# Umowa powierzenia przetwarzania danych (DPA) dla Screenway

> Niniejsza wersja jest wiążąca i może zostać skutecznie zawarta przez elektroniczną akceptację w portalu klienta (patrz sekcja „Skuteczność").

## Preambuła

Bergx2 GmbH prowadzi platformę Software-as-a-Service Screenway do sterowania digital signage. W ramach korzystania z usługi Bergx2 GmbH przetwarza dane osobowe na zlecenie klienta w rozumieniu art. 4 pkt 8 i art. 28 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych, RODO). Niniejsza umowa konkretyzuje obowiązki i prawa obu stron zgodnie z art. 28 ust. 3 RODO.

---

## § 1 Przedmiot i czas trwania przetwarzania

(1) Przedmiot. Bergx2 GmbH udostępnia klientowi platformę Screenway jako Software-as-a-Service. W ramach korzystania Bergx2 GmbH przetwarza opisane bliżej w załączniku 1 dane osobowe klienta wyłącznie zgodnie z jego poleceniami.

(2) Czas trwania. Umowa wchodzi w życie z chwilą zawarcia umowy głównej (umowa o usługę Screenway) i kończy się wraz z jej zakończeniem. Obowiązki usunięcia/zwrotu (§ 10) i zachowania poufności (§ 5 ust. 2) obowiązują także po zakończeniu okresu umowy.

---

## § 2 Rodzaj i cel przetwarzania

(1) Bergx2 GmbH przetwarza opisane w załączniku 1 dane osobowe w następujących celach:

- Udostępnianie platformy Screenway jako SaaS digital signage
- Przypisywanie lokalizacji ekranów do kont klientów
- Wyświetlanie treści przesłanych przez klienta na urządzeniach końcowych
- Uwierzytelnianie pracowników klienta przy logowaniu
- Świadczenie wsparcia, analizy błędów i monitoringu usługi

(2) Przetwarzanie do własnych celów Bergx2 GmbH (np. marketing, profilowanie, sprzedaż podmiotom trzecim) nie ma miejsca.

---

## § 3 Rodzaj danych osobowych i kategorie osób, których dane dotyczą

Konkretne wyliczenie – patrz załącznik 1. W skrócie:

- Rodzaj danych: dane kont, dane logowania, dane lokalizacji ekranów, treści przesłane przez klienta (z reguły nieosobowe)
- Kategorie osób, których dane dotyczą: pracownicy klientów (do logowania i przypisania kont)

Przetwarzanie szczególnych kategorii danych osobowych w rozumieniu art. 9 RODO nie ma miejsca w standardowej pracy Screenway. Jeżeli klient mimo to prześle takie dane, dzieje się to poza kategoriami objętymi niniejszą umową DPA i na własną odpowiedzialność klienta.

---

## § 4 Obowiązki i prawa administratora (klienta)

(1) Prawo wydawania poleceń. Klient pozostaje odpowiedzialny za zgodność przetwarzania z prawem (art. 24 RODO). Bergx2 GmbH przetwarza dane wyłącznie na udokumentowane polecenie klienta. Niniejsza umowa DPA stanowi ogólne polecenie; polecenia indywidualne są możliwe przez kanały komunikacji zdefiniowane w umowie o usługę.

(2) Rejestrowanie. Bergx2 GmbH dokumentuje procesy istotne dla poleceń w wewnętrznym śladzie audytowym ISMS (historia pull requestów, rejestr incydentów, rejestr dostawców).

(3) Obowiązki informacyjne. Klient jest zobowiązany do informowania osób, których dane dotyczą (swoich pracowników), zgodnie z art. 13 RODO o przetwarzaniu danych przez Bergx2 GmbH.

---

## § 5 Obowiązki podmiotu przetwarzającego (Bergx2 GmbH)

(1) Związanie poleceniami. Bergx2 GmbH przetwarza dane wyłącznie na udokumentowane polecenie klienta. W przypadku polecenia, które w ocenie Bergx2 GmbH jest niezgodne z prawem, Bergx2 GmbH niezwłocznie poinformuje klienta (art. 28 ust. 3 lit. h RODO).

(2) Poufność. Bergx2 GmbH zobowiązuje wszystkie osoby zajmujące się przetwarzaniem do zachowania poufności przed podjęciem czynności (art. 28 ust. 3 lit. b RODO). Następuje to przez oświadczenia o poufności (NDA) przy zatrudnieniu lub zleceniu i jest udokumentowane w ISMS Bergx2 (rejestr pracowników).

(3) Środki techniczne i organizacyjne. Bergx2 GmbH podejmuje opisane w załączniku 2 środki TOM, odpowiadające stanowi techniki i zapewniające poziom ochrony adekwatny do ryzyka (art. 32 RODO).

(4) Podprzetwarzający. Bergx2 GmbH korzysta z podprzetwarzających wymienionych w załączniku 3. Warunki i mechanizm zmian – patrz § 6.

(5) Wsparcie. Bergx2 GmbH wspiera klienta w wypełnianiu jego obowiązków z art. 32–36 RODO, w szczególności przy odpowiadaniu na wnioski osób, których dane dotyczą (§ 7), i zgłaszaniu naruszeń ochrony danych (§ 8).

(6) Dowody. Bergx2 GmbH udostępnia klientowi na wniosek informacje i dokumenty niezbędne do kontroli (art. 28 ust. 3 lit. h RODO). Dalsze zasady audytu – patrz § 9.

---

## § 6 Podprzetwarzający

(1) Zgoda. Zawierając niniejszą umowę DPA, klient wyraża ogólną zgodę na zlecanie podprzetwarzającym wymienionym w załączniku 3 (art. 28 ust. 2 zd. 1 RODO).

(2) Powiadomienie o zmianach. Bergx2 GmbH informuje klienta o zamierzonych zmianach w składzie podprzetwarzających (dodanie lub wymiana) co najmniej 30 dni przed wejściem w życie w formie tekstowej (e-mail na adres kontaktowy ds. ochrony danych zapisany w umowie o usługę).

(3) Prawo sprzeciwu. Klient może sprzeciwić się zmianie w terminie 30 dni z uzasadnionych powodów. W przypadku sprzeciwu Bergx2 GmbH szuka z klientem polubownego rozwiązania; jeśli się to nie powiedzie, klientowi przysługuje nadzwyczajne prawo wypowiedzenia umowy o usługę.

(4) Zobowiązanie. Bergx2 GmbH zobowiązuje każdego podprzetwarzającego umownie do obowiązków uzgodnionych w niniejszej umowie DPA (art. 28 ust. 4 RODO).

---

## § 7 Współdziałanie przy prawach osób, których dane dotyczą

Bergx2 GmbH wspiera klienta odpowiednimi środkami technicznymi i organizacyjnymi, w miarę możliwości, w wypełnianiu praw osób, których dane dotyczą, z rozdziału III RODO (dostęp, sprostowanie, usunięcie, ograniczenie, przenoszenie danych, sprzeciw).

Konkretnie: Bergx2 GmbH przekazuje odpowiednie wnioski, które osoby kierują bezpośrednio do Bergx2 GmbH, niezwłocznie klientowi i daje mu możliwość odpowiedzi. Samodzielna odpowiedź Bergx2 GmbH następuje tylko na wyraźne polecenie klienta.

---

## § 8 Zgłaszanie naruszeń ochrony danych

(1) Bergx2 GmbH informuje klienta niezwłocznie, najpóźniej w ciągu 24 godzin od powzięcia wiadomości, o każdym stwierdzonym naruszeniu ochrony danych w obszarze odpowiedzialności Bergx2 GmbH lub podprzetwarzającego, dotyczącym danych osobowych klienta.

(2) Zgłoszenie następuje pisemnie (e-mail na adres kontaktowy klienta ds. ochrony danych) i zawiera minimalne informacje wymienione w art. 33 ust. 3 RODO (rodzaj i zakres naruszenia, liczba osób dotkniętych, przewidywane skutki, podjęte środki zaradcze).

(3) Bergx2 GmbH dokumentuje własne naruszenia ochrony danych wewnętrznie w rejestrze incydentów (patrz `incidents/incidents.md` ISMS Bergx2, procedura zgodnie z `documents/verfahren/incident-management-verfahren.md`).

(4) Obowiązek zgłoszenia do właściwego organu nadzorczego zgodnie z art. 33 RODO i ewentualnie osobom, których dane dotyczą, zgodnie z art. 34 RODO pozostaje przy kliencie jako administratorze. Bergx2 GmbH wspiera klienta przy tych zgłoszeniach wszystkimi niezbędnymi informacjami.

---

## § 9 Prawa audytu i kontroli

(1) Dowód. Bergx2 GmbH udostępnia klientowi na wniosek informacje niezbędne do wykazania wypełniania obowiązków z niniejszej umowy DPA, w szczególności aktualną wersję środków TOM (załącznik 2) i listy podprzetwarzających (załącznik 3) oraz ewentualnie wyciągi z certyfikacji.

(2) Kontrola na miejscu. Klient ma prawo przekonać się o przestrzeganiu środków TOM na miejscu w siedzibie Bergx2 GmbH lub w lokalizacjach przetwarzania. Terminy należy zapowiedzieć pisemnie co najmniej cztery tygodnie wcześniej; kontrole należy ograniczyć do niezbędnego zakresu i nie mogą one nieproporcjonalnie zakłócać działalności. Maksymalnie jedna kontrola w roku kalendarzowym, z wyjątkiem uzasadnionych przypadków.

(3) Uznawanie certyfikacji. O ile Bergx2 GmbH jest certyfikowana według ISO/IEC 27001:2022 (certyfikacja w przygotowaniu) lub przedłoży równoważne niezależne kontrole podmiotów trzecich, zastępuje to kontrolę klienta na miejscu, o ile zakres certyfikacji obejmuje przedmiot umowy.

---

## § 10 Usunięcie i zwrot po zakończeniu umowy

(1) Po zakończeniu umowy o usługę Bergx2 GmbH – według wyboru klienta – dane osobowe:

- w całości zwróci (eksport w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego), lub
- w całości usunie (bezpieczne nadpisanie zgodnie ze stanem techniki), i to

w ciągu 30 dni od zakończenia umowy.

(2) Kopie zapasowe zawierające dane osobowe są zgodnie z załącznikiem 2 TOM § Cykl życia kopii zapasowych w ramach rotacji całkowicie nadpisywane najpóźniej po pięciu tygodniach (rotacja kopii). Bergx2 GmbH dokumentuje ostateczne usunięcie pisemnie na wniosek.

(3) Ustawowe obowiązki przechowywania pozostają nienaruszone (np. dane rozliczeniowe zgodnie z § 257 HGB, § 147 AO).

---

## § 11 Odpowiedzialność i postanowienia końcowe

(1) Odpowiedzialność. Obowiązują regulacje umowy głównej (umowa o usługę Screenway) i art. 82 RODO. Przy naruszeniu niniejszej umowy DPA odpowiedzialna strona odpowiada wobec osoby, której dane dotyczą.

(2) Forma. Zmiany i uzupełnienia wymagają formy tekstowej.

(3) Klauzula salwatoryjna. Jeżeli poszczególne postanowienia okażą się nieskuteczne, skuteczność pozostałych pozostaje nienaruszona.

(4) Prawo właściwe i sąd. Obowiązuje prawo niemieckie z wyłączeniem Konwencji ONZ o umowach międzynarodowej sprzedaży towarów. Sądem właściwym jest Monachium.

---

## Załącznik 1: Opis przetwarzania

| Kategoria | Treść |
|---|---|
| **Przedmiot** | Udostępnianie platformy SaaS Screenway wraz z hostingiem, transmisją danych, uwierzytelnianiem i sterowaniem wyświetlaniem |
| **Czas trwania** | Aktywny okres umowy + 30 dni okresu przejściowego na eksport/usunięcie |
| **Rodzaj przetwarzania** | Zbieranie, utrwalanie, przechowywanie, modyfikowanie, przeglądanie, wyświetlanie, przesyłanie, usuwanie |
| **Cel** | Świadczenie uzgodnionej umownie usługi Screenway |
| **Osoby, których dane dotyczą** | Pracownicy klienta, którym przyznano dostęp logowania/sterowania do Screenway |
| **Kategorie danych** | Dane kont (imię i nazwisko, służbowy e-mail, rola), dane logowania (hash hasła, pliki cookie sesji, adres IP), dane lokalizacji ekranów (nazwa, ew. adres lokalizacji), treści przesłane przez klienta (z reguły **nie**osobowe – materiały marketingowe, teksty informacyjne itp.) |
| **Szczególne kategorie danych (art. 9 RODO)** | W standardowej pracy **nie**przetwarzane |
| **Region hostingu** | Wyłącznie Unia Europejska – Hetzner Norymberga (główny) + Hetzner Helsinki (lustro kopii zapasowych) |
| **Transfer do państw trzecich** | **Brak** |

---

## Załącznik 2: Środki techniczne i organizacyjne (TOM)

Poniższe środki TOM odpowiadają art. 32 RODO i są skategoryzowane tak, jak wymagają tego organy nadzorcze i branżowy standard RODO-DPA. Środki są dokumentowane w systemie zarządzania bezpieczeństwem informacji (ISMS) Bergx2 według ISO/IEC 27001:2022 i prowadzone wewnętrznie w szczegółach. Konkretne szczegóły implementacji (modele producentów, parametry konfiguracji, lokalizacje poszczególnych komponentów, mechanizmy kluczy) nie są ze względów bezpieczeństwa ujawniane w niniejszym publicznie dostępnym załączniku umownym. Na uzasadniony wniosek klienta w ramach jego prawa audytu z § 9 Bergx2 GmbH udostępni odpowiednie szczegółowe dowody w ramach pisemnych ram poufności.

### 1. Poufność (art. 32 ust. 1 lit. b RODO)

| Środek | Realizacja |
|---|---|
| **Kontrola dostępu fizycznego** | Wielostopniowa fizyczna kontrola dostępu w siedzibie z mechaniczną ochroną przed włamaniem zgodnie z odpowiednimi normami DIN, szkleniem bezpiecznym, automatycznie ryglowanymi drzwiami, kamerową wstępną kontrolą wejścia bez transmisji do sieci zewnętrznych i uwierzytelnianiem wieloskładnikowym na najgłębszym poziomie zamknięcia. Uprawnienia dostępu są nadawane według zasady need-to-be-present imiennie ograniczonemu kręgowi osób i dokumentowane w prowadzonym rejestrze kluczy ze śladem audytowym wydań/zwrotów. Reprodukcja kluczy jest możliwa tylko za zgodą wynajmującego przez certyfikowanych ślusarzy. Goście wchodzą do pomieszczeń firmowych tylko w towarzystwie. |
| **Kontrola dostępu (systemy)** | Kontrola dostępu oparta na rolach (RBAC) we wszystkich systemach produkcyjnych; uwierzytelnianie wieloskładnikowe (MFA) dla dostępów administracyjnych; wiążąca polityka haseł według stanu techniki; dostęp do serwerów oparty na kluczach lub certyfikatach bez hasła; obowiązkowe kierowanie dostępów administracyjnych przez wewnętrzną wirtualną sieć prywatną (VPN). |
| **Kontrola dostępu (dane)** | Separacja tenantów na konto klienta na poziomie bazy danych; reguły dostępu na poziomie rekordów (row-level security); rewizyjnie bezpieczne protokołowanie wszystkich dostępów odczytu i zapisu do danych osobowych. |
| **Pseudonimizacja** | Wszędzie tam, gdzie da się to pogodzić z celem przetwarzania, wewnętrzne przetwarzania są pseudonimizowane. Okresowa kontrola wyrywkowa na niezamierzone wystąpienia prawdziwych nazwisk jest ustanowiona jako KPI bezpieczeństwa informacji. |
| **Szyfrowanie** | Szyfrowanie transportu według stanu techniki dla wszystkich połączeń zewnętrznych z regularną rotacją certyfikatów. Silne szyfrowanie w spoczynku dla nośników kopii zapasowych i dysków urządzeń końcowych. Wrażliwe dane dostępowe (hasła, tokeny, klucze) są zarządzane wyłącznie w wewnętrznej procedurze odpowiadającej stanowi techniki – szczegóły nie są ujawniane ze względów bezpieczeństwa. |

### 2. Integralność (art. 32 ust. 1 lit. b RODO)

| Środek | Realizacja |
|---|---|
| **Kontrola wprowadzania** | Walidacja wszystkich danych wejściowych po stronie serwera; rewizyjnie bezpieczne protokoły audytu; prawa zapisu wyłącznie przez uwierzytelnione i autoryzowane interfejsy programistyczne. |
| **Kontrola przekazywania** | Obowiązkowe szyfrowanie transportu dla wszystkich połączeń zewnętrznych; żadnego przekazywania danych bez udokumentowanej podstawy umownej. |
| **Kontrola zleceń** | Umowy powierzenia przetwarzania ze wszystkimi podprzetwarzającymi (patrz załącznik 3); ustrukturyzowany proces zarządzania dostawcami z okresową ponowną oceną. |

### 3. Dostępność i odporność (art. 32 ust. 1 lit. b RODO)

| Środek | Realizacja |
|---|---|
| **Kopie zapasowe** | Codzienna przyrostowa kopia zapasowa systemów produkcyjnych z geograficznie oddzielonym lustrem **w Unii Europejskiej**; przechowywanych jest kilka wersji; planowe testy odtwarzania w rytmie kwartalnym. |
| **Dostępność** | Architektura cloud-first z hostingiem w centrach danych certyfikowanych ISO/IEC 27001 z rezerwą zasilania awaryjnego; ciągły monitoring ze zdefiniowanymi ścieżkami eskalacji. |
| **Business continuity** | Sprawdzony plan ciągłości działania wraz z analizą wpływu na biznes; pełna zdolność pracy zdalnej funkcji opartych na wiedzy; udokumentowane czasy wznowienia dla każdego systemu. |
| **Odporność urządzeń końcowych** | Zapasowe urządzenie końcowe jako rezerwa na wypadek usterki; wystarczające rezerwy czasu pracy akumulatorów na krótkotrwałe przerwy w zasilaniu. |

### 4. Procedury regularnego przeglądu, oceny i ewaluacji (art. 32 ust. 1 lit. d RODO)

| Środek | Realizacja |
|---|---|
| **System zarządzania bezpieczeństwem informacji (ISMS)** | Ustanowiony ISMS według ISO/IEC 27001:2022 ze Statement of Applicability dla kontroli Annex A; certyfikacja w przygotowaniu. |
| **Zarządzanie ochroną danych** | Prowadzony rejestr czynności przetwarzania; powołana inspektor ochrony danych; okresowe przeglądy czynności przetwarzania. |
| **Świadomość** | Ustrukturyzowane i udokumentowane szkolenia świadomościowe i z ochrony danych dla wszystkich pracowników z obowiązkowymi modułami dla ról. |
| **Zarządzanie ryzykiem** | Co najmniej coroczna ocena ryzyka z zatwierdzeniem najwyższego kierownictwa; plan postępowania z ryzykiem z przypisanymi środkami. |
| **Zarządzanie dostawcami** | Wiążąca polityka i procedura dostawców; obowiązek DPA dla wszystkich podmiotów przetwarzających; okresowe przeglądy dostawców. |
| **Incident response** | Udokumentowana procedura zarządzania incydentami ze zdefiniowanymi ścieżkami zgłoszeń, stopniami eskalacji i weryfikacją skuteczności. |
| **Zarządzanie poprawkami** | Prowadzony rejestr poprawek z możliwą do prześledzenia aplikacją poprawek. |
| **Przegląd zarządczy** | Co najmniej coroczna ocena przez najwyższe kierownictwo na podstawie ilościowych KPI. |
| **Audyt wewnętrzny** | Coroczny niezależny wewnętrzny audyt ISMS z udokumentowanymi ustaleniami i działaniami korygującymi. |

### 5. Cykl życia kopii zapasowych i usuwanie

Dane osobowe w kopiach zapasowych są przez zdefiniowaną rotację kopii całkowicie nadpisywane w ciągu kilku tygodni.

Po zakończeniu umowy ostateczne usunięcie danych na systemach produkcyjnych następuje w ciągu 30 dni; rotacja kopii zapasowych wyklucza następnie dane z zasobów w ciągu kilku tygodni.

Konkretne okna retencji na generację kopii są ujawniane na uzasadniony wniosek w ramach prawa audytu (§ 9).

---

## Załącznik 3: Lista podprzetwarzających

Stan: 25.05.2026.

| Nr | Podprzetwarzający | Siedziba | Cel przetwarzania | Przetwarzane dane | Certyfikacje / DPA |
|---|---|---|---|---|---|
| 1 | **Hetzner Online GmbH** | Industriestraße 25, 91710 Gunzenhausen, Niemcy – centra danych w Niemczech i Finlandii (UE) | Hosting infrastruktury produkcyjnej i kopii zapasowych Screenway | Wszystkie dane wymienione w załączniku 1; wyłącznie szyfrowane at-rest i in transit | Certyfikaty ISO/IEC 27001 + ISO/IEC 9001; umowa powierzenia przetwarzania aktywnie zaakceptowana przez Bergx2 GmbH; lista podwykonawców hostera publicznie pod www.hetzner.com/AV/subunternehmer.pdf |

Uwaga o dalszych dostawcach Bergx2: Bergx2 GmbH korzysta na potrzeby własnej działalności (komunikacja pracownicza, zarządzanie kodem źródłowym, narzędzia biurowe i produktywności) z dalszych usługodawców SaaS. Nie przetwarzają oni danych klientów z platformy Screenway i nie są zatem podprzetwarzającymi w rozumieniu niniejszej umowy DPA. Na uzasadniony wniosek klienta w ramach jego prawa audytu (§ 9) Bergx2 GmbH ujawni pełną listę własnych dostawców.

---

## Skuteczność

Niniejsza umowa DPA staje się przez akceptację w portalu klienta ze znacznikiem czasu i oznaczeniem wersji skutecznym elementem umowy o usługę Screenway (art. 28 ust. 9 RODO: forma pisemna także w formacie elektronicznym).

Zapis akceptacji jest przez Bergx2 GmbH archiwizowany w backendzie klienta w sposób rewizyjnie bezpieczny i obejmuje co najmniej:

- Oznaczenie wersji niniejszej umowy DPA (patrz tabela wersji poniżej)
- Datę i godzinę akceptacji
- Tożsamość osoby akceptującej (ID użytkownika konta klienta)
- Tożsamość klienta (ID konta/umowy)
- Wartość hash zaakceptowanej wersji umowy (kryptograficzny dowód integralności)

Przy aktualizacji niniejszej umowy DPA klient otrzymuje co najmniej 30 dni przed wejściem w życie powiadomienie w formie tekstowej oraz przy następnym logowaniu do portalu klienta wezwanie do ponownej akceptacji.

Opcjonalny podpis fizyczny lub kwalifikowany elektroniczny: jeżeli klient – np. ze względu na wewnętrzne wymogi compliance – życzy sobie dodatkowego kontrasygnowania, umowa DPA może zostać kontrasygnowana fizycznie lub za pomocą kwalifikowanego podpisu elektronicznego (rozporządzenie eIDAS (UE) nr 910/2014) między stronami umowy. Dostarczenie następuje w tym przypadku przez klienta. Elektroniczna akceptacja w portalu klienta pozostaje nienaruszona i sama w sobie stanowi zgodne z RODO zawarcie umowy.

---

## Wersjonowanie

| Wersja | Stan |
|---|---|
| 1.0 | 25.05.2026 |