

Verwerkersovereenkomst (DPA) voor Screenway

Deze versie is bindend en kan door elektronische aanvaarding in het klantenportaal rechtsgeldig worden gesloten (zie het onderdeel "Inwerkingtreding").

Preamble

Bergx2 GmbH exploiteert het software-as-a-serviceplatform Screenway voor de aansturing van digital signage. In het kader van het gebruik van de dienst verwerkt Bergx2 GmbH persoonsgegevens in opdracht van de klant in de zin van art. 4 punt 8 en art. 28 van Verordening (EU) 2016/679 (Algemene verordening gegevensbescherming, AVG). Deze overeenkomst geeft nadere invulling aan de verplichtingen en rechten van beide partijen op grond van art. 28 lid 3 AVG.

§ 1 Onderwerp en duur van de verwerking

(1) Onderwerp. Bergx2 GmbH stelt het Screenway-platform als software-as-a-service ter beschikking van de klant. In het kader van het gebruik verwerkt Bergx2 GmbH de in bijlage 1 nader beschreven persoonsgegevens van de klant uitsluitend volgens diens instructies.

(2) Duur. De overeenkomst treedt in werking bij het sluiten van de onderliggende hoofdovereenkomst (Screenway-serviceovereenkomst) en eindigt bij de beëindiging daarvan. De verplichtingen tot wissing/teruggave (§ 10) en tot geheimhouding (§ 5 lid 2) blijven ook na afloop van de looptijd van de overeenkomst van kracht.

§ 2 Aard en doel van de verwerking

(1) Bergx2 GmbH verwerkt de in bijlage 1 beschreven persoonsgegevens voor de volgende doeleinden:

- Beschikbaarstelling van het Screenway-platform als SaaS voor digital signage
- Koppeling van schermlocaties aan klantaccounts
- Weergave van de door de klant geüploade content op de eindapparaten
- Authenticatie van medewerkers van de klant bij het inloggen
- Verlening van support, foutanalyse en servicemonitoring

(2) Een verwerking voor eigen doeleinden van Bergx2 GmbH (bijv. marketing, profilering, verkoop aan derden) vindt niet plaats.

§ 3 Soort persoonsgegevens en categorieën van betrokkenen

Zie bijlage 1 voor een concrete opsomming. Samengevat:

- Soort gegevens: accountgegevens, inloggegevens, gegevens over schermlocaties, door de klant geüploade content (doorgaans geen persoonsgegevens)
- Categorieën van betrokkenen: medewerkers van de klant (voor het inloggen en de koppeling aan accounts)

De verwerking van bijzondere categorieën van persoonsgegevens in de zin van art. 9 AVG vindt bij het standaardgebruik van Screenway niet plaats. Indien de klant dergelijke gegevens toch uploadt, gebeurt dit buiten de door deze DPA geregelde categorieën en op eigen verantwoordelijkheid van de klant.

§ 4 Verplichtingen en rechten van de verwerkingsverantwoordelijke (klant)

(1) Instructierecht. De klant blijft verantwoordelijk voor de rechtmatigheid van de verwerking (art. 24 AVG). Bergx2 GmbH verwerkt de gegevens uitsluitend op basis van gedocumenteerde instructies van de klant. Deze DPA geldt als algemene instructie; individuele instructies kunnen worden gegeven via de in de serviceovereenkomst vastgelegde communicatiekanalen.

(2) Vastlegging. Bergx2 GmbH documenteert voor instructies relevante handelingen in de interne audittrail van het ISMS (pull-requestgeschiedenis, incidentregister, leveranciersregister).

(3) Informatieplicht. De klant is verplicht de betrokkenen (zijn medewerkers) overeenkomstig art. 13 AVG te informeren over de gegevensverwerking door Bergx2 GmbH.

§ 5 Verplichtingen van de verwerker (Bergx2 GmbH)

(1) Gebondenheid aan instructies. Bergx2 GmbH verwerkt de gegevens uitsluitend op basis van gedocumenteerde instructies van de klant. Indien een instructie naar het oordeel van Bergx2 GmbH onrechtmatig is, stelt Bergx2 GmbH de klant daarvan onverwijld in kennis (art. 28 lid 3 onder h AVG).

(2) Geheimhouding. Bergx2 GmbH verplicht alle bij de verwerking betrokken personen vóór aanvang van hun werkzaamheden tot geheimhouding (art. 28 lid 3 onder b AVG). Dit gebeurt door middel van geheimhoudingsverklaringen (NDA) bij indiensttreding respectievelijk opdrachtverlening en wordt in het ISMS van Bergx2 (medewerkersregister) gedocumenteerd.

(3) Technische en organisatorische maatregelen. Bergx2 GmbH treft de in bijlage 2 beschreven TOM's, die in overeenstemming zijn met de stand van de techniek en een op het risico afgestemd beveiligingsniveau waarborgen (art. 32 AVG).

(4) Subverwerkers. Bergx2 GmbH schakelt de in bijlage 3 vermelde subverwerkers in. Zie § 6 voor de voorwaarden en het wijzigingsmechanisme.

(5) Bijstand. Bergx2 GmbH staat de klant bij in het nakomen van zijn verplichtingen op grond van art. 32–36 AVG, in het bijzonder bij de beantwoording van verzoeken van betrokkenen (§ 7) en de melding van inbreuken in verband met persoonsgegevens (§ 8).

(6) Bewijsstukken. Bergx2 GmbH stelt de klant op verzoek de voor controle benodigde informatie en documenten ter beschikking (art. 28 lid 3 onder h AVG). Zie § 9 voor verdere auditmodaliteiten.

§ 6 Subverwerkers

(1) Toestemming. Met het sluiten van deze DPA verleent de klant algemene toestemming voor de inschakeling van de in bijlage 3 vermelde subverwerkers (art. 28 lid 2, eerste zin, AVG).

(2) Kennisgeving van wijzigingen. Bergx2 GmbH informeert de klant over voorgenomen wijzigingen in de lijst van subverwerkers (toevoeging of vervanging) ten minste 30 dagen vóór de inwerkingtreding in tekstvorm (e-

mail aan het in de serviceovereenkomst vastgelegde contactadres voor gegevensbescherming).

(3) Recht van bezwaar. De klant kan binnen de termijn van 30 dagen om gegronde redenen bezwaar maken tegen de wijziging. Bij bezwaar zoekt Bergx2 GmbH samen met de klant naar een oplossing in onderling overleg; lukt dat niet, dan heeft de klant het recht de serviceovereenkomst tussentijds op te zeggen.

(4) Verplichting. Bergx2 GmbH legt elke subverwerker op zijn beurt contractueel de in deze DPA overeengekomen verplichtingen op (art. 28 lid 4 AVG).

§ 7 Medewerking bij de rechten van betrokkenen

Bergx2 GmbH staat de klant met passende technische en organisatorische maatregelen, voor zover mogelijk, bij in het nakomen van de rechten van betrokkenen op grond van hoofdstuk III van de AVG (inzage, rectificatie, wissing, beperking, overdraagbaarheid van gegevens, bezwaar).

Concreet: Bergx2 GmbH stuurt dergelijke verzoeken die betrokkenen rechtstreeks aan Bergx2 GmbH richten, onverwijld door aan de klant en geeft deze de gelegenheid om te antwoorden. Bergx2 GmbH beantwoordt verzoeken alleen zelf op uitdrukkelijke instructie van de klant.

§ 8 Melding van inbreuken in verband met persoonsgegevens

(1) Bergx2 GmbH informeert de klant onverwijld, uiterlijk binnen 24 uur nadat zij er kennis van heeft genomen, over elke vastgestelde inbreuk in verband met persoonsgegevens binnen het verantwoordelijkheidsgebied van Bergx2 GmbH of van een subverwerker, die persoonsgegevens van de klant betreft.

(2) De melding geschiedt schriftelijk (e-mail aan het contactadres voor gegevensbescherming van de klant) en bevat de in art. 33 lid 3 AVG genoemde minimale gegevens (aard en omvang van de inbreuk, aantal betrokkenen, waarschijnlijke gevolgen, genomen tegenmaatregelen).

(3) Bergx2 GmbH documenteert eigen inbreuken in verband met persoonsgegevens intern in het incidentregister (zie `incidents/incidents.md` van het ISMS van Bergx2, procedure volgens `documents/verfahren/incident-management-verfahren.md`).

(4) De verplichting tot melding aan de bevoegde toezichthoudende autoriteit op grond van art. 33 AVG en in voorkomend geval aan de betrokkenen op grond van art. 34 AVG blijft bij de klant als verwerkingsverantwoordelijke. Bergx2 GmbH staat de klant bij deze meldingen bij met alle benodigde informatie.

§ 9 Audit- en controlerechten

(1) Bewijsvoering. Bergx2 GmbH stelt de klant op verzoek de informatie ter beschikking die nodig is om de verplichtingen uit deze DPA na te komen, in het bijzonder de meest actuele versie van de TOM's (bijlage 2) en de lijst van subverwerkers (bijlage 3), alsmede in voorkomend geval uittreksels uit certificeringen.

(2) Controle ter plaatse. De klant heeft het recht zich ter plaatse, op de vestigingslocatie van Bergx2 GmbH of op de verwerkingslocaties, te vergewissen van de naleving van de TOM's. Afspraken moeten ten minste vier weken van tevoren schriftelijk worden aangekondigd; controles worden beperkt tot het noodzakelijke en mogen de bedrijfsvoering niet onevenredig verstoren. Ten hoogste één controle per kalenderjaar, behalve bij gegronde aanleiding.

(3) Erkenning van certificeringen. Voor zover Bergx2 GmbH volgens ISO/IEC 27001:2022 gecertificeerd is (certificering in voorbereiding) of gelijkwaardige onafhankelijke controles door derden overlegt, vervangt dit de controle ter plaatse door de klant, mits het toepassingsgebied van de certificering het onderwerp van de overeenkomst mede omvat.

§ 10 Wissing en teruggave na afloop van de overeenkomst

(1) Bij beëindiging van de serviceovereenkomst zal Bergx2 GmbH – naar keuze van de klant – de persoonsgegevens hetzij:

- volledig teruggeven (export in een gestructureerd, gangbaar en machineleesbaar formaat), hetzij
- volledig wissen (veilig overschrijven volgens de stand van de techniek), en wel

binnen 30 dagen na afloop van de overeenkomst.

(2) Back-ups die persoonsgegevens bevatten, worden overeenkomstig bijlage 2 TOM's § Back-uplevenscyclus als gevolg van de rotatie na uiterlijk vijf weken volledig overschreven (back-uprotatie). Bergx2 GmbH documenteert de definitieve wissing op verzoek schriftelijk.

(3) Wettelijke bewaarplichten blijven onverlet (bijv. factuurgegevens op grond van § 257 HGB, § 147 AO).

§ 11 Aansprakelijkheid en slotbepalingen

(1) Aansprakelijkheid. De bepalingen van de hoofdovereenkomst (Screenway-serviceovereenkomst) en art. 82 AVG zijn van toepassing. Bij schending van deze DPA is de verantwoordelijke partij jegens de betrokkene aansprakelijk.

(2) Vorm. Wijzigingen en aanvullingen dienen in tekstvorm te geschieden.

(3) Partiële nietigheid. Indien afzonderlijke bepalingen ongeldig zijn, blijft de geldigheid van de overige bepalingen onverlet.

(4) Toepasselijk recht en bevoegde rechter. Op deze overeenkomst is Duits recht van toepassing, met uitsluiting van het Weens Koopverdrag (CISG). Bevoegde rechter is die te München.

Bijlage 1: Beschrijving van de verwerking

Categorie	Inhoud
Onderwerp	Beschikbaarstelling van het Screenway-SaaS-platform, inclusief hosting, gegevensoverdracht, authenticatie en weergaveaansturing
Duur	Actieve looptijd van de overeenkomst + overgangstermijn van 30 dagen voor export/wissing
Aard van de verwerking	Verzamelen, vastleggen, opslaan, wijzigen, opvragen, weergeven, doorzenden, wissen
Doel	Verlening van de contractueel overeengekomen Screenway-dienst
Betrokkenen	Medewerkers van de klant aan wie inlog-/beheerrechten voor Screenway worden verleend
Categorieën van gegevens	Accountgegevens (naam, zakelijk e-mailadres, rol), inloggegevens (wachtwoord-hash, sessiecookies, IP-adres), gegevens over schermlocaties (aanduiding, in voorkomend geval adres van de locatie), door de klant geüploade content (doorgaans geen persoonsgegevens – marketingmateriaal, informatieteksten enz.)
Bijzondere categorieën van gegevens (art. 9 AVG)	Bij standaardgebruik niet verwerkt
Hostingregio	Uitsluitend Europese Unie – Hetzner Neurenberg (primair) + Hetzner Helsinki (back-upmirror)
Doorgifte naar derde landen	Geen

Bijlage 2: Technische en organisatorische maatregelen (TOM's)

De volgende TOM's voldoen aan art. 32 AVG en zijn zo ingedeeld als de toezichthoudende autoriteiten en de in de branche gebruikelijke AVG-DPA-standaard voorschrijven. De maatregelen worden in het information security management system (ISMS) van Bergx2 volgens ISO/IEC 27001:2022 gedocumenteerd en intern gedetailleerd bijgehouden. Concrete implementatiedetails (modellen van fabrikanten, configuratieparameters, locaties van afzonderlijke componenten, sleutelmechanismen) worden om veiligheidsredenen niet in deze openbaar toegankelijke bijlage bij de overeenkomst bekendgemaakt. Op gemotiveerd verzoek van de klant in het kader van zijn auditrecht op grond van § 9 stelt Bergx2 GmbH de relevante gedetailleerde bewijsstukken ter beschikking binnen een schriftelijk geheimhoudingskader.

1. Vertrouwelijkheid (art. 32 lid 1 onder b AVG)

Maatregel	Uitvoering
Toegangscontrole (ruimten)	Fysieke toegangscontrole in meerdere lagen op de vestigingslocatie met mechanische inbraakwering volgens de relevante DIN-normen, veiligheidsbeglazing, automatisch vergrendelende deuren, cameraondersteunde toegangscontrole vooraf zonder doorgifte naar externe netwerken en meervoudige authenticatie op het binnenste sluitniveau. Toegangsrechten worden volgens het need-to-be-present-principe toegekend aan een bij naam beperkte kring van personen en gedocumenteerd in een bijgehouden sleutelregister met audittrail van uitgifte en inlevering. Sleutels kunnen alleen met toestemming van de verhuurder door gecertificeerde slotenmakers worden bijgemaakt. Bezoekers betreden de bedrijfsruimten uitsluitend onder begeleiding.
Toegangscontrole (systemen)	Op rollen gebaseerde toegangscontrole (RBAC) in alle productiesystemen; meervoudige authenticatie (MFA) voor beheerderstoegang; bindend wachtwoordbeleid volgens de stand van de techniek; server-toegang op basis van sleutels of certificaten zonder wachtwoord; verplichte routering van beheerderstoegang via een intern virtual private network (VPN).
Toegangscontrole (gegevens)	Scheiding van tenants per klantaccount op databaseniveau; toegangsregels op recordniveau (row-level security); controleerbare, onwijzigbare logging van alle lees- en schrijfbewerkingen op persoonsgegevens.
Pseudonimisering	Waar verenigbaar met het doel van de verwerking worden interne verwerkingen gepseudonimiseerd. Een periodieke steekproefcontrole op onbedoeld voorkomende echte namen is ingevoerd als KPI voor informatiebeveiliging.
Versleuteling	Transportversleuteling volgens de stand van de techniek voor alle externe verbindingen met regelmatige rotatie van certificaten. Sterke versleuteling in rust voor back-up-media en harde schijven van eindapparaten. Gevoelige toegangsgegevens (wachtwoorden, tokens, sleutels) worden uitsluitend beheerd in een interne procedure die voldoet aan de stand van de techniek – details worden om veiligheidsredenen niet bekendgemaakt.

2. Integriteit (art. 32 lid 1 onder b AVG)

Maatregel	Uitvoering
Invoercontrole	Server-side validatie van alle invoer; controleerbare, onwijzigbare auditlogs; schrijfrechten uitsluitend via geauthenticeerde en geautoriseerde programmeerinterfaces.
Doorgiftecontrole	Verplichte transportversleuteling voor alle externe verbindingen; geen doorgifte van gegevens zonder gedocumenteerde contractuele grondslag.
Opdrachtcontrole	Verwerkersovereenkomsten met alle subverwerkers (zie bijlage 3); gestructureerd proces voor leveranciersbeheer met periodieke herbeoordeling.

3. Beschikbaarheid en veerkracht (art. 32 lid 1 onder b AVG)

Maatregel	Uitvoering
Back-up	Dagelijkse incrementele back-up van de productiesystemen met geografisch gescheiden spiegeling binnen de Europese Unie ; er worden meerdere versies bewaard; geplande hersteltests per kwartaal.
Beschikbaarheid	Cloud-first-architectuur met hosting in ISO/IEC 27001-gecertificeerde datacenters met noodstroomvoorziening; continue monitoring met vastgelegde escalatiepaden.
Business continuity	Getoetst bedrijfscontinuïteitsplan inclusief business impact analysis; volledige thuiswerkgeschiktheid van de kennisgebaseerde functies; gedocumenteerde hersteltijden per systeem.
Veerkracht van eindapparaten	Vervangend eindapparaat als reserve bij defecten; voldoende accureserve voor kortstondige stroomstoringen.

4. Procedure voor het regelmatig testen, beoordelen en evalueren (art. 32 lid 1 onder d AVG)

Maatregel	Uitvoering
Information security management system (ISMS)	Ingevoerd ISMS volgens ISO/IEC 27001:2022 met Statement of Applicability voor de Annex A-controls; certificering in voorbereiding.
Beheer van gegevensbescherming	Bijgehouden register van verwerkingsactiviteiten; aangestelde functionaris voor gegevensbescherming; periodieke reviews van de verwerkingsactiviteiten.
Bewustwording	Gestructureerde en aantoonbare trainingen in bewustwording en gegevensbescherming voor alle medewerkers met rolspecifieke verplichte modules.
Risicobeheer	Ten minste jaarlijkse risicobeoordeling met goedkeuring door het topmanagement; risicobehandelingsplan met toegewezen maatregelen.
Leveranciersbeheer	Bindend leveranciersbeleid en bijbehorende procedure; DPA-plicht voor alle verwerkers; periodieke leveranciersreviews.
Incidentrespons	Gedocumenteerde procedure voor incidentbeheer met vastgelegde meldingskanalen, escalatieniveaus en verificatie van de doeltreffendheid.
Patchbeheer	Bijgehouden patchregister met navolgbare toepassing van patches.
Directiebeoordeling	Ten minste jaarlijkse beoordeling door het topmanagement op basis van kwantitatieve KPI's.
Interne audit	Jaarlijkse onafhankelijke interne ISMS-audit met gedocumenteerde bevindingen en corrigerende maatregelen.

5. Levenscyclus van back-ups en wissing

Persoonsgegevens in back-ups worden door de vastgelegde back-uprotatie binnen enkele weken volledig overschreven.

Bij afloop van de overeenkomst vindt de definitieve wissing van gegevens op productiesystemen plaats binnen 30 dagen; de back-uprotatie verwijdert de gegevens vervolgens binnen enkele weken uit het bestand.

Concrete bewaartermijnen per back-upgeneratie worden op gemotiveerd verzoek in het kader van het auditrecht (§ 9) bekendgemaakt.

Bijlage 3: Lijst van subverwerkers

Stand: 25.05.2026.

Nr.	Subverwerker	Vestigingsplaats	Doel van de verwerking	Verwerkte gegevens	Certificeringen / DPA
1	Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Duitsland – datacenters in Duitsland en Finland (EU)	Hosting van de productie- en back-upinfrastructuur van Screenway	Alle in bijlage 1 genoemde gegevens; uitsluitend versleuteld at rest en in transit	ISO/IEC 27001 + ISO/IEC 9001 gecertificeerd; verwerkersovereenkomst door Bergx2 GmbH actief aanvaard; lijst van onderaannemers van de hostingprovider openbaar beschikbaar op www.hetzner.com/AV/subunternehmer.pdf

Opmerking over overige leveranciers van Bergx2: Bergx2 GmbH maakt voor de eigen bedrijfsvoering (communicatie met medewerkers, broncodebeheer, kantoor- en productiviteitstools) gebruik van andere SaaS-dienstverleners. Deze verwerken geen klantgegevens uit het Screenway-platform en zijn daarom geen subverwerkers in de zin van deze DPA. Op gemotiveerd verzoek van de klant in het kader van zijn auditrecht (§ 9) zal Bergx2 GmbH de volledige lijst van haar eigen leveranciers bekendmaken.

Inwerkingtreding

Deze DPA wordt door aanvaarding in het klantenportaal met tijdstempel en versieaanduiding een rechtsgeldig onderdeel van de Screenway-serviceovereenkomst (art. 28 lid 9 AVG: schriftelijk, waaronder in elektronische vorm).

Het aanvaardingsrecord wordt door Bergx2 GmbH in de klantenbackend controleerbaar en onwijzigbaar gearchiveerd en omvat ten minste:

- Versieaanduiding van deze DPA (zie de versietabel hieronder)
- Datum en tijdstip van aanvaarding
- Identiteit van de aanvaardende persoon (gebruikers-ID van het klantaccount)
- Identiteit van de klant (account-/contract-ID)
- Hashwaarde van de aanvaarde versie van de overeenkomst (cryptografisch bewijs van integriteit)

Bij een actualisering van deze DPA ontvangt de klant ten minste 30 dagen vóór de inwerkingtreding een kennisgeving in tekstvorm en bij de volgende login in het klantenportaal een verzoek om de DPA opnieuw te aanvaarden.

Optionele fysieke of gekwalificeerde elektronische handtekening: Indien de klant – bijv. op grond van interne compliancevoorschriften – een aanvullende medeondertekening wenst, kan de DPA fysiek of met een gekwalificeerde elektronische handtekening (eIDAS-verordening (EU) nr. 910/2014) tussen de contractpartijen worden medeondertekend. Het aanleveren daarvan geschiedt in dat geval door de klant. De elektronische

aanvaarding in het klantenportaal blijft daardoor onverlet en vormt op zichzelf een AVG-conforme totstandkoming van de overeenkomst.

Versiebeheer

Versie	Stand
1.0	25.05.2026