RUDOLF-STEINER SCHULVEREIN SCHWABING e.V.

Datenschutzhinweise für ehrenamtlich tätige Personen

Stand: 16.02.2023, v1.1

Einleitung

Am 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in Kraft getreten.

Ziel der DSGVO ist der besondere Schutz der personenbezogenen Daten. Im Umfeld der Schule und der Kindertagesstätte betrifft dies die Kinder und Jugendlichen, die Beschäftigen mit dem Kollegium und der Verwaltung und die Eltern.

Nicht nur das Schulpersonal kommt mit personenbezogenen Daten in Berührung, sondern auch die ehrenamtlich tätigen Menschen in den Gremien, auf deren Unterstützung die Schule angewiesen ist. Für sie gelten aus datenschutzrechtlicher Sicht vergleichbare Regelungen, wie sie beim hauptamtlich tätigen Personal zur Anwendung kommen. Um zu gewährleisten, dass auch ehrenamtlich mitarbeitende Menschen verantwortungsbewusst und rechtskonform mit personenbezogenen Daten umgehen, hat der Datenschutzbeauftragte des im Sinne der DSGVO verantwortlichen Rudolf-Steiner-Schulvereins Schwabing e.V. nachfolgende Hinweise erstellt.

Generell gilt für unseren Verein folgende allgemeine Datenschutzerklärung:
https://www.waldorfschule-schwabing.de/datenschutz

Der Rudolf-Steiner-Schulverein Schwabing e.V. ist gesetzlich verpflichtet, personenbezogene Daten unter Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften zu verarbeiten.

Einschlägige Rechtsvorschriften sind dabei die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz sowie ggf. bereichsspezifische Rechtsvorschriften.

Der Datenschutzbeauftragte des Rudolf-Steiner-Schulvereins Schwabing e.V. ist für die Überprüfung der Einhaltung der gesetzlichen Vorschriften zum Datenschutz zuständig. Erforderlich sind dabei auch Verhaltensanweisungen für die Beschäftigten und ehrenamtlich tätige Personen.

In diesem Zusammenhang werden personenbezogene Daten, die im Schulinteresse von hauptamtlich und ehrenamtlich tätigen Personen verarbeitet werden, gleichermaßen als „dienstliche“ Daten bezeichnet.

Ehrenamtliche tätige Personen sind Menschen, die innerhalb des Rudolf-Steiner-Schulvereins Schwabing e.V. als Mitglieder eines Gremiums, Arbeitskreises o.ä. mitarbeiten (z.B. Elternrat). Auch ehrenamtlich tätige Personen sollen mithelfen, das Bewusstsein für den Datenschutz zu erhöhen und dies entsprechend in ihrer Klasse zu vertreten. Falls innerhalb der Elternschaft der Klassengemeinschaft Bedarf für die Unterstützung in datenschutzrechtlichen Fragen besteht, kann jederzeit der Datenschutzbeauftragte des Vereins angesprochen werden.

Die Hinweise in diesem Dokument sollen dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden.

Grundsätze für den Umgang mit personenbezogenen Daten

Die nachfolgenden Grundsätze sind von den ehrenamtlich tätigen Personen des Rudolf-Steiner-Schulvereins Schwabing e.V. zu beachten:

a) *Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)*

Auch ehrenamtlich tätige Personen sind schriftlich zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO), insbesondere auch zur Wahrung der Vertraulichkeit und des Datengeheimnisses, zu verpflichten. Ein entsprechendes Formular wird ausgehändigt und ist von den ehrenamtlich tätigen Personen zu unterschreiben.

b) *Einwilligungserklärungen*

Um die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu gewährleisten, ist es für bestimmte Zwecke notwendig, die Einwilligung der betroffenen Person einzuholen und zu dokumentieren. Dies geschieht über entsprechende Formulare als „Einwilligungserklärungen“.

c) *Datenschutzrechtliche Hinweise für den Gebrauch privater Datenverarbeitungsgeräte*

Auf privaten Datenverarbeitungsgeräten dürfen lediglich personenbezogene Daten verarbeitet werden, die zur Ausführung des Ehrenamts erforderlich sind. Dies betrifft im Wesentlichen die Erstellung von Sitzungsprotokollen und Kontaktlisten.

Die personenbezogenen Daten müssen verschlüsselt gespeichert und verschlüsselt übers Internet übermittelt werden. Diese Daten sind getrennt von privaten, persönlichen Daten zu speichern und gegen unbefugten Zugriff zu schützen.

Empfohlen wird eine Speicherung dienstlicher personenbezogener Daten auf einem verschlüsselten USB-Stick (Crypto-USB-Stick), um eine Trennung von dienstlichen und privaten Daten zu gewährleisten.

Personenbezogene Daten müssen umgehend gelöscht werden, sobald diese für die Aufgabenerfüllung nicht mehr erforderlich sind, aber spätestens nach dem Ende des Ehrenamts.

d) *Technische und organisatorische Datenschutzmaßnahmen beim Gebrauch privater Datenverarbeitungsgeräte*

Die DSGVO führt in Art. 32 Abs. 1 zur „Sicherheit der Verarbeitung“ folgendes aus:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher

Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung."

Generell müssen Datenschutzmaßnahmen insbesondere gewährleisten, dass ein unbefugter Zugriff auf die Daten wirksam verhindert wird.

Bei der Festlegung der zu treffenden technischen und organisatorischen Maßnahmen müssen die folgenden Aspekte berücksichtigt werden:

- Zutrittskontrolle
  Die Geräte sollen in einem abschließbaren Raum und / oder abschließbarem Schrank aufbewahrt werden

- Benutzerkontrolle
  Es muss sichergestellt werden, dass das private Gerät nicht durch Unbefugte genutzt werden kann, z.B. durch ein geheimes Passwort für den Gerätezugang

- Zugriffskontrolle
  Es muss gewährleistet sein, dass andere Benutzer des Gerätes, z.B. Familienangehörige, nicht auf die „dienstlichen" Daten zugreifen können, z.B. wird durch Einrichtung verschiedener Benutzerprofile der Zugriff auf die dienstlichen Daten verhindert oder durch Ablage der Daten in einem speziellen Bereich des Dateisystems mit eingeschränkter Zugriffsberechtigung. Es wird empfohlen, dass das Benutzerkonto über keine administrativen Berechtigungen verfügt.

- Datenträger und Speicherkontrolle (Verschlüsselung)
  Es muss sichergestellt sein, dass Unbefugte die gespeicherten Daten nicht lesen können. Die Daten müssen in jedem Fall verschlüsselt abgelegt werden (Festplattenverschlüsselung oder Software ähnlich „TrueCrypt" oder „Cryptomator"). Werden weitere Datenträger wie z.B. USB-Sticks oder externe Festplatten verwendet, müssen die „dienstlichen" Daten auch dort verschlüsselt sein.

- Transportkontrolle
  Wenn Daten an andere Stellen oder Personen übermittelt oder transportiert werden, müssen zuvor die Daten verschlüsselt werden. Das betrifft die Kommunikation über E-Mail oder Messenger, aber auch den physikalischen Transport, hier z.B. über Crypto-USB-Stick.

- **Verfügbarkeitskontrolle**
  Datensicherungen (Backups) sind regelmäßig anzulegen.

- **Datenlöschung**
  Das Löschen mit Betriebssystemmitteln reicht i.d.R. nicht aus, weil Daten trotz dieser Löschung wiederhergestellt werden können. Hinweise, welche Software eingesetzt werden kann, finden Sie auf der Homepage des BSI (Bundesamt für Sicherheit in der Informationstechnik).

Ferner ist folgendes zu beachten:

- Das eingesetzte Betriebssystem muss durch die Installation von Updates oder Patches regelmäßig auf dem aktuellen Stand gehalten werden.

- Es ist eine Firewall einzusetzen (für den Fall, dass sich das Gerät im Internet befindet) sowie eine Virenschutzsoftware. Diese sind stets auf dem aktuellen Programmstand (Version) und aktuellen Stand der Virensignaturen (mehrmals tägliche Updates) zu halten.

- Empfohlen wird, sämtliche Updates (Betriebssystem, Firewall, Virenschutz) automatisiert erfolgen zu lassen, dies kann durch entsprechende Konfiguration der Software erfolgen.

- Passwörter sind so zu wählen, dass sie dem Stand der Technik entsprechen. Es soll nicht dasselbe Passwort für verschiedene Zugänge benutzt werden. Das Passwort muss sicher verwahrt werden und darf nicht irgendwo sichtbar notiert werden (unter Tastatur, als Post-it, in der Schublade auf einem Zettel etc.). Nützlich und sinnvoll ist die Wahl eines „Passwortmanagers“.
  Empfehlungen zum richtigen Umgang mit Passwörtern siehe BSI: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

- Bei der Nutzung von Webportalen darf das eingegebene Passwort nicht im Browser für weitere Sitzungen gespeichert werden. Dies verhindert die unberechtigte Nutzung des Webportals durch andere Nutzer Ihres privaten Umfelds, z. B. durch im Haushalt wohnende Kinder.

- Die Nutzung fremder Internetzugänge (z. B. in Internet-Cafés oder Hot-Spots an öffentlichen Plätzen) ist grundsätzlich verboten, es sei denn, der Internetzugang verfügt über eine Verschlüsselung. Die Nutzung des eigenen WLAN darf nur erfolgen, wenn das WLAN sicher verschlüsselt ist (z.B. aktuelle WPA2-Verschlüsselung).

- Für die Speicherung und sonstige Verarbeitung auch verschlüsselter personenbezogener Daten von privaten Datenverarbeitungsgeräten auf Clouds gelten besondere Anforderungen (siehe BSI).

e) *Einsatz von Software und Diensten auf privaten Datenverarbeitungsgeräten*

Für die Nutzung von Kommunikations- und Organisationsfunktionen kommen Software und internetbasierte Dienstleistungen zum Einsatz.

Es ist darauf zu achten, dass diese Software und Dienste sich den Grundsätzen des europäischen Datenschutzrechts (z.B. DSGVO) verpflichten. Dies ist z.B. bei US-amerikanischen Diensten nicht immer der Fall.

In dem Zusammenhang wird darauf hingewiesen, dass die Nutzung von US-amerikanischen Diensten möglich sein kann, wenn ein angemessenes Datenschutzniveau zum einen durch eine „Privacy Shield"-Zertifizierung, zum anderen aber auch durch den Abschluss eines Auftragsverarbeitungsvertrages auf Basis der sog. EU-Standardvertragsklauseln garantiert wird. Zu berücksichtigen ist auf jeden Fall der CLOUD Act, der amerikanische Internet-Firmen und IT-Dienstleister dazu verpflichtet, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt.

Grundsätzlich sind daher folgende unter Datensicherheitsaspekten weniger kritische Software und Dienste zu verwenden, z.B.:

- E-Mail (Alternativen zu Gmail, Yahoo etc.)
  - Web Access (bereitgestellt vom Provider über https-Protokoll)
  - E-Mail-Client-Software: z.B. Thunderbird

- E-Mail-Verschlüsselung (PGP/MIME)
  - GPG Suite
  - Enigmail
  - Passwortgeschützte ZIP-Anhänge:
    Alternativ können Anhänge als ZIP (z.B. 7-Zip) verschlüsselt und via E-Mail versendet werden. Über einen zweiten Kanal (SMS, Telefon) muss dem Empfänger dann das Passwort mitgeteilt werden. Dies ist eine universelle Lösung, da sie auf allen Betriebssystemen und E-Mail-Clients funktioniert und nicht von der Installation z.B. eines "Add-In" abhängig ist.

- Messenger (Alternativen zu WhatsApp & FB Messenger)
  - Threema
  - Signal
  - Wire

- Umfragetools (Alternativen zu Doodle)
  - Dudle (https://dudle.inf.tu-dresden.de/)
  - Nuudle (https://nuudel.digitalcourage.de/)

- Cloudspeicher (Alternativen zu Dropbox & Google Drive) mit Datenspeicherung innerhalb der Europäischen Union
  - NextCloud
  - ownCloud

f) Nutzung und Verteilung von E-Mails

Unter Einhaltung der in Kapitel c) und d) genannten Maßnahmen ist die Nutzung eines privaten E-Mail-Kontos für „dienstliche“ Zwecke datenschutzrechtlich zulässig.

Dabei ist folgendes zusätzlich zu beachten:

- Um die Vertraulichkeit von Mitteilungen zu gewährleisten, ist sicherzustellen, dass jeder Nutzer ein eigenes personalisiertes E-Mail-Konto verwendet, worauf niemand anderer Zugriff hat. Sogenannte „Familien-Mail-Accounts“ sind datenschutzrechtlich bedenklich und dürfen in dem Zusammenhang nicht verwendet werden.

- Für den Ausnahmefall, dass eine Ende-zu-Ende-Verschlüsselung gemäß Kapitel c) technisch nicht realisiert wurde ist bei der Übermittlung von E-Mails (Verfassen, Weiterleitung, Antworten) darauf zu achten, dass keine personenbezogenen Daten von Menschen übersendet werden, von denen keine Einwilligung vorliegt oder deren Daten nicht ohnehin aufgrund ihrer Position in der Schule (z.B. Geschäftsführer) bekannt sind. Alternativ ist es zulässig, passwortgeschützte Dateien (z.B. MS-Word und MS-Excel) und ZIP-Archive als Anhang einer E-Mail, die ansonsten keine personenbezogenen Daten enthält, zu versenden. Das Passwort muss dann über einen von der E-Mail unabhängigen Kanal (z.B. SMS oder Telefonat) vereinbart werden.

- Für die Übermittlung von E-Mails an eine große Anzahl von Absendern sind die eingerichteten E-Mail-Verteiler nach Maßgabe der folgenden Vorgabe zu verwenden.

- Um zu verhindern, dass E-Mail-Adressen für jeden sichtbar sind, ist eine E-Mail in BCC zu versenden, sodass kein Empfänger sieht, wer diese E-Mail noch erhalten hat. Das geht übrigens auch mit E-Mail-Verteilern. Hierbei handelt es sich um datenschutzrechtlich gebotenes Vorgehen zum Schutz der betroffenen Personen.

Ausnahmen

In begründeten Eil – und Ausnahmefällen kann es der Rudolf-Steiner-Schulverein Schwabing e.V. auch unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit erlauben, dass von den vorstehend ausgeführten Grundsätzen abgewichen wird, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten betroffener Personen, die den Schutz personenbezogener Daten erfordern, überwiegen.

Solche Ausnahmen sind vom DSB zu prüfen und mit der Geschäftsführung abzustimmen, die als Vertretung des Verantwortlichen entscheidet. Genehmigte Ausnahmen sind inklusive einer Begründung zur Gewährleistung der Nachweispflicht zu dokumentieren.

Schulung

Der Verein trägt Sorge dafür, dass auch die ehrenamtlich Tätigen die erforderlichen Unterweisungen erhalten, die für den jeweiligen Umgang mit den Datenschutzvorgaben erforderlich sind.

Informationen und Verantwortlichkeiten

Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	Rudolf-Steiner-Schulverein Schwabing e.V., Leopoldstraße 17, 80802 München Mail: mail@waldorfschule-schwabing.de Fon: (089) 380140-0
Datenschutzbeauftragter (gemäß Art. 37 ff DSGVO)	Rudolf-Steiner-Schulverein Schwabing e.V., Leopoldstraße 17, 80802 München Mail: datenschutz@waldorfschule-schwabing.de Fon: (089) 380140-0
Allgemeine Datenschutzerklärung (gemäß Art. 13 ff DSGVO)	Web: https://www.waldorfschule-schwabing.de/datenschutz