



Vertrag über die Auftragsverarbeitung

Inhaltsverzeichnis

1. Vertragsgegenstand	3
2. Anwendung der EU Standardvertragsklauseln	3
3. Ergänzungen zu den EU Standardvertragsklauseln	4
4. Gegenstand des Auftrags	4
5. Dauer des Auftrags	4
Anlagenverzeichnis	4

For English version please see after page 23

Userlike UG (haftungsbeschränkt)

Probsteigasse 44-46

D-50670 Köln

verpflichtet sich als Auftragnehmer gegenüber dem Kunden (nachfolgend entweder als „**Kunde**“ oder „**Auftraggeber**“ bezeichnet)

nach Maßgabe der folgenden Bestimmungen:

1. Vertragsgegenstand

Dieser Vertrag zur Auftragsverarbeitung gemäß Art 28 DSGVO (nachfolgend „**Vertrag**“) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, welche sich aus den zwischen den Parteien bereits bestehenden oder künftig abzuschließenden Verträgen (nachfolgend „**Hauptvertrag/AGB**“) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch Userlike für den Auftraggeber kommt. Er findet Anwendung auf alle Tätigkeiten, die mit dem Gegenstand des Auftrags (Ziffer 4) in Zusammenhang stehen und bei denen Beschäftigte von Userlike oder durch Userlike Beauftragte, personenbezogene Daten des Verantwortlichen verarbeiten.

2. Anwendung der EU Standardvertragsklauseln

2.1 Die Parteien legen diesem Vertrag in **Anlage 1** die „Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR“ gemäß Durchführungsbeschluss der Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 (7) DSGVO und Artikel 29 (7) der Verordnung (EU) 2018/1725 vom 4. Juni 2021 (nachfolgend „**EU Standardvertragsklauseln**“) zugrunde.

2.2 Dabei vereinbaren die Parteien folgende in den EU Standardvertragsklauseln aufgeführten Optionen:

- Klausel 1: Option 1
- Klausel 7.7. a): Option 2, Zeitraum: 30 Tage (siehe Anlage 5 Ziffer 2)
- Klausel 8.c) 4: Option 1
- Klausel 9.1.b): Option 1
- Klausel 9.1.c): Option 1
- Klausel 9.2.c): Option 1

3. Ergänzungen zu den EU Standardvertragsklauseln

Die Parteien vereinbaren in **Anlage 5** Ergänzungen und Aktualisierungen zu den EU Standardvertragsklauseln im Sinne der Klausel 2 der EU Standardvertragsklauseln.

4. Gegenstand des Auftrags

Gegenstand der Verarbeitung ist die Bereitstellung der im Hauptvertrag/[AGB](#) bezeichneten Userlike Services durch den Auftragnehmer für den Auftraggeber.

Userlike bietet eine Messenger Funktion für den Web- und Mobilsupport. Die softwarebasierte Lösung zur Chat-Kommunikation bietet einen Kundensupport in Echtzeit und asynchroner Kommunikation, und hilft den Kundenservice auszubauen.

5. Dauer des Auftrags

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags/[AGB](#). Eine Kündigung des Hauptvertrags/[AGB](#) bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

Anlagenverzeichnis:

- [Anlage 1](#): EU Standardvertragsklauseln (Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR – Stand: 4. Juni 2021, Sprache: deutsch)
- [Anlage 2](#): Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen
- [Anlage 3](#): Unterauftragsverarbeiter
- [Anlage 4](#): Technische und organisatorische Maßnahmen gem. Art 32 DSGVO
- [Anlage 5](#): Ergänzungen zu den EU Standardvertragsklauseln

Anlage 1: EU Standardvertragsklauseln (Stand 4. Juni 2021)

Siehe:

<https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=DE>

[EU_SCC_20210604_DE.pdf](#)

Anlage 2: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

1. Zweck der Verarbeitung

Userlike bietet eine Messenger Funktion für den Web- und Mobilsupport. Die softwarebasierte Lösung zur Chat-Kommunikation bietet einen Kundensupport in Echtzeit und asynchroner Kommunikation, und hilft den Kundenservice auszubauen.

2. Kategorien von Daten

Die von der Verarbeitung betroffenen Kategorien von Daten hängen von der Nutzung der Userlike Services durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind:

Endnutzer

- Chat-Transkript
- Email-Adresse
- Browser
- Betriebssystem
- Endgerät
- Anzahl der Seitenaufrufe
- Anzahl der Seitenbesuche
- Referrer
- URL (wo der Chat gestartet ist)
- Umfrage vor und nach dem Chat (optional)
- Chat-Thema
- Chat-Status (neu, wartend, beendet)
- Chat-Bewertung nach dem Chat
- Dauer des Chats
- Datum des Chats
- Geo-Location (freiwillig, optional)

- Mediale Dateien, die der Kontakt während des Chats mit dem Operatoren teilt
- Optionale Datenfelder, die der Auftraggeber an Userlike übergibt
- IP-Adresse

Profileinstellungen des Operators

- Username
- Vorname
- Nachname
- Alias-Name
- Email-Adresse
- Sprache
- Zeitzone
- Operator-Gruppe
- Profilfoto
- Chat Transkripte
- Analytics-Kennzahlen zur Chat-Performance
- IP-Adresse

3. Kategorien betroffener Personen

Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der individuellen Nutzung der Userlike Services durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht:

- Kunden
- Website-Besucher
- Interessenten
- Operatoren des Auftraggebers

Anlage 3: Unterauftragsverarbeiter

Userlike setzt für die Verarbeitung folgende Unterauftragsverarbeiter ein:

Dienstleister	Erläuterung und Zweck	Funktion, in deren Rahmen der Einsatz des Unterauftragnehmers stattfindet	Serverstandort	Rechtsgrundlage für etwaige Drittstaatentransfers
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	<i>Hosting der Server</i> <i>Speicherung der Daten</i> Verarbeitete Daten: Siehe Anlage 2, Ziffer 2	Systemimmanent	Deutschland	–
Myra Security GmbH Landsberger Str. 187 80687 München Deutschland	<i>Erweiterter DDoS-Schutz</i> Verarbeitete Daten: Siehe Anlage 2, Ziffer 2	Systemimmanent	Deutschland	–
BunnyWay, informacijske storitve d.o.o. Škofjeloška Cesta 13 1215 Medvode, Slowenien	<i>Ausspielen der technischen Komponenten</i> (DNS, Bilder der Webseite, JavaScript Code, Stylesheet-Dateien) <ul style="list-style-type: none"> • IP-Adresse • Browser • Betriebssystem • Operator Profil-Bilder 	Systemimmanent	Regionsabhängig	–
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	<i>Ausspielen der technischen Komponenten</i> (JavaScript Code, Bilder) <ul style="list-style-type: none"> • IP-Adresse • Browser • Betriebssystem • Operator Profil-Bilder 	Systemimmanent	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)

	<p><i>Angebot des File Uploads.</i> Erweiterung und Verbesserung der Kerndienstleistung.</p> <ul style="list-style-type: none"> • User File-Uploads • Operator File-Uploads • IP-Adresse • Browser • Betriebssystem 	Optional	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)
	<p><i>Angebot einer Benachrichtigungs-E-Mail</i> über die Antwort des Operators, die dem Endnutzer zugesendet wird, während dieser offline ist, sowie das Senden der Operator-Benachrichtigungen und Chat-Transkripte. Erweiterung und Verbesserung der Kerndienstleistung.</p> <ul style="list-style-type: none"> • E-Mail-Adresse • Nutzergenerierter Inhalt • IP-Adresse • Browser • Betriebssystem 	Optional	Irland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)
<p>DeepL GmbH</p> <p>Im Mediapark 8a 50670 Köln Deutschland</p>	<p><i>Angebot einer maschinellen Übersetzung von Nachrichteninhalten</i> (verschlüsselt, für die Dauer der Übersetzung). Erweiterung und Verbesserung der Kerndienstleistung.</p> <ul style="list-style-type: none"> • Nutzergenerierter Inhalt 	Optional	Deutschland	–
<p>Mailgun Technologies, Inc.</p> <p>112 E Pecan St #1135 San Antonio, Texas 78205 USA</p>	<p><i>Email-Benachrichtigungen für Endnutzer</i></p> <p>Dient als Backup für AWS. Benachrichtigungs-Email (Outbound) über die Antwort des Operators, die dem Endnutzer zugesendet wird, während dieser offline ist, sowie Operator-E-Mails, Chat-Transkripte und Operator-Benachrichtigungen.</p> <ul style="list-style-type: none"> • E-Mail-Adresse • Kontakt Name 	Optional	EU	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)

	<ul style="list-style-type: none"> • Nutzergenerierter Inhalt <p><i>Angebot einer E-Mail-Antwortmöglichkeit des Endnutzers auf eine E-Mail-Benachrichtigung.</i></p> <p>Erweiterung und Verbesserung der Kerndienstleistung.</p> <ul style="list-style-type: none"> • E-Mail-Adresse • Nutzergenerierter Inhalt • IP-Adresse • Browser • Betriebssystem 			
Twilio Inc. 375 Beale Street, Suite 300, San Francisco, California 94105 USA	<p><i>Audio- und Video Chat.</i></p> <p>Erweiterung und Verbesserung der Kerndienstleistung.</p> <ul style="list-style-type: none"> • Nutzergenerierter Inhalt • IP-Adressen • Browser • Betriebssystem 	Optional	USA	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)
FullContact 1624 Market St Ste 226, PMB 45057, Denver, Colorado 80202 USA	<p><i>Angebot, öffentliche Profile der Endnutzer anhand der E-Mail Adresse in den Kontakt Details anzuzeigen.</i></p> <p>Erweiterung und Verbesserung der Kerndienstleistung.</p> <ul style="list-style-type: none"> • Endnutzer E-Mail-Adresse 	Optional	USA	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)
OMQ GmbH Chausseestraße 22 10115 Berlin Deutschland	<p><i>Optionales KI-Software Angebot.</i></p> <p>Zugriff nur in Verbindung mit Chatbot API.</p> <p>Möglichkeit, eine KI-basierte Wissensdatenbank zu erstellen, um den Kundenservice zu automatisieren (z. B. über Chatbots oder smart FAQ u.a.) vom Userlike Dashboard aus:</p> <ul style="list-style-type: none"> • Operator IP-Adresse • Operator Name • Operator E-Mail Adresse 	Optional	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)

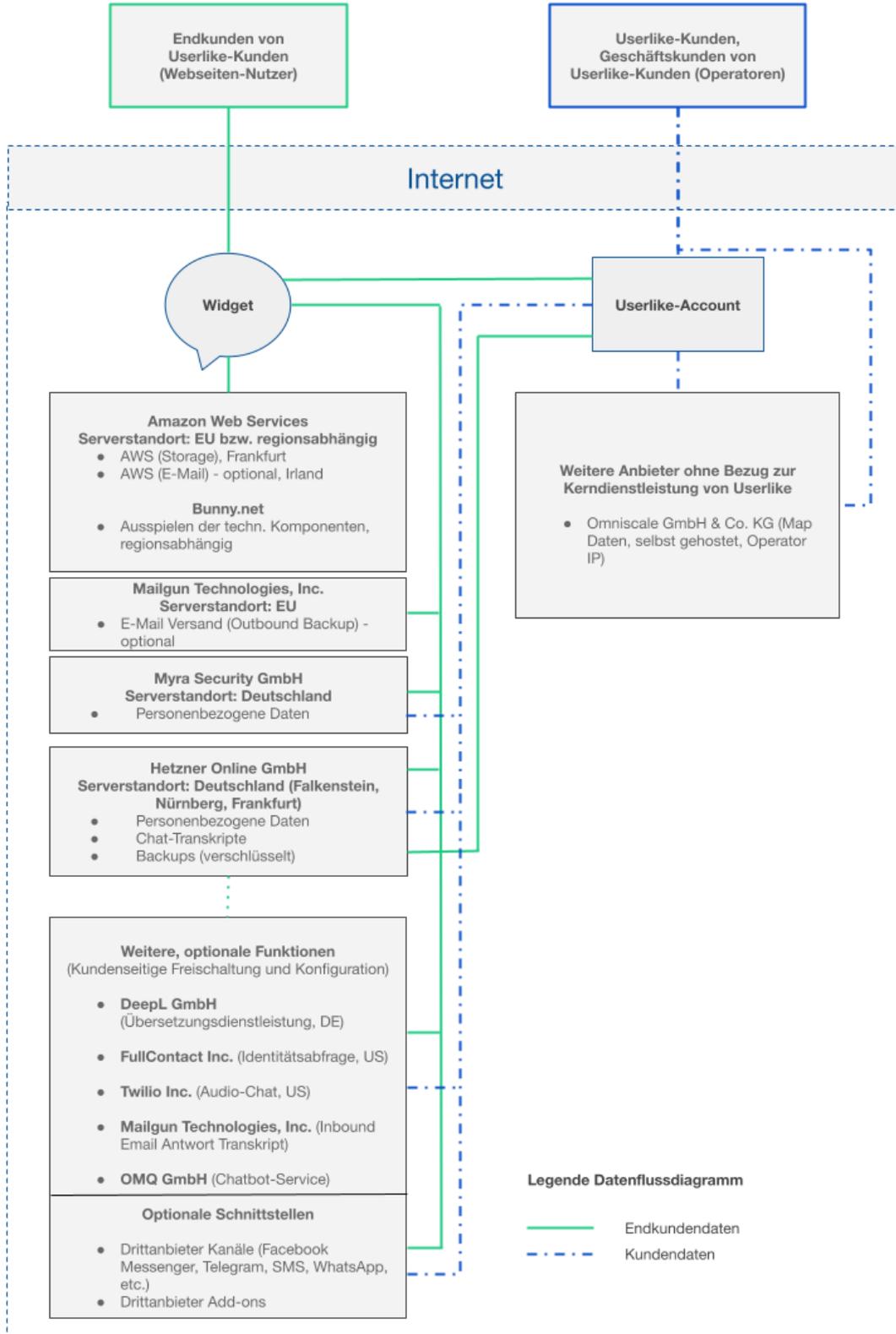
	<p><i>Optionales Angebot des KI-Software Hostings:</i></p> <p>Der Algorithmus entfernt personenbezogene Daten bevor diese von der KI gespeichert werden:</p> <ul style="list-style-type: none"> • Nutzergenerierter Inhalt (KI-Nachrichten und Kontakt Antworten) wird anonymisiert 	<p>Optional (immanent bei Nutzung des KI-Software Angebots)</p>	<p>Deutschland</p>	<p>SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)</p>
--	--	---	--------------------	---

Anlage 4: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Zum Zeitpunkt des Vertragsschlusses hat Userlike die nachfolgend dargestellten technisch-organisatorischen Maßnahmen implementiert:

1. Datenflussdiagramm

Auf dem nachfolgenden Chart ist der grobe Datenfluss dargestellt:



2. Organisationskontrolle

Sollvorgabe: Das Personal des Auftragnehmers ist auf das Datengeheimnis und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten. Die Tatsache der Verpflichtung sollte zum Zweck eines jederzeitigen Nachweises in der Personalakte dokumentiert werden.

Entsprechende Unterlagen sind in der Personalakte hinterlegt.

- Textbaustein ist im Standardvertrag für alle Mitarbeiter hinterlegt.
- Mitarbeiter werden nochmals in internen Schulungen darauf hingewiesen.

3. Zutrittskontrolle

Sollvorgabe: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (wobei der Begriff räumlich zu verstehen ist). Der Auftragnehmer hat zu diesem Zweck ein Zutrittskontrollsystem zu installieren.

Beschreibung der Zutrittskontrollsysteme im Büro (inklusive der physischen Schutzvorkehrungen):

- mechanische Schließanlage Haupteingang sowie Büroeingänge
- elektronische Alarmanlage und Entriegelung mit 24/7 Wachschutz
- Kameras

Beschreibung der Überwachungseinrichtungen:

- Alarmanlage mit Aufschaltung auf Wachschutz - Wachschutz Berger, Köln
- 3 x Ubiquity Cameras + externer Server

4. Zugangskontrolle

Sollvorgabe: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Zu diesem Zweck muss der Zugang zu den DV-Anlagen kontrolliert und protokolliert werden (z. B. Anmelden im System,

unerlaubtes Hochfahren und Eindringen in DV- System verhindern).

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Beschreibung der implementierten Authentifizierungsmechanismen (z.B. Passwortkomplexität, Wechselzyklen, SSH Keys):

- SSH: personalisierte Public Private Keys
- Wartungsarbeiten: OpenVPN (Zertifikate) S2S Kommunikation: VPN
- C2S (Client to Server) Kommunikation: TLS 1.3 und TLS 1.2

Beschreibung der Maßnahmen bei temporärer Inaktivität der Nutzer (z.B. Mitarbeiter verlässt den Arbeitsplatz):

- Beim MacOS X System sind Hot Corners konfiguriert, sodass die Maus in eine Ecke geschoben wird, um den Bildschirm schnell zu sperren. Andernfalls sperrt sich der Monitor nach 5 Minuten.
- Alle MA werden aufgerufen, Bildschirme immer zu sperren.

Beschreibung der technischen Schutzmaßnahmen für Ihre Netzwerkumgebung:

- iptables-Regeln auf externen Schnittstellen
- Dienste lauschen nur auf internen Netzen
- VPN-Kommunikation für Server
- wöchentliche nmap-Scans
- wöchentliche OpenVAS-Scans
- tägliches Monitoring
- tägliches Audit neuer kritischer Fehler
- Anti-DDoS im Datacenter Hetzner online GmbH
- Zusätzliches Anti-DDoS bei Dienst Myra Security GmbH
- OpenVPN-Tunnel zu internen Diensten

5. Zugriffskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Personenbezogene Daten müssen bei persistenter Speicherung verschlüsselt werden.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beschreibung der Verhinderung unerlaubter Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen (Rollen und Berechtigungen nach dem Need-to-Know Prinzip):

- Rechte- und Rollenmanagement
- Technisches Onboarding und Offboarding von Mitarbeitern
- Zugänge und Rechtevergabe nur nach Erforderlichkeit

Beschreibung der Maßnahmen gegen unzulässige Zugriffe (z. B. Brute Force, SQL Injection, Login Validierung):

- SSH: fail2ban
- SQL Injections werden durch Nutzung von Query Parameterization bei Datenbankabfragen systematisch ausgeschlossen
- Alle kritischen Endpunkte werden mit Rate Limits gegen Brute Force Angriffe geschützt
- Darüber hinaus werden alle üblichen Django Framework Sicherheitsfeatures (CSRF-Token etc.) genutzt.
- Zugänge für Userlike Mitarbeiter sind durch eine 2-Faktor Authentifizierung zusätzlich geschützt.
- Kundenseitig können weitere Sicherheitsfeatures wie eine Login-Validierung per Email aktiviert werden.

Beschreibung der Sicherstellung, dass ausschließlich personalisierte Benutzerkonten für den Zugriff auf die Systeme genutzt werden (ein Konto je Benutzer):

- personalisierter Produkt/Backend-Account je Nutzer.
- personalisierter VPN Account je Nutzer
- personalisierter Benutzer-Account auf einem Computer

Beschreibung der implementierten Verschlüsselungsmaßnahmen der personenbezogenen Daten:

- Festplattenverschlüsselung mit LUKS2 (cipher: aes-xts-plain64, keysize: 512 bits)
- Transportverschlüsselung mit TLS 1.3 und 1.2
- VPN
- SSH-Sicherungen: GPG

5.1. Weitergabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Personenbezogene Daten sind nur verschlüsselt zu übertragen (Transportverschlüsselung).

Beschreibung der Transportverschlüsselung:

- Transportverschlüsselung mit TLS 1.3 und 1.2
- VPN

- SSH

Beschreibung der Protokollierung der Weitergabe von personenbezogenen Daten:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern heruntergeladen oder weitergegeben. Ausnahme: Sicherungen. Sicherungen werden protokolliert und verschlüsselt. Täglich manuell geprüft.

Beschreibung der Transportsicherung bei einem physikalischen Transport:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern physikalisch transportiert.

5.2. Eingabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Ein detailliertes Logging System über die Eingabe, Veränderung oder Löschung von personenbezogenen Daten (z. B. Logdateien) ist zu implementieren und regelmäßig auszuwerten.

Beschreibung der Logging / Monitoringsystem zur Überwachung der Zugriffe:

- Dem Kunden steht ein Auditlog zur Verfügung. Das Auditlog ist ein Protokoll, in dem alle Änderungen am Account des Kunden verzeichnet sind.
- Auf der Ebene von Servern werden diverse Protokolle mitgeschrieben, die durch das Anmelden von Mitarbeitern bei Wartungsarbeiten erstellt werden. Diese Protokolle werden stichprobenartig kontrolliert.
- Weiterhin werden diverse Protokolle generiert, die den technischen Zustand des Systems darstellen.

5.3. Verfügbarkeitskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Datensicherungskonzepts (z. B. Back-Up Verfahren, Redundanzen, USV, Notfallpläne):

- 3 Datacenter (System 3-fach vorhanden)
- 2 verschiedene Standorte/Rechenzentren
- USVs und Dieselgeneratoren an allen Datacenter-Standorten
- gespiegelte Festplatten
- Enterprise-Festplatten
- Autofailover für Webnodes
- Autofailover für Statistikdaten
- Automatisiertes Monitoring
- tägliche Backups aller Daten
- Backups an 2 verschiedenen Orten
- mehrere Mitarbeiter, die Prozess beherrschen

5.4. Trennungsgebot

Sollvorgaben: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Der Auftragnehmer sorgt für eine nachweislich logische Trennung der Daten des Mandanten, d.h. Daten verschiedener Auftraggeber sind getrennt zu verarbeiten. Gegenseitiger Zugriff ist auszuschließen. Ebenso werden die Daten nur zweckgebunden verarbeitet.

Beschreibung der Umsetzung zur Mandantenfähigkeit:

- Daten werden zweckgebunden verarbeitet. Daten werden auf Datenbankebene logisch nach Mandanten getrennt (Mandantenfähigkeit).

Beschreibung der Sicherstellung der Trennung von Entwicklung-, Test- und Produktivsystemen:

Physikalische Trennung (verschiedene Server) in 3 Umgebungen:

- Development
- Staging
- Produktion

5.5. Informationssicherheit

Beschreibung des Informationssicherheitsmanagementsystems (ISMS):

Diverse Prozesse:

- IT-Sicherheitsprozess
 - Input: Scans, Meldungen, Protokolle
 - Verarbeitung: Bewertung
 - Output: Maßnahmen
 - Tools: nmap, rkhunter, Lynis
- Verantwortung:
 - IT-Security: security@userlike.com
 - Datenschutz: privacy@userlike.com
- Regelmäßige Schulungen
 - IT Security
 - Datenschutz
 - Feste Prozesse
 - Onboarding
 - Offboarding
- Rechte und Rollenmanagement

5.6. Sonstiges

Beschreibung der Sicherstellung der vertraulichen Aufbewahrung sowie der Löschung oder Vernichtung von Test- und Ausschussmaterialien mit personenbezogenen Daten (z. B. Papier):

- Nicht anwendbar. Da keine Nutzung von Papier. Ausnahme: Buchhaltung, sowie Verträge. Dokumente werden geschreddert.
- Festplatten werden grundsätzlich immer verschlüsselt und vor Abgabe mehrfach überschrieben.

6. Einsatz von Unterauftragnehmern

Die von uns eingesetzten weiteren Auftragsverarbeiter jeweils zum Zeitpunkt des Abschlusses dieser Vereinbarung implementierten technischen und organisatorischen Maßnahmen sind auf Anfrage zu erhalten. Wir versichern uns in regelmäßigen Abständen von der Angemessenheit und Wirksamkeit der von unseren Unterauftragnehmern getroffenen Maßnahmen.

7. Versicherung des Auftragnehmers

Der Auftragnehmer garantiert, dass alle in diesem Dokument genannten Angaben der Wahrheit entsprechen.

Anlage 5: Ergänzungen zu den EU Standardvertragsklauseln

Die Parteien vereinbaren folgende Ergänzungen und Aktualisierungen zu den EU Standardvertragsklauseln (Anlage 1):

1. Dokumentation und Einhaltung der Klauseln (Klausel 7.6)

Klausel 7.6 der EU Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

Zur Durchführung solcher Inspektionen gem. Klausel 7.6 c) ff. ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen Userlikes die Geschäftsräume zu betreten, in denen Auftraggeber Daten verarbeitet werden.

2. Einsatz von Unterauftragsverarbeitern (Klausel 7.7)

Klausel 7.7. a) der EU Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

Userlike wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter in elektronischem Format mit einer Frist von 30 Tagen informieren. In Ausnahmefällen, beispielsweise wenn die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter aus Gründen akuter Vorkommnisse im Bereich der IT-Sicherheit geboten erscheint, ist es Userlike gestattet, den Auftraggeber über beabsichtigte Änderungen mit einer Frist von 5 Tagen zu informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, Userlike nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Werktagen nach Zugang der Benachrichtigung Einspruch

erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist Userlike berechtigt, den Hauptvertrag (AGB) und diesen Vertrag zum nach dem Hauptvertrag (AGB) nächstmöglichen Zeitpunkt zu kündigen.

3. Internationale Datenübermittlungen (Klausel 7.8)

Klausel 7.8 der EU Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

Es ist Userlike gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

4. Umfang der Beauftragung

Die EU Standardvertragsklauseln werden um die folgenden Regelungen ergänzt:

Userlike bleibt es vorbehalten, die Auftraggeber-Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten. Userlike wird den Auftraggeber vor der erstmaligen Anonymisierung in Textform über die näheren Umstände informieren.



Data Processing Agreement for Userlike

Table of contents

1. Object of agreement	3
2. Implementation of the EU Standard Contractual Clauses	3
3. Additions to the EU Standard Contractual Clauses	4
4. Scope of the contract	4
5. Term of the agreement	4
Schedule of annexes	4

Userlike UG (haftungsbeschränkt)

Probsteigasse 44-46

D-50670 Cologne, Germany,

the Processor, undertakes to provide services to the Customer (hereinafter referred to as “Customer” or “Controller”)

in accordance with the following provisions:

1. Object of Agreement

This data processing addendum pursuant to Art. 28 of the GDPR (hereinafter "**Contract**") specifies the obligations of the contracting parties with regard to data protection, which result from the contracts already existing between the parties or to be concluded in the future (hereinafter "**principal contract/ Terms and conditions**"), under which personal data is processed by Userlike for the Controller. It shall apply to all activities which are related to the scope of the contract (Section 4) and in which employees of Userlike or persons authorized by Userlike process personal data of the Controller.

2. Implementation of the EU Standard Contractual Clauses

2.1 The Parties shall base this Agreement on the "Standard Contractual Clauses for Controllers and Processors in the EU / EEA" pursuant to the Commission Implementing Decision on Standard Contractual Clauses between Controllers and Processors pursuant to Article 28 (7) of the GDPR and Article 29 (7) of Regulation (EU) 2018/1725 of June 4, 2021 (hereinafter "**EU Standard Contractual Clauses**") in **Annex 1**.

2.2 The parties shall agree on the following options listed in the EU Standard Contractual Clauses:

- Clause 1: Option 1
- Clause 7.7. a): Option 2, time period: 30 days (see Annex 5, point 2)
- Clause 8.c) 4: Option 1
- Clause 9.1.b): Option 1
- Clause 9.1.c): Option 1
- Clause 9.2.c): Option 1

3. Additions to the EU Standard Contractual Clauses

The parties agree in **Annex 5** on additions and updates to the EU Standard Contractual Clauses within the terms of clause 2 of the EU Standard Contractual Clauses.

4. Scope of the agreement

Scope of the Processing is the provision of the Userlike services designated in the principal contract/Terms and conditions by the Processor for the Controller

Userlike offers a messenger function for web and mobile support. The software-based chat communication solution offers customer support in real time and asynchronous communication and helps to develop customer service.

1. Term of the agreement

The term and termination of this Agreement is based on the provisions on term and termination of the principal contract/[Terms and conditions](#). Termination of the principal contract/[Terms and conditions](#) automatically results in termination of this Agreement. This Agreement cannot be terminated individually.

Schedule of annexes:

- [Annex 1](#): EU Standard Contractual Clauses (Standard contractual clauses for controllers and processors in the EU/EEA – published: Juni 4, 2021, English)
- [Annex 2](#): Purpose, type and scope of data processing, type of data and data subject categories
- [Annex 3](#): Sub-processors
- [Annex 4](#): Technical and organizational measures in accordance with Art. 32 GDPR
- [Annex 5](#): Additions to the EU Standard Contractual Clauses

Annex 1: EU Standard Contractual Clauses (as per June 4, 2021)

See:

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0915&from=EN>

[EU_SCC_20210604_EN.pdf](#)

Annex 2: Purpose, type and scope of data processing, type of data and data subject categories

1. Purpose of the processing

Userlike offers a messenger function for web and mobile support. The software-based chat communication solution offers customer support in real time and asynchronous communication and helps to develop the customer service.

2. Categories of data

The categories of data affected by the processing depend on the use of Userlike services by the Controller. The possible categories of data that fall within the subject matter of the processing are:

End user

- Chat transcript
- E-mail address
- Browser
- Operating system
- Device
- Number of page requests
- Number of page visits
- Referrer
- URL (where the chat originated)
- Questionnaire before and after the chat (optional)
- Chat topic
- Chat status (new, pending, closed)
- Chat evaluation after the chat
- Duration of the chat
- Date of the chat
- Geo location (voluntary, optional)
- Media files shared by the contact with the operator during the chat
- Optional data fields that the Controller passes on to Userlike

- IP addresses

Operator's profile settings

- Username
- First name
- Surname
- Alias name
- E-mail address
- Language
- Time zone
- Operator group
- Profile photo
- Chat transcripts
- Analytics figures on chat performance
- IP addresses

3. Categories of data subjects

The categories of data subjects affected by the processing depend on the individual use of Userlike services by the Controller. Possible categories of data subjects are:

- Customers
- Website visitors
- Interested parties
- Controller's operators

Annex 3: Sub-processors

Userlike engages the following sub-processors for the processing:

Service provider	Explanation and purpose	Function within the scope of which the subcontract or is being engaged	Server location	Legal basis for possible third country transfer
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Germany	<i>Hosting of the servers</i> <i>Data storage</i> Data processing: See Annex 2, Section 2	Inherent in the system	Germany	–
Myra Security GmbH Landsberger Str. 187 80687 München Germany	<i>Expanded DDoS protection</i> Data processing: See Annex 2, Section 2	Inherent in the system	Germany	–
BunnyWay, informacijske storitve d.o.o. Škofjeloška Cesta 13 1215 Medvode, Slovenia	Displaying of the technical components (DNS, website images, JavaScript code, stylesheet files) <ul style="list-style-type: none"> • IP address • Browser • Operating system • Operator profile images 	Inherent in the system	region-dependent	–
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	Displaying of the technical components (JavaScript code, pictures). <ul style="list-style-type: none"> • IP address • Browser • Operating system • Operator profile images 	Inherent in the system	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)

	<p><i>File upload offer.</i> Expansion and improvement of core services.</p> <ul style="list-style-type: none"> • User file uploads • Operator file uploads • IP address • Browser • Operating system 	Optional	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)
	<p><i>Offer of a notification email</i> regarding the operator's response that is sent to the end user whilst the latter is offline and sending the operator notifications and chat transcripts. Expansion and improvement of core services.</p> <ul style="list-style-type: none"> • E-mail address • User-generated content • IP address • Browser • Operating system 	Optional	Ireland	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)
<p>DeepL GmbH</p> <p>Im Mediapark 8a 50670 Cologne Germany</p>	<p><i>Offer of machine translation of notification content</i> (encrypted, for the duration of the translation). Expansion and improvement of core services.</p> <ul style="list-style-type: none"> • User-generated content 	Optional	Germany	–
<p>Mailgun Technologies, Inc.</p> <p>112 E Pecan St #1135 San Antonio, Texas 78205 USA</p>	<p><i>Optional end user email notifications</i></p> <p>Serves as backup for AWS SES. Notification email (outbound) about the operator's response that is sent to the end user whilst the latter is offline as well as operator emails, chat transcripts and operator notifications.</p> <ul style="list-style-type: none"> • E-mail address • Contact name • User-generated content <p><i>Offer of an option for the end user to respond to email notifications.</i> Expansion and improvement of core services.</p> <ul style="list-style-type: none"> • E-mail address 	Optional	EU	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)

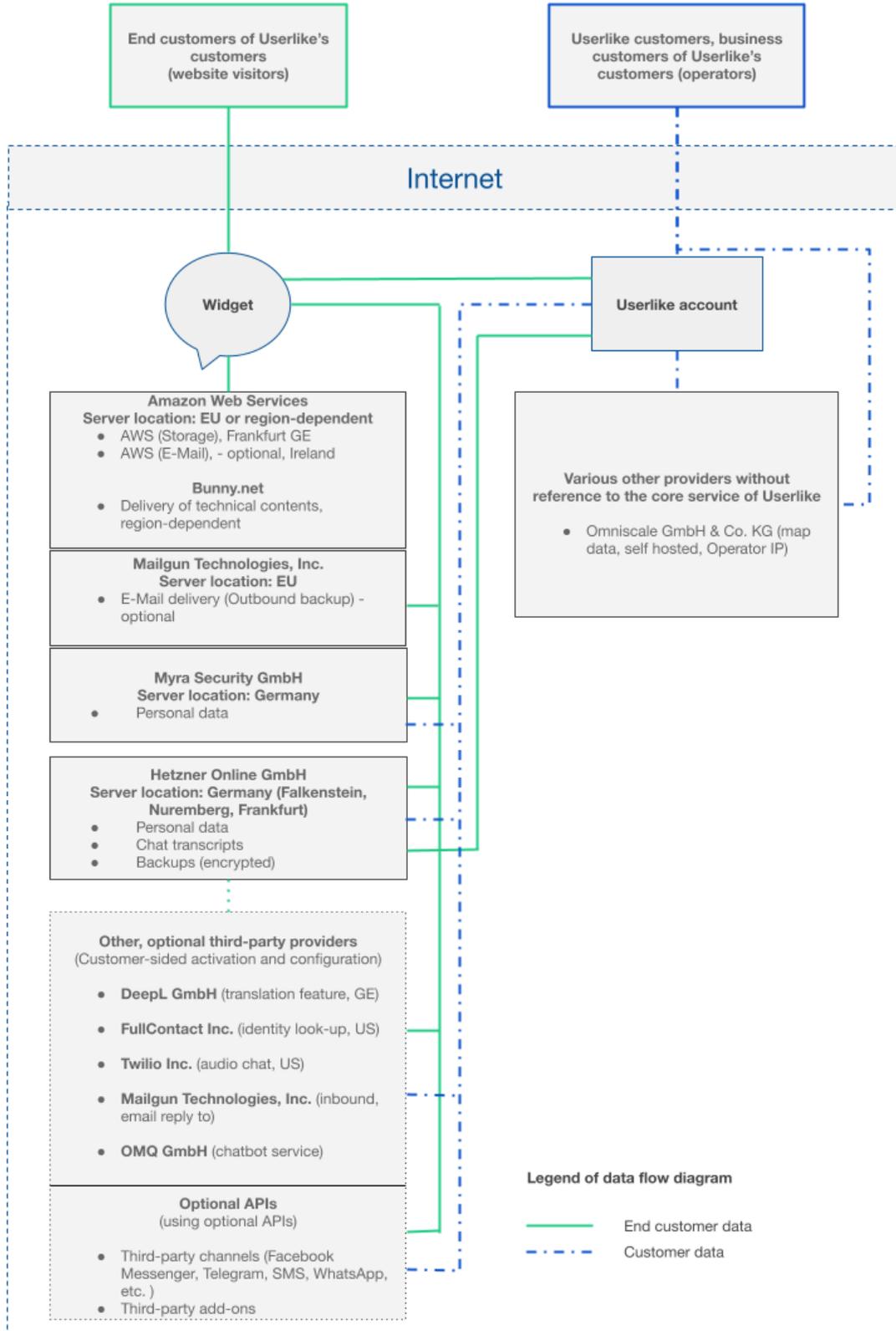
	<ul style="list-style-type: none"> • User-generated content • IP addresses • Browser • Operating system 			
Twilio Inc. 375 Beale Street, Suite 300, San Francisco, California 94105 USA	<i>Audio and video chat.</i> Expansion and improvement of core services. <ul style="list-style-type: none"> • User-generated content • IP address • Browser • Operating system 	Optional	USA	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)
FullContact 1624 Market St Ste 226, PMB 45057, Denver, Colorado 80202 USA	<i>Offer to display public end user profiles</i> based on the email address in the user information. Expansion and improvement of core services. <ul style="list-style-type: none"> • End user email address 	Optional	USA	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)
OMQ GmbH Chausseestraße 22 10115 Berlin Germany	<i>Optional AI software offer.</i> Only offered when access to Chatbot API is available in the package. Option to create an AI-based knowledge base to automate customer service (e.g. via chatbots, or smart FAQ etc.) from the Userlike dashboard: <ul style="list-style-type: none"> • Operator IP address • Operator name • Operator email address 	Optional	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)
	<i>Optional AI software hosting offer:</i> The algorithm removes personal data before it is stored by the AI <ul style="list-style-type: none"> • User-generated content (AI messages and contact responses) is anonymized 	Optional (immanent when using the AI software offer)	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)

Annex 4: Technical and organizational measures in accordance with Art. 32 GDPR

Userlike has implemented the following technical and organizational measures at the time of the conclusion of Agreement:

1. Data flow diagram

The general flow of data is shown on the following chart:



2. Organisational control

Objective: The processor's staff must be obligated to maintain data secrecy and to comply with confidentiality provisions. Commitment to this obligation must be documented in personnel files so that it can be produced as evidence at any time.

Corresponding documents are stored in personnel files.

- There is a text module set out in the standard contract for all employees.
- Employees are informed of their duties again in internal training sessions.

3. Physical access control

Objective: Unauthorized persons must be prevented from gaining (physical) access to data processing systems on which personal data is processed or used. The processor shall install an entry control system for this purpose.

Description of entry control systems in the office (including physical precautions):

- Mechanical locking system on main entrance and office entrances
- Electronic alarm system and unlocking with 24/7 site security
- Cameras

Description of surveillance systems:

- Alarm system with link to site security – Wachschutz Berger, Cologne
- 3 x Ubiquity cameras + external server

4. System access control

Objective: Use of data processing systems by unauthorized persons must be prevented. To this end, access to DP systems must be monitored and logged

(e.g. prevention of system login, unauthorized upload to and intrusion into DP system).

Intrusion of unauthorized persons into the DP systems must be prevented.

Description of the authentication mechanisms implemented (e.g. password complexity, change cycles, SSH keys):

- SSH: personalized public private keys
- Maintenance work: OpenVPN (certificates) S2S communication: VPN
- C2S (Client to Server) communication: TLS 1.3 and TLS 1.2

Description of measures upon temporary inactivity of users (e.g. when an employee leaves their desk):

- Hot Corners are configured in the MacOS X system; this allows users to quickly swipe the cursor to a corner in order to bring up the lock-out screensaver. Otherwise, the monitor locks out after 5 minutes.
- All employees are encouraged to always lock their screens.

Description of technical safeguards for your network environment:

- iptables rules on external interfaces
- Services only listen in on internal networks
- VPN communication for servers
- Weekly nmpa scans
- Weekly OpenVAS scans
- Daily monitoring
- Daily audit of new critical errors
- Anti-DDoS in the data centre with Hetzner online GmbH
- Additional anti-DDoS service with Myra Security GmbH
- OpenVPN tunnel to internal services

5. Data access control

Objective: It must be ensured that persons authorized to use a data processing system are only able to access the data for which they have access authorization

and that personal data cannot be read, copied, modified or erased without authorization during processing or use or after storage.

Personal data must be encrypted in the case of persistent storage.

Needs-oriented design of the authorization concept and access rights, as well as monitoring and logging thereof:

Description of the prevention of unauthorized activity in DP systems outside of granted authorizations (roles and authorizations according to the need-to-know principle):

- Rights and role management
- Technical onboarding and offboarding of employees
- Access rights only as required

Description of measures to prevent unauthorized access (e.g. brute force, SQL injection, login validation):

- SSH: fail2ban
- SQL injections are systematically excluded by using query parameterization for database queries.
- All critical endpoints are protected against brute force attacks with rate limits.
- The usual Django Framework security features (CSRF tokens etc.) are used.
- Access for Userlike employees is protected by a 2-factor authentication.
- Customers can activate further security features such as login validation by email.

Description of mechanisms to ensure that only personalized user accounts are used to access the systems (one account per user):

- 1 account per user
- 1 VPN account per user
- 1 account on a computer

Description of encryption measures implemented for personal data:

- Hard drive encryption with LUKS2 (cipher: aes-xts-plain64, keysize: 512 bits)

- Transport encryption with TLS 1.3 and TLS 1.2
- VPN
- SSH safeguards: GPG

5.1. Transfer control

Objective: It must be ensured that personal data cannot be read, copied, modified or erased without authorization during electronic transfer or during transport or storage on data carriers, and that it is possible to check and identify where transfer of personal data by data transfer systems is expected to take place.

Personal data must be encrypted for transfer (transport encryption).

Description of transport encryption:

- Transport encryption with TLS 1.3 and TLS 1.2
- VPN
- SSH

Description of the logging of personal data transfer:

- Not applicable. Personal data is not downloaded or transferred from servers. Back-ups are the exception. Back-ups are logged and encrypted. Manually checked on a daily basis.
- Hard drives are always encrypted and overwritten before being returned.

Description of transport protection for physical transport:

- Not applicable. Personal data is not physically transported from servers.

5.2. Input control

Objective: It must be ensured that it is possible to check and establish at a later date whether personal data was entered into, modified in or erased from data processing systems, and by whom.

A detailed logging system for the input, modification and erasure of personal data (e.g. log files) must be implemented and assessed on a regular basis.

Description of the logging/monitoring system for monitoring access:

- The customer has an audit log available to them. The audit log is a log listing all changes to the customer's account.
- Various logs are kept on server level; these are compiled upon login of employees during maintenance work. These logs are checked on a random basis.
- In addition, various logs showing the technical status of the system are generated.

5.3. Availability control

Objective: It must be ensured that personal data is protected against accidental loss or destruction.

Description of the data security concept (e.g. back-up procedure, redundancies, UPS, emergency plans):

- 3 data centres (system available in triplicate)
- 2 different sites/data centres
- UPSs and diesel generators
- Mirrored hard drives
- Enterprise hard drives
- Auto failover for web nodes
- Auto failover for statistical data
- Automated monitoring
- Daily back-ups of all data
- Back-ups in 2 different locations
- Several employees managing the process

5.4. Separation rule

Objectives: It must be ensured that personal data collected for different purposes can be processed separately. The processor shall ensure demonstrable logical separation of the client's data, i.e. data from different controllers must be processed separately. Mutual access must be excluded. In addition, data must only be processed for a specific purpose.

Description of implementation for multi-client capability:

- Data is processed for a specific purpose and is separated logically by client on database level (multi-client capability).

Description of mechanisms to ensure the separation of development, testing and productive systems:

Physical separation (different servers) in 3 environments:

- Development
- Staging
- Production

5.5. Information security

Description of the information security management system (ISMS):

Various processes:

- IT security process
 - Input: Scans, messages, logs
 - Processing: Evaluation
 - Output: Measures
 - Tools: nmap, rkhunter, Lynis
- Responsibility:
 - IT Security: security@userlike.com
 - Data Privacy: privacy@userlike.com
- Regular training
 - IT security
 - Data protection
 - Fixed processes
 - Onboarding

- Offboarding
- Rights and role management

5.6. Miscellaneous

Description of mechanisms to ensure confidential storage and erasure or destruction of test and scrap materials containing personal data (e.g. paper):

- Not applicable. No paper used. Excluding bookkeeping and contracts. Documents are shredded.
- Hard disks are always encrypted and overwritten several times before delivery.

6. Use of subcontractors

The technical and organizational measures implemented by the other processors that we use at the point at which this agreement is concluded are available on request. We regularly verify the appropriateness and effectiveness of the measures implemented by our subcontractors.

7. Processor's assurance

The processor guarantees that all information provided in this document is truthful.

Annex 5: Additions to the EU Standard Contractual Clauses

The Parties agree on the following additions and updates to the EU Standard Contractual Clauses (Annex 1):

1. Documentation and compliance (Clause 7.6)

Clause 7.6 of the EU Standard Contractual Clauses is supplemented by the following provisions:

In order to perform audits in accordance with clause 7.6 c) ff., the Controller may enter Userlike's business premises where the Controller data is being processed during ordinary working hours (Monday to Friday from 10.00 am to 6.00 pm), after giving adequate notice in accordance at its own costs, without disrupting daily operations, and under strictest non-disclosure of Userlike's operating and business secrets.

2. Use of sub-processors (Clause 7.7)

Clause 7.7. a) of the EU Standard Contractual Clauses is supplemented by the following provisions:

Userlike shall inform the Controller in electronic format about planned changes regarding the engagement or replacement of additional processors 30 days in advance. In exceptional circumstances, Userlike may give 5 days' notice to the Controller about planned changes, for example, if the involvement or replacement of additional processors appears necessary for acute IT security reasons. In individual cases, the Controller may object to the potential engagement of an additional processor. The Controller may only raise an objection for good cause that shall be proven to Userlike. Failure of the Controller to raise an objection within 14 working days from receipt of the notification shall result in its right to object against the corresponding engagement expiring. If the Controller raises an objection, Userlike may terminate the principal contract and this Agreement at the next possible date after the principal contract.

3. International transfers (Clause 7.8)

Clause 7.8 of the EU Standard Contractual Clauses is supplemented by the following provisions:

Userlike may also process Controller data in compliance with the provisions of this Agreement outside the EEA if Userlike informs the Controller in advance about the place where the data is to be processed and the conditions of Art. 44 to 48 GDPR have been met or there is an exception in accordance with Art. 49 GDPR.

4. Scope of the contract

The EU Standard Contractual Clauses are supplemented by the following provisions:

Userlike reserves the right to anonymise or aggregate the Controller data to make it impossible to identify individual data subjects and to use the data in this form for the purpose of creating a needs-based design, further development and optimisation, and provision of the service agreed in accordance with the principal contract. The Parties agree that anonymised Controller data and/or Controller data that has been aggregated according to the specifications above is no longer classed as Controller data within the meaning of this Agreement. Userlike will inform the client in text form about the detailed technical aspects prior to the first anonymization.