

Datenschutzkonzept

Stand: Juli 2023

1. Präambel

- Vorwort

2. Allgemeine Bestimmungen

- Schutzzweck
- Anwendungsbereich
- Allgemeine Begriffsbestimmungen

3. Datenschutzpolitik und Verantwortlichkeiten

- Interne Datenschutzgrundsätze
- Örtlich Beauftragte für den Datenschutz
- Schweigepflicht/Datengeheimnis

4. Rechtliche Rahmenbedingungen

- gesetzliche Grundlagen
- Rechtmäßigkeit der Verarbeitung
- Rechtmäßigkeit der Zweckänderung
- Einwilligung

5. Dokumentation/technische und organisatorische Maßnahmen (TOMs)

- Richtlinie für Betroffenenrechte
- Verarbeitungsverzeichnis
- Schutzbedarf der Daten (Datenschutz-Folgeabschätzung)
- Dokumentation der TOMs
- Offenlegung gemäß Art. 44ff. DSGVO
- Auftragsdatenverarbeitung
- Umgang mit Datenpannen
- Sensibilisierungsmaßnahmen für Mitarbeiter/innen
- Aufbewahrungsfristen/Datenvernichtung
- Kontrolle/Überprüfungen

1. Präambel

Innerhalb unseres Vereins genießt der Datenschutz unter Einbeziehung personenbezogener und anderer vertraulicher Daten höchste Priorität. Alle personenbezogenen sowie vertraulichen Daten und Informationen sind in den Schutzbereich miteinbezogen.

Dieses Datenschutzkonzept dient der Gewährleistung des Schutzes der personenbezogenen Daten in unserem Verein.

Grundlage für das Datenschutzkonzept ist die Datenschutz-Grundverordnung (DSGVO). Dieses Gesetz ist europarechtlich anerkannt und regelt die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die Datenverarbeitung dient der Erfüllung unseres Vereinszwecks.

2. Allgemeine Bestimmungen

Zweck dieses Datenschutzkonzeptes ist es, die einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.

Das Datenschutzkonzept gilt für den Verein „Stiller Stern Trier e.V.“ und findet Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit des Vereins oder in dessen Auftrag, unabhängig vom Ort der Verarbeitung. Es gilt für die ganz oder teilweise automatisierte Verarbeitung sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Soweit andere Rechtsvorschriften die Verarbeitung personenbezogener Daten regeln, gehen sie diesem Datenschutzkonzept vor.

Die verwendeten Begriffe in diesem Datenschutzkonzept ergeben sich aus Art. 4 DSGVO (**Anlage 1**).

Darüber hinaus werden folgende **Kurzbezeichnungen** verwendet:

Datenschutz-Grundverordnung:	DSGVO
Stiller Stern Trier e.V.:	Verein Stiller Stern Trier

Die in diesem Datenschutzkonzept genannten „Mitarbeitende“ umfassen folgende Personengruppen:

- alle berufsmäßig im Verein Stiller Stern Trier tätigen Personen
- alle zu ihrer Berufsausbildung tätigen Personen (z.B. Auszubildende, Praktikanten, Studenten etc.)
- Praktikanten ohne Vergütung (z.B. Schülerpraktikanten, andere Ausbildungsträger etc.)
- sonstige Mitarbeitende (z.B. Mitarbeiter für ein Freiwilliges Soziales Jahr, Bundesfreiwilligendienst etc.)
- ehrenamtlich tätige Personen und Personen, die für ihre Tätigkeit eine Aufwandsentschädigung nach § 3 Nr. 26 EStG erhalten
- alle Personen, die im Auftrag des Vereins Stiller Stern Trier tätig werden (z.B. Lieferanten, externe Dienstleister, Leiharbeiter etc.)

Nachfolgend werden diese Personen als Mitarbeitende bezeichnet.

3. Datenschutzpolitik und Verantwortlichkeiten

Die obersten Datenschutzziele des Vereins Stiller Stern Trier sind in den internen Datenschutzrichtlinien zusammengefasst (**Anlage 2**). Die Datenschutzziele orientieren sich an den Datenschutz-Grundsätzen und sind an den Verein Stiller Stern Trier angepasst. Die Grundsätze zur Verarbeitung personenbezogener Daten ergeben sich aus Art. 5 DSGVO (**Anlage 3**). Der Verein Stiller Stern Trier trifft alle erforderlichen Maßnahmen, um die Datenschutz-Grundsätze einzuhalten und deren Einhaltung nachzuweisen.

Der Verein Stiller Stern Trier verpflichtet sich zur kontinuierlichen Verbesserung des Datenschutzmanagementsystems.

Die Gesamtverantwortung für die Einhaltung der DSGVO liegt beim Vereinsvorstand.

Es wurde ein/e Datenschutzbeauftragte/r schriftlich berufen.

Das Datengeheimnis gemäß DSGVO besteht für alle Mitglieder des Vereinsvorstandes sowie für ehrenamtlich Tätige des Vereins Stiller Stern Trier.

Haupt- und ehrenamtliche Tätige werden auf Vertraulichkeit verpflichtet. Hierzu ist eine Verpflichtungserklärung (**Anlage 4**) unter Aushändigung des beigefügten Merkblattes zu unterschreiben.

Bei selbstständigen Honorarkräften wird die Verpflichtungserklärung auf das Datengeheimnis entsprechend mit dem Vertrag vorgenommen (Schweigepflichterklärung als Bestandteil des Honorarvertrags).

4. Rechtliche Rahmenbedingungen

Datenschutz, Datensicherheit und Schweigepflicht sind in unterschiedlichen Gesetzen geregelt und sollen den Umgang mit personenbezogenen Daten und anvertrauten Geheimnissen als besonders sensiblen Bereich regeln.

Für den Verein Stiller Stern Trier gelten bindend folgende rechtlichen Grundlagen:

- Datenschutz-Grundverordnung (DSGVO)
- Interne Nutzungsrichtlinien
- Telemediengesetz (TMG)
- Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG).

Die Rechtmäßigkeit der Datenverarbeitung ergibt sich aus Art. 6 DSGVO (**Anlage 5**). Die Erhebung und Verarbeitung der Daten innerhalb des Vereins Stiller Stern Trier ist zulässig und rechtmäßig, da Einwilligungen, Mitgliedsverträge sowie Förderrichtlinien die Verarbeitung erlauben bzw. anordnen und die Verarbeitung zur Erfüllung der Vereinszwecke erforderlich ist. Der Vereinsvorstand prüft vor der Datenerhebung die Rechtmäßigkeit der Datenverarbeitung gemäß Art. 6 DSGVO.

Personenbezogene Daten werden nur für festgelegte, eindeutige und legitime Zwecke erhoben. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Zweckbindung gemäß Art. 5 DSGVO). Von diesem Grundsatz kann abgewichen werden, wenn eine Voraussetzung besteht, die nach Art. 6 Abs. 4 DSGVO (**Anlage 5**) zulässig ist.

Beruhet die Verarbeitung auf einer Einwilligung, muss nachgewiesen werden können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten

eingewilligt hat (schriftliche Einwilligungserklärung). Es gilt der Grundsatz, dass die Einwilligung verständlich in klarer und einfacher Sprache sowie leicht zugänglich vorgelegt wird. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung hat in jedem Fall schriftlich zu erfolgen.

Bei Minderjährigen hat die Einwilligung durch die Sorgeberechtigten zu erfolgen.

5. Dokumentation/technische und organisatorische Maßnahmen (TOMs)

Art. 25 DSGVO enthält Rahmenregelungen, welche die Betroffenenrechte aus Art. 15 ff. und Art. 34 DSGVO um weitere Vorgaben ergänzen. Diese Rahmenregelungen gelten durchweg für alle Betroffenenrechte. Grundsätzlich muss der Verein Stiller Stern Trier geeignete Maßnahmen treffen, um der betroffenen Person alle Informationen, die nach DSGVO hinsichtlich der Verarbeitung zu geben sind, in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln. Dies gilt insbesondere für Informationen, die sich speziell an Minderjährige richten.

Die Gewährleistung der Informationspflichten gemäß Art. 13 + 14 DSGVO sowie die genaue Verfahrensweise hinsichtlich der Wahrung der Betroffenenrechte gemäß Art. 15 ff. DSGVO sind in der Prozessbeschreibung Betroffenenrechte ausführlich beschrieben. ***Der Leitfaden ist aktuell in Bearbeitung. Die Fertigstellung des Prozessleitfadens ist bis Ende 2023 geplant.***

Gemäß Art. 30 DSGVO ist ein Verzeichnis von Verarbeitungstätigkeiten zu führen, aus dem neben Angaben zum Verein auch Verarbeitungszweck, Beschreibung der Kategorien betroffener Personen sowie der Datenkategorien, Löschfristen, Rechtsgrundlagen für die Verarbeitung, technische und organisatorische Maßnahmen etc. beschrieben werden. ***Das Verzeichnis ist aktuell in Bearbeitung. Die Fertigstellung ist bis Ende 2023 geplant.***

Der Vereinsvorstand hat in Zusammenarbeit mit externen fachkundigen Beauftragten eine Folgenabschätzung der durch die Datenerhebung entstehenden Risiken auf Grundlage des Verzeichnisses von Verarbeitungstätigkeiten zu erstellen. Basis hierfür ist die aktuelle Liste von Verarbeitungsvorgängen für eine Datenschutz-Folgenabschätzung (DSFA) seitens der Aufsichtsbehörde. Die Liste benennt Beispiele von Verarbeitungstätigkeiten, für die eine Datenschutz-Folgeabschätzung durchgeführt werden muss. Sie konkretisiert somit die in Art. 35 Abs. 3 der DSGVO genannten abstrakten Anforderungen an eine DSFA. Die Liste ist jedoch nicht abschließend. ***Ein Leitfaden zur Durchführung der DSFA ist aktuell in Bearbeitung und soll bis spätestens 31.03.2024 erstellt werden.***

Bei neuen Formen der Datenverarbeitung mit hohem Risiko, insbesondere bei Verwendung neuer Technologien, führt der Verein Stiller Stern Trier vorab eine DSFA unter Einbeziehung von externem Fachpersonal durch.

Zusätzlich erstellt der Verein Stiller Stern Trier ein IT-Sicherheitskonzept, in dem die technischen und organisatorischen Maßnahmen bzgl. der Datenverarbeitung genau beschrieben sind. ***Das komplette IT-Sicherheitskonzept soll bis spätestens 31.03.2024 fertiggestellt sein.***

Werden Daten erhoben, verarbeitet oder genutzt, ist der Verein Stiller Stern Trier verpflichtet, alle notwendigen technischen und organisatorischen Maßnahmen zu treffen, um

- den besonderen Anforderungen der DSGVO gerecht zu werden,
- ein angemessenes Schutzniveau zu gewährleisten und
- einen Nachweis hierüber führen zu können.

Grundsätzliche Ziele der TOMs innerhalb des Vereins Stiller Stern Trier sind:

- größtmögliche Verschlüsselung, Pseudonymisierung und Anonymisierung
- Sicherstellung von Vertraulichkeit und Integrität
- Verfügbarkeit
- Belastbarkeit und Wiederherstellbarkeit der Systeme
- Zweckbindung

Der Verein Stiller Stern Trier stellt hierfür folgende Kontrollen sicher:

- Zugangs-, Zutritts- und Zugriffskontrolle
- Datenträgerkontrolle
- Eingabekontrolle
- Transportkontrolle
- Speicherkontrolle
- Übertragungskontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit der Systeme bzw. der Daten

Die TOMs basieren auf einer Risikobetrachtung und entsprechen dem Stand der Technik. Sie werden regelmäßig (nach Bedarf) geprüft und aktualisiert.

Für die Datenübermittlung bzw. Offenlegung von personenbezogenen Daten gelten die Grundsätze gem. Art. 44 ff. DSGVO.

Werden Daten im Auftrag des Vereins Stiller Stern Trier zur Verarbeitung an Dritte weitergegeben, sind die Regelungen dieses Datenschutzkonzeptes und der DSGVO zwingend zu beachten und einzuhalten. Die Verantwortung zur Einhaltung der DSGVO verbleibt auch dann beim Verein Stiller Stern Trier. Der Auftragsverarbeiter wird wie ein Teil des Vereins Stiller Stern Trier gewertet und unterliegt dem Weisungsrecht der beauftragenden Vereinsstelle. Daher ist bei der auftragsbezogenen Weitergabe von Daten besonders auf die Einhaltung der Datenschutzbestimmungen zu achten. Entsprechende schriftliche Vereinbarungen (AV-Vertrag gemäß Art. 28 DSGVO) sind zu treffen. **Ein Verzeichnis über alle Auftragsdatenverarbeitungen wird bis Ende 2023 erstellt.**

Im Falle einer Verletzung des Schutzes personenbezogener Daten hat sofort eine Meldung an den Vorstand zu erfolgen. Für den Verein Stiller Stern Trier wird eine Verfahrensanweisung Beschwerdemanagement (**Anlage 6**) entwickelt.

Der Vereinsvorstand meldet die Datenschutzverletzung - falls erforderlich - unmittelbar an die Aufsichtsbehörde und verwendet hierfür das Muster-Meldeformular der Aufsichtsbehörde. Die gesetzlichen Meldefristen sind einzuhalten.

Die Einhaltung von datenschutzrechtlichen Bestimmungen hängt auch von einer ausreichenden Sensibilisierung und Datenschutzbildung der haupt- und ehrenamtlich

Tätigen des Vereins ab. Datenschulungen stärken insbesondere das Problembewusstsein für datenschutzrelevante Fragestellungen. Schulungen und kurze Unterweisungen sind ein fester Bestandteil des Datenschutzmanagements des Vereins Stiller Stern Trier. Die Themen hierfür unterscheiden sich in Grundschulungen und Schulungen zu speziellen Themen. Die Datenschutz-Schulungen werden mittels Teilnehmerlisten und Handouts dokumentiert. Schulungen für Ehrenamtliche des Vereins Stiller Stern Treir werden nach Bedarf angeboten.

Darüber hinaus werden allen haupt- und ehrenamtlich Tätigen regelmäßig Informationen zu datenschutzrechtlichen Themen in Form von Handreichungen, Aushängen oder Fachartikeln zur Verfügung gestellt.

Der Verein Stiller Stern Trier ist verpflichtet, personenbezogene Daten zu löschen, wenn diese für den Geschäftsprozess nicht mehr erforderlich sind und keine gesetzlichen Aufbewahrungsfristen bestehen.

Da Daten nur für den jeweiligen Zweck und für eine gewisse Dauer erhoben, benutzt und archiviert werden dürfen, sind die Aufbewahrungsfristen in einer Übersicht festgelegt und zusammengefasst. Hierfür werden aktuell entsprechende Löschkonzepte und Löschroutinen erstellt. **Die Liste „Aufbewahrungsfristen“ bzw. das Löschkonzept werden bis spätestens 31.032024 erstellt.**

Die Aufsichtsbehörde kann jederzeit Kontrollen und Überprüfungen im Verein Stiller Stern Trier durchführen. Hierzu ist ihr der Zutritt zu den Räumen, den entsprechenden Unterlagen und PCs zu gewähren. Haupt- und ehrenamtlich tätige Mitarbeitende sowie der Vereinsvorstand müssen sie bei der Erfüllung ihrer Aufgaben unterstützen.

Anlagen

- Anlage 1: Begriffsbestimmungen
- Anlage 2: interne Datenschutz-Richtlinien
- Anlage 3: Grundsätze der Datenverarbeitung
- Anlage 4: Vertraulichkeitserklärung
- Anlage 5: Rechtmäßigkeit der Datenverarbeitung
- Anlage 6: Verfahrensanweisung Beschwerdemanagement