> Nota: La versión vinculante de este contrato de encargo de tratamiento es el original alemán disponible en `/rechtliches/avv`. Esta traducción al español se facilita únicamente a título informativo. En caso de discrepancias prevalece la versión alemana.

Contrato de encargo de tratamiento (DPA) para Screenway

> Esta versión es vinculante y puede celebrarse válidamente mediante aceptación electrónica en el portal de clientes (véase la sección «Eficacia»).

Preámbulo

Bergx2 GmbH opera la plataforma de software como servicio Screenway para la gestión de señalización digital. En el marco del uso del servicio, Bergx2 GmbH trata datos personales por encargo del cliente en el sentido del art. 4, punto 8, y del art. 28 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, RGPD). El presente contrato concreta las obligaciones y los derechos de ambas partes conforme al art. 28, apartado 3, del RGPD.

---

§ 1 Objeto y duración del tratamiento

(1) Objeto. Bergx2 GmbH pone a disposición del cliente la plataforma Screenway como software como servicio. En el marco del uso, Bergx2 GmbH trata los datos personales del cliente descritos con más detalle en el Anexo 1 exclusivamente conforme a sus instrucciones.

(2) Duración. El contrato entra en vigor con la celebración del contrato principal subyacente (contrato de servicio Screenway) y finaliza con su terminación. Las obligaciones de supresión/devolución (§ 10) y de confidencialidad (§ 5, apdo. 2) subsisten más allá de la duración del contrato.

---

§ 2 Naturaleza y finalidad del tratamiento

(1) Bergx2 GmbH trata los datos personales descritos en el Anexo 1 para las siguientes finalidades:

- Puesta a disposición de la plataforma Screenway como SaaS de señalización digital
- Asignación de las ubicaciones de pantallas a las cuentas de cliente
- Visualización en los dispositivos de los contenidos cargados por el cliente
- Autenticación de los empleados del cliente al iniciar sesión
- Prestación de soporte, análisis de errores y supervisión del servicio

(2) No se realiza ningún tratamiento para fines propios de Bergx2 GmbH (p. ej. marketing, elaboración de perfiles, venta a terceros).

---

§ 3 Tipo de datos personales y categorías de interesados

Para la enumeración concreta, véase el Anexo 1. En resumen:

- Tipo de datos: datos de cuenta, datos de inicio de sesión, datos de ubicación de las pantallas, contenidos cargados por el cliente (por regla general, no personales)

- Categorías de interesados: empleados de los clientes (para el inicio de sesión y la asignación de cuentas)

En el funcionamiento estándar de Screenway no se tratan categorías especiales de datos personales en el sentido del art. 9 del RGPD. Si el cliente carga, no obstante, tales datos, esto sucede fuera de las categorías contempladas por este contrato y bajo la exclusiva responsabilidad del cliente.

---

§ 4 Obligaciones y derechos del responsable (cliente)

(1) Facultad de impartir instrucciones. El cliente sigue siendo responsable de la licitud del tratamiento (art. 24 RGPD). Bergx2 GmbH trata los datos exclusivamente según las instrucciones documentadas del cliente. Este contrato se considera instrucción general; las instrucciones individuales son posibles a través de los canales de comunicación definidos en el contrato de servicio.

(2) Registro. Bergx2 GmbH documenta los procesos relevantes para las instrucciones en la pista de auditoría interna del SGSI (historial de pull requests, registro de incidentes, registro de proveedores).

(3) Obligaciones de información. El cliente está obligado a informar a los interesados (sus empleados) sobre el tratamiento de datos por parte de Bergx2 GmbH conforme al art. 13 del RGPD.

---

§ 5 Obligaciones del encargado del tratamiento (Bergx2 GmbH)

(1) Sujeción a instrucciones. Bergx2 GmbH trata los datos exclusivamente según las instrucciones documentadas del cliente. Si, a juicio de Bergx2 GmbH, una instrucción es contraria a derecho, Bergx2 GmbH informará de ello al cliente sin dilación (art. 28, apdo. 3, letra h, RGPD).

(2) Confidencialidad. Bergx2 GmbH obliga a la confidencialidad a todas las personas que intervienen en el tratamiento antes de iniciar su actividad (art. 28, apdo. 3, letra b, RGPD). Esto se realiza mediante declaraciones de confidencialidad (NDA) en la contratación o el encargo y está documentado en el SGSI de Bergx2 (registro de personal).

(3) Medidas técnicas y organizativas. Bergx2 GmbH adopta las medidas descritas en el Anexo 2, que corresponden al estado de la técnica y garantizan un nivel de protección adecuado al riesgo (art. 32 RGPD).

(4) Subencargados. Bergx2 GmbH emplea los subencargados enumerados en el Anexo 3. Para las condiciones y el mecanismo de cambios, véase el § 6.

(5) Asistencia. Bergx2 GmbH asiste al cliente en el cumplimiento de sus obligaciones conforme a los arts. 32 a 36 del RGPD, en particular en la respuesta a las solicitudes de los interesados (§ 7) y en la notificación de violaciones de la seguridad de los datos (§ 8).

(6) Pruebas. Bergx2 GmbH pone a disposición del cliente, previa solicitud, la información y la documentación necesarias para la verificación (art. 28, apdo. 3, letra h, RGPD). Para otras modalidades de auditoría, véase el § 9.

---

§ 6 Subencargados del tratamiento

(1) Autorización. Con la celebración de este contrato, el cliente autoriza de forma general el recurso a los subencargados enumerados en el Anexo 3 (art. 28, apdo. 2, primera frase, RGPD).

(2) Notificación de cambios. Bergx2 GmbH informará al cliente de los cambios previstos en la lista de subencargados (incorporación o sustitución) al menos 30 días antes de su entrada en vigor, en forma textual

(correo electrónico a la dirección de contacto de protección de datos indicada en el contrato de servicio).

(3) Derecho de oposición. El cliente puede oponerse al cambio por motivos justificados dentro del plazo de 30 días. En caso de oposición, Bergx2 GmbH buscará con el cliente una solución de mutuo acuerdo; si no se alcanza, el cliente tiene un derecho de resolución extraordinaria del contrato de servicio.

(4) Obligación. Bergx2 GmbH obliga contractualmente a cada subencargado, por su parte, a las obligaciones acordadas en este contrato (art. 28, apdo. 4, RGPD).

---

§ 7 Colaboración en los derechos de los interesados

Bergx2 GmbH asiste al cliente, en la medida de lo posible, con medidas técnicas y organizativas apropiadas para el cumplimiento de los derechos de los interesados del Capítulo III del RGPD (acceso, rectificación, supresión, limitación, portabilidad de los datos, oposición).

En concreto: Bergx2 GmbH remite sin dilación al cliente las solicitudes que los interesados dirijan directamente a Bergx2 GmbH y le da la posibilidad de responder. Bergx2 GmbH solo responde por sí misma previa instrucción expresa del cliente.

---

§ 8 Notificación de violaciones de la seguridad de los datos

(1) Bergx2 GmbH informará al cliente sin dilación, a más tardar dentro de las 24 horas siguientes a tener conocimiento, de toda violación de la seguridad de los datos constatada en el ámbito de responsabilidad de Bergx2 GmbH o de un subencargado que afecte a datos personales del cliente.

(2) La notificación se realiza por escrito (correo electrónico a la dirección de contacto de protección de datos del cliente) y contiene la información mínima indicada en el art. 33, apdo. 3, del RGPD (naturaleza y alcance de la violación, número de afectados, consecuencias probables, medidas correctivas adoptadas).

(3) Bergx2 GmbH documenta internamente sus propias violaciones de la seguridad de los datos en el registro de incidentes (véase `incidents/incidents.md` del SGSI de Bergx2, procedimiento conforme a `documents/verfahren/incident-management-verfahren.md`).

(4) La obligación de notificación a la autoridad de control competente conforme al art. 33 del RGPD y, en su caso, a los interesados conforme al art. 34 del RGPD corresponde al cliente como responsable. Bergx2 GmbH asiste al cliente en estas notificaciones con toda la información necesaria.

---

§ 9 Derechos de auditoría y control

(1) Prueba. Bergx2 GmbH pone a disposición del cliente, previa solicitud, la información necesaria para acreditar el cumplimiento de las obligaciones de este contrato, en particular la versión vigente de las medidas técnicas y organizativas (Anexo 2) y de la lista de subencargados (Anexo 3), así como, en su caso, extractos de certificaciones.

(2) Inspección in situ. El cliente tiene derecho a comprobar el cumplimiento de las medidas técnicas y organizativas in situ en el domicilio social de Bergx2 GmbH o en los lugares del tratamiento. Las citas deben anunciarse por escrito con al menos cuatro semanas de antelación; las inspecciones deben limitarse a lo necesario y no pueden perturbar de forma desproporcionada la actividad empresarial. Máximo una inspección por año natural, salvo motivo justificado.

(3) Reconocimiento de certificaciones. En la medida en que Bergx2 GmbH esté certificada conforme a ISO/IEC 27001:2022 (certificación en preparación) o presente verificaciones independientes equivalentes de terceros, estas sustituyen a la inspección in situ del cliente, siempre que el alcance de la certificación comprenda el objeto del contrato.

---

§ 10 Supresión y devolución al finalizar el contrato

(1) Al finalizar el contrato de servicio, Bergx2 GmbH — a elección del cliente — procederá con los datos personales de una de las siguientes maneras:

- devolución completa (exportación en un formato estructurado, de uso común y legible por máquina), o
- supresión completa (sobrescritura segura conforme al estado de la técnica), y

dentro de los 30 días siguientes a la finalización del contrato.

(2) Las copias de seguridad que contengan datos personales se sobrescriben completamente, por rotación, a más tardar transcurridas cinco semanas, conforme al Anexo 2 (medidas técnicas y organizativas, ciclo de vida de las copias de seguridad). Bergx2 GmbH documenta por escrito la supresión final previa solicitud.

(3) Las obligaciones legales de conservación no se ven afectadas (p. ej. datos de facturación conforme al § 257 del Código de Comercio alemán (HGB) y al § 147 del Código Tributario alemán (AO)).

---

§ 11 Responsabilidad y disposiciones finales

(1) Responsabilidad. Se aplican las disposiciones del contrato principal (contrato de servicio Screenway) y el art. 82 del RGPD. En caso de infracción de este contrato, la parte responsable en cada caso responde frente al interesado.

(2) Forma escrita. Las modificaciones y adiciones requieren forma textual.

(3) Cláusula de salvaguardia. Si alguna disposición resultara ineficaz, la eficacia de las restantes no se verá afectada.

(4) Derecho aplicable y fuero. Se aplica el derecho alemán con exclusión de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. El fuero competente es Múnich.

Anexo 1: Descripción del tratamiento

Categoría	Contenido
Objeto	Puesta a disposición de la plataforma SaaS Screenway, incl. alojamiento, transmisión de datos, autenticación y control de visualización
Duración	Vigencia activa del contrato + 30 días de periodo transitorio para exportación/supresión
Naturaleza del tratamiento	Recogida, registro, almacenamiento, modificación, consulta, visualización, transmisión, supresión
Finalidad	Prestación del servicio Screenway acordado contractualmente
Interesados	Empleados del cliente a los que se conceden accesos de inicio de sesión/control a Screenway
Categorías de datos	Datos de cuenta (nombre, correo electrónico profesional, rol), datos de inicio de sesión (hash de contraseña, cookies de sesión, dirección IP), datos de ubicación de las pantallas (denominación y, en su caso, dirección de la ubicación), contenidos cargados por el cliente (por regla general **no** personales — material de marketing, textos informativos, etc.)
Categorías especiales de datos (art. 9 RGPD)	**No** se tratan en el funcionamiento estándar
Región de alojamiento	Exclusivamente la Unión Europea — Hetzner Núremberg (primario) + Hetzner Helsinki (réplica de copias de seguridad)
Transferencia a terceros países	**Ninguna**

Anexo 2: Medidas técnicas y organizativas (TOM)

Las siguientes medidas corresponden al art. 32 del RGPD y están categorizadas según lo establecen las autoridades de control y el estándar habitual del sector para contratos de encargo conforme al RGPD. Las medidas se documentan en el sistema de gestión de la seguridad de la información (SGSI) de Bergx2 conforme a ISO/IEC 27001:2022 y se mantienen internamente con detalle. Los detalles concretos de implementación (modelos de fabricantes, parámetros de configuración, ubicaciones de componentes individuales, mecanismos de claves) no se divulgan en este anexo contractual de acceso público por motivos de seguridad. Previa solicitud justificada del cliente en el marco de su derecho de auditoría conforme al § 9, Bergx2 GmbH facilitará los justificantes de detalle pertinentes en el marco de un acuerdo escrito de confidencialidad.

1. Confidencialidad (art. 32, apdo. 1, letra b, RGPD)

Medida	Implementación
Control de acceso físico	Control de acceso físico de varios niveles en el domicilio social con protección mecánica antiintrusión conforme a las normas DIN aplicables, acristalamiento de seguridad, puertas con bloqueo automático, control previo de entrada asistido por cámara sin transmisión a redes externas y autenticación multifactor en el nivel de cierre más interno. Las autorizaciones de acceso se conceden según el principio de necesidad de presencia a un círculo de personas limitado nominalmente y se documentan en un registro de llaves con pista de auditoría de entrega/devolución. La reproducción de llaves solo es posible con autorización del arrendador a través de cerrajeros certificados. Los visitantes acceden a los locales únicamente acompañados.
Control de acceso (sistemas)	Control de acceso basado en roles (RBAC) en todos los sistemas de producción; autenticación multifactor (MFA) para accesos administrativos; política de contraseñas vinculante conforme al estado de la técnica; acceso a servidores basado en claves o certificados sin contraseña; enrutamiento obligatorio de los accesos administrativos a través de una red privada virtual (VPN) interna.
Control de acceso (datos)	Separación de inquilinos por cuenta de cliente a nivel de base de datos; reglas de acceso a nivel de registro (Row-Level-Security); registro a prueba de revisiones de todos los accesos de lectura y escritura a datos personales.
Seudonimización	Siempre que sea compatible con la finalidad del tratamiento, los tratamientos internos se seudonimizan. Se ha establecido como KPI de seguridad de la información una comprobación periódica por muestreo de apariciones involuntarias de nombres reales.
Cifrado	Cifrado de transporte conforme al estado de la técnica para todas las conexiones externas con rotación periódica de certificados. Cifrado fuerte en reposo para soportes de copia de seguridad y discos duros de dispositivos finales. Los datos de acceso sensibles (contraseñas, tokens, claves) se gestionan exclusivamente mediante un procedimiento interno conforme al estado de la técnica; los detalles no se divulgan por motivos de seguridad.

2. Integridad (art. 32, apdo. 1, letra b, RGPD)

Medida	Implementación
Control de entrada	Validación en el servidor de todas las entradas; registros de auditoría a prueba de revisiones; derechos de escritura exclusivamente a través de interfaces de programación autenticadas y autorizadas.
Control de transmisión	Cifrado de transporte obligatorio para todas las conexiones externas; ninguna transmisión de datos sin base contractual documentada.
Control de encargos	Contratos de encargo de tratamiento con todos los subencargados (véase el Anexo 3); proceso estructurado de gestión de proveedores con reevaluación periódica.

3. Disponibilidad y resiliencia (art. 32, apdo. 1, letra b, RGPD)

Medida	Implementación
Copias de seguridad	Copia de seguridad incremental diaria de los sistemas de producción con réplica geográficamente separada **dentro de la Unión Europea**; se conservan varias versiones; pruebas de restauración programadas con periodicidad trimestral.
Disponibilidad	Arquitectura «cloud first» con alojamiento en centros de datos certificados ISO/IEC 27001 con reserva de energía de emergencia; supervisión continua con vías de escalado definidas.
Continuidad de negocio	Plan de continuidad de negocio verificado, incluido un análisis de impacto en el negocio; plena capacidad de teletrabajo de las funciones basadas en conocimiento; tiempos de reanudación documentados por sistema.
Resiliencia de dispositivos finales	Dispositivo final de repuesto como reserva ante defectos; reservas suficientes de autonomía de batería para cortes de electricidad breves.

4. Procedimientos de revisión, valoración y evaluación periódicas (art. 32, apdo. 1, letra d, RGPD)

Medida	Implementación
Sistema de gestión de la seguridad de la información (SGSI)	SGSI establecido conforme a ISO/IEC 27001:2022 con declaración de aplicabilidad sobre los controles del Anexo A; certificación en preparación.
Gestión de la protección de datos	Registro de actividades de tratamiento mantenido; delegados de protección de datos designados; revisiones periódicas de las actividades de tratamiento.
Concienciación	Formaciones estructuradas y acreditadas de concienciación y protección de datos para todo el personal, con módulos obligatorios específicos por rol.
Gestión de riesgos	Evaluación de riesgos al menos anual con aprobación de la alta dirección; plan de tratamiento de riesgos con medidas asignadas.
Gestión de proveedores	Directriz y procedimiento de proveedores vinculantes; obligación de contrato de encargo para todos los encargados; revisiones periódicas de proveedores.
Respuesta a incidentes	Procedimiento documentado de gestión de incidentes con vías de notificación, niveles de escalado y verificación de eficacia definidos.
Gestión de parches	Registro de parches mantenido con aplicación trazable de los parches.
Revisión por la dirección	Evaluación al menos anual por la alta dirección sobre la base de KPI cuantitativos.
Auditoría interna	Auditoría interna anual e independiente del SGSI con hallazgos documentados y medidas correctivas.

5. Ciclo de vida de las copias de seguridad y supresión

Los datos personales contenidos en las copias de seguridad se sobrescriben completamente en pocas semanas mediante la rotación de copias definida.

Al finalizar el contrato, la supresión definitiva de los datos en los sistemas productivos se realiza dentro de los 30 días; la rotación de copias excluye después los datos del inventario en pocas semanas.

Las ventanas de retención concretas por generación de copia se divulgan previa solicitud justificada en el marco del derecho de auditoría (§ 9).

Anexo 3: Lista de subencargados del tratamiento

Situación a 25.05.2026.

N.º	Subencargado	Sede	Finalidad del tratamiento	Datos tratados	Certificaciones / contrato de encargo
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Alemania — centros de datos en Alemania y Finlandia (UE)	Alojamiento de la infraestructura de producción y copias de seguridad de Screenway	Todos los datos indicados en el Anexo 1; exclusivamente cifrados en reposo y en tránsito	Certificado ISO/IEC 27001 + ISO/IEC 9001; contrato de encargo de tratamiento aceptado activamente por Bergx2 GmbH; lista de subcontratistas del proveedor de alojamiento disponible públicamente en www.hetzner.com/AV/subunternehmer.pdf

Nota sobre otros proveedores de Bergx2: para su propia actividad empresarial (comunicación interna, gestión de código fuente, herramientas de ofimática y productividad), Bergx2 GmbH utiliza otros proveedores SaaS. Estos no tratan datos de clientes de la plataforma Screenway y, por tanto, no son subencargados en el sentido de este contrato. Previa solicitud justificada del cliente en el marco de su derecho de auditoría (§ 9), Bergx2 GmbH divulgará la lista completa de sus propios proveedores.

Eficacia

Este contrato se convierte, mediante su aceptación en el portal de clientes con marca de tiempo y designación de versión, en parte integrante eficaz del contrato de servicio Screenway (art. 28, apdo. 9, RGPD: por escrito, también en formato electrónico).

El registro de aceptación es archivado por Bergx2 GmbH de forma inalterable en el backend de clientes y comprende como mínimo:

- Designación de versión de este contrato (véase la tabla de versiones)
- Fecha y hora de la aceptación
- Identidad de la persona aceptante (ID de usuario de la cuenta de cliente)
- Identidad del cliente (ID de cuenta/contrato)
- Valor hash de la versión contractual aceptada (prueba criptográfica de integridad)

En caso de actualización de este contrato, el cliente recibirá una notificación en forma textual al menos 30 días antes de su entrada en vigor, así como una solicitud de reaceptación en el siguiente inicio de sesión en el portal de clientes.

Firma física o electrónica cualificada opcional: si el cliente desea una contrafirma adicional — p. ej. por requisitos internos de cumplimiento —, el contrato puede contrafirmarse físicamente o mediante firma electrónica cualificada (Reglamento eIDAS (UE) n.º 910/2014) entre las partes contratantes. En ese caso, la aportación corre a cargo del cliente. La aceptación electrónica en el portal de clientes no se ve afectada por ello y constituye por sí sola una celebración del contrato conforme al RGPD.

Versiones

Versión	Fecha
1.0	25.05.2026