

Contrat de sous-traitance de données personnelles (DPA)

FinitoApp — version 1.0 du 3 août 2026

1. Objet et champ d'application

Le présent contrat de sous-traitance (« DPA ») régit le traitement de données personnelles effectué par FinitoApp pour le compte du Client dans le cadre de l'utilisation de l'application FinitoApp (la « Solution »), conformément à l'art. 9 de la Loi fédérale suisse sur la protection des données (nLPD) et, lorsque celui-ci s'applique, à l'art. 28 du Règlement (UE) 2016/679 (RGPD).

Il complète les Conditions générales d'utilisation (CGU) de FinitoApp, dont il fait partie intégrante, et s'applique automatiquement à tout Client qui traite dans la Solution des données personnelles de tiers en qualité de responsable du traitement. En cas de contradiction entre le DPA et les CGU sur des questions de protection des données, le DPA prévaut.

2. Parties et rôles

- Responsable du traitement : le Client (professionnel du bâtiment,

entreprise ou organisation utilisant la Solution), qui détermine les finalités et les moyens du traitement des données de tiers qu'il saisit dans la Solution (collaborateurs, intervenants, maîtres d'ouvrage, personnes visibles sur les photographies de chantier, etc.).

- Sous-traitant : Orestis Zacharakis, entreprise individuelle de droit

suisse exerçant sous le nom commercial « FinitoApp », canton de Vaud, Suisse (« FinitoApp »), qui traite ces données exclusivement pour le compte du Client aux fins de fourniture de la Solution.

Pour les données des utilisateurs eux-mêmes (compte, facturation), FinitoApp agit en qualité de responsable du traitement ; ce traitement est régi par la Politique de confidentialité et n'entre pas dans le champ du présent DPA.

3. Description du traitement (Annexe 1)

La nature, la finalité, la durée du traitement, les catégories de données et de personnes concernées sont décrites à l'Annexe 1, qui fait partie intégrante du présent DPA.

4. Instructions du Client

FinitoApp traite les données du Client uniquement sur instructions documentées de celui-ci. Les CGU, le présent DPA et l'utilisation des fonctionnalités de la Solution par le Client (création de chantiers, réserves, invitations, exports...) constituent les instructions documentées du Client. FinitoApp informe le Client si, à son avis, une instruction viole le droit applicable en matière de protection des données.

5. Confidentialité

FinitoApp garantit que toute personne autorisée à traiter les données du Client est tenue à la confidentialité, contractuellement ou de par la loi. À la date du présent DPA, seul l'exploitant identifié à l'art. 2 dispose d'un accès administrateur aux systèmes.

6. Sécurité du traitement

FinitoApp met en œuvre les mesures techniques et organisationnelles (« TOM ») décrites à l'Annexe 2, appropriées au regard du risque, conformément à l'art. 8 nLPD et à l'art. 32 RGPD. Les TOM peuvent évoluer, à condition que le niveau de sécurité global ne soit pas réduit.

7. Sous-traitants ultérieurs

Le Client autorise de manière générale le recours aux sous-traitants ultérieurs figurant sur la liste publique tenue à jour à l'adresse app.finitoapp.ch/sous-traitants, laquelle indique pour chacun l'identité, le pays, la finalité et les garanties de transfert. FinitoApp informe le Client de tout ajout ou remplacement prévu via cette page et par les canaux de notification de la Solution, au moins 30 jours à l'avance ; le Client peut s'y opposer par écrit pour des motifs légitimes ; à défaut d'accord, le Client peut résilier le service et exporter ses données. FinitoApp impose à chaque sous-traitant ultérieur des obligations équivalentes à celles du présent DPA et répond envers le Client de leur exécution.

8. Assistance au Client

Compte tenu de la nature du traitement, FinitoApp assiste le Client, par des mesures techniques et organisationnelles appropriées :

- pour donner suite aux demandes d'exercice des droits des personnes concernées

(accès, rectification, effacement, portabilité) — notamment via les fonctions intégrées d'export (TXT/ZIP) et de suppression ;

- pour le respect des obligations de sécurité, de notification des violations

et, le cas échéant, d'analyse d'impact (art. 22 nLPD / art. 35 RGPD), en fournissant les informations pertinentes dont FinitoApp dispose.

9. Notification des violations de données

FinitoApp notifie le Client dans les meilleurs délais, et au plus tard 72 heures après en avoir pris connaissance, toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou la divulgation non autorisée de données traitées pour le compte du Client. La notification décrit la nature de la violation, les catégories et le volume approximatif de données et de personnes concernées, les conséquences probables et les mesures prises ou proposées.

10. Audit et démonstration de conformité

FinitoApp met à la disposition du Client les informations nécessaires pour démontrer le respect du présent DPA (documentation de sécurité, liste des sous-traitants, description des TOM). Le Client peut, au maximum une fois par période de douze mois et moyennant un préavis écrit de 30 jours, faire réaliser un audit documentaire ; les audits sur site sont limités aux cas exigés par une autorité de contrôle ou consécutifs à une violation avérée, sont menés pendant les heures ouvrables sans perturber l'exploitation, et les coûts en sont supportés par le Client sauf si l'audit révèle un manquement matériel.

11. Localisation et transferts internationaux

Les données de production (base de données, fichiers, sauvegardes) sont hébergées exclusivement en Suisse (Infomaniak, Genève). Certains sous-traitants ultérieurs listés sur app.finitoapp.ch/sous-traitants sont établis dans l'UE ou aux États-Unis ; les transferts correspondants sont encadrés par une décision d'adéquation ou par des clauses contractuelles types (SCC), tel qu'indiqué dans la liste.

12. Durée, fin du traitement et sort des données

Le présent DPA s'applique pendant toute la durée d'utilisation de la Solution. Au terme de la relation contractuelle, le Client peut exporter ses données via les fonctions intégrées, puis obtenir leur suppression complète via la fonction « Supprimer mon compte » (effacement immédiat et définitif, cascade incluse chez les sous-traitants ultérieurs concernés), sous réserve des obligations légales de conservation. À défaut de suppression volontaire, les règles de conservation décrites dans la Politique de confidentialité s'appliquent.

13. Responsabilité

La responsabilité des parties au titre du présent DPA est régie par l'art. 6 des CGU. Chaque partie répond des dommages causés par un traitement non conforme aux obligations qui lui incombent en propre.

14. Droit applicable et for

Le présent DPA est soumis au droit suisse. Le for est celui prévu par les CGU (tribunaux ordinaires du canton de Vaud), sous réserve des dispositions impératives applicables.

Annexe 1 — Description du traitement

- Nature et finalité : hébergement, stockage, affichage, organisation, partage au sein des équipes de chantier, export documentaire (PDF/Excel/ Word) et sauvegarde des données saisies par le Client dans la Solution, aux fins de gestion et de documentation de chantiers (constats, réserves, réceptions d'ouvrage).
- Durée : durée d'utilisation de la Solution par le Client, puis délais de conservation décrits dans la Politique de confidentialité.
- Catégories de personnes concernées : collaborateurs et sous-traitants du Client ; intervenants et artisans invités sur les chantiers ; maîtres d'ouvrage et clients finaux du Client ; toute personne identifiable sur les photographies ou documents déposés par le Client.
- Catégories de données : données d'identification et de contact (nom, prénom, e-mail, téléphone, entreprise, corps de métier) ; contenus de chantier (photographies, plans, descriptions de réserves, commentaires, signatures électroniques) ; métadonnées d'activité liées au chantier.
- Données sensibles : la Solution n'est pas destinée au traitement de données sensibles au sens de l'art. 5 let. c nLPD ; le Client s'engage à ne pas en soumettre.

Annexe 2 — Mesures techniques et organisationnelles (TOM)

Hébergement et localisation. Serveurs et stockage objet exclusivement en Suisse (Infomaniak, certifié ISO 27001) ; aucune donnée de production hors de Suisse.

Chiffrement. TLS 1.2+ pour toutes les communications ; chiffrement au repos assuré par l'hébergeur ; sauvegardes de la base de données chiffrées GPG-AES-256 côté client avant dépôt ; stockage S3 avec SSE-AES-256 et versionnement activé.

Contrôle d'accès. Authentification par jetons de courte durée (15 min) avec refresh révocable ; hachage des mots de passe argon2id (recommandations OWASP) et contrôle de compromission (HIBP) ; MFA TOTP disponible (secret chiffré AES-256-GCM) ; contrôle d'accès par rôle au niveau de chaque chantier (propriétaire, intervenant, partenaire, observateur) ; verrouillage biométrique optionnel sur mobile.

Sécurité applicative. Validation stricte des entrées (schémas Zod) ; re-encodage systématique des images téléversées et suppression des métadonnées EXIF/IPTC ; validation des types de fichiers par signature binaire ; limites anti-abus (rate limiting global et renforcé sur l'authentification) ; Content Security Policy avec nonce par requête ; protection CSRF multicouche ; en-têtes de sécurité (HSTS, X-Content-Type-Options, Referrer-Policy).

Sauvegardes et continuité. Sauvegarde quotidienne de la base de données, chiffrée avant dépôt, rétention roulante (7 quotidiennes, 4 hebdomadaires, 3 mensuelles) plus copie locale 7 jours ; fichiers protégés par versionnement S3 et snapshot hebdomadaire ; restauration testée périodiquement.

Journalisation et minimisation. Journaux techniques avec caviardage des données personnelles ; aucun outil d'analyse comportementale ni traqueur publicitaire ; collecte limitée au nécessaire.

Organisation. Accès administrateur limité à l'exploitant ; postes de travail chiffrés ; principe du moindre privilège pour les clés et secrets ; revue de sécurité périodique du code et des dépendances (analyse statique, audit des dépendances, scan de secrets).

Gestion des violations. Procédure de détection, d'analyse et de notification décrite à l'art. 9 du DPA.