Databehandleraftale (DPA) for Screenway

> Denne version er bindende og kan indgås med retsvirkning ved elektronisk accept i kundeportalen (se afsnittet »Ikrafttræden«).

Præambel

Bergx2 GmbH driver software-as-a-service-platformen Screenway til styring af digital signage. Som led i brugen af tjenesten behandler Bergx2 GmbH personoplysninger på vegne af kunden, jf. artikel 4, nr. 8, og artikel 28 i forordning (EU) 2016/679 (databeskyttelsesforordningen, GDPR). Denne aftale præciserer begge parters forpligtelser og rettigheder i henhold til artikel 28, stk. 3, i GDPR.

---

§ 1 Behandlingens genstand og varighed

(1) Genstand. Bergx2 GmbH stiller Screenway-platformen til rådighed for kunden som software-as-a-service. Som led i brugen behandler Bergx2 GmbH de personoplysninger, der er nærmere beskrevet i bilag 1, udelukkende efter kundens instrukser.

(2) Varighed. Aftalen træder i kraft ved indgåelsen af den underliggende hovedaftale (Screenway-serviceaftalen) og ophører samtidig med denne. Forpligtelserne vedrørende sletning/tilbagelevering (§ 10) og fortrolighed (§ 5, stk. 2) gælder fortsat ud over aftalens løbetid.

---

§ 2 Behandlingens art og formål

(1) Bergx2 GmbH behandler de personoplysninger, der er beskrevet i bilag 1, til følgende formål:

- Levering af Screenway-platformen som digital signage-SaaS
- Tilknytning af skærmplaceringer til kundekonti
- Visning af indhold uploadet af kunden på slutenhederne
- Autentificering af kundens medarbejdere ved login
- Levering af support, fejlanalyse og serviceovervågning

(2) Behandling til Bergx2 GmbH's egne formål (f.eks. markedsføring, profilering, salg til tredjeparter) finder ikke sted.

---

§ 3 Typer af personoplysninger og kategorier af registrerede

Konkret opregning, se bilag 1. Sammenfattende:

- Typer af oplysninger: kontooplysninger, loginoplysninger, oplysninger om skærmplaceringer, indhold uploadet af kunden (som regel ikke personoplysninger)
- Kategorier af registrerede: kundens medarbejdere (til login og kontotilknytning)

Behandling af særlige kategorier af personoplysninger i henhold til artikel 9 i GDPR finder ikke sted ved standarddrift af Screenway. Uploader kunden alligevel sådanne oplysninger, sker dette uden for de kategorier, som denne DPA omfatter, og på kundens eget ansvar.

---

§ 4 Den dataansvarliges (kundens) forpligtelser og rettigheder

(1) Instruksbeføjelse. Kunden er fortsat ansvarlig for behandlingens lovlighed (artikel 24 i GDPR). Bergx2 GmbH behandler oplysningerne udelukkende efter dokumenteret instruks fra kunden. Denne DPA gælder som generel instruks; individuelle instrukser kan gives via de kommunikationskanaler, der er fastlagt i serviceaftalen.

(2) Registrering. Bergx2 GmbH dokumenterer instruksrelevante forhold i ISMS'ets interne revisionsspor (pull request-historik, hændelsesregister, leverandørregister).

(3) Oplysningspligt. Kunden er forpligtet til at underrette de registrerede (sine medarbejdere) i henhold til artikel 13 i GDPR om Bergx2 GmbH's behandling af oplysningerne.

---

§ 5 Databehandlerens (Bergx2 GmbH's) forpligtelser

(1) Instruksbundethed. Bergx2 GmbH behandler oplysningerne udelukkende efter dokumenteret instruks fra kunden. Er en instruks efter Bergx2 GmbH's opfattelse ulovlig, underretter Bergx2 GmbH straks kunden herom (artikel 28, stk. 3, litra h, i GDPR).

(2) Fortrolighed. Bergx2 GmbH forpligter alle personer, der er beskæftiget med behandlingen, til fortrolighed, inden de påbegynder deres arbejde (artikel 28, stk. 3, litra b, i GDPR). Dette sker ved fortrolighedserklæringer (NDA) ved ansættelse eller opgaveoverdragelse og er dokumenteret i Bergx2-ISMS'et (medarbejderregister).

(3) Tekniske og organisatoriske foranstaltninger. Bergx2 GmbH træffer de TOM'er, der er beskrevet i bilag 2, og som svarer til det aktuelle tekniske niveau og sikrer et beskyttelsesniveau, der passer til risikoen (artikel 32 i GDPR).

(4) Underdatabehandlere. Bergx2 GmbH anvender de underdatabehandlere, der er opført i bilag 3. Betingelser og ændringsmekanisme, se § 6.

(5) Bistand. Bergx2 GmbH bistår kunden med opfyldelsen af dennes forpligtelser i henhold til artikel 32-36 i GDPR, navnlig ved besvarelse af anmodninger fra registrerede (§ 7) og anmeldelse af brud på persondatasikkerheden (§ 8).

(6) Dokumentation. Bergx2 GmbH stiller efter anmodning de oplysninger og dokumenter, der er nødvendige for kontrol, til rådighed for kunden (artikel 28, stk. 3, litra h, i GDPR). Øvrige revisionsbestemmelser, se § 9.

---

§ 6 Underdatabehandlere

(1) Godkendelse. Ved indgåelsen af denne DPA giver kunden generel godkendelse til anvendelsen af de underdatabehandlere, der er opført i bilag 3 (artikel 28, stk. 2, 1. pkt., i GDPR).

(2) Underretning om ændringer. Bergx2 GmbH underretter kunden om påtænkte ændringer i kredsen af underdatabehandlere (tilføjelse eller udskiftning) mindst 30 dage før ikrafttræden i tekstform (e-mail til den databeskyttelseskontaktadresse, der er angivet i serviceaftalen).

(3) Indsigelsesret. Kunden kan inden for fristen på 30 dage gøre indsigelse mod ændringen af saglige grunde. Ved indsigelse søger Bergx2 GmbH sammen med kunden en løsning i mindelighed; lykkes dette ikke, har kunden en ekstraordinær opsigelsesret til serviceaftalen.

(4) Forpligtelse. Bergx2 GmbH forpligter kontraktligt hver underdatabehandler til at overholde de forpligtelser, der er aftalt i denne DPA (artikel 28, stk. 4, i GDPR).

---

§ 7 Bistand i forbindelse med de registreredes rettigheder

Bergx2 GmbH bistår kunden gennem passende tekniske og organisatoriske foranstaltninger, så vidt muligt, med opfyldelsen af de registreredes rettigheder i henhold til kapitel III i GDPR (indsigt, berigtigelse, sletning, begrænsning, dataportabilitet, indsigelse).

Konkret: Bergx2 GmbH videresender straks sådanne anmodninger, som registrerede retter direkte til Bergx2 GmbH, til kunden og giver denne mulighed for at svare. Bergx2 GmbH besvarer kun selv anmodningerne efter udtrykkelig instruks fra kunden.

---

§ 8 Anmeldelse af brud på persondatasikkerheden

(1) Bergx2 GmbH underretter kunden uden unødig forsinkelse og senest inden for 24 timer efter at være blevet bekendt hermed om ethvert konstateret brud på persondatasikkerheden inden for Bergx2 GmbH's eller en underdatabehandlers ansvarsområde, der vedrører kundens personoplysninger.

(2) Anmeldelsen sker skriftligt (e-mail til kundens databeskyttelseskontaktadresse) og indeholder de minimumsoplysninger, der er nævnt i artikel 33, stk. 3, i GDPR (bruddets art og omfang, antal berørte registrerede, sandsynlige konsekvenser, trufne modforanstaltninger).

(3) Bergx2 GmbH dokumenterer egne brud på persondatasikkerheden internt i hændelsesregistret (se `incidents/incidents.md` i Bergx2-ISMS'et, procedure i henhold til `documents/verfahren/incident-management-verfahren.md`).

(4) Forpligtelsen til at anmelde bruddet til den kompetente tilsynsmyndighed i henhold til artikel 33 i GDPR og i givet fald til at underrette de registrerede i henhold til artikel 34 i GDPR påhviler fortsat kunden som dataansvarlig. Bergx2 GmbH bistår kunden ved disse anmeldelser med alle nødvendige oplysninger.

---

§ 9 Revisions- og kontrolrettigheder

(1) Dokumentation. Bergx2 GmbH stiller efter anmodning de oplysninger til rådighed for kunden, der er nødvendige for at påvise overholdelsen af forpligtelserne i denne DPA, navnlig den til enhver tid gældende version af TOM'erne (bilag 2) og listen over underdatabehandlere (bilag 3) samt i givet fald uddrag af certificeringer.

(2) Kontrol på stedet. Kunden har ret til på stedet at forvisse sig om overholdelsen af TOM'erne på Bergx2 GmbH's hjemsted eller på behandlingsstederne. Tidspunkter skal varsles skriftligt mindst fire uger i forvejen; kontroller skal begrænses til det nødvendige omfang og må ikke forstyrre forretningsdriften uforholdsmæssigt. Højst én kontrol pr. kalenderår, medmindre der foreligger en begrundet anledning.

(3) Anerkendelse af certificeringer. Såfremt Bergx2 GmbH er certificeret efter ISO/IEC 27001:2022 (certificering under forberedelse) eller fremlægger tilsvarende uafhængige tredjepartsrevisioner, træder dette i stedet for kundens kontrol på stedet, forudsat at certificeringens anvendelsesområde omfatter aftalens genstand.

---

§ 10 Sletning og tilbagelevering efter aftalens ophør

(1) Ved ophør af serviceaftalen vil Bergx2 GmbH – efter kundens valg – enten:

- tilbagelevere personoplysningerne fuldstændigt (eksport i et struktureret, almindeligt anvendt og maskinlæsbart format), eller
- slette personoplysningerne fuldstændigt (sikker overskrivning i henhold til det aktuelle tekniske niveau), og

dette inden for 30 dage efter aftalens ophør.

(2) Backups, der indeholder personoplysninger, overskrives i henhold til bilag 2 TOM'er, § Backup-livscyklus, som følge af rotation fuldstændigt senest efter fem uger (backup-rotation). Bergx2 GmbH dokumenterer efter anmodning den endelige sletning skriftligt.

(3) Lovbestemte opbevaringspligter berøres ikke (f.eks. faktureringsoplysninger i henhold til § 257 HGB, § 147 AO).

---

§ 11 Ansvar og afsluttende bestemmelser

(1) Ansvar. Hovedaftalens bestemmelser (Screenway-serviceaftalen) og artikel 82 i GDPR finder anvendelse. Ved overtrædelse af denne DPA hæfter den pågældende ansvarlige part over for den registrerede.

(2) Skriftlighed. Ændringer og tilføjelser kræver tekstform.

(3) Ugyldighedsklausul. Skulle enkelte bestemmelser være ugyldige, berøres de øvrige bestemmelsers gyldighed ikke.

(4) Gældende ret og værneting. Aftalen er underlagt tysk ret med undtagelse af FN's konvention om internationale køb (CISG). Værneting er München.

Bilag 1: Beskrivelse af behandlingen

Kategori	Indhold
Genstand	Levering af Screenway-SaaS-platformen inkl. hosting, dataoverførsel, autentificering og visningsstyring
Varighed	Aftalens aktive løbetid + 30 dages overgangsperiode til eksport/sletning
Behandlingens art	Indsamling, registrering, opbevaring, ændring, søgning, visning, overførsel, sletning
Formål	Levering af den kontraktligt aftalte Screenway-tjeneste
Registrerede	Kundens medarbejdere, der får tildelt login-/styringsadgang til Screenway
Kategorier af oplysninger	Kontooplysninger (navn, arbejds-e-mail, rolle), loginoplysninger (password-hash, sessionscookies, IP-adresse), oplysninger om skærmplaceringer (betegnelse, i givet fald placeringens adresse), indhold uploadet af kunden (som regel **ikke** personoplysninger – markedsføringsmateriale, informationstekster osv.)
Særlige kategorier af oplysninger (artikel 9 i GDPR)	Behandles **ikke** ved standarddrift
Hostingregion	Udelukkende Den Europæiske Union – Hetzner Nürnberg (primær) + Hetzner Helsinki (backup-spejl)
Overførsel til tredjelande	**Ingen**

Bilag 2: Tekniske og organisatoriske foranstaltninger (TOM'er)

Følgende TOM'er svarer til artikel 32 i GDPR og er kategoriseret således, som tilsynsmyndighederne og den branchesædvanlige GDPR-DPA-standard foreskriver. Foranstaltningerne dokumenteres i Bergx2's information security management system (ISMS) efter ISO/IEC 27001:2022 og føres internt i detaljeret form. Konkrete implementeringsdetaljer (producentmodeller, konfigurationsparametre, placering af enkelte komponenter, nøglemekanismer) offentliggøres af sikkerhedsmæssige grunde ikke i dette offentligt tilgængelige aftalebilag. Efter begrundet anmodning fra kunden som led i dennes revisionsret i henhold til § 9 stiller Bergx2 GmbH de relevante detaljerede dokumenter til rådighed inden for rammerne af en skriftlig fortrolighedsaftale.

1. Fortrolighed (artikel 32, stk. 1, litra b, i GDPR)

Foranstaltning	Gennemførelse
Fysisk adgangskontrol	Fysisk adgangskontrol i flere niveauer på hjemstedet med mekanisk indbrudssikring i henhold til relevante DIN-standarder, sikkerhedsglas, automatisk låsende døre, kamerabaseret forudgående adgangskontrol uden overførsel til eksterne netværk og multifaktorautentificering på det inderste låseniveau. Adgangstilladelser tildeles efter need-to-be-present-princippet til en navngivet, begrænset personkreds og dokumenteres i et ført nøgleregister med revisionsspor for udlevering/returnering. Nøglekopiering er kun mulig med udlejerens godkendelse via certificerede låsesmede. Besøgende har kun adgang til forretningslokalerne i følgeskab.
Adgangskontrol (systemer)	Rollebaseret adgangskontrol (RBAC) i alle produktionssystemer; multifaktorautentificering (MFA) for administrative adgange; bindende passwordpolitik i overensstemmelse med det aktuelle tekniske niveau; nøgle- eller certifikatbaseret serveradgang uden password; obligatorisk routing af administrative adgange via et internt virtual private network (VPN).
Adgangsstyring (data)	Adskillelse af klienter pr. kundekonto på databaseniveau; adgangsregler på postniveau (row-level security); revisionssikker logning af alle læse- og skriveadgange til personoplysninger.
Pseudonymisering	Så vidt det er foreneligt med behandlingsformålet, pseudonymiseres interne behandlinger. En periodisk stikprøvekontrol for utilsigtede forekomster af rigtige navne er etableret som KPI for informationssikkerhed.
Kryptering	Transportkryptering i overensstemmelse med det aktuelle tekniske niveau for alle eksterne forbindelser med regelmæssig certifikatrotation. Stærk kryptering af hvilende data for backupmedier og harddiske i slutenheder. Følsomme adgangsoplysninger (passwords, tokens, nøgler) administreres udelukkende i en intern procedure, der svarer til det aktuelle tekniske niveau – detaljer offentliggøres ikke af sikkerhedsmæssige grunde.

2. Integritet (artikel 32, stk. 1, litra b, i GDPR)

Foranstaltning	Gennemførelse
Inputkontrol	Serverside-validering af alle input; revisionssikre auditlogs; skriverettigheder udelukkende via autentificerede og autoriserede programmeringsgrænseflader.
Videregivelseskontrol	Obligatorisk transportkryptering for alle eksterne forbindelser; ingen videregivelse af data uden dokumenteret kontraktligt grundlag.
Opgavekontrol	Databehandleraftaler med alle underdatabehandlere (se bilag 3); struktureret proces for leverandørstyring med periodisk revurdering.

3. Tilgængelighed og robusthed (artikel 32, stk. 1, litra b, i GDPR)

Foranstaltning	Gennemførelse
Backup	Daglig inkrementel backup af produktionssystemerne med geografisk adskilt spejling **inden for Den Europæiske Union**; flere versioner opbevares; planlagte gendannelsestest hvert kvartal.
Tilgængelighed	Cloud first-arkitektur med hosting i ISO/IEC 27001-certificerede datacentre med nødstrømsreserve; løbende overvågning med definerede eskaleringsveje.
Business continuity	Testet business continuity-plan inklusive business impact-analyse; fuld mulighed for hjemmearbejde for de videnbaserede funktioner; dokumenterede genstartstider pr. system.
Slutenheders robusthed	Reserveenhed ved enhedsfejl; tilstrækkelig batterikapacitet ved kortvarige strømafbrydelser.

4. Procedurer for regelmæssig afprøvning, vurdering og evaluering (artikel 32, stk. 1, litra d, i GDPR)

Foranstaltning	Gennemførelse
Information security management system (ISMS)	Etableret ISMS efter ISO/IEC 27001:2022 med statement of applicability for Annex A-kontrollerne; certificering under forberedelse.
Databeskyttelsesstyring	Ført fortegnelse over behandlingsaktiviteter; udpeget databeskyttelsesrådgiver; periodiske gennemgange af behandlingsaktiviteterne.
Awareness	Strukturerede og dokumenterede awareness- og databeskyttelseskurser for alle medarbejdere med rollespecifikke obligatoriske moduler.
Risikostyring	Risikovurdering mindst én gang årligt med godkendelse fra topledelsen; risikohåndteringsplan med tilknyttede foranstaltninger.
Leverandørstyring	Bindende leverandørpolitik og -procedure; krav om DPA for alle databehandlere; periodiske leverandørgennemgange.
Incident response	Dokumenteret procedure for hændelseshåndtering med definerede rapporteringsveje, eskaleringsniveauer og verifikation af effektivitet.
Patch management	Ført patchregister med sporbar anvendelse af patches.
Management review	Evaluering mindst én gang årligt af topledelsen på grundlag af kvantitative KPI'er.
Intern audit	Årlig uafhængig intern ISMS-audit med dokumenterede fund og korrigerende handlinger.

5. Backup-livscyklus og sletning

Personoplysninger i backups overskrives fuldstændigt inden for få uger gennem den definerede backup-rotation.

Ved aftalens ophør sker den endelige sletning af data i produktionssystemerne inden for 30 dage; backup-rotationen fjerner derefter dataene fra beholdningen inden for få uger.

Konkrete opbevaringsperioder pr. backupgeneration oplyses efter begrundet anmodning som led i revisionsretten (§ 9).

Bilag 3: Liste over underdatabehandlere

Status: 25.05.2026.

Nr.	Underdatabehandler	Hjemsted	Behandlingsformål	Behandlede oplysninger	Certificeringer / DPA
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Tyskland – datacentre i Tyskland og Finland (EU)	Hosting af Screenways produktions- og backupinfrastruktur	Alle oplysninger nævnt i bilag 1; udelukkende krypteret at rest og in transit	ISO/IEC 27001 + ISO/IEC 9001-certificeret; databehandleraftale aktivt accepteret af Bergx2 GmbH; hostingudbyderens liste over underleverandører offentligt tilgængelig på www.hetzner.com/AV/subunternehmer.pdf

Bemærkning om øvrige Bergx2-leverandører: Bergx2 GmbH anvender til sin egen forretningsdrift (medarbejderkommunikation, kildekodestyring, kontor- og produktivitetsværktøjer) yderligere SaaS-udbydere. Disse behandler ingen kundedata fra Screenway-platformen og er derfor ikke underdatabehandlere i henhold til denne DPA. Efter begrundet anmodning fra kunden som led i dennes revisionsret (§ 9) offentliggør Bergx2 GmbH den fuldstændige liste over sine egne leverandører.

Ikrafttræden

Denne DPA bliver ved accept i kundeportalen med tidsstempel og versionsbetegnelse en gyldig del af Screenway-serviceaftalen (artikel 28, stk. 9, i GDPR: skriftligt, herunder i elektronisk form).

Acceptposten arkiveres revisionssikkert af Bergx2 GmbH i kunde-backend og omfatter mindst:

- Versionsbetegnelse for denne DPA (se versionstabellen nedenfor)
- Dato og klokkeslæt for accepten
- Identiteten på den accepterende person (bruger-id for kundekontoen)
- Kundens identitet (konto-/aftale-id)
- Hashværdi for den accepterede aftaleversion (kryptografisk integritetsbevis)

Ved en opdatering af denne DPA modtager kunden mindst 30 dage før ikrafttræden en underretning i tekstform samt ved næste login i kundeportalen en opfordring til fornyet accept.

Valgfri fysisk eller kvalificeret elektronisk signatur: Såfremt kunden – f.eks. på grund af interne compliancekrav – ønsker en yderligere kontrasignatur, kan DPA'en kontrasigneres fysisk eller ved hjælp af kvalificeret elektronisk signatur (eIDAS-forordningen (EU) nr. 910/2014) mellem aftaleparterne. Fremskaffelsen påhviler i så fald kunden. Den elektroniske accept i kundeportalen berøres ikke heraf og udgør i sig selv en GDPR-konform aftaleindgåelse.

Versionsstyring

Version	Status
1.0	25.05.2026