

Vertragsparteien

zwischen

dem Betrieb, der Verbrieft nutzt und dessen Firma, Anschrift und gegebenenfalls UID im Kundenkonto von Verbrieft hinterlegt sind (im Folgenden „Verantwortlicher“),

und

The-Y e.U., Inhaber Thomas Nuri Yilmaz, Senefeldergasse 25, 1100 Wien, Österreich, UID ATU81770102, E-Mail verbrieft@the-y.at (im Folgenden „Auftragsverarbeiter“),

gemeinsam „die Parteien“.

Präambel

Der Verantwortliche nutzt die Online-Anwendung Verbrieft auf Grundlage der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters (im Folgenden „Nutzungsvertrag“). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag regelt die Rechte und Pflichten der Parteien nach Art. 28 der Verordnung (EU) 2016/679 (DSGVO). Er folgt im Aufbau den Standardvertragsklauseln der Europäischen Kommission nach dem Durchführungsbeschluss (EU) 2021/915, ist aber ein eigenständiger Vertrag.

1. Gegenstand und Dauer

1.1 Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung von Verbrieft: Schulung, Lernkontrolle, Zertifikate, Schulungsregister, KI-Inventar, Vorlagen, Export und Erinnerungen. Die Einzelheiten der Verarbeitung sind in Anlage 1 beschrieben.

1.2 Die Laufzeit dieses Vertrags entspricht der Laufzeit des Nutzungsvertrags. Er beginnt mit dessen Abschluss und endet mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten nach Abschnitt 13 gelten über das Vertragsende hinaus.

2. Art und Zweck der Verarbeitung

2.1 Der Auftragsverarbeiter erhebt (durch Eingabe des Verantwortlichen und der Teilnehmenden), speichert, ordnet, wertet aus, übermittelt an den Verantwortlichen und die von ihm eingeladenen Personen und löscht personenbezogene Daten, soweit dies für die Funktionen von Verbrieft erforderlich ist.

2.2 Zweck der Verarbeitung ist ausschließlich die Erfüllung und Dokumentation der Pflichten des Verantwortlichen nach Art. 4 der Verordnung (EU) 2024/1689 (KI-Verordnung): Durchführung von Schulungen, Ausstellung von Zertifikaten, Führung eines Schulungsregisters und eines KI-Inventars sowie die Erstellung exportierbarer Nachweise.

2.3 Eine Verarbeitung für eigene Zwecke des Auftragsverarbeiters, etwa für Werbung oder Profilbildung, findet nicht statt. Vertrags- und Rechnungsdaten des Verantwortlichen, die der Auftragsverarbeiter für die Abwicklung des Nutzungsvertrags als eigenständig Verantwortlicher verarbeitet, sind nicht Gegenstand dieses Vertrags; hierfür gilt die Datenschutzerklärung von Verbrieft.

3. Kategorien betroffener Personen

Von der Verarbeitung betroffen sind:

- a) Mitarbeitende des Verantwortlichen sowie sonstige Personen, die der Verantwortliche zur Schulung einlädt (etwa freie Mitarbeitende, Lehrlinge oder Aushilfen);
- b) Ansprechpersonen des Verantwortlichen, die das Kundenkonto verwalten.

4. Kategorien personenbezogener Daten

4.1 Verarbeitet werden folgende Datenkategorien:

- a) zu Teilnehmenden: Name, Rolle oder Funktion im Betrieb, optional E-Mail-Adresse, Schulungsdatum, Ergebnis der Lernkontrolle, Zertifikatsnummer, Gültigkeit des Zertifikats;
- b) zum Betrieb: Firma, Anschrift, UID, Personenzahl, Angaben zu eingesetzten KI-Systemen sowie Inhalte der KI-Richtlinie und des Schulungskonzepts, soweit sie personenbezogen sind;
- c) zu Ansprechpersonen: Name und Login-E-Mail-Adresse.

4.2 Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand dieses Vertrags. Der Verantwortliche stellt sicher, dass solche Daten nicht in Freitextfelder eingegeben werden.

5. Weisungsrecht

5.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dies gilt auch für die Übermittlung an ein Drittland oder eine internationale Organisation, sofern der Auftragsverarbeiter nicht durch Unionsrecht oder das Recht eines Mitgliedstaats dazu verpflichtet ist; in diesem Fall teilt er dem Verantwortlichen diese Anforderung vor der Verarbeitung mit, soweit das Recht dies nicht verbietet.

5.2 Dieser Vertrag, der Nutzungsvertrag und die Einstellungen, die der Verantwortliche im Kundenkonto vornimmt (etwa Einladung von Personen, Erinnerungsintervalle, Exporte, Löschungen), gelten als dokumentierte Weisungen. Darüber hinausgehende Weisungen erteilt der Verantwortliche in Textform an verbrieft@the-y.at. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

5.3 Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung der Weisung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

5.4 Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, kann der Auftragsverarbeiter ablehnen oder gesondert nach angemessenem Aufwand vergüten lassen.

6. Vertraulichkeit

6.1 Der Auftragsverarbeiter gewährt nur solchen Personen Zugang zu den personenbezogenen Daten, die diesen für die Erbringung der Leistung unbedingt benötigen. Derzeit hat ausschließlich der Inhaber des Auftragsverarbeiters Zugriff auf die Produktivsysteme.

6.2 Werden weitere Personen mit der Verarbeitung betraut, verpflichtet der Auftragsverarbeiter sie vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht über das Ende der Tätigkeit hinaus fort.

7. Sicherheit der Verarbeitung

7.1 Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau nach Art. 32 DSGVO zu gewährleisten.

7.2 Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie weiterentwickeln, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen auf Anfrage mit.

7.3 Der Verantwortliche bleibt dafür verantwortlich, zu beurteilen, ob die Maßnahmen für die von ihm eingegebenen Daten angemessen sind.

8. Unterauftragsverarbeiter

8.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, die in Anlage 3 genannten Unterauftragsverarbeiter einzusetzen.

8.2 Beabsichtigt der Auftragsverarbeiter, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, informiert er den Verantwortlichen mindestens 30 Tage vorher per E-Mail und nennt Name, Anschrift, Leistung und Verarbeitungsort. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Finden die Parteien nach einem Widerspruch keine einvernehmliche Lösung, kann der Verantwortliche den Nutzungsvertrag zum Zeitpunkt der geplanten Änderung kündigen; im Voraus gezahltes Entgelt wird anteilig erstattet.

8.3 Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der diesem im Wesentlichen dieselben Datenschutzpflichten auferlegt wie dieser Vertrag dem Auftragsverarbeiter. Auf Anfrage stellt er dem Verantwortlichen eine Kopie dieses Vertrags zur Verfügung; Geschäftsgeheimnisse und Preise dürfen geschwärzt werden.

8.4 Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Pflichten durch den Unterauftragsverarbeiter.

9. Übermittlung in Drittländer

Sämtliche Verarbeitungen im Auftrag des Verantwortlichen finden in der Europäischen Union statt (Anlage 1 und Anlage 3). Eine Übermittlung personenbezogener Daten in ein Drittland erfolgt nur auf dokumentierte Weisung des Verantwortlichen und nur unter den Voraussetzungen des Kapitels V DSGVO.

10. Unterstützungspflichten

10.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Art. 12 bis 22 DSGVO zu beantworten. Dazu kann der Verantwortliche Daten von Teilnehmenden im Kundenkonto selbst einsehen, berichtigen, exportieren und löschen. Anträge, die unmittelbar beim Auftragsverarbeiter eingehen, leitet dieser unverzüglich an den Verantwortlichen weiter und beantwortet sie nur auf dessen Weisung.

10.2 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation der Aufsichtsbehörde) und stellt dazu die ihm vorliegenden Informationen bereit.

10.3 Unterstützungsleistungen, die über die Bereitstellung vorhandener Informationen und die Funktionen des Kundenkontos hinausgehen, vergütet der Verantwortliche nach angemessenem Aufwand, sofern die Notwendigkeit nicht vom Auftragsverarbeiter zu vertreten ist.

11. Meldung von Verletzungen des Schutzes personenbezogener Daten

11.1 Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich, spätestens binnen 48 Stunden nach Kenntnis, per E-Mail an die Login-E-Mail-Adresse der Ansprechperson.

11.2 Die Meldung enthält, soweit bekannt: die Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Abhilfemaßnahmen und eine Kontaktstelle. Liegen nicht alle Informationen vor, werden sie ohne unangemessene Verzögerung nachgereicht.

11.3 Der Auftragsverarbeiter dokumentiert die Verletzung, ihre Auswirkungen und die Abhilfemaßnahmen und unterstützt den Verantwortlichen bei der Erfüllung seiner Pflichten nach Art. 33 und 34 DSGVO. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen obliegen dem Verantwortlichen.

12. Nachweis und Kontrollen

12.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO und dieses Vertrags erforderlich sind. Dazu gehören insbesondere eine aktuelle Beschreibung der Maßnahmen nach Anlage 2, die Liste der Unterauftragsverarbeiter und die ihm vorliegenden Nachweise der Unterauftragsverarbeiter (etwa Zertifikate oder Prüfberichte des Rechenzentrumsbetreibers).

12.2 Der Auftragsverarbeiter verfügt derzeit über keine Zertifizierung nach Art. 42 DSGVO und keine Zertifizierung nach ISO/IEC 27001. Er weist die getroffenen Maßnahmen auf Anfrage durch Beschreibung und Einsicht nach.

12.3 Der Verantwortliche oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer darf die Einhaltung dieses Vertrags überprüfen, auch vor Ort in den Geschäftsräumen des Auftragsverarbeiters. Kontrollen werden mit angemessener Frist, in der Regel mindestens 14 Tage, angekündigt, finden zu den üblichen Geschäftszeiten statt und dürfen den Betrieb nicht unverhältnismäßig beeinträchtigen; ohne konkreten Anlass sind sie einmal je Kalenderjahr möglich. Kontrollen im Rechenzentrum richten sich nach den Bedingungen des Unterauftragsverarbeiters.

12.4 Der Auftragsverarbeiter wirkt an Prüfungen durch die zuständige Aufsichtsbehörde mit und informiert den Verantwortlichen unverzüglich über Anfragen der Aufsichtsbehörde, die dessen Daten betreffen, soweit ihm dies rechtlich gestattet ist.

13. Löschung und Rückgabe nach Vertragsende

13.1 Der Verantwortliche kann während der Laufzeit jederzeit alle Daten seines Betriebs im Kundenkonto exportieren (Nachweis-Ordner als PDF). Es obliegt dem Verantwortlichen, vor der Beendigung des Nutzungsvertrags einen Export durchzuführen.

13.2 Der Auftragsverarbeiter löscht alle personenbezogenen Daten des Verantwortlichen 90 Tage nach Beendigung des Nutzungsvertrags. Innerhalb dieser Frist bleibt der Export im Kundenkonto möglich. Sicherungskopien werden mit Ablauf der Aufbewahrungsfrist von 14 Tagen nach der Löschung überschrieben.

13.3 Auf ausdrückliche Weisung des Verantwortlichen erfolgt die Löschung früher. Der Auftragsverarbeiter bestätigt die Löschung auf Anfrage in Textform.

13.4 Daten, die der Auftragsverarbeiter aufgrund gesetzlicher Aufbewahrungspflichten in eigener Verantwortung speichern muss (etwa Rechnungsdaten), bleiben von der Löschung unberührt und werden nach Ablauf der gesetzlichen Fristen gelöscht.

14. Haftung

14.1 Die Haftung der Parteien gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO. Der Auftragsverarbeiter haftet danach nur, wenn er den speziell den Auftragsverarbeitern auferlegten Pflichten der DSGVO nicht nachgekommen ist oder entgegen den rechtmäßigen Weisungen des Verantwortlichen gehandelt hat.

14.2 Wird eine Partei für den gesamten Schaden in Anspruch genommen, kann sie von der anderen Partei den Teil des Schadenersatzes zurückfordern, der dem Anteil der anderen Partei an der Verantwortung für den Schaden entspricht (Art. 82 Abs. 5 DSGVO).

14.3 Im Innenverhältnis zwischen den Parteien gelten ergänzend die Haftungsregelungen des Nutzungsvertrags, soweit sie mit Art. 82 DSGVO vereinbar sind. Eine Haftungsbeschränkung gilt nicht für Ansprüche betroffener Personen.

15. Laufzeit und Beendigung

15.1 Die Laufzeit richtet sich nach Abschnitt 1.2.

15.2 Der Verantwortliche kann den Nutzungsvertrag und diesen Vertrag aus wichtigem Grund fristlos kündigen, wenn der Auftragsverarbeiter seine Pflichten aus diesem Vertrag schwerwiegend oder wiederholt verletzt und den Verstoß nicht innerhalb einer angemessenen, vom Verantwortlichen gesetzten Frist beendet, oder wenn er eine Weisung nicht befolgt, ohne sie nach Abschnitt 5.3 beanstandet zu haben.

15.3 Nach Beendigung gilt Abschnitt 13.

16. Schlussbestimmungen

16.1 Bei Widersprüchen geht dieser Vertrag dem Nutzungsvertrag vor, soweit es um die Verarbeitung personenbezogener Daten im Auftrag geht. Im Übrigen gilt der Nutzungsvertrag.

16.2 Änderungen dieses Vertrags bedürfen der Textform. Der Auftragsverarbeiter kann Anlage 2 nach Abschnitt 7.2 und Anlage 3 nach Abschnitt 8.2 aktualisieren; die jeweils aktuelle Fassung ist unter verbrieft.at/avv abrufbar; Änderungen werden im Kundenkonto angezeigt.

16.3 Es gilt österreichisches Recht unter Ausschluss des UN-Kaufrechts und der Kollisionsnormen. Zwingende Vorschriften der DSGVO bleiben unberührt. Für Streitigkeiten mit Unternehmern ist das sachlich zuständige Gericht in Wien ausschließlich zuständig.

16.4 Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

17. Abschluss

17.1 Der Vertrag wird geschlossen, indem der Verantwortliche seinen Betrieb in Verbrieft einrichtet; beim Anlegen wird auf diesen Vertrag hingewiesen und die Einrichtung gilt als Annahme. Der Auftragsverarbeiter protokolliert Zeitpunkt, Kundenkonto und Fassung des Vertrags. Alternativ oder zusätzlich kann der Vertrag in Papierform unterschrieben werden; ein von beiden Parteien unterzeichnetes Exemplar geht dem elektronischen Abschluss vor, soweit es abweicht.

17.2 Wahlweise kann der Vertrag in schriftlicher Form geschlossen werden. Dazu füllt der Verantwortliche die nachstehenden Felder aus, unterschreibt und sendet den Vertrag per E-Mail an verbrieft@the-y.at. Der Auftragsverarbeiter sendet ein gegengezeichnetes Exemplar zurück.

Für den Verantwortlichen

Firma: _____

Ort, Datum: _____

Name, Funktion: _____

Unterschrift: _____

Für den Auftragsverarbeiter

The-Y e.U.

Ort, Datum: Wien, _____

Name: Thomas Nuri Yilmaz, Inhaber

Unterschrift: _____

Anlage 1: Gegenstand der Verarbeitung

Punkt	Beschreibung
Gegenstand	Bereitstellung der Online-Anwendung Verbrieft zur Schulung und Dokumentation von KI-Kompetenz nach Art. 4 KI-Verordnung
Zweck	Durchführung und Nachweis von Schulungen, Ausstellung von Zertifikaten, Führung von Schulungsregister und KI-Inventar, Erstellung von KI-Richtlinie und Schulungskonzept, Export als Nachweis-Ordner, Erinnerungen
Art der Verarbeitung	Erheben (Eingabe durch den Verantwortlichen und die Teilnehmenden), Speichern, Ordnen, Auswerten (Lernkontrolle), Übermitteln an den Verantwortlichen und die Teilnehmenden (Zertifikate, Erinnerungen), Exportieren, Löschen
Kategorien betroffener Personen	Mitarbeitende und sonstige vom Verantwortlichen zur Schulung eingeladene Personen; Ansprechpersonen des Verantwortlichen
Kategorien personenbezogener Daten	Name, Rolle oder Funktion, optional E-Mail-Adresse, Schulungsdatum, Ergebnis der Lernkontrolle, Zertifikatsnummer, Gültigkeit; Betriebsdaten (Firma, Anschrift, UID, Personenzahl, eingesetzte KI-Systeme); Login-E-Mail-Adresse der Ansprechpersonen
Besondere Kategorien	Keine; die Eingabe von Daten nach Art. 9 DSGVO ist nicht vorgesehen
Häufigkeit	Laufend während der Vertragslaufzeit, ausgelöst durch Eingaben des Verantwortlichen und der Teilnehmenden sowie durch zeitgesteuerte Erinnerungen
Dauer	Laufzeit des Nutzungsvertrags zuzüglich 90 Tage (Abschnitt 13)
Ort der Verarbeitung	Rechenzentrum Wien, Österreich (netcup GmbH); Sicherungen auf einem eigenen System des Auftragsverarbeiters in Wien

Anlage 2: Technische und organisatorische Maßnahmen

Stand: 8. September 2026. Die Maßnahmen beschreiben den tatsächlichen Betrieb von Verbrieft (zur Zertifizierung siehe Abschnitt 12.2).

1. Standort und Hosting. Verbrieft läuft auf einem Server der netcup GmbH im Rechenzentrum Wien, Österreich; andere Rechenzentren werden nicht genutzt. Die physische Zutrittskontrolle obliegt der netcup GmbH nach dem mit ihr geschlossenen Auftragsverarbeitungsvertrag.

2. Verschlüsselung. Die Übertragung zwischen Browser und Server sowie zwischen Server und Mailserver erfolgt TLS-verschlüsselt. Sicherungskopien werden vor der Ablage verschlüsselt.

3. Zugangskontrolle. Die Anmeldung von Verantwortlichen und Teilnehmenden erfolgt über einen einmalig gültigen, zeitlich befristeten Link, der an die hinterlegte E-Mail-Adresse gesendet wird. Passwörter werden nicht gespeichert. Nach der Anmeldung wird ein Sitzungs-Cookie gesetzt, das nur für den Kundenbereich gilt.

4. Zugriffskontrolle. Administrativen Zugriff auf Server und Datenbank hat ausschließlich der Inhaber des Auftragsverarbeiters. Der Zugriff erfolgt über kryptografische Schlüssel, nicht über Passwörter. Es gibt keine weiteren Nutzerkonten mit Zugriff auf Produktivdaten.

5. Trennungskontrolle. Die Daten der Verantwortlichen werden in der Datenbank nach Betrieb (Mandant) getrennt. Jede Abfrage ist auf den angemeldeten Betrieb beschränkt. Test- und Produktivumgebung sind getrennte Systeme; das Testsystem enthält keine Produktivdaten.

6. Verfügbarkeit und Wiederherstellung. Täglich wird eine verschlüsselte Sicherung der Datenbank auf einem eigenen System des Auftragsverarbeiters in Wien abgelegt. Sicherungen werden 14 Tage aufbewahrt und danach überschrieben.

7. Protokollierung. Exporte aus dem Kundenkonto werden mit Zeitpunkt, Kundenkonto und Art des Exports protokolliert. Serverprotokolle mit IP-Adressen werden nach spätestens 14 Tagen gelöscht.

8. Datensparsamkeit. Verbrieft setzt keine Tracking-Dienste und keine Analyse- oder Werbedienste Dritter ein. Auf den öffentlichen Seiten wird kein Cookie gesetzt. Es werden nur die Daten erhoben, die für die Funktionen erforderlich sind; die E-Mail-Adresse von Teilnehmenden ist optional.

9. Wartung und Sicherheitsupdates. Betriebssystem und eingesetzte Softwarekomponenten werden regelmäßig mit Sicherheitsupdates versorgt.

10. Überprüfung. Der Auftragsverarbeiter überprüft die Maßnahmen bei wesentlichen Änderungen der Anwendung, mindestens jährlich, und passt diese Anlage bei Bedarf an.

Anlage 3: Unterauftragsverarbeiter

Unternehmen	Anschrift	Leistung	Ort der Verarbeitung	Grundlage
netcup GmbH	Emmy-Noether-Str. 10, 76131 Karlsruhe, Deutschland	Hosting des Servers, auf dem Verbrieft be- trieben wird	Rechenzentrum Wien, Österreich	Auftragsver- arbeitungsvertrag nach Art. 28 DSGVO abgeschlossen

Zur Transparenz genannt, aber keine Unterauftragsverarbeiter im Sinne dieses Vertrags:

- Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Dublin, Irland: Zahlungsabwicklung für den Nutzungsvertrag. Stripe erhält ausschließlich Zahlungsdaten des Verantwortlichen (Name, E-Mail, Rechnungsadresse, UID, Zahlungsmittel) und verarbeitet sie als eigenständig Verantwortlicher. Daten von Teilnehmenden werden nicht an Stripe übermittelt.
- E-Mail-Versand (Anmeldelinks, Zertifikate, Erinnerungen): über den eigenen Mailserver von The-Y e.U. Es ist kein Dritter beteiligt.