Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

Parteien

Verantwortlicher: der jeweilige Verein, , vertreten durch das annehmende vertretungsberechtigte Vorstandsmitglied laut Annahmeprotokoll („Verein").

Auftragsverarbeiter: Roger Schlegel, Im Mühlahl 6
61203 Reichelsheim (Wetterau) („Betreiber").

§ 1 Gegenstand, Dauer, Abgrenzung

1.1 Der Betreiber verarbeitet personenbezogene Daten im Auftrag des Vereins beim Betrieb der Plattform e.V.-Vorstand. Art, Zweck, Datenkategorien und betroffene Personen ergeben sich aus Anlage 1.

1.2 Die Dauer entspricht der Laufzeit des Nutzungsvertrags zuzüglich der Löschfristen nach § 9.

1.3 Nicht Gegenstand dieses Vertrags sind Daten, die der Betreiber als eigener Verantwortlicher verarbeitet: Kontodaten des Vereins-Admins als Vertragspartner, Abrechnungs- und Bankdaten des Vereins, Support-Korrespondenz und Server-Protokolle der Plattform. Hierfür gilt die Datenschutzerklärung der Plattform.

§ 2 Weisungen (Art. 28 Abs. 3 Buchst. a)

2.1 Der Betreiber verarbeitet die Daten nur auf dokumentierte Weisung des Vereins. Die Nutzung der Plattformfunktionen durch den Verein und seine Nutzer gilt als Weisung; weitere Weisungen erteilt der Vereins-Admin in Textform.

2.2 Hält der Betreiber eine Weisung für rechtswidrig, teilt er dies dem Verein unverzüglich mit und darf die Ausführung bis zur Klärung aussetzen.

2.3 Eine Übermittlung in ein Drittland erfolgt nur an den in Anlage 3 genannten KI-Dienst für die automatische Auswertung von Anträgen und Unterlagen, die der Vorstand einliest.

§ 3 Vertraulichkeit (Buchst. b)

Der Betreiber verpflichtet alle Personen, die Zugang zu Daten des Vereins haben können, auf Vertraulichkeit nach Art. 28 Abs. 3 Buchst. b und Art. 29 DSGVO. Derzeit ist das ausschließlich Roger Schlegel; eine Vertrauensperson für den Notfall (Nutzungsbedingungen Ziff. 10.4) erhält Zugang erst im Notfall und ist ebenso verpflichtet.

§ 4 Sicherheit der Verarbeitung (Buchst. c)

4.1 Der Betreiber trifft die technischen und organisatorischen Maßnahmen der Anlage 2 und hält sie auf dem Stand der Technik. Er darf Maßnahmen durch gleichwertige ersetzen; das Schutzniveau darf nicht sinken.

4.2 Der Betreiber prüft die Wirksamkeit mindestens jährlich (Restore-Test, Konten- und Rechteprüfung, Patch-Stand) und dokumentiert das Ergebnis.

§ 5 Unterstützung des Vereins (Buchst. e und f)

5.1 Der Betreiber unterstützt den Verein bei Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit) mit den Funktionen der Plattform; Anfragen, die den Betreiber direkt erreichen, leitet er unverzüglich an den Vereins-Admin weiter.

5.2 Verletzungen des Schutzes personenbezogener Daten meldet der Betreiber dem Vereins-Admin unverzüglich, spätestens 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt; Nachmeldungen folgen. Die Entscheidung über Meldungen an die Aufsichtsbehörde und Benachrichtigungen trifft der Verein.

5.3 Der Betreiber unterstützt den Verein bei Datenschutz-Folgenabschätzungen und Konsultationen der Aufsichtsbehörde mit den ihm verfügbaren Informationen.

§ 6 Unterauftragsverarbeiter (Buchst. d, Art. 28 Abs. 2 und 4)

6.1 Der Verein genehmigt die in Anlage 3 genannten Unterauftragsverarbeiter allgemein.

6.2 Neue oder geänderte Unterauftragsverarbeiter kündigt der Betreiber dem Vereins-Admin mindestens 30 Tage vorher in Textform an. Der Verein kann binnen 14 Tagen aus wichtigem datenschutzrechtlichen Grund widersprechen; können sich die Parteien nicht einigen, darf der Verein den Nutzungsvertrag außerordentlich zum Wirksamwerden der Änderung kündigen.

6.3 Der Betreiber schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem die Pflichten dieses Vertrags auferlegt, und bleibt dem Verein gegenüber für dessen Pflichterfüllung verantwortlich.

6.4 Hilfsleistungen ohne Zugriff auf Vereinsdaten (Telekommunikation, Reinigung, Wartung von Hardware im Rechenzentrum) sind keine Unterauftragsverarbeitung.

§ 7 Nachweise und Kontrollen (Buchst. h)

7.1 Der Betreiber stellt dem Verein auf Anfrage die Informationen bereit, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind: Anlage 2 in aktueller Fassung, Prüfberichte der Unterauftragsverarbeiter (Hetzner: Prüfung der technischen und organisatorischen Maßnahmen durch TÜV Rheinland), Ergebnis der jährlichen Eigenprüfung nach § 4.2.

7.2 Eine Kontrolle vor Ort oder per Videokonferenz kann der Verein bei berechtigtem Anlass einmal jährlich mit 30 Tagen Vorlauf verlangen; sie stört den Betrieb nicht und wahrt die Vertraulichkeit anderer Vereine. Den Aufwand trägt jede Partei selbst.

§ 8 Pflichten des Vereins

8.1 Der Verein ist für die Rechtmäßigkeit der Verarbeitung, die Information der betroffenen Personen (Datenschutzhinweise des Vereins) und die Wahrung der Betroffenenrechte verantwortlich. Er führt sein Verzeichnis der Verarbeitungstätigkeiten; Anlage 1 dient als Vorlage für den Eintrag.

8.2 Der Verein benennt den Vereins-Admin als Ansprechperson für Datenschutzfragen und hält die Angabe aktuell.

8.3 Der Verein stellt sicher, dass über die Plattform keine besonderen Kategorien personenbezogener Daten und keine Daten von Schülerinnen und Schülern über das Notwendige hinaus erhoben werden.

§ 9 Löschung und Rückgabe (Buchst. g)

9.1 Während der Laufzeit kann der Vereins-Admin jederzeit einen Vollexport ziehen; einzelne Daten löscht der Verein selbst in der Plattform.

9.2 Nach Vertragsende gilt: 30 Tage Zugriff auf den Vollexport, danach Löschung aller Daten des Mandanten, Überschreiben der Sicherungen spätestens 90 Tage nach Vertragsende, Löschbestätigung in Textform auf Wunsch. Gesetzliche Aufbewahrungspflichten des Betreibers für eigene Vertrags- und Abrechnungsdaten bleiben unberührt.

9.3 Bei Einstellung der Plattform gilt Ziff. 10.3 der Nutzungsbedingungen: Der Vollexport bleibt sechs Wochen nach dem Einstellungstermin abrufbar; danach löscht der Betreiber alle Daten des Vereins, Sicherungskopien werden spätestens 30 Tage später überschrieben. Vertrags- und Abrechnungsdaten des Betreibers nach § 1.3 bleiben unberührt.

§ 10 Haftung und Schlussbestimmungen

10.1 Die Haftung richtet sich nach Art. 82 DSGVO. Im Innenverhältnis der Parteien gilt die Haftungsregelung der Nutzungsbedingungen, soweit gesetzlich zulässig.

10.2 Bei Widersprüchen in Datenschutzfragen geht dieser Vertrag den Nutzungsbedingungen vor. Änderungen bedürfen der Textform; Änderungen der Anlagen 2 und 3 nach § 4.1 und § 6.2 genügen. Für sonstige Änderungen gilt Ziff. 12.1 der Nutzungsbedingungen entsprechend.

10.3 Abschluss: Der Vertrag wird in der Plattform elektronisch bestätigt (Art. 28 Abs. 9 DSGVO, elektronisches Format). Die Plattform speichert Version, Zeitpunkt und bestätigende Person und stellt den Vertrag als PDF bereit.

Anlage 1 — Gegenstand der Verarbeitung

Zweck: Unterstützung der Vorstandsarbeit des Vereins — Entgegennahme und Bearbeitung von Förderanträgen, Beschlussfassung im Umlaufverfahren, Terminfindung, Versand von Rundmails des Vereins (Mailversand), Archivierung der Vorgänge für zwölf Jahre, Auswertungen, Vollexport. Art der Verarbeitung: Speichern, Anzeigen, Versenden von E-Mails, Konvertieren von Dokumenten in PDF, automatische Auswertung von Anträgen und Unterlagen, die der Vorstand über „Neuer Vorgang“ einliest, durch einen KI-Dienst (Anlage 3).

Betroffene Personen	Datenkategorien	Besonderheiten
Vorstandsmitglieder und Vereins-Admins	Name, E-Mail, Passwort-Hash, Rolle, Zeitraum der Stimmberechtigung, namentliche Stimmen und Anmerkungen, Zeitstempel	Stimmen bleiben zwölf Jahre im Archiv
Antragstellerinnen und Antragsteller (meist Lehrkräfte)	Name, E-Mail, Antragsinhalte, Anhänge, Kopie der Eingangsmail, Korrespondenz zum Vorgang	keine Daten von Schülerinnen und Schülern, keine besonderen Kategorien
Externe Eingeladene (Terminfindung)	Name, E-Mail, Antworten zu Terminvorschlägen	automatische Löschung 90 Tage nach dem Termin, der Absage oder dem letzten Terminvorschlag

Betroffene Personen	Datenkategorien	Besonderheiten
Empfängerinnen und Empfänger von Rundmails des Vereins (Mailversand)	E-Mail-Adresse und Inhalt der Mail; bei Unzustellbarkeit Adresse und Grund; Antworten an die Absenderadresse	Adressen gespeichert bis sechs Wochen nach dem Versand (zum Nachsehen im Verlauf), nicht in den Sicherungen der Plattform; Rückläufer höchstens 7 Tage; Antworten werden als Text an den Verein weitergeleitet und nicht gespeichert; Betreff, Text und Anlagen bleiben im Verlauf des Vereins
Zahlungsempfänger von Förderungen	Name oder Bezeichnung, Betrag, Datum, Förderkategorie	keine Bankverbindungen von Privatpersonen
Kassenwart und weitere Empfänger von Beschlussmitteilungen	Name, E-Mail	—
Alle Nutzer	Anmelde- und Antragsversuche mit Netzadresse	90 Tage, dann Löschung
Alle Nutzer	Verlauf: Anmeldungen, Exporte, Rollenänderungen, Änderungen am Vorgang, gekürzte IP-Adresse	so lange wie der Vorgang bzw. der Verein, dann Löschung mit diesem

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Bereich	Maßnahmen
Zutritt und Infrastruktur	Betrieb auf Servern der Hetzner Online GmbH in deutschen Rechenzentren (ISO 27001, technische und organisatorische Maßnahmen jährlich durch TÜV Rheinland geprüft); keine Verarbeitung auf privaten Geräten
Zugang	Persönliche Konten je Person; Passwortmindestlänge, Rate-Limit gegen Brute-Force, sofortige Sperrung deaktivierter Konten; Betreiberzugänge (Hetzner, IONOS, Repository, Anthropic-Konsole) mit Zwei-Faktor-Authentifizierung, Server nur per SSH-Schlüssel
Zugriff und Rollen	Rollen Admin, Vorstandsmitglied, Antragsteller; Betreiber sieht auf Plattformebene nur Zähler und technische Zustände, keine Inhalte der Vereine; Anmeldungen am Server protokolliert das Betriebssystem (90 Tage), jede Anmeldung am Server wird dem Betreiber gemeldet
Mandantentrennung	Jeder Verein in eigenem Mandanten, Zuordnung über Hostname und Mandanten-ID; automatisierte Cross-Tenant-Tests vor jedem Deployment; täglicher automatischer Kontrolllauf im Betrieb mit Testvereinen; personalisierte Links mit Token, zeitlich begrenzt
Übertragung	TLS für alle Verbindungen (automatische Zertifikate); E-Mail-Versand über authentifizierten SMTP mit SPF, DKIM und DMARC; Rückläufer werden über IMAP mit TLS abgerufen, andere Nachrichten im Absenderpostfach bleiben unberührt
Eingabe und Nachvollziehbarkeit	Verlauf (Anmeldung, Passwort-Reset, Rollenänderung, Export, Sperrung, Betreiberaktionen, Vertragsannahmen) so lange wie der Verein; Anmelde- und Antragsversuche 90 Tage; Beschlüsse nach Feststellung unveränderbar; Verlauf am Vorgang

Bereich	Maßnahmen
Verfügbarkeit	Tägliche konsistente Sicherung der Datenbank und der Dateien mit Integritätsprüfung, 18 Sicherungsstände, zusätzlich tägliche Server-Sicherung des Hosting-Anbieters an getrenntem Speicherort in Deutschland, die Empfängeradressen des Mailversands der letzten sechs Wochen enthalten kann und nach sieben Tagen überschrieben wird; vierteljährlicher Restore-Test; Ziel Wiederanlauf 48 Stunden, Datenverlust höchstens 24 Stunden; täglicher automatischer Funktionscheck mit Alarmierung
Eingaben Dritter	Antragsformular mit Bestätigungslink, Spam-Schutz ohne Drittdienste, Datei-Whitelist mit Inhaltsprüfung, Größenlimit; Dokumentkonvertierung isoliert mit Zeitlimit; KI-Ergebnisse nur als Vorschlag
Datensparsamkeit und Löschung	IP-Adressen nur zur Abwehr von Missbrauch vollständig (Anmelde- und Antragsversuche, 90 Tage), sonst gekürzt; keine Protokollierung von Seitenaufrufen, Fehlermeldungen der Dienste nach Größe begrenzt; Empfängeradressen des Mailversands sechs Wochen nach dem Versand und nicht in den Sicherungen der Plattform, Rückläufer 7 Tage; unbestätigte Anträge 7 Tage, Exportdateien 7 Tage, Terminfindungen 90 Tage nach dem Termin; keine Analyse- oder Tracking-Dienste, keine Cookies außer Sitzung
Betrieb und Updates	Monatliches Patch-Fenster (Abhängigkeiten, Container-Image neu gebaut); Deployment-Routine Sicherung → Tests → Deployment → Funktionscheck → Rückfall auf vorheriges Image; getrennte Umgebungen für Entwicklung und Produktion
Vorfallmanagement	Ablauf für Verdacht auf Kompromittierung: Eindämmung, Schlüsseltausch, Neuaufbau aus Sicherung, Information der Vereine binnen 24 Stunden, Nachbereitung; Notfallumschlag für den Ausfall des Betreibers
Auftragskontrolle	AV-Verträge mit allen Unterauftragsverarbeitern (Anlage 3); jährliche Durchsicht des Sicherheitskonzepts; Verzeichnis der Verarbeitungstätigkeiten des Betreibers

Anlage 3 — Unterauftragsverarbeiter

Unternehmen	Leistung	Standort der Verarbeitung	Grundlage
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server (VPS) und Server-Backups	Deutschland (Falkenstein oder Nürnberg)	AV-Vertrag online im Kundenkonto; technische und organisatorische Maßnahmen jährlich durch TÜV Rheinland geprüft; Subunternehmer laut Hetzner-Liste
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Domains, DNS, E-Mail-Postfächer, Versand (SMTP) einschließlich Mailversand des Vereins und Abruf der Rückläufer (IMAP), Mail-Import	Deutschland	AV-Vertrag Bestandteil der IONOS-Vertragsbedingungen seit 19.07.2022

Unternehmen	Leistung	Standort der Verarbeitung	Grundlage
Anthropic, PBC, San Francisco, USA	Automatische Auswertung von Anträgen und Dokumenten, die der Vorstand über „Neuer Vorgang“ einliest (Überführung in die Formularfelder der Bearbeitung)	USA	Data Processing Addendum mit EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO), Bestandteil der Commercial Terms; vertraglich kein Training mit Kundeninhalten

Zusatzmaßnahmen und Kurzbewertung für die Übermittlung an Anthropic: Übermittelt werden nur Antragstext und Anhang eines eingelesenen Antrags oder einer anderen Beschlussunterlage — Beträge, Projektbeschreibungen und, soweit sie im Dokument stehen, Namen und Kontaktdaten der Antragstellenden (meist Lehrkräfte), bei anderen Beschlussunterlagen zusätzlich Namen von Vorstandsmitgliedern und Inhalte von Vorstandssitzungen; keine besonderen Kategorien. Name, E-Mail und Bankverbindung aus den Formularfeldern werden nicht übermittelt, Bankverbindungen in Texten vorher entfernt; auf Fotos und Scans können sie enthalten sein. Anträge sollen keine Namen von Schülerinnen und Schülern enthalten. Die Daten werden nur zur Antwort verarbeitet und nicht zum Training genutzt; die Übertragung ist verschlüsselt. Anthropic ist nicht nach dem EU-US Data Privacy Framework zertifiziert; die Übermittlung stützt sich auf die Standardvertragsklauseln. Das Risiko für die Betroffenen ist gering; die Auswertung ist Bestandteil der Plattform und in den Datenschutzhinweisen des Vereins beschrieben.