> Avis : La version juridiquement contraignante du présent contrat de sous-traitance est l'original allemand disponible sous `/rechtliches/avv`. Cette traduction française n'est fournie qu'à titre informatif. En cas de divergence, la version allemande prévaut.

Contrat de sous-traitance (CTSP) pour Screenway

> Cette version est contraignante et peut être valablement conclue par acceptation électronique dans le Customer-Portal (voir la section « Effectivité »).

Préambule

Bergx2 GmbH exploite la plateforme Software-as-a-Service Screenway pour le pilotage d'affichage numérique. Dans le cadre de l'utilisation du service, Bergx2 GmbH traite des données à caractère personnel pour le compte du Client au sens de l'art. 4 nº 8 et de l'art. 28 du règlement (UE) 2016/679 (règlement général sur la protection des données, RGPD). Le présent contrat précise les obligations et les droits des deux parties conformément à l'art. 28, paragraphe 3, du RGPD.

---

§ 1 Objet et durée du traitement

(1) Objet. Bergx2 GmbH met à la disposition du Client la plateforme Screenway en tant que Software-as-a-Service. Dans le cadre de cette utilisation, Bergx2 GmbH traite les données à caractère personnel du Client décrites plus en détail à l'Annexe 1 exclusivement selon les instructions de celui-ci.

(2) Durée. Le présent contrat entre en vigueur dès la conclusion du contrat principal sous-jacent (contrat de service Screenway) et prend fin avec la cessation de ce dernier. Les obligations de suppression/restitution (§ 10) et de confidentialité (§ 5, al. 2) continuent de s'appliquer au-delà de la durée du contrat.

---

§ 2 Nature et finalité du traitement

(1) Bergx2 GmbH traite les données à caractère personnel décrites à l'Annexe 1 aux fins suivantes :

- mise à disposition de la plateforme Screenway en tant que SaaS d'affichage numérique
- attribution des emplacements d'écrans aux comptes clients
- affichage des contenus téléchargés par le Client sur les terminaux
- authentification des collaborateurs du Client lors de la connexion
- fourniture du support, analyse des erreurs et supervision du service

(2) Un traitement à des fins propres de Bergx2 GmbH (p. ex. marketing, profilage, vente à des tiers) n'a pas lieu.

---

§ 3 Nature des données à caractère personnel et catégories de personnes concernées

Pour l'énumération concrète, voir l'Annexe 1. En résumé :

- Nature des données : données de compte, données de connexion, données de localisation d'écran, contenus téléchargés par le Client (en règle générale non personnels)
- Catégories de personnes concernées : collaborateurs du Client (pour la connexion et l'attribution de compte)

Le traitement de catégories particulières de données à caractère personnel au sens de l'art. 9 du RGPD n'a pas lieu dans l'exploitation standard de Screenway. Si le Client télécharge néanmoins de telles données, cela se produit en dehors des catégories couvertes par le présent CTSP et sous la responsabilité exclusive du Client.

---

§ 4 Obligations et droits du Responsable du traitement (Client)

(1) Droit d'instruction. Le Client demeure responsable de la licéité du traitement (art. 24 du RGPD). Bergx2 GmbH traite les données exclusivement sur instruction documentée du Client. Le présent CTSP vaut instruction générale ; des instructions individuelles peuvent être données via les canaux de communication définis dans le contrat de service.

(2) Documentation. Bergx2 GmbH documente les opérations pertinentes au regard des instructions dans la piste d'audit interne du SMSI (historique des pull-requests, registre des incidents, registre des fournisseurs).

(3) Obligations d'information. Le Client est tenu d'informer les personnes concernées (ses collaborateurs) conformément à l'art. 13 du RGPD au sujet du traitement des données effectué par Bergx2 GmbH.

---

§ 5 Obligations du Sous-traitant (Bergx2 GmbH)

(1) Respect des instructions. Bergx2 GmbH traite les données exclusivement sur instruction documentée du Client. Si une instruction apparaît, du point de vue de Bergx2 GmbH, comme illicite, Bergx2 GmbH en informera le Client sans délai (art. 28, par. 3, lit. h, du RGPD).

(2) Confidentialité. Bergx2 GmbH soumet à une obligation de confidentialité toutes les personnes participant au traitement avant qu'elles ne commencent leur activité (art. 28, par. 3, lit. b, du RGPD). Cela s'effectue par des engagements de confidentialité (NDA) lors de l'embauche ou du mandat et est documenté dans le SMSI de Bergx2 GmbH (registre du personnel).

(3) Mesures techniques et organisationnelles. Bergx2 GmbH met en œuvre les MTO décrites à l'Annexe 2, qui correspondent à l'état de l'art et garantissent un niveau de protection adapté au risque (art. 32 du RGPD).

(4) Sous-traitants ultérieurs. Bergx2 GmbH fait appel aux sous-traitants ultérieurs énumérés à l'Annexe 3. Les conditions et le mécanisme de modification figurent au § 6.

(5) Assistance. Bergx2 GmbH assiste le Client dans l'exécution de ses obligations au titre des art. 32 à 36 du RGPD, en particulier pour répondre aux demandes des personnes concernées (§ 7) et pour notifier les violations de données à caractère personnel (§ 8).

(6) Justificatifs. Bergx2 GmbH met à la disposition du Client, sur demande, les informations et documents nécessaires au contrôle (art. 28, par. 3, lit. h, du RGPD). Les autres modalités d'audit figurent au § 9.

---

§ 6 Sous-traitants ultérieurs

(1) Autorisation. Par la conclusion du présent CTSP, le Client autorise de manière générale le recours aux sous-traitants ultérieurs énumérés à l'Annexe 3 (art. 28, par. 2, première phrase, du RGPD).

(2) Notification de modification. Bergx2 GmbH informe le Client des modifications envisagées concernant la liste des sous-traitants ultérieurs (ajout ou remplacement) au moins 30 jours avant leur prise d'effet, en forme textuelle (courriel à l'adresse de contact « protection des données » indiquée dans le contrat de service).

(3) Droit d'opposition. Le Client peut s'opposer à la modification pour des motifs légitimes dans le délai de 30 jours. En cas d'opposition, Bergx2 GmbH recherche avec le Client une solution amiable ; en l'absence d'accord, le Client dispose d'un droit de résiliation extraordinaire du contrat de service.

(4) Obligation. Bergx2 GmbH impose contractuellement à chaque sous-traitant ultérieur, de son côté, les obligations convenues dans le présent CTSP (art. 28, par. 4, du RGPD).

---

§ 7 Coopération aux droits des personnes concernées

Bergx2 GmbH assiste le Client par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, dans l'exécution des droits des personnes concernées au titre du chapitre III du RGPD (information, rectification, effacement, limitation, portabilité, opposition).

Concrètement : Bergx2 GmbH transmet sans délai au Client les demandes que les personnes concernées adresseraient directement à Bergx2 GmbH et donne à celui-ci la possibilité d'y répondre. Une réponse propre de Bergx2 GmbH n'a lieu que sur instruction expresse du Client.

---

§ 8 Notification des violations de données à caractère personnel

(1) Bergx2 GmbH informe le Client sans délai, et au plus tard dans un délai de 24 heures après en avoir eu connaissance, de toute violation de données à caractère personnel constatée dans le domaine de responsabilité de Bergx2 GmbH ou d'un sous-traitant ultérieur, qui concerne des données à caractère personnel du Client.

(2) La notification est faite par écrit (courriel à l'adresse de contact « protection des données » du Client) et contient les informations minimales mentionnées à l'art. 33, par. 3, du RGPD (nature et étendue de la violation, nombre de personnes concernées, conséquences probables, contre-mesures prises).

(3) Bergx2 GmbH documente ses propres violations de données à caractère personnel en interne dans le registre des incidents (voir `incidents/incidents.md` du SMSI de Bergx2 GmbH, procédure selon `documents/verfahren/incident-management-verfahren.md`).

(4) L'obligation de notification à l'autorité de contrôle compétente au titre de l'art. 33 du RGPD et, le cas échéant, aux personnes concernées au titre de l'art. 34 du RGPD incombe au Client en sa qualité de Responsable du traitement. Bergx2 GmbH assiste le Client dans ces notifications en lui fournissant toutes les informations nécessaires.

---

§ 9 Droits d'audit et de contrôle

(1) Justificatif. Bergx2 GmbH met à la disposition du Client, sur demande, les informations nécessaires à l'exécution des obligations découlant du présent CTSP, en particulier la version en vigueur des MTO (Annexe 2) et de la liste des sous-traitants ultérieurs (Annexe 3), ainsi que, le cas échéant, des extraits de certifications.

(2) Contrôle sur place. Le Client a le droit de s'assurer du respect des MTO sur place, au siège social de Bergx2 GmbH ou aux lieux de traitement. Les rendez-vous doivent être annoncés par écrit au moins quatre semaines à l'avance ; les contrôles doivent se limiter au nécessaire et ne doivent pas perturber de manière disproportionnée l'activité commerciale. Au maximum un contrôle par année civile, sauf motif justifié.

(3) Reconnaissance des certifications. Dans la mesure où Bergx2 GmbH est certifié selon la norme ISO/IEC 27001:2022 (certification en préparation) ou présente des examens indépendants équivalents par des tiers, ceci remplace le contrôle sur place du Client, à condition que le périmètre de la certification couvre également l'objet du contrat.

---

§ 10 Suppression et restitution après la fin du contrat

(1) À la fin du contrat de service, Bergx2 GmbH procédera – au choix du Client – soit :

- à la restitution intégrale des données à caractère personnel (export dans un format structuré, couramment utilisé et lisible par machine), soit
- à la suppression intégrale des données à caractère personnel (écrasement sécurisé conforme à l'état de l'art), et

dans les 30 jours suivant la fin du contrat.

(2) Les sauvegardes contenant des données à caractère personnel sont, en raison de la rotation des sauvegardes, intégralement écrasées en l'espace de cinq semaines au maximum, conformément à l'Annexe 2 MTO § Cycle de vie des sauvegardes. Bergx2 GmbH documente la suppression finale par écrit sur demande.

(3) Les obligations légales de conservation restent inchangées (p. ex. les données de facturation conformément au § 257 HGB, au § 147 AO).

---

§ 11 Responsabilité et dispositions finales

(1) Responsabilité. Les dispositions du contrat principal (contrat de service Screenway) et l'art. 82 du RGPD s'appliquent. En cas de violation du présent CTSP, la partie responsable répond vis-à-vis de la personne concernée.

(2) Forme écrite. Les modifications et compléments requièrent la forme textuelle.

(3) Clause salvatrice. Si certaines dispositions devaient être nulles, la validité des autres dispositions n'en serait pas affectée.

(4) Droit applicable et juridiction compétente. Le droit allemand est applicable, à l'exclusion de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. La juridiction compétente est Munich.

Annexe 1 : Description du traitement

Catégorie	Contenu
Objet	Mise à disposition de la plateforme SaaS Screenway, y compris hébergement, transmission de données, authentification et pilotage de l'affichage
Durée	Durée active du contrat + 30 jours de période transitoire pour l'export/la suppression
Nature du traitement	Collecte, enregistrement, conservation, modification, consultation, affichage, transmission, suppression
Finalité	Fourniture de la prestation Screenway convenue contractuellement
Personnes concernées	Collaborateurs du Client auxquels des accès de connexion/de pilotage à Screenway sont octroyés
Catégories de données	Données de compte (nom, courriel professionnel, rôle), données de connexion (empreinte de mot de passe, cookies de session, adresse IP), données de localisation d'écran (désignation, le cas échéant adresse du site), contenus téléchargés par le Client (en règle générale **non** personnels – matériel marketing, textes d'information, etc.)
Catégories particulières de données (art. 9 du RGPD)	**Non** traitées en exploitation standard
Région d'hébergement	Exclusivement Union européenne – Hetzner Nuremberg (primaire) + Hetzner Helsinki (miroir de sauvegarde)
Transfert vers un pays tiers	**Aucun**

Annexe 2 : Mesures techniques et organisationnelles (MTO)

Les MTO suivantes correspondent à l'art. 32 du RGPD et sont catégorisées conformément aux exigences des autorités de contrôle et au standard CTSP-RGPD usuel dans le secteur. Les mesures sont documentées dans le système de management de la sécurité de l'information (SMSI) de Bergx2 GmbH selon ISO/IEC 27001:2022 et sont maintenues en détail en interne. Les détails concrets de mise en œuvre (modèles fabricants, paramètres de configuration, emplacements des différents composants, mécanismes de clés) ne sont, pour des raisons de sécurité, pas divulgués dans la présente annexe contractuelle accessible au public. Sur demande motivée du Client dans le cadre de son droit d'audit au titre du § 9, Bergx2 GmbH met à disposition les justificatifs détaillés pertinents dans le cadre d'un engagement de confidentialité écrit.

1. Confidentialité (art. 32, par. 1, lit. b, du RGPD)

Mesure	Mise en œuvre
Contrôle d'accès physique	Contrôle d'accès physique à plusieurs niveaux au siège social, avec résistance mécanique à l'effraction conforme aux normes DIN applicables, vitrage de sécurité, portes à verrouillage automatique, contrôle préalable d'entrée par caméra sans transmission vers des réseaux externes, et authentification multifacteur au niveau de fermeture le plus interne. Les droits d'accès sont attribués selon le principe « need-to-be-present » à un cercle de personnes nommément limité et sont documentés dans un registre des clés tenu à jour avec une piste d'audit de remise/restitution. La reproduction de clés n'est possible qu'avec l'accord du bailleur, par l'intermédiaire de serruriers certifiés. Les visiteurs ne pénètrent dans les locaux qu'accompagnés.
Contrôle d'accès système	Contrôle d'accès basé sur les rôles (RBAC) dans tous les systèmes de production ; authentification multifacteur (MFA) pour les accès administratifs ; politique de mots de passe contraignante conforme à l'état de l'art ; accès aux serveurs par clé ou certificat, sans mot de passe ; acheminement obligatoire des accès administratifs via un Virtual Private Network (VPN) interne.
Contrôle d'accès aux données	Séparation des locataires par compte client au niveau de la base de données ; règles d'accès au niveau de l'enregistrement (Row-Level-Security) ; journalisation à l'épreuve d'audit de tous les accès en lecture et en écriture aux données à caractère personnel.
Pseudonymisation	Partout où cela est compatible avec la finalité du traitement, les traitements internes sont pseudonymisés. Une vérification par échantillon périodique des occurrences involontaires de noms réels est établie en tant qu'indicateur clé (KPI) de sécurité de l'information.
Chiffrement	Chiffrement du transport conforme à l'état de l'art pour toutes les connexions externes, avec rotation régulière des certificats. Chiffrement fort au repos pour les supports de sauvegarde et les disques des terminaux. Les identifiants sensibles (mots de passe, jetons, clés) sont gérés exclusivement selon une procédure interne conforme à l'état de l'art – les détails ne sont pas divulgués pour des raisons de sécurité.

2. Intégrité (art. 32, par. 1, lit. b, du RGPD)

Mesure	Mise en œuvre
Contrôle des entrées	Validation côté serveur de toutes les entrées ; journaux d'audit à l'épreuve d'audit ; droits d'écriture exclusivement via des interfaces de programmation authentifiées et autorisées.
Contrôle de transmission	Chiffrement obligatoire du transport pour toutes les connexions externes ; aucune transmission de données sans base contractuelle documentée.
Contrôle de la sous-traitance	Contrats de sous-traitance avec tous les sous-traitants ultérieurs (voir Annexe 3) ; processus structuré de gestion des fournisseurs, avec réévaluation périodique.

3. Disponibilité et résilience (art. 32, par. 1, lit. b, du RGPD)

Mesure	Mise en œuvre
Sauvegarde	Sauvegarde incrémentielle quotidienne des systèmes de production, avec mise en miroir géographiquement séparée **au sein de l'Union européenne** ; plusieurs versions sont conservées ; tests planifiés de restauration au rythme trimestriel.
Disponibilité	Architecture cloud-first avec hébergement dans des centres de données certifiés ISO/IEC 27001 dotés d'une alimentation de secours ; surveillance continue avec chemins d'escalade définis.
Continuité d'activité	Plan de continuité d'activité éprouvé, incluant une analyse d'impact métier (Business Impact Analysis) ; capacité complète de télétravail pour les fonctions fondées sur la connaissance ; temps de reprise documentés par système.
Résilience des terminaux	Terminal de remplacement comme réserve en cas de panne matérielle ; réserves d'autonomie batterie suffisantes pour des coupures de courant de courte durée.

4. Procédures de contrôle, d'évaluation et d'appréciation réguliers (art. 32, par. 1, lit. d, du RGPD)

Mesure	Mise en œuvre
Système de management de la sécurité de l'information (SMSI)	SMSI établi selon ISO/IEC 27001:2022, avec une déclaration d'applicabilité (Statement of Applicability) couvrant les contrôles de l'annexe A ; certification en préparation.
Gestion de la protection des données	Registre des activités de traitement tenu à jour ; déléguée à la protection des données nommée ; revues périodiques des activités de traitement.
Sensibilisation	Formations structurées et traçables de sensibilisation et de protection des données pour l'ensemble du personnel, avec modules obligatoires spécifiques aux rôles.
Gestion des risques	Évaluation des risques au moins annuelle avec approbation par la direction générale ; plan de traitement des risques avec mesures attribuées.
Gestion des fournisseurs	Politique et procédures de gestion des fournisseurs contraignantes ; obligation de CTSP pour tous les sous-traitants ; revues périodiques des fournisseurs.
Réponse aux incidents	Procédure documentée de gestion des incidents, avec voies de notification définies, niveaux d'escalade et vérification de l'efficacité.
Gestion des correctifs	Registre des correctifs tenu à jour, avec application traçable des correctifs.
Revue de direction	Évaluation au moins annuelle par la direction générale, sur la base d'indicateurs clés (KPI) quantitatifs.
Audit interne	Audit interne indépendant annuel du SMSI, avec constats documentés et mesures correctives.

5. Cycle de vie des sauvegardes et suppression

Les données à caractère personnel présentes dans les sauvegardes sont intégralement écrasées en l'espace de quelques semaines par la rotation de sauvegarde définie.

À la fin du contrat, la suppression finale des données sur les systèmes de production a lieu dans les 30 jours ; la rotation de sauvegarde élimine ensuite les données du stock en l'espace de quelques semaines.

Les fenêtres de rétention concrètes par génération de sauvegarde sont communiquées sur demande motivée dans le cadre du droit d'audit (§ 9).

Annexe 3 : Liste des sous-traitants ultérieurs

État au : 25.05.2026.

N°	Sous-traitant ultérieur	Siège	Finalité du traitement	Données traitées	Certifications / CTSP
1	**Hetzner Online GmbH**	Industriestraße 25, 91710 Gunzenhausen, Allemagne – centres de données en Allemagne et en Finlande (UE)	Hébergement de l'infrastructure de production et de sauvegarde de Screenway	Toutes les données mentionnées à l'Annexe 1 ; exclusivement chiffrées au repos et en transit	Certifié ISO/IEC 27001 + ISO/IEC 9001 ; contrat de sous-traitance activement accepté par Bergx2 GmbH ; liste des sous-traitants de l'hébergeur publiquement disponible sous www.hetzner.com/AV/subunternehmer.pdf

Note relative aux autres fournisseurs de Bergx2 GmbH : Bergx2 GmbH fait appel, pour ses propres activités (communication interne du personnel, gestion du code source, outils bureautiques et de productivité), à d'autres prestataires SaaS. Ceux-ci ne traitent aucune donnée client issue de la plateforme Screenway et ne sont donc pas des sous-traitants ultérieurs au sens du présent CTSP. Sur demande motivée du Client dans le cadre de son droit d'audit (§ 9), Bergx2 GmbH communiquera la liste complète de ses propres fournisseurs.

Effectivité

Le présent CTSP devient une composante effective du contrat de service Screenway par acceptation dans le Customer-Portal avec horodatage et indication de version (art. 28, par. 9, du RGPD : forme écrite, également au format électronique).

L'enregistrement d'acceptation est archivé par Bergx2 GmbH dans le backend client à l'épreuve d'audit et comprend au minimum :

- l'indication de version du présent CTSP (voir le tableau de versionnement ci-dessous)
- la date et l'heure de l'acceptation
- l'identité de la personne acceptante (User-ID du compte client)
- l'identité du client (identifiant de compte/de contrat)
- la valeur de hachage de la version contractuelle acceptée (justificatif cryptographique d'intégrité)

En cas de mise à jour du présent CTSP, le Client reçoit une notification en forme textuelle au moins 30 jours avant sa prise d'effet, ainsi qu'une invitation à réaccepter lors de la prochaine connexion au Customer-Portal.

Signature physique ou électronique qualifiée, en option : Si le Client – p. ex. en raison d'exigences internes de conformité – souhaite un contreseing supplémentaire, le CTSP peut être contresigné physiquement ou au moyen d'une signature électronique qualifiée (règlement eIDAS (UE) n° 910/2014) entre les parties contractantes. Dans ce cas, la fourniture incombe au Client. L'acceptation électronique dans le Customer-Portal demeure inchangée et constitue, en soi, une conclusion de contrat conforme au RGPD.

Versionnement

Version	Date
1.0	25.05.2026