> Nota: la versione vincolante del presente accordo sul trattamento dei dati è l'originale tedesco disponibile su `/rechtliches/avv`. Questa traduzione italiana è fornita esclusivamente a titolo informativo. In caso di divergenze prevale la versione tedesca.

Accordo sul trattamento dei dati (DPA) per Screenway

> Questa versione è vincolante e può essere validamente conclusa mediante accettazione elettronica nel portale clienti (si veda la sezione «Efficacia»).

Preambolo

Bergx2 GmbH gestisce la piattaforma software-as-a-service Screenway per il controllo del digital signage. Nell'ambito dell'utilizzo del servizio, Bergx2 GmbH tratta dati personali per conto del cliente ai sensi dell'art. 4, punto 8, e dell'art. 28 del Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati, GDPR). Il presente accordo specifica gli obblighi e i diritti di entrambe le parti ai sensi dell'art. 28, paragrafo 3, del GDPR.

---

§ 1 Oggetto e durata del trattamento

(1) Oggetto. Bergx2 GmbH mette a disposizione del cliente la piattaforma Screenway come software-as-a-service. Nell'ambito dell'utilizzo, Bergx2 GmbH tratta i dati personali del cliente descritti in dettaglio nell'Allegato 1 esclusivamente secondo le sue istruzioni.

(2) Durata. L'accordo entra in vigore con la conclusione del contratto principale sottostante (contratto di servizio Screenway) e termina con la sua cessazione. Gli obblighi di cancellazione/restituzione (§ 10) e di riservatezza (§ 5, comma 2) permangono oltre la durata del contratto.

---

§ 2 Natura e finalità del trattamento

(1) Bergx2 GmbH tratta i dati personali descritti nell'Allegato 1 per le seguenti finalità:

- Messa a disposizione della piattaforma Screenway come SaaS di digital signage
- Associazione delle ubicazioni degli schermi agli account cliente
- Visualizzazione sui dispositivi dei contenuti caricati dal cliente
- Autenticazione dei collaboratori del cliente al login
- Fornitura di supporto, analisi degli errori e monitoraggio del servizio

(2) Non ha luogo alcun trattamento per finalità proprie di Bergx2 GmbH (ad es. marketing, profilazione, vendita a terzi).

---

§ 3 Tipo di dati personali e categorie di interessati

Per l'elenco concreto si veda l'Allegato 1. In sintesi:

- Tipo di dati: dati dell'account, dati di login, dati di ubicazione degli schermi, contenuti caricati dal cliente (di norma non personali)
- Categorie di interessati: collaboratori dei clienti (per login e associazione degli account)

Nel funzionamento standard di Screenway non vengono trattate categorie particolari di dati personali ai sensi dell'art. 9 del GDPR. Qualora il cliente carichi comunque tali dati, ciò avviene al di fuori delle categorie contemplate dal presente accordo e sotto la sua esclusiva responsabilità.

---

§ 4 Obblighi e diritti del titolare (cliente)

(1) Potere di impartire istruzioni. Il cliente resta responsabile della liceità del trattamento (art. 24 GDPR). Bergx2 GmbH tratta i dati esclusivamente su istruzione documentata del cliente. Il presente accordo vale come istruzione generale; istruzioni individuali sono possibili tramite i canali di comunicazione definiti nel contratto di servizio.

(2) Registrazione. Bergx2 GmbH documenta i processi rilevanti ai fini delle istruzioni nella traccia di audit interna dell'ISMS (cronologia delle pull request, registro degli incidenti, registro dei fornitori).

(3) Obblighi di informazione. Il cliente è tenuto a informare gli interessati (i propri collaboratori) sul trattamento dei dati da parte di Bergx2 GmbH ai sensi dell'art. 13 del GDPR.

---

§ 5 Obblighi del responsabile del trattamento (Bergx2 GmbH)

(1) Vincolo alle istruzioni. Bergx2 GmbH tratta i dati esclusivamente su istruzione documentata del cliente. In caso di istruzione che, a parere di Bergx2 GmbH, sia illecita, Bergx2 GmbH ne informerà senza indugio il cliente (art. 28, par. 3, lett. h, GDPR).

(2) Riservatezza. Bergx2 GmbH vincola alla riservatezza tutte le persone coinvolte nel trattamento prima dell'inizio dell'attività (art. 28, par. 3, lett. b, GDPR). Ciò avviene mediante dichiarazioni di riservatezza (NDA) all'assunzione o all'incarico ed è documentato nell'ISMS di Bergx2 (registro del personale).

(3) Misure tecniche e organizzative. Bergx2 GmbH adotta le misure descritte nell'Allegato 2, corrispondenti allo stato della tecnica e tali da garantire un livello di protezione adeguato al rischio (art. 32 GDPR).

(4) Sub-responsabili. Bergx2 GmbH ricorre ai sub-responsabili elencati nell'Allegato 3. Per condizioni e meccanismo di modifica si veda il § 6.

(5) Assistenza. Bergx2 GmbH assiste il cliente nell'adempimento dei suoi obblighi ai sensi degli artt. 32–36 del GDPR, in particolare nella risposta alle richieste degli interessati (§ 7) e nella notifica delle violazioni dei dati personali (§ 8).

(6) Prove. Bergx2 GmbH mette a disposizione del cliente, su richiesta, le informazioni e la documentazione necessarie per la verifica (art. 28, par. 3, lett. h, GDPR). Per ulteriori modalità di audit si veda il § 9.

---

§ 6 Sub-responsabili del trattamento

(1) Autorizzazione. Con la conclusione del presente accordo il cliente autorizza in via generale il ricorso ai sub-responsabili elencati nell'Allegato 3 (art. 28, par. 2, primo periodo, GDPR).

(2) Notifica delle modifiche. Bergx2 GmbH informa il cliente delle modifiche previste all'elenco dei sub-responsabili (aggiunta o sostituzione) almeno 30 giorni prima della loro efficacia, in forma testuale (e-mail all'indirizzo di contatto per la protezione dei dati indicato nel contratto di servizio).

(3) Diritto di opposizione. Il cliente può opporsi alla modifica per motivi giustificati entro il termine di 30 giorni. In caso di opposizione, Bergx2 GmbH cerca con il cliente una soluzione concordata; se ciò non riesce, il cliente ha un

diritto di recesso straordinario dal contratto di servizio.

(4) Vincolo. Bergx2 GmbH vincola contrattualmente ciascun sub-responsabile, a sua volta, agli obblighi concordati nel presente accordo (art. 28, par. 4, GDPR).

---

§ 7 Collaborazione nell'esercizio dei diritti degli interessati

Bergx2 GmbH assiste il cliente, per quanto possibile, con misure tecniche e organizzative adeguate nell'adempimento dei diritti degli interessati di cui al Capo III del GDPR (accesso, rettifica, cancellazione, limitazione, portabilità dei dati, opposizione).

In concreto: Bergx2 GmbH inoltra senza indugio al cliente le richieste che gli interessati rivolgono direttamente a Bergx2 GmbH e gli dà la possibilità di rispondere. Una risposta autonoma da parte di Bergx2 GmbH avviene solo su espressa istruzione del cliente.

---

§ 8 Notifica delle violazioni dei dati personali

(1) Bergx2 GmbH informa il cliente senza indugio, al più tardi entro 24 ore dalla presa di conoscenza, di ogni violazione dei dati personali accertata nell'ambito di responsabilità di Bergx2 GmbH o di un sub-responsabile che riguardi dati personali del cliente.

(2) La notifica avviene per iscritto (e-mail all'indirizzo di contatto per la protezione dei dati del cliente) e contiene le indicazioni minime di cui all'art. 33, par. 3, del GDPR (natura e portata della violazione, numero di interessati, probabili conseguenze, contromisure adottate).

(3) Bergx2 GmbH documenta internamente le proprie violazioni dei dati nel registro degli incidenti (si veda `incidents/incidents.md` dell'ISMS di Bergx2, procedura secondo `documents/verfahren/incident-management-verfahren.md`).

(4) L'obbligo di notifica all'autorità di controllo competente ai sensi dell'art. 33 del GDPR e, se del caso, agli interessati ai sensi dell'art. 34 del GDPR resta in capo al cliente quale titolare. Bergx2 GmbH assiste il cliente in tali notifiche con tutte le informazioni necessarie.

---

§ 9 Diritti di audit e di controllo

(1) Prova. Bergx2 GmbH mette a disposizione del cliente, su richiesta, le informazioni necessarie a dimostrare l'adempimento degli obblighi del presente accordo, in particolare la versione di volta in volta vigente delle misure tecniche e organizzative (Allegato 2) e dell'elenco dei sub-responsabili (Allegato 3), nonché, se del caso, estratti di certificazioni.

(2) Controllo in loco. Il cliente ha il diritto di verificare in loco il rispetto delle misure tecniche e organizzative presso la sede di Bergx2 GmbH o presso i luoghi del trattamento. Gli appuntamenti devono essere annunciati per iscritto con almeno quattro settimane di anticipo; i controlli devono limitarsi al necessario e non possono disturbare in modo sproporzionato l'attività aziendale. Al massimo un controllo per anno civile, salvo motivo giustificato.

(3) Riconoscimento delle certificazioni. Nella misura in cui Bergx2 GmbH sia certificata secondo ISO/IEC 27001:2022 (certificazione in preparazione) o presenti verifiche indipendenti equivalenti di terzi, queste

sostituiscono il controllo in loco del cliente, purché l'ambito della certificazione comprenda l'oggetto del contratto.

---

§ 10 Cancellazione e restituzione alla fine del contratto

(1) Alla cessazione del contratto di servizio, Bergx2 GmbH — a scelta del cliente — procederà con i dati personali in uno dei seguenti modi:

- restituzione completa (esportazione in un formato strutturato, di uso comune e leggibile da dispositivo automatico), oppure
- cancellazione completa (sovrascrittura sicura secondo lo stato della tecnica), e

entro 30 giorni dalla fine del contratto.

(2) I backup contenenti dati personali vengono completamente sovrascritti, per rotazione, al più tardi dopo cinque settimane, secondo l'Allegato 2 (misure tecniche e organizzative, ciclo di vita dei backup). Bergx2 GmbH documenta per iscritto la cancellazione finale su richiesta.

(3) Restano impregiudicati gli obblighi legali di conservazione (ad es. dati di fatturazione ai sensi del § 257 del Codice commerciale tedesco (HGB) e del § 147 del Codice tributario tedesco (AO)).

---

§ 11 Responsabilità e disposizioni finali

(1) Responsabilità. Si applicano le disposizioni del contratto principale (contratto di servizio Screenway) e l'art. 82 del GDPR. In caso di violazione del presente accordo, la parte di volta in volta responsabile risponde nei confronti dell'interessato.

(2) Forma scritta. Modifiche e integrazioni richiedono la forma testuale.

(3) Clausola salvatoria. L'eventuale inefficacia di singole disposizioni non pregiudica l'efficacia delle restanti.

(4) Diritto applicabile e foro competente. Si applica il diritto tedesco con esclusione della Convenzione delle Nazioni Unite sui contratti di compravendita internazionale di merci. Il foro competente è Monaco di Baviera.

Allegato 1: Descrizione del trattamento

Categoria	Contenuto
Oggetto	Messa a disposizione della piattaforma SaaS Screenway, incl. hosting, trasmissione dei dati, autenticazione e controllo della visualizzazione
Durata	Durata attiva del contratto + 30 giorni di periodo transitorio per esportazione/cancellazione
Natura del trattamento	Raccolta, registrazione, conservazione, modifica, consultazione, visualizzazione, trasmissione, cancellazione
Finalità	Erogazione del servizio Screenway concordato contrattualmente
Interessati	Collaboratori del cliente ai quali sono concessi accessi di login/controllo a Screenway
Categorie di dati	Dati dell'account (nome, e-mail di lavoro, ruolo), dati di login (hash della password, cookie di sessione, indirizzo IP), dati di ubicazione degli schermi (denominazione ed eventualmente indirizzo dell'ubicazione), contenuti caricati dal cliente (di norma **non** personali — materiale di marketing, testi informativi, ecc.)
Categorie particolari di dati (art. 9 GDPR)	**Non** trattate nel funzionamento standard
Regione di hosting	Esclusivamente Unione Europea — Hetzner Norimberga (primario) + Hetzner Helsinki (mirror di backup)
Trasferimento verso paesi terzi	**Nessuno**

Allegato 2: Misure tecniche e organizzative (TOM)

Le seguenti misure corrispondono all'art. 32 del GDPR e sono categorizzate secondo quanto previsto dalle autorità di controllo e dallo standard di settore per gli accordi sul trattamento dei dati conformi al GDPR. Le misure sono documentate nel sistema di gestione della sicurezza delle informazioni (ISMS) di Bergx2 secondo ISO/IEC 27001:2022 e mantenute internamente in dettaglio. I dettagli concreti di implementazione (modelli dei produttori, parametri di configurazione, ubicazioni di singoli componenti, meccanismi delle chiavi) non vengono divulgati in questo allegato contrattuale pubblicamente accessibile per motivi di sicurezza. Su richiesta motivata del cliente nell'ambito del suo diritto di audit ai sensi del § 9, Bergx2 GmbH mette a disposizione le evidenze di dettaglio pertinenti nell'ambito di un accordo scritto di riservatezza.

1. Riservatezza (art. 32, par. 1, lett. b, GDPR)

Misura	Attuazione
Controllo degli accessi fisici	Controllo fisico degli accessi a più livelli presso la sede con protezione meccanica antieffrazione secondo le pertinenti norme DIN, vetri di sicurezza, porte a chiusura automatica, controllo preventivo degli ingressi assistito da telecamere senza trasmissione a reti esterne e autenticazione a più fattori al livello di chiusura più interno. Le autorizzazioni di accesso sono concesse secondo il principio need-to-be-present a una cerchia di persone limitata nominativamente e documentate in un registro delle chiavi con traccia di audit di consegna/restituzione. La riproduzione delle chiavi è possibile solo con autorizzazione del locatore tramite fabbri certificati. I visitatori accedono ai locali solo accompagnati.
Controllo degli accessi (sistemi)	Controllo degli accessi basato sui ruoli (RBAC) in tutti i sistemi di produzione; autenticazione a più fattori (MFA) per gli accessi amministrativi; direttiva vincolante sulle password secondo lo stato della tecnica; accesso ai server basato su chiavi o certificati senza password; instradamento obbligatorio degli accessi amministrativi tramite una rete privata virtuale (VPN) interna.
Controllo degli accessi (dati)	Separazione dei tenant per account cliente a livello di banca dati; regole di accesso a livello di record (Row-Level-Security); registrazione a prova di revisione di tutti gli accessi in lettura e scrittura ai dati personali.
Pseudonimizzazione	Ove compatibile con la finalità del trattamento, i trattamenti interni vengono pseudonimizzati. È stabilito come KPI di sicurezza delle informazioni un controllo periodico a campione sulle occorrenze involontarie di nomi reali.
Cifratura	Cifratura del trasporto secondo lo stato della tecnica per tutte le connessioni esterne con rotazione periodica dei certificati. Cifratura forte a riposo per i supporti di backup e i dischi dei dispositivi finali. I dati di accesso sensibili (password, token, chiavi) sono gestiti esclusivamente mediante una procedura interna conforme allo stato della tecnica; i dettagli non vengono divulgati per motivi di sicurezza.

2. Integrità (art. 32, par. 1, lett. b, GDPR)

Misura	Attuazione
Controllo degli input	Convalida lato server di tutti gli input; protocolli di audit a prova di revisione; diritti di scrittura esclusivamente tramite interfacce di programmazione autenticate e autorizzate.
Controllo della trasmissione	Cifratura del trasporto obbligatoria per tutte le connessioni esterne; nessuna trasmissione di dati senza base contrattuale documentata.
Controllo degli incarichi	Accordi sul trattamento dei dati con tutti i sub-responsabili (si veda l'Allegato 3); processo strutturato di gestione dei fornitori con rivalutazione periodica.

3. Disponibilità e resilienza (art. 32, par. 1, lett. b, GDPR)

Misura	Attuazione
Backup	Backup incrementale giornaliero dei sistemi di produzione con mirroring geograficamente separato **all'interno dell'Unione Europea**; vengono conservate più versioni; test di ripristino pianificati con cadenza trimestrale.
Disponibilità	Architettura cloud-first con hosting in centri di calcolo certificati ISO/IEC 27001 con riserva di alimentazione di emergenza; monitoraggio continuo con percorsi di escalation definiti.
Continuità operativa	Piano di continuità operativa verificato, inclusa una business impact analysis; piena capacità di lavoro da remoto delle funzioni basate sulla conoscenza; tempi di ripristino documentati per sistema.
Resilienza dei dispositivi finali	Dispositivo finale di riserva in caso di guasto; riserve sufficienti di autonomia delle batterie per brevi interruzioni di corrente.

4. Procedure di verifica, valutazione e valutazione periodica (art. 32, par. 1, lett. d, GDPR)

Misura	Attuazione
Sistema di gestione della sicurezza delle informazioni (ISMS)	ISMS consolidato secondo ISO/IEC 27001:2022 con Statement of Applicability sui controlli dell'Annex A; certificazione in preparazione.
Gestione della protezione dei dati	Registro delle attività di trattamento mantenuto; responsabili della protezione dei dati nominati; revisioni periodiche delle attività di trattamento.
Sensibilizzazione	Formazioni strutturate e documentate su sensibilizzazione e protezione dei dati per tutto il personale, con moduli obbligatori specifici per ruolo.
Gestione dei rischi	Valutazione dei rischi almeno annuale con approvazione del top management; piano di trattamento dei rischi con misure assegnate.
Gestione dei fornitori	Direttiva e procedura vincolanti sui fornitori; obbligo di accordo sul trattamento per tutti i responsabili; revisioni periodiche dei fornitori.
Risposta agli incidenti	Procedura documentata di gestione degli incidenti con canali di segnalazione, livelli di escalation e verifica di efficacia definiti.
Gestione delle patch	Registro delle patch mantenuto con applicazione tracciabile delle patch.
Riesame della direzione	Valutazione almeno annuale da parte del top management sulla base di KPI quantitativi.
Audit interno	Audit interno annuale e indipendente dell'ISMS con rilievi documentati e misure correttive.

5. Ciclo di vita dei backup e cancellazione

I dati personali contenuti nei backup vengono completamente sovrascritti entro poche settimane tramite la rotazione dei backup definita.

Alla fine del contratto, la cancellazione definitiva dei dati sui sistemi produttivi avviene entro 30 giorni; la rotazione dei backup esclude poi i dati dal patrimonio entro poche settimane.

Le finestre di conservazione concrete per generazione di backup vengono divulgate su richiesta motivata nell'ambito del diritto di audit (§ 9).

Allegato 3: Elenco dei sub-responsabili del trattamento

Aggiornato al 25.05.2026.

N.	Sub-responsabile	Sede	Finalità del trattamento	Dati trattati	Certificazioni / accordo sul trattamento
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Germania — centri di calcolo in Germania e Finlandia (UE)	Hosting dell'infrastruttura di produzione e di backup di Screenway	Tutti i dati indicati nell'Allegato 1; esclusivamente cifrati at-rest e in transito	Certificata ISO/IEC 27001 + ISO/IEC 9001; accordo sul trattamento dei dati attivamente accettato da Bergx2 GmbH; elenco dei subappaltatori dell'hoster pubblicamente disponibile su www.hetzner.com/AV/subunternehmer.pdf

Nota sugli altri fornitori di Bergx2: per la propria attività aziendale (comunicazione interna, gestione del codice sorgente, strumenti di office e produttività), Bergx2 GmbH utilizza altri fornitori SaaS. Questi non trattano dati dei clienti della piattaforma Screenway e non sono quindi sub-responsabili ai sensi del presente accordo. Su richiesta motivata del cliente nell'ambito del suo diritto di audit (§ 9), Bergx2 GmbH divulgherà l'elenco completo dei propri fornitori.

Efficacia

Il presente accordo diventa, mediante accettazione nel portale clienti con marca temporale e indicazione della versione, parte integrante efficace del contratto di servizio Screenway (art. 28, par. 9, GDPR: per iscritto, anche in formato elettronico).

Il record di accettazione viene archiviato da Bergx2 GmbH in modo inalterabile nel backend clienti e comprende almeno:

- Indicazione della versione del presente accordo (si veda la tabella delle versioni)
- Data e ora dell'accettazione
- Identità della persona accettante (ID utente dell'account cliente)
- Identità del cliente (ID account/contratto)
- Valore hash della versione contrattuale accettata (prova crittografica di integrità)

In caso di aggiornamento del presente accordo, il cliente riceve una notifica in forma testuale almeno 30 giorni prima dell'efficacia, nonché un invito alla riaccettazione al successivo login nel portale clienti.

Firma fisica o elettronica qualificata facoltativa: qualora il cliente — ad es. per requisiti interni di conformità — desideri una controfirma aggiuntiva, l'accordo può essere controfirmato fisicamente o mediante firma elettronica qualificata (Regolamento eIDAS (UE) n. 910/2014) tra le parti contraenti. In tal caso la predisposizione è a carico del cliente. L'accettazione elettronica nel portale clienti resta impregiudicata e costituisce di per sé una conclusione del contratto conforme al GDPR.

Versioni

Versione	Data
1.0	25.05.2026