Auftragsverarbeitungsvereinbarung (AVV) für Screenway

> Diese Fassung ist verbindlich und kann durch elektronische Akzeptanz im Customer-Portal wirksam abgeschlossen werden (siehe Abschnitt „Wirksamkeit").

Präambel

Bergx2 GmbH betreibt die Software-as-a-Service-Plattform Screenway zur Digital-Signage-Steuerung. Im Rahmen der Service-Nutzung verarbeitet Bergx2 GmbH personenbezogene Daten im Auftrag des Kunden im Sinne der Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO). Diese Vereinbarung konkretisiert die Pflichten und Rechte beider Parteien nach Art. 28 Abs. 3 DSGVO.

---

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand. Bergx2 GmbH stellt dem Kunden die Screenway-Plattform als Software-as-a-Service zur Verfügung. Im Rahmen der Nutzung verarbeitet Bergx2 GmbH die in Anhang 1 näher beschriebenen personenbezogenen Daten des Kunden ausschließlich nach dessen Weisungen.

(2) Dauer. Die Vereinbarung tritt mit Vertragsschluss des zugrundeliegenden Hauptvertrags (Screenway-Service-Vertrag) in Kraft und endet mit dessen Beendigung. Die Pflichten zu Löschung/Rückgabe (§ 10) und zur Vertraulichkeit (§ 5 Abs. 2) gelten über die Vertragsdauer hinaus fort.

---

§ 2 Art und Zweck der Verarbeitung

(1) Bergx2 GmbH verarbeitet die in Anhang 1 beschriebenen personenbezogenen Daten zu folgenden Zwecken:

- Bereitstellung der Screenway-Plattform als Digital-Signage-SaaS
- Zuordnung von Bildschirm-Standorten zu Kunden-Accounts
- Anzeige der vom Kunden hochgeladenen Inhalte auf den Endgeräten
- Authentifizierung der Kunden-Mitarbeiter beim Login
- Bereitstellung von Support, Fehleranalyse und Service-Monitoring

(2) Eine Verarbeitung zu eigenen Zwecken Bergx2 GmbHs (z. B. Marketing, Profiling, Verkauf an Dritte) findet nicht statt.

---

§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen

Konkrete Aufzählung siehe Anhang 1. Zusammenfassend:

- Art der Daten: Account-Daten, Login-Daten, Bildschirm-Standortdaten, durch den Kunden hochgeladene Inhalte (i. d. R. nicht-personenbezogen)
- Kategorien betroffener Personen: Mitarbeiter der Kunden (für Login und Account-Zuordnung)

Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO findet im Screenway-Standardbetrieb nicht statt. Falls der Kunde solche Daten dennoch hochlädt, geschieht dies außerhalb der von dieser AVV adressierten Kategorien und auf eigene Verantwortung des Kunden.

---

§ 4 Pflichten und Rechte des Verantwortlichen (Kunden)

(1) Weisungsrecht. Der Kunde bleibt für die Rechtmäßigkeit der Verarbeitung verantwortlich (Art. 24 DSGVO). Bergx2 GmbH verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Kunden. Diese AVV gilt als allgemeine Weisung, individuelle Weisungen sind über die im Service-Vertrag definierten Kommunikationskanäle möglich.

(2) Aufzeichnung. Bergx2 GmbH dokumentiert weisungsrelevante Vorgänge in der internen Audit-Spur des ISMS (Pull-Request-Historie, Incident- Register, Lieferantenregister).

(3) Informationspflichten. Der Kunde ist verpflichtet, die betroffenen Personen (seine Mitarbeiter) gemäß Art. 13 DSGVO über die Datenverarbeitung durch Bergx2 GmbH zu informieren.

---

§ 5 Pflichten des Auftragsverarbeiters (Bergx2 GmbH)

(1) Weisungsgebundenheit. Bergx2 GmbH verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Kunden. Bei einer aus Sicht von Bergx2 GmbH rechtswidrigen Weisung wird Bergx2 GmbH den Kunden unverzüglich informieren (Art. 28 Abs. 3 lit. h DSGVO).

(2) Vertraulichkeit. Bergx2 GmbH verpflichtet alle mit der Verarbeitung befassten Personen vor Aufnahme der Tätigkeit auf Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO). Dies erfolgt durch Vertraulichkeitserklärungen (NDA) bei Einstellung bzw. Beauftragung und ist im Bergx2-ISMS (Mitarbeiterregister) dokumentiert.

(3) Technische und organisatorische Maßnahmen. Bergx2 GmbH ergreift die in Anhang 2 beschriebenen TOMs, die dem Stand der Technik entsprechen und ein dem Risiko angemessenes Schutzniveau gewährleisten (Art. 32 DSGVO).

(4) Sub-Auftragsverarbeiter. Bergx2 GmbH setzt die in Anhang 3 gelisteten Sub-Auftragsverarbeiter ein. Bedingungen und Änderungs- Mechanismus siehe § 6.

(5) Unterstützung. Bergx2 GmbH unterstützt den Kunden bei der Erfüllung seiner Pflichten nach Art. 32–36 DSGVO, insbesondere bei der Beantwortung von Betroffenenanfragen (§ 7) und der Meldung von Datenschutzverletzungen (§ 8).

(6) Nachweise. Bergx2 GmbH stellt dem Kunden auf Anfrage die zur Prüfung erforderlichen Informationen und Unterlagen zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO). Weitere Audit-Modalitäten siehe § 9.

---

§ 6 Sub-Auftragsverarbeiter

(1) Genehmigung. Mit Abschluss dieser AVV genehmigt der Kunde allgemein die Beauftragung der in Anhang 3 aufgeführten Sub- Auftragsverarbeiter (Art. 28 Abs. 2 Satz 1 DSGVO).

(2) Änderungsbenachrichtigung. Bergx2 GmbH informiert den Kunden über beabsichtigte Änderungen am Sub-Auftragsverarbeiter-Bestand (Hinzunahme oder Austausch) mindestens 30 Tage vor Wirksamwerden in Textform (E-Mail an die im Service-Vertrag hinterlegte Datenschutz-Kontaktadresse).

(3) Widerspruchsrecht. Der Kunde kann der Änderung innerhalb der 30-Tage-Frist aus berechtigten Gründen widersprechen. Bei Widerspruch sucht Bergx2 GmbH mit dem Kunden eine einvernehmliche Lösung; gelingt das nicht, hat der Kunde ein außerordentliches Kündigungsrecht des Service- Vertrags.

(4) Verpflichtung. Bergx2 GmbH verpflichtet jeden Sub-Auftragsverarbeiter seinerseits vertraglich auf die in dieser AVV vereinbarten Pflichten (Art. 28 Abs. 4 DSGVO).

---

§ 7 Mitwirkung bei Betroffenenrechten

Bergx2 GmbH unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen, soweit möglich, bei der Erfüllung der Rechte betroffener Personen aus Kapitel III der DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).

Konkret: Bergx2 GmbH leitet entsprechende Anfragen, die Betroffene direkt an Bergx2 GmbH richten, unverzüglich an den Kunden weiter und gibt diesem die Möglichkeit zur Antwort. Eine eigene Beantwortung durch Bergx2 GmbH erfolgt nur auf ausdrückliche Weisung des Kunden.

---

§ 8 Meldung von Datenschutzverletzungen

(1) Bergx2 GmbH informiert den Kunden unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnisnahme, über jede festgestellte Datenschutzverletzung im Verantwortungsbereich von Bergx2 GmbH oder eines Sub-Auftragsverarbeiters, die personenbezogene Daten des Kunden betrifft.

(2) Die Meldung erfolgt schriftlich (E-Mail an die Kunden-Datenschutz- Kontaktadresse) und enthält die in Art. 33 Abs. 3 DSGVO genannten Mindestangaben (Art und Umfang der Verletzung, Anzahl Betroffener, voraussichtliche Folgen, ergriffene Gegenmaßnahmen).

(3) Bergx2 GmbH dokumentiert eigene Datenschutzverletzungen intern im Incident-Register (siehe `incidents/incidents.md` des Bergx2-ISMS, Verfahren gemäß `documents/verfahren/incident-management-verfahren.md`).

(4) Die Pflicht zur Meldung an die zuständige Aufsichtsbehörde nach Art. 33 DSGVO und ggf. an die betroffenen Personen nach Art. 34 DSGVO verbleibt beim Kunden als Verantwortlichem. Bergx2 GmbH unterstützt den Kunden bei diesen Meldungen mit allen notwendigen Informationen.

---

§ 9 Audit- und Kontrollrechte

(1) Nachweis. Bergx2 GmbH stellt dem Kunden auf Anfrage die zur Erfüllung der Pflichten aus dieser AVV erforderlichen Informationen zur Verfügung, insbesondere die jeweils aktuelle Fassung der TOMs (Anhang 2) und der Sub-Auftragsverarbeiter-Liste (Anhang 3) sowie ggf. Auszüge aus Zertifizierungen.

(2) Vor-Ort-Kontrolle. Der Kunde hat das Recht, sich von der Einhaltung der TOMs vor Ort am Geschäftssitz von Bergx2 GmbH oder an den Standorten der Verarbeitung zu überzeugen. Termine sind mindestens vier Wochen vorher schriftlich anzukündigen; Kontrollen sind auf das notwendige Maß zu beschränken und dürfen den Geschäftsbetrieb nicht unverhältnismäßig stören. Maximal eine Kontrolle pro Kalenderjahr, außer bei begründetem Anlass.

(3) Anerkennung von Zertifizierungen. Soweit Bergx2 GmbH nach ISO/IEC 27001:2022 zertifiziert ist (Zertifizierung in Vorbereitung) oder gleichwertige unabhängige Drittprüfungen vorlegt, ersetzt dies die Vor-Ort-Kontrolle des Kunden, sofern der Geltungsbereich der Zertifizierung den Vertragsgegenstand mit umfasst.

---

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Bei Beendigung des Service-Vertrags wird Bergx2 GmbH – nach Wahl des Kunden – die personenbezogenen Daten entweder:

- vollständig zurückgeben (Export in einem strukturierten, gängigen, maschinenlesbaren Format), oder
- vollständig löschen (sicheres Überschreiben gemäß Stand der Technik), und

binnen 30 Tagen nach Vertragsende.

(2) Backups, die personenbezogene Daten enthalten, werden gemäß Anhang 2 TOMs § Backup-Lebenszyklus rotationsbedingt nach spätestens fünf Wochen vollständig überschrieben (Backup-Rotation). Bergx2 GmbH dokumentiert die finale Löschung schriftlich auf Anfrage.

(3) Gesetzliche Aufbewahrungspflichten bleiben unberührt (z. B. Abrechnungsdaten gemäß § 257 HGB, § 147 AO).

---

§ 11 Haftung und Schlussbestimmungen

(1) Haftung. Es gelten die Regelungen des Hauptvertrags (Screenway-Service-Vertrag) und Art. 82 DSGVO. Bei Verstoß gegen diese AVV haftet die jeweils verantwortliche Partei gegenüber dem Betroffenen.

(2) Schriftform. Änderungen und Ergänzungen bedürfen der Textform.

(3) Salvatorische Klausel. Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt.

(4) Anwendbares Recht und Gerichtsstand. Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts. Gerichtsstand ist München.

Anhang 1: Beschreibung der Verarbeitung

Kategorie	Inhalt
Gegenstand	Bereitstellung der Screenway-SaaS-Plattform inkl. Hosting, Datenübertragung, Authentifizierung und Anzeigesteuerung
Dauer	Aktive Vertragslaufzeit + 30 Tage Übergangsfrist für Export/Löschung
Art der Verarbeitung	Erheben, Erfassen, Speichern, Verändern, Abfragen, Anzeigen, Übertragen, Löschen
Zweck	Erbringung der vertraglich vereinbarten Screenway-Dienstleistung
Betroffene Personen	Mitarbeiter des Kunden, denen Login-/Steuerungszugriffe auf Screenway eingeräumt werden
Datenkategorien	Account-Daten (Name, dienstliche E-Mail, Rolle), Login-Daten (Passwort-Hash, Session-Cookies, IP-Adresse), Bildschirm-Standortdaten (Bezeichnung, ggf. Anschrift des Standorts), durch den Kunden hochgeladene Inhalte (in der Regel **nicht** personenbezogen – Marketing-Material, Hinweistexte etc.)
Besondere Datenkategorien (Art. 9 DSGVO)	Im Standardbetrieb **nicht** verarbeitet
Hosting-Region	Ausschließlich Europäische Union – Hetzner Nürnberg (Primär) + Hetzner Helsinki (Backup-Mirror)
Drittlandtransfer	**Keiner**

Anhang 2: Technische und organisatorische Maßnahmen (TOMs)

Die folgenden TOMs entsprechen Art. 32 DSGVO und sind so kategorisiert, wie es die Aufsichtsbehörden und der branchenübliche DSGVO-AVV-Standard vorgeben. Die Maßnahmen werden im Bergx2-Information-Security-Management-System (ISMS) nach ISO/IEC 27001:2022 dokumentiert und intern detailliert geführt. Konkrete Implementierungsdetails (Hersteller-Modelle, Konfigurations-Parameter, Standorte einzelner Komponenten, Schlüssel- Mechanismen) werden aus Sicherheitsgründen nicht in diesem öffentlich zugänglichen Vertragsanhang offengelegt. Auf begründete Anfrage des Kunden im Rahmen seines Audit-Rechts nach § 9 stellt Bergx2 GmbH die relevanten Detail-Belege im Rahmen eines schriftlichen Geheimhaltungs- Rahmens zur Verfügung.

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

Maßnahme	Umsetzung
Zutrittskontrolle	Mehrstufige physische Zugangskontrolle am Geschäftssitz mit mechanischer Einbruchhemmung gemäß einschlägiger DIN-Normen, Sicherheitsverglasung, automatisch verriegelten Türen, kameragestützter Vorab-Einlasskontrolle ohne Übertragung in externe Netze und Multi-Faktor-Authentisierung an der innersten Schließebene. Zutrittsberechtigungen werden nach dem Need-to-be-present-Prinzip auf einen namentlich begrenzten Personenkreis vergeben und in einem geführten Schlüsselregister mit Ausgabe-/Rückgabe-Audit-Trail dokumentiert. Schlüssel-Reproduktion ist nur mit Freigabe des Vermieters über zertifizierte Schlosser möglich. Besucher betreten Geschäftsräume nur in Begleitung.
Zugangskontrolle (Systeme)	Rollenbasierte Zugriffskontrolle (RBAC) in allen Produktionssystemen; Multi-Faktor-Authentifizierung (MFA) für administrative Zugänge; verbindliche Passwort-Richtlinie nach Stand der Technik; Schlüssel- bzw. Zertifikats-basierter Server-Zugang ohne Passwort; Pflicht-Routing administrativer Zugriffe über ein internes Virtual Private Network (VPN).
Zugriffskontrolle (Daten)	Mandanten-Trennung pro Kunden-Account auf Datenbankebene; Datensatz-Ebene-Zugriffsregeln (Row-Level-Security); revisionssichere Protokollierung aller Lese- und Schreibzugriffe auf personenbezogene Daten.
Pseudonymisierung	Wo immer mit dem Verarbeitungszweck vereinbar werden interne Verarbeitungen pseudonymisiert. Eine periodische Stichprobenprüfung auf unbeabsichtigte Echtnamen-Vorkommen ist als Informationssicherheits-KPI etabliert.
Verschlüsselung	Transportverschlüsselung nach Stand der Technik für alle externen Verbindungen mit regelmäßiger Zertifikats-Rotation. Starke Verschlüsselung im Ruhezustand für Backup-Medien und Endgeräte-Festplatten. Sensitive Zugangsdaten (Passwörter, Tokens, Schlüssel) werden ausschließlich in einem internen, dem Stand der Technik entsprechenden Verfahren verwaltet – Details werden aus Sicherheitsgründen nicht offengelegt.

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

Maßnahme	Umsetzung
Eingabekontrolle	Server-seitige Validierung aller Eingaben; revisionssichere Audit-Protokolle; Schreibrechte ausschließlich über authentisierte und autorisierte Programmierschnittstellen.
Weitergabekontrolle	Pflicht-Transportverschlüsselung für alle externen Verbindungen; keine Datenweitergabe ohne dokumentierte vertragliche Grundlage.
Auftragskontrolle	Auftragsverarbeitungsverträge mit allen Sub-Auftragsverarbeitern (siehe Anhang 3); strukturierter Lieferantenmanagement-Prozess mit periodischer Re-Bewertung.

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

Maßnahme	Umsetzung
Backup	Tägliches inkrementelles Backup der Produktionssysteme mit geografisch getrennter Spiegelung **innerhalb der Europäischen Union**; mehrere Versionen werden vorgehalten; planmäßige Wiederherstellungstests im Quartalsrhythmus.
Verfügbarkeit	Cloud-First-Architektur mit Hosting in ISO/IEC 27001-zertifizierten Rechenzentren mit Notstrom-Reserve; kontinuierliches Monitoring mit definierten Eskalationspfaden.
Business Continuity	Geprüfter Business Continuity Plan inklusive Business Impact Analysis; vollständige Home-Office-Fähigkeit der wissensbasierten Funktionen; dokumentierte Wiederanlaufzeiten je System.
Endgeräte-Resilienz	Ersatz-Endgerät als Gerätedefekt-Reserve; ausreichende Akku-Laufzeit-Reserven für kurzfristige Stromausfälle.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Maßnahme	Umsetzung
Information-Security-Management-System (ISMS)	Etabliertes ISMS nach ISO/IEC 27001:2022 mit Statement of Applicability über die Annex-A-Controls; Zertifizierung in Vorbereitung.
Datenschutz-Management	Geführtes Verzeichnis von Verarbeitungstätigkeiten; bestellte Datenschutzbeauftragte; periodische Reviews der Verarbeitungstätigkeiten.
Awareness	Strukturierte und nachgewiesene Awareness- und Datenschutz-Schulungen für alle Mitarbeitenden mit rollenspezifischen Pflichtmodulen.
Risiko-Management	Mindestens jährliche Risikobewertung mit Top-Management-Approval; Risikobehandlungsplan mit zugeordneten Maßnahmen.
Lieferantenmanagement	Verbindliche Lieferantenrichtlinie und -verfahren; AVV-Pflicht für alle Auftragsverarbeiter; periodische Lieferanten-Reviews.
Incident Response	Dokumentiertes Incident-Management-Verfahren mit definierten Meldewegen, Eskalationsstufen und Wirksamkeitsverifikation.
Patch-Management	Geführtes Patch-Register mit nachvollziehbarer Patch-Anwendung.
Management Review	Mindestens jährliche Bewertung durch das Top-Management auf Basis quantitativer KPIs.
Internes Audit	Jährliches unabhängiges internes ISMS-Audit mit dokumentierten Findings und Korrekturmaßnahmen.

5. Backup-Lebenszyklus und Löschung

Personenbezogene Daten in Backups werden durch die definierte Backup- Rotation innerhalb weniger Wochen vollständig überschrieben.

Bei Vertragsende erfolgt die finale Datenlöschung auf Produktivsystemen binnen 30 Tagen; die Backup-Rotation schließt anschließend die Daten binnen weniger Wochen aus dem Bestand aus.

Konkrete Retention-Fenster pro Backup-Generation werden auf begründete Anfrage im Rahmen des Audit-Rechts (§ 9) offengelegt.

Anhang 3: Liste der Sub-Auftragsverarbeiter

Stand: 25.05.2026.

Nr.	Sub-Auftragsverarbeiter	Sitz	Verarbeitungszweck	Verarbeitete Daten	Zertifizierungen / AVV
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Deutschland – Rechenzentren in Deutschland und Finnland (EU)	Hosting der Screenway-Produktions- und Backup-Infrastruktur	Alle in Anhang 1 genannten Daten; ausschließlich verschlüsselt at-rest und in transit	ISO/IEC 27001 + ISO/IEC 9001 zertifiziert; Auftragsverarbeitungsvertrag durch Bergx2 GmbH aktiv akzeptiert; Subunternehmer-Liste des Hosters öffentlich unter www.hetzner.com/AV/subunternehmer.pdf

Hinweis zu weiteren Bergx2-Lieferanten: Bergx2 GmbH nutzt für den eigenen Geschäftsbetrieb (Mitarbeiterkommunikation, Quellcode-Verwaltung, Office- und Produktivitäts-Werkzeuge) weitere SaaS-Dienstleister. Diese verarbeiten keine Kunden-

Daten aus der Screenway-Plattform und sind daher keine Sub-Auftragsverarbeiter im Sinne dieser AVV. Auf begründete Anfrage des Kunden im Rahmen seines Audit-Rechts (§ 9) wird Bergx2 GmbH die vollständige Liste der eigenen Lieferanten offenlegen.

Wirksamkeit

Diese AVV wird durch Akzeptanz im Customer-Portal mit Zeitstempel und Versionsbezeichnung wirksamer Vertragsbestandteil des Screenway- Service-Vertrags (Art. 28 Abs. 9 DSGVO: schriftlich auch in elektronischem Format).

Der Akzeptanz-Datensatz wird durch Bergx2 GmbH im Customer-Backend revisionssicher archiviert und umfasst mindestens:

- Versionsbezeichnung dieser AVV (siehe Versionierungs-Tabelle unten)
- Datum und Uhrzeit der Akzeptanz
- Identität der akzeptierenden Person (User-ID des Kunden-Accounts)
- Kunden-Identität (Account-/Vertrags-ID)
- Hash-Wert der akzeptierten Vertragsfassung (kryptographischer Integritätsbeleg)

Bei einer Aktualisierung dieser AVV erhält der Kunde mindestens 30 Tage vor Wirksamwerden eine Benachrichtigung in Textform sowie beim nächsten Login im Customer-Portal eine Aufforderung zur Re-Akzeptanz.

Optionale physische oder qualifiziert-elektronische Signatur: Falls der Kunde – z. B. aufgrund interner Compliance-Vorgaben – eine zusätzliche Gegenzeichnung wünscht, kann die AVV physisch oder mittels qualifizierter elektronischer Signatur (eIDAS-Verordnung (EU) Nr. 910/2014) zwischen den Vertragsparteien gegengezeichnet werden. Die Beibringung erfolgt in diesem Fall durch den Kunden. Die elektronische Akzeptanz im Customer- Portal bleibt davon unberührt und stellt für sich genommen einen DSGVO-konformen Vertragsschluss dar.

Versionierung

Version	Stand
1.0	25.05.2026