorie:** | **Sensible Daten** | **Empfänger­kategorie** |
| Alle | 01 | Einwilligung nach Art 4 abgelegt(insbesondere Newsletter und Fotos) | Nein | 3 - 4 |
| BewerberAuszubildende | 02 | Mitgliedsnummer / Ordnungsnummer | Nein | 3 - 4 |
| 03 | Name oder Bezeichnung der Organisation, Firma | Nein | 1 - 4 |
| 04 | Anrede / Geschlecht | Nein | 1 - 4 |
| 05 | Geburtsdatum/-jahr(Volljährigkeit, Mindestalter) | Nein | 3 - 4 |
| 06 | Anschrift | Nein | 1 - 4 |
| 07 | Telefon-, Faxnummer Email und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | Nein | 1 - 4 |
| 08 | Termine | Nein | 3 - 4 |
| 09 | Leumund-Zeugnis,falls notwendig | Art 10 | 3 - 4 |
| 10 | Lebenslauf | Vertraulich | 3 - 4 |
| 11 |  Gesundheitsdaten, falls notwendig | Art 9 | 3 - 4 |
| 12 |  Voraussetzungen für Ausbildung erfüllt | Vertraulich | 3 - 4 |
| 13 |  Weitere Daten gemäß Schulungsbeschreibungen  | Vertraulich | 3 - 4 |
| 14 |  Anwesenheitsliste (nur Name und Unterschrift) | Vertraulich | 3 - 4 |
| 15 | Diplom-/Abschlussarbeiten und ähnliches  | Vertraulich | 3 - 4 |
| 16 | Interessen bzw. freiwillig zusätzliche Informationen seitens des Betroffenen | Vertraulich | 3 - 4 |
| 17 | Ausbildungsrelevante Aktivitäten, insb. Aus-/Weiterbildungs-Veranstaltungen, Workshops, Seminaren, Supervision, …. | Nein | 3 - 4 |
| 18  | Zeugnisse, Zertifikate, Bestätigungen, ... | Vertraulich | 3 - 4 |
| 19 | Angaben betreffend die Inanspruchnahme von Leistungen des Auftraggebers mit Zahlungsverpflichtungen des Betroffenen an den Auftraggeber | Nein | 3 - 4 |
| 20 | Zahlungen oder sonstige Leistungen Betroffenen | Nein | 1 - 4 |
| 21 | Bankverbindung | Nein | 1 - 4 |
| 22 | Newsletter-Sperre | Nein | 3 - 4 |
| Lehrkraft, Vortragende | 23 | Ordnungsnummerwie zB Mitgliedernummer, ... | Nein | 1 - 4 |
| 24 | Name | Nein | 1 - 4 |
| 25 | Anrede / Geschlecht | Nein |  |
| 26 | Verschwiegenheitsverpflichtung  | Vertraulich | 3 - 4 |
| 27 | Zustellanschrift im Rahmen der Funktion | Nein | 1 - 4 |
|  28 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben, beim Auftraggeber | Nein | 1 - 4 |
| 29 | Zeugnisse, Bestätigungen, ... | Nein | 3 - 4 |
| 30 | Beginn und Ende der Lehrtätigkeit | Nein | 3 - 4 |
| 31 | Zahlungsverpflichtungen des Betroffenen an den Auftraggeber | Nein | 3 - 4 |
| 32 | Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen | Nein | 3 - 4 |
| 33 | Newsletter-Sperre | Nein | 3 - 4 |
| mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen | 34 | OrdnungsnummerLieferantennummer, ... | Nein | 1 - 4 |
| 34 | Name oder Bezeichnung der Organisation und Firmenbuch- und andere Kennzahlen (UID-Nummer, ...) | Nein | 1 - 4 |
| 36 | Anrede/Geschlecht | Nein | 1 - 4 |
| 37 | Anschrift | Nein | 1 - 4 |
| 38 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | Nein | 1 - 4 |
| 39 | Ausbildungsrelevante Aktivitäten bzw. Veranstaltungen  | Nein | 3 - 4 |
| 40 | Bankverbindungen | Nein | 1 - 4 |
| 41 | Namen Kontaktpersonen | Nein | 3 - 4 |
| 42 | Zuordnung zu einer bestimmten Kategorie (einschließlich regionale Zuordnung, usw.) | Nein | 3 - 4 |
| 43 | Vertragstext und Geschäftskorrespondenzen, Rechnungen,.. | Nein | 1 - 4 |
| 44 | Gegenstand der Lieferung oder LeistungzB Seminarraummiete + Verköstigung | Nein | 1 - 4 |
| 45 | Rechnungsbetrag | Nein | 1 - 4 |
| Alle | 46 | Newslettersperre\* | Nein | 3 - 4 |
| 47 | Auftragssperre= Recht auf Einschränkung geltend gemacht | Nein | 3 - 4 |

\* Hier sind Werbemails gemeint! Auszubildende und Vortragende können auch bei Widerruf vom Newsletter über ausbildungsrelevante Dinge zur Vertragserfüllung per Email informiert werden.

### Löschungs- und Aufbewahrungsfristen

|  |  |
| --- | --- |
| **Daten** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** |
| 1 - 22BewerberAuszubildende | Die von den Bewerbern zur Verfügung gestellten Daten, können im Fall einer erfolgreichen Bewerbung für die Zwecke der Schulung von uns weiterverarbeitet werden. Andernfalls, sofern die Bewerbung nicht erfolgreich ist, werden die Daten der Bewerber gelöscht. Die Daten der Bewerber werden ebenfalls gelöscht, wenn eine Bewerbung zurückgezogen wird, wozu die Bewerber jederzeit berechtigt sind.Die Löschung erfolgt, vorbehaltlich eines berechtigten Widerrufs der Bewerber, nach dem Ablauf eines Zeitraums von 2 Jahren, damit wir etwaige Anschlussfragen zu der Bewerbung beantworten können. Bis zur Beendigung der Ausbildung des Betroffenen und Ablauf der für den Verantwortlichen geltenden Verjährungs- und gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. |
| 23 - 47LehrkräfteVortragendeDritte | Bis zum Ablauf der für den Auftraggeber geltenden Verjährungs- und gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. |
|  | Newsletter und Fotos: Recht auf jederzeitigen Widerspruch (Art 21 DSGVO) |
| 14, 18, 29 | Die für die Herstellung vom Duplikaten von Zeugnissen, die Teile staatlich anerkannter Ausbildungen sind (zB LSB, Mediation, Psychotherapie), bewahren wir die entsprechenden Daten 30 Jahre lang auf.  |

### Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Empfängerkategorien** | **Drittstaat außerhalb der EU** | **Internationale Organisation** |
| 1 | Banken | Nein | Nein |
| 2 | Steuerberater, Bilanzbuchhalter | Nein | Nein |
| 3 | Behörden und sonstige Institutionen auf Grund gesetzlicher Melde- oder Berichtspflichten sowie zwecks Anerkennung /Zeugnisse der Ausbildung | Nein | Nein |
| 4 | Rechtsanwälte, Gerichte und sonstige Stellen, zum Zweck der Rechtsdurchsetzung. | *Nein* | *Nein* |
|  |  |  |  |

### Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten *?*

### TOMs

Soweit im Rahmen des Bewerbungsverfahrens freiwillig oder auf Grund der Statuten besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO bzw. Art 10 Leumund mitgeteilt werden, erfolgt deren Verarbeitung zusätzlich nach Art. 9 Abs. 2 lit. b bzw Art 10 DSGVO (z.B. Gesundheitsdaten, wie z.B. Schwerbehinderteneigenschaft oder ethnische Herkunft). Soweit im Rahmen des Bewerbungsverfahrens besondere Kategorien von personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO bei Bewerbern angefragt werden, erfolgt deren Verarbeitung zusätzlich nach Art. 9 Abs. 2 lit. a DSGVO (z.B. Gesundheitsdaten, wenn diese für die Berufsausübung erforderlich sind).

Ferner können Bewerber uns ihre Bewerbungen per Brief oder via E-Mail übermitteln. Hierbei bitten wir jedoch zu beachten, dass E-Mails grundsätzlich nicht verschlüsselt versendet werden und die Bewerber selbst für die Verschlüsselung sorgen müssen. Wir können daher für den Übertragungsweg der Bewerbung zwischen dem Absender und dem Empfang auf unserem Server keine Verantwortung übernehmen und empfehlen daher den postalischen Versand zu nutzen.

## Kommunikation

### Verantwortliche

|  |
| --- |
| **Verantwortliche** |
| **Titel/ Name**Obfrau/mannAdresseEmailTelefon |

### Zweck

Vereinsorientierte Information und Betreuung von kategorisierten Mitglieder, Funktionären, Auszubildende, Förderern und an den Vereinsaktivitäten mitwirkende Schule sowie Dritte inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter und Informationsmaterial.

### Rechtsgrundlagen (in geltender Fassung)

* Art 6 Z 1 lit a (Einwilligung der Betroffenen), Fotos + Newsletter + SMS
* Ansonsten: b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen)
* § 151 GewO 1994
* Standard- und Musteranwendungen nach Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018
* Vereinsgesetz 2002

### Kategorien der betroffenen Personen

|  |  |
| --- | --- |
| **Lfd.Nr.** | **Beschreibung der Kategorien betroffener Personen** |
| 1 | eigene Mitglieder, Funktionäre, Auszubildende, Förderer, Interessierte, an Vereinstätigkeiten mitwirkende Institutionen sowie Dritte |
| 2 | Kontaktpersonen von oben |

### Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Zustimmungserklärungen bzw. Verträge sowie Verträge mit Auftragsverarbeitern usw. sind im Archiv abgelegt.

### Kategorien der verarbeiteten Daten

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Kategorien der betroffenen Personengruppe** | **Lf. Nr.:** | **Datenkategorien** | **Besondere Datenkategorien iSd Art 9 u. Art 10 d. DSGVO** | **Rechtsvertreter im Anlassfall** | **Gericht im Anlassfall** | **Externes Newsletter-Tool** |
| 1. eigene Mitglieder, Funktionäre, Auszubildende, Förderer, an Vereinsaktivitäten mitwirkende Institutionen sowie Dritte | 01 | Mitgliedernummersonstige Ordnungszahlen | *Nein* | ***X*** | ***X*** |  |
| 02 | Name bzw. Bezeichnung | *Nein* | ***X*** | ***X*** | ***X*** |
| 03 | Anrede/Geschlecht | *Nein* | ***X*** | ***X*** | ***X*** |
| 04 | Anschrift bzw. Lieferadresse | *Nein* | ***X*** | ***X*** |  |
| 05 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | *Nein* | ***X*** | ***X*** | NurEmail |
| 06 | Termine | *Nein* | ***X*** | ***X*** |  |
| 07 | Homepage, Soziale Netzwerke | *Nein* | ***X*** | ***X*** |  |
| 08 | IP-Adresse, Meta-Daten | *Nein* | ***X*** | ***X*** |  |
| 09 | Einwilligung nach Art 4 abgelegt | *Nein* | ***X*** | ***X*** |  |
| 11 | Berufs-, Branchen- Geschäftsbezeichnung | *Nein* | ***X*** | ***X*** |  |
| 12 | Firmenbuch- und andere Kennzahlen (UID-Nummer, ...) | *Nein* | ***X*** | ***X*** |  |
| 13 | Vom Betroffenen bekannt gegebene Interessen und Spezialgebiete | *Nein* | ***X*** | ***X*** |  |
| 14 | Vereinszweckrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen | *Nein* | ***X*** | ***X*** |  |
| 15 | Interessen (auf Grund bisherigen Teilnahme oder eigener Angaben des Vereinsmitgliedes gegenüber dem Auftraggeber) | *Nein* | ***X*** | ***X*** |  |
| 16 |  Newsletter-Sperre | *Nein* | ***X*** | ***X*** |  |
| 17 | Auftragssperre= Recht auf Einschränkung geltend gemacht | *Nein* | ***X*** | ***X*** |  |
| Kontaktpersonen von oben | 18 | Name bzw. Bezeichnung, Anrede/Geschlecht | *Nein* | ***X*** | ***X*** | ***X*** |
| 19 | Anschrift | *Nein* | ***X*** | ***X*** |  |
| 20 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | *Nein* | ***X*** | ***X*** | ***NurEmail*** |
| 21 | Funktion oder betreutes Aufgabengebiet | *Nein* | ***X*** | ***X*** |  |
| 22 | Einwilligung nach Art 4 abgelegt | *Nein* | ***X*** | ***X*** |  |
| 23 |  Newsletter-Sperre | *Nein* | ***X*** | ***X*** |  |
| 24 | Auftragssperre= Recht auf Einschränkung geltend gemacht | *Nein* | ***X*** | ***X*** |  |

### Löschungs- und Aufbewahrungsfristen

|  |  |
| --- | --- |
| **Daten (Lfd. Nr.)** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** |
| 1 – 24 | Aufgrund der gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen |
| Newsletter | Recht auf Widerspruch (Art 21 DSGVO) |
| IP-Adresse. Meta-Daten | Zu eigenen Sicherheitszwecken: Speicherfrist von maximal 7 Tagen(siehe auch Datenschutzerklärung auf der Homepage) |

### Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

|  |  |  |
| --- | --- | --- |
| **Empfängerkategorien** | **Drittstaat (d.h. Staaten außerhalb der EU)** | **Internationale Organisation** |
| 1.Rechtsvertreter im Anlassfall | Nein | Nein |
| 2.Gericht im Anlassfall | Nein | Nein |
| 3 Externer Newsletter-Tool-Anbieter | ? | Nein |
| Sichere und verschlüsselte Datendiensten | ? | Nein |

### Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten.

### TOMs siehe dort

## **Personalwesen**

### Verantwortliche

|  |
| --- |
| **Name**AdresseTelefonEmail |

### Zweck

Verarbeitung und Übermittlung von Daten für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten

Verwendung von personenbezogenen Daten von Bewerbern, soweit diese Daten vom Betroffenen angegeben wurden.

### Rechtsgrundlagen

* Art 6 Z 1 b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen), f (berechtigte Interessen des Verantwortlichen) DSGVO
* §8 Arbeitsinspektionsgesetz
* Betriebsrat gemäß § 89 Z 4 ArbVG, Sicherheitsvertrauensperson nach § 10 ArbeitnehmerInnenschutzgesetz (ASchG), [BGBl. Nr.450/1994](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1994_450_0/1994_450_0.pdf) idgF., Jugendvertrauensperson gemäß § 125ff ArbVG und Behinderten- vertrauensperson gemäß §22a Behinderteneinstellungsgesetz
* Gewerbebehörde, Zuständigkeiten nach ASchG,
* §16 Behinderteneinstellungsgesetz
* §19 Berufsausbildungsgesetz
* §73 Abs.3 ArbVG
* §11 Abs.2 Z5 und § 13 BMVG
* [BGBl. Nr. 142/1969](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1969_142_0/1969_142_0.pdf) idgF

### Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen und Verträge zum Personalwesen sowie Verträge mit Auftragsverarbeitern sind im Archiv abgelegt.

### Kategorien der betroffenen Personen

|  |  |
| --- | --- |
| **Lfd.Nr.** | **Beschreibung der Kategorien betroffener Personen** |
| 1 | Arbeitnehmer, arbeitnehmerähnliche Personengruppen, Leiharbeitnehmer, freie Dienstnehmer, Lehrlinge, Volontäre und Ferialpraktikanten (auch ehemalige Beschäftigte): |
| 2 | Bewerber als Mitarbeiter |

### Kategorien der verarbeiteten Daten

* Die DSGVO verpflichtet den Verantwortlichen vorab alle Verarbeitungen, Betroffenen und deren Daten zu dokumentieren, um so im Anlassfall DSGVO-konform vorgehen zu können.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorien der betroffenen Personengruppe** | **Lfd Nr** | **Datenkategorie** | **Empfängerkategorien** |  **Datenkategorien iSd Art 9 und Art 10 DSGVO[[1]](#footnote-2)** |
| 1. Arbeitnehmer, arbeitnehmerähnliche Personengruppen, Leiharbeitnehmer, freie Dienstnehmer, Lehrlinge, Volontäre und Ferialpraktikanten (auch ehemalige Beschäftigte): | 01 | Mitarbeiter-KennungOrdnungsnummer |  | Nein |
| 02 | Name | 1 – 25 | Nein |
| 03 | Frühere Namen (Namensteile) | 1 – 24 | Nein |
| 04 | Geburtsdatum | 1 – 13, 15 – 23 | Vertraulich |
| 05 | Geburtsort | 1 – 13, 15 – 22 | Nein |
| 06 | Geschlecht | 1 – 23 | Nein |
| 07 | Personenstand | 1, 2, 4, 5, 9 – 13, 17 – 19, 21, 22 | Bis 31.12.2018 Jaab dann Nein |
| 08 | Kinder und sonstige Familienangehörige, im Zusammenhang mit Leistungen, die in Verbindung mit dem Arbeitsverhältnis des Betroffenen erbracht werden (insbesondere Name, Geburtsdatum, Sozialversicherungsnummer) | 2, 4, 5, 9 – 13, 17 – 19, 21, 22 | Vertraulich |
| 09 | Gesetzlicher Vertreter | 1, 2, 4, 5, 8 – 19, 21, 22 | Nein |
| 10 | Staatsbürgerschaft | 2 – 12, 16, 21, 22 | Nein |
| 11 | Bankverbindung | 1, 2, 4, 5, 9 – 11, 14, 21, 22 | Vertraulich |
| 12 | Organisatorische Zuordnung im Betrieb einschließlich Beginn und Ende | 2 – 7, 9 – 11, 15, 16, 18, 21, 22, 25 | Nein |
| 13 | Betriebl. Telefon, Faxnummer Email und andere zur Adressierung im Betrieb erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | 1 – 23, 25 | Nein |
| 14 | Wohnadresse | 1 – 17, 21 – 23 | Vertraulich |
| 15 | Private Telefon- und Faxnummer - nur dann ausnahmsweise zulässig, wenn der Arbeitgeber ohne Kenntnis der Mobiltelefonnummer im Einzelfall eine legitime Aufgabe, für die der\*die Arbeitnehmer\*in eingestellt ist, nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und ihm eine andere Organisation der Aufgabenerfüllung nicht möglich oder nicht zumutbar ist oder bei Betriebsvereinbarung | 1 – 17, 21 – 23 | Vertraulich |
| 16 | Kostenstelle(n) | 5, 19, 21, 22 | Nein |
| 17 | Sozialversicherungsnummer | 2, 4, 5, 9 – 12, 18, 19, 21 – 24 | Nein |
| 18 | Sozialversicherungsträger | 2, 4, 5, 9 – 12, 19, 21 – 23 | Nein |
| 19 | Daten zur Krankenscheinverwaltung | 2, 18, 21 – 23 | Art 9 |
| 20 | * Dienstnehmer-Sozialversicherungsdaten Versichertenmeldung:
* Beitragsgruppe
* An-/Abmeldedatum und Änderungsdatum Zugehörigkeit (Arbeiter, Angestellter, ...) Geringfügigkeit
* Verwandtschaftsverhältnis zum Dienstgeber Beteiligung am Unternehmen des Dienstgebers
* Lehrzeit (1. Lehrjahr von – bis, Lehrzeitende)
* Nacht- Schwerarbeit (Anfang, Ende
* Art des Bezuges (Monatslohn, Zeitlohn)
* Beitragsgrundlagenmeldung:
* Beitragszeitraum (von-bis-Monat, Jahr, Verrechnungsart)
* Allgemeine Beitragsgrundlage Beitragsgrundlage Sonderzahlung
* Anzahl der Tage mit Teilentgelt Beitragspflichtiges Teilentgelt
* Zugehörigkeit (Arbeiter, Angestellter, ...) Anspruch auf Sonderzahlung (ja, nein)
* Erstattungsantrag Krankenentgelt gemäß § 8 EFZG
* Anspruch auf Pauschalbetrag
* Kennzeichen für Krankheit/Unglücksfall, Arbeitsunfall/Berufskrankheit
* Anspruch in Wochen
* Vorbezugstage (Summe, Angabe in Arbeitstagen oder Kalendertagen) Erstattungszeitraum (Beginn, Ende) Fortgezahltes Bruttoentgelt
* Art der Beschäftigung (Arbeiter, Lehrling, Heimarbeiter, Sonstige)
* Tagesturnus (Anzahl der Tage)
* Berechnung der Ansprüche nach Kalenderjahr/Arbeitsjahr
* Ende des Entgeltanspruches
* Vordienstzeiten (von, bis)
* Arbeitsfreie Tage
* Arbeits- und Entgeltsbestätigung für Krankengeld
* Grund der Arbeitseinstellung
* Beschäftigungsverhältnis (gelöst, nicht gelöst)
* Bruttoentgelt im letzten Beitragszeitraum ohne Sonderzahlung
* Bezug (von, bis, Betrag)
* Betragssumme
* Sonderzahlungsanspruch (ja, nein)
* Sachbezug (Anzahl der Tage, Text)
* Entgelt wird bezahlt bis
* EFZ-Anspruch in Wochen
* Berechnung der Ansprüche nach Arbeits-Kalenderjahr, Arbeits- Kalendertage
* Teilentgelt – Prozentanteil des Gesamtentgeltes (Prozente, von, bis)
* Provision während der Arbeitsunfähigkeit (ja,nein)
* Anrechnung Vorerkrankungen (von, bis)
* Arbeits- und Entgeltsbestätigung für Wochengeld
* Grund der Arbeitseinstellung Beschäftigungsverhältnis (gelöst, nicht gelöst) Urlaub vor Eintritt der Mutterschaft (von, bis) Arbeitsverdienst der letzten drei Kalendermonate (ohne SZ, minus gesetzliche Abzüge) Arbeitsverdienstzeitraum (von, bis)
* Unterbrechung des Bezuges während der letzten drei Monate (von, bis)
* Ausmaß der Sonderzahlung (Anzahl Monate, Anzahl Wochen)
* Anspruch auf Fortbezug des Entgeltes (gesetzlich, vertraglich, kein Anspruch)
* Anspruch auf das halbe Entgelt (bis)
* Anspruch auf mehr als das halbe Entgelt (bis
* Mitarbeitervorsorge gemäß BMVG
* MVK-Leitzahl
* MV-Beitragsgrundlage (inklusive Sonderzahlungen)
* Beitragshöhe gemäß BMVG (Gruppensumme
* Beginn und Ende der MV-Beitragszahlung (Stichtag)
* Eingezahlter Betrag an MV
* MV-Beitragszeiten (Beitragsmonat von – bis
* Vordienstzeiten (bei Übertritt ins neue Abfertigungsmodell)
* Übertragungsbetrag an die MVK und Zahlungsmodus
* Zuordnung zu Dienstgeberkontonummer
* Abmeldegründe (zB Unterbrechung der Beitragszahlung durch Karenzurlaub)
 | 2, 4, 5, 10, 19, 21, 22 | Art 9 |
| 21 | Eintrittsdatum | 2 – 8, 10, 11, 13, 16, 19, 21, 22 | Nein |
| 22 | Vordienstzeiten | 10, 13, 19, 21, 22 | Nein |
| 23 | Austrittsdatum, Kündigungsfrist | 2 – 8, 10, 11, 13, 16, 19, 21, 22 | Nein |
| 24 | Art der Beendigung des Dienstverhältnisses | 2, 4, 5, 9 – 11, 21, 22 | Vertraulich |
| 25 | Gesetzliche Beschäftigungsvoraussetzungen | 4 – 8, 11, 21, 22 | Nein |
| 26 | Daten der Beschäftigungsbewilligung | 4 – 7, 9, 21, 22 | Nein |
| 27 | Bezeichnung der Tätigkeit | 2, 4 – 7, 9, 18, 21, 22 | Nein |
| 28 | Gruppenzugehörigkeit (Arbeiter/Angestellte) | 2 – 7, 9, 15, 16, 21, 22 | Nein |
| 29 | Kammerzugehörigkeit | 2, 5, 16, 21, 22 | Nein |
| 30 | Sicherheitsstufe / Zugangs- (Zugriffs-)rechte | 4, 5, 21, 22 | Vertraulich |
| 31 | Lichtbild des Betroffenen (für Ausweiskarten) | 4, 5, 21, 22 | Nein |
| 32 | Gültigkeitsdauer der Ausweiskarte | 4, 5, 21, 22 | Nein |
| 33 | Arbeitszeiterfassung | 4, 5, 21, 22 | Nein |
| 34 | Sonstige Daten zur Arbeitszeit (insbesondere Geringfügigkeit, Arbeitsstunden, Überstunden, Gleitzeit, Nacht- und Teilzeitarbeit) | 2, 4 – 7, 9, 10, 12, 21, 22 | Nein |
| 35 | Daten zur Urlaubsverwaltung | 3 – 5, 9, 10, 21, 22 | Nein |
| 36 | Religionsbekenntnis (zur Abwesenheitsverwaltung) | 4, 5, 21, 22 | nach Angabe des BetroffenenArt 9 |
| 37 | Krankenstand, einschließlich Arbeitsunfall und Berufskrankheit (Beginn, Ende und Dauer) | 2 – 5, 10, 18, 19, 21, 22 | Art 9 |
| 38 | Zeitpunkt eines Arbeitsunfalls | 2 – 5, 10, 18, 19, 21, 22 | Art 9 |
| 39 | Kuraufenthalte | 2 – 5, 10, 18, 19, 21, 22 | Art 9 |
| 40 | Mutterschutz (Beginn und Ende) | 2 – 5, 9, 10, 18, 19, 21, 22 | Art 9 |
| 41 | Karenzurlaub gemäß MSchG und EKUG (Beginn und Ende) | 2 – 5, 9, 10, 15, 18, 19, 21, 22 | Art 9 |
| 42 | Präsenzdienst, Ausbildungsdienst oder Zivildienst (Beginn und Ende) | 2 – 5, 9, 10, 15, 19, 21, 22 | Nein |
| 43 | Art und Dauer der sonstigen Abwesenheit wegen Dienstverhinderung oder Dienstfreistellung (einschließlich vereinbarte Karenzierung) | 2 – 5, 9, 10, 19, 21, 22 | Nein |
| 44 | Daten zur Entgeltfortzahlung | 2 – 5, 10, 19, 21, 22 | Nein |
| 45 | Beschäftigungsrelevante Daten gemäß Arbeit- nehmerInnenschutzgesetz, [BGBl. Nr. 450/1994](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1994_450_0/1994_450_0.pdf) idgF., Bazillenausscheidergesetz, [BGBl. Nr. 153/1945](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1945_153_0/1945_153_0.pdf) idgF., Tuberkulosegesetz, [BGBl. Nr. 127/1968](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1968_127_0/1968_127_0.pdf) idgF. und ähnlichen Rechtsvorschriften | 4 – 7, 18, 21, 22 | Art 9 |
| 46 | Grad der Behinderung gemäß Behinderteneinstellungsgesetz (nach Bekanntgabe des Betroffenen) | 2 – 5, 9, 11, 15, 21, 22 | Art 9 |
| 47 | Gesetzliche, kollektivvertragliche, betriebsvereinbarungsmäßige und einzelvertragliche Grundlagen der Entgeltberechnung (Einstufung) | 2, 4 – 5, 8, 9, 10, 19, 21, 22 | Nein |
| 48 | Brutto- und Nettoentgelt (Daten des Gehaltszettels) | 1, 2, 4, 5, 9, 10, 12, 14, 19, 21, 22 | Vertraulich |
| 49 | Daten der Entgeltsfortzahlung | --- | Nein |
| 50 | Abzüge vom Nettoentgelt auf Grund Gesetzes oder betrieblicher Vereinbarungen | 13 – 14, 17, 19, 21, 22 | Nein |
| 51 | Sachbezüge | 1, 2, 4, 5, 10, 12, 21, 22 | Nein |
| 52 | Aufwandsentschädigungen (wie Reisegebühren) | 1, 2, 4, 5, 10, 12, 14, 19, 21, 22 | Nein |
| 53 | Sozialleistungen im Zusammenhang mit dem Arbeitsverhältnis | 2, 4, 5, 12, 14, 21, 22 | Nein |
| 54 | Daten nach Bezügebegrenzungsgesetz, [BGBl. I Nr. 64/1997](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1997_64_1/1997_64_1.pdf) idgF. | 20, 21, 22 | Nein |
| 55 | Höhe des Gewerkschaftsbeitrages und Bezeichnung und Adresse des Empfängers  | 14, 15, 21, 22 | nach Bekanntgabe des BetroffenenArt 9 |
| 56 | Versicherungsprämien als Leistung des Arbeitgebers | 4, 5, 13, 14, 21, 22 | Vertraulich |
| 57 | Verwaltung von Vorschüssen und Darlehen | 1, 14, 21, 22 | Vertraulich |
| 58 | Lohnpfändungsdaten | 1, 4, 5, 21, 22 | Vertraulich |
| 59 | Daten des Lohnzettels (L – 16 Formular) | 10, 12, 21, 22 | Vertraulich |
| 60 | Alleinverdiener- oder Alleinerzieher-Absetzbetrag (ja/nein) | 2, 12, 21, 22 | Nein |
| 61 | Wohnsitzfinanzamt | 21, 22 | Nein |
| 62 | Daten zur Pensionskasse (insbesondere Ein- und Austritt, Beitragsdaten und Versicherungszeiten in der gesetzlichen Sozialversicherung im Zeitraum der Beschäftigung) | 5, 12, 14, 19, 21, 22 | Nein |
| 63 | Daten zur Verwendung von Dienstfahrzeugen (insbesondere Führerschein, Abrechnungen, Schadensfälle, Versicherungen) | 4, 5, 13, 21, 22 | Nein |
| 64 | Besondere Qualifikationen (z. B. Gewerbeschein, besondere Ausbildung) | 4, 5, 7, 21, 22 | Nein |
| 65 | Nebenbeschäftigungen | 20, 21, 22 | Vertraulich |
| 66 | Daten nach dem Berufsausbildungsgesetz, [BGBl. Nr. 142/1969](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1969_142_0/1969_142_0.pdf) idgF., und einschlägigen kollektivvertraglichen Regelungen bei Lehrlingen, insbesondere Lehrvertragsdaten und sonstige Daten aus dem Ausbildungsverhältnis und Berufsschulbesuch | 4, 5, 8, 9, 16, 21, 22 | Nein |
| 66a | Schwerarbeitszeiten | 2 | Nein |
| 2. Bewerber als Mitarbeiter | 67 | Ordnungszahl(en) | 21, 22 | Nein |
| 68 | Name  | 21, 22 | wenn vom Betroffenen angegeben |
| 69 | Geburtsdatum | 21, 22 | wenn vom Betroffenen angegeben |
| 70 | Staatsbürgerschaft  | 21, 22 | wenn vom Betroffenen angegeben |
| 71 | Geschlecht  | 21, 22 | wenn vom Betroffenen angegeben |
| 72 | Anschrift  | 21, 22 | wenn vom Betroffenen angegeben |
| 73 | Telefonnummer  | 21, 22 | wenn vom Betroffenen angegeben |
| 74 | E-Mail-Adresse  | 21, 22 | wenn vom Betroffenen angegeben |
| 75 | Lichtbild) | 21, 22 | wenn vom Betroffenen angegeben |
| 76 | Ausbildungsdaten  | 21, 22 | wenn vom Betroffenen angegeben |
| 77 | Berufserfahrung und Lebenslauf  | 21, 22 | wenn vom Betroffenen angegeben |
| 78 | Angestrebte Beschäftigung  | 21, 22 | wenn vom Betroffenen angegeben |
| 79 | Beginn der angestrebten Beschäftigung  | 21, 22 | wenn vom Betroffenen angegeben |
| 80 | Sprachkenntnisse | 21, 22 | wenn vom Betroffenen angegeben |
| 81 | Spezielle Berufserfordernisse | 21, 22 | Nein |
| 82 | div. Testergebnisse | 21, 22 | Vertraulichbzw. Art 9 |

### Löschungs- und Aufbewahrungsfristen

|  |  |
| --- | --- |
| **Daten (Lfd. Nr.)** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** |
|  |  |
| 1 - 66 | Bis zur Beendigung der Beziehung mit dem Betroffenen und darüber hinaus solange als gesetzliche Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 bestehen somit auf jeden Fall **7 Jahre** oder solange Rechtsansprüche aus dem Arbeitsverhältnis gegenüber dem Arbeitgeber geltend gemacht werden können |
| 67- 82 | Die von den Bewerbern zur Verfügung gestellten Daten, können im Fall einer erfolgreichen Bewerbung für die Zwecke des Beschäftigungsverhältnisses von uns weiterverarbeitet werden. Andernfalls, sofern die Bewerbung auf ein Stellenangebot nicht erfolgreich ist, werden die Daten der Bewerber gelöscht. Die Daten der Bewerber werden ebenfalls gelöscht, wenn eine Bewerbung zurückgezogen wird, wozu die Bewerber jederzeit berechtigt sind.Die Löschung erfolgt, vorbehaltlich eines berechtigten Widerrufs der Bewerber, nach dem Ablauf eines Zeitraums von **sechs Monaten**, damit wir etwaige Anschlussfragen zu der Bewerbung beantworten und unseren Nachweispflichten aus dem Gleichbehandlungsgesetz genügen können.  |
| Dienstzeugnis | Anspruch auf Ausstellung eines Dienstzeugnisses nach § 1163 iVm § 1478 ABGB: **30 Jahre** |

Weitere Fristen für Personalwesen, siehe <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html>

#### Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lf. Nr** | **Empfängerkategorien**  | **Drittstaat (Angabe des Drittstaats, d.h. außerhalb der EU)** | **Internationale Organisation** |
| 1 | Gläubiger des Betroffenen sowie sonstige an der allenfalls damit verbundenen Rechtsverfolgung Beteiligte, auch bei freiwilligen Gehaltsabtretungen für fällige Forderungen; | Nein | Vertraulich |
| 2 | Sozialversicherungsträger (einschließlich Betriebskrankenkassen); | Nein | Nein |
| 3 | Wahlvorstand für Betriebsratswahlen; | Nein | Nein |
| 4 | Arbeitsinspektorat, Verkehrs-Arbeitsinspektion und Land- und Forstwirtschaftsinspektion, insbesondere gemäß § 8 Arbeitsinspektionsgesetz; | Nein | Nein |
| 5 | Organe der betrieblichen Interessensvertretung (insbesondere Betriebsrat gemäß § 89 Z 4 ArbVG, Sicherheitsvertrauensperson nach § 10 ArbeitnehmerInnenschutzgesetz (ASchG), [BGBl. Nr. 450/1994](http://www.ris.bka.gv.at/Dokumente/BgblPdf/1994_450_0/1994_450_0.pdf) idgF., Jugendvertrauensperson gemäß § 125ff ArbVG und Behindertenvertrauensperson gemäß § 22a Behinderteneinstellungsgesetz); | Nein | Nein |
| 6 | Gemeindebehörden in verwaltungspolizeilichen Agenden; | Nein | Nein |
| 7 | Bezirksverwaltungsbehörde in verwaltungspolizeilichen Agenden (Gewerbebehörde, Zuständigkeiten nach ASchG, usw.); | Nein | Nein |
| 8 | Lehrlingsstelle gemäß § 19 Berufsausbildungsgesetz und Berufsschulen; | Nein | Nein |
| 9 | Arbeitsmarktservice; | Nein | Nein |
| 10 | Bauarbeiter- Urlaubs- und -Abfertigungskasse; | Nein | Nein |
| 11 | Bundesamt für Soziales und Behindertenwesen (Bundessozialamt) z. B. gemäß § 16 Behinderteneinstellungsgesetz; | Nein | Nein |
| 12 | Finanzamt; | Nein | Nein |
| 13 | Versicherungsanstalten im Rahmen einer bestehenden Gruppen- oder Einzelversicherung; | Nein | Nein |
| 14 | mit der Auszahlung an den Betroffenen oder an Dritte befasste Banken; | Nein | Nein |
| 15 | vom Dienstnehmer angegebene Gewerkschaft, mit Zustimmung des Betroffenen; | Nein | Nein |
| 16 | gesetzliche Interessensvertretungen; | Nein | Nein |
| 17 | Betriebsratsfonds gemäß § 73 Abs. 3 ArbVG; | Nein | Nein |
| 18 | Betriebsärzte; | Nein | Nein |
| 19 | Pensionskassen; | Nein | Nein |
| 20 | Rechnungshof; | Nein | Nein |
| 21 | Rechtsvertreter; Wirtschaftstreuhand, externe Buchhalter | Nein | Nein |
| 22 | Gerichte; | Nein | Nein |
| 23 | Mitversicherte; | Nein | Nein |
| 24 | Mitarbeitervorsorgekassen (MVK) gemäß § 11 Abs. 2 Z 5 und § 13 BMVG; | Nein | Nein |
| 25 | Kunden und Interessenten des Auftraggebers | Nein | Nein |
| 26 | Provider, IT-Dienstleister inklusive Fernwartung | Nein | Nein |

Wenn EU-Ausland bitte die notwendigen Sicherheitsmaßnahmen usw angeben

### *Technisch-organisatorische Maßnahmen*

Da hier auch sensible Daten nach Art 9 DSGVO (Gesundheitsdaten, Religion, Gewerkschaft der Mitarbeiter) verarbeitet werden, bestehen die TOMs insbesondere in der Verschlüsselung am Datenträger (encryption of data in rest), bei der Übertragung (data in motion) vom und zum Kunden/Auszubildenen/Vortragenden bzw anderen Empfängern und Backup!

Hier die Mindesterfordernisse:

### **Vertraulichkeit**

1. **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Betrieb mit Schlüssel und Sicherheitsschloss, nur über Anmeldung vorab, Alarmanlage, ...
2. **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung mit Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Data in Rest und Motion und somit keine Weiterleitung ohne sichere und verschlüsselter Übertragung.

Folgende Methode/Prozesse wurden für die Verschlüsselung der Daten in Rest gewählt: …………………………………………….

Folgende Methode/Prozesse wurden für die verschlüsselte und sichere Übertragung (in Motion) von Daten und Dateien gewählt:…………………………………………….
3. **Zugriffskontrolle**: Zugriff nur durch Verantwortlichen/Personalwesen-Zuständige/...

### **I****ntegrität**

1. **Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen/Personalwesen-Zuständige/... eingegeben, verändert oder entfernt, Dokumentenmanagement

### **Ve****rfügbarkeit**

1. **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, Sicherungskonzept mit verschlüsselter Lagerung der Sicherungen.
Folgende Maßnahmen wurden getroffen: …………………………………………….

### **Rasche Wiederherstellbarkeit:**

Ein Backup-Konzept wie folgt wurde erstellt: ……………………………………………

# **Auftragsverarbeitungsvereinbarungen**

Bitte hier alle Verträge bzw Links zu deren AGBs usw für alle ihre Auftrags/Datenverarbeiter eintragen:

|  |  |  |  |
| --- | --- | --- | --- |
| **Zweck** | **Firma** | **Vertrag archiviert** | **Bemerkungen**zB Link, AGBs |
| Homepage-Hoster |  |  |  |
| Newsletter Extern |  |  |  |
|  |  |  |  |
|  |  |  |  |
| IT mit Fernwartung |  |  |  |

# Impressum und Statuten

**Impressum** sowie **Datenschutzerklärung** als Link - von jeder Seite erreichbar - auf der Homepage

**Statuten** sowie **Regelungen betreffs Ausbildung** sollen unbedingt auch auf einer eigenen Unterpage veröffentlicht sein.

Die Datenschutzerklärung als Link wird in allen unseren Emails im Footer, bei Anboten und allen Erstinformationen für Auszubildende verwendet.

# Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

## Kontaktaufnahme

Wenn ein potentielles Vereinsmitglied bzw Auszubildender von seiner Seite mit uns per Email oder telefonisch Kontakt aufnimmt, so dürfen wir dessen Namen, Kontaktdaten, Interesse an Vereinsaktivitäten zur Durchführung vorvertraglicher Maßnahmen (Vereinsmitgliedschaft, Ausbildung) verarbeiten (siehe Art 6 (1) b DSGVO ... auf Anfrage der betroffenen Person ...). Sollte es zu keiner Mitgliedschaft/Ausbildung kommen, so werde wir diese Daten nach 2 Jahren löschen.

## Fotos bei Vereinsveranstaltungen

Wie wir als Verein mit dem Fotografieren bei Veranstaltungen umgehen, finden Sie hier:
<https://www.dataprotect.at/2018/05/15/verwendung-von-fotos-von-veranstaltungen-nach-dem-25-05-2018/> , wobei wir ergänzend hinzufügen wollen, dass wir das Fotografieren auch zeitlich und/oder örtlich eingrenzen, denn es sollten auch Leute auf unsere Veranstaltungen kommen können, die nicht unbedingt fotografiert werden wollen!

**Zeitlich**: Nur von 19 bis 20 Uhr oder nur bei der Verleihung oder ….

**Örtlich**: Bei Ausstellungen zb nur in den markierten Räumen oder bei Vorträgen, ..nur bis in die ersten 10 Reihen oder ……..

## Selbstschutz

Wir versuche unser Such- und Surfverhalten soweit wie möglich „sicher“ zu gestalten und verwenden daher zB den europäischen Open Source Browser <https://cliqz.com/> inklusive Ghostery (verhindert und zeigt mir die Trackingversuche) und zB die europäische Suchmaschine: [https://www.startpage.com](https://www.startpage.com/) statt Google .

## Clear Desk Policy

Unter der Clear Desk Policy versteht man, dass Mitarbeiter und Funktionäre alle vertraulichen Dokumente, die sich auf ihrem Arbeitsplatz befinden, verschließen. Unberechtigte Personen (Reinigungspersonal, unbefugte Kolleginnen und Kollegen, oder Besucher) dürfen keinen Zugriff darauf erhalten.

Bitte beachten sie folgende Punkte:

* Bei Verlassen des Arbeitsplatzes müssen alle Ausdrucke, Kopien oder dergleichen so verstaut werden, dass diese Dokumente nicht für Dritte zugänglich sind (Schreibtisch, versperrbaren Kästen, Datenträgersafe).
* Lassen sie keine Ausdrucke im Drucker/Kopierer liegen.
* Bewahren sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf.
* Sperren sie Ihren Computer, wenn sie Ihren Arbeitsplatz verlassen (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.

## Umgang mit mobilen IT-Geräten

Mobile IT Geräte (Notebooks, Smartphones...) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar. Portable Geräte sind für Diebe ein attraktives Ziel.

Bitte beachten sie folgende Punkte:

* Lassen sie das Gerät nicht unbeaufsichtigt.
* Überlassen sie das Gerät nicht anderen Personen.
* Achten sie bei Passworteingabe am Gerät auf ihren Sichtschutz – ähnlich wie bei einem Bankomaten.
* Verwenden sie ihren privaten Cloud-Speicher nicht für Unternehmensdaten.
* Installieren sie nur Anwendungen, die ihnen als vertrauenswürdig und sicher bekannt sind und von ihrer IT-Abteilung frei gegeben wurden.
* Melden sie einen Diebstahl oder Verlust sofort der IT-Abteilung.
* Achten sie auf eventuelle Daten- und Gesprächspaketvolumen um zusätzliche Kosten für das Unternehmen zu vermeiden.
* WhatsUp ist vom Datenschutz her als sehr unsicher zu betrachten und daher vom beruflichen Handy zu deinstallieren (Erstaz zB www.signal.org)

## Emails

In allen unseren Emails an Vereinsmitglieder und sonstige Personen - Newsletter, siehe dort - gibt es immer einen Link zu unserer Datenschutzerklärung

## Datengeheimnis

Funktionäre und Mitarbeiter sind geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet (siehe Schulung)

## Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Wir raten die **X als Mindeststandart sofort anzugehen** und für die anderen Punkte einen **Zeitplan mit IT extern/intern zu erstellen.**

|  |  |  |  |
| --- | --- | --- | --- |
| ? | Alarmanlage |  | Absicherung von Gebäudeschächten |
| X | Rücksicht beim Aufrufen der Kunden bzw Auszubildenen |  | Chipkarten-/Transponder-Schließsystem |
|  | Schließsystem mit Codesperre |  | Manuelles Schließsystem |
|  | Automatisches Zugangskontrollsystem |  | Videoüberwachung der Zugänge |
|  | Lichtschranken / Bewegungsmelder | X | Sicherheitsschlösser – auch bei Aktenkästen |
| X | Schlüsselregelung (Schlüsselausgabe etc.) |  | Personenkontrolle beim Pförtner / Empfang |
|  | Protokollierung der Besucher |  | Sorgfältige Auswahl von Reinigungspersonal |
| X | Bildschirmsperre nach 10 Minuten |  | Tragepflicht von Berechtigungsausweisen |
| X | Verschlossene Türen bei Abwesenheit |  | Fenstersicherung (Erdgeschoss) |

## Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

|  |  |  |  |
| --- | --- | --- | --- |
| X | Zuordnung von Benutzerrechten | X | Erstellen von Benutzerprofilen |
| X | Passwortvergabe |  | Authentifikation mit biometrischen Verfahren |
| X | Authentifikation mit Benutzername / Passwort |  | Zuordnung von Benutzerprofilen zu IT-Systemen |
|  | Gehäuseverriegelungen |  | Einsatz von VPN-Technologie |
|  | Sperren von externen Schnittstellen (USB etc.) | X | Sicherheitsschlösser |
| X | Schlüsselregelung (Schlüsselausgabe etc.) |  | Personenkontrolle beim Pförtner / Empfang |
|  | Protokollierung der Besucher |  | Sorgfältige Auswahl von Reinigungspersonal |
|  | Eigenes Handy für Verein |  | Tragepflicht von Berechtigungsausweisen |
| X | Einsatz von Intrusion-Detection-Systemen | X | Verschlüsselung von mobilen Datenträgern |
| X | Verschlüsselung von Smartphone-Inhalten | X | Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)Bei A1, Drei usw nachfragen! |
| X | Einsatz von Anti-Viren-Software | X | Verschlüsselung von Datenträgern in Laptops / Notebooks / USB |
| X | Einsatz einer Hardware-Firewall | X | Einsatz einer Software-Firewall |

## Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung, hier nur der Verantwortliche. unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

|  |  |  |  |
| --- | --- | --- | --- |
| X | Erstellen eines Berechtigungskonzepts |  | Verwaltung der Rechte durch Systemadministrator |
|  | Anzahl der Administratoren auf das „Notwendigste“ reduziert | X | Passwortlänge, Passwortwechsel |
| X | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | X | Sichere Aufbewahrung von Datenträgern(Data-Safe) |
| X | physische Löschung von Datenträgern vor Wiederverwendung(extern nur mit Datenverarbeitungsvereinbarung) | X | ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
|  | Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) |  | Protokollierung der Vernichtung |
| X | Verschlüsselung von Datenträgern |  |  |

## Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Einrichtungen von Standleitungen bzw. VPN-Tunneln |  | Weitergabe von Daten in anonymisierter oder pseudonymisierter Form=> siehe Verarbeitungsverzeichnis |
| X | E-Mail-Verschlüsselungsichere verschlüsselter Upload von Datein | X | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen=> siehe Verarbeitungsverzeichnis |
| X | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen => siehe Verarbeitungsverzeichnis |  | Beim physischen Transport: sichere Transportbehälter/-verpackungen |
|  | Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen | X | Verschlüsselung der übertragenen Daten |

## Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

|  |  |  |  |
| --- | --- | --- | --- |
| X | Protokollierung der Eingabe, Änderung und Löschung von Daten | X | Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.=> siehe Verarbeitungsverzeichnis |
| X | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | X | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| X | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |  |  |

## Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Hier kommt die **Datenverarbeitungs-Vereinbarung nach Art 28 DSGVO** zum Tragen, somit alles ankreuzen, siehe Anhang

|  |  |  |  |
| --- | --- | --- | --- |
| X | Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)Sollte eine Dokumentation gemäß DSGVO vorweisen können! | X | vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| X | schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) siehe Anhang | X | Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis |
|  | Auftragnehmer hat Datenschutzbeauftragten bestellt | X | Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| X | Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | X | laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |
| ? | Vertragsstrafen bei Verstößen |  |  |

## Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unterbrechungsfreie Stromversorgung (USV) |  | Klimaanlage in Serverräumen |
|  | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen |  | Schutzsteckdosenleisten in Serverräumen |
| X | Feuer- und Rauchmeldeanlagen | X | Feuerlöschgeräte (in Serverräumen) |
|  | Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | X | Erstellen eines Backup- & Recoverykonzepts |
| X | Testen von Datenwiederherstellung |  | Erstellen eines Notfallplans |
| X | Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort |  | Serverräume nicht unter sanitären Anlagen |
|  | In Hochwassergebieten: Serverräume über der Wassergrenze |  |  |

## Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

|  |  |  |  |
| --- | --- | --- | --- |
|  | physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern |  | Logische Mandantentrennung (softwareseitig) |
| X | Erstellung eines Berechtigungskonzepts | X | Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
| X | Versehen der Datensätze mit Zweckattributen/Datenfeldern=> siehe Verarbeitungsverzeichnis bzw Risikoanalyse | X | Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System=> siehe Verarbeitungsverzeichnis |
| X | Festlegung von Datenbankrechten |  | Trennung von Produktiv- und Testsystem |

Quelle unter anderem: [https://www.datenschutz-guru.de/files/**Ausfuellhilfe\_TOM\_9\_BDSG\_V2**.docx](https://www.datenschutz-guru.de/files/Ausfuellhilfe_TOM_9_BDSG_V2.docx)

## Regelmäßigen Überprüfung, Bewertung und Evaluierung

* Risikoanalyse
* Datenschutzfreundliche Voreinstellungen
* Weiterbildung siehe Schulung

## Auftragskontrolle:

Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, sichere und verschlüsselte Speicherung und Übertragung, ( zB. Ob Datenschutzbeauftragter und/oder Dokumentation nach DSGVO vorhanden, Vorabüberzeugungspflicht, Nachkontrollen)

### Ein Kontroll- und Verbesserungsprozess wir mindestens 1x jährlich durchgeführt:

|  |  |
| --- | --- |
| **Jahr** | Ergebnisse der Überprüfung, Bewertung und Evaluierung |
| 2019 |  |
| 2020 |  |

Referenzen: Art 32 Z 1 DSGVO

# **Betroffenenrechte wahren**

Gemäß der DSGVO hat jeder Betroffene folgende Rechte:

* Recht auf Auskunft (Art 15 DSGVO)
* Recht auf Berichtigung (Art 16 DSGVO)
* Recht auf Löschung (Art 17 DSGVO )
* Recht auf Einschränkung (Art 18 DSGVO)
* Recht auf Übertragbarkeit (Art 20 DSGVO)
* Recht auf Widerspruch (Art 21 DSGVO)
* Recht auf Beschwerde bei der [Datenschutzbehörde](https://www.dsb.gv.at/rechte-der-betroffenen%22%20%5Cl%20%22Zustaendigkeit_der_Datenschutzbehoerde)

## Prozess betreffs Betroffenenrechte

### Recht auf Auskunft

Gemäß Art 15 hat die betroffene Person das Recht, von den Verantwortlichen eine Bestätigung darüber zu verlangen, ob personenbezogene Daten über sie vom Verantwortlichen verarbeitet werden. Sollte dies der Fall sein, hat die betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten und darüber hinaus auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Sollten personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt werden, so hat die betroffene Person darüber hinaus das Recht, über die geeigneten Garantien gemäß Art 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden. Sollte die betroffene Person dies wünschen, stellt Die verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, dem Betroffenen zur Verfügung.

Für jede weitere Kopie, die die betroffene Person beantragt, kann Die Verantwortliche ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen. Dieses Recht hat der Betroffene allerdings nur aufgrund unbegründeter oder exzessiver Ausübung des Rechts auf Auskunft.

Die betroffene Person hat das Recht den Antrag elektronisch zu stellen. In diesem Fall sind die Informationen in einem gängigen elektronischen Format (gesichert) zur Verfügung zu stellen, sofern die betroffene Person nichts Anderes angibt.

**In Entsprechung dieser Verpflichtungen wird Die verantwortliche das Auskunftsrecht der betroffenen Person wie folgt handhaben:**

Sobald der Betroffene einen Antrag auf Auskunft an den Verantwortlichen stellt, wird der Ansprechpartner des Verantwortlichen alle vertretbaren Mittel nutzen, um die Identität der betroffenen Person zu überprüfen. Der Antrag der betroffenen Person bedarf keiner besonderen Form und darf auch elektronisch erfolgen.

Der Antrag muss dem Verantwortlichen aber ermöglichen, die Informationen herauszufinden, die er beauskunften soll. Für die Beauskunftung ist beim Verantwortlichen **der Ansprechpartner** zuständig.

Sollte der Betroffene eine **mündliche Auskunft** verlangen, so wird der Zuständige die Identität des Betroffenen in geeigneter Weise feststellen und die Auskunft ebenso mündlich erteilen. Der Zuständige wird sämtliche Datenbestände nach Informationen, die die betroffene Person betreffen, durchsuchen und diese Informationen zusammenstellen.

Der Ansprechpartner wird sämtliche Datenbestände, in denen personenbezogene Daten über den Betroffenen zu finden sind, zusammenstellen und – sofern diese inhaltlich unübersichtlich sind – kurz erläutern.

 **Die Auskunft wird folgende Informationen umfassen:**

- **Verarbeitete Daten:** Die Verantwortliche wird die betroffene Person darüber informieren, welche Informationen er über die Person verarbeitet.

- **Informationen:** Darüber hinaus wird Die Verantwortliche der betroffenen Person folgende Informationen über die Datenverarbeitung zur Verfügung stellen:

* die Zwecke der Verarbeitung
* Datenkategorien
* Empfänger und Kategorien von Empfängern
* Dauer der Datenspeicherung
* Herkunft der Daten
* Sollte eine automatisierte Entscheidungsfindung und Profiling erfolgt sein, die Methoden und Kriterien sowie die Tragweite und Auswirkungen der Datenverarbeitung

 - **Betroffene Rechte:** Die verantwortliche wird die betroffene Person über Folgendes informieren:

*„Die betroffene Person hat das Recht auf Auskunft über die gespeicherten Daten gemäß Art 15 DSGVO, auf Berichtigung unzutreffender Daten gemäß Art 16 DSGVO, auf Löschung von Daten gemäß Art 17 DSGVO, auf Einschränkung der Verarbeitung von Daten gemäß Art 18 DSGVO, auf Widerspruch gegen die unzumutbare Datenverarbeitung gemäß Art 21 DSGVO sowie auf Datenübertragbarkeit gemäß Art 20 DSGVO.*

*Der Betroffene hat das Recht, sich bei der Aufsichtsbehörde zu beschweren – zuständig ist in Österreich die Datenschutzbehörde.“*

Die Verantwortliche wird – sofern der Betroffene dies wünscht – die personenbezogenen Daten, die die betroffene Person betreffen, dieser so zur Verfügung stellen, dass diese in einem strukturierten, gängigen und maschinenlesbaren Format vorliegen.

Der Betroffene soll so die Möglichkeit haben, die Daten einem anderen Verantwortlichen ohne Behinderung zu übermitteln.

**Frist:**

Die Verantwortliche wird die Auskunft unverzüglich erteilen, jedenfalls binnen eines Monats ab Eingang beim Verantwortlichen. Sollte es sich um eine umfangreiche und komplexe Auskunft handeln, kann Die Verantwortliche im Einzelfall die Frist zur Beauskunftung einmalig um weitere zwei Monate verlängern. Die Verantwortliche wird dies unter Nennung der Gründe dem Betroffenen binnen eines Monats mitteilen.

**Negativauskunft:**

Sollte Die Verantwortliche die Beauskunftung nicht erteilen, wird er dies ebenso binnen eines Monats unter Angabe von Gründen dem Betroffenen mitteilen.

Sollte Die Verantwortliche keine Daten über die betroffene Person verarbeiten, wird Die Verantwortliche eine Negativauskunft (eine Bestätigung, dass er keine Daten über den Betroffenen verarbeitet) dem Betroffenen übermitteln.

### Recht auf Berichtigung

Sollte der Betroffene den Verantwortlichen darüber informieren, dass dieser unrichtige oder (für den Zweck der Datenverarbeitung) unvollständige Daten verarbeitet, hat der Betroffene das Recht, sich an den **Ansprechpartner** beim Verantwortlichen zu melden. Dieser wird die von der betroffenen Person bekanntgegeben Daten unverzüglich inhaltlich prüfen und gegebenenfalls vervollständigen bzw. richtigstellen.

Sollte die Korrektheit der Daten strittig sein, wird Die Verantwortliche die Verarbeitung einschränken (siehe dazu unten).

Weiters wird Die Verantwortliche etwaige Empfänger der (unrichtigen) Daten über die berichtigten Daten informieren.

### **Recht auf Löschung**

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass betreffende personenbezogene Daten unverzüglich gelöscht werden. Die Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig;

- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützt und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;

- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor;

- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet;

- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich;

- Bei den personenbezogenen Daten handelt es sich um die Daten eines Kindes in Bezug auf angebotene Internetdienste.

Die Verantwortliche wird jedes Löschungsbegehren umgehend prüfen und mit zumutbarem Aufwand die Voraussetzungen des Anspruchs prüfen.

Die Verantwortliche wird die betroffene Person jedenfalls innerhalb eines Monats nach Eingang des Antrags über die ergriffenen Maßnahmen bzw. über die Gründe der Ablehnung informieren. Gegebenenfalls wird Die Verantwortliche den Betroffenen – sofern es sich um ein komplexes Begehren handelt – über die Verlängerung der Prüfung des Löschungsbegehrens um zwei Monate ebenso binnen eines Monats informieren.

Sollte die betroffene Person einen Widerspruch erhoben haben, und hat die betroffene Person vom Verantwortlichen die Einschränkung der Verarbeitung verlangt, wird Die Verantwortliche die Verarbeitung einschränken (siehe dazu unten).

### **Recht auf Einschränkung**

Die Verantwortliche wird die personenbezogenen Daten eines Betroffenen nur eingeschränkt verarbeiten, sofern:

 - die betroffene Person die Richtigkeit der personenbezogenen Daten bestritten hat (für die Dauer der Prüfung der Richtigkeit der personenbezogenen Daten durch den Verantwortlichen);

 - die Verarbeitung unrechtmäßig erfolgt und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

 - Die Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt;

 - die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Sollte die Verarbeitung eingeschränkt worden sein, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Personen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen Personen oder aus Gründen eines wichtigen öffentlichen Interesses – verarbeitet werden.

Die Verantwortliche wird die betroffene Person jeweils schriftlich über die ergriffenen Maßnahmen informieren.

Die Verantwortliche wird allen Empfängern, denen personenbezogene Daten offengelegt wurden, die Einschränkung der Verarbeitung mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Sofern die betroffene Person dies wünscht, wird Die Verantwortliche die betroffene Person über die Empfänger dieser Mitteilung informieren.

### **Recht auf Widerspruch**

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen, sofern die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde oder aber die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist.

Die Verantwortliche wird die Identität der betroffenen Person und anschließend – sollte die Identität einwandfrei nachgewiesen worden sein – den Widerspruch inhaltlich prüfen.

Im Anschluss wird Die Verantwortliche die betroffene Person über die Entscheidung informieren.

### **Meldung an die Behörde**

Die DSGVO definiert in Art 33 eine „Verletzung des Schutzes personenbezogener Daten“ (data breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet Die Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der österreichischen Datenschutzbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Meldung an die Behörde siehe Vorlage im Anhang

* + 1. **Meldung an den Betroffenen (siehe Risikoabschätzung)**

Hat die Verletzung des Schutzes personenbezogener Daten gemäß neuerlichen risikoanalyse voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt Die Verantwortliche die betroffene Person unverzüglich von der Verletzung.

## **Dokumentation**

Wir werden alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht, siehe Art 33 DSGVO.

# Profiling light

Wir in unserem Verein verarbeiten (siehe Verfahrensverzeichnis Marketing) teil-automatisiert auch personenbezogener Daten von natürliche Personen, um Art und Form der jeweilig in Anspruch genommenen Dienstleistung/Produkt, Interessen, Ort, Branche, …, Interesse dieser natürlichen Person, … zu kategorisieren und um im berechtigtes Interesse eine zielgerichtete Information und Betreuung (= simples Mitgliederprofil) sowie um eine personalisierte Direktwerbung (siehe E-Mail-Marketing) für unsere Mitglieder, Interessierten, Auszubildende, Lieferanten, Projektpartner zu ermöglichen.

Da nur eine teilautomatisierte und keine umfassende Bewertung persönlicher Aspekte natürlicher Personen, keine umfangreiche Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt und auch ausdrücklich damit keinerlei automatische Generierung von Einzelentscheidungen verbunden ist und es gänzlich ohne rechtliche oder ähnliche Wirkung für den Betroffenen ist, ist dies Verarbeitung daher nicht als Profiling im Sinne des DSGVO (siehe unten Referenzen), sondern als **[Profiling light](https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-betroffenenrechte-profiling-faq.html%22%20%5Cl%20%228)**, als **mitglieder**-**orientierte Service** zu sehen und es bedarf darüber hinaus auch keiner Datenschutz-Folgeabschätzung.

Referenzen: Art 4, Art 8, Art 9 DSGVO; Erwägungsgründe: 26ff, 51ff; § 4 Abs 4 DSGVO 2018

# E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO)

Vorab beachten wir die sogenannte Robinson-Liste und setzte ein Hackerl bei „Keine Zusendungen von Werbematerial, Newsletter erwünscht“ für alle natürlichen und juristischen Personen, die in dieser Liste ausdrücklich auf die Zusendung von Werbematerial sowie Werbemails verzichten, siehe <https://www.rtr.at/de/tk/TKKS_ECGListe> , Referenz: [§ 7 E-Commerce-Gesetz (ECG)](https://www.rtr.at/de/tk/WeitereGesetze)

Die Newsletter-Abonnenten, die ihre **klare Einwilligung nach Art 4 DSGVO nachweislich** abgegeben haben, werden hinreichend sowohl über Zweck, Art und Umfang der Datenverarbeitung als auch über ihre Rechte als Betroffene wie Recht auf Information, auf Auskunft und Richtigstellung, Widerspruchsrecht, auf Löschung und Einschränkung im E-Mail-Newsletter informiert.

Darüber hinaus gibt es in jedem E-Mail-Newsletter die einfache und rasche Möglichkeit für den Betroffenen, sich vom E-Mail-Newsletter abzumelden (mit einem automatisierten Email, dass er von der Newsletter-Liste gelöscht wurde).

Sollte dieses eMail-Newsletter-Tool von einem Dritten bereitgestellt sein, so gibt es dazu eine Vereinbarung mit diesem Auftragsverarbeiter nach Art 28 DSGVO (siehe Marketing-Verzeichnis bzw. Anhang). Einige Newletter-Anbieter fragen bei der Robinson-Liste automatisch nach

Individuelles Tracking der Newsletter, auch über eine Übermittlungs- bzw. Lesebestätigung, **wird nicht gemacht,** da dafür eine eigene Einwilligungserklärung notwendig wäre!

Macht ein Betroffener seine Rechte auf Widerspruch nicht mit Hilfe des Links im Newsletter geltend, sondern in einer anderen Form, sei es z. B. mündlich, schriftlich, per Email (insbesondere datenschutz@ [ihre domain] )so gilt folgendes:

Sollte der Betroffene mir Name des für den Datenschutz-Zuständigen nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:

„Sehr geehrte Frau/Herr …… !
Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie z. B. personenbezogen Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zukommen zu lassen. Diese Kopie wird sogleich nach Identitätsfeststellung gelöscht.
Ich danke Ihnen für Ihr Verständnis“

Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits sind notwendig.

Identität zweifelsfrei festgestellt und Verlangen ist rechtens
=> Der Betroffene bekommt betreffs Recht auf Widerspruch (Art 15 DSGVO) ehest möglich folgende Antworten:

„Sehr geehrte Frau/Herr ……!
Gemäß Ihrem Wunsch habe ich Sie hiermit von der Newsletter-Verteiler-Liste gelöscht. Sie erhalten keinen Newsletter oder Werbezusendungen von mir mehr.“

Referenzen: Art 4, Art 8, Art 9 DSGVO; Erwägungsgründe: 26ff, 51ff; § 4 Abs 4 DSG 2018; Recht auf Widerspruch Art 21 DSGVO

# Risikoanalyse

Referenzen: Art 24 + 25 DSGVO, Erwägungsgründe: 74-78, 81

## Risikoanalyse ohne Maßnahmen

Schutzziele für unsere Risikobewertung nach Art 4 Z 12 sind: Vertraulichkeit, Integrität und Verfügbarkeit. Die Risiko-Bewertung erfolgt nach „Schwere“ und „Eintrittswahrscheinlichkeit (EWK)“ (siehe Anleitung)

Folgende Daten wurden vorab analysiert und dann hier in die entsprechenden Kategorien eingetragen:

### Risikokategorien

|  |  |
| --- | --- |
| **Kategorie** | **pb Daten** |
| **1** | **Besondere Datenkategorien iSd Art 9 DSGVO (zB Mitarbeiter, Auszubildende)**Kinder unter 14 Jahren gem. Art 8, Fotos, Bitte ausfüllen**=> geheim/vertraulich** |
| **2** | Schlüssel, Passwörter, … , Vertragstext und Geschäftskorrespondenzen, sonstige VereinbarungenBitte ausfüllen**=> geheim** |
| **3** | Geburtsdatum , Bankverbindungen, Kreditkartennummern und -unternehmenBitte ausfüllen**=> intern/vertraulich** |
| **4** | Pb Daten mit vernachlässigbaren bis begrenzten Schutzbedarf, siehe oben VorabanalyseBitte ausfüllen |

### Risiko-Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Schwere** |  |  |  |  |  |
| Existenzgefährdend |  |  |  |  |  |
| Wesentlich |  |  |  | **1** |  |
| Begrenzt |  |  |  | **2 , 3** |  |
| Vernachlässigbar |  |  |  | **4** |  |
|  | Vernachlässigbar | Möglich | Sehr wahrscheinlich | Garantiert | **EWK** |

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

**Folgen ohne Maßnahmen:**

|  |
| --- |
| **Data Breach** |
| **Kein Risiko** | **Risiko** | **Hohes Risiko** |
|  | Datenschutzbehörde **UND** Betroffene informierenFolgeabschätzung notwendig |

### Maßnahmen

Siehe TOMs, insbesondere **Verschlüsselung am Datenträger (encryption of data in rest), bei der Übertragung (data in motion) und Backup!**

### Vertraulichkeit

**Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mit Schlüssel

**Zugangskontrolle**: Schutz vor unbefugter Systembenutzung mit Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Data in Rest und Motion und somit keine Weiterleitung ohne sichere und verschlüsselter Übertragung bzw. RSB - Einzelpraxis

**Zugriffskontrolle**: Zugriff nur durch Verantwortlichen - Einzelpraxis

### Integrität

**Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt, Dokumentenmanagement - Einzelpraxis

### Verfügbarkeit

**Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, Sicherungskonzept mit verschlüsselter Lagerung der Sicherungen

Rasche **Wiederherstellbarkeit**: Backup mindestens wöchentlich, am besten täglich

## Risiko-Matrix mit Maßnahmen

Bitte hier die Kategorien 1 - 4 gemäß Ihrer Maßnahmen eintragen!

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Schwere** |  |  |  |  |  |
| Existenzgefährdend |  |  |  |  |  |
| Wesentlich |  |  |  |  |  |
| Begrenzt |  | **1** |  |  |  |
| Vernachlässigbar | **4** | **2, 3**  |  |  |  |
|  | Vernachlässigbar | Möglich | Sehr wahrscheinlich | Garantiert | **EWK** |

### Folgen der Maßnahmen betreffs Risiko

|  |
| --- |
| **Data Breach** |
| **Kein Risiko** | **Risiko** | **Hohes Risiko** |
|  | Datenschutzbehörde informieren |  |
| **Betroffene sind nicht zu informieren**Keine Folgenabschätzung notwendig |

Aufgrund der gesetzten TOMs muss bei einem Data Breach der Betroffene höchstwahrscheinlich nicht informiert werden, **nichts desto trotz muss eine neuerliche Risikoanalyse gemacht** und die Behörde bei Data Breach mit Risiko für pb Daten informiert werden. Sollte es bei der neuerlichen Risikoanalyse bei dieser bekannt gewordenen Datenschutzverletzung zu einem hohen Risiko für die Betroffenen kommen, so müssen auch sie informiert werden **– innerhalb von 72 Stunden!**

Referenzen: Art 22 + 35 DSGVO, Erwägungsgründe: 76, 84 und 89 – 93, Working Paper 240 der Art 29 Gruppe

# Zusammenfassung und GV-/Vorstands-Beschluss

Wir sehe das hier dokumentierte Datenschutzniveau mit den gesetzten TOMs für uns als Verein auch aufgrund unserer finanziellen, technischen und organisatorischen Beschränkungen als **angemessen und ausreichend** an.

*Liebe Mitglieder!*

*Vertrauen zwischen den Vereinsmitgliedern und den Funktionären ist die Grundlage und Voraussetzung für unsere Vereinstätigkeit, daher sind auch alle Ihre persönlichen und beruflichen Daten bei uns in guten Händen.*

 *Wir sichern Ihnen zu, dass wir sorgsam und streng vertraulich damit umgehe und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen sind.*

*Das hier vorliegende Datenschutzkonzept unseres Vereines wurde von der a.o. Generalversammlung am ……... 2018 mit Stimmen dafür: mit Stimmen dagegen: mit Enthaltungen: angenommen/abgelehnt.*

***oder***

*Das hier vorliegende Datenschutzkonzept unseres Vereines wurde vom gesamten Vorstand einstimmig am ……… angenommen (und wird später der Generalversammlung auch am …… vorgelegt.)*

……………………………………………………………...
Unterschrift
Obfrau/-mann

oder der Funktionäre gemäß Statuten

# Anhang

## Einwilligung für Newsletter (Homepage)

 **Und hier können Sie unseren Newsletter kostenlos abonnieren:**

Geben Sie einfach Ihre E-Mail-Adresse an:

*Hinweise:*
Ihre E-Mail-Adresse wird nur für den Zweck der Erbringung dieses Newsletters verwendet. Ihre E-Mail-Adresse wird aber niemals für Werbezwecke an Dritte weitergegeben.

E-Mail-Adresse\*

Einwilligung\*

 Ja, ich möchte Informationen über Zweck vom Verein Name bequem per E-Mail zugesendet bekommen. Die Datenschutzhinweise habe ich vorab zur Kenntnis genommen Mir ist bekannt, dass die Datenverarbeitung bei dem Newsletter-Dienstleister: Name erfolgt.

**ABSENDEN**

Wichtige Hinweise:
Bitte lesen Sie sich unsere detaillierten Datenschutzerklärung durch. Sie können diese Einwilligung jederzeit widerrufen , indem Sie sich aus der Liste abmeldest (Hinweise zur Abmeldung sind in jeder E-Mail enthalten) oder sich einfach an uns per email wenden.

## Kontaktformular (Homepage)

Vorname
Name
Email\*
Telefon
Adresse
Betreffs:
Bemerkungen

Die Daten, die über das Kontaktformular übermittelt werden, werden nur zum Zweck der Anfrage und ihrer Bearbeitung gespeichert und verarbeitet (Vorvertraglich im Sinne des Art 6 (1) b) DSGVO). Sollte doch keine Vertrag zu Stande kommen, werden die Daten für den Fall von Anschlussfragen bei uns für 2 Jahre gespeichert und danach gelöscht, siehe auch unsere Datenschutzerklärung.

## Vorlage für Messen, Vereinslokal, Vereinsaktivitäten,

Logo/Verein

INTERESSENTEN ANFRAGE\*

|  |  |
| --- | --- |
| Vorname  |  |
| Nachname |  |
| Straße |  |
| PLZ und Ort |  |
| Telefon |  |
| Email |  |

Bemerkungen:

|  |
| --- |
|  |

\* Die Daten, die hier in der Anfrage durch die betroffenen Person auf der Messe freiwillig eingetragen wurden, werden nur zum Zweck der Anfrage und ihrer Bearbeitung verarbeitet und sind für die Durchführung vorvertraglicher Maßnahmen im Sinne des Art 6 (1) b) DSGVO wie zB Zusendung von Produkt- und/oder Geschäftsinformationen im Wege von Email bzw. per Post sowie der Kontaktaufnahme per Telefon zwecks Produkt- und/oder Geschäftsvorstellung über bitte Produktkategorien einfügen inklusive des zugehörigen Schriftverkehrs erforderlich und/oder für Terminbestätigung/-absagen/-änderungen per SMS. Sollte keine Vertrag zu Stande kommen, werden die Daten für den Fall von Anschlussfragen bei uns für 2 Jahre gespeichert und danach gelöscht. Diese Daten werden niemals für Werbezwecke an Dritte weitergegeben.

*Ort, Datum*

 Ja, ich möchte zusätzlich Informationen über Zweck von Firma,Name bequem per Email-**Newsletter** zugesendet bekommen. \*\*

\*\* Die Datenschutzhinweise habe ich vorab zur Kenntnis genommen Mir ist bekannt, dass die Datenverarbeitung bei dem Newsletter-Dienstleister …………………….. erfolgt und ich diese Einwilligung jederzeit per Email oder per Link im Newsletter widerrufen kann.

Verantwortliche/r
Email, Telefon

Hinweis:
Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit zu, siehe auch unsere Datenschutzerklärung unter [www.xooox.com/datenschutz](http://www.xooox.com/datenschutz) . Dafür wenden Sie sich bitte per Email ………………. an uns. Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Datenschutzbehörde beschweren.

## Auskunftsbegehren

Sehr geehrte/r Frau/Herr …….!

Gemäß Ihrer rechtmäßigen Anfrage vom …… erteilen wir Ihnen hiermit Auskunft über:

den Zwecke und Rechtsgrundlagen der Datenverarbeitung:

die personenbezogener Daten von Ihnen, die ich/wir verarbeite/n:

die Empfänger/Empfängerkreise:

die Dauer der Speicherung:

die Herkunft der Daten (falls nicht bei der Person erhoben):

Eine automatisierten Entscheidungsfindung/Profiling findet nicht statt.

Sie haben das Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung der Daten sowie ein Widerspruchsrecht gegen die Verarbeitung der Daten und das Recht auf Datenübertragbarkeit. Sie haben das Recht auf Beschwerde bei der Aufsichtsbehörde.

Ihre Kontaktdaten als Verantwortliche/r

## Muster Datenschutzverletzung (WKO)

**Datenschutzverletzung**

Art 33 EU-Datenschutzgrund-Verordnung (DSGVO) -

Meldung an die Aufsichtsbehörde:

Österreichische Datenschutzbehörde,

Hohenstaufengasse 3, 1010 Wien

E-Mail:dsb@dsb.gv.at

Name und Kontaktdaten des **Verantwortlichen**

**Name und Anschrift:**

|  |
| --- |
|  |

**E-Mail-Adresse, Tel.Nr.:**

|  |
| --- |
| *Email: …………...@…………………….* |
| Tel |

**2.** Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

|  |
| --- |
|  |
|  |
|  |

 a. soweit möglich Kategorien und ungefähre Zahl der **betroffenen Personen**:

|  |
| --- |
|  |
|  |
|  |

b. soweit möglich betroffene Kategorien und ungefähre Zahl der personenbezogenen Datensätze:

|  |
| --- |
|  |
|  |
|  |
|  |

**3.** Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten aufgrund einer neuerlichenRisikoanalyse:

|  |
| --- |
|  |
|  |
|  |

**4.** Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

|  |
| --- |
| Siehe TOMs |
|  |
|  |
|  |

ggf **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

|  |
| --- |
|  |
|  |
|  |
|  |

**5**. **Datum und Uhrzeit** des Vorfalls:

|  |
| --- |
|  |
|  |
|  |

**□ Begründung**, falls die Meldung länger als 72h nach dem Vorfall erfolgte:

|  |
| --- |
|  |
|  |
|  |

Wien, am ………………….

…………………………………………………………….
Unterschrift

## Mustervertrag Auftragsverarbeitung (WKO)

**Vereinbarung** **über eine** **Auftragsverarbeitung nach Art 28 DSGVO**

|  |  |  |
| --- | --- | --- |
| Der Verantwortliche: |  | Der Auftragsverarbeiter: |
| ***VereinName****AdresseTelefonEmail* |  | **Siehe Anleitung**[*Anschrift*] |
| (im Folgenden Auftraggeber) |  | (im Folgenden Auftragnehmer) |

### Gegenstand der Vereinbarung

Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: [*möglichst detaillierte Beschreibung der Aufgaben des Auftragnehmers, einschließlich Art und Zweck der vorgesehenen Verarbeitung].*

{Falls es einen weitergehenden Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, udgl gibt} Diese Vereinbarung ist als Ergänzung zu [*Vertrag, etc samt Datum ergänzen*] zu verstehen.

Folgende Datenkategorien werden verarbeitet: [*Datenkategorien möglichst detailliert aufzählen, zB Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, usw. bzw. als Anhang*.

Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung: [*Betroffenenkategorien ergänzen wie zB Klienten, Lieferanten, Ansprechpartner, Kollegen, Beschäftigte, usw.*]

### Dauer der Vereinbarung

**□** {Einmalige Durchführung} Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten.

**□** {Befristete Laufzeit} Die Vereinbarung ist befristet abgeschlossen und endet mit [*Fristende eintragen*]

**□** {Unbefristete Laufzeit} Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von [*Kündigungsfrist eintragen, zB ein Monat*] zum [*Kündigungstermin eintragen, zB Kalenderviertaljahr*] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

### Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.

Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

### Ort der Durchführung der Datenverarbeitung

**O** Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

**O**  Folgende Datenverarbeitungstätigkeiten werden auch außerhalb der EU bzw. des EWR durchgeführt:

### Sub-Auftragsverarbeiter

**O** Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

**O** Der Auftragnehmer ist berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen. Liste:

|  |  |  |
| --- | --- | --- |
| Wien am [*Datum*] |  | [*Ort*], am [*Datum*] |
| *Für den Auftraggeber:* |  | *Für den Auftragnehmer:* |
| ...................................................*Name* |  | ................................................… Name |

### Vorlage Wartung und Pflege von IT-Systemen & Datenschutz

Bei der Wartung und Pflege von IT-Systemen ist auch das Thema Datenschutz zu berücksichtigen. Hintergrund hierfür ist, dass auch bei der Wartung oder Pflege von IT-Systemen eine „Verarbeitung“ von personenbezogenen Daten im Auftrag vorliegen kann. Dann wäre auch ein entsprechender Auftragsverarbeitung nach Art. 28 DSGVO zwischen Auftraggeber und Auftragnehmer abzuschließen, aber gemäß der DSGVO ist nunmehr stets entscheidend, ob denn eine „Verarbeitung“ vorliegt oder nicht.

Und dazu stelle RA Stephan Hansen-Oest kostenfrei nachfolgendes Muster auf Basis der DSGVO zur Verfügung. Das Muster ist so gestaltet, dass es eine gute Ausgangsgrundlage für gängige Fälle von Wartungen von IT-Systemen sein sollte.

Hier sind alle wesentlichen Punkte für ein klassisches Anwendungsszenario einer IT-Wartung vorausgefüllt. Auch für die erforderlichen technischen und organisatorischen Maßnahmen (TOM) wird hier eine Variante gewählt, bei der der Auftraggeber ein Mindestmaß an Maßnahmen vorgibt. Der Auftragnehmer muss hier dann jeweils schauen, ob er diese Maßnahmen erfüllt und ggf. Anpassungen oder Streichungen vornehmen. So kommt man in der Praxis recht schnell zu einem ordentlichen Vertragsschluss.

Das bedeutet natürlich für den Auftraggeber nicht, dass man den Auftragnehmer nicht sorgfältig vor der Beauftragung prüfen sollte. RA Stephan Hansen-Oest kann gerade im Bereich der IT-Dienstleister nur empfehlen, mal genauer hinzuschauen, wie der Dienstleister im Bereich der Datensicherheit so aufgestellt ist. Schließlich erhält der Dienstleister ggf. Zugangsdaten zu IT-Systemen des Auftraggebers. Und diese sind besonders gesichert zu verwahren.

[**https://www.datenschutz-guru.de/wartungsvertrag/**](https://www.datenschutz-guru.de/wartungsvertrag/)

## Muster: Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO)

|  |
| --- |
| **Diese Verpflichtungserklärung betrifft Mitarbeiter, Funktionäre, Lehrtätige und Dritte** |
| **Familienname:** |  |
| **Vornamen:** |  |

In Ausübung Ihrer beruflichen/ehrenamtlichenTätigkeit erhalten Sie voraussichtlich Kenntnis über teilweise sehr sensible personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse. Alle diese Informationen sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen und europäischen Datenschutzrechts sowie des Wettbewerbsrechts.

**Mit Ihrer Unterschrift verpflichten Sie sich,**

* das Datenschutzrecht zu wahren, insbesondere § 6 DSG, einschließlich entsprechender betrieblicher Anordnungen;
* Geschäfts- und Betriebsgeheimnisse zu wahren (§ 11 UWG);
* dass Sie das Handbuch <https://consulio.at/it-richtlinien-mitarbeiter-dsgvo/> als Anleitung für die Praxis nehmen
* bei einem Verstoß gegen das Datengeheimnis oder eine Verletzung von Geschäfts- und Betriebsgeheimnissen, Schadenersatz zu leisten, und zwar ohne Rücksicht auf den tatsächlich eingetretenen Schaden durch Vereinbarung einer Konventionalstrafe pauschaliert, und zwar im Ausmaß von 3-fachen Bruttomonatsentgelten/Kooperationsvereinbarung/Werkvertrag/ oder x.000,- Euro

Die zitierten Bestimmungen sind im Anhang zu dieser Erklärung abgedruckt.

**Ihnen ist bekannt, dass**

* die personenbezogenen Daten natürlicher wie juristischer Personen einem besonderen Schutz unterliegen und die Verwendung solcher Daten nur unter besonderen Voraussetzungen zulässig ist;
* personenbezogene Daten, die Ihnen auf Grund Ihrer beruflichen Beschäftigung anvertraut oder zugänglich gemacht wurden, nur auf Grund einer ausdrücklichen Anordnung des jeweiligen Vorgesetzten übermittelt werden dürfen;
* es untersagt ist, Daten an unbefugte Empfänger innerhalb und außerhalb des Unternehmens zu übermitteln oder sonst zugänglich zu machen;
* es untersagt ist, sich unbefugt Daten zu beschaffen oder zu verarbeiten;
* es untersagt ist, personenbezogene Daten zu einem anderen als dem zum rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden;
* anvertraute Benutzerkennwörter, Passwörter und sonstige Zugangsberechtigungen sorgfältig verwahrt und geheim zu halten sind;
* allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten ebenfalls zu beachten sind;
* diese Verpflichtung auch nach Beendigung Ihrer Tätigkeit fortbesteht;
* Verstöße gegen die hier genannten Verschwiegenheitsverpflichtungen nicht nur arbeitsrechtliche Folgen, sondern auch (verwaltungs-)strafrechtliche Folgen haben und schadenersatzpflichtig machen.

Hiermit erkläre ich, am [Datum der Belehrung] von [Titel / Name] über das Datengeheimnis nach § 6 DSG und die Verschwiegenheitsverpflichtungen nach § 11 UWG belehrt worden zu sein.

|  |  |  |
| --- | --- | --- |
| **Ort, Datum** |  | **Unterschrift des Verpflichteten** |

### Anhang zum Datengeheimnis

**Datengeheimnis nach § 6 DSG**

**(1)** Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

**(2)** Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

**(3)** Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

**(4)** Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

**(5)** Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

**Verletzung von Geschäfts- oder Betriebsgeheimnissen und Missbrauch
anvertrauter Vorlagen nach § 11 UWG**

**(1)** Wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (BGBl. Nr. 120/1980, Art. I Z 6)

**(2)** Die gleiche Strafe trifft den, der Geschäfts- oder Betriebsgeheimnisse, deren Kennt­nis er durch eine der im Abs. 1 bezeichneten Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt.

**(3)** Die Verfolgung findet nur auf Verlangen des Verletzten statt.

### Einwilligungserklärung – Mitglieder

„Verein ……………………..“

Name des Mitgliedes/Auszubildenden:

Mitgliedernummer:

Telefon:

Email:

Adresse:

Bitte nehmen sie unsere Datenschutzerklärung betreffs der Verarbeitung Ihrer personen-bezogenen Daten unter: www. ….at/datenschutz vorab zur Kenntnis und kreuzen Sie an, ob Sie zustimmen oder nicht zustimmen.

|  |  |  |
| --- | --- | --- |
| Ja | Nein |  |
|  |  | Das Mitglied/Auszubildende stimmt ausdrücklich zu, dass Fotos (zB bei Vereins-Veranstaltungen) vom Verein verarbeitet und veröffentlicht werden dürfen. |
|  |  | Das Mitglied/Auszubildende stimmt ausdrücklich zu, dass ihm/ihr vom Verein ein Newsletter zugesendet wird. |
|  |  | Das Mitglied/Auszubildende stimmt ausdrücklich zu, dass ihm/ihr vom Verein ein SMS geschickt wird, falls sich ein Termin unerwartet ändert oder abgesagt werden muss. |

Ort am………….

………………………….
Unterschrift

\* Gemäß der DSGVO haben Sie als Betroffene jederzeit folgende Rechte, die Sie bitte per Email an die Datenschutz Zuständige des Vereines datenschutz@……………........... geltend machen können:

 Recht auf Auskunft (Art 15 DSGVO)

 Recht auf Berichtigung (Art 16 DSGVO)

 Recht auf Löschung (Art 17 DSGVO )

 Recht auf Einschränkung (Art 18 DSGVO)

 Recht auf Übertragbarkeit (Art 20 DSGVO)

** Recht auf Widerspruch (Art 21 DSGVO) => Fotos, Newsletter, SMS**

 Recht auf Beschwerde bei der Datenschutzbehörde

1. [↑](#footnote-ref-2)