> Note: The binding version of this Data Processing Agreement is the German original available at `/rechtliches/avv`. This English translation is provided for convenience only. In case of discrepancies, the German version prevails.

Data Processing Agreement (DPA) for Screenway

> This version is binding and may be validly concluded by electronic acceptance in the Customer Portal (see section "Effectiveness").

Preamble

Bergx2 GmbH operates the Software-as-a-Service platform Screenway for digital signage control. In the course of service use, Bergx2 GmbH processes personal data on behalf of the Customer within the meaning of Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). This agreement specifies the obligations and rights of both parties pursuant to Art. 28(3) GDPR.

---

§ 1 Subject matter and duration of the processing

(1) Subject matter. Bergx2 GmbH provides the Customer with the Screenway platform as Software-as-a-Service. In the course of use, Bergx2 GmbH processes the personal data of the Customer described in more detail in Annex 1 exclusively in accordance with the Customer's instructions.

(2) Duration. The agreement enters into force upon the conclusion of the underlying main contract (Screenway service contract) and ends upon its termination. The obligations regarding deletion/return (§ 10) and confidentiality (§ 5 para. 2) continue to apply beyond the contract term.

---

§ 2 Nature and purpose of the processing

(1) Bergx2 GmbH processes the personal data described in Annex 1 for the following purposes:

- Provision of the Screenway platform as a Digital Signage SaaS
- Assignment of screen locations to customer accounts
- Display of content uploaded by the Customer on the end devices
- Authentication of the Customer's employees upon login
- Provision of support, error analysis and service monitoring

(2) Processing for Bergx2 GmbH's own purposes (e.g. marketing, profiling, sale to third parties) does not take place.

---

§ 3 Nature of the personal data and categories of data subjects

For the specific list, see Annex 1. In summary:

- Nature of the data: account data, login data, screen location data, content uploaded by the Customer (generally non-personal)
- Categories of data subjects: employees of the Customer (for login and account assignment)

The processing of special categories of personal data within the meaning of Art. 9 GDPR does not take place in the standard Screenway operation. If the Customer nevertheless uploads such data, this occurs outside the categories addressed by this DPA and at the Customer's sole responsibility.

---

§ 4 Obligations and rights of the Controller (Customer)

(1) Right to issue instructions. The Customer remains responsible for the lawfulness of the processing (Art. 24 GDPR). Bergx2 GmbH processes the data exclusively on the documented instructions of the Customer. This DPA constitutes the general instructions; individual instructions may be given via the communication channels defined in the service contract.

(2) Recording. Bergx2 GmbH documents instruction-relevant operations in the internal ISMS audit trail (pull request history, incident register, supplier register).

(3) Information obligations. The Customer is obliged to inform the data subjects (its employees) pursuant to Art. 13 GDPR about the data processing carried out by Bergx2 GmbH.

---

§ 5 Obligations of the Processor (Bergx2 GmbH)

(1) Compliance with instructions. Bergx2 GmbH processes the data exclusively on the documented instructions of the Customer. If Bergx2 GmbH considers an instruction to be unlawful, Bergx2 GmbH will inform the Customer without undue delay (Art. 28(3) lit. h GDPR).

(2) Confidentiality. Bergx2 GmbH places all persons involved in the processing under a confidentiality obligation before they take up their activity (Art. 28(3) lit. b GDPR). This is done by confidentiality agreements (NDA) upon hiring or engagement and is documented in the Bergx2 GmbH ISMS (employee register).

(3) Technical and organisational measures. Bergx2 GmbH implements the TOMs described in Annex 2, which correspond to the state of the art and ensure a level of protection appropriate to the risk (Art. 32 GDPR).

(4) Sub-processors. Bergx2 GmbH uses the sub-processors listed in Annex 3. Conditions and the change mechanism are set out in § 6.

(5) Support. Bergx2 GmbH supports the Customer in fulfilling its obligations under Art. 32–36 GDPR, in particular in responding to data subject requests (§ 7) and reporting data breaches (§ 8).

(6) Evidence. Bergx2 GmbH provides the Customer, upon request, with the information and documents required for inspection (Art. 28(3) lit. h GDPR). Further audit arrangements are set out in § 9.

---

§ 6 Sub-processors

(1) Authorisation. By concluding this DPA, the Customer generally authorises the engagement of the sub-processors listed in Annex 3 (Art. 28(2) sentence 1 GDPR).

(2) Change notification. Bergx2 GmbH will inform the Customer of intended changes to the sub-processor roster (addition or replacement) at least 30 days before the change takes effect, in text form (email to the data protection contact address stored in the service contract).

(3) Right of objection. The Customer may object to the change on legitimate grounds within the 30-day period. In the event of an objection, Bergx2 GmbH will seek an amicable solution with the Customer; if this is not successful, the Customer has an extraordinary right to terminate the service contract.

(4) Obligation. Bergx2 GmbH contractually imposes on each sub-processor the same obligations agreed in this DPA (Art. 28(4) GDPR).

---

§ 7 Cooperation in relation to data subject rights

Bergx2 GmbH supports the Customer with appropriate technical and organisational measures, in so far as possible, in fulfilling the rights of data subjects under Chapter III of the GDPR (information, rectification, erasure, restriction, data portability, objection).

Specifically: Bergx2 GmbH forwards corresponding requests that data subjects address directly to Bergx2 GmbH without undue delay to the Customer and gives the latter the opportunity to respond. Bergx2 GmbH itself only responds upon the express instruction of the Customer.

---

§ 8 Notification of data breaches

(1) Bergx2 GmbH informs the Customer without undue delay, and at the latest within 24 hours of becoming aware, of any identified data breach within the area of responsibility of Bergx2 GmbH or a sub-processor that affects personal data of the Customer.

(2) The notification is provided in writing (email to the Customer's data protection contact address) and contains the minimum information referred to in Art. 33(3) GDPR (nature and scope of the breach, number of data subjects affected, likely consequences, countermeasures taken).

(3) Bergx2 GmbH documents its own data breaches internally in the incident register (see `incidents/incidents.md` of the Bergx2 GmbH ISMS, procedure pursuant to `documents/verfahren/incident-management-verfahren.md`).

(4) The obligation to notify the competent supervisory authority pursuant to Art. 33 GDPR and, where applicable, the data subjects pursuant to Art. 34 GDPR remains with the Customer as Controller. Bergx2 GmbH supports the Customer in such notifications with all necessary information.

---

§ 9 Audit and inspection rights

(1) Evidence. Bergx2 GmbH provides the Customer, upon request, with the information necessary to fulfil the obligations arising from this DPA, in particular the current version of the TOMs (Annex 2) and the sub-processor list (Annex 3), as well as, where applicable, excerpts from certifications.

(2) On-site inspection. The Customer has the right to satisfy itself of compliance with the TOMs on site at Bergx2 GmbH's place of business or at the processing locations. Appointments must be announced in writing at least four weeks in advance; inspections must be limited to what is necessary and must not unreasonably disrupt business operations. Maximum one inspection per calendar year, unless there is justified cause.

(3) Recognition of certifications. Insofar as Bergx2 GmbH is certified under ISO/IEC 27001:2022 (certification in preparation) or provides equivalent independent third-party audits, this replaces the Customer's on-site inspection, provided that the scope of the certification also covers the subject matter of the contract.

---

§ 10 Deletion and return after termination of the contract

(1) Upon termination of the service contract, Bergx2 GmbH will – at the Customer's choice – either:

- fully return the personal data (export in a structured, commonly used, machine-readable format), or
- fully delete the personal data (secure overwriting in line with the state of the art), and

within 30 days after termination of the contract.

(2) Backups containing personal data are, due to backup rotation, fully overwritten within at most five weeks in accordance with Annex 2 TOMs § Backup lifecycle. Bergx2 GmbH documents the final deletion in writing upon request.

(3) Statutory retention obligations remain unaffected (e.g. billing data pursuant to § 257 HGB, § 147 AO).

---

§ 11 Liability and final provisions

(1) Liability. The provisions of the main contract (Screenway service contract) and Art. 82 GDPR apply. In the event of a breach of this DPA, the respective responsible party is liable vis-à-vis the data subject.

(2) Written form. Amendments and supplements require text form.

(3) Severability clause. Should individual provisions be invalid, the validity of the remaining provisions shall remain unaffected.

(4) Applicable law and place of jurisdiction. German law applies, excluding the UN Convention on Contracts for the International Sale of Goods. Place of jurisdiction is Munich.

Annex 1: Description of the processing

Category	Content
Subject matter	Provision of the Screenway SaaS platform incl. hosting, data transmission, authentication and display control
Duration	Active contract term + 30 days transition period for export/deletion
Nature of the processing	Collection, recording, storage, alteration, retrieval, display, transmission, deletion
Purpose	Provision of the contractually agreed Screenway service
Data subjects	Employees of the Customer who are granted login/control access to Screenway
Data categories	Account data (name, business email, role), login data (password hash, session cookies, IP address), screen location data (designation, where applicable the address of the location), content uploaded by the Customer (generally **not** personal – marketing material, notices etc.)
Special data categories (Art. 9 GDPR)	**Not** processed in standard operation
Hosting region	Exclusively European Union – Hetzner Nuremberg (primary) + Hetzner Helsinki (backup mirror)
Third-country transfer	**None**

Annex 2: Technical and organisational measures (TOMs)

The following TOMs correspond to Art. 32 GDPR and are categorised in accordance with the requirements of the supervisory authorities and the industry-standard GDPR-DPA framework. The measures are documented in the Bergx2 GmbH Information Security Management System (ISMS) pursuant to ISO/IEC 27001:2022 and are maintained in detail internally. Specific implementation details (manufacturer models, configuration parameters, locations of individual components, key mechanisms) are, for security reasons, not disclosed in this publicly accessible contract annex. Upon the Customer's reasoned request within the scope of its audit right pursuant to § 9, Bergx2 GmbH will make the relevant detailed evidence available under a written confidentiality framework.

1. Confidentiality (Art. 32(1) lit. b GDPR)

Measure	Implementation
Physical access control	Multi-stage physical access control at the business premises with mechanical burglary resistance in accordance with the relevant DIN standards, security glazing, automatically locking doors, camera-based pre-entry control without transmission to external networks, and multi-factor authentication at the innermost locking level. Access rights are granted on a need-to-be-present basis to a named limited group of persons and are documented in a maintained key register with issue/return audit trail. Key reproduction is only possible with the landlord's approval via certified locksmiths. Visitors only enter business premises when accompanied.
System access control	Role-based access control (RBAC) in all production systems; multi-factor authentication (MFA) for administrative access; binding password policy in line with the state of the art; key- or certificate-based server access without passwords; mandatory routing of administrative access via an internal Virtual Private Network (VPN).
Data access control	Tenant separation per customer account at the database level; record-level access rules (Row-Level Security); audit-proof logging of all read and write access to personal data.
Pseudonymisation	Wherever compatible with the processing purpose, internal processing is pseudonymised. A periodic sample check for unintended real-name occurrences is established as an information security KPI.
Encryption	Transport encryption in line with the state of the art for all external connections with regular certificate rotation. Strong encryption at rest for backup media and end-device hard drives. Sensitive credentials (passwords, tokens, keys) are managed exclusively in an internal procedure in line with the state of the art – details are not disclosed for security reasons.

2. Integrity (Art. 32(1) lit. b GDPR)

Measure	Implementation
Input control	Server-side validation of all inputs; audit-proof audit logs; write rights exclusively via authenticated and authorised programming interfaces.
Disclosure control	Mandatory transport encryption for all external connections; no transfer of data without a documented contractual basis.
Order control	Data processing agreements with all sub-processors (see Annex 3); structured supplier management process with periodic re-evaluation.

3. Availability and resilience (Art. 32(1) lit. b GDPR)

Measure	Implementation
Backup	Daily incremental backup of production systems with geographically separated mirroring **within the European Union**; several versions are retained; scheduled recovery tests on a quarterly basis.
Availability	Cloud-first architecture with hosting in ISO/IEC 27001-certified data centres with emergency power reserve; continuous monitoring with defined escalation paths.
Business continuity	Tested Business Continuity Plan including Business Impact Analysis; full home-office capability for knowledge-based functions; documented recovery times per system.
End-device resilience	Spare end-device as a hardware failure reserve; sufficient battery runtime reserves for short-term power outages.

4. Procedures for regular review, assessment and evaluation (Art. 32(1) lit. d GDPR)

Measure	Implementation
Information Security Management System (ISMS)	Established ISMS pursuant to ISO/IEC 27001:2022 with a Statement of Applicability covering the Annex A controls; certification in preparation.
Data protection management	Maintained record of processing activities; appointed data protection officer; periodic reviews of processing activities.
Awareness	Structured and verifiable awareness and data protection training for all employees with role-specific mandatory modules.
Risk management	At least annual risk assessment with top-management approval; risk treatment plan with assigned measures.
Supplier management	Binding supplier policy and procedures; DPA requirement for all processors; periodic supplier reviews.
Incident response	Documented incident management procedure with defined reporting paths, escalation levels and effectiveness verification.
Patch management	Maintained patch register with traceable patch application.
Management review	At least annual evaluation by top management on the basis of quantitative KPIs.
Internal audit	Annual independent internal ISMS audit with documented findings and corrective measures.

5. Backup lifecycle and deletion

Personal data in backups is fully overwritten within a few weeks by the defined backup rotation.

At the end of the contract, the final deletion of data on production systems takes place within 30 days; the backup rotation subsequently removes the data from the holding within a few weeks.

Specific retention windows per backup generation are disclosed upon reasoned request within the scope of the audit right (§ 9).

Annex 3: List of sub-processors

As of: 25.05.2026.

No.	Sub-processor	Location	Processing purpose	Data processed	Certifications / DPA
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Germany – data centres in Germany and Finland (EU)	Hosting of the Screenway production and backup infrastructure	All data listed in Annex 1; exclusively encrypted at rest and in transit	ISO/IEC 27001 + ISO/IEC 9001 certified; data processing agreement actively accepted by Bergx2 GmbH; the hoster's sub-processor list publicly available at www.hetzner.com/AV/subunternehmer.pdf

Note on other Bergx2 GmbH suppliers: Bergx2 GmbH uses additional SaaS providers for its own business operations (employee communication, source code management, office and productivity tools). These do not process customer data from the Screenway platform and therefore are not sub-processors within the meaning of this DPA. Upon the Customer's reasoned request within the scope of its audit right (§ 9), Bergx2 GmbH will disclose the complete list of its own suppliers.

Effectiveness

This DPA becomes an effective contractual component of the Screenway service contract through acceptance in the Customer Portal with timestamp and version designation (Art. 28(9) GDPR: in writing, also in electronic format).

The acceptance record is archived by Bergx2 GmbH in an audit-proof manner in the customer backend and contains at least:

- Version designation of this DPA (see version table below)
- Date and time of acceptance
- Identity of the accepting person (User ID of the customer account)
- Customer identity (account/contract ID)
- Hash value of the accepted contract version (cryptographic integrity evidence)

In the event of an update to this DPA, the Customer will receive a notification in text form at least 30 days before it takes effect, as well as a request for re-acceptance at the next login in the Customer Portal.

Optional physical or qualified electronic signature: If the Customer – e.g. due to internal compliance requirements – wishes additional countersignature, the DPA may be countersigned physically or by

means of a qualified electronic signature (eIDAS Regulation (EU) No. 910/2014) between the contracting parties. The provision is, in that case, made by the Customer. Electronic acceptance in the Customer Portal remains unaffected and, in itself, constitutes a GDPR-compliant conclusion of contract.

Versioning

Version	Date
1.0	25.05.2026