Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO zum Dienst **sharePAD**

Zwischen den Parteien

Verantwortlicher (nachfolgend „Kundenorganisation“) – vom Kunden auszufüllen:

Name der Organisation:

Anschrift:

Vertreten durch:

E-Mail:

Registernummer (falls vorhanden):

und

Auftragsverarbeiter (nachfolgend „sharePAD-Betreiber“):

Robert Hölzl Cloud Platforms
Traunsteinerstr. 44
83093 Bad Endorf
Deutschland
E-Mail: robert.hoelzl@sharepad.de

wird der folgende Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (nachfolgend „Vertrag“ oder „AVV“) geschlossen. Er konkretisiert die Pflichten der Parteien zum Datenschutz, die sich aus dem zwischen ihnen bestehenden Hauptvertrag über die Nutzung des Dienstes sharePAD (nachfolgend „Hauptvertrag“) ergeben.

§ 1 Gegenstand, Art und Zweck der Verarbeitung

(1) Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten durch den sharePAD-Betreiber für die Kundenorganisation im Rahmen der Bereitstellung des Internetdienstes sharePAD (abrufbar unter app.sharepad.de bzw. beta.sharepad.de).

(2) sharePAD ermöglicht Organisationen, gemeinschaftlich genutzte Ressourcen (z. B. Fahrzeuge) unter ihren Mitgliedern zu verwalten und zu reservieren. Die Verarbeitung umfasst insbesondere das Anlegen, Bearbeiten und Löschen von Mitgliedsdaten und Reservierungen, die Authentifizierung der Nutzer, den Versand transaktionaler E-Mails, die Abrechnung sowie unterstützende Funktionen wie Geocoding und Bildverarbeitung.

(3) Art der Verarbeitung: Erheben, Erfassen, Speichern, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleichen, Einschränken, Löschen und Vernichten personenbezogener Daten mittels automatisierter Verfahren.

(4) Zweck der Verarbeitung ist ausschließlich die vertragsgemäße Erbringung der Leistungen nach dem Hauptvertrag. Eine Verarbeitung zu eigenen Zwecken des sharePAD-Betreibers findet – außerhalb der gesetzlich erlaubten Ausnahmen – nicht statt.

§ 2 Dauer des Auftrags

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er endet automatisch mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten aus § 10 (Löschung und Rückgabe) sowie aus datenschutz- und handelsrechtlichen Aufbewahrungsvorschriften bleiben hiervon unberührt.

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Kategorien betroffener Personen

Mitglieder der Kundenorganisation (einschließlich Mitgliedern mit administrativen Rollen sowie Supervisor-Rollen), gegebenenfalls Mitglieder von Partner-Organisationen, an die einzelne Ressourcen freigegeben wurden.

(2) Kategorien personenbezogener Daten

• **Stammdaten:** Vor- und Nachname, E-Mail-Adresse, Telefonnummer, Postanschrift, Mitgliedsnummer, Rolle innerhalb der Organisation, Datum einer Beendigung der Mitgliedschaft.

• **Authentifizierungsdaten:** Passwort-Hashes (bcrypt), Sitzungs-Token (JWT) im Browser des Mitglieds, ggf. API-Schlüssel (SHA-256-Hash).

• **Reservierungsdaten:** Reservierungen mit Zeitraum, Kommentar und Bezug zum reservierenden Mitglied sowie vollständige Änderungshistorie (Audit-Log).

• **Technische Daten:** Server-Logs (IP-Adresse, Zeitstempel, aufgerufener Pfad, HTTP-Statuscode) sowie Fehler- und Performance-Ereignisse ohne personenbezogene Zusatzinformationen.

• **Organisationsdaten:** Name, Anschrift, Geokoordinaten, Logo sowie Vertrags- und Abrechnungsstatus der Kundenorganisation.

§ 4 Pflichten des sharePAD-Betreibers

(1) Der sharePAD-Betreiber verarbeitet personenbezogene Daten ausschließlich im Rahmen des Hauptvertrags, dieses AVV und auf dokumentierte Weisung der Kundenorganisation. Dies gilt auch für die Übermittlung in Drittländer. Ist er durch das Recht der Union oder eines Mitgliedstaats zu einer weitergehenden Verarbeitung verpflichtet, teilt er der Kundenorganisation diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der sharePAD-Betreiber gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Er trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOMs), die in Anlage 2 beschrieben sind. Eine Anpassung der TOMs an den Stand der Technik bleibt dem sharePAD-Betreiber vorbehalten, soweit das Schutzniveau nicht unterschritten wird.

(4) Er unterstützt die Kundenorganisation im Rahmen des technisch Möglichen und Zumutbaren bei der Beantwortung von Anträgen betroffener Personen (Art. 12–23 DSGVO), bei der Sicherstellung der Datensicherheit (Art. 32 DSGVO), bei der Meldung von Datenschutzverletzungen (Art. 33, 34 DSGVO) sowie bei Datenschutz-Folgenabschätzungen (Art. 35, 36 DSGVO).

(5) Er meldet der Kundenorganisation Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntnisnahme, per E-Mail an die in der Präambel angegebene Adresse. Die Meldung enthält die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit sie verfügbar sind.

(6) Er stellt der Kundenorganisation auf Anforderung die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlichen Informationen zur Verfügung.

(7) Er informiert die Kundenorganisation unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.

§ 5 Weisungsrecht der Kundenorganisation

(1) Die Kundenorganisation ist im Rahmen dieses Vertrags allein für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Betroffenenrechte verantwortlich.

(2) Weisungen erfolgen grundsätzlich in Textform (E-Mail genügt). Regelmäßige Bedienhandlungen innerhalb der Benutzeroberfläche von sharePAD (z. B. Anlegen, Ändern oder Löschen von Mitgliedern, Ressourcen und Reservierungen) gelten als vereinbarungsgemäße Einzelweisungen.

(3) Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

§ 6 Sub-Auftragsverarbeiter

(1) Die Kundenorganisation erteilt dem sharePAD-Betreiber die allgemeine schriftliche Genehmigung zum Einsatz der in **Anlage 1** benannten Sub-Auftragsverarbeiter.

(2) Der sharePAD-Betreiber ist berechtigt, weitere Sub-Auftragsverarbeiter hinzuzuziehen oder bestehende zu ersetzen. Er informiert die Kundenorganisation hierüber mindestens 14 Tage im Voraus in Textform unter Angabe von Name, Anschrift, Sitzland und Zweck der Beauftragung. Die Information erfolgt an die oben angegebene E-Mail-Adresse der Kundenorganisation oder durch Hinweis in der Administrationsoberfläche von sharePAD.

(3) Die Kundenorganisation kann einer Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb der Ankündigungsfrist in Textform widersprechen. Kommt keine Einigung zustande, sind beide Parteien berechtigt, den Hauptvertrag mit einer Frist von einem Monat zum Monatsende zu kündigen.

(4) Der sharePAD-Betreiber verpflichtet seine Sub-Auftragsverarbeiter vertraglich zu datenschutzrechtlichen Pflichten, die denen dieses Vertrags entsprechen, insbesondere zur Einhaltung hinreichender TOMs.

§ 7 Drittlandtransfers

Eine Übermittlung personenbezogener Daten in ein Drittland außerhalb der EU/des EWR findet nur statt, soweit die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (insbesondere Angemessenheitsbeschluss oder Standardvertragsklauseln). Aktuell betrifft dies die Übermittlung von Adressdaten und Geokoordinaten an Mapbox, Inc. (USA); Grundlage ist der Angemessenheitsbeschluss zum EU-US Data Privacy Framework bzw. ergänzend Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO). Weitere Einzelheiten sind in Anlage 1 aufgeführt.

§ 8 Kontroll- und Nachweisrechte

(1) Der sharePAD-Betreiber weist die Einhaltung der in diesem Vertrag niedergelegten Pflichten in geeigneter Weise nach, insbesondere durch aktuelle Dokumentation der TOMs, Selbstauskünfte oder – soweit vorhanden – Zertifikate, Testate oder Berichte unabhängiger Prüfstellen.

(2) Die Kundenorganisation ist berechtigt, nach vorheriger Anmeldung mit angemessener Vorlaufzeit (mindestens 30 Tage) während der üblichen Geschäftszeiten ohne Störung des Betriebsablaufs Kontrollen durchzuführen oder durch einen benannten Prüfer durchführen zu lassen. Der Prüfer darf kein Wettbewerber des sharePAD-Betreibers sein und ist zur Vertraulichkeit verpflichtet.

(3) Der sharePAD-Betreiber kann für den Mehraufwand einer solchen Prüfung ein angemessenes Entgelt nach seinem jeweils gültigen Stundensatz verlangen, sofern die Prüfung nicht aus einem konkreten Anlass (z. B. nach einer Datenpanne) erfolgt.

§ 9 Haftung

Für die Haftung der Parteien gelten Art. 82 DSGVO sowie die Regelungen des Hauptvertrags. Eine Haftungsbegrenzung im Hauptvertrag gilt auch für Ansprüche aus diesem AVV, soweit zwingendes Recht nicht entgegensteht.

§ 10 Löschung und Rückgabe nach Beendigung

(1) Nach Beendigung des Hauptvertrags hat der sharePAD-Betreiber nach Wahl der Kundenorganisation alle personenbezogenen Daten zu löschen oder an die Kundenorganisation in einem strukturierten, gängigen und maschinenlesbaren Format zurückzugeben, sofern nicht eine gesetzliche Pflicht zur Speicherung besteht.

(2) Bestehende gesetzliche Aufbewahrungspflichten (insbesondere handels- und steuerrechtliche Fristen nach § 147 AO und § 257 HGB) bleiben hiervon unberührt.

(3) Reservierungsdaten, die gemäß der Datenschutzerklärung nach Ablauf definierter Fristen anonymisiert werden, verbleiben in anonymisierter Form zu statistischen Zwecken beim sharePAD-Betreiber, soweit kein Personenbezug mehr besteht.

§ 11 Schlussbestimmungen

(1) Im Konfliktfall zwischen den Regelungen dieses AVV und des Hauptvertrags gehen die Regelungen dieses AVV vor. Im Konfliktfall zwischen diesem AVV und den jeweils aktuell geltenden datenschutzrechtlichen Vorschriften geht letzteres vor.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform.

(3) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.

(4) Ausschließlicher Gerichtsstand ist Rosenheim, soweit die Kundenorganisation Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

(5) Sollte eine Bestimmung dieses Vertrags unwirksam sein, wird davon die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Unterschriften

Ort, Datum:	Ort, Datum:
Unterschrift / Stempel	*Unterschrift / Stempel*
Für die Kundenorganisation (Verantwortlicher)	**Für den sharePAD-Betreiber (Auftragsverarbeiter)**

Anlage 1 – Sub-Auftragsverarbeiter

Stand bei Vertragsschluss. Der sharePAD-Betreiber informiert die Kundenorganisation über Änderungen gemäß § 6 Abs. 2.

Dienstleister	Zweck	Sitz / Region	Verarbeitete Daten
Fly.io, Inc.	Hosting der Anwendung, Runtime-Logs	Rechenzentrum Frankfurt a. M.	Sämtliche Anfragen (transient), Server-Logs
Neon, Inc.	Persistente PostgreSQL-Datenbank	Frankfurt a. M. (AWS eu-central-1)	Sämtliche in § 3 genannten Daten
Functional Software, Inc. (Sentry)	Fehler- und Performance-Monitoring	EU-Region (de.sentry.io)	Fehlermeldungen, Stacktraces, Umgebungsinformationen – ohne IP und Request-Header
Mapbox, Inc.	Geocoding, Entfernungsberechnung, Kartenkacheln	USA (Drittland, SCC / DPF)	Adressen und Geokoordinaten von Organisationen und Ressourcen
Kaleido AI GmbH (remove.bg)	Automatische Hintergrundentfernung bei Bild-Uploads	Wien, Österreich	Hochgeladene Bilddateien (Logos, Ressourcenbilder)
Strato AG	SMTP-Versand transaktionaler E-Mails	Deutschland	E-Mail-Adresse, Name, Einladungs- / Reset-Links
Haufe-Lexware GmbH & Co. KG	Rechnungsstellung für den sharePAD-Dienst	Freiburg, Deutschland	Kontaktdaten der Kundenorganisation und ihrer Administratoren

Drittlandtransfer: Die Übermittlung an Mapbox, Inc. (USA) erfolgt auf Grundlage des EU-US Data Privacy Framework (Art. 45 DSGVO) bzw. ergänzend auf Basis der Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO). Alle übrigen Dienstleister verarbeiten Daten innerhalb der EU bzw. des EWR.

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)

Der sharePAD-Betreiber setzt die folgenden Maßnahmen nach Art. 32 DSGVO um, um die Sicherheit der Verarbeitung zu gewährleisten. Die Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Ausschließlich verschlüsselte Übertragung aller Anfragen per TLS (HTTPS).

• Speicherung von Passwörtern ausschließlich als bcrypt-Hash; das Klartext-Passwort ist dem sharePAD-Betreiber nicht bekannt.

• Speicherung von API-Schlüsseln angebundener Fremdanwendungen ausschließlich als SHA-256-Hash.

• Rollen- und organisationsbezogene Zugriffskontrolle (Mandantentrennung): Mitglieder sehen nur Daten ihrer eigenen Organisation bzw. – bei Partner-Freigabe – nur die ausdrücklich freigegebenen Ressourcen.

• Zeitlich begrenzte Sitzungen: 90 Tage für reguläre Mitglieder, 4 Stunden für administrative Sitzungen.

• Getrennte administrative Konten zur Minimierung von Zugriffsrechten.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

• Vollständige Änderungshistorie (Audit-Log) auf Reservierungen: Wer hat wann welche Änderung vorgenommen.

• Eingabevalidierung und serverseitige Rechteprüfung bei allen schreibenden Operationen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

• Hosting der Anwendung und persistente Speicherung ausschließlich in Frankfurt a. M.

• Tägliche automatisierte Datensicherungen der Datenbank.

• Monitoring der Verfügbarkeit und Performance; Fehler- und Performance-Ereignisse werden an Sentry (EU-Region) übermittelt, ohne personenbezogene Zusatzinformationen (IP-Adresse und Request-Header sind in der Integration deaktiviert).

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

• Regelmäßige Aktualisierung der eingesetzten Software-Komponenten und Abhängigkeiten.

• Überprüfung der Wirksamkeit der TOMs mindestens einmal jährlich sowie anlassbezogen.

5. Auftragskontrolle

• Schriftliche Weisungen und Auftragsverarbeitungsverträge mit allen eingesetzten Sub-Auftragsverarbeitern gemäß Art. 28 DSGVO.

• Dokumentation der Sub-Auftragsverarbeiter in Anlage 1; Information der Kundenorganisation bei Änderungen gemäß § 6 Abs. 2.

6. Datenminimierung und Speicherbegrenzung

• Stammdaten eines Mitglieds werden ein Jahr nach Beendigung der Mitgliedschaft gelöscht.

• Reservierungen werden ein Jahr nach der letzten Abrechnung anonymisiert.

• Server-Logs werden beim Hoster nach 30 Tagen automatisch gelöscht.

• Ereignisdaten in Sentry werden gemäß Standard-Aufbewahrung (derzeit ca. 90 Tage) automatisch gelöscht.