Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO

Version: v1.1.6 Stand: 2026-04-01

0. Vertragsparteien

zwischen

Verantwortlicher (Schule/Schulträger)

- Name: [[NAME_VERANTWORTLICHER]]
- Anschrift: [[ANSCHRIFT_VERANTWORTLICHER]]
- Vertreten durch: [[VERTRETUNGSBERECHTIGTE_PERSON_VERANTWORTLICHER]]

und

Auftragsverarbeiter

- Name: SchulMessenger UG (haftungsbeschränkt)
- Anschrift: Am Sölenborn 9, 37085 Göttingen, Deutschland
- Kontakt: support@schulmessenger.de

gemeinsam “Parteien”, einzeln “Partei”.

1. Gegenstand des Auftrags

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen gemäss Art. 28 DSGVO.
2. Gegenstand, Art und Zweck der Verarbeitung ergeben sich aus diesem Vertrag sowie aus:
    - Anlage 1 (Verarbeitungstätigkeiten und Datenkategorien),
    - Anlage 2 (TOM-Matrix),
    - Anlage 3 (Unterauftragsverarbeiterregister),
3. Die Leistung umfasst die Bereitstellung und den Betrieb von SchulMessenger-Funktionen gemäss Bereitstellung der SchulMessenger Apps (iOS, Android, Web/Desktop) inkl. Push-Gateway, Schulverzeichnis-/Lizenzabgleich, In-App-Feedback sowie optionaler IServ- und Standortfunktionen.
4. Optionale Funktionen (z. B. IServ-Integration, Standortfunktion, Analytics-/Diagnosefunktionen) sind nur Vertragsgegenstand, wenn sie beim Verantwortlichen aktiviert sind.
5. Nicht Gegenstand dieses AVV sind Verarbeitungen, für die der Auftragsverarbeiter datenschutzrechtlich selbst Verantwortlicher ist (insbesondere Vertrags- und Abrechnungsdaten).

2. Dauer

1. Dieser AVV tritt am [[INKRAFTTRETENSDATUM]] in Kraft.
2. Der AVV gilt für die Laufzeit des Hauptvertrags über die Nutzung von SchulMessenger.
3. Er endet spätestens mit Beendigung des Hauptvertrags, vorbehaltlich gesetzlicher Aufbewahrungspflichten.

3. Art der personenbezogenen Daten und Kategorien betroffener Personen

1. Die Kategorien betroffener Personen und Datenarten ergeben sich im Einzelnen aus Anlage 1.
2. Der Verantwortliche stellt sicher, dass nur solche Daten verarbeitet werden, die für den vereinbarten Zweck erforderlich sind.

4. Rechte und Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmässigkeit der Verarbeitung, insbesondere für die zulässige Datenübermittlung an den Auftragsverarbeiter, verantwortlich.
2. Der Verantwortliche erteilt Weisungen in Textform.
3. Der Verantwortliche benennt eine weisungsberechtigte Kontaktstelle: [[WEISUNGSKONTAKT_VERANTWORTLICHER]].
4. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Verarbeitung feststellt.

5. Weisungsrecht

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschliesslich auf dokumentierte Weisung des Verantwortlichen, sofern keine zwingende gesetzliche Verpflichtung entgegensteht. Besteht eine solche gesetzliche Verpflichtung, informiert der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung, soweit das anwendbare Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.
2. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
3. Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtlich unzulässig, weist er den Verantwortlichen unverzüglich darauf hin. Die Verarbeitung kann bis zur Bestätigung/Anpassung der Weisung ausgesetzt werden.

6. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich insbesondere:

1. personenbezogene Daten vertraulich zu behandeln und nur befugten Personen zugänglich zu machen,
2. alle mit der Verarbeitung befassten Personen auf Vertraulichkeit zu verpflichten,

3. geeignete technische und organisatorische Massnahmen (TOM) gem. Art. 32 DSGVO umzusetzen und aufrechtzuerhalten,
4. den Verantwortlichen bei der Erfüllung von Betroffenenrechten sowie bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO angemessen zu unterstützen, einschliesslich Datenschutz-Folgenabschätzungen und erforderlicher Konsultationen nach Art. 36 DSGVO,
5. den Verantwortlichen unverzüglich über Datenschutzvorfälle zu informieren,
6. keine unbefugten Unterauftragsverarbeiter einzusetzen,
7. auf Anfrage Nachweise zur Einhaltung dieser Vereinbarung bereitzustellen,
8. Unterstützungsleistungen gemäss Kapitel 16 in dem dort beschriebenen Umfang und innerhalb der dort definierten Reaktionszeiten zu erbringen.

7. Technische und organisatorische Massnahmen (TOM)

1. Die TOM sind in Anlage 2 beschrieben.
2. Der Auftragsverarbeiter darf TOM weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird.
3. Wesentliche Änderungen werden gemäss Änderungsprozess dokumentiert und dem Verantwortlichen mitgeteilt.

8. Unterstützung bei Betroffenenrechten

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten bei der Erfüllung von Anträgen nach Art. 15 bis 22 DSGVO.
2. Gehen beim Auftragsverarbeiter Anfragen Betroffener ein, leitet er diese unverzüglich an den Verantwortlichen weiter, sofern eine Zuordnung möglich ist.
3. Eine direkte Beantwortung gegenüber Betroffenen erfolgt nur auf Weisung des Verantwortlichen.
4. Details zu Kommunikationskanälen, Servicezeiten, Reaktionszeiten und etwaig vergütungspflichtigen Zusatzleistungen ergeben sich aus Kapitel 16.

9. Meldung von Datenschutzverletzungen

1. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten.
2. Die Meldung enthält, soweit bekannt:
    - Art der Verletzung,
    - betroffene Datenkategorien und Personengruppen,
    - bekannte oder wahrscheinliche Folgen,
    - bereits ergriffene oder vorgeschlagene Abhilfemassnahmen,
    - Kontakt für Rückfragen.
3. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

4. Eine Erstmeldung kann unvollständig sein, sofern die fehlenden Informationen ohne schuldhaftes Zögern nachgereicht werden.

10. Unterauftragsverhältnisse

1. Der Verantwortliche erteilt eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern gemäss Anlage 3.
2. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Neuaufnahme/Ersetzung) gemäss der in Anlage 3 festgelegten Benachrichtigungsfrist.
3. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund innerhalb der Frist schriftlich widersprechen.
4. Der Auftragsverarbeiter stellt vertraglich sicher, dass Unterauftragsverarbeiter gleichwertige Datenschutzpflichten einhalten.
5. Im Fall eines berechtigten Widerspruchs prüfen die Parteien unverzüglich eine zumutbare Alternative ohne den betroffenen Unterauftragsverarbeiter.
6. Ist eine zumutbare Alternative nicht verfügbar, kann der Verantwortliche die von der Änderung betroffene Leistung gesondert kündigen; weitergehende Rechte aus Hauptvertrag und Gesetz bleiben unberührt.
7. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der Datenschutzpflichten seiner Unterauftragsverarbeiter voll verantwortlich (Art. 28 Abs. 4 DSGVO).

11. Datenübermittlung in Drittländer

1. Eine Übermittlung in Drittländer erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
2. Die jeweils eingesetzten Transfermechanismen sind in Anlage 3 dokumentiert.
3. Der Auftragsverarbeiter informiert den Verantwortlichen über relevante Änderungen der Transfergrundlagen.

12. Kontrollrechte und Nachweise

1. Der Verantwortliche hat das Recht, die Einhaltung dieses AVV angemessen zu kontrollieren oder durch geeignete, zur Vertraulichkeit verpflichtete Dritte kontrollieren zu lassen.
2. Kontrollen erfolgen stufenweise: primär durch aktuelle Zertifikate, Testate, Auditberichte, Selbstauskünfte und gleichwertige Nachweise.
3. Vor-Ort-Inspektionen sind zulässig, soweit die Dokumentenprüfung im Einzelfall nicht ausreicht, insbesondere bei konkreten Anhaltspunkten für erhebliche Pflichtverletzungen oder nach einem datenschutzrelevanten Sicherheitsvorfall.
4. Regelmässige Audits ohne besonderen Anlass sind auf maximal ein Audit je zwölf Monate je Verantwortlichem beschränkt. Weitere anlasslose Audits sind nur auf gesonderte Vereinbarung der Parteien zulässig.

5. Geplante Audits sind mit einer Vorankündigungsfrist von mindestens 30 Kalendertagen in Textform anzukündigen; bei begründeten dringenden Vorfällen gilt eine verkürzte Frist von mindestens 72 Stunden.
6. Audits sind während der üblichen Geschäftszeiten so durchzuführen, dass der Geschäftsbetrieb des Auftragsverarbeiters und Rechte anderer Kunden nicht unangemessen beeinträchtigt werden.
7. Jede Partei trägt ihre internen Aufwände selbst. Externe Prüfer des Verantwortlichen werden durch den Verantwortlichen vergütet. Ergibt ein Audit einen wesentlichen, vom Auftragsverarbeiter zu vertretenden Verstoss, trägt der Auftragsverarbeiter die angemessenen und nachgewiesenen externen Auditkosten des Verantwortlichen.
8. Der Verantwortliche und beauftragte Dritte dürfen nur auf solche Informationen zugreifen, die für die Prüfung dieses AVV erforderlich sind. Betriebs- und Geschäftsgeheimnisse sowie Mandantentrennung sind zu wahren.

13. Löschung und Rückgabe nach Vertragsende

1. Nach Ende des Auftrags löscht oder gibt der Auftragsverarbeiter alle bei ihm verarbeiteten bzw. in seinem Einflussbereich gespeicherten personenbezogenen Daten des Verantwortlichen nach dessen Wahl zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.
2. Der Verantwortliche teilt seine Wahl (Rückgabe oder Löschung) spätestens innerhalb von 30 Kalendertagen nach Vertragsende in Textform mit.
3. Erfolgt innerhalb dieser Frist keine Weisung, gilt als Standardweisung die sichere Löschung der beim Auftragsverarbeiter verbliebenen personenbezogenen Daten innerhalb weiterer 60 Kalendertage, vorbehaltlich gesetzlicher Aufbewahrungspflichten.
4. Daten in regelmässigen Sicherungen werden mit den turnusmässigen Backup-Rotationen gelöscht; eine produktive Wiederbereitstellung erfolgt nur, soweit technisch erforderlich und unter TOM-Schutz.
5. Art, Fristen und Nachweispflichten für Löschung/Rückgabe ergeben sich im Übrigen aus Anlage 1 und Anlage 2 sowie etwaigen gesetzlichen Anforderungen.
6. Der Auftragsverarbeiter bestätigt dem Verantwortlichen die Umsetzung auf Anfrage in Textform.

14. Vertraulichkeit und Geheimhaltung

1. Beide Parteien behandeln alle im Rahmen dieses AVV erhaltenen vertraulichen Informationen vertraulich.
2. Diese Pflicht bleibt auch nach Vertragsende bestehen.

15. Haftung

1. Die Haftung richtet sich nach den gesetzlichen Vorschriften, insbesondere Art. 82 DSGVO, sowie nach den Regelungen des Hauptvertrags.

2. Im Innenverhältnis der Parteien gelten die Haftungs- und Freistellungsregelungen des Hauptvertrags, soweit gesetzlich zulässig und soweit dadurch zwingende Rechte betroffener Personen nicht eingeschränkt werden.
3. Dieser AVV begründet keine von zwingendem Datenschutzrecht abweichende Haftungsprivilegierung.

16. Unterstützungs-, Audit- und Vergütungsparameter (integriert)

1. Dieses Kapitel konkretisiert die Zusammenarbeit der Parteien für Unterstützungsleistungen nach Art. 28 DSGVO, Auditabläufe sowie die Vergütung zusätzlicher Leistungen.
2. Zwingende gesetzliche Pflichten des Auftragsverarbeiters bleiben unberührt.
3. Dieses Kapitel gilt nur für Leistungen mit Bezug zum in Anlage 1 beschriebenen Verarbeitungsumfang.

16.1 Kommunikationskanäle und Ansprechpartner

Thema	**Primärer Kanal Auftragsverarbeiter**	**Kontakt Verantwortlicher**
Weisungen / Betroffenenrechte	support@schulmessenger.de	[[WEISUNGSKONTAKT_VERANTWORTLICHER]]
Datenschutzvorfälle	support@schulmessenger.de	[[INCIDENT_KONTAKT_VERANTWORTLICHER]]
Audit / Nachweise	support@schulmessenger.de	[[AUDIT_KONTAKT_VERANTWORTLICHER]]
Vertrags-/Abrechnungsthemen	support@schulmessenger.de	[[VERTRAGS_KONTAKT_VERANTWORTLICHER]]

Hinweis: Der Kanal support@schulmessenger.de ist der zentrale Eingang; Meldungen zu Datenschutzvorfällen werden dort mit 24x7-Incident-Triage priorisiert und gemäss den Reaktionszielen aus Abschnitt 16.2 behandelt.

16.2 Servicezeiten und Reaktionsziele

Leistung	**Servicezeit**	**Erstreaktion**	**Ziel zur fachlichen Rückmeldung**
Eingangsbestätigung Weisung/Anfrage	Mo-Fr 09:00-17:00 Uhr (CET/CEST)	8 Stunden	3 Werktage
Unterstützung Betroffenenrechte	Mo-Fr 09:00-17:00 Uhr (CET/CEST)	8 Stunden	5 Werktage
Datenschutzvorfall (hoch)	24x7	2 Stunden	Laufende Updates mind. alle 4 Stunden
Datenschutzvorfall (mittel/niedrig)	24x7	8 Stunden	Laufende Updates nach Lage
Audit-Nachweise	Mo-Fr 09:00-17:00	8 Stunden	Vollständige

(Dokumentenprüfung)	Uhr (CET/CEST)		Bereitstellung in 10 Werktagen

Hinweis: Die Fristen sind Zielwerte und keine Garantiezusagen, sofern nicht im Hauptvertrag abweichend vereinbart.

16.3 Vergütungsregeln

1. Von der laufenden Vergütung des Hauptvertrags umfasst sind:
    - gesetzlich zwingende Unterstützungspflichten nach Art. 28 DSGVO in angemessenem Umfang,
    - übliche Nachweise (z. B. vorhandene Zertifikate, Testate, Standardauskünfte),
    - incident-bezogene Erstunterstützung gemäss AVV.
2. Gesondert vergütungspflichtig sind insbesondere:
    - aussergewöhnlich umfangreiche Auswertungen, Datenaufbereitungen oder Sonderreports,
    - wiederholte gleichartige Audits ohne konkreten Anlass innerhalb eines Zwölfmonatszeitraums,
    - Vor-Ort-Audits, soweit nicht vom Auftragsverarbeiter zu vertretende wesentliche Pflichtverletzungen vorliegen,
    - technische Sonderumsetzungen ausserhalb des vereinbarten Leistungsumfangs.
3. Vergütungssatz für zusätzliche Leistungen: 145 EUR netto je Stunde, sofern keine abweichende Preisliste vereinbart ist.
4. Der Auftragsverarbeiter weist vor Beginn vergütungspflichtiger Zusatzleistungen auf die voraussichtlichen Aufwände hin und holt eine Freigabe des Verantwortlichen ein.

16.4 Auditprozess (operativ)

1. Audits erfolgen nach dem Stufenprinzip:
    - Stufe 1: Dokumentenprüfung (Zertifikate, Berichte, Selbstauskunft),
    - Stufe 2: Remote-Interview/Remote-Review,
    - Stufe 3: Vor-Ort-Inspektion nur, wenn Stufe 1 und 2 nicht ausreichen oder ein begründeter Anlass besteht.
2. Der Verantwortliche benennt den Auditumfang in Textform vorab und beschränkt ihn auf AVV-relevante Prozesse.
3. Der Auftragsverarbeiter darf Informationen schwärzen, soweit dies zum Schutz von Betriebs- und Geschäftsgeheimnissen oder fremden Mandantendaten erforderlich ist.
4. Ergebnisse und festgestellte Massnahmen werden in einem gemeinsamen Protokoll dokumentiert.
5. Bei festgestellten wesentlichen Abweichungen vereinbaren die Parteien risikobasierte Abstellfristen.

16.5 Incident-Kommunikation (operativ)

1. Die Erstmeldung enthält mindestens:
    - Kurzbeschreibung des Vorfalls,
    - bekannte betroffene Systeme/Datenkategorien,
    - Einschätzung der möglichen Auswirkungen,
    - initiale Gegenmassnahmen,
    - Ansprechpartner für Rückfragen.
2. Nachmeldungen erfolgen, sobald neue belastbare Informationen vorliegen.
3. Eine Meldung an Aufsichtsbehörden oder Betroffene durch den Auftragsverarbeiter erfolgt nur nach Weisung oder bei ausdrücklicher gesetzlicher Verpflichtung.

17. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses AVV bedürfen der Textform, soweit gesetzlich zulässig.
2. Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
3. Es gilt deutsches Recht.
4. Gerichtsstand ist, soweit gesetzlich zulässig, `Göttingen`.

---

18. Anlagen (Bestandteil des AVV)

- Anlage 1: Verarbeitungstätigkeiten und Datenkategorien
- Anlage 2: TOM-Matrix
- Anlage 3: Unterauftragsverarbeiterregister

---

19. Unterschriften

Ort, Datum: [[ORT_VERANTWORTLICHER]], [[DATUM_VERANTWORTLICHER]]

Für den Verantwortlichen

Name: [[NAME_UNTERZEICHNER_VERANTWORTLICHER]]

Funktion: [[FUNKTION_UNTERZEICHNER_VERANTWORTLICHER]]

Unterschrift: _____

Ort, Datum: Göttingen, [[DATUM_AUFTRAGSVERARBEITER]]

Für den Auftragsverarbeiter

Name: [[NAME_UNTERZEICHNER_AUFTRAGSVERARBEITER]]

Funktion: [[FUNKTION_UNTERZEICHNER_AUFTRAGSVERARBEITER]]

Unterschrift: _____

Anlage 1 - Verarbeitungstätigkeiten und Datenkategorien

Version: `v1.1.6` Stand: `2026-04-01`

1. Systemkontext (fachlich)

1. SchulMessenger stellt Client-Anwendungen (iOS, Android, Web/Desktop) und zentrale Zusatzdienste bereit.
2. Die Primärverarbeitung von Nachrichteninhalten erfolgt regelmässig auf den vom Verantwortlichen genutzten Matrix-/Schulservern.
3. Zentrale SchulMessenger-Dienste umfassen insbesondere Schulverzeichnis-/Lizenzschnittstellen, Push-Gateway-Funktionen und optionale Zusatzfunktionen.
4. Optionale Funktionen sind nur Bestandteil der Verarbeitung, wenn sie technisch aktiviert sind.

2. Verarbeitungstätigkeiten

Nr.	Verarbeitungstätigkeit	Zweck	Kategorien betroffener Personen	Kategorien personenbezogener Daten	Empfänger/Systeme	Speicher-/Löschfristen	Optionalität	Status
1	Bereitstellung von Nutzerkonten und Anmeldung (Matrix)	Authentifizierung, Sitzungsverwaltung, Berechtigung	Lehrkräfte, Schüler, Eltern, Schuladministration	Benutzername, User-ID, Device-ID, Session-/Access-Token, Rolleninformationen	Matrix-Homeserver des Verantwortlichen, Endgeräte-Clients	Sessiondaten gemäss App-/Serverkonfiguration; Löschung bei Logout/Kontoentfernung nach Systemregeln	Nein	Freigegeben (Basis)
2	Messenger-Kommunikation inkl. Medien	Sichere schulische Kommunikation	Lehrkräfte, Schüler, Eltern, Schulpersonal	Nachrichteninhalte, Dateianhänge, Metadaten (Zeitstempel, Raum-/Thread-ID, Zustell-/Lesestatus)	Primär Matrix-Infrastruktur des Verantwortlichen; Endgeräte	Fristen gemäss Verantwortlichem/Homeserver-Policy; Auftragsverarbeiter speichert Inhalte nicht dauerhaft ausserhalb vereinbarter	Nein	Freigegeben (Basis)

						Systeme		
3	Schulverzeichnis-/Lizenzabgleich	Auswahl Schule, Lizenzprüfung je Homeserver/Rolle	Lehrkräfte, Schüler, Eltern (indirekt), Schuladministration	Schulname, Stadt, Homeserver-Domain, Rollenklassifikation (z. B. Lehrer/Schüler/Eltern), technische Anfrage-Metadaten	API-Endpunkte	`30` Tage; fachliche Stammdaten bis Änderung/Entfall	Nein	Freigegeben (Basis)
4	IServ-Integration (Portal, Verzeichnis, Raumanlage)	Nutzung von IServ-Funktionen innerhalb von SchulMessenger	Lehrkräfte, Schüler, Eltern	IServ-Benutzername, je Plattform ggf. nur flüchtig verarbeitete Zugangsdaten, Session-Cookies, Messenger-Token/CSRF-Token, Privilegien, Suchtreffer aus Verzeichnis	IServ-Portal der jeweiligen Schule, lokale Client-Speicher, ggf. Web-Proxy	Zugangsdaten werden nicht serverseitig persistiert und nicht in zentralen SchulMessenger-Logs gespeichert; clientseitige Sitzungsdaten bis Logout/Reset/Sessionablauf; weitere Fristen gemäss IServ-Betreiber	Ja	Optional (aktivierbar)
5	Push-Benachrichtigungen	Zustellung von Nachrichten-/Ereignishinweisen	Lehrkräfte, Schüler, Eltern	Push-Token/Pushkey, App-ID, Device-Bezug, ggf. Ereignismetadaten	Push-Gateway `sygnal.schulmessenger.de`; optional FCM (Google) und APNS (Apple)	Tokens bis Abmeldung/Token-Rotation/Deinstallation; Gateway-Logs gemäss `30` Tage	Teilweise (plattformabhängig)	Optional (plattformabhängig)
6	Standortfunktion (Standort teilen/anzeigen)	Freiwillige Standortkommunikation in Chats	Lehrkräfte, Schüler, Eltern	Geo-Koordinaten, Genauigkeit, optionale	Matrix-Nachrichtensystem; Kartenvorschau	Standortdaten als Nachrichteninhalt nach den	Ja	Optional (aktivierbar)

				Beschreibung	je Client (Android: Google Maps SDK + Google Static Maps API, iOS: Apple MapKit/Apple Maps-App)	Fristen des Verantwortlichen; lokale Vorschaudaten kurzzeitig		
7	Support und Störungsbearbeitung inkl. In-App-Feedback	Fehleranalyse, Supportantworten, technische Stabilität	Kontaktpersonen des Verantwortlichen, betroffene Nutzer bei Tickets	Kontaktdaten (bei Kontaktaufnahme), Freitext-Nachricht (i. d. R. ohne vollständige Chatinhalte), `user_identifier`, App-/Build-Version, OS-Version, Gerätemodell, Sprache/Locale, ggf. freigegebene Logauszüge	Supportkanal (`support@schulmessenger.de`), In-App-Feedback-Endpunkt unter `www.schulmessenger.de` (`/api/db-feedback-submit`), interne Support- und Ticketingsysteme des Auftragsverarbeiters	Ticket-/Feedbackdaten gemäss 365 Tage; in Supportprozessen nur vom Verantwortlichen/Nutzer bereitgestellte und auf das erforderliche Minimum begrenzte Inhalte	Ja (nur bei Kontaktaufnahme)	Optional (bei Kontaktaufnahme)
8	Diagnostik/Crash-/Nutzungsanalyse (derzeit deaktiviert)	Qualitätssicherung, Stabilität, Fehlerbehebung nur bei expliziter Aktivierung	App-Nutzer	Geräte-/Diagnosedaten, Crash-Informationen, ggf. pseudonyme Nutzungsmetriken	In der Basiskonfiguration keine aktiven externen Diagnosedienste; Aktivierung nur nach dokumentiertem Change- und Freigabeprozess gemäss AVV-Mastervertrag, Kapitel 7 Ziffer 3, sowie mit ergänzendem Eintrag in	Bei deaktivierter Funktion keine Übermittlung an externe Diagnosedienste; bei Aktivierung Fristen gemäss Dienstkonfiguration `90 Tage`	Ja	Deaktiviert (Default)

					Anlage 3			

Statuslegende: - `Freigegeben (Basis)`: Bestandteil der Basiskonfiguration im AVV-Umfang. - `Optional (...)`: Nur bei technischer Aktivierung bzw. Nutzung Bestandteil der Verarbeitung. - `Deaktiviert (Default)`: In der Basiskonfiguration nicht aktiv; Aktivierung nur nach dokumentiertem Change-Prozess.

2.1 Transparenzhinweis (nicht vom AVV-Umfang umfasst)

Die Verarbeitung von Vertrags- und Abrechnungsdaten (z. B. Rechnungsstellung, kaufmännische Aufbewahrungspflichten) erfolgt in eigener datenschutzrechtlicher Verantwortlichkeit des Auftragsverarbeiters und ist nicht Gegenstand dieses AVV.

3. Betroffenengruppen (abschliessende Auflistung für den vereinbarten Leistungsumfang)

- Lehrkräfte
- Schüler
- Eltern/Erziehungsberechtigte
- Schulpersonal
- Schuladministration/Schulträgervertretung
- Supportansprechpartner

4. Datenarten (abschliessende Auflistung für den vereinbarten Leistungsumfang)

- Stammdaten (Name, Benutzerkennung, Rollenbezug)
- Authentifizierungs- und Sitzungsdaten (Token, Sessiondaten, Cookies)
- Kommunikationsinhalte (Text, Audio, Bild, Datei, Standort)
- Kommunikationsmetadaten (Zeitstempel, Raum-/Thread-Zuordnung, technische IDs)
- Geräte-/Pushdaten (Push-Token, Gerätebezug)
- Support- und Diagnosedaten (soweit aktiviert/erforderlich)

5. Lösch- und Aufbewahrungsgrundsätze

1. Der Auftragsverarbeiter setzt Löschung/Rückgabe gemäss Weisung und Vertragsende-Regelung um.

2. Nachrichten- und Fachinhalte folgen primär den Fristen der vom Verantwortlichen betriebenen oder beauftragten Schulserver.
3. Gesetzliche Aufbewahrungspflichten (z. B. handels-/steuerrechtlich) bleiben unberührt.
4. Erfolgt nach Vertragsende keine Weisung innerhalb der Frist aus dem AVV-Mastervertrag, gilt die dort definierte Standardweisung zur sicheren Löschung.

Anlage 2 - TOM-Matrix (Art. 32 DSGVO)

Version: `v1.1.6` Stand: `2026-04-01`

1. Bewertungsrahmen

- Ziel: Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit.
- Die nachfolgenden Massnahmen sind als Mindeststandard zu verstehen und bei Bedarf risikoadäquat zu verschärfen.
- Alle Einträge sind für den vereinbarten Leistungsumfang final freigegeben; Nachweise sind über die nachfolgenden Referenzen dokumentiert.
- Drittdienst- und Transferbezug ist konsistent mit Anlage 3 (`v1.1.6`) zu halten.

2. TOM-Matrix Auftragsverarbeiter

TOM-Bereich	Konkrete Massnahme	Verantwortlich	Nachweis/Intervall	Status
Zutrittskontrolle	Physischer Zutritt zu produktiven Serverstandorten nur für autorisierte Personen (Badge/Schlüsselkonzept, Besuchermanagement)	Auftragsverarbeiter / Unterauftragsverarbeiter	NWS-PHY-01 (Zutrittskonzept RZ), NWS-PHY-02 (Besuchermanagement), Review jährlich	Freigegeben (Basis)
Zutrittskontrolle	Dokumentierte Auswahl und Freigabe von Hostingstandorten inkl. Sicherheitsniveau	Auftragsverarbeiter	NWS-HOST-01 (Standortfreigabe), NWS-HOST-02 (Providerbewertung), Review jährlich	Freigegeben (Basis)
Zugangskontrolle	Administrative Zugänge nur personalisiert, MFA für privilegierte Konten, keine Shared Accounts	Auftragsverarbeiter	IAM-Richtlinie, Zugriffsreview quartalsweise	Freigegeben (Basis)
Zugangskontrolle	Starke Authentifizierung für interne Wartungszugriffe (VPN/Zero-Trust/Bastion)	Auftragsverarbeiter	NWS-IAM-02 (MFA-Konzept), NWS-IAM-03 (Bastion/VPN-Konfiguration), Review quartalsweise	Freigegeben (Basis)
Zugriffskontrolle	Rollen- und Rechtekonzept nach Least-Privilege-Prinzip für Produktivsysteme	Auftragsverarbeiter	Rollenmatrix, Review quartalsweise	Freigegeben (Basis)

TOM-Bereich	Konkrete Massnahme	Verantwortlich	Nachweis/Intervall	Status
Zugriffskontrolle	Trennung von Rollen (Entwicklung/Betrieb/Support) soweit organisatorisch möglich	Auftragsverarbeiter	NWS-ORG-01 (Rollen-/SoD-Matrix), NWS-ORG-02 (Rechteauswertung), Review quartalsweise	Freigegeben (Basis)
Zugriffskontrolle	Clientseitige Absicherung sensibler Sitzungs-/Credential-Daten (iOS Keychain/Secure Storage, Android EncryptedSharedPreferences, Web localStorage/IndexedDB mit kontrolliertem Session-Lifecycle)	Auftragsverarbeiter (Client-Software)	Architektur-/Code-Nachweis, Release-Review	Freigegeben (Basis)
Zugriffskontrolle	Web-/Desktop-Client-Hardening: Session-Clearing bei Logout, Schutz gegen Script-Injection (CSP/Dependency-Hardening), persistente Daten nur für erforderliche Funktionsanteile	Auftragsverarbeiter (Web-/Desktop-Client)	Sicherheitskonzept Web/Desktop, Release-Review	Freigegeben (Basis)
Weitergabekontrolle	Transportverschlüsselung (TLS) für externe und interne API-Kommunikation	Auftragsverarbeiter	TLS-Konfiguration, PenTest/Scan	Freigegeben (Basis)
Weitergabekontrolle	Dokumentierte Schnittstellen für Drittdienste; keine ungeprüfte Datenweitergabe (insb. FCM, APNS, Google Maps Platform, Apple MapKit)	Auftragsverarbeiter	API-Inventar, Change-Protokolle	Freigegeben (Basis)
Weitergabekontrolle	Drittlandtransfers nur auf gültiger Rechtsgrundlage (z. B. SCC, Angemessenheitsbeschluss)	Auftragsverarbeiter	Anlage 3, juristische Prüfung	Freigegeben (Basis)
Eingabekontrolle	Protokollierung administrativer Änderungen an sicherheitsrelevanten Systemparametern	Auftragsverarbeiter	NWS-LOG-01 (Admin-Audit-Logkonzept), NWS-LOG-02 (Aufbewahrungsregel), Review monatlich	Freigegeben (Basis)
Eingabekontrolle	Nachvollziehbarkeit von Weisungen und Umsetzungszeitpunkten	Beide	Weisungsregister, Ticket-/Change-System	Freigegeben (Basis)

TOM-Bereich	Konkrete Massnahme	Verantwortlich	Nachweis/Intervall	Status
Auftragskontrolle	Verbindliche AVV-/Datenschutzklauseln mit Unterauftragsverarbeitern	Auftragsverarbeiter	Vertragsregister, vor Einsatz	Freigegeben (Basis)
Auftragskontrolle	Vorabprüfung neuer Unterauftragsverarbeiter (Security + Datenschutz)	Auftragsverarbeiter	NWS-SUB-01 (Due-Diligence-Checkliste), NWS-SUB-02 (Freigabeprotokoll), vor Einsatz und jährlich	Freigegeben (Basis)
Verfügbarkeitskontrolle	Backup-/Restore-Konzept für zentrale Betriebsdaten und Konfigurationsstände	Auftragsverarbeiter	NWS-BCP-01 (Backup-Policy), NWS-BCP-02 (Restore-Testprotokoll), Tests halbjährlich	Freigegeben (Basis)
Verfügbarkeitskontrolle	Monitoring/Alerting für kritische Dienste und Schnittstellen	Auftragsverarbeiter	NWS-MON-01 (Monitoring-Konzept), NWS-MON-02 (Alerting-Runbook), Review monatlich	Freigegeben (Basis)
Verfügbarkeitskontrolle	Notfall-/Incident-Management mit Eskalationswegen und Kontaktmatrix	Auftragsverarbeiter	Incident-Runbook, Übungen jährlich	Freigegeben (Basis)
Belastbarkeit	Schutz gegen Denial-of-Service und Missbrauch (Rate-Limits, WAF/Firewall je nach Architektur)	Auftragsverarbeiter	NWS-NET-01 (Rate-Limit-/WAF-Regelwerk), NWS-NET-02 (Firewall-Review), Review halbjährlich	Freigegeben (Basis)
Trennungsgebot	Trennung von Test-/Staging-/Produktionsumgebungen	Auftragsverarbeiter	Deployment- und Umgebungsdoku	Freigegeben (Basis)
Trennungsgebot	Mandanten-/Datenkontexttrennung gemäss Plattformdesign	Auftragsverarbeiter und Verantwortlicher	Architekturdoku, Konfiguration	Freigegeben (Basis)
Pseudonymisierung/Minimierung	Verarbeitung nur erforderlicher Daten; optionale Features standardmässig deaktivierbar	Beide	Feature- und Privacy-Konfiguration	Freigegeben (Basis)
Datenschutzfreundliche Voreinstellungen	Privacy-by-Default in App-/Systemeinstellungen soweit technisch umsetzbar	Beide	Release-Checkliste	Freigegeben (Basis)
Löschbarkeit	Dokumentiertes Lösch-/Rückgabeverfahren nach Vertragsende	Auftragsverarbeiter	Löschprotokoll, Abschlussbestätigung	Freigegeben (Basis)

TOM-Bereich	Konkrete Massnahme	Verantwortlich	Nachweis/Intervall	Status
Integrität	Signierte Releases/Build-Pipeline-Schutz, Integritätsprüfung von Artefakten	Auftragsverarbeiter	NWS-CICD-01 (Signierprozess), NWS-CICD-02 (Artefakt-Integritätscheck), je Release	Freigegeben (Basis)
Personal	Vertraulichkeitsverpflichtung und datenschutzbezogene Sensibilisierung der Mitarbeitenden	Auftragsverarbeiter	NDAs/Schulungsnachweise, jährlich	Freigegeben (Basis)
Kontrolle	Interne Audits/Reviews zu TOM-Wirksamkeit und Nachbesserungsmassnahmen	Auftragsverarbeiter	NWS-AUD-01 (Auditplan), NWS-AUD-02 (Massnahmen-Tracking), Review jährlich	Freigegeben (Basis)

Statuslegende: - `Freigegeben (Basis)`: TOM-Massnahme ist im vereinbarten Leistungsumfang verbindlich umgesetzt und nachweisbezogen hinterlegt.

3. Schnittstellenpflichten des Verantwortlichen (Mitwirkung)

Bereich	Pflicht des Verantwortlichen
Rollen/Berechtigungen	Vergabe und Entzug von Nutzerrechten auf schulischen Systemen (z. B. Matrix-/IServ-Admin) gemäss Need-to-know
Endgeräte	Absicherung verwalteter Endgeräte, Betriebssystem-Updates, lokale Zugriffssicherung
Inhalte	Festlegung von Aufbewahrungs-/Löschfristen für Nachrichten und Medien auf den genutzten Schulsystemen
Rechtsgrundlagen	Sicherstellung der datenschutzrechtlichen Rechtsgrundlagen, Information Betroffener, ggf. Einwilligungsmanagement
Incident-Meldung	Unverzügliche Meldung erkannter Sicherheitsvorfälle mit Bezug zur Auftragsverarbeitung

4. Prüf- und Aktualisierungszyklus

1. Die TOM-Matrix wird mindestens jährlich sowie anlassbezogen (wesentliche Architektur-/Dienstleisteränderung) geprüft.
2. Jede Änderung wird versioniert dokumentiert und dem Verantwortlichen nach den vereinbarten Fristen mitgeteilt.
3. Kritische Feststellungen aus Audits, Vorfällen oder Penetrationstests werden risikobasiert priorisiert und mit Frist nachverfolgt.
4. Die operative Auditabwicklung (Stufenmodell, Kosten- und Vertraulichkeitsrahmen) richtet sich ergänzend nach Kapitel 16 des AVV-Mastervertrags.
5. AVV-relevante Nachweise zu den referenzierten TOM-Massnahmen werden dem Verantwortlichen im Regelfall innerhalb von `10` Werktagen nach begründeter Anfrage in geeigneter Form bereitgestellt.

Anlage 3 - Unterauftragsverarbeiterregister

Version: `v1.1.6` Stand: `2026-04-01`

1. Regelungen

1. Diese Anlage enthält alle für den Vertragsumfang relevanten Unterauftragsverarbeiter.
2. Neue oder ersetzte Unterauftragsverarbeiter werden dem Verantwortlichen mindestens `30` Kalendertage vor Wirksamwerden angezeigt.
3. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen.
4. Status `Freigegeben (Basis)` kennzeichnet die in der Basiskonfiguration produktiv berücksichtigten Dienste.
5. Für jeden Dienst ist die Rollenbewertung zu dokumentieren (`Unterauftragsverarbeiter`, `eigenständig Verantwortlicher`, `gemischte/kontextabhängige Rolle`).

2. Register

Nr.	Dienstleister	Rollenbewertung	Leistung/Zweck	Datenbezug	Verarbeitungsort	Drittlandbezug	Transfermechanismus	Benachrichtigungsfrist	Status
1	Hetzner Online GmbH, Industriestrasse 25, 91710 Gunzenhausen, Deutschland	Unterauftragsverarbeiter	Hosting/Betrieb zentraler API-Endpunkte	Schulstammdaten, Homeserver-Domain, rollenbezogene Lizenzanfragen, Support-/Feedbackdaten, technische Verbindungsdaten	EU (Deutschland, Hetzner Cloud Region NBG1)	Nein (Standardbetrieb)	Kein Drittlandtransfer im Standardbetrieb; bei Änderung nur auf gültiger Grundlage nach Art. 44 ff. DSGVO	30	Freigegeben (Basis)
2	Hetzner Online GmbH, Industriestrasse 25, 91710	Unterauftragsverarbeiter	Hosting/Betrieb Push-Gateway	Push-Token/Pushkey, App-ID, ereignisbezog	EU (Deutschland, Hetzner Cloud Region NBG1)	Nein (Gateway-Betrieb); nachgelagerte	Kein Drittlandtransfer auf Gateway-	30	Freigegeben (Basis)

Nr.	Dienstleister	Rollenbewertung	Leistung/Zweck	Datenbezug	Verarbeitungsort	Drittlandbezug	Transfermechanismus	Benachrichtigungsfrist	Status
	Gunzenhausen, Deutschland			ene Zustellinformationen		Plattformdienste siehe Nr. 3/4	Ebene im Standardbetrieb		
3	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Firebase Cloud Messaging)	Unterauftragsverarbeiter (bei aktivierter Android-Pushnutzung)	Push-Zustellung für Android	Push-Token, technische Nachrichtenzustellinformationen	EU/USA (dienstabhängig)	Ja (möglich)	EU-Standardvertragsklauseln gemäss Durchführungsbeschluss (EU) 2021/914 (Art. 46 Abs. 2 lit. c DSGVO), Transfer Impact Assessment und zusätzliche technische/organisatorische Massnahmen	30	Optional (bei Android-Pushnutzung)
4	Apple Inc., One Apple Park Way, Cupertino, CA 95014, USA (APNS)	Unterauftragsverarbeiter (bei aktivierter iOS-Pushnutzung)	Push-Zustellung für iOS	Push-Token, technische Nachrichtenzustellinformationen	EU/USA (dienstabhängig)	Ja (möglich)	EU-Standardvertragsklauseln gemäss Durchführungsbeschluss (EU) 2021/914 (Art. 46 Abs. 2 lit. c DSGVO), Transfer Impact Assessment und zusätzliche technische/organisatorische Massnahmen	30	Optional (bei iOS-Pushnutzung)

Nr.	Dienstleister	Rollenbewertung	Leistung/Zweck	Datenbezug	Verarbeitungsort	Drittlandbezug	Transfermechanismus	Benachrichtigungsfrist	Status
5	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Google Maps Platform: Maps SDK + Static Maps API)	Unterauftragsverarbeiter (bei aktivierter Android-Standortfunktion)	Interaktive Kartenansicht und statische Kartenvorschau in Android	Geo-Koordinaten, Kartenanfrageparameter, technische Verbindungsdaten	EU/USA (dienstabhängig)	Ja (möglich)	EU-Standardvertragsklauseln gemäss Durchführungsbeschluss (EU) 2021/914 (Art. 46 Abs. 2 lit. c DSGVO), Transfer Impact Assessment und zusätzliche technische/organisatorische Massnahmen	30	Optional (bei Android-Standortnutzung)
6	Apple Inc., One Apple Park Way, Cupertino, CA 95014, USA (Apple MapKit / Apple Maps)	Unterauftragsverarbeiter (bei aktivierter iOS-Standortfunktion)	Interaktive Kartenansicht und Kartenvorschau/Übergabe in iOS	Geo-Koordinaten, Kartenanfrageparameter, technische Verbindungsdaten	EU/USA (dienstabhängig)	Ja (möglich)	EU-Standardvertragsklauseln gemäss Durchführungsbeschluss (EU) 2021/914 (Art. 46 Abs. 2 lit. c DSGVO), Transfer Impact Assessment und zusätzliche technische/organisatorische Massnahmen	30	Optional (bei iOS-Standortnutzung)

Statuslegende: - `Freigegeben (Basis)`: Bestandteil der Basiskonfiguration. - `Optional (...)`: Bestandteil nur bei konkret aktivierter Nutzung.

3. Dienste mit gesonderter datenschutzrechtlicher Einordnung

Die folgenden Systeme können technisch beteiligt sein, ohne zwingend Teil der Unterauftragskette von SchulMessenger zu sein. Die finale Einordnung erfolgt pro Integrationsszenario durch Ops/Legal:

System	Typische Rolle	Hinweis
Matrix-/Schulserver der jeweiligen Schule	Infrastruktur des Verantwortlichen oder dessen eigene Dienstleister	In der Regel primäre Fachdatenverarbeitung ausserhalb der Unterauftragskette von SchulMessenger
IServ-Portal der jeweiligen Schule	System des Verantwortlichen/Schulbetreibers	IServ-bezogene Verarbeitung erfolgt in der Regel im Systemkontext der Schule
Plattformdienste der Endgeräteanbieter	ggf. eigenständige Verantwortliche oder gesonderte AV	Einordnung je Plattform-/Vertragslage separat dokumentieren, soweit der jeweilige Dienst nicht bereits in Abschnitt 2 geführt wird

4. Mindestangaben je Registereintrag (Freigabekriterium)

Ein Eintrag gilt erst als freigegeben, wenn folgende Punkte vollständig sind:

1. Vollständiger juristischer Name und Anschrift des Dienstleisters.
2. Dokumentierte Rollenbewertung (Unterauftragsverarbeiter / eigenständig Verantwortlicher / gemischte Rolle) mit Begründung.
3. Konkreter Leistungszweck und Datenbezug.
4. Verarbeitungsland/Region und Drittlandbezug.
5. Dokumentierter Transfermechanismus (falls erforderlich).
6. Definierter Benachrichtigungsprozess inkl. Frist.
7. Interne Freigabe durch Ops und Legal ist dokumentiert und versioniert.