Smlouva o zpracování osobních údajů (DPA) pro Screenway

> Toto znění je závazné a lze je účinně uzavřít elektronickou akceptací v zákaznickém portálu (viz oddíl „Účinnost").

Preambule

Bergx2 GmbH provozuje platformu Software-as-a-Service Screenway pro řízení digital signage. V rámci využívání služby zpracovává Bergx2 GmbH osobní údaje z pověření zákazníka ve smyslu čl. 4 bodu 8 a čl. 28 nařízení (EU) 2016/679 (obecné nařízení o ochraně osobních údajů, GDPR). Tato smlouva konkretizuje povinnosti a práva obou smluvních stran podle čl. 28 odst. 3 GDPR.

---

§ 1 Předmět a doba trvání zpracování

(1) Předmět. Bergx2 GmbH poskytuje zákazníkovi platformu Screenway jako Software-as-a-Service. V rámci jejího využívání zpracovává Bergx2 GmbH osobní údaje zákazníka blíže popsané v příloze 1 výhradně podle jeho pokynů.

(2) Doba trvání. Smlouva nabývá účinnosti uzavřením hlavní smlouvy (smlouva o službě Screenway) a končí jejím ukončením. Povinnosti týkající se výmazu/vrácení (§ 10) a mlčenlivosti (§ 5 odst. 2) trvají i po skončení doby trvání smlouvy.

---

§ 2 Povaha a účel zpracování

(1) Bergx2 GmbH zpracovává osobní údaje popsané v příloze 1 k následujícím účelům:

- Poskytování platformy Screenway jako SaaS pro digital signage
- Přiřazování umístění obrazovek k zákaznickým účtům
- Zobrazování obsahu nahraného zákazníkem na koncových zařízeních
- Autentizace zaměstnanců zákazníka při přihlášení
- Poskytování podpory, analýzy chyb a monitoringu služby

(2) Zpracování pro vlastní účely Bergx2 GmbH (např. marketing, profilování, prodej třetím stranám) neprobíhá.

---

§ 3 Typ osobních údajů a kategorie subjektů údajů

Konkrétní výčet viz příloha 1. Souhrnně:

- Typ údajů: údaje o účtu, přihlašovací údaje, údaje o umístění obrazovek, obsah nahraný zákazníkem (zpravidla bez osobních údajů)
- Kategorie subjektů údajů: zaměstnanci zákazníků (pro přihlášení a přiřazení k účtu)

Zpracování zvláštních kategorií osobních údajů ve smyslu čl. 9 GDPR ve standardním provozu Screenway neprobíhá. Pokud zákazník takové údaje přesto nahraje, děje se tak mimo kategorie upravené touto DPA a na vlastní odpovědnost zákazníka.

---

§ 4 Povinnosti a práva správce (zákazníka)

(1) Právo udělovat pokyny. Zákazník zůstává odpovědný za zákonnost zpracování (čl. 24 GDPR). Bergx2 GmbH zpracovává údaje výhradně na základě doložených pokynů zákazníka. Tato DPA se považuje za obecný pokyn; individuální pokyny jsou možné prostřednictvím komunikačních kanálů definovaných ve smlouvě o službě.

(2) Záznamy. Bergx2 GmbH dokumentuje procesy relevantní pro pokyny v interní auditní stopě ISMS (historie pull requestů, registr incidentů, registr dodavatelů).

(3) Informační povinnosti. Zákazník je povinen informovat subjekty údajů (své zaměstnance) podle čl. 13 GDPR o zpracování údajů ze strany Bergx2 GmbH.

---

§ 5 Povinnosti zpracovatele (Bergx2 GmbH)

(1) Vázanost pokyny. Bergx2 GmbH zpracovává údaje výhradně na základě doložených pokynů zákazníka. V případě pokynu, který je z pohledu Bergx2 GmbH protiprávní, Bergx2 GmbH zákazníka bez zbytečného odkladu informuje (čl. 28 odst. 3 písm. h) GDPR).

(2) Mlčenlivost. Bergx2 GmbH zavazuje všechny osoby podílející se na zpracování před zahájením činnosti k mlčenlivosti (čl. 28 odst. 3 písm. b) GDPR). Děje se tak prostřednictvím prohlášení o mlčenlivosti (NDA) při přijetí do zaměstnání, resp. při pověření, a je to dokumentováno v ISMS Bergx2 (registr zaměstnanců).

(3) Technická a organizační opatření. Bergx2 GmbH přijímá opatření TOM popsaná v příloze 2, která odpovídají stavu techniky a zajišťují úroveň ochrany odpovídající danému riziku (čl. 32 GDPR).

(4) Dílčí zpracovatelé. Bergx2 GmbH využívá dílčí zpracovatele uvedené v příloze 3. Podmínky a mechanismus změn viz § 6.

(5) Podpora. Bergx2 GmbH podporuje zákazníka při plnění jeho povinností podle čl. 32–36 GDPR, zejména při vyřizování žádostí subjektů údajů (§ 7) a při ohlašování porušení zabezpečení osobních údajů (§ 8).

(6) Doklady. Bergx2 GmbH poskytne zákazníkovi na požádání informace a podklady nezbytné k provedení kontroly (čl. 28 odst. 3 písm. h) GDPR). Další podmínky auditu viz § 9.

---

§ 6 Dílčí zpracovatelé

(1) Povolení. Uzavřením této DPA uděluje zákazník obecné povolení k zapojení dílčích zpracovatelů uvedených v příloze 3 (čl. 28 odst. 2 věta první GDPR).

(2) Oznámení změn. Bergx2 GmbH informuje zákazníka o zamýšlených změnách v okruhu dílčích zpracovatelů (přibrání nebo nahrazení) nejméně 30 dnů před nabytím účinnosti v textové podobě (e-mailem na kontaktní adresu pro ochranu osobních údajů uvedenou ve smlouvě o službě).

(3) Právo vznést námitku. Zákazník může proti změně ve lhůtě 30 dnů z oprávněných důvodů vznést námitku. V případě námitky hledá Bergx2 GmbH se zákazníkem smírné řešení; pokud se to nepodaří, má zákazník právo na mimořádnou výpověď smlouvy o službě.

(4) Zavázání. Bergx2 GmbH smluvně zavazuje každého dílčího zpracovatele k povinnostem sjednaným v této DPA (čl. 28 odst. 4 GDPR).

---

§ 7 Součinnost při výkonu práv subjektů údajů

Bergx2 GmbH podporuje zákazníka vhodnými technickými a organizačními opatřeními, pokud je to možné, při plnění práv subjektů údajů podle kapitoly III GDPR (přístup, oprava, výmaz, omezení, přenositelnost údajů, námitka).

Konkrétně: Bergx2 GmbH předává příslušné žádosti, které subjekty údajů směřují přímo na Bergx2 GmbH, bez zbytečného odkladu zákazníkovi a dává mu možnost odpovědět. Vlastní vyřízení ze strany Bergx2 GmbH probíhá pouze na výslovný pokyn zákazníka.

---

§ 8 Ohlašování porušení zabezpečení osobních údajů

(1) Bergx2 GmbH informuje zákazníka bez zbytečného odkladu, nejpozději do 24 hodin od okamžiku, kdy se o něm dozví, o každém zjištěném porušení zabezpečení osobních údajů v oblasti odpovědnosti Bergx2 GmbH nebo dílčího zpracovatele, které se týká osobních údajů zákazníka.

(2) Ohlášení se provádí písemně (e-mailem na kontaktní adresu zákazníka pro ochranu osobních údajů) a obsahuje minimální údaje uvedené v čl. 33 odst. 3 GDPR (povaha a rozsah porušení, počet dotčených subjektů údajů, pravděpodobné důsledky, přijatá nápravná opatření).

(3) Bergx2 GmbH dokumentuje vlastní porušení zabezpečení osobních údajů interně v registru incidentů (viz `incidents/incidents.md` ISMS Bergx2, postup podle `documents/verfahren/incident-management-verfahren.md`).

(4) Povinnost ohlásit porušení příslušnému dozorovému úřadu podle čl. 33 GDPR a případně oznámit je subjektům údajů podle čl. 34 GDPR zůstává zákazníkovi jako správci. Bergx2 GmbH podporuje zákazníka při těchto ohlášeních všemi nezbytnými informacemi.

---

§ 9 Práva na audit a kontrolu

(1) Doklady. Bergx2 GmbH poskytne zákazníkovi na požádání informace nezbytné k doložení plnění povinností vyplývajících z této DPA, zejména aktuální znění opatření TOM (příloha 2) a seznamu dílčích zpracovatelů (příloha 3), jakož i případně výpisy z certifikací.

(2) Kontrola na místě. Zákazník má právo přesvědčit se o dodržování opatření TOM na místě v sídle Bergx2 GmbH nebo v místech zpracování. Termíny je nutno písemně oznámit nejméně čtyři týdny předem; kontroly je třeba omezit na nezbytnou míru a nesmějí nepřiměřeně narušovat provoz podniku. Maximálně jedna kontrola za kalendářní rok, s výjimkou odůvodněných případů.

(3) Uznávání certifikací. Pokud je Bergx2 GmbH certifikována podle ISO/IEC 27001:2022 (certifikace se připravuje) nebo předloží rovnocenné nezávislé kontroly třetích stran, nahrazuje to kontrolu zákazníka na místě, pokud rozsah platnosti certifikace zahrnuje předmět smlouvy.

---

§ 10 Výmaz a vrácení po skončení smlouvy

(1) Při ukončení smlouvy o službě Bergx2 GmbH – podle volby zákazníka – osobní údaje buď:

- v plném rozsahu vrátí (export ve strukturovaném, běžně používaném a strojově čitelném formátu), nebo
- v plném rozsahu vymaže (bezpečné přepsání podle stavu techniky), a to

do 30 dnů od skončení smlouvy.

(2) Zálohy obsahující osobní údaje jsou podle přílohy 2 TOM § Životní cyklus záloh v rámci rotace nejpozději po pěti týdnech zcela přepsány (rotace záloh). Bergx2 GmbH na požádání písemně dokumentuje konečný výmaz.

(3) Zákonné povinnosti uchovávání zůstávají nedotčeny (např. fakturační údaje podle § 257 HGB, § 147 AO).

---

§ 11 Odpovědnost a závěrečná ustanovení

(1) Odpovědnost. Platí ustanovení hlavní smlouvy (smlouva o službě Screenway) a čl. 82 GDPR. Při porušení této DPA odpovídá vůči subjektu údajů vždy příslušná odpovědná smluvní strana.

(2) Písemná forma. Změny a doplnění vyžadují textovou podobu.

(3) Salvátorská doložka. Pokud by jednotlivá ustanovení byla neplatná, platnost ostatních ustanovení tím zůstává nedotčena.

(4) Rozhodné právo a soudní příslušnost. Platí německé právo s vyloučením Úmluvy OSN o smlouvách o mezinárodní koupi zboží. Místně příslušným soudem je soud v Mnichově.

Příloha 1: Popis zpracování

Kategorie	Obsah
Předmět	Poskytování platformy SaaS Screenway včetně hostingu, přenosu dat, autentizace a řízení zobrazování
Doba trvání	Aktivní doba trvání smlouvy + 30 dnů přechodné lhůty pro export/výmaz
Povaha zpracování	Shromažďování, zaznamenávání, ukládání, pozměňování, vyhledávání, zobrazování, přenos, výmaz
Účel	Poskytování smluvně sjednané služby Screenway
Subjekty údajů	Zaměstnanci zákazníka, kterým jsou udělena přihlašovací/řídicí oprávnění ke Screenway
Kategorie údajů	Údaje o účtu (jméno, služební e-mail, role), přihlašovací údaje (hash hesla, session cookies, IP adresa), údaje o umístění obrazovek (označení, příp. adresa stanoviště), obsah nahraný zákazníkem (zpravidla **bez** osobních údajů – marketingové materiály, informační texty apod.)
Zvláštní kategorie údajů (čl. 9 GDPR)	Ve standardním provozu se **nezpracovávají**
Region hostingu	Výhradně Evropská unie – Hetzner Norimberk (primární) + Hetzner Helsinky (záložní zrcadlo)
Předávání do třetích zemí	**Žádné**

Příloha 2: Technická a organizační opatření (TOM)

Následující opatření TOM odpovídají čl. 32 GDPR a jsou kategorizována tak, jak to stanoví dozorové úřady a v oboru obvyklý standard GDPR-DPA. Opatření jsou dokumentována v systému řízení bezpečnosti informací (ISMS) Bergx2 podle ISO/IEC 27001:2022 a jsou interně podrobně vedena. Konkrétní detaily implementace (modely výrobců, konfigurační parametry, umístění jednotlivých komponent, mechanismy klíčů) nejsou z bezpečnostních důvodů v této veřejně přístupné smluvní příloze zveřejňovány. Na odůvodněnou žádost zákazníka v rámci jeho práva na audit podle § 9 poskytne Bergx2 GmbH příslušné podrobné doklady v rámci písemného závazku mlčenlivosti.

1. Důvěrnost (čl. 32 odst. 1 písm. b) GDPR)

Opatření	Realizace
Kontrola vstupu	Vícestupňová fyzická kontrola vstupu v sídle společnosti s mechanickou ochranou proti vloupání podle příslušných norem DIN, bezpečnostním zasklením, automaticky zamykanými dveřmi, kamerovou předběžnou kontrolou vstupu bez přenosu do externích sítí a vícefaktorovou autentizací na nejvnitřnější úrovni uzamčení. Oprávnění ke vstupu jsou udělována podle zásady need-to-be-present jmenovitě vymezenému okruhu osob a dokumentována ve vedeném registru klíčů s auditní stopou výdeje/vrácení. Zhotovení kopií klíčů je možné pouze se souhlasem pronajímatele prostřednictvím certifikovaných zámečníků. Návštěvníci vstupují do obchodních prostor pouze v doprovodu.
Kontrola přístupu (systémy)	Řízení přístupu na základě rolí (RBAC) ve všech produkčních systémech; vícefaktorová autentizace (MFA) pro administrátorské přístupy; závazná politika hesel podle stavu techniky; přístup k serverům založený na klíčích, resp. certifikátech bez hesla; povinné směrování administrátorských přístupů přes interní virtuální privátní síť (VPN).
Kontrola přístupu (údaje)	Oddělení tenantů pro každý zákaznický účet na úrovni databáze; pravidla přístupu na úrovni záznamů (row-level security); revizně bezpečné protokolování všech přístupů pro čtení a zápis k osobním údajům.
Pseudonymizace	Kdekoli je to slučitelné s účelem zpracování, jsou interní zpracování pseudonymizována. Periodická namátková kontrola nezamýšleného výskytu skutečných jmen je zavedena jako KPI bezpečnosti informací.
Šifrování	Šifrování přenosu podle stavu techniky pro všechna externí spojení s pravidelnou rotací certifikátů. Silné šifrování v klidovém stavu pro záložní média a pevné disky koncových zařízení. Citlivé přístupové údaje (hesla, tokeny, klíče) jsou spravovány výhradně v interním postupu odpovídajícím stavu techniky – podrobnosti nejsou z bezpečnostních důvodů zveřejňovány.

2. Integrita (čl. 32 odst. 1 písm. b) GDPR)

Opatření	Realizace
Kontrola zadávání	Serverová validace všech vstupů; revizně bezpečné auditní protokoly; práva zápisu výhradně prostřednictvím autentizovaných a autorizovaných programových rozhraní.
Kontrola předávání	Povinné šifrování přenosu pro všechna externí spojení; žádné předávání údajů bez doloženého smluvního základu.
Kontrola zakázek	Smlouvy o zpracování osobních údajů se všemi dílčími zpracovateli (viz příloha 3); strukturovaný proces řízení dodavatelů s periodickým přehodnocováním.

3. Dostupnost a odolnost (čl. 32 odst. 1 písm. b) GDPR)

Opatření	Realizace
Zálohování	Denní inkrementální zálohování produkčních systémů s geograficky odděleným zrcadlením **v rámci Evropské unie**; uchovává se více verzí; plánované testy obnovy ve čtvrtletním rytmu.
Dostupnost	Architektura cloud-first s hostingem v datových centrech certifikovaných podle ISO/IEC 27001 s rezervou nouzového napájení; nepřetržitý monitoring s definovanými eskalačními cestami.
Business continuity	Ověřený plán kontinuity činností včetně analýzy dopadů na podnikání; plná způsobilost znalostních funkcí k práci z domova; dokumentované doby obnovení provozu pro jednotlivé systémy.
Odolnost koncových zařízení	Náhradní koncové zařízení jako rezerva pro případ závady zařízení; dostatečné rezervy výdrže baterií pro krátkodobé výpadky napájení.

4. Postupy pravidelného testování, posuzování a hodnocení (čl. 32 odst. 1 písm. d) GDPR)

Opatření	Realizace
Systém řízení bezpečnosti informací (ISMS)	Zavedený ISMS podle ISO/IEC 27001:2022 se Statement of Applicability pro opatření Annex A; certifikace se připravuje.
Řízení ochrany osobních údajů	Vedené záznamy o činnostech zpracování; jmenovaný pověřenec pro ochranu osobních údajů; periodické přezkumy činností zpracování.
Povědomí	Strukturovaná a doložená školení bezpečnostního povědomí a ochrany osobních údajů pro všechny zaměstnance s povinnými moduly specifickými pro jednotlivé role.
Řízení rizik	Nejméně jednou ročně posouzení rizik se schválením vrcholovým vedením; plán zvládání rizik s přiřazenými opatřeními.
Řízení dodavatelů	Závazná směrnice a postup pro dodavatele; povinnost uzavření DPA se všemi zpracovateli; periodické přezkumy dodavatelů.
Incident response	Dokumentovaný postup řízení incidentů s definovanými cestami hlášení, stupni eskalace a ověřováním účinnosti.
Patch management	Vedený registr záplat s dohledatelným nasazováním záplat.
Přezkoumání vedením	Nejméně jednou ročně hodnocení vrcholovým vedením na základě kvantitativních KPI.
Interní audit	Roční nezávislý interní audit ISMS s dokumentovanými zjištěními a nápravnými opatřeními.

5. Životní cyklus záloh a výmaz

Osobní údaje v zálohách jsou definovanou rotací záloh během několika týdnů zcela přepsány.

Při skončení smlouvy proběhne konečný výmaz údajů na produkčních systémech do 30 dnů; rotace záloh následně údaje během několika týdnů vyřadí ze zálohovaného stavu.

Konkrétní retenční okna pro jednotlivé generace záloh jsou na odůvodněnou žádost zveřejněna v rámci práva na audit (§ 9).

Příloha 3: Seznam dílčích zpracovatelů

Stav ke dni: 25.05.2026.

Č.	Dílčí zpracovatel	Sídlo	Účel zpracování	Zpracovávané údaje	Certifikace / DPA
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Německo – datová centra v Německu a Finsku (EU)	Hosting produkční a záložní infrastruktury Screenway	Všechny údaje uvedené v příloze 1; výhradně šifrované at-rest a in transit	Certifikace ISO/IEC 27001 + ISO/IEC 9001; smlouva o zpracování osobních údajů aktivně akceptována společností Bergx2 GmbH; seznam subdodavatelů poskytovatele hostingu veřejně dostupný na www.hetzner.com/AV/subunternehmer.pdf

Upozornění k dalším dodavatelům Bergx2: Bergx2 GmbH využívá pro vlastní provoz podniku (komunikace se zaměstnanci, správa zdrojového kódu, kancelářské a produktivní nástroje) další poskytovatele SaaS. Ti nezpracovávají žádné zákaznické údaje z platformy Screenway, a nejsou proto dílčími zpracovateli ve smyslu této DPA. Na odůvodněnou žádost zákazníka v rámci jeho práva na audit (§ 9) Bergx2 GmbH zveřejní úplný seznam vlastních dodavatelů.

Účinnost

Tato DPA se akceptací v zákaznickém portálu s časovým razítkem a označením verze stává účinnou součástí smlouvy o službě Screenway (čl. 28 odst. 9 GDPR: písemně, v to počítaje i elektronickou formu).

Záznam o akceptaci je společností Bergx2 GmbH revizně bezpečně archivován v zákaznickém backendu a obsahuje nejméně:

- Označení verze této DPA (viz tabulka verzí níže)
- Datum a čas akceptace
- Identitu akceptující osoby (ID uživatele zákaznického účtu)
- Identitu zákazníka (ID účtu/smlouvy)
- Hodnotu hash akceptovaného znění smlouvy (kryptografický doklad integrity)

Při aktualizaci této DPA obdrží zákazník nejméně 30 dnů před nabytím účinnosti oznámení v textové podobě a při příštím přihlášení do zákaznického portálu výzvu k opětovné akceptaci.

Volitelný fyzický nebo kvalifikovaný elektronický podpis: Pokud si zákazník – např. na základě interních požadavků compliance – přeje dodatečný spolupodpis, může být DPA mezi smluvními stranami spolupodepsána fyzicky nebo pomocí kvalifikovaného elektronického podpisu (nařízení eIDAS (EU) č.

910/2014). Obstarání v tomto případě zajišťuje zákazník. Elektronická akceptace v zákaznickém portálu tím zůstává nedotčena a sama o sobě představuje uzavření smlouvy v souladu s GDPR.

Verzování

Verze	Stav
1.0	25.05.2026