Datenschutz-Konzept
Verein ÖAS

Österreichische Arbeitsgemeinschaft für systemische Therapie und systemische Studien

gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

ZVR-Zahl des Vereins gemäß § 18 Abs. 3: **204223903**

Wien, am 25. Mai 2018

Amtierender Obmann/frau

zur Zeit der Erstellung Mag. Andreas Höher

Verantwortliche_r gemäß DSGVO

Eßlinggasse 17/2
Telefon 01/ 212 41 35
Email office@oeas.at

Inhaltsverzeichnis

Allgemeine Angaben

1.1 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).

1.2 Sachliche und räumliche Tätigkeit

Unser Verein ÖAS ZVR-Nr: 204223903 verarbeitet personenbezogene Daten von natürlichen Personen ganz oder teilweise automatisiert und hat seine Niederlassung in der EU, in der Vereinsadresse.

1.3 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 (Anmeldung Lehrpersonal beim BMG)	**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 nur einer der obigen Kriterien zutrifft, dies aber keine sensiblen Daten beinhaltet und mit Einwilligung der Personen erfolgt, wird kein DSB bestellt.

1.4 Verantwortliche (Stammdaten)

Verantwortliche
Amtierende_r Obmann/frau zur Zeit der Erstellung Mag. Andreas Höher Verantwortliche_r gemäß DSGVO Eßlinggasse 17/2 Telefon 01/ 212 41 35

Email office@oeas.at

Referenzen: Art 4 Z 7 DSGVO

1.5 Weiterbildung und Stand der Technik

Betreffs Weiterbildung und Stand der Technik setze ich folgende Aktivität:

Aktivitäten	Veranstalter
Homepages bzw. Newsletter	https://www.dataprivacydoctors.at/vorlagen/
	https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung-
Informationsveranstaltung	Taylor Wessing Rechtsberatung

Referenzen: Art 4, 5-11 DSGVO

2 Datenverarbeitungen/Datenverarbeitungszwecke

2.1 Zwecke und Beschreibung der Datenverarbeitung:

2.1.1 Mitgliederverwaltung inkl. Studierende

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, siehe Vereinsstatuten auf ÖAS-Website, 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

2.1.2 Kommunikation

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

2.1.3 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, soweit diese Daten vom Betroffenen angegeben wurden.

2.2 Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

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 umfangreichen Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt. Auch die beim Zugang des Vereinslokals angebrachte Videokamera der Türöffnungsanlage speichert keine Daten.

Referenzen: Art 35 Z1-3 DSGVO

3 Verarbeitungsverzeichnis (Verzeichnis der Verarbeitungstätigkeit – VV)

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

3.1 Mitglieder- und Student_innenverwaltung

3.1.1 Verantwortliche

Verantwortliche	***Für Datenschutz-Zuständige***
Amtierende_r Obmann/frau zur Zeit der Erstellung Mag. Andreas Höher Verantwortliche_r gemäß DSGVO Eßlinggasse 17/2 Telefon 01/ 212 41 35 Email office@oeas.at	

3.1.2 Zweck

Führung, Verarbeitung und Übermittlung von Mitgliederverzeichnissen, Evidenz der Mitgliedsbeiträge, Verkehr mit Mitgliedern 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, (siehe Statuten im Anhang 1) analog siehe 2.1.1.

3.1.3 Kategorien der betroffenen Personen

Lfd.Nr.	**Beschreibung der Kategorien betroffener Personen**
1	Vereinsmitglieder und Funktionär_innen
2	Studierende
3	Kund_innen, Abonnent_innen
4	Angestellte, freie Mitarbeiter_innen
5	An den Vereinsaktivitäten mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen

3.1.4 Rechtsgrundlagen (in geltender Fassung)

- Art 6 Z 1 lit a (Einwilligung der Betroffenen), Fotos + Newsletter
- Art 6 Z 1 lit b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen-Vereinszweck) DSGVO
- § 132 BAO
- §§ 190, 212 UGB

- EStG, UStG
- Österr. Psychotherapiegesetz
- Vereinsgesetz 2002
- ÖAS Vereinsstatuten

3.1.5 Verträge , Zustimmungserklärungen oder sonstige Unterlagen

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

3.1.6 Kategorien der verarbeiteten Daten

Vorlage ist SA003 Mitgliederverwaltung
(https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495&FassungVom=2018-05-24)

Betroffene Personengruppen:	Nr.:	Datenarten:	Bes. Daten lsd Art.9	Empfängerkreis:
Mitglieder, Funktionär_innen	1	Mitgliedsnummer (Kontonummer winline)	nein	56
	2	Name oder Bezeichnung der Organisation	nein	123456
	3	Anrede / Titel / Geschlecht	nein	123456
	4	Geburtsdatum	nein	23456
	5	Adresse	nein	13456
	6	Telefonnummer / Emailadresse	nein	13456
	7	Berufsausbildung, Quellberuf	nein	356
	8	anonyme Statistikdaten fürs BM f. Gesundheit, wenn nicht oben erwähnt (=Staatsbürgerschaft, Hauptwohnsitz, Studienabschluss, -abbruch, Status und Statuspause)	nein	236
	9	Mitgliederkategorie z.B. Bewerber, Interessent, Mitglied, usw...	nein	3456
	10	Eintritts-, Austrittsdaten	nein	3456
	11	Beiträge (Zahlungen)	nein	13456
	12	Vom Betroffenen bekannt gegebene Spezialisierungen	nein	356
	13	Vereinsrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen, Curricula, Listeneinträge, Zertifizierungen	nein	123456
	14	Zahlungsverpflichtungen des Betroffenen an den Auftraggeber	nein	13456
	15	Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen	nein	123456
	16	Bankverbindung	nein	1235
	17	Auszeichnungen, Ehrungen	nein	3
	18	Fotos	nein	36

	19	Funktion	nein	123456
	20	Seminarbuchungen und -anwesenheiten	nein	236
Studierende	21	Mitgliedsnummer (Kontonummer winline)	nein	56
	22	Name oder Bezeichnung der Organisation	nein	123456
	23	Anrede / Titel / Geschlecht	nein	123456
	24	Geburtsdatum	nein	23456
	25	Adresse	nein	13456
	26	Telefonnummer / Emailadresse	nein	13456
	27	Beruf oder Branche	nein	356
	28	anonyme Statistikdaten fürs BM f. Gesundheit, wenn nicht oben erwähnt (=Staatsbürgerschaft, Hauptwohnsitz, Studienabschluss, -abbruch, Status und Statuspause)	nein	236
	29	Mitgliederkategorie z.B. Bewerber, Interessent, Mitglied, usw...	nein	3456
	30	Eintritts-, Austrittsdaten	nein	3456
	31	Beiträge (Zahlungen)	nein	13456
	32	Vom Betroffenen bekannt gegebene Spezialisierungen	nein	356
	33	Vereinsrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen, Curricula, Listeneinträge, Zertifizierungen	nein	123456
	34	Zahlungsverpflichtungen des Betroffenen an den Auftraggeber (ev. Sonderregelung Teilzahlung)	nein	123456
	35	Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen	nein	1235
	36	Bankverbindung	nein	1235
	37	Seminarbuchungen und -anwesenheiten	nein	236
	38	Bewerbungs- /Motivationsschreiben	ja	346
	39	Fotos	nein	36
	40	Auszeichnungen, Ehrungen	nein	3
Kunden, Abonnenten (Mieten, SKJ, Workshop- u. Kongressbesucher etc.)	41	Kundennummer (Kontonummer winline)	nein	3456
	42	Name oder Bezeichnung der Organisation	nein	123456
	43	Anrede / Titel	nein	123456
	44	Adresse	nein	23456
	45	Telefonnummer / Emailadresse	nein	23456
	46	Beiträge (Zahlungen)	nein	123456
	47	Zahlungsverpflichtungen des Betroffenen an den Auftraggeber	nein	123456
	48	Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen	nein	123456
	49	Bankverbindung	nein	123456
Angestellte, freie	50	Kontonummer winline	nein	23456
	51	Name	nein	123456

Mitarbeiter_innen	52	Anrede / Titel / Geschlecht	nein	123456
	53	Geburtsdatum	nein	23456
	54	Adresse	nein	23456
	55	Telefonnummer / Emailadresse	nein	3456
	56	Beruf oder Branche	nein	23456
	57	Mitgliederkategorie z.B. Vollmitgl, Ehren-mitgl., karenziert	nein	3456
	58	Eintritts-, Austrittsdaten	nein	23456
	59	Vom Betroffenen bekannt gegebene Interes-sen und Spezialgebiete sh. Motivations-schreiben, Lebenslauf	nein	356
	60	Vereinsrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen, Curricula,…	nein	23456
	61	Zahlungsverpflichtungen des Betroffenen an den Auftraggeber	nein	123456
	62	Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen	nein	123456
	63	Bankverbindung	nein	13456
	64	Auszeichnungen, Ehrungen	nein	3
Kreditor_innen, Lieferant_innen	65	Kreditorennummer (Kontonummer winline)	nein	3456
	66	Name oder Bezeichnung der Organisation, Firmenname	nein	123456
	67	Firmenbuch- und DVR-Nummer	nein	2345
	68	Adresse	nein	23456
	69	Telefonnummer / Emailadresse/Website	nein	23456
	70	Beruf oder Branche	nein	3456
	71	Angaben betreffend Leistungen/Zahlungen des Betroffenen an den Auftraggeber	nein	123456
	72	Vertragstext	nein	346
	73	Bankverbindung	nein	13456
	74	Rechnungsbetrag, Rechnung	nein	123456
	75	Zahlungen oder Leistungen des Auftragge-bers an den Betroffenen	nein	123456

3.1.7 Löschungs- und Aufbewahrungsfristen

Daten	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-40	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 8 Jahre**; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. **Ausnahme: Daten von Studierenden im Fachspezifikum Behalte-**

	frist 12 Jahre ab Studienabschluss (BMfG)
50-64	Bis zur Beendigung des Dienstverhältnisse 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 30 Jahre**; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. Job Bewerbungsschreiben von Nichtangenommenen Dienstnehmer_innen max. 6 Monate
41-49, 65-75	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 **8 Jahre**; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden.
18, 39	Fotos: Recht auf jederzeitigen Widerspruch (Art 21 DSGVO)

3.1.8 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 Finanzamt, Sozialversicherung, Vereinsbehörden, Bundesministerium,…	Nein	Nein
3	Personen und Institutionen auf Grund einer Ermächtigung oder Verpflichtung zur Datenübermittlung in den Statuten oder auf Grund besonderer Zustimmung des Betroffenen (Lehrende, Office, Studierende, ferner Mitglieder)	Nein	Nein
4	Rechtsanwälte, Gerichte und sonstige Stellen, zum Zweck der Rechtsdurchsetzung.	Nein	Nein
5	Steuerberater, Bilanzbuchhalter, Lohnverrechnung	Nein	Nein
6	IT-Dienstleister (Mesonic, Ipodion, Webex Teams, Gugler GmbH, PR)	Nein	Nein

3.1.9 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

3.2 Kommunikation

3.2.1 Verantwortliche

Verantwortliche	Für Datenschutz zuständig
Amtierende_r Obmann/frau zur Zeit der Erstellung Mag. Andreas Höher Verantwortliche_r gemäß DSGVO Eßlinggasse 17/2 Telefon 01/ 212 41 35 Email office@oeas.at	

3.2.2 Zweck

Vereinsorientierte Information und Betreuung von kategorisierten Mitgliedern, Studierenden, Funktionären und an den Vereinsaktivitäten mitwirkenden Institutionen und Lehrpersonal sowie Dritte inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter und Informationsmaterial.

3.2.3 Kategorien der betroffenen Personen

Lfd.Nr.	Beschreibung der Kategorien betroffener Personen
1	Vereinsmitglieder und Funktionär_innen
2	Studierende
3	Kund_innen, Abonnent_innen
4	Angestellte, freie Mitarbeiter_innen
5	An den Vereinsaktivitäten mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen

3.2.4 Rechtsgrundlagen (in geltender Fassung)

- Newsletter: Art 6 Z 1 lit f (berechtigte Interessen des Verantwortlichen - Vereinzszweck)
- Ansonsten: a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen)
- § 151 GewO 1994 - „SA022 Kundenbetreuung und Marketing für eigene Zwecke“ siehe Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: BGBl. II Nr. 312/2004
- Vereinsgesetz 2002
- Vereinsstatuen

3.2.5 Verträge , Zustimmungserklärungen oder sonstige Unterlagen

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

3.2.6 Kategorien der verarbeiteten Daten

Vorlage ist die Standardanwendung „SA022 Kundenbetreuung und Marketing für eigene Zwecke“

Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden sind auf Grund **der konkreten Prüfung gemäß Datenminimierung nach Art 5 Z 1 DSGVO für unseren Verein mit (X)** angekreuzt.

Kategorien der betroffenen Personengruppe	Lf. Nr.:	Datenkategorien	Besondere Datenkategorien iSd Art 9 u. Art 10 d. DSGVO	Rechtsvertreter im Anlassfall	Gericht im Anlassfall	
1-5 Vereinsmitglieder und Funktionär_innen Studierende Kund_innen, Abonnent_innen Angestellte, freie Mitarbeiter_innen An den Vereinsaktivitäten mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen	01	Mitgliedernummer sonstige Ordnungszahlen	*Nein*	X	X	
	02	Name bzw. Bezeichnung	*Nein*	X	X	
	03	Anrede/Geschlecht	*Nein*	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	
	06	Homepage, Soziale Netzwerke	*Nein*	X	X	
	07	IP-Adresse	*Nein*			
	08	Einwilligungen nach Art 4 abgelegt	*Nein*	X	X	
	09	Berufs-, Branchen- Geschäftsbezeichnung	*Nein*	X	X	
	11	Firmenbuch- und andere Kennzahlen (UID-Nummer, ...)	*Nein*	X	X	
	12	Vom Betroffenen bekannt gegebene Interessen und Spezialgebiete	*Nein*	X	X	
	13	Vereinszweckrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen	*Nein*	X	X	
	14	Interessen (auf Grund bisherigen Teilnahme oder eigener Angaben des Vereinsmitgliedes gegenüber dem Auftraggeber)	*Nein*	X	X	
	15	Newsletter-Sperre	*Nein*	X	X	

- IP-Adresse der Webseitenbesucher
- Bewegungen und Clicks der Besucher auf der Webseite
- Browser-Fingerprints

3.2.7 Löschungs- und Aufbewahrungsfristen

Daten (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw.

	Aufbewahrungsfristen
1 – 15	Aufgrund der gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf 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	Zu eigenen Sicherheitszwecken: Speicherfrist von maximal 7 Tagen

3.2.8 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	Nein

3.2.9 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.

3.3 Personalwesen

3.3.1 Zuständigkeiten

Verantwortliche	Für Datenschutz-Zuständige
Amtierende_r Obmann/frau zur Zeit der Erstellung Mag. Andreas Höher Verantwortliche_r gemäß DSGVO Eßlinggasse 17/2 Telefon 01/ 212 41 35 Email office@oeas.at	Titel/ Name ..... Adresse Email Telefon

3.3.2 Zweck

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

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

3.3.3 Rechtsgrundlagen

- Art 6 Z 1 lit a (Einwilligung der Betroffenen), 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 in der geltenden Fassung, Jugendvertrauensperson gemäß § 125ff ArbVG und Behindertenvertrauensperson 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 in der geltenden Fassung
- „SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse“ (siehe http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495

3.3.4 Verträge, Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen und Verträge zum Personalwesen sowie Verträge mit Auftragsverarbeitern sind im Archiv abgelegt.
Bewerbungsunterlagen werden nach Abschluss des Bewerbungsverfahren vernichtet

3.3.5 Kategorien der betroffenen Personen

Lfd. Nr.	Beschreibung der Kategorien betroffener Personen
1	Arbeitnehmer_innen, fiktive echte Dienstnehmer_innen, freie Dienstnehmer_innen, Volontär_innen und Ferialpraktikant_innen (auch ehemalige Beschäftigte):
2	Bewerber_innen

3.3.6 Kategorien der verarbeiteten Daten

Vorlage ist die Standardanwendung „SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse“

Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden, müssen auf Grund **der konkreten Prüfung im Einzelfall gemäß Datenminimierung nach Art 5 Z 1 DSGVO mit der jeweiligen Nummer angegeben werden**.

Kategorien der betroffenen Personengruppe	Lfd. Nr.	Datenkategorie	Empfängerkategorien (die in der Empfängerliste gelöschten Nummern sind hier aufgelistet aber hinfällig – dh. 3,5,8,10,15,17,18,20,25 ,26 sind keine Empfänger)	Datenkategorien im Sinne der Art 9 und Art 10 DSGVO
1. Arbeitnehmer_innen, fiktive echte Dienstnehmer_innen, freie Dienstnehmer_innen, Volontär_innen und Ferialpraktikant_innen (auch ehemalige Beschäftigte):	01	Ordnungsnummer (von Steuerberater)		Nein
	02	Name	1 – 25	Nein
	03	Frühere Namen (Namensteile)	1 – 24	Nein
	04	Geburtsdatum	1 – 13, 15 – 23	Nein
	05	Geburtsort	1 – 13, 15 – 22	Nein
	06	Geschlecht	1 – 23	Nein
	07	Personenstand	1, 2, 4, 5, 9 – 13, 17 – 19, 21, 22	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	Kinder siehe Art 8 DSGVO
	~~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	Nein
	12	Organisatorische Zuordnung im Betrieb einschließlich Beginn und Ende	2 – 7, 9 – 11, 15, 16, 18, 21, 22, 25	Nein
	13	Betriebliches 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	Nein
	15	Private Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	1 – 17, 21 – 23	nach Angabe des Betroffenen
	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~~	~~Nein~~
	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)	2, 4, 5, 10, 19, 21, 22	Nein

		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 (z. B. Unterbrechung der Beitragszahlung durch Karenzurlaub)		
	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	Nein
	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	Nein
	31	Lichtbild des Betroffenen (für Ausweiskarten)	4, 5, 21, 22	Einwilligung des Betroffenen oder Betriebsvereinbarung
	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)	Keine Weitergabe	nach Angabe des Betroffenen
	37	Krankenstand, einschließlich Arbeitsunfall und Berufskrankheit (Beginn, Ende und Dauer)	2 – 5, 10, 18, 19, 21, 22	ja
	38	Zeitpunkt eines Arbeitsunfalls	2 – 5, 10, 18, 19, 21, 22	Nein
	39	Kuraufenthalte	2 – 5, 10, 18, 19, 21, 22	Nein
	40	Mutterschutz (Beginn und Ende)	2 – 5, 9, 10, 18, 19, 21, 22	Nein
	41	Karenzurlaub gemäß MSchG und EKUG (Beginn und Ende)	2 – 5, 9, 10, 15, 18, 19, 21, 22	Nein
	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 ArbeitnehmerInnenschutzgesetz, BGBl. Nr. 450/1994 i. d. g. F., Bazillenausscheidergesetz, BGBl. Nr. 153/1945 i. d. g. F., Tuberkulosegesetz, BGBl. Nr. 127/1968 i. d. g. F. und ähnliche Rechtsvorschriften~~	~~4 – 7, 18, 21, 22~~	Nein
	46	Grad der Behinderung gemäß Behinderteneinstellungsgesetz (nach Bekanntgabe des Betroffenen)	2 – 5, 9, 11, 15, 21, 22	Ja
	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	Nein
	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 i. d. g. F.	20, 21, 22	Nein

	55	~~Höhe des Gewerkschaftsbeitrages und Bezeichnung und Adresse des Empfängers~~	~~14, 15, 21, 22~~	
	56	Versicherungsprämien als Leistung des Arbeitgebers	4, 5, 13, 14, 21, 22	Nein
	57	Verwaltung von Vorschüssen und Darlehen	1, 14, 21, 22	Nein
	58	Lohnpfändungsdaten	1, 4, 5, 21, 22	Nein
	59	Daten des Lohnzettels (L – 16 Formular)	10, 12, 21, 22	Nein
	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~~	Nein
	66	Daten nach dem Berufsausbildungsgesetz, BGBl. Nr. 142/1969 i. d. g. F., 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. Bewerberinnen	67	~~Ordnungszahl(en)~~	~~21, 22~~	
	68	Name	21, 22	
	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~~	

3.3.7 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 z. B. § 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
67-81	Für Bewerber_innen-Daten gilt eine **6-Monatsfrist** gemäß Gleichbehandlungsgesetz …
Dienstzeugnisses	Anspruch auf Ausstellung eines Dienstzeugnisses nach § 1163 i. V. m. § 1478 ABGB: **30 Jahre**

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

Lfd. Nr.	Empfängerkategorien Unterstehende Liste ist nicht nummerisch gereiht Folg. Nummern wurden gelöscht: 3,5,8,10,15,17,18,20,25,26	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	Nein
2	Sozialversicherungsträger (einschließlich Betriebskrankenkassen);	Nein	Nein
4	Arbeitsinspektorat, Verkehrs-Arbeitsinspektion und Land- und Forstwirtschaftsinspektion, insbesondere gemäß § 8 Arbeitsinspektionsgesetz;	Nein	Nein
6	Gemeindebehörden in verwaltungspolizeilichen Agenden;	Nein	Nein
7	Bezirksverwaltungsbehörde in verwaltungspolizeilichen Agenden (Gewerbebehörde, Zuständigkeiten nach ASchG, usw.);	Nein	Nein
9	Arbeitsmarktservice;	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
16	gesetzliche Interessensvertretungen;	Nein	Nein
19	Pensionskassen;	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

3.3.9 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

4 Impressum und Statuten

Impressum: http://www.oeas.at/impressum.html

Statuten: http://www.oeas.at/vereinsstatuten.html

5 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

5.1 Kontaktaufnahme

Wenn ein potentielles Vereinsmitglied 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) verarbeiten (siehe Art 6 (1) b DSGVO ... auf Anfrage der betroffenen Person ...). Sollte es zu keiner Mitgliedschaft kommen, so werden wir diese Daten nach 6 Monaten löschen.

5.2 Handy

Derzeit keine Mobiltelefone in Verwendung

5.3 Emails

In allen unseren Emails an Vereinsmitglieder und sonstige Personen weisen wir auf die Datenschutzerklärung hin

5.4 Datengeheimnis

Funktionäre und Mitarbeiter sind mit Stand 16.11.2018 geschult und sind auf Vertraulichkeit/ Datengeheimnis verpflichtet. Datum nächster Schulung AK-Sitzung Herbst 2019

5.5 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

	Schließsystem mit Codesperre		*Manuelles Schließsystem*
	Automatisches Zugangskontrollsystem		*Videoüberwachung des Zugangs, keine Speicherdaten*

	Schlüsselregelung Vereinslokal (Schlüsselausgabe etc.)		*Listenführung mit Unterzeichnung*
	Schlüsselregelung Office		*Listenführung mit Unterzeichnung 4 Angestellte*
	Bildschirmsperre nach 10 Minuten		*Sorgfältige Auswahl von Reinigungspersonal*
	Verschlossene Türen bei Abwesenheit		

5.6 Zugangskontrolle

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

	Zuordnung von Benutzerrechten		*Erstellen von Benutzerprofilen*
	Passwortvergabe		*Zuordnung von Benutzerprofilen zu IT-Systemen*
	Authentifikation mit Benutzername / Passwort		*Einsatz von VPN-Technologie*
	Schlüsselregelung (Schlüsselausgabe etc.)		*Sicherheitsschlösser*
	Einsatz von Anti-Viren-Software		*Sorgfältige Auswahl von Reinigungspersonal*
	Einsatz einer Software-Firewall		*Verschlüsselung von mobilen Datenträgern*

5.7 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.

nein	*Erstellen eines Berechtigungskonzepts*	*ja*	*Verwaltung der Rechte durch Systemadministrator*
ja	*Anzahl der Administratoren auf das „Notwendigste“ reduziert*	*nein*	*Passwortlänge, Passwortwechsel*
nein	*Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten*	*ja*	*Sichere Aufbewahrung von Datenträgern*
nein	*physische Löschung von Datenträgern vor Wiederverwendung (extern nur mit Datenverarbeitungsvereinbarung)*	*ja*	*ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)*

ja	*Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)*	*ja*	*Protokollierung der Vernichtung*
nein	*Verschlüsselung von Datenträgern*		

5.8 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.

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

5.9 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.

*Nein**	*Protokollierung der Eingabe, Änderung und Löschung von Daten (*Winline und Ipodion nein, Gugler Website ja)*	*nein*	*Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. => siehe Verarbeitungsverzeichnis*
*Ja**	*Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) (*Ipodion Nein)*	*nein*	*Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind*

ja	*Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (nur Office-Personal, Vorstand)*		

5.10 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*

ja	*Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)*	*ja*	*vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen*
ja	*schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) siehe Anhang*	*ja*	*Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis*
nein	*Auftragnehmer hat Datenschutzbeauftragten bestellt*	*ja*	*Forderung der Vernichtung von Daten nach Beendigung des Auftrags*
nein	*Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart*	*X*	*laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten*
nein	*Vertragsstrafen bei Verstößen*		

5.11 Verfügbarkeitskontrolle

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

ja	*Unterbrechungsfreie Stromversorgung (USV) (rote Steckdosen)*	*nein*	*Klimaanlage in Serverraum*
nein	*Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen*	*nein*	*Schutzsteckdosenleisten in Serverräumen*
nein	*Feuer- und Rauchmeldeanlagen*	*ja*	*Feuerlöschgeräte*
nein	*Alarmmeldung bei unberechtigten Zutritten zu Serverräumen*	*ja*	*Erstellen eines Backup- & Recoverykonzepts*
*nein ja **	*Testen von Datenwiederherstellung (* Ipodion nein, Mesonic ja Stickspicherung)*	*nein*	*Erstellen eines Notfallplans*
ja	*Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort (Ipodion Backup Festplatte Serverraum, Winlinesicherung auf Stick im Safe), Website Gugler*	*ja*	*Serverräume nicht unter sanitären Anlagen*
ja	*In Hochwassergebieten: Serverräume über der Wassergrenze*		

5.12 Trennungsgebot

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

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

Quelle unter anderem: https://www.datenschutz-guru.de/files/**Ausfuellhilfe_TOM_9_BDSG_V2**.docx

5.13 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.13.1 Risikoanalyse – siehe Punkt 10

5.13.2 Weiterbildung siehe Schulung

5.13.3 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)

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

Jahr	Ergebnisse der Überprüfung, Bewertung und Evaluierung
2019	8.8.2019 Finalisierung des Konzepts zur DSGVO
2020	Geplant August 2020 neuer Vorstand überprüft Stand des DSGVO

Referenzen: Art 32 Z 1 DSGVO

6 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

7 Prozess betreffs Betroffenenrechte

Der / die ÖAS-Datenschutzbeauftragte (zur Zeit der Erstellung Obmann, Mag. Andreas Höher) erhält Kenntnis, dass ein Betroffener seine Rechte geltend machen will, sei es z.B. mündlich, schriftlich. (insbesondere per Email an office@oeas.at)

- **Feststellung der Identität:**
  Sollte dem ÖAS-Datenschutzbeauftragen der/die Betroffene nicht persönlich bekannt sein, so muss er/sie zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:

- Feststellung der Identität entweder persönlich vorsprechend mit Ausweiskontrolle oder schriftlich mit Unterschrift und Ausweiskopie.

- Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten seitens des DS-Beauftragten sind notwendig.

- Identität zweifelsfrei festgestellt und die Anfrage ist rechtens
  => Der Betroffene bekommt gemäß Art 19 DSGVO innerhalb von maximal 14 Tagen abhängig von seiner Anfrage in klarer und verständlicher Sprache folgende Antworten:

- Recht auf Auskunft (Art 15 DSGVO)
  Der Betroffene erhält
  - Auskunft über die zu seiner Person gespeicherten Daten
- Recht auf Berichtigung (Art 16 DSGVO)
  - sein Stammdatenblatt mit den berichtigten Daten (Screenshot)
- Recht auf Löschung (Art 17 DSGVO)
  - sein gelöschtes Stammdatenblatt (ausgenommen Name) als Screenshot als Nachweis, dass die Löschung erfolgt ist, mit den Hinweis, dass alle Daten inklusive Namen anschließend unwiderruflich gelöscht wurden.
  - Bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werden alle „Marketingdaten“ umgehend gelöscht. Pb Daten aus „Buchhaltungsunterlagen“ und „Kundenverwaltung/kartei“ werden aufgrund gesetzlicher Aufbewahrungsfristen „eingeschränkt“ (siehe Art 18) und nach 7 Jahren gelöscht, darüber hinaus gehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen.

- Recht auf Einschränkung (Art 18 DSGVO)
  Der Betroffene bekommt als Screenshot
- sein Stammdatenblatt, dem er entnehmen kann, dass der Satz „Recht auf Einschränkung geltend gemacht“ vermerkt ist und somit keine Verarbeitung seiner pb Daten erfolgt.

- Recht auf Übertragbarkeit (Art 20 DSGVO)
  Gemäß Art 20 Z2 DSGVO übermittelt der/die DS-Beauftragte alle Daten des Betroffenen als CC. an einen anderen verantwortlichen Berufsangehörigen, sobald der/die Datenschutzbeauftragte dessen Benennung und Pflichtenübernahme schriftlich erhalten hat, aber nur wenn eine sichere und verschlüsselte Übertragung möglich ist. Ansonsten nur per eingeschriebener Post.
- Recht auf Beschwerde bei der Datenschutzbehörde

8 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, Lieferanten, Projektpartner zu ermöglichen.

Da nur eine teilautomatisierte und keine umfassende Bewertung persönlicher Aspekte natürlicher Personen, keine 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**, 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

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

Vorab beachtet der/die ÖAS-Datenschutzbeauftragte die sogenannte Robinson-Liste und setzt einen Vermerk „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)

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 mittels Rückemail „unsubscribe“ abzumelden.

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).

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

Macht ein Betroffener seine Rechte auf Widerspruch nicht mit Hilfe des Unsubscribe-Emails geltend, sondern in einer anderen Form, sei es z. B. mündlich oder schriftlich so gilt folgendes:

Sollte der Betroffene dem/der ÖAS-Datenschutbeauftragten nicht persönlich bekannt sein, so muss er/sie 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.
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) innerhalb von maximal 14 Tagen 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 uns.“

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

9.1 Meldung von Datenschutzverletzungen

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.

- Der/die ÖAS-Datenschutzbeauftragte erlangt Kenntnis von einer Datenschutzverletzung.
- **Innerhalb von 72 Stunden** macht er/sie eine Meldung mit Hilfe des „Muster Datenschutzverletzung“ (siehe Anhang) an die gemäß Art 55 DSGVO zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes pb Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Gemäß Art 34 Z3 DSGVO muss keine Benachrichtigung der Betroffenen erfolgen, da die Verletzung des Schutzes pb Daten aufgrund des ÖAS-TOMs (zB Verschlüsselung in Rest und Motion, Backup, …) voraussichtlich kein **hohes Risiko** für deren persönlichen Rechte und Freiheiten zur Folge hat
- Die Datenschutzbehörde ist wohlbegründet gegenteiliger Meinung und fordert die ÖAS auf, alle/gewisse Betroffenen zu informieren, siehe Art 34 Z4 DSGVO.
  - Der / die Datenschutzbeauftragte informiert die Betroffenen umgehend mit einer entsprechenden Variation des „Muster Datenschutzverletzung“ (siehe Anhang)
- Der / die ÖAS-DS-Beauftragte wird 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 Z5 DSGVO.

10 Risikoanalyse

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

10.1 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)“

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

10.1.1 Risikokategorien

Kategorie	pb Daten
1	**Besondere Datenkategorien iSd Art 9 DSGVO (zB Mitarbeiter)**, siehe Punkt 3.3.6. Kat. 08, 15, 36, 37, 46 **=> geheim/vertraulich**
2	Schlüssel, Passwörter, sonstige Vereinbarungen **=> geheim**
3	Geburtsdatum , Bankverbindungen, Kreditkartennummern und -unternehmen, Vertragstext und Geschäftskorrespondenzen, Bewerbungsschreiben, Bewerbungsfotos (siehe Punkt 3.3.6. Kategorien der verarbeiteten Daten) **=> intern/vertraulich**
4	Pb Daten mit vernachlässigbaren bis begrenzten Schutzbedarf, siehe oben alle restlichen Daten

10.1.2 Risiko-Matrix

Schwere					
Existenzgefährdend					
Wesentlich	1,2,3				
Begrenzt					
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 informieren Folgeabschätzung notwendig

10.1.3 Maßnahmen

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

10.1.4 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 (Office, Vorstand)

10.1.5 Integrität

Eingabekontrolle: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt.

10.1.6 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

10.2 Risiko-Matrix mit Maßnahmen

Schwere					
Existenzgefährdend					
Wesentlich	1,2,3				
Begrenzt					

Vernachlässigbar	4				
	Vernachlässigbar	Möglich	Sehr wahrscheinlich	Garantiert	**EWK**

10.2.1 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 Klient nicht informiert werden, nichts desto trotz wird die Behörde bei Data Breach mit Risiko für pb Daten der Kategorie 1 informiert.

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

11 Zusammenfassung und Vorstandsbeschluss

Wir sehen 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.

Lieber Vorstand!

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

Das hier vorliegende Datenschutzkonzept des Vereines ÖAS wurde vom gesamten Vorstand einstimmig am 6.10.2019 angenommen.

……..

Unterschrift
Obmann und Schriftführer

gemäß Statuten

12 Anhang

12.1 Formular Auskunftsrecht

Nimmt eine Person ihr Auskunftsrecht in Anspruch, kann sie eine Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung sind, innerhalb eines Monats nach Antrag verlangen, sofern keine Rechte und Freiheiten anderer Personen beeinträchtigt werden.

Recht auf Auskunft (Art 15 DSGVO)

Ort, am…..

Sehr geehrte/r Frau/Herr …….!

Gemäß Ihrer 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 automatisierte 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.

Kontaktdaten des Verantwortlichen bzw des für den Datenschutz-Zuständigen

Vorstand der ÖAS

12.2 Formular Datenschutzverletzung (WKO)

Datenschutzverletzung

Art 33 EU-Datenschutzgrund-Verordnung (DSGVO) -
Meldung an die Aufsichtsbehörde:
Österreichische Datenschutzbehörde,
Hohenstaufenallee 3, 1010 Wien
E-Mail: dsb@dsb.gv.at

Name und Kontaktdaten des **Verantwortlichen[1]:**

Name und Anschrift:

E-Mail-Adresse, Tel.Nr.:

2.Name und Kontaktdaten des für den **Datenschutz-Zuständigen:**

Name und Anschrift:

E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z. B. Tel. Nr.):

datenschutz@.....

1

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

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

soweit möglich betroffene Kategorien und ungefähre Zahl der **personenbezogenen Datensätze**:

4. Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

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

Siehe TOMs

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

Siehe TOMs

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

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

Wien, am ……

……
Unterschrift Vorstand/Datenschutzbeauftragte*r der ÖAS

12.3 Formular Vertrag Auftragsverarbeitung (WKO)

VEREINBARUNG

ÜBER EINE

AUFTRAGSVERARBEITUNG NACH ART 28 DSGVO

Verantwortliche:	Der Auftragsverarbeiter:
ÖAS Amtierender Obmann/frau zur Zeit der Erstellung Mag. Andreas Höher Verantwortliche*r gemäß DSGVO Eßlinggasse 17/2 Telefon 01/ 212 41 35 Email office@oeas.at	Siehe Liste Anleitung Firma / Name Adresse Email Telefon
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

12.3.1 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].*
Diese Vereinbarung ist als Ergänzung zum bereits geschlossenen Vertrag zu verstehen.

Folgende Datenkategorien werden verarbeitet: *Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bestelldaten, Entgeltdaten, usw.*].
Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung: *Kund*innen, Interessent*innen, Lieferant*innen, Ansprechpartner*innen, Beschäftigte, usw.*]

12.3.2 Dauer der Vereinbarung

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

☐ {Befristete Laufzeit} Die Vereinbarung ist befristet abgeschlossen und endet mit …….

☐ {Unbefristete Laufzeit} Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist laut Vertrag gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

12.3.3 Pflichten der Auftragnehmer*in

(1) Die Auftragnehmer*in verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge der ÖAS zu verarbeiten. Erhält die Auftragnehmer*in einen behördlichen Auftrag, Daten der ÖAS herauszugeben, so hat er - sofern gesetzlich zulässig - die ÖAS unverzüglich darüber zu informieren und die Behörde an diese zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke der Auftragnehmer*in eines schriftlichen Auftrages.
(2) Die Auftragnehmer*in erklärt rechtsverbindlich, dass sie 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 bei der Auftragnehmer*in aufrecht.
(3) Die Auftragnehmer*in erklärt rechtsverbindlich, dass sie/er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.
(4) Die Auftragnehmer*in ergreift die technischen und organisatorischen Maßnahmen, damit die ÖAS 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 der ÖAS alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an die Auftragnehmer*in gerichtet und lässt dieser erkennen, dass die Antragsteller*in sie/ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat die Auftragnehmer*in den Antrag unverzüglich an die ÖAS weiterzuleiten und dies der Antragsteller*in mitzuteilen.
(5) Die Auftragnehmer*in unterstützt die ÖAS 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).

(6) Die Auftragnehmer*in wird darauf hingewiesen, dass sie für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
(7) Der Auftragnehmer*in 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. Die Auftragnehmer*in verpflichtet sich, der ÖAS jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
(8) Die Auftragnehmer*in ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, in ihren Auftrag zu vernichten. Wenn die Auftragnehmer*in die Daten in einem speziellen technischen Format verarbeitet, ist sie verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch der ÖAS in dem Format, in dem sie die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
(9) Die Auftragnehmer*in hat die ÖAS unverzüglich zu informieren, falls sie der Ansicht ist, eine Weisung der ÖAS verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

Nur bei Fernwartung

(a) Sofern die Auftragnehmer*in die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist die Auftragnehmer*in verpflichtet, der ÖAS eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die der ÖAS ermöglicht, die von der Auftragnehmer*in durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(b) Wenn die ÖAS bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

12.3.4 Ort der Durchführung der Datenverarbeitung

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

12.3.5 Sub-Auftragsverarbeiter

Die Auftragnehmer*in ist nicht berechtigt, eine Sub-Auftragsverarbeiter*in heranzuziehen.

12.3.6 Homepage

Die Auftragnehmer*in ist einverstanden, dass ihre Kontaktdaten inkl. Foto ihrer Person auf der Homepage oder anderen Seminarplänen der ÖAS veröffentlicht werden.

Ich nehme diese gesetzlichen Rahmenbedingung laut DSGVO zur Kenntnis.

Datum

Name der Auftragnehmer*in:

Unterschrift:

12.4 Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO)

Diese Verpflichtungserklärung betrifft:

Familienname:

Vornamen:

In Ausübung Ihrer beruflichen oder ehrenamtlichen Tätigkeit erhalten Sie voraussichtlich Kenntnis über personenbezogene Daten (ev. auch von Kindern) gemäß Art 8 DSGVO 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);
- bei einem Verstoß gegen das Datengeheimnis oder eine Verletzung von Geschäfts- und Betriebsgeheimnissen, ist Schadenersatz zu leisten, und zwar ohne Rücksicht auf den tatsächlich eingetretenen Schaden, das durch ein Hearing im Vorstand festgesetzt wird.

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*innen 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 der ÖAS 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, von der Auftraggeberin ÖAS über das Datengeheimnis nach § 6 DSG und die Verschwiegenheitsverpflichtungen nach § 11 UWG belehrt worden zu sein.

Ort, Datum	**Unterschrift des Verpflichteten**

12.4.1 Anhang zum Datengeheimnis

Datengeheimnis nach § 6 DSG

(1) Die Verantwortliche, die Auftragsverarbeiter*in und ihre Mitarbeiter*innen – das sind Arbeitnehmer*innen (Dienstnehmer*innen) 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*innen dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihrer Arbeitgeber*in (Dienstgeber*in) übermitteln. Die Verantwortliche und die Auftragsverarbeiter*in haben, sofern eine solche Verpflichtung ihrer Mitarbeiter*innen 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) zur Verantwortlichen und zur Auftragsverarbeiter*in einzuhalten.

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

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

(5) Ein zugunsten einer Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diese tätige Auftragsverarbeiter*in, 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 Bedienstete eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihr aufgrund des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht 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 der Verletzten statt.

13 Einwilligungserklärung – ÖAS-Mitglieder

13.1.1 BEITRITTSERKLÄRUNG