**Datenverarbeitungsverzeichnis nach Art V30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO)**

**(Verantwortlicher)**

*In Anlehnung an die Vorlage der WKO
Stand Mai 2018*

**Inhalt**

1. **Stammdatenblatt: Allgemeine Angaben**
2. **Datenverarbeitungen/Datenverarbeitungszwecke**
3. **Detailangaben zu den einzelnen Datenverarbeitungszwecken**
4. **Allgemeine Beschreibung organisatorisch-technischer Maßnahmen**
5. **Stammdatenblatt**

**Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen**

* 1. **Name(n) und Anschrift(en):**

*IG Kaufleute Einkaufsstraße
Einkaufsstraße 1
1000 Wien*

* 1. **E-Mail-Adresse(n) und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.:** *einkaufstrasse@einkaufstrasse.at*
	2. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel..Nr.) des Datenschutzbeauftragten[[1]](#footnote-1):***Kein Datenschutzbeauftragter notwendig*
	3. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.) des Vertreters des (der) Verantwortlichen:[[2]](#footnote-2)**

*Obmann: Max Obmann
Schriftführerin: Susanne Schriftführerin*

* 1. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.) des Auftragsverarbeiters:**

***Auftragsverarbeiter Buchhaltung:***

*Buchhaltungs GmbH*

*Buchhaltungsstraße 1*

*1000 Wien*

*Verantwortlich: Mag. Buch Haltung (Funktion: Geschäftsführung)*

*buch@haltung.at*

*01/123 456 789*

***Auftragsverarbeiter Eventagentur:***

*Event Agentur e.U.*

*Veranstaltungssstraße 1*

*1000 Wien*

*Verantwortlich: Susi Party (Funktion: Unternehmerin)*

*event@agentur.at*

*01/987 654 321*

***Auftragsverarbeiter Homepagebetreuung:***

*Internetz OG*

*Netzerkgasse 1*

*1000 Wien*

*Verantwortlich: Hans Netz (Funktion: Unternehmer)*

*hans@netz.at*

*01/654 321 987*

1. **Datenverarbeitungen/Datenverarbeitungszwecke**
2. **Zwecke und Beschreibung der Datenverarbeitung[[3]](#footnote-3):**

*Abwicklung der Vereinstätigkeit
(Mitgliederverwaltung, Marketing, Sponsoren und Geschäftspartner)*

*Buchführung entsprechend § 20ff VerG*

1. **Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[[4]](#footnote-4)**

**Ja 🞎 Nein 🞎X**

**Wenn Nein, aus welchem Grund nicht?** *Da kein hohes Risiko besteht wird auf die Datenschutz-Folgeabschätzung verzichtet[[5]](#footnote-5).*

**C. Detailangaben zu Vereinstätigkeit**

1. **Kategorien der betroffenen Personen**
2. *Vereinsmitglieder (inkl. Kontaktpersonen)*
3. a*n der Vereinsverwaltung mitwirkende Dritte (inkl. Kontaktpersonen)*
4. *Sponsoren und Geschäftspartner(inkl. Kontaktpersonen)*
5. **Beschreibung**

Mitgliederverwaltung als Erfordernis der Vereinsführung, Erfüllung der Statuten, Erfüllung aller vereinsbezogenen Aufgaben und Verpflichtungen*.*

Führung der Mitgliederverwaltung in Form von *Excel-Listen/Datenbank in Excel.* Die Rechtsgrundlage für diese Verarbeitungstätigkeit entspringt dem Mitgliedsvertrag = vertragliche Grundlage. Die Originale der Beitrittserklärungen liegen auf*.* Mittels einer Datenschutzvereinbarung am Beitrittsformular wird der Interessent vor Abschluss der Mitgliedschaft über Verarbeitungszwecke, verarbeitete Datenkategorien, Empfänger, Dauer der Datenspeicherung, etc. informiert.
*Zusätzlich erfolgt die Erteilung der Information nach Art 13, 14 DSGVO im Detail über einen Datenschutzbutton auf der Webpage des Vereines.*

*Die Excel-Datenbank ist passwortgeschützt. Zugriff hat folgender eingeschränkter Personenkreis:  Obmann, Kassier und Schriftführer, sowie deren Stellvertreter.*

Nach Beendigung der Mitgliedschaft werden alle Daten - soweit kein Rückstand an Zahlungen (offener Mitgliedsbeitrag, Teilbeträge hiervon, sonstige berechtigte Forderungen des Vereins) seitens des Mitglieds besteht, und die Daten auch nicht zur Geltendmachung, Ausübung oder Vermeidung von Rechtsansprüchen des Vereins benötigt werden -  nach Ablauf eines Jahres nach Austritt, gelöscht. Diese Frist dient dem Vereinszweck und soll sicherstellen, dass die Abwicklung des Vertrages mit dem Mitglied und die damit zusammenhängenden Aufgaben gewährleistet sind. Im Falle des Bestehens offener Forderungen zum Zeitpunkt des Austritts beginnt der Fristablauf mit dem Zeitpunkt des Begleichens der offenen Zahlungen. Auf die einjährige Frist wird in der oben geschilderten Datenschutzerklärung gesondert hingewiesen.

Daten/Datensätze, die zur Erfüllung der gesetzlichen Anforderungen (z.B. Buchführung) benötigt werden, bleiben für die in den Materiengesetzen normierter Aufbewahrungsdauer gespeichert und werden anschließend gelöscht.

*Ein Backup des Excel-Files wird auf einem verschlüsselten USB-Stick/externer Festplatte abgelegt, welcher/welche der Obmann an seinem Wohnort aufbewahrt.*

1. **Rechtsgrundlagen**

*Art 6 Abs. 1 lit a (Einwilligung der Betroffenen),
b (zur Vertragserfüllung erforderlich)*

1. **Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten[[6]](#footnote-6)) sind abgelegt:***[[7]](#footnote-7)* **(*freiwillig*)**
2. **Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[[8]](#footnote-8)**
	1. **Kategorien der verarbeiteten Daten und Ankreuzen, ob sie an Empfänger übermittelt werden**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes** | **Lfd. Nr.** | **Datenkategorien** | **Besondere Datenkategorien iSd Art 9 DSGVO[[9]](#footnote-9), strafrechtlich relevant iSd Art 10 DSGVO[[10]](#footnote-10)** | **Vereinsbehörde** | **Inkassounternehmen im Anlassfall** | **Fördergeber** | **Rechtsanwälte** | **Versicherungen im Anlassfall** | **IT-Dienstleister (Provider)** | **Mitwirkende Vertrags- und Geschäftspartner**  |
| 1Vereinsmitglieder | 1 | *Name, Firma oder Geschäftsbezeichnung* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* | *X* |
| 2 | *Anschrift* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* | *X* |
| 3 | *Kontaktdaten* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* | *X* |
| 4 | *Firmenbuchdaten* | *Nein* |  | *X* |  | *X* | *X* |  | *X* |
| 5 | *UID-Nummer* | *Nein* |  | *X* |  | *X* |  |  | *X* |
| 6 | *Bankverbindung* | *Nein* |  | *X* |  | *X* | *X* |  | *X* |
| 7 | *Kontaktperson (Name und Kontaktdaten)* | *Nein* | *X* | *X* |  | *X* | *X* | *X* | *X* |
| 8 | *Vertragstexte und Vereinskorrespondenz* | *Nein* |  | *X* |  | *X* |  |  | *X* |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes** | **Lfd. Nr.** | **Datenkategorien** | **Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO** | **Vereinsbehörde** | **Inkassounternehmen im Anlassfall** | **Fördergeber** | **Rechtsanwälte** | **Versicherungen im Anlassfall** | **IT-Dienstleister (Provider)** | **Mitwirkende Vertrags- und Geschäftspartner**  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2Vereinsverwaltung | 9 | *Name, Firma oder Geschäftsbezeichnung* | *Nein* |  | *X* | *X* | *X* | *X* | *X* | *X* |
| 102 | *Anschrift* | *Nein* |  | *X* | *X* | *X* | *X* | *X* | *X* |
| 11 | *Kontaktdaten* | *Nein* |  | *X* | *X* | *X* | *X* | *X* | *X* |
| 12 | *Firmenbuchdaten* | *Nein* |  | *X* |  | *X* | *X* |  | *X* |
| 13 | *UID-Nummer* | *Nein* |  | *X* |  | *X* |  |  | *X* |
| 14 | *Bankverbindung* | *Nein* |  | *X* |  | *X* |  |  | *X* |
| 15 | *Kontaktperson (Name und Kontaktdaten)* | *Nein* |  | *X* |  | *X* | *X* |  | *X* |
| 16 | *Vertragstexte und Vereinskorrespondenz* | *Nein* |  | *X* |  | *X* |  |  | *X* |
| 3Dritte (Sponsoren und Geschäftspartner) | 17 | *Name, Firma oder Geschäftsbezeichnung* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* | *X* |
| 18 | *Anschrift* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* | *X* |
| 19 | *Kontaktdaten* | *Nein* | *X* | *X* | *X* | *X* | *X* | *X* | *X* |
| 20 | *Firmenbuchdaten* | *Nein* |  | *X* |  | *X* | *X* |  | *X* |
| 21 | *UID-Nummer* | *Nein* |  | *X* |  | *X* |  |  | *X* |
| 22 | *Bankverbindung* | *Nein* |  | *X* |  | *X* |  |  | *X* |
| 23 | *Kontaktperson (Name und Kontaktdaten)* | *Nein* | *X* | *X* |  | *X* | *X* | *X* | *X* |
| 24 | *Vertragstexte und Vereinskorrespondenz* | *Nein* |  | *X* |  | *X* |  |  | *X* |

* 1. **Löschungs- und Aufbewahrungsfristen (wenn möglich)**

|  |  |
| --- | --- |
| **Daten aus 4.a.** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** |
| *1-24* | *Nach Beendigung der Mitgliedschaft werden alle Daten - soweit kein Rückstand an Zahlungen (offener Mitgliedsbeitrag, Teilbeträge hiervon, sonstige berechtigte Forderungen des Vereins) seitens des Mitglieds besteht, und die Daten auch nicht zur Geltendmachung, Ausübung oder Vermeidung von Rechtsansprüchen des Vereins benötigt werden - nach Ablauf eines Jahres nach Austritt, gelöscht. Diese Frist dient dem Vereinszweck und soll sicherstellen, dass die Abwicklung des Vertrages mit dem Mitglied und die damit zusammenhängenden Aufgaben gewährleistet sind. Im Falle des Bestehens offener Forderungen zum Zeitpunkt des Austritts beginnt der Fristablauf mit dem Zeitpunkt des Begleichens der offenen Zahlungen. Auf die einjährige Frist wird in der oben geschilderten Datenschutzerklärung gesondert hingewiesen.**Daten/Datensätze, die zur Erfüllung der gesetzlichen Anforderungen (z.B. Buchführung) benötigt werden, bleiben für die in den Materiengesetzen normierter Aufbewahrungsdauer gespeichert und werden anschließend gelöscht. Aufgrund der gesetzlichen Aufbewahrungsfristen jedenfalls 7 Jahre darüberhinausgehend bis zur Beendigung eines allfälligen Rechtsstreites.* |

1. **Kategorien von Empfängern[[11]](#footnote-11), an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern**14
	1. **Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)**

|  |  |  |
| --- | --- | --- |
| **Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus 4.a.)** | **Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)** | **Internationale Organisation (Angabe der intern. Organisation)** |
| *Verwaltungsbehörde* |  |  |
| *Inkassobüro* |  |  |
| *Fördergeber* |  |  |
| *Rechtsanwälte* |  |  |
| *Versicherungen* |  |  |
| *IT-Dienstleister (Provider)* | *USA* |  |
| *Mitwirkende Vertrags- und Geschäftspartner* |  |  |

* 1. **Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt** (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt)**:[[12]](#footnote-12)**

*Dokumentation*

1. **Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen**
	1. **Vertraulichkeit[[13]](#footnote-13):**

*Die Daten befinden sich auf einem vereinseigenen passwortgeschützten Notebook mit Festplattenverschlüsselung. Zugang zu diesem Notebook hat folgender eingeschränkter Personenkreis: Obmann, Kassier und Schriftführer, sowie deren Stellvertreter. Die Excel-Datenbank ist passwortgeschützt. Zugriff hat der o.a. eingeschränkte Personenkreis.*

* 1. **Integrität**[[14]](#footnote-14)**:**

*Die Eingabe der Daten erfolgt durch den o.a. eingeschränkten Personenkreis entsprechend deren Funktion. Die Zugriffskontrolle erfolgt über die Systemlogs der Software. Die Übertragung von Daten erfolgt mittels passwortgeschützter Archivfiles bzw. über VPN.*

* 1. **Verfügbarkeit und Belastbarkeit:**

 *Die Daten werden wöchentlich/monatlich/quartalsweise (Nichtzutreffendes streichen) auf einen USB-Stick bzw. eine externe Festplatte gesichert. Diese befindet sich beim Obmann unter Verschluss.
Die Daten werden durch das Virenschutzprogramm xxxxxx in seiner jeweils aktuellsten Version und durch eine Betreibssystemfirewall bzw. das Produkt xxxx geschützt.
Die Daten, die auf Papier vorhanden sind befinden sich in einem versperrten Schrank im Unternehmen des Obmanns und sind nur dem Obmann, dem Kassier und dem Schriftführer zugänglich. Mitarbeiter des Vereins, sofern sie mit den Mitgliederdaten in Kontakt kommen müssen eine Verpflichtungserklärung unterschreiben.*

* 1. **Pseudonymisierung und Verschlüsselung:**

*Ein Backup des Excel-Files wird auf einem verschlüsselten USB-Stick oder einer verschlüsselten externer Festplatte abgelegt, welcher/welche der Obmann an seinem Wohnort aufbewahrt.*

* 1. **Evaluierungsmaßnahmen:**

*Einmal jährlich werden alle Maßnahmen überprüft und nötigenfalls angepasst. Der berechtigte Personenkreis wird einmal jährlich auf Einhaltung geschult.*

1. Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde.

**HINWEIS:** Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „*Datenschutzbeauftragter*“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (zB „*Datenschutzkoordinator*“). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt [„Datenschutzbeauftragter“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Der-Datenschutzbeauftragt.html). [↑](#footnote-ref-1)
2. Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen. [↑](#footnote-ref-2)
3. Zum Begriff „Verarbeitung“ siehe das Merkblatt [„Wichtige Begriffsbestimmungen“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Wichtige-Begriffsbestimmu.html); sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren. [↑](#footnote-ref-3)
4. Zur Datenschutz-Folgenabschätzung siehe das Merkblatt „[Datenschutz-Folgenabschätzung](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html)“. Im Verarbeitungsverzeichnis sind zwar Angaben zur Datenschutz-Folgenabschätzung nicht zwingend vorgesehen. Aus Gründen der Rechenschaftspflicht empfehlen sich aber grundsätzliche Angaben darüber auch ins Verarbeitungsverzeichnis aufzunehmen. [↑](#footnote-ref-4)
5. Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, wenn durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht oder die Datenverarbeitungsart in der sogenannten „white list“ der Datenschutzbehörde gelistet ist (derzeit besteht noch keine „white list“); Näheres dazu siehe auch das Merkblatt [„Datenschutz-Folgenabschätzung“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html). [↑](#footnote-ref-5)
6. Siehe zu den Informationspflichten das Merkblatt [„Informationspflichten“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Informationspflichten.html). [↑](#footnote-ref-6)
7. Die Angabe, wo die Unterlagen innerhalb der Organisation abgelegt wurden, ist nicht verpflichtend im Verarbeitungsverzeichnis zu dokumentieren, erleichtert aber vor allem in größeren, arbeitsteilig organisierten Organisationen das Auffinden der entscheidenden Unterlagen (dient also lediglich der innerbetrieblichen Arbeitserleichterung). [↑](#footnote-ref-7)
8. Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verarbeitungsverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (zB „nach Ablauf des Vertrages“). [↑](#footnote-ref-8)
9. Daten nach Art 9 DSGVO sind besondere Datenkategorien („sensible Daten“): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung. [↑](#footnote-ref-9)
10. Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln unter behördlicher Aufsicht. [↑](#footnote-ref-10)
11. Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren. [↑](#footnote-ref-11)
12. Siehe dazu das Merkblatt [„Internationaler Datenverkehr“](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Internationaler-Datenverk.html). Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield“-System) empfiehlt sich eine namentliche Nennung des Empfängers. [↑](#footnote-ref-12)
13. Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten. [↑](#footnote-ref-13)
14. Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten. [↑](#footnote-ref-14)