Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

Sergej Prokopkin

Kaiserin-Augusta-Allee 97D

Berlin

10553

Deutschland

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter:

fairkom Gesellschaft
Badgasse 3
6850 Dornbirn
Österreich

(im Folgenden Auftragnehmerin)

GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

- ***Bereitstellung der fairapps Anwendungen***
  - ***faircloud***
  - ***fairchat***
  - ***board.net***
  - ***fairlogin***
  - ***GitLab+***
  - ***fairsuch***
  - ***fairteaching***
-
- ***Backup der Daten, Systemadministration, Hosting***

(1) Folgende Datenkategorien werden verarbeitet:

Persönliche Daten der Mitarbeiter:innen und Kunden, wie IP-Adressen, Namen, Kontaktdaten, Kommunikationsinhalte und Nutzerdaten für die fairapps basic – Anwendungen, so wie sie vom Kunden hochgeladen werden.

(2) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

Personen, die Zugriff auf die fairapps basic - Anwendungen haben, also Beschäftigte, Kunden, Interessenten, Lieferanten, usw.

DAUER DER VEREINBARUNG

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem Monat gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Die Vereinbarung endet jedoch auf jeden Fall mit der Beendigung der Kundenbeziehung, also etwa bei der Kündigung von Dienstleistungspaketen zu den gegenständlichen Anwendungen oder bei Angeboten, die kein Paket erfordern, wenn diese länger als sechs Monate nicht mehr genutzt werden.

PFLICHTEN DER AUFTRAGNEHMERIN

(1) Die Auftragnehmerin verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält die Auftragnehmerin einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat sie - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke der Auftragnehmerin eines schriftlichen Auftrages.

(1) Die Auftragnehmerin erklärt rechtsverbindlich, dass sie alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(2) Die Auftragnehmerin erklärt rechtsverbindlich, dass sie alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(3) Die Auftragnehmerin ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an die Auftragnehmerin gerichtet und lässt diese erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat die Auftragnehmerin den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(4) Die Auftragnehmerin unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(5) Die Auftragnehmerin wird darauf hingewiesen, dass sie für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(6) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die

zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(7) Die Auftragnehmerin darf nach Beendigung dieser Vereinbarung oder bei Beendigung der Kundenbeziehung aus allen genutzten Anwendungen, die Daten enthalten, diese vernichten. Vorher muss die Auftraggeberin dafür Sorge tragen, die Daten auf eigenen Medien abzuspeichern. Die Auftragnehmerin wird dabei auf Anfrage Unterstützung leisten.

(8) Die Auftragnehmerin hat den Auftraggeber unverzüglich zu informieren, falls sie der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist befugt, folgende Unternehmen als Sub-Auftragsverarbeiter hinzuzuziehen:

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland (Hosting)
- internex GmbH, Lagerstraße 15, 3950 Gmünd, Österreich (Hosting)
- Johannes Büchele, (App Programmierung), Jägerstrasse 58/2/7, 1200 Wien
- Armin Felder, Trientlstrasse 24, 6060 Hall in Tirol (Betrtiebsunterstützung)

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters/der Sub-Auftragsverarbeiterin sind dem Auftraggeber rechtzeitig schriftlich bekannt zu geben, dass sie dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem/der Sub-Auftragsverarbeiter/in ab.

Dornbirn, am 18.02.2026

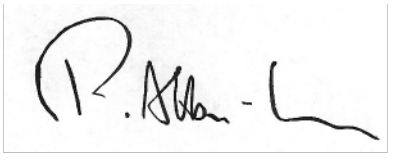
Für den Auftraggeber:

Sergej Prokopkin

.....

Dornbirn, am 18.02.2026

Für den Auftragnehmer:



.....

Roland Alton, Vorstand

Anlage ./1 – TOM (Technisch-Organisatorische Massnahmen) bei der fairkom Gesellschaft

Version 2026-02-11

Vertraulichkeit

Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen wird gewährleistet durch Schlüssel und RFID-Chips sowie elektrische Türöffner. Zutrittsmedien werden nicht an Dritte weitergegeben. Türen zum Büro oder Serverräumen werden stets geschlossen gehalten.

Zugangskontrolle

Schutz vor unbefugter Systembenutzung wird gewährleistet durch starke Passwörter, welches aus mindestens 12 Zeichen bestehen muss mit einer Mischung aus Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen oder alternativ eine Wortkombination die eine Entropie von mehr als 120 hat. Arbeitsrelevante Passwörter dürfen ausschließlich im vorgegebenen Passwortmanager gespeichert werden. Zusätzlich ist die Nutzung der Zwei-Faktor-Authentifizierung für alle kritischen Systemzugänge verpflichtend. Passwörter dürfen nicht weiter gegeben werden.

Auf Arbeitsgeräten ist der Datenbereich standardmäßig kryptografisch verschlüsselt. Wenn Mitarbeitende eigene Geräte nutzen, müssen auch deren Speichermedien entsprechend verschlüsselt werden. Es dürfen keine personenbezogenen Daten auf Datenträger (USB Sticks etc) unverschlüsselt abgelegt werden.

Bildschirme müssen immer gesperrt werden, wenn der Arbeitsplatz verlassen wird. Jeder Mitarbeitende ist verpflichtet, einen eigenen Sperrmechanismus einzurichten.

Der Zugriff auf Server erfolgt ausschließlich über SSH-Verbindungen mit asymmetrischer Verschlüsselung, wobei der Schlüssel zusätzlich durch ein Passwort geschützt sein muss.

Zugriffskontrolle

Es dürfen nur Daten eingesehen oder bearbeitet werden, die für den jeweiligen Arbeitsvorgang erforderlich sind. Änderungen an Berechtigungen werden nach dem „need to know-Prinzip“ durchgeführt.

Es gibt Standardprozesse bei Neuzugang/Wechsel/Ausscheiden von Mitarbeitern und Überprüfungen der vergebenen Berechtigungen bei administrativen Benutzerkonten werden periodisch durchgeführt.

Sicherheitsrelevante Unterlagen müssen nach der Nutzung verschlossen aufbewahrt werden.

Falls eine Simulation eines Nutzerkontos erforderlich ist, wird der Vorgang mit einem Zeitstempel protokolliert.

Klassifikationsschema für Daten

Die Klassifikation erfolgt aufgrund gesetzlicher Verpflichtungen oder einer Selbsteinschätzung in geheim/vertraulich/intern/öffentlich. Geheime oder vertrauliche Daten dürfen nicht unverschlüsselt oder sonst wie einsehbar versendet werden – geteilte Links sollten zusätzlich mit einem Passwort versehen werden.

Bei Kundenkommunikation gilt Vertraulichkeit, sofern diese nicht über Foren oder öffentliche Chatkanäle stattfindet. Im gitlab sind vertrauliche Nachrichten oder Issues als solche zu markieren.

Integrität

Weitergabekontrolle

Um die Integrität von Daten bestmöglich zu gewährleisten setzen wir unter anderem auf

- Transportverschlüsselung
- Generieren von Teilen - Links statt Attachments
- Beschränkung der Gültigkeit geteilter externer Links standardmäßig auf ein halbes Jahr
- Ende-zu-Ende Verschlüsselung bei Messenger-Nachrichten

Eingabekontrolle

Mitarbeitende dürfen personenbezogene Daten nur über ihren eigenen Benutzeraccount oder einen dedizierten Administrationszugang bearbeiten.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Datenverlust werden von den wichtigsten Diensten Backups auch offsite durchgeführt. Im Rechenzentrum ist eine unterbrechungsfreie Stromversorgung (USV) verfügbar.

Monitoring

Die Kapazität und Verfügbarkeit der Dienste wird überwacht.
Logins werden protokolliert und üblicherweise ein Monat aufbewahrt.

Löschungsfristen

Logfiles werden in der Regel nicht länger als drei Monate für allfällige technische Auswertungen aufbewahrt.

Wenn ein Mitarbeiter das Unternehmen verlässt, muss dieser alle Daten auf den eigenen Geräten, die in Bezug mit Kunden der fairkom Gesellschaft stehen, sofern diese nicht öffentlich sind, löschen.

Datenträger, die unverschlüsselten Daten enthalten, werden mehrfach überschrieben oder geshreddert, wenn sie das Unternehmen verlassen.

Datenschutz Management

Vertraulichkeit

Mitarbeiter erhalten mindestens einmal jährlich eine entsprechende Sensibilisierung in einer Datenschutzschulung.

Im Home-Office gelten die selben Anforderungen bezüglich Datenschutz.

Datensparsamkeit

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Incident-Response-Management

Dokumentation

Bei einem Ausfall wichtiger Systeme erfolgt eine Eskalation über das Betriebsteam. Sicherheitsvorfälle oder Datenpannen werden im Ticketsystem als Incident erfasst.