Vereinbarung über eine Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO

Version 1.0.0 · Stand: 30.09.2026

Vertragsparteien

Der Verantwortliche (Auftraggeber): das Unternehmen, das über die Plattform praktiko.at ein Abonnement (Enterprise-Paket) abschließt. Die Identifikation erfolgt durch die im Onboarding angegebenen Daten: Firmenwortlaut, Anschrift, Firmenbuch- bzw. ZVR-Nummer, vertretungsbefugte Person und E-Mail-Adresse. Diese Daten werden in die Annahmeerklärung übernommen.

Der Auftragsverarbeiter (Auftragnehmer): Praktiko Junior Company, Bahnhofstraße 42, 4840 Vöcklabruck, Österreich, ein Schulprojekt im Rahmen des Junior Company Programms von Junior Achievement. Rechtsträger bzw. Vertragspartner Siegmar Kroismayr. Vertreten durch: Siegmar Kroismayr.

Ansprechpartner Datenschutz des Auftragnehmers: office@praktiko.at

1. Gegenstand, Rollenabgrenzung und Dauer

1.1 Gegenstand. Gegenstand ist die Bereitstellung und der Betrieb der Vermittlungsplattform „Praktiko“ (praktiko.at) durch den Auftragnehmer. Dazu gehören Stelleninserate, Bewerbungsmanagement, Direktkommunikation (Chat) zwischen Bewerbern und Auftraggeber sowie das Modul „QR-Connect“ zur Lead-Erfassung auf Messen, soweit dabei personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden.

1.2 Rollenabgrenzung. Der Auftragnehmer handelt nur in folgendem Umfang als Auftragsverarbeiter: Verarbeitung der Bewerbungsdaten ab Eingang einer Bewerbung oder ab Freigabe eines Profils an den Auftraggeber (auch über QR-Connect), der Notizen, Bewertungen und Statusangaben des Auftraggebers, der Chat-Kommunikation im Bewerbungsverfahren, der Stelleninserate sowie der Daten der Nutzer des Auftraggebers, soweit sie für dessen Bewerbungsmanagement erforderlich sind.

Der Auftragnehmer ist **eigener Verantwortlicher** für den Betrieb der Plattform selbst, insbesondere für Bewerberkonten und Bewerberprofile, das automatisierte Job-Matching, die Kontoverwaltung und Abrechnung, die Sicherheits- und Systemprotokollierung sowie eigene Nutzungsstatistiken. Hierfür informiert der Auftragnehmer die Betroffenen in seiner eigenen Datenschutzerklärung. Diese Verarbeitungen sind nicht Gegenstand dieser Vereinbarung.

1.3 Dauer. Die Vereinbarung wird auf unbestimmte Zeit geschlossen und gilt, solange der Hauptvertrag (Enterprise-Abonnement) besteht. Sie endet nicht mit dem Abonnement, sondern erst mit der vollständigen Rückgabe oder Löschung der Daten nach Abschnitt 7 (einschließlich Ruhefrist).

2. Art, Zweck, Betroffene und Datenkategorien

2.1 Art und Zweck. Die Verarbeitung erfolgt ausschließlich zur Abwicklung von Bewerbungsprozessen und zur Vermittlung von Praktika, Ferialjobs, Lehrstellen und Diplomarbeiten, einschließlich der dafür erforderlichen Systemfunktionen und Kommunikationskanäle. Bei „QR-Connect“ dient die Verarbeitung der Kontaktaufnahme zu Vermittlungszwecken auf Grundlage der aktiven Profilfreigabe durch die Bewerberin bzw. den Bewerber. Eine Verwendung für Direktwerbung ist nicht Gegenstand des Auftrags.

2.2 Betroffene. (a) Bewerberinnen und Bewerber (Schülerinnen und Schüler, Studierende, Arbeitssuchende), die **mindestens 14 Jahre alt** sind; (b) Mitarbeiterinnen, Mitarbeiter, Vertreter, Vertreterinnen und Recruiter des Auftraggebers.

2.3 Datenkategorien.

- **Stammdaten:** Vor- und Nachname, Geburtsdatum, Geschlecht.
- **Kontaktdaten:** E-Mail-Adresse, Telefonnummer, Anschrift bzw. Wohnort.
- **Profil- und Bewerbungsdaten:** Schulbildung, Schultyp, Fachrichtung, Kenntnisse, Interessen, Mobilitätsangaben, Lebensläufe, Zeugnisse, Motivationsschreiben.
- **Inhalts- und Kommunikationsdaten:** Chat-Nachrichten, hochgeladene Dateien und Anhänge, Profil- und Firmenbilder.
- **Technische Nutzungsdaten, soweit für Betrieb, Sicherheit und Nachvollziehbarkeit der Auftragsleistung erforderlich:** IP-Adressen, Session-Tokens, Zeitstempel, Logfiles. Darüber hinausgehende Nutzungsauswertungen (z. B. Verweildauern) erfolgen nur in eigener Verantwortung des Auftragnehmers nach Abschnitt 1.2.

2.4 Minderjährige. Bewerberinnen und Bewerber können minderjährig sein. Der Auftragnehmer lässt Registrierungen erst ab 14 Jahren zu. Der Auftraggeber verarbeitet die Daten Minderjähriger nur für den konkreten Vermittlungszweck, beschränkt den Zugriff auf die mit dem Verfahren befassten Personen und gibt die Daten nicht an Dritte weiter. Für den Abschluss von Verträgen mit Minderjährigen (z. B. Lehr- oder Praktikumsverträge) ist der Auftraggeber verantwortlich.

2.5 Besondere Kategorien (Art. 9 DSGVO). Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nicht Zweck der Plattform. Der Auftragnehmer weist Bewerber/innen im Upload-Dialog darauf hin, sensible Angaben (insbesondere Gesundheitsdaten und religiöse Überzeugungen) aus hochgeladenen Zeugnissen und Lebensläufen zu entfernen oder zu schwärzen, soweit sie für die Bewerbung nicht zwingend erforderlich sind. Ein Inhaltsfilter findet nicht statt; die Einhaltung obliegt den Bewerber/innen als datenschutzrechtlich Verantwortlichen für die Inhalte der von ihnen hochgeladenen Dokumente.

3. Pflichten des Auftragnehmers

3.1 Weisungsbindung. Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers. Weisungen ergeben sich aus dem Hauptvertrag, dieser Vereinbarung, den vom Auftraggeber vorgenommenen Einstellungen in der Plattform und aus Weisungen in Textform an office@praktiko.at. Weisungsberechtigt sind die Nutzer mit der Rolle „Owner“ sowie weitere vom Auftraggeber in Textform benannte Personen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

Dies gilt auch für die Übermittlung in Drittländer (Abschnitt 5). Ist der Auftragnehmer nach Unionsrecht oder dem Recht eines Mitgliedstaats zu einer weiteren Verarbeitung verpflichtet (z. B. behördliche oder gerichtliche Anordnung), informiert er den Auftraggeber vorab, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

3.2 Keine Verarbeitung zu eigenen Zwecken. Die im Auftrag verarbeiteten Daten (Abschnitt 1.2) verwendet der Auftragnehmer nicht für eigene Zwecke.

3.3 Vertraulichkeit. Alle zur Verarbeitung befugten Personen sind vor Aufnahme der Tätigkeit auf Vertraulichkeit und Datengeheimnis (§ 6 DSG) verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht. Die Verpflichtung besteht über das Ende der Tätigkeit hinaus fort.

3.4 Datensicherheit. Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO gemäß Anlage ./1 und entwickelt sie entsprechend dem Stand der Technik weiter, ohne das vereinbarte Schutzniveau zu unterschreiten.

3.5 Unterstützung. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Betroffenenanfragen (Kapitel III

DSGVO) und bei den Pflichten nach Art. 32 bis 36 DSGVO. Anfragen Betroffener zu im Auftrag verarbeiteten Daten leitet er unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

3.6 Verletzungen des Schutzes personenbezogener Daten. Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes der im Auftrag verarbeiteten Daten unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis. Die Meldung enthält, soweit bekannt, Art der Verletzung, betroffene Personen und Datenkategorien (mit ungefährer Anzahl), wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen sowie einen Ansprechpartner. Fehlende Angaben werden nachgereicht. Der Auftragnehmer dokumentiert jede Verletzung.

3.7 Nachweise und Überprüfungen. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung dieser Vereinbarung zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer. Überprüfungen sind mit mindestens 14 Tagen Vorlauf anzukündigen, finden während der üblichen Geschäftszeiten statt, beeinträchtigen den Betrieb und andere Kunden nicht unverhältnismäßig und erfolgen höchstens einmal jährlich, außer bei einer Datenschutzverletzung oder konkretem Verdacht. Der Nachweis kann auch durch aktuelle Prüfberichte oder Zertifikate erbracht werden. Jede Partei trägt ihre eigenen Kosten.

3.8 Verzeichnis. Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

4. Pflichten und Rechte des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Wahl der Rechtsgrundlage und die Information der Betroffenen nach Art. 13 und 14 DSGVO verantwortlich, soweit er für die Verarbeitung verantwortlich ist.

4.2 Der Auftraggeber legt für abgelehnte Bewerbungen angemessene Löschfristen fest (üblich sind etwa sieben Monate) und nutzt dafür die Löschfunktionen der Plattform.

4.3 Der Auftraggeber schützt seine Zugangsdaten, vergibt Rollen nach dem Minimalprinzip und nennt dem Auftragnehmer einen Ansprechpartner für Datenschutzfragen.

4.4 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Kenntnis von einem Bewerber unter 14 Jahren oder von Fehlern in der Verarbeitung erhält.

4.5 Der Auftraggeber hat das Recht, Weisungen zu erteilen und den Auftragnehmer nach Abschnitt 3.7 zu überprüfen.

5. Ort der Verarbeitung und Drittlandübermittlung

5.1 Grundsatz. Hosting und Speicherung der Datenbanken, Dateien und Backups erfolgen ausschließlich in Rechenzentren in der Europäischen Union bzw. im EWR. Der Standort ist: Deutschland. Ein Standort in einem Drittland (z. B. USA) ist ausgeschlossen.

5.2 Drittlandbezug einzelner Sub-Auftragsverarbeiter. Übermittlungen in Drittländer erfolgen nur, soweit sie sich aus dem Einsatz der in Abschnitt 6 genannten Dienste ergeben, und nur auf Grundlage des Kapitels V DSGVO. Betroffen sind:

- **Google (Anmeldung, Standortsuche):** Es können Daten (insbesondere IP-Adresse, Kennungen und Suchbegriffe) an Google-Gesellschaften in den USA übermittelt werden. Grundlage ist der Angemessenheitsbeschluss zum EU-US Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795), soweit der Empfänger zertifiziert ist, sowie hilfsweise die Standardvertragsklauseln im Vertrag mit Google. Über diese Dienste werden keine Bewerbungsunterlagen, Lebensläufe oder Chat-Inhalte übermittelt.

- **Zoho (E-Mail-Dienste):** Verarbeitung in EU-Rechenzentren. Ein Zugriff aus Drittländern (z. B. für Support) ist durch Standardvertragsklauseln im Vertrag mit dem Anbieter abgesichert.

5.3 Änderungen. Fällt eine Übermittlungsgrundlage weg oder wird sie für unwirksam erklärt, informiert der Auftragnehmer den Auftraggeber unverzüglich und schaltet den betroffenen Dienst ab oder ersetzt ihn, sofern keine andere Grundlage nach Kapitel V besteht. Weitere Drittlandübermittlungen erfolgen nur nach Abschnitt 6.2 und 6.3 sowie auf Weisung des Auftraggebers.

6. Sub-Auftragsverarbeiter

6.1 Allgemeine Genehmigung. Der Auftraggeber genehmigt den Einsatz der folgenden Sub-Auftragsverarbeiter:

Unternehmen	Standort / Verarbeitung	Leistung	Vertrag / Übermittlungsgrundlage
Netcup GmbH	Deutschland; Rechenzentrum: Nürnberg	VPS-Hosting, Serverinfrastruktur, Datenbank- und Dateispeicherung, Backups	Auftragsverarbeitungsvertrag nach Art. 28 Abs. 4 DSGVO; keine Drittlandübermittlung
Zoho Corporation B.V.	EU-Rechenzentrum; möglicher Support-Zugriff aus Drittländern	ZeptoMail (transaktionale E-Mails, Verifikation) und Zoho Mail (Support-, Office- und Sales-Kommunikation)	Auftragsverarbeitungsvertrag nach Art. 28 Abs. 4 DSGVO; Standardvertragsklauseln (Art. 46 Abs. 2 lit. c)
Google Cloud EMEA Limited	EU/EWR; Übermittlung in die USA möglich	Google-Anmeldung (OAuth) und Google Maps API (Standortsuche)	Auftragsverarbeitungsvertrag nach Art. 28 Abs. 4 DSGVO; EU-US Data Privacy Framework, hilfsweise Standardvertragsklauseln

6.2 Änderungen. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Hinzuziehung oder Ersetzung eines Sub-Auftragsverarbeiters in Textform (E-Mail an die Owner-Adresse und Hinweis in der Plattform) mindestens **30 Tage** vor dem Einsatz. Die Information enthält Name, Sitz, Leistung, Verarbeitungsort und Übermittlungsgrundlage.

6.3 Widerspruch. Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Die Parteien suchen eine gemeinsame Lösung. Kommt sie nicht zustande, kann der Auftraggeber den Hauptvertrag mit Wirkung zum Einsatzbeginn außerordentlich kündigen; bereits bezahlte Entgelte für den Zeitraum nach Vertragsende werden anteilig erstattet. Ohne fristgerechten Widerspruch gilt der Sub-Auftragsverarbeiter als genehmigt.

6.4 Pflichtenübertragung und Haftung. Der Auftragnehmer verpflichtet jeden Sub-Auftragsverarbeiter vertraglich zu denselben Datenschutzpflichten wie in dieser Vereinbarung, insbesondere zu hinreichenden Garantien für geeignete technische und organisatorische Maßnahmen. Kommt ein Sub-Auftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für dessen Verstöße (Art. 28 Abs. 4 DSGVO). Auf Anfrage legt der Auftragnehmer die datenschutzrelevanten Vertragsteile offen.

7. Rückgabe und Löschung nach Vertragsende

7.1 Wahlrecht. Der Auftraggeber entscheidet, ob die im Auftrag verarbeiteten Daten nach Beendigung des Hauptvertrags zurückgegeben, gelöscht oder beides (erst Rückgabe, dann Löschung) werden sollen. Er erklärt seine Wahl über die Plattform oder in Textform an den Auftragnehmer,

jederzeit während der Laufzeit und während der Ruhefrist. Trifft er keine Wahl, werden die Daten nach der Ruhefrist gelöscht.

7.2 Ruhefrist (Soft-Delete). Nach Beendigung des Hauptvertrags wird der Zugang des Auftraggebers für 30 Tage gesperrt. In dieser Zeit beschränkt sich die Verarbeitung auf Speicherung sowie Export und Rückgabe an den Auftraggeber. Diese Vereinbarung gilt in dieser Zeit fort.

7.3 Rückgabe. Die Rückgabe erfolgt einmal kostenfrei in einem strukturierten, gängigen und maschinenlesbaren Format (JSON), Dokumente und Anhänge als Dateien, Chat-Verläufe zusätzlich als PDF-Export. PDF-Export der Chatverläufe, Dokumente als Dateien. Der Auftraggeber sichert erforderliche Unterlagen für seine gesetzlichen Aufbewahrungspflichten selbst.

7.4 Löschung. Nach Ablauf der Ruhefrist (oder auf Verlangen des Auftraggebers früher) löscht der Auftragnehmer alle im Auftrag verarbeiteten Daten einschließlich vorhandener Kopien endgültig und unwiderruflich, spätestens binnen 14 Tagen. Backups werden nach Ablauf ihres Rotationszyklus, spätestens 30 Tage nach der Löschung, überschrieben; bis dahin werden sie nicht für andere Zwecke verwendet, und bei einer Wiederherstellung wird die Löschung erneut durchgeführt. Der Auftragnehmer veranlasst zudem die Löschung bei Sub-Auftragsverarbeitern.

7.5 Bestätigung. Der Auftragnehmer bestätigt dem Auftraggeber die Löschung auf Verlangen in Textform.

7.6 Aufbewahrungspflichten. Bestehen Pflichten zur Speicherung nach Unionsrecht oder dem Recht eines Mitgliedstaats, wird die Verarbeitung auf die Speicherung beschränkt und nach Ablauf der Frist gelöscht. Der Auftragnehmer informiert den Auftraggeber darüber.

7.7 Abgrenzung. Gelöscht bzw. zurückgegeben werden die Daten aus dem Bereich des Auftraggebers (Bewerbungen, Notizen, Bewertungen, Leads, Chat-Verläufe, Inserate, Nutzerkonten des Auftraggebers). Bewerberkonten und -profile, für die der Auftragnehmer selbst verantwortlich ist (Abschnitt 1.2), bleiben davon unberührt.

8. Beendigung

8.1 Die Vereinbarung endet nach Abschnitt 1.3. Pflichten zur Vertraulichkeit sowie Haftungs- und Nachweispflichten bestehen fort.

8.2 Bei einem schwerwiegenden Verstoß gegen diese Vereinbarung kann der Auftraggeber sie und den Hauptvertrag aus wichtigem Grund fristlos kündigen.

9. Allgemeine Bestimmungen

9.1 Abschluss. Die Vereinbarung wird elektronisch im Onboarding durch Bestätigung einer vertretungsbefugten Person des Auftraggebers geschlossen (Art. 28 Abs. 9 DSGVO). Der Auftragnehmer protokolliert Zeitpunkt, Version, annehmende Person und Firma und stellt dem Auftraggeber jederzeit eine PDF-Kopie zur Verfügung.

9.2 Vorrang. Bei Widersprüchen zu Datenschutzfragen geht diese Vereinbarung dem Hauptvertrag und den AGB vor.

9.3 Änderungen. Änderungen bedürfen der Textform. Der Auftragnehmer darf die Vereinbarung aus Gründen einer geänderten Rechtslage anpassen; er informiert den Auftraggeber mindestens 30 Tage vorher. Der Auftraggeber kann innerhalb dieser Frist widersprechen; dann gilt Abschnitt 6.3 sinngemäß.

9.4 Haftung. Die Haftung richtet sich nach Art. 82 DSGVO und dem Hauptvertrag.

9.5 Salvatorische Klausel. Ist eine Bestimmung unwirksam, bleibt die Wirksamkeit der übrigen unberührt; an ihre Stelle tritt eine wirksame, die dem Zweck möglichst nahekommt.

9.6 Recht und Gerichtsstand. Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen. Gerichtsstand ist das Bezirksgericht Vöcklabruck.

Annahme durch den Auftraggeber: Firma, Name und Funktion der vertretungsbefugten Person, Datum und Uhrzeit (elektronisch im Onboarding).

Für den Auftragnehmer: Siegmar Kroismayr, Geschäftsführer, 30.09.2026

Anlage ./1 – Technisch-organisatorische Maßnahmen (TOMs)

Der Auftragnehmer setzt gemäß Art. 32 DSGVO folgende Maßnahmen um. Sie berücksichtigen, dass Schülerinnen, Schüler und teils Minderjährige betroffen sind.

A. Vertraulichkeit

- **Zutrittskontrolle:** Produktivdaten liegen ausschließlich in den Rechenzentren des Hosters (physischer Zutrittsschutz und Zertifizierungen des Hosters); keine Speicherung von Produktivdaten auf lokalen Endgeräten.
- **Zugangskontrolle:** Passwort-Hashing nach Bcrypt, Passwort-Mindestanforderungen, Zwei-Faktor-Authentifizierung (für alle Konten optional aktivierbar), geschützte Sessions (HTTPOnly, SameSite=Lax, Secure). Serverzugang nur mit SSH-Schlüsseln, Firewall und Fail2Ban.
- **Zugriffskontrolle:** Rollenbasierte Rechte (Owner, Manager, Contributor) nach dem Minimalprinzip, Session-Timeout nach 30 Minuten Inaktivität (außer bei aktivierter Option ‚Angemeldet bleiben'), serverseitige Autorisierungsprüfung bei jedem API-Aufruf, Administratorzugriff nur für wenige namentlich benannte Personen.
- **Mandantentrennung:** Daten eines Unternehmens sind ausschließlich für dessen Nutzer abrufbar; die Firmenzuordnung wird serverseitig bei jedem Zugriff geprüft.
- **Pseudonymisierung und Datenminimierung:** Bewerberdaten werden dem Unternehmen erst mit Bewerbung oder Freigabe sichtbar; Logs und Statistiken arbeiten mit Kennungen statt Klarnamen; Formulare erheben nur erforderliche Felder.
- **Verschlüsselung ruhender Daten:** Datenbank, Dateispeicher und Backups sind verschlüsselt mit Passwort und 2-Faktor Authentifizierung.

B. Integrität und Weitergabekontrolle

- **Transportverschlüsselung:** Durchgängig HTTPS/TLS für alle Datenübertragungen (mindestens TLS 1.2, HSTS); Transportverschlüsselung beim E-Mail-Versand, soweit vom Empfänger unterstützt.
- **Geschützte Dateispeicherung:** Bewerbungsunterlagen liegen im Verzeichnis uploads_secure/ außerhalb des öffentlichen Web-Roots und werden nur nach Autorisierungsprüfung ausgeliefert.
- **Upload-Schutz:** Zufallsgenerierte Dateinamen, serverseitige Prüfung von MIME-Typ und Dateiendung, Deaktivierung der Skriptausführung in Upload-Verzeichnissen.
- **Angriffsschutz:** CSRF-Tokens für alle zustandsändernden Formulare, Eingabevalidierung und Schutz vor SQL-Injection und Cross-Site-Scripting.

C. Verfügbarkeit und Belastbarkeit

- **Datensicherung:** Tägliche automatische Datenbanksicherung, verschlüsselt und auf einem vom Produktivsystem getrennten Speicher, Aufbewahrung 30 Tage, Wiederherstellungstest mindestens halbjährlich, Ziel für Wiederherstellung 24 Stunden.
- **Serverhärtung und Patch-Management:** Firewall, Fail2Ban, minimale Dienste, zeitnahes Einspielen von Sicherheitsupdates (kritische Updates innerhalb von 7 Tagen).
- **Ratenbegrenzung und Überwachung:** Mehrstufiges Rate-Limiting gegen Brute-Force und DoS; Systemüberwachung mit Alarmierung.
- **Bot-Abwehr:** Honeypot-Mechanismen gegen automatisierte Scraper und Spam.

D. Überprüfung, Bewertung und Evaluierung

- **Protokollierung:** Audit-Log administrativer Aktionen sowie Protokollierung von Zugriffen auf Bewerbungsdokumente (Ansicht, Download); Logs sind gegen nachträgliche Änderung geschützt.

- **Sicherheitsüberprüfung:** Code-Review vor Veröffentlichung, Prüfung der Abhängigkeiten auf bekannte Schwachstellen mindestens vierteljährlich, Überprüfung der Sicherheitsfilter und API-Endpunkte mindestens jährlich.
- **Löschkonzept:** Definierte Löschfristen und Löschroutinen einschließlich Backups gemäß Abschnitt 7.

E. Organisation

- **Vorfallmanagement:** Prozess zur Erkennung, Bewertung, Dokumentation und Meldung von Datenschutzverletzungen an den Auftraggeber innerhalb von 24 Stunden.
- **Verpflichtung und Schulung:** Alle Teammitglieder mit Datenzugriff werden auf Vertraulichkeit verpflichtet und in den Datenschutz eingewiesen.
- **Auftragskontrolle:** Auswahl und Vertragsprüfung von Sub-Auftragsverarbeitern, Prüfung ihrer Zertifikate und Sicherheitsangaben.
- **Datenschutz durch Technikgestaltung (Art. 25):** Mindestalter 14 bei Registrierung, datensparsame Voreinstellungen, eingeschränkte Sichtbarkeit von Bewerberprofilen, Hinweis beim Upload zu sensiblen Angaben.