

Ergänzungsvereinbarung: DORA-Anforderungen

Gültig ab: 17.01.2025

zwischen

Organisation und Rechtsform
Straße Nr.
PLZ, Stadt
Land

- im Folgenden „**Auftraggeber**“ genannt –

Und

Evermood GmbH
c/o betahaus
Rudi-Dutschke-Str. 23
10969
Berlin
Deutschland

- Im Folgenden „**Auftragnehmer**“ genannt –

- gemeinsam als „**Vertragsparteien**“ bezeichnet –

1. Zwischen dem Auftraggeber und dem Auftragnehmer (gemeinsam die „Parteien“) besteht eine Leistungsvereinbarung, unter der der separate Vertragsschluss zwischen Auftragnehmer und Auftraggeber verstanden wird, der durch den Abschluss eines Nutzungsvertrags - gemäß der Allgemeinen Geschäftsbedingungen („AGB“) des Auftragnehmers - entsteht.
2. Diese Ergänzungsvereinbarung (einschließlich ihrer Anlagen und Anhänge nachfolgend „Ergänzungsvereinbarung“ genannt) dient der Umsetzung der Anforderungen der DORA-Verordnung („DORA-Verordnung“ bezeichnet die Verordnung (EU) 2022/2554 vom 14. Dezember 2022 über die digitale operationelle Resilienz im Finanzsektor sowie jede nachfolgende Fassung dieser Verordnung, sowie etwaige gesetzliche oder aufsichtsbehördliche Anforderungen auf nationaler oder supranationaler Ebene, die diese in Zukunft ersetzen oder ergänzen mögen). Die Begriffsbestimmungen in Art. 3 der DORA-Verordnung finden auf diese Ergänzungsvereinbarung entsprechende Anwendung.
3. Die Parteien vereinbaren hiermit, dass ergänzend zum Vertrag die in dieser Ergänzungsvereinbarung getroffenen Regelungen gelten. Im Falle von Abweichungen zu den Regelungen des Vertrags haben die Regelungen dieser Ergänzungsvereinbarung Vorrang. Soweit der Vertrag zu Gegenständen dieser Ergänzungsvereinbarung jedoch zusätzliche oder weiter-gehende Regelungen enthält, bleiben diese durch diese Ergänzungsvereinbarung unberührt.
4. Die Regelungen dieser Ergänzungsvereinbarung basieren auf dem gemeinsamen Verständnis der Parteien, dass es sich bei den vertraglichen Leistungen des Auftragnehmers nicht um solche handelt, die der Unterstützung einer kritischen oder wichtigen Funktion im Sinne der DORA-Verordnung dienen. Sofern sich dieses Verständnis ändern sollte oder zur Umsetzung der Anforderungen der DORA-Verordnung aus anderem Grund weitere Änderungen oder Ergänzungen des Vertrages erforderlich sind, werden die Parteien den Vertrag entsprechend anpassen.

_____ Ort, Datum	_____ Ort, Datum
_____ Auftraggeber	_____ Auftragnehmer

Anlagen:

- Anhang 1 (Vertragsregelungen)
- Anhang 2 (Sicherheitsanforderungen)

Anhang 1: Vertragsregelungen

5. Der Auftragnehmer (oder dessen Subunternehmer einschließlich nachgelagerter Subunternehmer) wird die Vertragsleistungen von den in Anhang A.1 (Standorte) genannten Standorten erbringen. Der Anhang A.1 (Standorte) enthält darüber hinaus die Standorte, an denen Daten des Auftraggebers gespeichert und/oder verarbeitet werden. Der Auftragnehmer wird dem Auftraggeber rechtzeitig vorab benachrichtigen, wenn er die – vollständige oder teilweise – Verlegung eines Standortes, die Erbringung von Vertragsleistungen an einem anderen Standort, die Speicherung oder Verarbeitung von Daten an einem anderen Standort oder die Aufgabe eines bestehenden Standortes beabsichtigt. Zum Zwecke dieser Benachrichtigung wird der Auftragnehmer dem Auftraggeber eine Aktualisierung des vorgenannten Anhangs A.1 (Standorte) übermitteln. Zusätzliche oder weitergehende Anforderungen bezüglich der Standorte oder des Einsatzes von Subunternehmern (z.B. Zustimmungsvorbehalte), die an anderer Stelle im Vertrag, insbesondere in den Regelungen zum Datenschutz, geregelt sind, bleiben unberührt.
6. Ist der Auftragnehmer im Rahmen der Erbringung der vertraglichen Leistungen in den Besitz von Daten des Auftraggebers gelangt (z.B. Geschäftsdaten, Kundendaten etc.), ungeachtet, ob es sich um personenbezogene oder nicht personenbezogene Daten handelt, so ist dem Auftraggeber im Falle der Insolvenz, Liquidation, Einstellung der Geschäftstätigkeit des Auftragnehmers oder einer Beendigung des Vertrages ungehinderter Zugang zu den Daten des Auftraggebers zu gewähren. Die Daten sind in einem leicht zugänglichen Format an den Auftraggeber oder an einen von dem Auftraggeber benannten Dritten zu übermitteln. Ein Zurückbehaltungsrecht des Auftragnehmers im Hinblick auf die Rückgabe der Daten des Auftraggebers ist ausgeschlossen.
7. Der Auftragnehmer ist verpflichtet, dem Auftraggeber bei einem IKT- bezogenem Vorfall im Sinne der DORA, der mit der für den Auftraggeber bereitgestellten Leistung in Verbindung steht, ohne zusätzliche Kosten Unterstützung zu leisten.
8. Der Auftragnehmer ist verpflichtet, vollumfänglich mit den für den Auftraggeber zuständigen Aufsichtsbehörden und den von diesen Aufsichtsbehörden benannten Personen zusammenzuarbeiten. „Aufsichtsbehörden“ im Sinne dieser Anlage sind die Europäische Zentralbank, die Bundesanstalt für Finanzdienstleistungsaufsicht, die European Banking Authority, die European Securities and Markets Authority, die Abwicklungsbehörden, einschließlich des Single Resolution Board und der Finanzmarktstabilisierungsanstalt, und jede andere für den Auftraggeber zuständige Behörde.
9. Der Auftraggeber ist berechtigt, den Vertrag aus wichtigem Grund außerordentlich zu dem in der Kündigungserklärung genannten Zeitpunkt zu kündigen, wenn insbesondere einer der folgenden Umstände vorliegt:
 - 9.1. Ein erheblicher Verstoß des Auftragnehmers gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen;
 - 9.2. Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen des Vertrages vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf den Vertrag oder die Verhältnisse des Auftragnehmers auswirken;
 - 9.3. Nachweisliche Schwächen des Auftragnehmers in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt;
 - 9.4. Eine Aufsichtsbehörde kann der Auftraggeber infolge der Bedingungen des Vertrages oder der mit dem Vertrag verbundenen Umstände nicht mehr wirksam beaufsichtigen.
10. Rechte zur Kündigung aus wichtigem Grund, die an anderer Stelle im Vertrag geregelt sind oder sich aus dem Gesetz ergeben, bleiben unberührt.

Anhang A.1 (Standorte)

1. Die folgende Aufstellung beinhaltet die Standorte, an denen vertragliche Leistungen für den Auftraggeber erbracht, Daten Auftraggebers verarbeitet oder Daten des Auftraggebers gespeichert werden.
2. Für jeden Standort, an dem durch den Auftragnehmer oder einen von dessen Subunternehmern Vertragsleistungen erbracht, Daten des Auftraggebers verarbeitet oder gespeichert werden, ist eine gesonderte Zeile auszufüllen.

Name der Gesellschaft	Angabe des Standortes	Leistungen am Standort	Verarbeitung von Daten	Speicherung von Daten	Verarbeitung personenbezogener Daten
T –Systems Internation GmbH (Open Telekom Cloud)	Magdeburg, Deutschland	Hosting der Server zum Betrieb der Software und Versand von (transaktionalen) E-Mails	Personalstammdaten von Ansprechpersonen und Administratoren des Auftraggebers (insb. Name, Position, Telefonnummer, E-Mail-Adresse) Profilfoto von Ansprechpersonen und Administratoren des Auftraggebers Allgemeine und besondere Personendaten von Beschäftigten des Auftraggebers, die diese - im Rahmen von Umfrageteilnahmen, Beratungsanfragen oder zwecks Abgabe von Hinweisen übermitteln	Personalstammdaten von Ansprechpersonen und Administratoren des Auftraggebers (insb. Name, Position, Telefonnummer, E-Mail-Adresse) Profilfoto von Ansprechpersonen und Administratoren des Auftraggebers Allgemeine und besondere Personendaten von Beschäftigten des Auftraggebers, die diese - im Rahmen von Umfrageteilnahmen, Beratungsanfragen oder zwecks Abgabe von Hinweisen übermitteln	Personalstammdaten von Ansprechpersonen und Administratoren des Auftraggebers (insb. Name, Position, Telefonnummer, E-Mail-Adresse) Profilfoto von Ansprechpersonen und Administratoren des Auftraggebers Allgemeine und besondere Personendaten von Beschäftigten des Auftraggebers, die diese - im Rahmen von Umfrageteilnahmen, Beratungsanfragen oder zwecks Abgabe von Hinweisen übermitteln
Edudip GmbH	Frankfurt, Deutschland	Anbieten von virtuellen Live-Events in Form von Videokonferenzen	Nein	Nein	IP-Adresse für die Aufrechterhaltung einer Videokonferenz
3Q GmbH	Nürnberg, Deutschland	Bereitstellung von Video- und Audiodateien	Nein	Nein	Nein
Confrere AS	Dublin, Irland	Bereitstellung von Videoberatungen	Nein	Nein	IP-Adresse für die Aufrechterhaltung einer Videokonferenz

Anhang 2: Sicherheitsanforderungen

1. Allgemeines

- 1.1. Der Auftragnehmer hat im Rahmen seiner Leistungserbringung angemessene Maßnahmen zur Aufrechterhaltung der Informationssicherheit und Geschäftskontinuität zu gewährleisten. Diese Verpflichtung bezieht sich auch auf relevante organisatorische und technische Schnittstellen zum Auftraggeber. Ein angemessenes Sicherheitsniveau hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit ist sicherzustellen.
- 1.2. Der Auftragnehmer verpflichtet sich, den bewährten Stand der Technik und allgemein anerkannte Security Standards und Best Practices (z.B. ISO2700X, BSI-Grundschutz, NIST) für die jeweilig eingesetzten Technologien einzusetzen bzw. einzuhalten und deren Informationssicherheit und Risiken durch ein geeignetes und kontinuierlich zu verbesserndes Managementsystem zu steuern.
- 1.3. Der Auftragnehmer verpflichtet sich, bei einem Sicherheitsvorfall, der mit der zu erbringenden Leistung in Verbindung steht, ohne zusätzliche Kosten Unterstützung zu leisten.
- 1.4. Der Auftragnehmer wird die für die vertragliche Leistung genutzten Systeme, Software und Daten durch technische und organisatorische Maßnahmen gegen unberechtigten Zugang und Zugriffe schützen.
- 1.5. Im Übrigen wird der Auftragnehmer bei der Leistungserbringung das geltende Recht, insbesondere verpflichtende Produktsicherheitspflichten, spezifische IT-sicherheitsrechtliche Anforderungen, und gesetzliche Sorgfaltspflichten einhalten.
- 1.6. Über die Anforderungen dieses Anhang 2 (Sicherheitsanforderungen) hinausgehende Verpflichtungen, die sich aus anderen Vertragsdokumenten ergeben, bleiben unberührt.

2. Sichere Übermittlung von Informationen und Daten

- 2.1. Die Vertragspartner vereinbaren für die Übermittlung von nicht öffentlichen Daten und Informationen den Einsatz von aktuell als sicher angesehenen Verschlüsselungsverfahren.
- 2.2. Nicht öffentlich sind alle Informationen und Daten, die vertraulich oder für die interne Kommunikation bestimmt sind (z.B.: Passwörter, Kommunikationsinhalte, nicht öffentliche Finanzdaten, Informationen über Geschäftsstrategien oder Geschäftsbeziehungen, alle personenbezogenen oder personenbeziehenden Informationen, Fachkonzepte, Systemarchitekturen, Netzwerkpläne).
- 2.3. Die Vertragspartner treffen Vorkehrungen, um die Authentizität der Gegenstellen sowie die Authentizität der Zugriff nehmenden Nutzer für nicht öffentliche Informationen und Daten zu gewährleisten.

3. Informationspflichten

- 3.1. Damit der Auftraggeber in der Lage ist, seine Sorgfaltspflichten umzusetzen und eventuell seinerseits notwendige Meldewege (z.B. durch das IT-Sicherheitsgesetz) zu bedienen, ergeben sich folgende Kommunikationspflichten: Bei Änderungen der technischen oder organisatorischen Gegebenheiten, die potenziell Einfluss auf die Informationssicherheit oder die Geschäftskontinuität haben könnten, sind vorab Ansprechpartner des Auftraggebers zu informieren.
- 3.2. Bei sicherheitsrelevanten Zwischenfällen oder erkannten, die die Sicherheit der Daten oder Prozesse des Auftraggebers verletzt haben oder gefährden können, sind unverzüglich geeignete reaktive oder proaktive Maßnahmen einzuleiten und die Ansprechpartner des Auftraggebers zu informieren. Dies gilt auch für Sicherheitsverstöße bei Subunternehmern des Auftragnehmers. Der Auftragnehmer ist zudem verpflichtet, Sicherheitsvorfälle, die im Sinne der Meldepflichten die für den Auftraggeber erbrachte Dienstleistung betreffen, unverzüglich, d.h. ohne schuldhaftes Zögern, spätestens jedoch am Tage des Bekanntwerdens zu melden, damit der Auftraggeber den Vorfall geeignet behandeln und seinen eigenen Meldepflichten nachkommen kann.

- 3.3. Der Auftragnehmer hat dem Auftraggeber bei sicherheitsrelevanten Anfragen unverzüglich und vollumfänglich entsprechende Auskünfte zu erteilen. Der Auftragnehmer wird dem Auftraggeber auf erste Anforderung zudem umfassend und unverzüglich bei der Aufklärung von Zwischenfällen sowie bei der erforderlichen Kommunikation gegenüber Betroffenen, Behörden oder Gerichten und in sonstiger Weise unterstützen und dem Auftraggeber alle hierfür erforderliche Informationen umfassend zur Verfügung stellen. Diese Unterstützungsleistungen werden ohne zusätzliche Kosten erbracht. Alle Informationen, die die Informationssicherheit des Vertragsverhältnisses zwischen dem Auftraggeber und dem Auftragnehmer betreffen, sind vertraulich zu behandeln.

4. Ansprechpartner für Sicherheitsfragen

- 4.1. Die Parteien benennen einander einen für Informationssicherheit verantwortlichen Ansprechpartner. Die Ansprechpartner koordinieren bei einem sicherheitsrelevanten Zwischenfall die Maßnahmen.

5. Subdienstleister

- 5.1. Der Auftragnehmer verpflichtet alle seine Subunternehmer, die Informationen oder Daten des Auftraggebers weiterverarbeiten, einen Sicherheitsstandard einzuhalten, der mindestens den hier vereinbarten Regelungen, entspricht. Der Auftragnehmer wird dem Auftraggeber hierüber auf Anforderung einen Nachweis erbringen.

6. Schutzbedarf

- 6.1. Für die Leistungserbringung ist ein Schutzbedarf von „mittel“ festgelegt.

7. Sicherheitsanalysen

- 7.1. Beinhaltet die erbrachte Leistung einen Anschluss oder eine Bereitstellung über das Internet, so stellt der Auftragnehmer sicher, dass eine Absicherung nach dem aktuellen Stand der Technik erfolgt. Hierzu führt der Auftragnehmer regelmäßig sowie vor Inbetriebnahme der Leistung und vor wesentlichen Änderungen der Software (Major-Release-Wechsel) eine Sicherheitsanalyse (Penetrationstest) für den Umfang der zu erbringenden Leistung durch. Dem Auftraggeber steht das Recht zu, entsprechende Nachweise einzusehen.
- 7.2. Der Auftragnehmer verpflichtet sich, die bei einer Sicherheitsanalyse festgestellten Schwachstellen auf der Basis eines abgestimmten Umsetzungsplans zu beheben.
- 7.3. Der Auftraggeber ist gemäß der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor („DORA“) aufgefordert, regelmäßig bedrohungsorientierte, fortgeschrittene Tests der operationellen Resilienz (Threat Led Penetration Tests („TLPT“)) durchzuführen. Liegt die zu erbringende Leistung des Auftragnehmers im Spektrum eines TLPTs des Auftraggebers, so verpflichtet sich der Auftragnehmer, sich an dem TLPT zu beteiligen und uneingeschränkt daran mitzuwirken.