Verfahrensverzeichnis gemäß EU-Datenschutz-Grundverordnung (DSGVO)

1. Stammdaten des Verantwortlichen (Art. 30+13)

Name: Österreichische Gesellschaft für Sexualwissenschaften
Vereinssitz: Windmühlgasse 15/1/7, 1060 Wien
Kontaktdaten: ✆ +43 664 243 11 78 ✉ office@oegs.or.at

2. Datenverarbeitungen/Datenverarbeitungszwecke (Art. 30+13) Zweck und Beschreibung der Mitglieder-, Sexualakademieteilnehmer*innen, Mitarbeiter*innen- und Bewerber*innenverwaltung

Mitglieder ÖGS:
Führen einer Datenbank (Excel Tabelle) zur Verwaltung der (aktiven) Mitglieder (Zahlungseingänge, Postanschrift, E-Mailadresse) sowie Aufbewahrung der Mitgliedsanträge abgelegt in Ordnern.
Führen einer Mitglieder-Buchhaltung und Rechnungswesen.

Mitarbeiter*innen und Bewerber*innen:
Die Personalverwaltung: Verarbeitung und Übermittlung von Daten für die Personalplanung, Personalanstellung sowie die Personalentlohnung und die damit verbundenen Verarbeitungen und Übermittlungen für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von arbeits- und sozialrechtlich vorgegebener Aufzeichnungs-, Auskunfts- und Meldepflichten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (zB. Korrespondenzen, Bewerbungsschreiben, Dienstzeugnisse, Testergebnisse, Stellenbeschreibungen) in diesen Angelegenheiten etc.

Sexualakademieteilnehmer*innen
Speichern der Anmeldeformulare, Führen von Teilnehmer*innen- und Interessent*innenlisten (Excel-Tabellen), Kontaktaufnahme für die Organisation und Koordination einzelner Module/Curricula (E-Mail, Post, Telefon), Buchhaltung und Rechnungswesen (Excel-Tabellen, Rechnungslegung, Kontoführung), Speichern von Unterlagen für die Zertifizierung/den Abschluss, Korrespondenz mit dem Fort- und Weiterbildungsausschuss der ÖGS bzw. der Lehrgangsleitung (lehrinhaltliche Zuständigkeit), Korrespondenz mit dem Vorstand der ÖGS (finanzielle, rechtliche Zuständigkeit), Korrespondenz mit der externen Steuerberatung (Buchhaltung, Rechnungswesen).

3. Verpflichtung zur Zusammenarbeit mit der Datenschutzbehörde

Die Verpflichtung zur Zusammenarbeit mit der Datenschutzbehörde ist bekannt.

4. Datenschutz-Folgeabschätzung (Art.35)

Eine Datenschutz-Folgeabschätzung gemäß Art. 35 DSGVO wird nicht vorgenommen, da aufgrund der vorgenommenen technischen und organisatorischen Maßnahmen (Maßnahmen gegen Datenverlust und -missbrauch) und durch Zweck und Ausmaß der Verar-

beitung (auf die jeweils gegenständliche Betreuung beschränkt ohne weitergehende Verarbeitung) voraussichtlich ein nur sehr geringes Risiko für die Rechte und Freiheiten der Betroffenen vorliegt.

5. Rechtsgrundlagen

Verpflichtung zur Lohnverrechnung und Buchführung
Bundesabgabenordnung § 4 Abs. 4
ArbeitnehmerInnenschutzgesetz (ASchG); § 349a
Allgemeines Sozialversicherungsgesetz (ASVG), BGBl. Nr. 189/1955 etc.

6. Verträge, Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen zu aufrechten Geschäftsabwicklungen und Mitarbeiter*innendaten in der Geschäftsführung; erledigte Geschäftsfälle im Archiv.

7. Daten der Anwendung, Kategorien der Betroffenen und Empfänger*innen

7.1. Datenverarbeitung Mitglieder

Kategorie	Lfd. Nr.	Datenkategorien	besondere Datenkategorien	Herkunft der Daten	Empfänger*innen	Aufbewahrungsdauer (Jahre)
Mitglieder	1	Name, Vorname	nein	MG		7 Jahre
	2	Adresse	nein	MG		7 Jahre
	3	E-Mailadresse	nein	MG		7 Jahre

7.2. Datenverarbeitung Sexualakademieteilnehmer*innen

Kategorie	Lfd. Nr.	Datenkategorien	besondere Datenkategorien	Herkunft der Daten	Empfänger*innen	Aufbewahrungsdauer (Jahre)
Sexualakademie-teilnehmer*innen	1	Name, Vorname		SATN		7 Jahre
	2	Adresse		SATN		7 Jahre
	3	E-Mailadresse		SATN		7 Jahre
	4	Telefonnummer		SATN		7 Jahre
	5	Geburtsdatum		SATN		7 Jahre
	6	Bankdaten		SATN		7 Jahre
	7	Daten zur Abrechnung		SATN		10 Jahre
	8	Unterlagen zur Zertifizierung		SATN		10 Jahre
	9	Unterlagen für den Abschluss		SATN		7 Jahre

7.3. Datenverarbeitung Mitarbeiter*innen und Bewerber*innen

Kategorie	Lfd. Nr.	Datenkategorien	besondere Datenkategorien	Herkunft der Daten	Empfänger*innen	Aufbewahrungsdauer (Jahre)
Mitarbeiter*innen	1	Name, Vorname				7 Jahre

	2	Adresse				7 Jahre
	3	E-Mailadresse				7 Jahre
	4	Telefonnummer				7 Jahre
	5	Geburtsdatum				7 Jahre
	6	Bankdaten				7 Jahre
	7	Gehalt, Einstufung				7 Jahre
	8	Vordienstzeiten				7 Jahre
	9	Ausbildung und Berufslaufbahn				7 Jahre
	10	Familienstand, Information zu Kindern				7 Jahre
	11	Dienstzeugnisse				7 Jahre
	12	ZA und Urlaubsanträge				7 Jahre
	13	Krankenbestätigungen				7 Jahre
	14	Krankmeldungen				7 Jahre
	15	Lohnabrechnungen				7 Jahre
	16	Stundenzettel				7 Jahre
	17	Ausweis				7 Jahre
	18	An-/Abmeldung SV				7 Jahre
	19	Dienstvertrag				7 Jahre
	20	Arbeitszeitvereinbarung				7 Jahre
	21	Bewerbungsunterlagen				7 Jahre
	22	Jahreslohnkonten				7 Jahre
Bewerber*innen						
	24	Name				Löschen nach Beendigung der Bewerbungsfrist
	25	Anschrift				Löschen nach Beendigung der Bewerbungsfrist
	26	Telefon				Löschen nach Beendigung der Bewerbungsfrist

	27	E-Mailadresse				Löschen nach Beendigung der Bewerbungsfrist
	28	Geburtsdatum				Löschen nach Beendigung der Bewerbungsfrist
	29	Ausbildung und Berufslaufbahn				Löschen nach Beendigung der Bewerbungsfrist
	30	Familienstand; Information zu Kindern				Löschen nach Beendigung der Bewerbungsfrist
	31	Dienstzeugnisse				Löschen nach Beendigung der Bewerbungsfrist

8. Empfänger*innen von Daten

8.1. Behörde

8.1.1. Finanzamt
8.1.2. Sozialversicherungsträger
8.1.3. Mitarbeiter*innenvorsorgekasse

8.2. Vertrags- und Geschäftspartner*innen

8.2.1. Grafikagentur
8.2.2. Banken
8.2.3. Vorstand
8.2.4. Versicherungen
8.2.5. Steuerberatung

8.3. Auftragsverarbeiter*innen

8.3.1. Externe Buchhaltung, Lohnverrechnung, Steuerberatung und Bilanzierung
8.3.2. Provider- und Webdienstleister*in
8.3.3. IT-Verantwortliche*r

9. Beschreibung der technisch-organisatorischen Maßnahmen

9.1. Vereinbarung zwischen Verantwortlichem und Betroffenen (Art.13-21)

Vor Beginn einer Datenverarbeitung wird die Berechtigung zur Verarbeitung der benötigten Daten vertraglich festgelegt. (Muster der Einverständniserklärung im Anhang)

9.2. Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter*innen (Art.28)

Mit allen Auftragsverarbeiter*innen wird eine Vereinbarung abgeschlossen. Die abgeschlossenen Vereinbarungen liegen dieser Dokumentation bei.

9.3. Vereinbarungen zwischen Verantwortlichem und anderen Personen

Mit allen Personen, die für den Verantwortlichen Datenverarbeitungen vornehmen bzw. Zugriff zu Daten haben (z. B. Mitarbeiter*innen) wird eine Vereinbarung abgeschlossen, die die Vertraulichkeit und Sorgfaltspflichten im Umgang mit den Daten festlegt.

9.4. Zugriffskontrolle (Art.32)

Der Zugang zu den Systemen über die personenbezogene Daten zugänglich sind, ist nur über eine einer Person eindeutig zugeordneten Benutzer*innenkennung und ein gemäß untenstehender Definition sicheres Passwort möglich. Das Passwort darf an Andere nicht weitergegeben werden und muss - wenn der Verdacht vorliegt, dass das Passwort bekannt ist - unverzüglich geändert werden. Ein regelmäßiger Passwortwechsel ist nicht notwendig. Mindeststandard für ein Passwort: minimal 8 Zeichen, die Zeichenarten "Kleinbuchstaben", "Großbuchstaben", "Ziffern", "Sonderzeichen" sind möglich und es werden zumindest 2 Zeichenarten verwendet.

9.5. Datensicherheit und Verschlüsselung (Art.32)

Personenbezogene Daten, die nicht auf einem Server abgelegt sind, dürfen nur in verschlüsselten Bereichen/Laufwerken gespeichert werden. Dies bezieht sich sowohl auf mobile (Notebook, USB-Stick, USB-Festplatte, etc.) als auch auf stationäre Datenspeicher (PC). Die Verschlüsselung entspricht 256Bit AES oder besser. Wenn Daten auf einem Server abgelegt sind, werden diese in einem verschlossenem Serverbereich gegen Diebstahl geschützt aufbewahrt und/oder am Server abgelegten Daten sind verschlüsselt (z.B. Windows Server Bitlocker). Mindeststandard für ein Verschlüsselungspasswort: 12 Zeichen

9.6. Datensicherung (Art.32)

Die personenbezogenen Daten werden zumindest 1x pro Woche auf einem externen, Datenträger verschlüsselt gesichert. (Empfohlen: Ein Backup wird außerhalb der Räumlichkeiten wo sich die Arbeitsdaten befinden, aufgehoben).

9.7. Betriebssicherheit (Art.32)

Server und Arbeitsplätze werden so aufgestellt und betrieben, dass eine gemäß Spezifikation ausreichende Temperierung, Schutz vor Feuchtigkeit und ausreichende, sichere Stromversorgung gewährleistet ist. Verwendet werden nur Betriebssysteme, die vom Hersteller mit Updates versorgt und gewartet werden. Updates der Betriebssysteme und wichtigen Applikationen werden laufend und zumindest monatlich überprüft und durchgeführt. Wenn bei aktiver Internetverbindung keine eigene Firewall für ein Netzwerk in Betrieb ist, ist jedenfalls die Firewall des Arbeitsplatzes aktiviert. Auf den Arbeitsplätzen ist ein Virenscanner installiert, aktiviert und laufend mit Updates versorgt.

9.8. Sorgfaltspflicht

Es wird darauf geachtet, dass Bildschirme so platziert sind, dass der Inhalt derselben von anderen Anwesenden nicht ausgespäht werden kann. Wenn die Gefahr besteht, dass andernfalls andere Personen Zugriff zu den Daten erhalten können, wird beim Verlassen des PC-Arbeitsplatzes zumindest der "Bildschirm" gesperrt (z.B. <Windows-Taste>-<L>). Es kommen keine Technologien zur Anwendung, die Eingriffe in die Rechte Betroffener erlauben bzw. verlangen (z.B. Whatsapp). Das Drucken in frei zugänglichen Räumlichkeiten erfolgt über eine Kennwort geschützte Box. Anrufer*innen werden auf die Datenverarbeitung- und speicherung hingewiesen, bevor sie Daten bekannt geben.

9.9. Pseudonymisierung (Art.6, Art.25, Art.32)

Es wird keine über die notwendigen Vorgänge zur Organisation, Abrechnung und Dokumentation der Mitglieder- und Sexualakademieteilnehmender Arbeit hinausgehende Verarbeitung personenbezogener Daten vorgenommen, weswegen mangels weiterer Auswertungsschritte eine Pseudonymisierung nicht notwendig ist.