Vereinbarung zur Auftragsverarbeitung

gemäss Art. 28 DSGVO

zwischen

– Verantwortlicher –

und

Threema GmbH
Churerstrasse 82
8808 Pfäffikon SZ
Schweiz

– Auftragnehmer –

1. Gegenstand der Vereinbarung

Der Auftragnehmer verarbeitet Daten, um die Übertragung von Kurznachrichten und Medien zwischen Teilnehmern zu ermöglichen. Die Datenverarbeitung erfolgt im Rahmen der Nutzung der Kommunikationslösung «Threema Work» (nachfolgend «Dienstleistung») durch den Verantwortlichen vollumfänglich konform zu den geltenden gesetzlichen Bestimmungen, insbesondere der EU-Verordnung 2016/679 (nachfolgend «DSGVO») und dem Schweizerischen Bundesgesetz über den Datenschutz (DSG). Die in dieser Vereinbarung stipulierten Rechte und Pflichten der Vertragspartner beziehen sich im Sinne von Art. 28 DSGVO ausschliesslich auf Datenverarbeitung, welche im expliziten Auftrag des Verantwortlichen und weisungsbezogen erfolgt.

2. Kategorien betroffener Personen

Nutzer der Dienstleistung mit einer durch den Verantwortlichen zur Verfügung gestellten Lizenz.

3. Art und Umfang der verarbeiteten Daten

Der Auftragnehmer verarbeitet im Rahmen der Auftragserfüllung keine besonderen Datenkategorien im Sinne von Art. 9 Abs. 1 oder Art. 10 DSGVO. Personenbezogene Daten werden, gestützt auf Art. 5 Abs. 1 DSGVO, ausschliesslich aufgrund ihrer Selbstdeklaration und in dem Umfang verarbeitet, wie es für die Nutzung der Dienstleistung erforderlich ist.

A) Bestandsdaten

Nicht personenbezogene Daten, die vom System generiert werden:

- Threema-ID, bestehend aus Kombination von 8 Einzelziffern und/oder -buchstaben.
- Öffentlicher Schlüssel eines lokal generierten Schlüsselpaars.
- Kenndaten zur periodischen Lizenzprüfung, bestehend aus Threema-ID, App-Version, Betriebssystem und Zeitstempel der letzten Lizenzprüfung.

Personenbezogene Daten gemäss Art. 4 Abs. 1 DSGVO, die optional durch den Verantwortlichen oder dessen Nutzer erfasst werden können und für die Nutzung der Dienstleistung nicht zwingend erforderlich sind:

- Rufnummer und/oder E-Mail-Adresse eines Nutzers (in einwegverschlüsseltem Zustand).
- Frei wählbare Zugangsdaten zur Lizenzierung der Threema Work-App, falls individuelle Zugangsdaten verwendet werden.
- Pseudonym / Nickname (vom Verantwortlichen oder Nutzer beliebig gewählt).
- Vorbelegte Einträge auf der Kontaktliste, falls die Option zur Markierung firmeninterner Kontakte verwendet wird. Die Einträge können zusätzlich zur Threema-ID eines Nutzers nach Wahl des Verantwortlichen Angaben zum Namen und/oder zur Funktion oder Abteilung enthalten.

B) Nachrichteninhalte

Sämtliche Nachrichten, einschliesslich Steuernachrichten, werden mit einem hochsicheren Ende-zu-Ende-Verschlüsselungsverfahren verschlüsselt.

Die Header-Informationen einer Nachricht (Absender, Empfänger etc.) werden für die Übertragung an den Server, bzw. vom Server an den Empfänger, zusätzlich verschlüsselt, um ein Mithören dieser Informationen durch Dritte (z.B. in offenen Wireless LANs) zu verunmöglichen.

Der Auftragnehmer hat keine Möglichkeit, Nachrichten der Benutzer zu entschlüsseln, da er keinerlei Kenntnis der privaten Schlüssel hat.

C) Adressbuchdaten

Auf ausdrücklichen Wunsch des Nutzers können E-Mail-Adressen und Telefonnummern aus dem Adressbuch abgeglichen werden. Diese Daten werden ausschliesslich einwegverschlüsselt («gehasht») und zusätzlich mit SSL gesichert an die Server übertragen. Die Server halten diese Hashes nur kurzzeitig im Arbeitsspeicher, um die Liste der übereinstimmenden Threema-IDs zu ermitteln, und löschen sie sofort wieder. Zu keinem Zeitpunkt werden Hashes oder Ergebnisse des Abgleichs auf einen Datenträger geschrieben.

4. Dauer der Datenspeicherung

Der Auftragnehmer löscht automatisch und unwiederbringlich sämtliche Daten im Zusammenhang mit dem Betrieb der Dienstleistung nach folgendem Schema:

1. Ausgelieferte Nachrichten, Steuernachrichten, Medien, Dateien, Profilbilder (alle Ende-zu-Ende verschlüsselt): sofort nach erfolgreichem Download;
2. Nicht ausgelieferte Nachrichten, Steuernachrichten, Medien, Dateien, Profilbilder (alle Ende-zu-Ende verschlüsselt) nach 14 Tagen;

3. Threema-ID, öffentliche Schlüssel, Rufnummer und E-Mail-Verknüpfungen (einwegverschlüsselt) innerhalb von 24 Stunden nach Widerruf;
4. Kenndaten für die Lizenzprüfung sowie Benutzername und Passwort sofort nach Aufhebung des Benutzerkontos durch den Verantwortlichen;
5. Auftragsdaten nach 10 Jahren zur Erfüllung der gesetzlichen Aufbewahrungspflicht.

Der Auftragnehmer erstellt keinerlei Sicherung von Nachrichtendaten. Spätestens nach Ablauf der unter 4.2 genannten Frist löscht er sämtliche Nachrichtendaten vollständig und unwiederbringlich.

5. Technische und organisatorische Massnahmen zur Datensicherheit

Der Auftragnehmer ergreift zur Wahrung der Datensicherheit alle geeigneten technischen und organisatorischen Massnahmen gemäss Art. 32 DSGVO und prüft die administrativen Prozesse regelmässig mittels Audits. Massnahmen umfassen insbesondere:

1. Gewährleistung der Vertraulichkeit
    a) Ausschliesslich eigene Server-Hardware, keine Cloud-Lösung, kein Shared Hosting
    b) Biometrische Zutrittskontrolle zu eigenen Servern in einem hochsicheren Datacenter eines ISO/IEC 27001 zertifizierten Colocation-Partners in Zürich, Schweiz mit Personenvereinzelungsanlage und Videoüberwachung
    c) Zugang nur für designierten Personenkreis und nur für administrative Tätigkeiten
    d) Protokollierung sämtlicher Zugriffe
2. Gewährleistung der Integrität
    a) Speicherung und Verarbeitung ausschliesslich stark verschlüsselt
    b) Keine Weitergabe von Daten, keinerlei Untervertragsverhältnisse oder Outsourcing
    c) URLs für Administrationszwecke nur mittels VPN mit zusätzlicher Zwei-Faktor-Authentifizierung und HTTPS erreichbar
    d) Schutz sämtlicher zur Erbringung der Dienstleistung benötigter Anlagen, Software und Netzwerke mit aktuellen sicherheitstechnischen Massnahmen nach Stand der Technik
3. Gewährleistung der Verfügbarkeit
    a) Datacenter mit Notstromsystemen, Brandschutzeinrichtungen, ausfallsicherer Klimatisierung und vollständig redundanter Internetanbindung
4. Gewährleistung der Belastbarkeit der Systeme
    a) Zweiter Hosting-Standort zur Abwehr von DDoS-Attacken oder zur Überbrückung im Falle von Netzwerk-Ausfällen, vom Hauptstandort örtlich getrennt und mit vergleichbarem Sicherheitsstandard.

6. Rechte und Pflichten des Auftragnehmers

1. Die Auftragsverarbeitung erfolgt grundsätzlich nur durch den Auftragnehmer. Die Verarbeitung durch Dritte, Subunternehmen oder aufgrund von Untervertragsverhältnissen ist ausgeschlossen.

2. Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich im Rahmen der getroffenen Vereinbarung und/oder unter Einhaltung der ggf. vom Verantwortlichen erteilten ergänzenden Weisungen. Eine hiervon abweichende Datenverarbeitung ist dem Auftragnehmer ohne schriftliche Zustimmung des Verantwortlichen untersagt. Bekanntgabe, Verkauf, Vermietung oder anderweitige Verwendung der Daten durch Dritte bzw. die kommerzielle Verwendung schliesst der Auftragnehmer ausdrücklich aus.

3. Der Auftragnehmer sichert die datenschutzkonforme Verarbeitung von personenbezogenen Daten und die vertragsmässige Abwicklung aller vereinbarten Massnahmen zu. Er stellt sicher, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Mass gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

4. Die vorhandenen Datenverarbeitungsprozesse gewährleisten die Einhaltung der gesetzlichen Vorschriften, der Regelungen dieser Vereinbarung sowie etwaiger weiterer Weisungen des Verantwortlichen. Der Auftragnehmer informiert den Verantwortlichen frühzeitig über allfällige Änderungen der hier dargelegten Zusicherungen.

5. Der Auftragnehmer informiert den Verantwortlichen, falls

    - er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Europäischen Union oder deren Mitgliedstaaten verstösst;
    - verarbeitete Daten unrechtmässig übermittelt worden oder auf sonstige Weise Dritten unrechtmässig zur Kenntnis gelangt sind.

6. Der Auftragnehmer unterstützt den Verantwortlichen bei seiner Meldepflicht nach Art. 33 DSGVO und stellt dem Verantwortlichen einen Nachweis über die Einhaltung dieser Pflichten gemäss Art. 28 Abs. 3. lit. h gegen Vergütung allfälliger Mehraufwände zur Verfügung.

7. Rechte und Pflichten des Verantwortlichen

1. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Verantwortlichen.

2. Der Verantwortliche hat das Recht, vor Beginn und während der Datenverarbeitung Auskunft über die beim Auftragnehmer getroffenen technischen und organisatorischen Massnahmen zur Wahrung der Datensicherheit zu erhalten.

3. Der Verantwortliche ist für die Sicherheit der Daten auf den Endgeräten sowie dem Transportweg zum Auftragnehmer verantwortlich und bestimmt die Art und den Umfang der technischen und organisatorischen Sicherheitsmassnahmen (z.B. Verschlüsselung).

4. Der Verantwortliche kann weisungsberechtigte Personen benennen. Für den Fall, dass sich die weisungsberechtigten Personen beim Verantwortlichen ändern, wird der Verantwortliche dies dem Auftragnehmer schriftlich per E-Mail mitteilen.

5. Der Verantwortliche hat das Recht, sich bei Fragen zur Datenverarbeitung und zur Gewährleistung der Einhaltung dieser Vereinbarung an den Datenschutzbeauftragten des Auftragnehmers zu wenden:

   Threema GmbH
   Datenschutzbeauftragter
   Churerstrasse 82
   8808 Pfäffikon
   Schweiz
   privacy@threema.ch

   Vertreter in der Europäischen Union gemäss Art. 27 DSGVO: GeKaCe GmbH, Abt. T, Weilerweg 13, 72411 Bodelshausen, Deutschland.

8. Vertraulichkeitsverpflichtung

1. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung des Datengeheimnisses und zu Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Verantwortlichen obliegen. Der Verantwortliche ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit deren Anwendung vertraut ist.

3. Der Auftragnehmer verpflichtet alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Verantwortlichen erbringen, alle Daten des Verantwortlichen, insbesondere die für den Verantwortlichen verarbeiteten personenbezogenen Daten, vertraulich zu behandeln.

9. Berichtigung, Löschung und Sperrung von Daten

1. Der Verantwortliche ist für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Verantwortlichen unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Verantwortlichen erforderlich ist und er dies mit den ihm vom Auftragnehmer zur Verfügung gestellten Mitteln nicht selbst erbringen kann, wird der Auftragnehmer die jeweils erforderlichen Massnahmen nach Weisung des Verantwortlichen treffen.

3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Verantwortlichen beim Auftragnehmer entstehen, bleiben unberührt.

10. Laufzeit und Kündigung des Auftrags

1. Die Vereinbarung tritt zum Zeitpunkt der Aktivierung der lizenzierten Dienstleistung in Kraft und wird auf ein Jahr abgeschlossen. Ohne Kündigung verlängert sich die Laufzeit nach Ablauf eines Jahres automatisch um ein weiteres Jahr.

2. Beide Parteien können das Vertragsverhältnis jederzeit auf Ende der jährlichen Vertragsdauer unter Einhaltung einer Kündigungsfrist von 3 Monaten schriftlich kündigen. Der Vertrag endet automatisch, falls die Nutzungslizenz nicht erneuert wird bzw. wenn die Nutzung eingestellt wird.

3. Dessen ungeachtet ist der Verantwortliche zu einer ausserordentlichen fristlosen Kündigung des Vertrags aus wichtigem Grund berechtigt, wenn der Auftragnehmer schwerwiegende Vertragsverletzungen wie z.B. einen Verstoss gegen die datenschutzrechtlichen Bestimmungen begangen hat.

11. Beendigung

1. Nach Beendigung des Vertrages löscht der Auftragnehmer physisch sämtliche in seinen Besitz gelangten Daten, die im Zusammenhang mit der Auftragserfüllung stehen und gemäss 4. noch nicht gelöscht wurden, mit Ausnahme der zur Wahrung der gesetzlichen Aufbewahrungspflicht notwendigen Informationen und Dokumente am Sitz des Auftragnehmers.

2. Der Verantwortliche hat das Recht, sich die vollständige und vertragsgemässe Löschung der Daten beim Auftragnehmer dokumentieren und bestätigen zu lassen.

12. Schlussbestimmungen

Änderungen dieser Vereinbarung bedürfen der Schriftform. Mündliche Nebenabreden bestehen nicht.

Sollte eine der vorstehenden Bestimmungen ganz oder teilweise unwirksam oder lückenhaft sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, die unwirksame oder lückenhafte Bestimmung durch eine solche wirksame zu ersetzen, die dem wirtschaftlichen Zweck und Willen der Parteien am nächsten kommt.

Gerichtsstand ist Sitz des Auftragnehmers, es gilt Schweizer Recht.

_____ _____

_____

Unterschrift(en) Verantwortlicher

Pfäffikon SZ,

Unterschrift Auftragnehmer