> Nota: A versão vinculativa do presente acordo de subcontratação do tratamento de dados é o original alemão, disponível em `/rechtliches/avv`. Esta tradução para português é disponibilizada apenas a título informativo. Em caso de divergências, prevalece a versão alemã.

Acordo de subcontratação do tratamento de dados (DPA) para a Screenway

> A presente versão é vinculativa e pode ser validamente celebrada mediante aceitação eletrónica no portal de clientes (ver a secção «Eficácia»).

Preâmbulo

A Bergx2 GmbH opera a plataforma de software como serviço Screenway para a gestão de Digital Signage. No âmbito da utilização do serviço, a Bergx2 GmbH trata dados pessoais por conta do cliente, na aceção do artigo 4.º, ponto 8, e do artigo 28.º do Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados, RGPD). O presente acordo concretiza as obrigações e os direitos de ambas as partes nos termos do artigo 28.º, n.º 3, do RGPD.

---

§ 1 Objeto e duração do tratamento

(1) Objeto. A Bergx2 GmbH disponibiliza ao cliente a plataforma Screenway como software como serviço. No âmbito da utilização, a Bergx2 GmbH trata os dados pessoais do cliente descritos em maior detalhe no Anexo 1 exclusivamente de acordo com as instruções deste.

(2) Duração. O acordo entra em vigor com a celebração do contrato principal subjacente (contrato de serviço Screenway) e cessa com a cessação deste. As obrigações de apagamento/devolução (§ 10) e de confidencialidade (§ 5, n.º 2) subsistem para além da duração do contrato.

---

§ 2 Natureza e finalidade do tratamento

(1) A Bergx2 GmbH trata os dados pessoais descritos no Anexo 1 para as seguintes finalidades:

- Disponibilização da plataforma Screenway como SaaS de Digital Signage
- Atribuição das localizações dos ecrãs às contas de cliente
- Apresentação, nos dispositivos terminais, dos conteúdos carregados pelo cliente
- Autenticação dos colaboradores do cliente no início de sessão
- Prestação de suporte, análise de erros e monitorização do serviço

(2) Não é efetuado qualquer tratamento para fins próprios da Bergx2 GmbH (p. ex., marketing, definição de perfis, venda a terceiros).

---

§ 3 Tipo de dados pessoais e categorias de titulares dos dados

Para a enumeração concreta, ver o Anexo 1. Em resumo:

- Tipo de dados: dados de conta, dados de início de sessão, dados de localização dos ecrãs, conteúdos carregados pelo cliente (em regra, não pessoais)
- Categorias de titulares dos dados: colaboradores dos clientes (para o início de sessão e a atribuição de contas)

No funcionamento normal da Screenway não são tratadas categorias especiais de dados pessoais na aceção do artigo 9.º do RGPD. Caso o cliente carregue, ainda assim, tais dados, tal ocorre fora das categorias abrangidas pelo presente DPA e sob a exclusiva responsabilidade do cliente.

---

§ 4 Obrigações e direitos do responsável pelo tratamento (cliente)

(1) Poder de instrução. O cliente continua a ser responsável pela licitude do tratamento (artigo 24.º do RGPD). A Bergx2 GmbH trata os dados exclusivamente mediante instruções documentadas do cliente. O presente DPA vale como instrução geral; instruções individuais são possíveis através dos canais de comunicação definidos no contrato de serviço.

(2) Registo. A Bergx2 GmbH documenta os processos relevantes para as instruções na pista de auditoria interna do SGSI (histórico de pull requests, registo de incidentes, registo de fornecedores).

(3) Deveres de informação. O cliente é obrigado a informar os titulares dos dados (os seus colaboradores) sobre o tratamento de dados pela Bergx2 GmbH, nos termos do artigo 13.º do RGPD.

---

§ 5 Obrigações do subcontratante (Bergx2 GmbH)

(1) Vinculação às instruções. A Bergx2 GmbH trata os dados exclusivamente mediante instruções documentadas do cliente. Se, no entender da Bergx2 GmbH, uma instrução for ilícita, a Bergx2 GmbH informará imediatamente o cliente (artigo 28.º, n.º 3, alínea h), do RGPD).

(2) Confidencialidade. A Bergx2 GmbH obriga à confidencialidade todas as pessoas envolvidas no tratamento antes do início da respetiva atividade (artigo 28.º, n.º 3, alínea b), do RGPD). Tal é feito mediante declarações de confidencialidade (NDA) no momento da contratação ou da adjudicação e encontra-se documentado no SGSI da Bergx2 (registo de colaboradores).

(3) Medidas técnicas e organizativas. A Bergx2 GmbH adota as MTO descritas no Anexo 2, que correspondem ao estado da técnica e garantem um nível de proteção adequado ao risco (artigo 32.º do RGPD).

(4) Subcontratantes ulteriores. A Bergx2 GmbH recorre aos subcontratantes ulteriores enumerados no Anexo 3. Para as condições e o mecanismo de alteração, ver o § 6.

(5) Assistência. A Bergx2 GmbH presta assistência ao cliente no cumprimento das suas obrigações nos termos dos artigos 32.º a 36.º do RGPD, em particular na resposta a pedidos dos titulares dos dados (§ 7) e na notificação de violações de dados pessoais (§ 8).

(6) Comprovativos. A Bergx2 GmbH disponibiliza ao cliente, a pedido, as informações e os documentos necessários à verificação (artigo 28.º, n.º 3, alínea h), do RGPD). Para outras modalidades de auditoria, ver o § 9.

---

§ 6 Subcontratantes ulteriores

(1) Autorização. Com a celebração do presente DPA, o cliente autoriza de forma geral o recurso aos subcontratantes ulteriores enumerados no Anexo 3 (artigo 28.º, n.º 2, primeira frase, do RGPD).

(2) Notificação de alterações. A Bergx2 GmbH informa o cliente sobre as alterações previstas ao conjunto de subcontratantes ulteriores (adição ou substituição) com, pelo menos, 30 dias de antecedência relativamente à sua produção de efeitos, sob forma de texto (correio eletrónico para o endereço de contacto para a proteção de dados indicado no contrato de serviço).

(3) Direito de oposição. O cliente pode opor-se à alteração, por motivos legítimos, dentro do prazo de 30 dias. Em caso de oposição, a Bergx2 GmbH procurará, em conjunto com o cliente, uma solução consensual; se tal não for possível, o cliente tem o direito de resolução extraordinária do contrato de serviço.

(4) Vinculação. A Bergx2 GmbH vincula contratualmente, por sua vez, cada subcontratante ulterior às obrigações acordadas no presente DPA (artigo 28.º, n.º 4, do RGPD).

---

§ 7 Colaboração no exercício dos direitos dos titulares dos dados

A Bergx2 GmbH presta assistência ao cliente, na medida do possível, com medidas técnicas e organizativas adequadas, no cumprimento dos direitos dos titulares dos dados previstos no Capítulo III do RGPD (acesso, retificação, apagamento, limitação, portabilidade dos dados, oposição).

Em concreto: a Bergx2 GmbH reencaminha imediatamente ao cliente os pedidos correspondentes que os titulares dos dados dirijam diretamente à Bergx2 GmbH e dá-lhe a possibilidade de responder. A Bergx2 GmbH só responde por si própria mediante instrução expressa do cliente.

---

§ 8 Notificação de violações de dados pessoais

(1) A Bergx2 GmbH informa o cliente imediatamente, o mais tardar no prazo de 24 horas após a tomada de conhecimento, sobre qualquer violação de dados pessoais constatada na esfera de responsabilidade da Bergx2 GmbH ou de um subcontratante ulterior que afete dados pessoais do cliente.

(2) A notificação é feita por escrito (correio eletrónico para o endereço de contacto para a proteção de dados do cliente) e contém as informações mínimas referidas no artigo 33.º, n.º 3, do RGPD (natureza e âmbito da violação, número de titulares afetados, consequências prováveis, medidas corretivas adotadas).

(3) A Bergx2 GmbH documenta internamente as suas próprias violações de dados pessoais no registo de incidentes (ver `incidents/incidents.md` do SGSI da Bergx2, procedimento nos termos de `documents/verfahren/incident-management-verfahren.md`).

(4) A obrigação de notificação à autoridade de controlo competente nos termos do artigo 33.º do RGPD e, se aplicável, aos titulares dos dados nos termos do artigo 34.º do RGPD permanece a cargo do cliente enquanto responsável pelo tratamento. A Bergx2 GmbH presta assistência ao cliente nestas notificações com todas as informações necessárias.

---

§ 9 Direitos de auditoria e de controlo

(1) Comprovativo. A Bergx2 GmbH disponibiliza ao cliente, a pedido, as informações necessárias ao cumprimento das obrigações decorrentes do presente DPA, em particular a versão atual das MTO (Anexo 2) e da lista de subcontratantes ulteriores (Anexo 3), bem como, se aplicável, extratos de certificações.

(2) Inspeção no local. O cliente tem o direito de se certificar do cumprimento das MTO no local, na sede da Bergx2 GmbH ou nos locais do tratamento. As datas devem ser comunicadas por escrito com, pelo menos, quatro

semanas de antecedência; as inspeções devem limitar-se ao necessário e não podem perturbar de forma desproporcionada a atividade empresarial. No máximo, uma inspeção por ano civil, salvo motivo fundamentado.

(3) Reconhecimento de certificações. Na medida em que a Bergx2 GmbH esteja certificada segundo a ISO/IEC 27001:2022 (certificação em preparação) ou apresente verificações independentes equivalentes por terceiros, tal substitui a inspeção no local pelo cliente, desde que o âmbito da certificação abranja o objeto do contrato.

---

§ 10 Apagamento e devolução após a cessação do contrato

(1) Com a cessação do contrato de serviço, a Bergx2 GmbH – à escolha do cliente – procederá, relativamente aos dados pessoais, de uma das seguintes formas:

- devolução integral (exportação num formato estruturado, de uso corrente e de leitura automática), ou
- apagamento integral (sobrescrita segura de acordo com o estado da técnica), e

no prazo de 30 dias após a cessação do contrato.

(2) As cópias de segurança que contenham dados pessoais são integralmente sobrescritas por rotação, nos termos do Anexo 2, MTO, § Ciclo de vida das cópias de segurança, o mais tardar após cinco semanas (rotação de cópias de segurança). A Bergx2 GmbH documenta o apagamento final por escrito, a pedido.

(3) As obrigações legais de conservação não são afetadas (p. ex., dados de faturação nos termos do § 257 do Código Comercial alemão (HGB) e do § 147 do Código Tributário alemão (AO)).

---

§ 11 Responsabilidade e disposições finais

(1) Responsabilidade. Aplicam-se as disposições do contrato principal (contrato de serviço Screenway) e o artigo 82.º do RGPD. Em caso de violação do presente DPA, a parte responsável em cada caso responde perante o titular dos dados.

(2) Forma escrita. As alterações e os aditamentos carecem de forma de texto.

(3) Cláusula de salvaguarda. Caso alguma das disposições seja inválida, a validade das restantes não é afetada.

(4) Direito aplicável e foro competente. Aplica-se o direito alemão, com exclusão da Convenção das Nações Unidas sobre os Contratos de Compra e Venda Internacional de Mercadorias. O foro competente é Munique.

Anexo 1: Descrição do tratamento

Categoria	Conteúdo
Objeto	Disponibilização da plataforma SaaS Screenway, incl. alojamento, transmissão de dados, autenticação e controlo da apresentação
Duração	Vigência ativa do contrato + 30 dias de período transitório para exportação/apagamento
Natureza do tratamento	Recolha, registo, conservação, alteração, consulta, apresentação, transmissão, apagamento
Finalidade	Prestação do serviço Screenway contratualmente acordado
Titulares dos dados	Colaboradores do cliente aos quais são concedidos acessos de início de sessão/controlo à Screenway
Categorias de dados	Dados de conta (nome, endereço de correio eletrónico profissional, função), dados de início de sessão (hash da palavra-passe, cookies de sessão, endereço IP), dados de localização dos ecrãs (designação e, se aplicável, morada da localização), conteúdos carregados pelo cliente (em regra **não** pessoais – material de marketing, textos informativos, etc.)
Categorias especiais de dados (artigo 9.º do RGPD)	**Não** tratadas no funcionamento normal
Região de alojamento	Exclusivamente na União Europeia – Hetzner Nuremberga (primário) + Hetzner Helsínquia (réplica de cópias de segurança)
Transferência para países terceiros	**Nenhuma**

Anexo 2: Medidas técnicas e organizativas (MTO)

As MTO seguintes correspondem ao artigo 32.º do RGPD e estão categorizadas conforme estabelecido pelas autoridades de controlo e pelo padrão habitual do setor para DPA em conformidade com o RGPD. As medidas são documentadas no sistema de gestão da segurança da informação (SGSI) da Bergx2, segundo a ISO/IEC 27001:2022, e mantidas internamente em detalhe. Os detalhes concretos de implementação (modelos de fabricantes, parâmetros de configuração, localizações de componentes individuais, mecanismos de chaves) não são divulgados neste anexo contratual de acesso público, por motivos de segurança. Mediante pedido fundamentado do cliente, no âmbito do seu direito de auditoria nos termos do § 9, a Bergx2 GmbH disponibiliza os comprovativos de detalhe pertinentes no quadro de um acordo escrito de confidencialidade.

1. Confidencialidade (artigo 32.º, n.º 1, alínea b), do RGPD)

Medida	Implementação
Controlo de acesso físico	Controlo de acesso físico de vários níveis na sede, com proteção mecânica anti-intrusão de acordo com as normas DIN aplicáveis, vidro de segurança, portas com trancamento automático, controlo prévio de entrada assistido por câmara sem transmissão para redes externas e autenticação multifator no nível de fecho mais interno. As autorizações de acesso são atribuídas segundo o princípio da necessidade de presença («need to be present») a um círculo de pessoas nominalmente limitado e documentadas num registo de chaves com pista de auditoria de entrega/devolução. A reprodução de chaves só é possível com autorização do senhorio, através de serralheiros certificados. Os visitantes só entram nas instalações acompanhados.
Controlo de acesso (sistemas)	Controlo de acesso baseado em funções (RBAC) em todos os sistemas de produção; autenticação multifator (MFA) para acessos administrativos; política de palavras-passe vinculativa de acordo com o estado da técnica; acesso aos servidores baseado em chaves ou certificados, sem palavra-passe; encaminhamento obrigatório dos acessos administrativos através de uma rede privada virtual (VPN) interna.
Controlo de acesso (dados)	Separação de inquilinos (tenants) por conta de cliente ao nível da base de dados; regras de acesso ao nível do registo (Row-Level-Security); registo auditável e inalterável de todos os acessos de leitura e escrita a dados pessoais.
Pseudonimização	Sempre que compatível com a finalidade do tratamento, os tratamentos internos são pseudonimizados. Está estabelecida, como KPI de segurança da informação, uma verificação periódica por amostragem de ocorrências involuntárias de nomes reais.
Cifragem	Cifragem do transporte de acordo com o estado da técnica para todas as ligações externas, com rotação regular de certificados. Cifragem forte em repouso para suportes de cópias de segurança e discos rígidos de dispositivos terminais. Os dados de acesso sensíveis (palavras-passe, tokens, chaves) são geridos exclusivamente através de um procedimento interno conforme ao estado da técnica – os detalhes não são divulgados por motivos de segurança.

2. Integridade (artigo 32.º, n.º 1, alínea b), do RGPD)

Medida	Implementação
Controlo de introdução de dados	Validação do lado do servidor de todas as entradas; registos de auditoria inalteráveis; direitos de escrita exclusivamente através de interfaces de programação autenticadas e autorizadas.
Controlo de transmissão	Cifragem do transporte obrigatória para todas as ligações externas; nenhuma transmissão de dados sem base contratual documentada.
Controlo de subcontratação	Acordos de subcontratação do tratamento de dados com todos os subcontratantes ulteriores (ver o Anexo 3); processo estruturado de gestão de fornecedores com reavaliação periódica.

3. Disponibilidade e resiliência (artigo 32.º, n.º 1, alínea b), do RGPD)

Medida	Implementação
Cópias de segurança	Cópia de segurança incremental diária dos sistemas de produção com replicação geograficamente separada **dentro da União Europeia**; são conservadas várias versões; testes de restauro programados com periodicidade trimestral.
Disponibilidade	Arquitetura «cloud first» com alojamento em centros de dados certificados ISO/IEC 27001 com reserva de energia de emergência; monitorização contínua com vias de escalonamento definidas.
Continuidade de negócio	Plano de continuidade de negócio verificado, incluindo análise de impacto no negócio; plena capacidade de teletrabalho das funções baseadas no conhecimento; tempos de retoma documentados por sistema.
Resiliência dos dispositivos terminais	Dispositivo terminal de substituição como reserva em caso de avaria; reservas suficientes de autonomia de bateria para falhas de energia de curta duração.

4. Procedimentos de verificação, apreciação e avaliação regulares (artigo 32.º, n.º 1, alínea d), do RGPD)

Medida	Implementação
Sistema de gestão da segurança da informação (SGSI)	SGSI estabelecido segundo a ISO/IEC 27001:2022 com declaração de aplicabilidade sobre os controlos do Anexo A; certificação em preparação.
Gestão da proteção de dados	Registo das atividades de tratamento mantido; encarregados de proteção de dados designados; revisões periódicas das atividades de tratamento.
Sensibilização	Ações de sensibilização e formação em proteção de dados estruturadas e comprovadas para todos os colaboradores, com módulos obrigatórios específicos por função.
Gestão de riscos	Avaliação de riscos, pelo menos, anual, com aprovação da gestão de topo; plano de tratamento de riscos com medidas atribuídas.
Gestão de fornecedores	Política e procedimento de fornecedores vinculativos; obrigatoriedade de DPA para todos os subcontratantes; revisões periódicas de fornecedores.
Resposta a incidentes	Procedimento documentado de gestão de incidentes com vias de comunicação, níveis de escalonamento e verificação de eficácia definidos.
Gestão de patches	Registo de patches mantido, com aplicação rastreável dos patches.
Revisão pela gestão	Avaliação, pelo menos, anual pela gestão de topo com base em KPI quantitativos.
Auditoria interna	Auditoria interna anual e independente do SGSI com constatações documentadas e medidas corretivas.

5. Ciclo de vida das cópias de segurança e apagamento

Os dados pessoais contidos em cópias de segurança são integralmente sobrescritos em poucas semanas através da rotação de cópias de segurança definida.

Com a cessação do contrato, o apagamento final dos dados nos sistemas produtivos é efetuado no prazo de 30 dias; em seguida, a rotação de cópias de segurança exclui os dados do conjunto de cópias existentes em poucas

semanas.

As janelas de retenção concretas por geração de cópia de segurança são divulgadas mediante pedido fundamentado, no âmbito do direito de auditoria (§ 9).

Anexo 3: Lista de subcontratantes ulteriores

Atualizado em 25.05.2026.

N.º	Subcontratante ulterior	Sede	Finalidade do tratamento	Dados tratados	Certificações / DPA
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Alemanha – centros de dados na Alemanha e na Finlândia (UE)	Alojamento da infraestrutura de produção e de cópias de segurança da Screenway	Todos os dados referidos no Anexo 1; exclusivamente cifrados em repouso (at rest) e em trânsito (in transit)	Certificada ISO/IEC 27001 + ISO/IEC 9001; acordo de subcontratação do tratamento de dados ativamente aceite pela Bergx2 GmbH; lista de subcontratados do fornecedor de alojamento publicamente disponível em www.hetzner.com/AV/subunternehmer.pdf

Nota sobre outros fornecedores da Bergx2: para a sua própria atividade empresarial (comunicação entre colaboradores, gestão de código-fonte, ferramentas de escritório e de produtividade), a Bergx2 GmbH utiliza outros prestadores de serviços SaaS. Estes não tratam dados de clientes da plataforma Screenway e, por conseguinte, não são subcontratantes ulteriores na aceção do presente DPA. Mediante pedido fundamentado do cliente, no âmbito do seu direito de auditoria (§ 9), a Bergx2 GmbH divulgará a lista completa dos seus próprios fornecedores.

Eficácia

O presente DPA torna-se, mediante aceitação no portal de clientes com selo temporal e designação de versão, parte integrante eficaz do contrato de serviço Screenway (artigo 28.º, n.º 9, do RGPD: por escrito, incluindo em formato eletrónico).

O registo de aceitação é arquivado pela Bergx2 GmbH de forma inalterável e auditável no backend de clientes e compreende, no mínimo:

- Designação da versão do presente DPA (ver a tabela de versões abaixo)
- Data e hora da aceitação
- Identidade da pessoa que aceita (ID de utilizador da conta de cliente)
- Identidade do cliente (ID de conta/contrato)
- Valor de hash da versão contratual aceite (comprovativo criptográfico de integridade)

Em caso de atualização do presente DPA, o cliente recebe, com, pelo menos, 30 dias de antecedência relativamente à produção de efeitos, uma notificação sob forma de texto, bem como, no início de sessão seguinte no portal de clientes, um pedido de nova aceitação.

Assinatura física ou eletrónica qualificada opcional: caso o cliente – p. ex., por força de requisitos internos de conformidade – pretenda uma contra-assinatura adicional, o DPA pode ser contra-assinado fisicamente ou mediante assinatura eletrónica qualificada (Regulamento eIDAS (UE) n.º 910/2014) entre as partes contratantes. Nesse caso, a apresentação fica a cargo do cliente. A aceitação eletrónica no portal de clientes não é afetada por tal facto e constitui, por si só, uma celebração do contrato em conformidade com o RGPD.

Versões

Versão	Data
1.0	25.05.2026