> Napomena: Obvezujuća verzija ovog ugovora o obradi podataka jest njemački izvornik, dostupan na `/rechtliches/avv`. Ovaj hrvatski prijevod služi isključivo za informaciju. U slučaju odstupanja mjerodavna je njemačka verzija.

# Ugovor o obradi podataka (DPA) za Screenway

> Ova je verzija obvezujuća i može se pravovaljano sklopiti elektroničkim prihvaćanjem na portalu za klijente (vidi odjeljak „Stupanje na snagu“).

## Preambula

Bergx2 GmbH upravlja platformom Screenway, koja se pruža kao softver kao usluga (SaaS), za upravljanje sustavima digital signage. U okviru korištenja usluge Bergx2 GmbH obrađuje osobne podatke u ime klijenta u smislu članka 4. točke 8. i članka 28. Uredbe (EU) 2016/679 – Opće uredbe o zaštiti podataka (GDPR). Ovim se ugovorom konkretiziraju obveze i prava obiju ugovornih strana u skladu s člankom 28. stavkom 3. GDPR-a.

---

## § 1 Predmet i trajanje obrade

(1) Predmet. Bergx2 GmbH stavlja klijentu na raspolaganje platformu Screenway kao softver kao uslugu (SaaS). U okviru korištenja Bergx2 GmbH obrađuje osobne podatke klijenta pobliže opisane u Prilogu 1 isključivo prema njegovim uputama.

(2) Trajanje. Ugovor stupa na snagu sklapanjem temeljnog glavnog ugovora (ugovora o usluzi Screenway) i prestaje njegovim prestankom. Obveze brisanja/vraćanja (§ 10) i povjerljivosti (§ 5 st. 2) vrijede i nakon isteka trajanja ugovora.

---

## § 2 Vrsta i svrha obrade

(1) Bergx2 GmbH obrađuje osobne podatke opisane u Prilogu 1 u sljedeće svrhe:

- Pružanje platforme Screenway kao SaaS rješenja za digital signage
- Dodjeljivanje lokacija zaslona korisničkim računima klijenata
- Prikaz sadržaja koje je klijent učitao na krajnjim uređajima
- Autentifikacija zaposlenika klijenta pri prijavi
- Pružanje podrške, analiza pogrešaka i nadzor usluge

(2) Obrada u vlastite svrhe društva Bergx2 GmbH (npr. marketing, izrada profila, prodaja trećim stranama) ne provodi se.

---

## § 3 Vrsta osobnih podataka i kategorije ispitanika

Konkretan popis vidi u Prilogu 1. Ukratko:

- Vrsta podataka: podaci o korisničkom računu, podaci za prijavu, podaci o lokacijama zaslona, sadržaji koje je učitao klijent (u pravilu nisu osobni podaci)
- Kategorije ispitanika: zaposlenici klijenta (za prijavu i dodjelu korisničkog računa)

Obrada posebnih kategorija osobnih podataka u smislu članka 9. GDPR-a ne provodi se u standardnom radu platforme Screenway. Ako klijent ipak učita takve podatke, to se događa izvan kategorija obuhvaćenih ovim ugovorom o obradi podataka i na vlastitu odgovornost klijenta.

---

## § 4 Obveze i prava voditelja obrade (klijenta)

(1) Pravo davanja uputa. Klijent ostaje odgovoran za zakonitost obrade (članak 24. GDPR-a). Bergx2 GmbH obrađuje podatke isključivo prema zabilježenim uputama klijenta. Ovaj ugovor o obradi podataka smatra se općom uputom; pojedinačne upute moguće su putem komunikacijskih kanala utvrđenih u ugovoru o usluzi.

(2) Evidentiranje. Bergx2 GmbH dokumentira postupke relevantne za upute u internom revizijskom tragu ISMS-a (povijest pull requestova, registar incidenata, registar dobavljača).

(3) Obveze informiranja. Klijent je dužan u skladu s člankom 13. GDPR-a obavijestiti ispitanike (svoje zaposlenike) o obradi podataka koju provodi Bergx2 GmbH.

---

## § 5 Obveze izvršitelja obrade (Bergx2 GmbH)

(1) Vezanost uputama. Bergx2 GmbH obrađuje podatke isključivo prema zabilježenim uputama klijenta. Ako je neka uputa prema mišljenju društva Bergx2 GmbH nezakonita, Bergx2 GmbH o tome bez odgađanja obavještava klijenta (članak 28. stavak 3. točka (h) GDPR-a).

(2) Povjerljivost. Bergx2 GmbH prije početka rada obvezuje sve osobe uključene u obradu na povjerljivost (članak 28. stavak 3. točka (b) GDPR-a). To se provodi izjavama o povjerljivosti (NDA) pri zapošljavanju odnosno angažmanu i dokumentirano je u ISMS-u društva Bergx2 (registar zaposlenika).

(3) Tehničke i organizacijske mjere. Bergx2 GmbH provodi tehničke i organizacijske mjere (TOM) opisane u Prilogu 2, koje odgovaraju najnovijim dostignućima tehnike i osiguravaju razinu zaštite primjerenu riziku (članak 32. GDPR-a).

(4) Podizvršitelji obrade. Bergx2 GmbH angažira podizvršitelje obrade navedene u Prilogu 3. Uvjete i mehanizam izmjena vidi u § 6.

(5) Pomoć. Bergx2 GmbH pomaže klijentu u ispunjavanju njegovih obveza iz članaka 32. – 36. GDPR-a, osobito pri odgovaranju na zahtjeve ispitanika (§ 7) i prijavljivanju povreda osobnih podataka (§ 8).

(6) Dokazi. Bergx2 GmbH na zahtjev stavlja klijentu na raspolaganje informacije i dokumentaciju potrebne za provjeru (članak 28. stavak 3. točka (h) GDPR-a). Daljnje modalitete revizije vidi u § 9.

---

## § 6 Podizvršitelji obrade

(1) Odobrenje. Sklapanjem ovog ugovora o obradi podataka klijent daje opće odobrenje za angažiranje podizvršitelja obrade navedenih u Prilogu 3 (članak 28. stavak 2. prva rečenica GDPR-a).

(2) Obavijest o izmjenama. Bergx2 GmbH obavještava klijenta o namjeravanim izmjenama u pogledu podizvršitelja obrade (dodavanje ili zamjena) najmanje 30 dana prije stupanja izmjene na snagu, u tekstualnom obliku (e-poštom na adresu za kontakt o zaštiti podataka navedenu u ugovoru o usluzi).

(3) Pravo na prigovor. Klijent može iz opravdanih razloga uložiti prigovor na izmjenu u roku od 30 dana. U slučaju prigovora Bergx2 GmbH zajedno s klijentom traži sporazumno rješenje; ako to ne uspije, klijent ima pravo na izvanredni otkaz ugovora o usluzi.

(4) Obvezivanje. Bergx2 GmbH ugovorno obvezuje svakog podizvršitelja obrade na obveze dogovorene u ovom ugovoru o obradi podataka (članak 28. stavak 4. GDPR-a).

---

## § 7 Pomoć u ostvarivanju prava ispitanika

Bergx2 GmbH pomaže klijentu, koliko je to moguće, odgovarajućim tehničkim i organizacijskim mjerama u ispunjavanju prava ispitanika iz poglavlja III. GDPR-a (pristup, ispravak, brisanje, ograničenje obrade, prenosivost podataka, prigovor).

Konkretno: zahtjeve koje ispitanici upute izravno društvu Bergx2 GmbH, Bergx2 GmbH bez odgađanja prosljeđuje klijentu i daje mu mogućnost odgovora. Bergx2 GmbH sam odgovara na zahtjeve samo na izričitu uputu klijenta.

---

## § 8 Prijava povreda osobnih podataka

(1) Bergx2 GmbH bez odgađanja, a najkasnije u roku od 24 sata od saznanja, obavještava klijenta o svakoj utvrđenoj povredi osobnih podataka u području odgovornosti društva Bergx2 GmbH ili nekog podizvršitelja obrade koja se odnosi na osobne podatke klijenta.

(2) Obavijest se daje pisanim putem (e-poštom na adresu klijenta za kontakt o zaštiti podataka) i sadržava minimalne podatke navedene u članku 33. stavku 3. GDPR-a (vrsta i opseg povrede, broj ispitanika, vjerojatne posljedice, poduzete protumjere).

(3) Bergx2 GmbH interno dokumentira vlastite povrede osobnih podataka u registru incidenata (vidi `incidents/incidents.md` ISMS-a društva Bergx2, postupak u skladu s `documents/verfahren/incident-management-verfahren.md`).

(4) Obveza izvješćivanja nadležnog nadzornog tijela u skladu s člankom 33. GDPR-a i, prema potrebi, obavješćivanja ispitanika u skladu s člankom 34. GDPR-a ostaje na klijentu kao voditelju obrade. Bergx2 GmbH pomaže klijentu pri tim prijavama svim potrebnim informacijama.

---

## § 9 Prava revizije i nadzora

(1) Dokazi. Bergx2 GmbH na zahtjev stavlja klijentu na raspolaganje informacije potrebne za ispunjavanje obveza iz ovog ugovora o obradi podataka, osobito važeću verziju TOM-a (Prilog 2) i popisa podizvršitelja obrade (Prilog 3) te, prema potrebi, izvatke iz certifikata.

(2) Nadzor na licu mjesta. Klijent ima pravo na licu mjesta, u sjedištu društva Bergx2 GmbH ili na lokacijama obrade, uvjeriti se u pridržavanje TOM-a. Termini se moraju pisano najaviti najmanje četiri tjedna unaprijed; nadzori se moraju ograničiti na nužnu mjeru i ne smiju nerazmjerno ometati poslovanje. Najviše jedan nadzor po kalendarskoj godini, osim u slučaju opravdanog povoda.

(3) Priznavanje certifikata. Ako je Bergx2 GmbH certificiran prema normi ISO/IEC 27001:2022 (certifikacija u pripremi) ili predoči jednakovrijedne neovisne revizije trećih strana, to zamjenjuje nadzor klijenta na licu mjesta, pod uvjetom da područje primjene certifikacije obuhvaća i predmet ugovora.

---

## § 10 Brisanje i vraćanje nakon prestanka ugovora

(1) Po prestanku ugovora o usluzi Bergx2 GmbH će – prema izboru klijenta – osobne podatke:

- u cijelosti vratiti (izvoz u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu), ili
- u cijelosti izbrisati (sigurno prepisivanje u skladu s najnovijim dostignućima tehnike), i to

u roku od 30 dana od prestanka ugovora.

(2) Sigurnosne kopije koje sadržavaju osobne podatke u skladu s Prilogom 2 TOM, § Životni ciklus sigurnosnih kopija, zbog rotacije se u potpunosti prepisuju najkasnije nakon pet tjedana (rotacija sigurnosnih kopija). Bergx2 GmbH na zahtjev pisano dokumentira konačno brisanje.

(3) Zakonske obveze čuvanja ostaju netaknute (npr. podaci za obračun u skladu s § 257 HGB, § 147 AO).

---

## § 11 Odgovornost i završne odredbe

(1) Odgovornost. Primjenjuju se odredbe glavnog ugovora (ugovora o usluzi Screenway) i članak 82. GDPR-a. U slučaju povrede ovog ugovora o obradi podataka prema ispitaniku odgovara ona ugovorna strana koja je za povredu odgovorna.

(2) Oblik. Izmjene i dopune zahtijevaju tekstualni oblik.

(3) Salvatorna klauzula. Ako bi pojedine odredbe bile ništetne, to ne utječe na valjanost ostalih odredaba.

(4) Mjerodavno pravo i nadležnost suda. Primjenjuje se njemačko pravo uz isključenje Konvencije Ujedinjenih naroda o ugovorima o međunarodnoj prodaji robe (CISG). Nadležan je sud u Münchenu.

---

## Prilog 1: Opis obrade

| Kategorija | Sadržaj |
|---|---|
| **Predmet** | Pružanje SaaS platforme Screenway uključujući hosting, prijenos podataka, autentifikaciju i upravljanje prikazom |
| **Trajanje** | Aktivno trajanje ugovora + prijelazni rok od 30 dana za izvoz/brisanje |
| **Vrsta obrade** | Prikupljanje, bilježenje, pohrana, izmjena, pretraživanje, prikaz, prijenos, brisanje |
| **Svrha** | Pružanje ugovorene usluge Screenway |
| **Ispitanici** | Zaposlenici klijenta kojima je dodijeljen pristup za prijavu i upravljanje platformom Screenway |
| **Kategorije podataka** | Podaci o korisničkom računu (ime, službena adresa e-pošte, uloga), podaci za prijavu (hash lozinke, kolačići sesije, IP adresa), podaci o lokacijama zaslona (naziv, prema potrebi adresa lokacije), sadržaji koje je učitao klijent (u pravilu **nisu** osobni podaci – marketinški materijali, informativni tekstovi itd.) |
| **Posebne kategorije podataka (članak 9. GDPR-a)** | U standardnom radu **ne** obrađuju se |
| **Regija hostinga** | Isključivo Europska unija – Hetzner Nürnberg (primarno) + Hetzner Helsinki (zrcalna sigurnosna kopija) |
| **Prijenos u treće zemlje** | **Nema** |

---

## Prilog 2: Tehničke i organizacijske mjere (TOM)

Sljedeće tehničke i organizacijske mjere (TOM) odgovaraju članku 32. GDPR-a i kategorizirane su onako kako to propisuju nadzorna tijela i uobičajeni standard u industriji za ugovore o obradi podataka prema GDPR-u. Mjere se dokumentiraju u sustavu upravljanja informacijskom sigurnošću (ISMS) društva Bergx2 prema normi ISO/IEC 27001:2022 i interno se detaljno vode. Konkretni detalji provedbe (modeli proizvođača, konfiguracijski parametri, lokacije pojedinih komponenti, mehanizmi ključeva) iz sigurnosnih se razloga ne objavljuju u ovom javno dostupnom prilogu ugovoru. Na obrazloženi zahtjev klijenta u okviru njegova prava na reviziju iz § 9 Bergx2 GmbH stavlja na raspolaganje relevantne detaljne dokaze u okviru pisanog sporazuma o povjerljivosti.

## 1. Povjerljivost (članak 32. stavak 1. točka (b) GDPR-a)

| Mjera | Provedba |
|---|---|
| **Kontrola fizičkog pristupa** | Višestupanjska fizička kontrola pristupa u sjedištu društva s mehaničkom zaštitom od provale u skladu s mjerodavnim normama DIN, sigurnosnim staklom, automatski zaključavajućim vratima, prethodnom kontrolom ulaska uz pomoć kamera bez prijenosa u vanjske mreže i višefaktorskom autentifikacijom na najunutarnjijoj razini zaključavanja. Ovlaštenja za pristup dodjeljuju se prema načelu need-to-be-present ograničenom krugu poimenično navedenih osoba i dokumentiraju se u vođenom registru ključeva s revizijskim tragom izdavanja i vraćanja. Izrada kopija ključeva moguća je samo uz odobrenje najmodavca putem certificiranih bravara. Posjetitelji ulaze u poslovne prostore samo u pratnji. |
| **Kontrola pristupa (sustavi)** | Kontrola pristupa temeljena na ulogama (RBAC) u svim produkcijskim sustavima; višefaktorska autentifikacija (MFA) za administrativne pristupe; obvezujuća pravila o lozinkama u skladu s najnovijim dostignućima tehnike; pristup poslužiteljima na temelju ključeva odnosno certifikata bez lozinke; obvezno usmjeravanje administrativnih pristupa kroz internu virtualnu privatnu mrežu (VPN). |
| **Kontrola pristupa (podaci)** | Odvajanje podataka klijenata po korisničkom računu na razini baze podataka; pravila pristupa na razini zapisa (Row-Level Security); zapisivanje svih pristupa osobnim podacima radi čitanja i pisanja, otporno na naknadne izmjene. |
| **Pseudonimizacija** | Gdje god je to spojivo sa svrhom obrade, interne obrade se pseudonimiziraju. Periodična provjera uzoraka na nenamjerno pojavljivanje stvarnih imena uspostavljena je kao KPI informacijske sigurnosti. |
| **Enkripcija** | Enkripcija prijenosa u skladu s najnovijim dostignućima tehnike za sve vanjske veze uz redovitu rotaciju certifikata. Snažna enkripcija pohranjenih podataka za medije sigurnosnih kopija i tvrde diskove krajnjih uređaja. Osjetljivim pristupnim podacima (lozinke, tokeni, ključevi) upravlja se isključivo internim postupkom koji odgovara najnovijim dostignućima tehnike – pojedinosti se iz sigurnosnih razloga ne objavljuju. |

## 2. Cjelovitost (članak 32. stavak 1. točka (b) GDPR-a)

| Mjera | Provedba |
|---|---|
| **Kontrola unosa** | Provjera valjanosti svih unosa na strani poslužitelja; revizijski zapisi otporni na izmjene; prava pisanja isključivo putem autentificiranih i autoriziranih programskih sučelja. |
| **Kontrola prijenosa** | Obvezna enkripcija prijenosa za sve vanjske veze; nema prosljeđivanja podataka bez dokumentirane ugovorne osnove. |
| **Kontrola naloga** | Ugovori o obradi podataka sa svim podizvršiteljima obrade (vidi Prilog 3); strukturirani postupak upravljanja dobavljačima s periodičnom ponovnom procjenom. |

### 3. Dostupnost i otpornost (članak 32. stavak 1. točka (b) GDPR-a)

| Mjera | Provedba |
|---|---|
| **Sigurnosna kopija** | Dnevna inkrementalna sigurnosna kopija produkcijskih sustava s geografski odvojenim zrcaljenjem **unutar Europske unije**; čuva se više verzija; planirana testiranja oporavka svakog tromjesečja. |
| **Dostupnost** | Cloud-first arhitektura s hostingom u podatkovnim centrima certificiranim prema ISO/IEC 27001 s rezervnim napajanjem u nuždi; kontinuirani nadzor s definiranim putovima eskalacije. |
| **Kontinuitet poslovanja** | Provjereni plan kontinuiteta poslovanja uključujući analizu utjecaja na poslovanje (Business Impact Analysis); potpuna mogućnost rada od kuće za funkcije temeljene na znanju; dokumentirana vremena ponovnog pokretanja za svaki sustav. |
| **Otpornost krajnjih uređaja** | Zamjenski krajnji uređaj kao rezerva u slučaju kvara uređaja; dostatne rezerve trajanja baterije za kratkotrajne nestanke struje. |

### 4. Postupci za redovito testiranje, ocjenjivanje i procjenjivanje (članak 32. stavak 1. točka (d) GDPR-a)

| Mjera | Provedba |
|---|---|
| **Sustav upravljanja informacijskom sigurnošću (ISMS)** | Uspostavljen ISMS prema normi ISO/IEC 27001:2022 s izjavom o primjenjivosti (Statement of Applicability) za kontrole iz Priloga A (Annex A); certifikacija u pripremi. |
| **Upravljanje zaštitom podataka** | Vođena evidencija aktivnosti obrade; imenovan službenik za zaštitu podataka; periodični pregledi aktivnosti obrade. |
| **Podizanje svijesti** | Strukturirane i dokumentirane edukacije o informacijskoj sigurnosti i zaštiti podataka za sve zaposlenike s obveznim modulima prilagođenima ulozi. |
| **Upravljanje rizicima** | Procjena rizika najmanje jednom godišnje uz odobrenje najviše uprave; plan postupanja s rizicima s dodijeljenim mjerama. |
| **Upravljanje dobavljačima** | Obvezujuća politika i postupak za dobavljače; obveza sklapanja ugovora o obradi podataka za sve izvršitelje obrade; periodični pregledi dobavljača. |
| **Odgovor na incidente** | Dokumentirani postupak upravljanja incidentima s definiranim kanalima prijave, razinama eskalacije i provjerom učinkovitosti. |
| **Upravljanje zakrpama** | Vođeni registar zakrpa sa sljedivom primjenom zakrpa. |
| **Preispitivanje od strane uprave (Management Review)** | Ocjena najviše uprave najmanje jednom godišnje na temelju kvantitativnih KPI-jeva. |
| **Interni audit** | Godišnji neovisni interni audit ISMS-a s dokumentiranim nalazima i korektivnim mjerama. |

### 5. Životni ciklus sigurnosnih kopija i brisanje

Osobni podaci u sigurnosnim kopijama u potpunosti se prepisuju definiranom rotacijom sigurnosnih kopija u roku od nekoliko tjedana.

Po prestanku ugovora konačno brisanje podataka u produkcijskim sustavima provodi se u roku od 30 dana; rotacija sigurnosnih kopija nakon toga u roku od nekoliko tjedana uklanja podatke iz skupa pohranjenih podataka.

Konkretni rokovi čuvanja po generaciji sigurnosnih kopija otkrivaju se na obrazloženi zahtjev u okviru prava na reviziju (§ 9).

---

## Prilog 3: Popis podizvršitelja obrade

Stanje na dan 25.05.2026.

| Br. | Podizvršitelj obrade | Sjedište | Svrha obrade | Obrađeni podaci | Certifikati / ugovor o obradi podataka |
|---|---|---|---|---|---|
| 1 | **Hetzner Online GmbH** | Industriestraße 25, 91710 Gunzenhausen, Njemačka – podatkovni centri u Njemačkoj i Finskoj (EU) | Hosting produkcijske infrastrukture i infrastrukture sigurnosnih kopija platforme Screenway | Svi podaci navedeni u Prilogu 1; isključivo enkriptirani u mirovanju i tijekom prijenosa (at rest i in transit) | Certificiran prema ISO/IEC 27001 + ISO/IEC 9001; ugovor o obradi podataka aktivno prihvaćen od strane društva Bergx2 GmbH; popis podizvođača pružatelja hostinga javno je dostupan na www.hetzner.com/AV/subunternehmer.pdf |

Napomena o ostalim dobavljačima društva Bergx2: Bergx2 GmbH za vlastito poslovanje (komunikacija među zaposlenicima, upravljanje izvornim kodom, uredski alati i alati za produktivnost) koristi i druge pružatelje SaaS usluga. Oni ne obrađuju podatke klijenata s platforme Screenway te stoga nisu podizvršitelji obrade u smislu ovog ugovora o obradi podataka. Na obrazloženi zahtjev klijenta u okviru njegova prava na reviziju (§ 9) Bergx2 GmbH će otkriti potpuni popis vlastitih dobavljača.

---

## Stupanje na snagu

Ovaj ugovor o obradi podataka prihvaćanjem na portalu za klijente uz vremensku oznaku i oznaku verzije postaje valjani sastavni dio ugovora o usluzi Screenway (članak 28. stavak 9. GDPR-a: u pisanom obliku, uključujući elektronički oblik).

Zapis o prihvaćanju Bergx2 GmbH arhivira u sustavu za klijente (Customer Backend) na način otporan na izmjene, a obuhvaća najmanje:

- Oznaku verzije ovog ugovora o obradi podataka (vidi tablicu verzija u nastavku)
- Datum i vrijeme prihvaćanja

- Identitet osobe koja prihvaća (korisnički ID korisničkog računa klijenta)
- Identitet klijenta (ID korisničkog računa/ugovora)
- Hash vrijednost prihvaćene verzije ugovora (kriptografski dokaz cjelovitosti)

U slučaju ažuriranja ovog ugovora o obradi podataka klijent najmanje 30 dana prije stupanja izmjena na snagu prima obavijest u tekstualnom obliku, a pri sljedećoj prijavi na portal za klijente poziv na ponovno prihvaćanje.

Neobvezni vlastoručni ili kvalificirani elektronički potpis: Ako klijent – npr. zbog internih zahtjeva usklađenosti – želi dodatni supotpis, ugovorne strane mogu ugovor o obradi podataka supotpisati vlastoručno ili kvalificiranim elektroničkim potpisom (Uredba eIDAS (EU) br. 910/2014). U tom slučaju supotpis pribavlja klijent. Elektroničko prihvaćanje na portalu za klijente time ostaje netaknuto i samo po sebi predstavlja sklapanje ugovora u skladu s GDPR-om.

---

## Verzije

| Verzija | Datum |
|---|---|
| 1.0 | 25.05.2026. |