Annexe B — Accord de traitement des données

Version du 17 novembre 2026 — accord fondé sur l'article 28 du RGPD

1. Parties, objet et durée

Le présent accord lie le client professionnel identifié à l'annexe I et **SUBVERSION SAS**, fournisseur de TrackCut. Le client est responsable des traitements dont il détermine les finalités ; SUBVERSION intervient pour son compte comme sous-traitant. Si le client traite lui-même pour un donneur d'ordre, la section 9 s'applique.

L'annexe II définit l'objet, la nature, les finalités, les données et les personnes concernées. Le traitement dure pendant l'abonnement, essai compris, puis uniquement le temps nécessaire aux opérations de sortie et de suppression de la section 7. L'accord demeure applicable jusqu'à la disparition des données confiées et de leurs copies.

Le client détermine les finalités et la licéité des traitements, informe les personnes, gère leurs droits et donne ses instructions. Il peut obtenir les informations, l'assistance, les audits, la restitution et la suppression prévus ici. Les traitements propres de SUBVERSION, notamment la facturation, la preuve du contrat et la prévention des essais répétés, sont distincts et décrits dans les CG et la politique de confidentialité ; ils n'autorisent aucune réutilisation des contenus confiés.

2. Instructions documentées

SUBVERSION traite les données uniquement pour fournir les prestations décrites à l'annexe II, sur les instructions documentées du client, y compris pour les transferts hors EEE. Constituent de telles instructions l'accord accepté, les actions des utilisateurs habilités dans le service et les demandes écrites du représentant habilité. Les instructions particulières incompatibles avec le service doivent être réglées avant le traitement concerné.

Si une obligation du droit de l'Union ou d'un État membre impose un autre traitement, SUBVERSION en informe le client avant d'agir, sauf interdiction légale motivée par un intérêt public important. Elle alerte immédiatement le client si une instruction lui paraît contraire au RGPD ou aux règles européennes ou nationales de protection des données et suspend l'opération litigieuse dans l'attente de sa clarification. Elle n'utilise pas les données confiées pour ses propres finalités.

3. Confidentialité et sécurité

SUBVERSION limite les accès aux personnes ayant besoin d'intervenir et soumises à un engagement de confidentialité ou à une obligation légale équivalente. La confidentialité survit à la fin du traitement. Les interventions humaines exceptionnelles sont documentées avec leur motif, leur date, leur auteur et les opérations réalisées ; les traces existantes peuvent être complétées manuellement.

SUBVERSION met en œuvre les mesures requises par l'article 32 du RGPD, adaptées à la nature des données, aux risques et à l'état des techniques : confidentialité, intégrité, disponibilité, résilience, restauration et évaluation régulière de leur efficacité. L'annexe III décrit les mesures du service et leurs limites. Les évolutions techniques ne réduisent pas le niveau de protection convenu.

SUBVERSION tient une évaluation des risques, la réexamine au moins annuellement et après tout changement ou incident important et documente les vérifications de restauration à une fréquence adaptée. Elle organise la continuité en cas d'indisponibilité de l'exploitant. Ces engagements n'instituent ni taux de disponibilité ni délai uniforme de reprise.

4. Sous-traitants ultérieurs

Le client donne une autorisation écrite générale de recourir aux prestataires de l'annexe IV, dans leur périmètre décrit. La liste publique à jour, datée, est disponible à **https://www.trackcut.io/sous-traitants** ; elle précise l'entité, la prestation, les données, les lieux de traitement et d'accès et les garanties de transfert.

Tout ajout ou remplacement est notifié par e-mail au propriétaire **au moins 30 jours avant** de confier les données au nouveau prestataire. L'avis indique le changement, sa date envisagée et les moyens de s'y opposer. Il ne dépend pas d'un abonnement aux notifications ; une simple publication ne le remplace pas. SUBVERSION conserve la liste datée et l'avis, et recherche un autre moyen de joindre le client en cas d'échec de remise connu.

Le client peut s'opposer pendant ce délai pour un motif relatif à la protection des données. SUBVERSION examine une solution ; à défaut, le client peut résilier le périmètre concerné sans frais avant le changement, avec remboursement de la période non fournie et restitution des données. Tant que l'opposition n'est pas résolue, les données du client, sauvegardes comprises, ne sont pas confiées au nouveau prestataire. À défaut d'opposition après information régulière et expiration du délai, l'autorisation générale couvre le changement ; aucune nouvelle signature n'est requise.

SUBVERSION impose à chaque prestataire, par contrat écrit, les mêmes obligations de protection applicables à sa prestation, notamment les garanties de sécurité suffisantes, conformément à l'article 28 §4 du RGPD. **SUBVERSION demeure pleinement responsable envers le client de l'exécution des obligations de ses sous-traitants ultérieurs.** Elle tient à disposition les contrats et éléments utiles, avec occultation limitée des secrets sans rapport avec le traitement. L'autorisation générale ne dispense pas des garanties de transfert de la section 10.

5. Droits des personnes

Les demandes peuvent être adressées à **rgpd@trackcut.io**, sans compte ni formulaire imposé. SUBVERSION accuse réception, transmet au client toute demande relative aux données confiées sans retard injustifié et **au plus tard sous deux jours ouvrés**, et informe la personne de cette transmission. Elle ne répond sur le fond que sur instruction du client, sauf obligation légale.

Compte tenu de la nature du traitement, SUBVERSION aide le client, par les moyens techniques et organisationnels appropriés et dans toute la mesure du possible, à traiter les droits du chapitre III du RGPD : recherche et accès aux données, rectification, effacement, limitation, portabilité et opposition. Elle fournit les informations nécessaires et aide à vérifier l'identité de manière proportionnée. L'urgence impose une transmission plus rapide ; ce délai interne ne prolonge pas les délais légaux du client.

6. Violations et assistance à la conformité

SUBVERSION notifie au client toute violation de données confiées **sans retard injustifié et au plus tard 48 heures après en avoir pris connaissance**, par e-mail au propriétaire et au contact de protection des données distinct éventuellement communiqué. Si l'e-mail échoue, elle utilise un autre moyen disponible. Contact : **rgpd@trackcut.io — 01 86 04 86 65**.

L'alerte décrit les faits connus, les catégories et nombres approximatifs de personnes et d'enregistrements concernés, les conséquences probables, les mesures prises ou envisagées et le contact de suivi. Les informations manquantes sont complétées progressivement, sans retarder l'alerte initiale. SUBVERSION documente l'incident, en limite les effets et aide le client à apprécier le risque et à préparer ses notifications aux autorités et aux personnes. Le délai contractuel ne reporte pas les délais légaux du responsable du traitement.

SUBVERSION aide le client à satisfaire les obligations des articles 32 à 36 du RGPD, compte tenu de la nature des traitements et des informations dont elle dispose : sécurité, notifications, analyse d'impact relative à la protection des données et consultation préalable de l'autorité. Elle transmet les éléments pertinents sur ses mesures, ses prestataires,

les transferts et les risques résiduels. Elle ne se substitue pas au client pour ses notifications légales, sauf instruction ou obligation légale propre.

7. Fin du traitement, restitution et suppression

Le client choisit la restitution suivie de suppression ou la suppression sans restitution. Le propriétaire peut donner une instruction particulière à contact@trackcut.io ou rgpd@trackcut.io ; SUBVERSION vérifie son habilitation de manière proportionnée et exécute l'instruction licite sans retard injustifié.

Le calendrier ordinaire est celui de l'article 13 des CG : **J0**, à la résiliation ou à la fin de l'essai, lecture seule ; **J+8**, coupure des clients du studio et des liens publics ; l'équipe conserve la lecture et la récupération pendant **30 jours** ; rappel au propriétaire à **J+23**. Les e-mails annoncent l'effacement « à partir du `<date>` ». Une reprise d'abonnement avant effacement rouvre les accès interrompus par la fin du contrat.

Toute l'équipe peut utiliser **« Télécharger le dossier » (ZIP) dans la Bibliothèque**, selon ses habilitations. Le propriétaire seul dispose de **« Exporter les données » dans Paramètres › Données**, disponible en permanence pendant le contrat et pendant les 30 jours de récupération : CSV, JSON et pièces jointes. L'assistance et les extractions complémentaires nécessaires sont demandées par e-mail. Une difficulté imputable à SUBVERSION donne lieu à préservation des données nécessaires et à un délai utile de récupération.

Hors reprise ou prolongation due, les données actives sont effacées **au plus tard 7 jours après la fin des 30 jours** : données du studio, fichiers et dérivés, comptabilité interne du stockage et comptes de l'équipe et des clients sans autre studio. Après une prolongation, ce délai de sept jours court après la fin de la récupération applicable.

Les sauvegardes de base et les sauvegardes complètes des serveurs, **Drive compris**, sont supprimées **au plus 90 jours après l'effacement des données actives**, sursis, versions cachées et délais de purge compris. La copie de secours des fichiers SBG est supprimée **au plus 30 jours après l'effacement réussi**. Ces maxima ne se cumulent pas. Les copies restent protégées, réservées à la restauration et sans utilisation courante ; les suppressions sont réappliquées avant toute remise en service. Les informations nécessaires à cette réapplication sont conservées jusqu'à la disparition de la dernière copie restaurable.

SUBVERSION détruit les copies existantes, sauf conservation imposée par le droit de l'Union ou d'un État membre ; elle en précise alors la base et la durée au client, sauf interdiction légale. Les délais de rotation ne constituent pas une exception générale à l'effacement : une instruction licite ou une exigence légale imposant une suppression plus rapide est respectée. Les conservations propres limitées de l'article 13.3 des CG restent distinctes et n'autorisent aucune conservation générale des contenus.

À la demande du client, SUBVERSION fournit par e-mail une certification d'effacement après vérification. Elle distingue les données actives effacées des copies encore présentes et de leur échéance ; elle ne certifie la suppression complète qu'après sa réalisation effective. Aucun document automatique n'est requis.

En cas de changement de fournisseur, l'article 13 bis des CG prime pour le calendrier, le maintien du service, la récupération et l'effacement intégral. SUBVERSION empêche toute coupure ou purge prématurée, au besoin manuellement. Une purge différée des sauvegardes nécessite l'accord écrit distinct prévu par cet article, qui ne réduit pas les exigences du RGPD.

8. Informations, audits et manquements

SUBVERSION fournit les informations nécessaires pour démontrer le respect de cet accord et de l'article 28, et permet les audits, inspections comprises, du client ou de son auditeur mandaté ; elle y contribue. Les informations ordinaires sont fournies sans supplément, dans les 30 jours au plus, plus rapidement en cas d'urgence.

L’organisation ordinaire prévoit un audit sur place par période de douze mois, avec préavis de 30 jours et confidentialité. Ces modalités ne limitent pas les contrôles nécessaires en présence d’indices de non-conformité, d’un incident, d’un changement important ou d’une demande d’autorité ; le préavis est adapté à l’urgence. Une documentation préalable ne conditionne pas le droit d’audit et les pouvoirs de l’autorité ne sont pas restreints.

Le contrôle protège les données des autres clients et les secrets sans rapport avec son objet. Un auditeur ne peut être refusé que pour un conflit d’intérêts concret et motivé, avec acceptation d’un remplaçant approprié. Le client supporte les honoraires de son auditeur ; les dépenses exceptionnelles sont convenues préalablement, raisonnables et non dissuasives. Aucun forfait ne conditionne les informations ordinaires ni le droit de contrôle.

En cas de manquement, le client peut suspendre le traitement puis résilier le périmètre concerné si la conformité n’est pas rétablie dans un délai raisonnable, au plus tard un mois ; il peut résilier immédiatement si la gravité ou la persistance le justifie, ou en cas de non-respect d’une décision contraignante. SUBVERSION peut arrêter un traitement dont le client maintient l’instruction illicite après alerte. Restitution et suppression restent dues.

9. Studio lui-même sous-traitant

Lorsque le client traite pour son propre donneur d’ordre, le présent accord constitue aussi l’accord écrit de sous-traitance ultérieure entre ce client et SUBVERSION au sens de l’article 28 §3 et §4. Toutes les obligations des sections 1 à 8 et 10 à 11 s’appliquent ; le studio ne devient pas responsable du traitement du seul fait d’utiliser TrackCut.

Lorsqu’il agit pour un donneur d’ordre, le client obtient avant le traitement l’autorisation nécessaire de son donneur d’ordre pour SUBVERSION et sa chaîne de prestataires, et conserve l’identité et les coordonnées du responsable final, les projets, les instructions et les autorisations. Il transmet ces informations sur demande justifiée, dans la mesure nécessaire, sans dossier systématique ni avenant à signer pour chaque projet. Les exigences amont particulières doivent être réglées avant le dépôt.

Le client transmet les instructions du responsable final et lui relaie sans délai les avis de changement, demandes des personnes, alertes de violation et demandes d’audit. SUBVERSION agit dans les limites de ces instructions, impose les obligations de protection à ses propres prestataires et demeure responsable de leur exécution. Les délais de deux jours ouvrés et de 48 heures ne justifient aucun retard supplémentaire de transmission au responsable final.

SUBVERSION assiste le client et le responsable final et permet leurs audits dans les conditions de la section 8. Sur instruction ou selon un circuit convenu, elle peut transmettre directement une alerte au responsable final. Son choix de restitution ou de suppression, transmis par le client, gouverne la sortie ; aucune modalité commerciale ne prolonge une conservation contraire à une instruction licite ou à la loi. Le client ne peut donner à SUBVERSION plus de pouvoirs qu’il n’en détient lui-même.

10. Transferts hors EEE

Tout transfert, y compris un accès depuis un pays tiers, respecte les instructions et le chapitre V du RGPD. SUBVERSION identifie l’exportateur, l’importateur, les rôles, les pays, le mécanisme applicable et les mesures complémentaires nécessaires. Les garanties publiées par fournisseur figurent à l’annexe IV ; elles ne valent pas preuve, à elles seules, du contrat ou du flux réellement utilisé.

Selon le flux, la garantie repose sur une décision d’adéquation applicable, dont le cadre UE–États-Unis (DPF) seulement pour une entité certifiée et un traitement couvert, ou sur les clauses de transfert **2021/914**, avec le module correspondant aux rôles réels, leurs annexes et l’évaluation des garanties et mesures complémentaires nécessaires. Un module destiné au transfert de responsable à sous-traitant ne couvre pas par assimilation un transfert entre sous-traitants.

SUBVERSION vérifie l'applicabilité et le maintien de ces garanties et en tient les justificatifs à disposition. À défaut de garantie valable, elle n'engage pas ou suspend le flux concerné. Elle examine la légalité des demandes d'autorités étrangères, conteste celles incompatibles avec le droit applicable et informe le client lorsque la loi le permet ; une demande étrangère ne suffit pas à autoriser la communication. Les engagements et droits impératifs résultant des garanties de transfert applicables demeurent intacts.

11. Acceptation, preuve et hiérarchie

L'accord, avec ses annexes I à IV, est proposé par SUBVERSION et accepté électroniquement avec les CG, par la même case non précochée et la même validation du représentant habilité, avant les traitements confiés. L'identité du client résulte du récapitulatif de commande ; les versions, l'auteur et l'horodatage sont conservés selon l'article 21 des CG. La confirmation et les documents conservables constituent l'écrit électronique prévu par l'article 28 §9 du RGPD ; aucune signature séparée ni admission par e-mail n'est requise.

En cas de contradiction concernant la protection des données, **l'annexe B (accord de traitement des données) prévaut sur les CG et les stipulations commerciales incompatibles**. Les règles impératives, les droits des personnes, l'article 82 du RGPD et les pouvoirs des autorités demeurent applicables. L'article 26 des CG ne réduit aucune obligation de faire. Le droit applicable et les juridictions compétentes sont ceux des CG, sous réserve des règles impératives et des garanties de transfert applicables.

Les mises à jour suivent l'article 17 des CG ; les ajouts et remplacements de sous-traitants suivent la section 4. Aucune évolution ne réduit les garanties légalement obligatoires.

ANNEXE I — PARTIES ET CONTACTS

Client professionnel : dénomination ou nom professionnel, adresse, identifiant d'entreprise, nom et fonction du représentant habilité figurent au récapitulatif présenté avant validation et confirmé par e-mail. L'adresse du propriétaire sert de contact contractuel et de protection des données, sauf autre contact communiqué. Il est responsable du traitement pour ses propres données et sous-traitant lorsqu'il agit pour un responsable final ; la section 9 couvre ce second cas.

SUBVERSION SAS, capital 7 622,45 €, RCS Nevers 345 019 459, TVA FR04 345 019 459 ; 22 rue Nicolas Cornette, 58410 Entrains-sur-Nohain, France. Activité : fourniture, hébergement, maintenance et assistance de TrackCut ; sous-traitant ou sous-traitant ultérieur selon le traitement.

Représentant et référent protection des données : **Thibaut Duez, président — rgpd@trackcut.io — 01 86 04 86 65**. Ce contact n'est pas présenté comme un délégué à la protection des données désigné au titre de l'article 37 du RGPD.

Le récapitulatif et la preuve de la validation en ligne complètent l'identification du client et datent l'engagement. SUBVERSION propose l'accord sous l'autorité de son représentant ; sa confirmation constate cet engagement sans contre-signature manuelle, selon la section 11 et l'article 21 des CG.

ANNEXE II — DESCRIPTION DU TRAITEMENT

Objet, nature et finalités

La prestation permet au client de gérer ses projets audiovisuels, de déposer et organiser ses fichiers, de préparer leur lecture, d'échanger avec les membres et invités, de recueillir commentaires et validations et de livrer les contenus. Les opérations comprennent collecte, enregistrement, hébergement, organisation, consultation autorisée, conversion technique, transcodage, génération de copies de lecture et de miniatures, transmission, synchronisation, sauvegarde, restauration, extraction, restitution et effacement, ainsi que l'assistance et la sécurité nécessaires à ces opérations.

Les notifications par e-mail, les envois WhatsApp sélectionnés et la publication sur le compte Instagram connecté sont exécutés selon les choix et instructions applicables. Les mesures techniques de format, durée, résolution et compatibilité nécessaires à la lecture sont distinctes de cet usage.

Personnes concernées

Représentants, collaborateurs et prestataires du client ; membres et invités ; donneurs d'ordre, contacts et destinataires de partages ; personnes identifiables dans les images, les voix, les documents, les commentaires, les messages ou les données de planning. Des mineurs ou personnes vulnérables peuvent apparaître dans les contenus.

Catégories de données

Identité, entreprise, fonction, e-mail, téléphone lorsqu'il est fourni, image de profil ; identifiants et habilitations ; adresses IP et traces techniques liées au service ; vidéos, rushs, images, sons, briefs, documents, fichiers du Drive, versions et dérivés ; commentaires, réponses, décisions et historique de validation ; messages et pièces jointes ; rendez-vous, planning, liens, destinataires, dates et métadonnées de projet ; jetons d'une intégration activée, limités à son fonctionnement.

Les numéros complets de carte de paiement ne font pas partie des données confiées à SUBVERSION pour les projets ; le paiement est traité dans la relation commerciale propre de SUBVERSION.

Données particulières et garanties adaptées

Une image ou une voix n'est pas, par sa seule présence, une donnée biométrique utilisée pour identifier une personne de manière unique. Les contenus peuvent néanmoins révéler des données de santé, convictions ou autres catégories de l'article 9, des données pénales ou des situations de vulnérabilité. Le client vérifie les conditions légales de leur traitement et informe SUBVERSION, avant un usage organisé présentant un risque élevé, de la nature des risques et des garanties spécifiques requises, sans transmettre plus de données que nécessaire à cette évaluation.

Les parties définissent alors les restrictions d'accès, de partage, de conservation et d'assistance adaptées avant le dépôt concerné. TrackCut n'est pas proposé comme un service certifié d'hébergement de données de santé ; un usage légalement soumis à une certification ou à des garanties indisponibles n'est pas accepté sans dispositif approprié. Cette règle ne dispense pas SUBVERSION de protéger les données sensibles effectivement présentes ni de traiter un incident.

Durée et fréquence

Le traitement est continu ou répété selon l'utilisation pendant l'abonnement, essai compris, puis limité à la sortie, aux copies de sécurité et à leur suppression selon la section 7. Les prestataires interviennent uniquement pendant la période nécessaire à leur mission ; les données de messages et journaux propres à une opération ne sont pas conservées par principe pendant toute la durée des sauvegardes.

Les données strictement nécessaires à la facturation, à la preuve et à la défense des droits sont distinguées des contenus et conservées pour les finalités propres de SUBVERSION selon l'article 13.3 et sa politique de confidentialité. Les preuves d'effacement ne contiennent pas une copie générale des projets.

ANNEXE III — MESURES TECHNIQUES ET ORGANISATIONNELLES

1. Architecture et séparation des espaces

Les serveurs applicatifs et de fichiers, la base de données et le service d'authentification sont hébergés sur les serveurs loués par SUBVERSION chez OVH en France. Les médias utilisent des compartiments de stockage objet

par studio, avec des identifiants d'accès associés à ces compartiments. Les droits de l'application et les règles de sécurité par ligne de la base limitent les accès ordinaires selon le studio, le rôle et les habilitations.

Les identifiants d'administration de la base et l'accès au registre des identifiants de stockage permettent à l'exploitation de réaliser des opérations sur plusieurs espaces, même lorsque chaque opération de stockage utilise la clé du studio concerné. La séparation entre studios est donc une séparation des accès ordinaires, non une impossibilité technique d'accès pour l'administration. Les règles d'usage de ces pouvoirs sont celles des sections 2 et 3.

2. Authentification et habilitations

L'authentification est exploitée par SUBVERSION sur ses serveurs loués chez OVH en France. Les utilisateurs disposent de comptes individuels et de rôles ; les mots de passe ne sont pas stockés en clair. La double authentification est proposée aux utilisateurs. Un second facteur est exigé pour l'administration générale de l'application, avec contrôle dans le portail et dans la base pour les opérations concernées. Cette exigence n'est pas présentée comme une seconde authentification de chaque connexion système ou de chaque service automatisé.

L'administration humaine est assurée par le président de SUBVERSION. Les comptes techniques nécessaires aux services ont leurs propres fonctions. Les clés d'API de gestion OVH sont restreintes aux adresses IP des deux serveurs de production ; cette restriction concerne l'API de gestion OVH et ne vaut pas déclaration d'une restriction identique de toutes les clés du stockage S3. Les secrets S3 et la clé de chiffrement des identifiants de stockage ont été retirés des environnements locaux de développement utilisés pour l'exploitation ; cela ne remplace pas le contrôle des accès directs à la base.

3. Chiffrement

Les échanges avec l'application et les téléchargements utilisent HTTPS/TLS. Le service n'est pas chiffré de bout en bout et SUBVERSION conserve la capacité technique de traiter les fichiers.

Le stockage objet OVH applique le chiffrement serveur AES-256 aux objets écrits depuis le 30 août 2026 ; les clés de ce chiffrement sont gérées par OVH. Cette description ne garantit pas le chiffrement rétroactif de tous les objets antérieurs. Les fichiers du Drive sont conservés sur un disque serveur non chiffré au repos, protégé par les droits du système et les contrôles réseau.

Les exports de sauvegarde de base sont chiffrés côté SUBVERSION en AES-256-GCM avant leur envoi. Les sauvegardes de serveurs utilisent le chiffrement du dépôt de sauvegarde avant transfert. Les clés de déchiffrement de ces sauvegardes restent chez SUBVERSION, séparées des copies. La base active est hébergée sur le serveur de SUBVERSION loué chez OVH en France ; le chiffrement des sauvegardes décrit ci-dessus ne constitue pas une garantie de chiffrement au repos de la base active.

4. Disponibilité, copies et restauration

Les fichiers du stockage objet font l'objet d'une copie de secours dans une seconde région OVH. Les sauvegardes de base et de serveurs, incluant le Drive, sont effectuées quotidiennement vers des dépôts chiffrés chez OVH, en France, distincts des serveurs du service. Elles sont distinctes du service actif ; elles ne garantissent ni l'absence de perte entre deux copies ni un délai uniforme de reprise.

Après l'effacement des données actives, les copies subsistent pendant **au plus 90 jours** pour les bases et **au plus 90 jours** pour les serveurs et le Drive, **sursis, versions cachées et délais de purge compris**. La copie de secours des fichiers SBG est supprimée **au plus 30 jours après l'effacement réussi**. Les délais ne se cumulent pas ; aucune rotation ou restauration ne peut les faire repartir à zéro pour des données déjà effacées.

La procédure de restauration prévoit une restauration isolée et la réapplication des suppressions avant remise en service. Les copies restent chiffrées et à accès restreint. Les informations nécessaires à la réapplication des

effacements sont conservées jusqu'à la disparition de la dernière copie restaurable. Les contrôles, le traitement des échecs et les instructions de suppression suivent les sections 3 et 7.

5. Journaux et protection réseau

L'application comporte des contrôles de droits et des limitations de débit ; l'infrastructure utilise des filtres réseau et CrowdSec contre les attaques. Un journal d'audit enregistre des modifications et certaines opérations d'administration, avec une rétention de 365 jours. Les journaux applicatifs sont conservés au plus six mois et les journaux d'accès du serveur au plus sept jours.

Il n'existe pas de journal exhaustif et non modifiable de toutes les consultations humaines ou techniques des contenus. Aucune conservation de trois ans de toutes les lectures n'est annoncée. Les fiches d'intervention exigées par la section 3 complètent les traces existantes sans être présentées comme un enregistrement automatique de chaque accès.

6. Suppression et restitution

Les fonctions disponibles sont **« Télécharger le dossier » dans la Bibliothèque** pour toute l'équipe selon habilitations et **« Exporter les données » dans Paramètres › Données** pour le propriétaire, avec CSV, JSON et pièces jointes. Le calendrier J0/J+8/J+23/J+30, la reprise avant effacement et les opérations de suppression suivent la section 7 et l'article 13 des CG.

La purge couvre les données du studio, les fichiers et dérivés, la comptabilité interne du stockage et les comptes sans autre studio. SUBVERSION vérifie son résultat et traite les échecs ; un début de purge ne vaut pas effacement complet. Les demandes particulières et transitions sont prises en charge par e-mail, avec préservation manuelle des données et accès nécessaires selon l'article 13 bis. Les preuves et traitements propres restent séparés selon l'article 13.3.

ANNEXE IV — SOUS-TRAITANTS ULTÉRIEURS ET GARANTIES PAR FLUX

Liste initiale autorisée ; version publique datée : **https://www.trackcut.io/sous-traitants**. Les changements suivent la section 4. Les garanties indiquées sont celles des contrats des fournisseurs en vigueur à la date de la présente version. Une localisation dans l'Espace économique européen n'exclut pas un accès depuis un pays tiers ; ces accès sont alors couverts par la garantie indiquée. Les copies suivent les durées de la section 7.

1. OVH SAS

Coordonnées : 2 rue Kellermann, 59100 Roubaix, France ; contact protection des données via OVHcloud.

Prestations et données : hébergement de l'application, du Drive, de la base de données et de l'authentification sur les serveurs loués par SUBVERSION chez OVH en France ; stockage des médias et de leur copie de secours, sauvegardes chiffrées de la base et des serveurs, messagerie ; fichiers et métadonnées nécessaires, identités, habilitations, données structurées des projets, commentaires, messages et traces techniques. Les sauvegardes sont chiffrées avant leur envoi ; les clés de déchiffrement restent chez SUBVERSION.

Lieu : France (serveurs et sauvegardes ; stockage objet et copie de secours à Gravelines et Strasbourg).

Garanties : accord de traitement des données OVHcloud du 3 octobre 2025. Pour d'éventuels accès depuis des filiales situées hors de l'Espace économique européen, cet accord prévoit les clauses contractuelles types de la Commission (décision 2021/914, module 3).

2. Sendinblue SAS (Brevo)

Coordonnées : 9-17 rue Salneuve, 75017 Paris, France ; contact protection des données via la politique de confidentialité de Brevo.

Prestations et données : envoi des e-mails du service (invitations, notifications, codes) ; adresses et noms des destinataires, contenu des messages et données de remise.

Lieu : Union européenne.

Garanties : accord de traitement des données intégré aux conditions d'utilisation de Brevo ; pour ses propres sous-traitants hors de l'Union européenne, clauses contractuelles types de la Commission ou Data Privacy Framework selon les flux.

3. WhatsApp Ireland Limited (groupe Meta), si ce canal est choisi

Coordonnées : Merrion Road, Dublin 4, D04 X2K5, Irlande ; contact via la politique de confidentialité EEE de WhatsApp.

Prestations et données : envoi de messages par la plateforme WhatsApp Business, uniquement lorsque ce canal est choisi : numéro de téléphone, code, noms, date et intitulé du projet, lien et, le cas échéant, miniature. Le client informe ses destinataires de ce canal.

Lieu : Irlande ; traitements possibles aux États-Unis par WhatsApp LLC et Meta Platforms, Inc.

Garanties : conditions de traitement des données WhatsApp Business et avenant de transfert : les transferts vers WhatsApp LLC et Meta Platforms, Inc. reposent sur le Data Privacy Framework ; l'avenant permet à WhatsApp de recourir à un autre mécanisme reconnu, notamment les clauses contractuelles types de la Commission (décision 2021/914, module 3).

4. Périmètres distincts

Stripe traite les paiements et abonnements dans le cadre des traitements propres de SUBVERSION ; il ne reçoit pas par principe les contenus des projets. La publication Instagram résulte d'une instruction expresse vers le compte connecté du client et ses destinataires ; elle n'autorise pas la transmission générale des autres contenus à Meta.

Les traitements de sécurité générale, notamment les informations d'attaque adressées à CrowdSec, sont distingués des traitements de projets ; rôles, base légale et destinataires sont décrits dans la politique de confidentialité.