> Merk: Den bindende versjonen av denne databehandleravtalen er den tyske originalen, som er tilgjengelig på `/rechtliches/avv`. Denne norske oversettelsen er kun ment som informasjon. Ved avvik har den tyske versjonen forrang.

Databehandleravtale (DPA) for Screenway

> Denne versjonen er bindende og kan inngås med rettsvirkning ved elektronisk aksept i kundeportalen (se avsnittet «Ikrafttredelse»).

Innledning

Bergx2 GmbH driver Screenway, en software-as-a-service-plattform for styring av digital skilting. I forbindelse med bruken av tjenesten behandler Bergx2 GmbH personopplysninger på vegne av kunden i henhold til artikkel 4 nr. 8 og artikkel 28 i forordning (EU) 2016/679, personvernforordningen (GDPR). Denne avtalen presiserer begge parters plikter og rettigheter etter artikkel 28 nr. 3 i GDPR.

---

§ 1 Behandlingens gjenstand og varighet

(1) Gjenstand. Bergx2 GmbH stiller Screenway-plattformen til rådighet for kunden som software-as-a-service. I forbindelse med bruken behandler Bergx2 GmbH kundens personopplysninger, som er nærmere beskrevet i vedlegg 1, utelukkende etter kundens instrukser.

(2) Varighet. Avtalen trer i kraft ved inngåelsen av den underliggende hovedavtalen (Screenway-tjenesteavtalen) og opphører når denne opphører. Pliktene knyttet til sletting/tilbakelevering (§ 10) og taushetsplikt (§ 5 (2)) gjelder også etter at avtaleperioden er utløpt.

---

§ 2 Behandlingens art og formål

(1) Bergx2 GmbH behandler personopplysningene som er beskrevet i vedlegg 1, for følgende formål:

- Levering av Screenway-plattformen som SaaS for digital skilting
- Tilordning av skjermplasseringer til kundekontoer
- Visning av innhold som kunden har lastet opp, på sluttenhetene
- Autentisering av kundens ansatte ved innlogging
- Levering av brukerstøtte, feilanalyse og tjenesteovervåking

(2) Behandling for Bergx2 GmbHs egne formål (f.eks. markedsføring, profilering, salg til tredjeparter) finner ikke sted.

---

§ 3 Typer personopplysninger og kategorier av registrerte

Konkret oversikt, se vedlegg 1. Oppsummert:

- Typer opplysninger: kontoopplysninger, innloggingsopplysninger, opplysninger om skjermplasseringer, innhold lastet opp av kunden (som regel ikke personopplysninger)
- Kategorier av registrerte: kundens ansatte (for innlogging og kontotilordning)

Behandling av særlige kategorier av personopplysninger etter artikkel 9 i GDPR finner ikke sted ved standard drift av Screenway. Dersom kunden likevel laster opp slike opplysninger, skjer dette utenfor kategoriene som omfattes av denne databehandleravtalen, og på kundens eget ansvar.

---

§ 4 Den behandlingsansvarliges (kundens) plikter og rettigheter

(1) Instruksjonsrett. Kunden er fortsatt ansvarlig for at behandlingen er lovlig (artikkel 24 i GDPR). Bergx2 GmbH behandler opplysningene utelukkende etter dokumenterte instrukser fra kunden. Denne databehandleravtalen gjelder som generell instruks; individuelle instrukser kan gis via kommunikasjonskanalene som er fastsatt i tjenesteavtalen.

(2) Registrering. Bergx2 GmbH dokumenterer forhold som er relevante for instruksene, i det interne revisjonssporet i ISMS-et (pull request-historikk, hendelsesregister, leverandørregister).

(3) Informasjonsplikt. Kunden er forpliktet til å informere de registrerte (sine ansatte) i samsvar med artikkel 13 i GDPR om Bergx2 GmbHs behandling av opplysningene.

---

§ 5 Databehandlerens (Bergx2 GmbHs) plikter

(1) Instruksbundethet. Bergx2 GmbH behandler opplysningene utelukkende etter dokumenterte instrukser fra kunden. Dersom en instruks etter Bergx2 GmbHs vurdering er ulovlig, vil Bergx2 GmbH umiddelbart informere kunden (artikkel 28 nr. 3 bokstav h i GDPR).

(2) Taushetsplikt. Bergx2 GmbH pålegger alle personer som er involvert i behandlingen, taushetsplikt før de begynner arbeidet (artikkel 28 nr. 3 bokstav b i GDPR). Dette skjer gjennom taushetserklæringer (NDA) ved ansettelse eller oppdragsinngåelse og er dokumentert i Bergx2-ISMS-et (medarbeiderregister).

(3) Tekniske og organisatoriske tiltak. Bergx2 GmbH gjennomfører de tekniske og organisatoriske tiltakene (TOM) som er beskrevet i vedlegg 2, som er i samsvar med den tekniske utviklingen og sikrer et beskyttelsesnivå som er tilpasset risikoen (artikkel 32 i GDPR).

(4) Underdatabehandlere. Bergx2 GmbH benytter underdatabehandlerne som er oppført i vedlegg 3. Vilkår og endringsmekanisme, se § 6.

(5) Bistand. Bergx2 GmbH bistår kunden med å oppfylle kundens plikter etter artikkel 32–36 i GDPR, særlig ved besvarelse av henvendelser fra registrerte (§ 7) og melding av brudd på personopplysningssikkerheten (§ 8).

(6) Dokumentasjon. Bergx2 GmbH stiller på forespørsel den informasjonen og de dokumentene som er nødvendige for kontroll, til rådighet for kunden (artikkel 28 nr. 3 bokstav h i GDPR). Øvrige revisjonsvilkår, se § 9.

---

§ 6 Underdatabehandlere

(1) Godkjenning. Ved inngåelsen av denne databehandleravtalen gir kunden generell godkjenning til bruk av underdatabehandlerne som er oppført i vedlegg 3 (artikkel 28 nr. 2 første punktum i GDPR).

(2) Varsling om endringer. Bergx2 GmbH varsler kunden om planlagte endringer i bruken av underdatabehandlere (tillegg eller utskifting) minst 30 dager før endringen trer i kraft, i tekstform (e-post til personvernkontaktadressen som er registrert i tjenesteavtalen).

(3) Rett til å protestere. Kunden kan innen fristen på 30 dager protestere mot endringen av saklige grunner. Ved protest søker Bergx2 GmbH sammen med kunden en løsning i minnelighet; lykkes ikke dette, har kunden rett til ekstraordinær oppsigelse av tjenesteavtalen.

(4) Forpliktelse. Bergx2 GmbH forplikter på sin side hver underdatabehandler kontraktsmessig til å overholde pliktene som er avtalt i denne databehandleravtalen (artikkel 28 nr. 4 i GDPR).

---

§ 7 Bistand ved de registrertes rettigheter

Bergx2 GmbH bistår kunden, så langt det er mulig, gjennom egnede tekniske og organisatoriske tiltak med å oppfylle de registrertes rettigheter etter kapittel III i GDPR (innsyn, retting, sletting, begrensning, dataportabilitet, protest).

Konkret: Bergx2 GmbH videresender uten opphold henvendelser som registrerte retter direkte til Bergx2 GmbH, til kunden og gir kunden mulighet til å svare. Bergx2 GmbH besvarer bare henvendelsene selv etter uttrykkelig instruks fra kunden.

§ 8 Melding av brudd på personopplysningssikkerheten

(1) Bergx2 GmbH informerer kunden uten ugrunnet opphold, senest innen 24 timer etter å ha fått kjennskap til det, om ethvert konstatert brudd på personopplysningssikkerheten innenfor ansvarsområdet til Bergx2 GmbH eller en underdatabehandler som berører kundens personopplysninger.

(2) Meldingen gis skriftlig (e-post til kundens personvernkontaktadresse) og inneholder minimumsopplysningene nevnt i artikkel 33 nr. 3 i GDPR (bruddets art og omfang, antall berørte registrerte, sannsynlige konsekvenser, iverksatte mottiltak).

(3) Bergx2 GmbH dokumenterer egne brudd på personopplysningssikkerheten internt i hendelsesregisteret (se `incidents/incidents.md` i Bergx2-ISMS-et, prosedyre i henhold til `documents/verfahren/incident-management-verfahren.md`).

(4) Plikten til å melde bruddet til den kompetente tilsynsmyndigheten etter artikkel 33 i GDPR og eventuelt til å underrette de registrerte etter artikkel 34 i GDPR ligger fortsatt hos kunden som behandlingsansvarlig. Bergx2 GmbH bistår kunden ved disse meldingene med all nødvendig informasjon.

---

§ 9 Revisjons- og kontrollrettigheter

(1) Dokumentasjon. Bergx2 GmbH stiller på forespørsel den informasjonen som er nødvendig for å oppfylle pliktene etter denne databehandleravtalen, til rådighet for kunden, særlig den til enhver tid gjeldende versjonen av TOM-ene (vedlegg 2) og listen over underdatabehandlere (vedlegg 3) samt eventuelt utdrag fra sertifiseringer.

(2) Kontroll på stedet. Kunden har rett til på stedet å forvisse seg om at TOM-ene overholdes, ved Bergx2 GmbHs forretningsadresse eller på behandlingsstedene. Tidspunkter skal varsles skriftlig minst fire uker i forveien; kontroller skal begrenses til det nødvendige omfanget og må ikke forstyrre forretningsdriften uforholdsmessig. Høyst én kontroll per kalenderår, med mindre det foreligger en begrunnet foranledning.

(3) Anerkjennelse av sertifiseringer. Dersom Bergx2 GmbH er sertifisert etter ISO/IEC 27001:2022 (sertifisering under forberedelse) eller legger fram likeverdige uavhengige tredjepartsrevisjoner, erstatter dette kundens kontroll på stedet, forutsatt at sertifiseringens omfang også dekker avtalens gjenstand.

---

§ 10 Sletting og tilbakelevering etter avtalens opphør

(1) Ved opphør av tjenesteavtalen vil Bergx2 GmbH – etter kundens valg – enten:

- tilbakelevere personopplysningene i sin helhet (eksport i et strukturert, alminnelig brukt og maskinlesbart format), eller
- slette personopplysningene fullstendig (sikker overskriving i samsvar med den tekniske utviklingen), og

gjøre dette innen 30 dager etter avtalens opphør.

(2) Sikkerhetskopier som inneholder personopplysninger, blir i samsvar med vedlegg 2 TOM, § Livssyklus for sikkerhetskopier, fullstendig overskrevet som følge av rotasjon senest etter fem uker (backup-rotasjon). Bergx2 GmbH dokumenterer den endelige slettingen skriftlig på forespørsel.

(3) Lovpålagte oppbevaringsplikter berøres ikke (f.eks. faktureringsopplysninger i henhold til § 257 HGB, § 147 AO).

---

§ 11 Ansvar og avsluttende bestemmelser

(1) Ansvar. Bestemmelsene i hovedavtalen (Screenway-tjenesteavtalen) og artikkel 82 i GDPR gjelder. Ved brudd på denne databehandleravtalen er den parten som er ansvarlig i det enkelte tilfellet, ansvarlig overfor den registrerte.

(2) Skriftlighet. Endringer og tillegg krever tekstform.

(3) Delvis ugyldighet. Dersom enkelte bestemmelser skulle være ugyldige, berøres ikke gyldigheten av de øvrige bestemmelsene.

(4) Lovvalg og verneting. Avtalen er underlagt tysk rett, med unntak av FN-konvensjonen om kontrakter for internasjonale løsørekjøp (CISG). Verneting er München.

Vedlegg 1: Beskrivelse av behandlingen

Kategori	Innhold
Gjenstand	Levering av Screenway-SaaS-plattformen inkl. hosting, dataoverføring, autentisering og visningsstyring
Varighet	Aktiv avtaleperiode + 30 dagers overgangsperiode for eksport/sletting
Behandlingens art	Innsamling, registrering, lagring, endring, søk, visning, overføring, sletting
Formål	Levering av den avtalte Screenway-tjenesten
Registrerte	Kundens ansatte som får tildelt innloggings- og styringstilgang til Screenway
Opplysningskategorier	Kontoopplysninger (navn, e-postadresse på jobb, rolle), innloggingsopplysninger (passord-hash, sesjonscookies, IP-adresse), opplysninger om skjermplasseringer (betegnelse, eventuelt stedets adresse), innhold lastet opp av kunden (som regel **ikke** personopplysninger – markedsføringsmateriell, informasjonstekster osv.)
Særlige kategorier av personopplysninger (artikkel 9 i GDPR)	Behandles **ikke** ved standard drift
Hostingregion	Utelukkende Den europeiske union – Hetzner Nürnberg (primær) + Hetzner Helsinki (backup-speil)
Overføring til tredjeland	**Ingen**

Vedlegg 2: Tekniske og organisatoriske tiltak (TOM)

De følgende TOM-ene er i samsvar med artikkel 32 i GDPR og er kategorisert slik tilsynsmyndighetene og den bransjevanlige standarden for databehandleravtaler etter GDPR foreskriver. Tiltakene dokumenteres i Bergx2s styringssystem for informasjonssikkerhet (ISMS) etter ISO/IEC 27001:2022 og føres internt i detalj. Konkrete implementeringsdetaljer (produsentmodeller, konfigurasjonsparametere, plassering av enkelte komponenter, nøkkelmekanismer) offentliggjøres av sikkerhetshensyn ikke i dette offentlig tilgjengelige avtalevedlegget. Etter begrunnet forespørsel fra kunden innenfor rammen av kundens revisjonsrett etter § 9 stiller Bergx2 GmbH de relevante detaljerte dokumentene til rådighet innenfor rammen av en skriftlig taushetsavtale.

1. Konfidensialitet (artikkel 32 nr. 1 bokstav b i GDPR)

Tiltak	Gjennomføring
Fysisk adgangskontroll	Fysisk adgangskontroll i flere nivåer ved forretningsadressen med mekanisk innbruddssikring i henhold til relevante DIN-standarder, sikkerhetsglass, automatisk låsende dører, kamerabasert forhåndskontroll av adgang uten overføring til eksterne nettverk og flerfaktorautentisering på det innerste låsenivået. Adgangstillatelser tildeles etter need-to-be-present-prinsippet til en navngitt, begrenset personkrets og dokumenteres i et ført nøkkelregister med revisjonsspor for utlevering og innlevering. Kopiering av nøkler er bare mulig med utleiers godkjenning via sertifiserte låsesmeder. Besøkende har bare adgang til forretningslokalene i følge med ansatte.
Tilgangskontroll (systemer)	Rollebasert tilgangskontroll (RBAC) i alle produksjonssystemer; flerfaktorautentisering (MFA) for administrative tilganger; bindende passordpolicy i samsvar med den tekniske utviklingen; nøkkel- eller sertifikatbasert servertilgang uten passord; obligatorisk ruting av administrative tilganger via et internt virtuelt privat nettverk (VPN).
Tilgangsstyring (data)	Atskillelse av klienter per kundekonto på databasenivå; tilgangsregler på radnivå (row-level security); revisjonssikker logging av alle lese- og skrivetilganger til personopplysninger.
Pseudonymisering	Så langt det er forenlig med behandlingsformålet, pseudonymiseres interne behandlinger. En periodisk stikkprøvekontroll for utilsiktede forekomster av ekte navn er etablert som KPI for informasjonssikkerhet.
Kryptering	Transportkryptering i samsvar med den tekniske utviklingen for alle eksterne forbindelser med regelmessig sertifikatrotasjon. Sterk kryptering av lagrede data for sikkerhetskopimedier og harddisker i sluttenheter. Sensitive tilgangsopplysninger (passord, tokens, nøkler) forvaltes utelukkende i en intern prosedyre som er i samsvar med den tekniske utviklingen – detaljer offentliggjøres ikke av sikkerhetshensyn.

2. Integritet (artikkel 32 nr. 1 bokstav b i GDPR)

Tiltak	Gjennomføring
Inndatakontroll	Validering av alle inndata på serversiden; revisjonssikre revisjonslogger; skriverettigheter utelukkende via autentiserte og autoriserte programmeringsgrensesnitt.
Overføringskontroll	Obligatorisk transportkryptering for alle eksterne forbindelser; ingen videreformidling av data uten dokumentert avtalemessig grunnlag.
Oppdragskontroll	Databehandleravtaler med alle underdatabehandlere (se vedlegg 3); strukturert prosess for leverandørstyring med periodisk ny vurdering.

3. Tilgjengelighet og robusthet (artikkel 32 nr. 1 bokstav b i GDPR)

Tiltak	Gjennomføring
Sikkerhetskopiering	Daglig inkrementell sikkerhetskopiering av produksjonssystemene med geografisk atskilt speiling **innenfor Den europeiske union**; flere versjoner oppbevares; planlagte gjenopprettingstester hvert kvartal.
Tilgjengelighet	Cloud first-arkitektur med hosting i ISO/IEC 27001-sertifiserte datasentre med nødstrømsreserve; kontinuerlig overvåking med definerte eskaleringsveier.
Kontinuitet (business continuity)	Testet kontinuitetsplan inkludert konsekvensanalyse for virksomheten (business impact analysis); full mulighet for hjemmekontor for de kunnskapsbaserte funksjonene; dokumenterte gjenopprettingstider per system.
Sluttenheters robusthet	Reserveenhet ved enhetsfeil; tilstrekkelige batterireserver ved kortvarige strømbrudd.

4. Prosedyrer for regelmessig testing, vurdering og evaluering (artikkel 32 nr. 1 bokstav d i GDPR)

Tiltak	Gjennomføring
Styringssystem for informasjonssikkerhet (ISMS)	Etablert ISMS etter ISO/IEC 27001:2022 med Statement of Applicability for kontrollene i Annex A; sertifisering under forberedelse.
Personvernstyring	Ført protokoll over behandlingsaktiviteter; oppnevnt personvernombud; periodiske gjennomganger av behandlingsaktivitetene.
Bevisstgjøring (awareness)	Strukturert og dokumentert opplæring i informasjonssikkerhet og personvern for alle ansatte med obligatoriske rollespesifikke moduler.
Risikostyring	Risikovurdering minst én gang i året med godkjenning fra toppledelsen; plan for risikohåndtering med tilordnede tiltak.
Leverandørstyring	Bindende leverandørpolicy og -prosedyre; krav om databehandleravtale for alle databehandlere; periodiske leverandørgjennomganger.
Hendelseshåndtering (incident response)	Dokumentert prosedyre for hendelseshåndtering med definerte rapporteringsveier, eskaleringsnivåer og verifisering av effektivitet.
Patchhåndtering	Ført patchregister med sporbar installasjon av patcher.
Ledelsens gjennomgang (management review)	Evaluering minst én gang i året av toppledelsen på grunnlag av kvantitative KPI-er.
Internrevisjon	Årlig uavhengig intern ISMS-revisjon med dokumenterte funn og korrigerende tiltak.

5. Livssyklus for sikkerhetskopier og sletting

Personopplysninger i sikkerhetskopier blir fullstendig overskrevet innen få uker gjennom den definerte backup-rotasjonen.

Ved avtalens opphør skjer den endelige slettingen av data i produksjonssystemene innen 30 dager; backup-rotasjonen fjerner deretter dataene fra beholdningen innen få uker.

Konkrete oppbevaringsperioder per generasjon av sikkerhetskopier gjøres kjent etter begrunnet forespørsel innenfor rammen av revisjonsretten (§ 9).

Vedlegg 3: Liste over underdatabehandlere

Per 25.05.2026.

Nr.	Underdatabehandler	Forretningsadresse	Behandlingsformål	Behandlede opplysninger	Sertifiseringer / databehandleravtale
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Tyskland – datasentre i Tyskland og Finland (EU)	Hosting av Screenways produksjons- og backupinfrastruktur	Alle opplysninger nevnt i vedlegg 1; utelukkende kryptert ved lagring og under overføring (at rest og in transit)	ISO/IEC 27001 + ISO/IEC 9001-sertifisert; databehandleravtale aktivt akseptert av Bergx2 GmbH; vertsleverandørens liste over underleverandører er offentlig tilgjengelig på www.hetzner.com/AV/subunternehmer.pdf

Merknad om andre leverandører til Bergx2: Bergx2 GmbH bruker andre SaaS-leverandører for sin egen forretningsdrift (kommunikasjon mellom ansatte, kildekodeforvaltning, kontor- og produktivitetsverktøy). Disse behandler ingen kundedata fra Screenway-plattformen og er derfor ikke underdatabehandlere i henhold til denne databehandleravtalen. Etter begrunnet

forespørsel fra kunden innenfor rammen av kundens revisjonsrett (§ 9) vil Bergx2 GmbH gjøre den fullstendige listen over egne leverandører kjent.

Ikrafttredelse

Denne databehandleravtalen blir ved aksept i kundeportalen med tidsstempel og versjonsbetegnelse en gyldig del av Screenway-tjenesteavtalen (artikkel 28 nr. 9 i GDPR: skriftlig, herunder i elektronisk form).

Akseptposten arkiveres revisjonssikkert av Bergx2 GmbH i kundebackend og omfatter minst:

- Versjonsbetegnelsen for denne databehandleravtalen (se versjonstabellen nedenfor)
- Dato og klokkeslett for aksepten
- Identiteten til personen som aksepterer (bruker-ID i kundekontoen)
- Kundens identitet (konto-/avtale-ID)
- Hashverdi for den aksepterte avtaleversjonen (kryptografisk integritetsbevis)

Ved en oppdatering av denne databehandleravtalen mottar kunden et varsel i tekstform minst 30 dager før endringen trer i kraft, og ved neste innlogging i kundeportalen en oppfordring til ny aksept.

Valgfri fysisk eller kvalifisert elektronisk signatur: Dersom kunden – f.eks. på grunn av interne compliancekrav – ønsker en ytterligere kontrasignatur, kan databehandleravtalen kontrasigneres fysisk eller ved hjelp av kvalifisert elektronisk signatur (eIDAS-forordningen (EU) nr. 910/2014) mellom avtalepartene. I så fall er det kunden som sørger for dette. Den elektroniske aksepten i kundeportalen berøres ikke av dette og utgjør i seg selv en avtaleinngåelse i samsvar med GDPR.

Versjonering

Versjon	Dato
1.0	25.05.2026