Freie Waldorfschule Hof

RICHTLINIE zum Datenschutz für Beschäftigte

Stand: 01.02.2026, v1.1 (bn)

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 Beschäftigten mit dem Kollegium und der Verwaltung und die Eltern.

Um zu gewährleisten, dass die Beschäftigte verantwortungsbewusst und rechtskonform mit personenbezogenen Daten umgehen, hat der Datenschutzbeauftragte des im Sinne der DSGVO verantwortlichen Vereins "Arbeitskreis Waldorfschule Hof e.V." nachfolgende Hinweise erstellt.

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

Der Verein "Arbeitskreis Waldorfschule Hof 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 Vereins "Arbeitskreis Waldorfschule Hof e.V." ist für die Überprüfung der Einhaltung der gesetzlichen Vorschriften zum Datenschutz zuständig. Erforderlich sind dabei auch Verhaltensanweisungen für die Beschäftigte und ehrenamtlich tätige Personen.

Die Beschreibungen 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 Beschäftigten des Verein "Arbeitskreis Waldorfschule Hof e.V." zu beachten:

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

   Alle Beschäftigte 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 Beschäftigten 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 für schulische Zwecke zur Ausübung der jeweiligen Tätigkeit erforderlich sind. Dies betrifft im Wesentlichen die Daten von Schüler, deren Eltern und ggfs. der Kollegen. 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.

Für Lehrkräfte gilt zusätzlich: Auf privaten Datenverarbeitungsgeräten dürfen lediglich die personenbezogenen Daten jener Schülerinnen und Schüler verarbeitet werden, die von der jeweiligen Lehrkraft selbst unterrichtet werden bzw. deren Klassenlehrer bzw. Oberstufenbetreuer sie ist. Art und Umfang der verarbeiteten Daten orientieren sich an den herkömmlich etwa in einem Notenbuch geführten oder bei der manuellen Zeugniserstellung benötigten Daten. Besonders sensible Daten, etwa über Krankheiten oder Erziehungs- und Ordnungsmaßnahmen von Schülerinnen und Schülern, dürfen nicht auf dem privaten Datenverarbeitungsgerät verarbeitet werden.

Personenbezogene Daten müssen umgehend gelöscht werden, sobald diese für die Aufgabenerfüllung nicht mehr erforderlich sind. Die Aufbewahrungsfristen richten sich nach der Erforderlichkeit der Datenverarbeitung zur Erfüllung schulischer Aufgaben.

Dabei orientieren wir uns unter anderem an den Fristen der Bayerischen Schulordnung (BaySchO, § 37 i.V.m § 40) vom 1. Juli 2016, soweit sie zur Erfüllung des Erziehungs- und Bildungsauftrags nach Art. 1 BayEUG mit den rechtlichen Vorgaben für öffentliche Schulen vergleichbar sind. So bewahren wir zum Beispiel Kopien der Abgangs- und Abschlusszeugnisse bzw. Unterlagen zum Nachweis der Schulpflicht 50 Jahre auf, schriftliche Leistungsnachweise zwei Jahre. Außerdem sind gesetzliche Aufbewahrungsfristen zu beachten.

Personenbezogene Daten von Schülerinnen und Schülern, die Lehrkräfte mit Genehmigung der Schulleitung auf einem privaten Datenverarbeitungsgerät verarbeiten, werden grundsätzlich spätestens nach dem Ende des nächsten Schuljahres auf dem privaten Datenverarbeitungsgerät gelöscht.

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 (z.B. Crypto-USB-Stick).

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 dabei allgemein 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.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Umgang-mit-Passwoertern/umgang-mit-passwoertern_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 in Betracht.

Teilweise kommen Dienste aus datenschutzrechtlich nicht sicheren Drittstaaten zur Anwendung. Als nicht sichere Drittstaaten gelten alle Staaten außer der nachfolgend aufgelisteten: Andorra, Argentinien, FaröerInseln, Großbritannien, Guernesey, Israel, Isle of Man, Japan, Jersey, Kanada (eingeschränkt), Neuseeland, Schweiz, Uruguay, Liechtenstein, Island, Norwegen, bis 10. Juli 2023 auch die USA.

Die Datenübertragung in nicht sicherere Drittstaaten ist nur zulässig, wenn geeignete Garantien für die korrekte Datenverarbeitung im Zielland vorhanden sind. Als geeignete Garantien kommen vor allem EU-Standardvertragsklauseln (teilweise auch „Model Clauses“, „Standard Contractual Clauses“ oder „SCCs“ genannt) in Betracht - die Standardvertragsklauseln müssen zwischen Ihnen und dem Anbieter des Tools vereinbart werden.

Hinsichtlich der bisherigen Einstufung der USA als nicht sicheren Drittstaat hat die EU-Kommission am 10. Juli 2023 mit dem EU-U.S. Data Privacy Framework (Angemessenheitsbeschluss) eine Nachfolgeregelung für den 2020 vom Europäischen Gerichtshof aufgrund einer Klage des Datenschutzaktivisten Max Schems aufgehobenen „Privacy Shield“ angenommen und in Kraft gesetzt.

Der neue Angemessenheitsbeschluss der EU-Kommission für den sicheren Datenverkehr zwischen der EU und den USA, dem “Trans-Atlantic-Data-Privacy-Framework" (TADPF) hat zur Folge, dass die USA datenschutzrechtlich erneut als sicheres Drittland gelten und für Datenexporte mit Sitz in den USA keine zusätzlichen Legitimationsinstrumente mehr erforderlich sind. Die privilegierende Wirkung des TADPF gilt jedoch nur für Datenempfänger, die sich einem Selbstzertifizierungsprozess unterworfen haben, in dessen Rahmen sie sich verpflichten, eine Reihe detaillierter Datenschutzbestimmungen einzuhalten. Es ist also von Relevanz, ob es sich bei dem jeweiligen Anbieter um einen zertifizierten Anbieter, also um ein Unternehmen handelt, das nach den Kriterien des TADPF zertifiziert und unter www.dataprivacyframework.gov gelistet ist.

Allerdings stellt sich weiterhin die rechtliche Problematik des Cloud Acts, einem US-amerikanischen Gesetz, das es US-amerikanischen Sicherheitsbehörden und Geheimdiensten gestattet, Zugriff auf von US-Unternehmen gespeicherte personenbezogene Daten von Bürgern

der Europäischen Union zu nehmen, auch wenn sich die Server dieser Unternehmen und damit auch die personenbezogenen Daten in der EU befinden.

Es ist zudem jedenfalls nicht auszuschließen, dass der Angemessenheitsbeschluss der EU-Kommission wegen der rechtsstaatswidrigen und Handlungen und Vorgehensweisen der amerikanischen Regierung und des damit verbundenen, mit der EU-Rechtslage nicht mehr vergleichbaren Datenschutzniveaus in nächster Zeit aufgehoben wird.

Diese Problematik stellt sich insbesondere auch bei der Nutzung von KI-Chatbots, so dass grundsätzlich vermieden werden muss, personenbezogene Daten in die Prompts einzugeben.

Kommt es im Zusammenhang mit einer Datenverarbeitung zu einem Drittstaatentransfer, ist jedenfalls nicht nur der Transfer selbst legitimationsbedürftig. Datenverarbeiter treffen in diesen Fällen weitere Compliance-Pflichten, u.a. im Zusammenhang mit den Betroffenenrechten, sowie die Pflicht zur Anpassung ihrer datenschutzrechtlichen Dokumentation an die durch das TADPF geänderte Rechtslage.

Aufgrund der mit dem Betrieb US-amerikanischer Systeme verbundenen rechtlichen Risiken, wird daher auch im Sinne der digitalen Souveränität empfohlen, nach Möglichkeit und vorzugsweise die überwiegend datenschutzkonformen Dienstleistungen und Systeme europäischer Anbieter zu erwerben und zu nutzen.

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

- 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

Auch unter Einhaltung der in Kapitel c), d) und e) genannten Maßnahmen ist die Nutzung eines privaten E-Mail-Kontos für „dienstliche“ Zwecke datenschutzrechtlich **NICHT** zulässig.

Es ist ausschließlich das „dienstliche“ E-Mail-Konto zu verwenden!

Dabei ist folgendes zusätzlich zu beachten:

- Um die Vertraulichkeit von Mitteilungen zu gewährleisten, ist sicherzustellen, dass jeder Nutzer sein eigenes personalisiertes E-Mail-Konto verwendet, worauf niemand anderer Zugriff hat. Eine Weiterleitung auf ein privates E-Mail-Konto ist nicht zulässig.

- 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 passwortgeschützte ZIP-Archive als Anhang einer E-Mail (siehe Kapitel e), 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 Verein "Arbeitskreis Waldorfschule Hof 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 Beschäftigte 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)	Arbeitskreis Waldorfschule Hof e.V. Kolpingshöhe 3, 95032 Hof Telefon: (09281) 738150 E-Mail: schulverwaltung@waldorfschule-hof.de
Datenschutzbeauftragter (gemäß Art. 37 ff DSGVO)	Arbeitskreis Waldorfschule Hof e.V. Kolpingshöhe 3, 95032 Hof Telefon: (09281) 738150 E-Mail: datenschutz@waldorfschule-hof.de
Allgemeine Datenschutzerklärung (gemäß Art. 13 ff DSGVO)	Web: www.waldorfschule-hof.de/datenschutzhinweise