

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

nach Art. 28 DSGVO · ÜbCon One – Beobachtungsmodul · Version 1.0 · Stand 11.10.2026

Ausfüllen: Bitte nur die farbig hinterlegten Felder ausfüllen (Name, Anschrift, Ansprechperson), danach drucken und unterschreiben oder digital unterzeichnen. Der übrige Text ist unveränderlich.

Zwischen

Auftraggeber (Verantwortlicher)

Name der Organisation

Straße und Hausnummer

Postleitzahl und Ort

Vertreten durch (Name, Funktion)

– nachfolgend „Auftraggeber“ –

und

Jan Krebs, ÜbCon (Einzelunternehmen), Usinger Straße 20, 61273 Wehrheim, E-Mail: jan.krebs@uebcon.org – nachfolgend „Auftragnehmer“ –

Der Auftraggeber nutzt das Beobachtungsmodul von ÜbCon One (uebcon.org/ÜebConOne/Beobachtungsmodul), um Übungen zu beobachten, auszuwerten und darüber zu berichten. Dabei verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag regelt die Rechte und Pflichten beider Seiten nach Art. 28 der Datenschutz-Grundverordnung (DSGVO).

Ansprechperson des Auftraggebers für Weisungen und Datenpannen (§ 4 Abs. 5, § 6 Abs. 3)

Name

E-Mail

Telefon (erreichbar auch bei Störungen)

Datenschutzbeauftragte/r des Auftraggebers, falls benannt (Name, Kontakt)

§ 1 Gegenstand und Dauer

1. Gegenstand ist die Bereitstellung des Beobachtungsmoduls und die damit verbundene Verarbeitung personenbezogener Daten, die der Auftraggeber in seiner Umgebung des Moduls erfasst (Inhalte).
2. Der Vertrag gilt ab Unterzeichnung durch beide Seiten, spätestens mit der Freischaltung des Zugangs, und so lange der Auftragnehmer Daten des Auftraggebers verarbeitet. Er endet mit der Beendigung der Nutzung; die Pflichten aus § 8 bestehen darüber hinaus fort. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt, insbesondere bei einem schwerwiegenden Verstoß gegen diesen Vertrag.

§ 2 Art, Zweck, Daten und Betroffene

1. Art und Zweck der Verarbeitung: Speichern, Bereitstellen, Anzeigen und Auswerten der Inhalte zur Durchführung, Dokumentation und Auswertung von Übungen des Auftraggebers sowie zur Nachverfolgung abgeleiteter Maßnahmen (Lessons Learned) einschließlich Erstellung und Versand von Berichten per Link und Hinweis auf amtliche Warnungen.

2. Arten der Daten und Kategorien Betroffener ergeben sich aus Anlage 1.
3. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), insbesondere Gesundheitsdaten, und Daten Minderjähriger sind nicht Gegenstand dieses Vertrags und sollen nicht erfasst werden. Erfasst der Auftraggeber sie dennoch oder regelt er dies für seinen Einsatz ausdrücklich, ist er dafür allein verantwortlich (§ 7 Abs. 2).
4. Für Registrierung, Benutzerkonto, Anmeldung, Sicherheit des Betriebs und Support verarbeitet der Auftragnehmer Daten zu eigenen Zwecken und ist dafür nach seiner Datenschutzerklärung (uebcon.org/datenschutz) selbst Verantwortlicher. Dieser Vertrag betrifft die Inhalte nach Absatz 1.

§ 3 Weisungen

1. Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers, auch hinsichtlich der Übermittlung in ein Drittland, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dies dem Auftraggeber vor der Verarbeitung mit, sofern das Recht dies nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).
2. Dokumentierte Weisungen sind dieser Vertrag und die Bedienung des Moduls durch die Administration des Auftraggebers. Weitere Weisungen erteilt der Auftraggeber in Textform (E-Mail genügt) über seine Ansprechperson.
3. Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin. Er darf die Ausführung aussetzen, bis die Weisung bestätigt oder geändert ist.

§ 4 Pflichten des Auftragnehmers

1. Vertraulichkeit: Der Auftragnehmer gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).
2. Sicherheit: Er trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und entwickelt sie fort. Das vereinbarte Schutzniveau wird nicht unterschritten; wesentliche Änderungen teilt er auf Anfrage mit (Art. 28 Abs. 3 lit. c DSGVO).
3. Betroffenenrechte: Anfragen Betroffener, die erkennbar den Auftraggeber betreffen, leitet er unverzüglich an diesen weiter und beantwortet sie nicht selbst. Er unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte Betroffener (Art. 28 Abs. 3 lit. e DSGVO).
4. Unterstützung: Er unterstützt den Auftraggeber bei den Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenpannen, Datenschutz-Folgenabschätzung, Konsultation der Aufsichtsbehörde), indem er die ihm vorliegenden Informationen bereitstellt (Art. 28 Abs. 3 lit. f DSGVO). Eine Datenschutz-Folgenabschätzung für das Modul stellt er auf Anfrage zur Verfügung.
5. Datenpannen: Wird ihm eine Verletzung des Schutzes personenbezogener Daten der Inhalte bekannt, meldet er sie dem Auftraggeber unverzüglich über die oben genannte Ansprechperson und teilt die ihm bekannten Angaben mit (Art. 33 Abs. 2 DSGVO). Die Meldung an die Aufsichtsbehörde und die Benachrichtigung Betroffener obliegen dem Auftraggeber.
6. Verzeichnis: Er führt ein Verzeichnis aller im Auftrag durchgeführten Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO).
7. Zweckbindung: Er verwendet die Daten nicht für eigene Zwecke und gibt sie nicht an Dritte weiter, außer an Unterauftragsverarbeiter nach § 5 oder auf Weisung des Auftraggebers.

§ 5 Unterauftragsverarbeiter

1. Der Auftraggeber erteilt eine allgemeine Genehmigung zum Einsatz der in Anlage 3 genannten Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO).
2. Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage im Voraus in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Lässt sich der Widerspruch nicht ausräumen, kann der Auftraggeber die Nutzung des Moduls zum Zeitpunkt der Änderung beenden.

3. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten wie in diesem Vertrag (Art. 28 Abs. 4 DSGVO). Er haftet dem Auftraggeber nach den gesetzlichen Vorgaben für deren Pflichterfüllung.

§ 6 Verarbeitung in Drittländern

Unterauftragsverarbeiter nach Anlage 3 haben ihren Sitz in den USA oder können Daten in Drittländern verarbeiten. Die Übermittlung stützt sich nach den Angaben der Anbieter auf das EU-US Data Privacy Framework und/oder EU-Standardvertragsklauseln (Anlage 3). Der Auftragnehmer prüft den Stand dieser Garantien mindestens einmal jährlich und informiert den Auftraggeber über wesentliche Änderungen.

§ 7 Pflichten des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung (Rechtsgrundlage), für die Information der Betroffenen (Art. 13, 14 DSGVO), für die Wahrung ihrer Rechte und für die Rechtmäßigkeit seiner Weisungen verantwortlich. Er weist seine Nutzenden an, das Modul nur im Rahmen dieses Vertrags zu verwenden.
2. Er stellt sicher, dass keine besonderen Kategorien personenbezogener Daten und keine Daten Minderjähriger erfasst werden, sofern er dies nicht ausdrücklich geregelt und rechtlich geprüft hat. Er prüft für seinen Einsatz außerdem, ob die Personalvertretung zu beteiligen ist.
3. Er benennt die Ansprechperson für Weisungen und Datenpannen (siehe oben) und hält deren Angaben aktuell.
4. Er führt, soweit erforderlich, eine Datenschutz-Folgenabschätzung für seinen Einsatz durch.

§ 8 Löschung und Rückgabe

1. Nach Beendigung der Nutzung löscht der Auftragnehmer die Inhalte des Auftraggebers einschließlich der Videos spätestens 30 Tage nach der Beendigung, es sei denn, der Auftraggeber verlangt vorher Herausgabe oder Löschung. Auf Verlangen gibt er die Inhalte vor der Löschung in einem gängigen, maschinenlesbaren Format heraus (Art. 28 Abs. 3 lit. g DSGVO). Löscht der Auftraggeber seine Organisation im Modul, werden alle Daten der Organisation entfernt.
2. Sicherungs- und Zwischenspeicher bei Unterauftragsverarbeitern können kurzzeitig fortbestehen. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

§ 9 Nachweise und Kontrollen

1. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Pflichten erforderlich sind (Art. 28 Abs. 3 lit. h DSGVO), insbesondere die Beschreibung der Maßnahmen und das Verzeichnis nach § 4 Abs. 6.
2. Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer kann Überprüfungen nach mindestens 14 Tagen Ankündigung, während üblicher Geschäftszeiten und im erforderlichen Umfang durchführen. Der Auftragnehmer darf geeignete Nachweise Dritter (z. B. Zertifikate der Unterauftragsverarbeiter) zugrunde legen. Der Zugang zu Systemen der Unterauftragsverarbeiter richtet sich nach deren Bedingungen.

§ 10 Haftung

Für die Haftung gilt Art. 82 DSGVO. Im Übrigen richtet sich die Haftung nach den für die Nutzung des Moduls vereinbarten Bedingungen.

§ 11 Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags, auch dieser Klausel, bedürfen der Textform. Ausgenommen sind Änderungen der Anlagen nach § 5 und Aktualisierungen der Maßnahmen nach § 4 Abs. 2.
2. Bei Widersprüchen gehen die Regelungen dieses Vertrags denen anderer Vereinbarungen vor, soweit sie den Datenschutz betreffen.
3. Es gilt deutsches Recht. Sollten einzelne Bestimmungen unwirksam oder undurchführbar sein, bleibt der Vertrag im Übrigen wirksam.

Unterschriften

Auftraggeber

Ort, Datum

Unterschrift Auftraggeber (Name, Funktion)

Auftragnehmer

Ort, Datum

Unterschrift Auftragnehmer (Jan Krebs)

Anlage 1 – Verarbeitungen, Daten und Betroffene

Verarbeitung	Datenarten	Betroffene
Übungen, Szenarien, Beobachtungen, Berichte	Beobachtungstexte, Uhrzeiten, Bewertungen (positiv, neutral, verbesserungswürdig), Themenfelder, markierte Orte und Gebiete, Berichtstexte, Szenarien und Ziele	Übende, Beobachtende und Dritte, die in Beobachtungstexten genannt werden
Fotos und Videos	Fotos (im Browser verkleinert, Metadaten entfallen) und Videos (mit möglichen Metadaten wie Aufnahmeort und -zeit)	Erkennbar abgebildete Personen
Beobachter-ID und Freigabe von Übungen	zufällige Beobachter-ID, Zuordnung zum Konto (nur für die Administration des Auftraggebers sichtbar), Protokoll jeder Auflösung	Beobachtende
Lessons Learned mit Verantwortlichen	Name und E-Mail-Adresse der verantwortlichen Person, Aufgabe, Frist, Status, Zeitpunkte von Erinnerungen, Zugangscodes (nur als Hash)	Verantwortliche für Maßnahmen, auch ohne Konto
Berichtsversand per Link	E-Mail-Adresse des Empfängers, Berichtsinhalt; Link 30 Tage gültig und widerrufbar	Empfänger von Berichten, Übende
Warnung (Hinweis auf amtliche Warnungen)	Einstellungen der Nutzenden zur Warnung, Quittierungen (Kennung der Warnung, Zeitpunkt); amtliche Warnungen, Wetter, Pegel und Karten werden ohne Personenbezug abgerufen	Nutzende

Löschung: durch die Eigentümerin bzw. den Eigentümer der Umgebung oder die Administration des Auftraggebers; spätestens mit Löschung der Organisation (§ 8). Quittierungen der Warnung werden nach 180 Tagen gelöscht.

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

Bereich	Maßnahme
Zugangskontrolle	Anmeldung mit Passwort (PBKDF2-SHA256 mit individuellem Salz) und zusätzlichem sechsstelligem Code per E-Mail (nur als Hash gespeichert, 10 Minuten gültig); Sperre nach 8 Fehlversuchen für 15 Minuten; Begrenzung der Anfragen je IP-Adresse und Konto; Sitzung endet nach 12 Stunden bzw. 30 Minuten Inaktivität; Sitzungs-Cookie mit HttpOnly, Secure und SameSite; Passwort-Links nur einmal verwendbar und befristet.
Zugriffskontrolle	Rollen (Administration, Beobachter:in); jede Person sieht nur Daten ihrer eigenen Übungen (Eigentümerprinzip), auch die Administration hat darüber keinen Zugriff; Freigabe erzeugt eine eigene Kopie; Organisationen anlegen, sperren und löschen darf nur die Administration des Auftragnehmers.
Trennung	Jede Abfrage ist an die Organisation gebunden; automatisierte Tests prüfen bei Änderungen, dass fremde Übungen und Organisationen nicht erreichbar sind.
Pseudonymisierung und Datenminimierung	Zufällige Beobachter-ID statt Name in Beiträgen und Berichten der Administration; Fotos werden im Browser neu gerendert (Metadaten entfallen); Abrufe von Wetter, Pegeln, Warnungen und Karten erfolgen durch den Server ohne Personenbezug; IP-Adressen werden nur als Hash mit geheimem Schlüssel gespeichert.
Weitergabekontrolle	Übertragung ausschließlich per HTTPS (HSTS); Sicherheits-Header; Prüfung des Ursprungs bei jedem schreibenden Aufruf; Berichts- und Aufgabenlinks mit Zufallswert (nur als Hash gespeichert), befristet und widerrufbar, Aufgabenlinks zusätzlich mit E-Mail-Code.
Eingabekontrolle	Protokoll wichtiger Vorgänge (Freigaben, Rollenänderungen, Auflösung einer Beobachter-ID, Einsicht) mit Zeitpunkt, handelnder Person und IP-Hash; Aufbewahrung 24 Monate.
Auftragskontrolle	Verarbeitung nur auf Weisung des Auftraggebers; Unterauftragsverarbeiter vertraglich gebunden (§ 5); Zugriff auf Produktivdaten ausschließlich durch den Auftragnehmer.
Verfügbarkeit und Belastbarkeit	Betrieb bei einem großen Cloud-Anbieter (Rechenzentrum und physischer Schutz liegen beim Anbieter); Beobachtungen können ohne Netz im Browser erfasst und später gesendet werden.
Löschung und Speicherbegrenzung	Automatische tägliche Löschung abgelaufener Daten (z. B. Support-Meldungen nach 12 Monaten, Protokoll nach 24 Monaten, Quittierungen nach 180 Tagen, Sitzungen, Codes und Zähler); Löschung einer Organisation entfernt alle ihre Daten einschließlich Videos.
Organisation	Verfahren für Datenpannen und für Anfragen Betroffener sind festgelegt; Datenschutz-Unterlagen (Verzeichnis, Folgenabschätzung) werden bei Änderungen des Moduls und mindestens jährlich überprüft.

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Garantie / Grundlage
Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Hosting (Workers, Datenbank D1 mit Standorthinweis Westeuropa, Objektspeicher R2 für Videos) und Auslieferung; Verarbeitung auch in anderen Ländern möglich	EU-US Data Privacy Framework, EU-Standardvertragsklauseln; Auftragsverarbeitung nach den Bedingungen des Anbieters
Plus Five Five, Inc. (Resend), USA	Versand von E-Mails (Zugangs-codes, Einladungen, Aufgaben, Erinnerungen, Berichtslinks)	EU-Standardvertragsklauseln; Auftragsverarbeitung nach den Bedingungen des Anbieters