

Table des matières

LIBERTY Shield — Dossier de conformité	2
Bloc « Identité » — la seule source de cette information	2
Ce que contient le dossier	3
Le point de départ : ce que l'éditeur ne peut pas faire	3
Écarts assumés	4
Bases légales retenues	4
Droits des personnes	5
Registre des activités de traitement — article 30 du RGPD	6
T1 — Gestion du compte et authentification	6
T2 — Sessions et appareils	6
T3 — Contenu des coffres	6
T4 — Partage et coffre familial	7
T5 — Transmission / héritage	7
T6 — Surveillance du dispositif de transmission	7
T7 — Multisig du niveau Sanctuaire	7
T8 — E-mails transactionnels	7
T9 — Preuve de consentement aux documents contractuels	8
T10 — Abonnement et facturation	8
T11 — Journalisation	8
Mesures de sécurité communes	8
Procédure de violation de données — articles 33 et 34 du RGPD	9
Ce qu'une violation peut être ici, et ce qu'elle ne peut pas être	9
Qualification et délais	9
Niveaux de gravité	9
Qui fait quoi	10
Déroulé	10
Registre des violations	10
Modèle de notification à l'autorité de contrôle	10
Modèle d'information aux personnes concernées	11
Divulgaration responsable	11
Accord de traitement des données — modèle	12
Préambule — qui est quoi	12
Article 1 — Objet et durée	12
Article 2 — Instructions documentées	12
Article 3 — Confidentialité	12
Article 4 — Sécurité (article 32)	12
Article 5 — Sous-traitance ultérieure	13
Article 6 — Assistance aux droits des personnes	13
Article 7 — Assistance aux obligations des articles 32 à 36	13
Article 8 — Notification des violations	13
Article 9 — Sort des données en fin de contrat	13
Article 10 — Audit	13
Article 11 — Transferts internationaux	13
Annexe 1 — Périmètre du traitement	13
Annexe 2 — Signatures	14
Gouvernance des métadonnées	15
Pourquoi ce document existe	15
Ce que le serveur ne voit jamais	15
Ce que le serveur voit	15
Mesures de réduction en place	16

Ce qui n'est pas réduit, et pourquoi	16
Réquisitions et demandes d'autorités	16
Politique de conservation et d'effacement	17
Principe	17
Durées par catégorie	17
Suppression du compte	17
Ce qui survit, et pour combien de temps	18
Effacement à la demande	18
Plan de continuité et de reprise	19
Le risque propre à un coffre chiffré	19
Les trois lignes de défense	19
1. Sauvegarde native de l'hébergeur	19
2. Copie indépendante, chiffrée une seconde fois	19
3. Récupération sans serveur	20
Ce qui n'est pas couvert, et doit être dit	20
Objectifs de reprise	20
Exercice du 18 septembre 2026	21
Procédure de reprise	21
Inventaire des variables d'environnement	22
Noms de domaine	22
Le point de défaillance qu'aucune sauvegarde ne couvre	23
Rotation et effacement des sauvegardes	23
Continuité du service en cas de disparition de l'éditeur	23
Sous-traitants et transferts internationaux	24
Liste	24
Ce que chaque sous-traitant peut réellement voir	24
Transferts hors Union européenne	25
Gestion des évolutions	25
Analyse d'impact relative à la protection des données — décision motivée	26
Question posée	26
Examen au regard des critères de l'article 35.3	26
Décision	26
Le point qui a réellement été analysé : le déclenchement automatisé de la transmission	27
Réexamen	27

LIBERTY Shield — Dossier de conformité

Version 1.0 — 18 septembre 2026. Dossier autonome : il se lit et s'envoie seul, sans dépendre d'aucun document d'une autre activité de l'éditeur.

Bloc « Identité » — la seule source de cette information

Toutes les autres pièces du dossier renvoient ici. Aucune ne répète ces éléments. Un changement de structure porteuse se répercute donc en modifiant ce seul bloc.

Responsable du traitement	LIBERTY Club LLC
Forme	Limited Liability Company, État du Wyoming (États-Unis)
Siège	30N Gould Street, Sheridan, WY 82801, États-Unis
Contact protection des données	contact@libertyshield.app

Produit concerné	LIBERTY Shield — coffre-fort numérique chiffré de bout en bout (application web et extension de navigateur)
Domaines	libertyshield.app (application), docs.libertyshield.app (documentation), assets.libertyshield.app (ressources publiques)
Délégué à la protection des données	Non désigné — voir « Écarts assumés » ci-dessous
Représentant au sens de l'article 27	Non désigné à ce jour — voir « Écarts assumés » ci-dessous

Ce que contient le dossier

Section	Objet
1. Identité, périmètre et écarts	Le présent document : responsable du traitement, clé de lecture, écarts assumés, bases légales, droits
2. Registre des activités de traitement	Les onze traitements en production, champ par champ (article 30)
3. Procédure de violation de données	Qualification, délais, rôles, registre et modèles de notification (articles 33 et 34)
4. Accord de traitement des données	Modèle prêt à signer pour un client responsable de traitement (article 28.3)
5. Gouvernance des métadonnées	Ce que le serveur voit, ce qu'il ne voit jamais, et ce qui n'est pas réductible
6. Politique de conservation et d'effacement	Durées réelles appliquées par le code, et déroulé de la suppression de compte
7. Plan de continuité et de reprise	Trois lignes de défense, cibles de RTO et de RPO, rotation des sauvegardes
8. Sous-traitants et transferts internationaux	Liste exhaustive, ce que chacun peut réellement voir, encadrement des transferts
9. Analyse d'impact	Décision motivée au regard de l'article 35, et analyse du déclenchement automatisé

Documents publics associés, opposables et accessibles sans compte :

- Conditions générales d'utilisation et politique de confidentialité, version 1.2 du 18 septembre 2026, en français, anglais et espagnol, affichées dans l'application avant toute création de compte.
- Whitepaper sécurité — architecture cryptographique réellement déployée, modèle de menace, mesures en place : <https://assets.libertyshield.app/whitepaper-securite.pdf>
- Documentation produit et tutoriels : <https://docs.libertyshield.app>
- Module de chiffrement client et décrypteur hors-ligne, publiés en open source sous licence MIT.

Le point de départ : ce que l'éditeur ne peut pas faire

Shield chiffre chaque donnée sur l'appareil de l'utilisateur, sous une clé dérivée d'un secret que l'éditeur ne détient à aucun moment. Le serveur ne reçoit que des blocs opaques.

Cette architecture a une conséquence directe en matière de protection des données, et c'est la clé de lecture de tout le dossier : **pour le contenu des coffres, l'éditeur n'est pas en situation de porter atteinte à la confidentialité, y compris s'il le voulait, y compris sous contrainte légale.** Une réquisition ne peut produire que du chiffré. Une compromission de l'infrastructure ne peut produire que du chiffré. Un employé malveillant ne peut produire que du chiffré.

Le risque résiduel ne porte donc pas sur le contenu mais sur les **métadonnées** — qui a un compte, avec qui il partage, qui il a désigné comme bénéficiaire. Elles sont traitées pour ce qu'elles sont, à la section « Gouvernance des métadonnées », sans minimisation.

Écarts assumés

Ce dossier nomme ses manques plutôt que de les laisser découvrir. Chacun est daté, motivé et suivi.

Écart	Situation au 18/09/2026	Décision
Représentant article 27	Non désigné. La politique de confidentialité s'engage désormais à le désigner et à publier ses coordonnées.	Obligation reconnue, et non conditionnée à un volume : elle naît du fait de s'adresser à des personnes situées dans l'Union. La désignation interviendra à l'ouverture commerciale — mise en vente au public européen, ou premier contrat avec un partenaire institutionnel ou un distributeur — et non pendant la phase de prévente auprès d'un nombre restreint de clients identifiés. C'est un arbitrage de calendrier , énoncé comme tel et non habillé en exemption juridique. La désignation dépend par ailleurs de l'arbitrage en cours sur la structure porteuse.
Délégué à la protection des données	Non désigné.	Non requis en l'état : pas de suivi systématique à grande échelle au sens de l'article 37.1.b — l'éditeur n'a, par construction, aucun accès au contenu et ne profile pas ses utilisateurs. Position réexaminée à chaque changement de finalité.
Audit de sécurité tiers	Non réalisé.	Planifié après les premières préventes. Aucune certification ni validation externe n'est revendiquée ; le whitepaper le dit explicitement. D'ici là : audit interne documenté et publié, y compris les affirmations que cet audit a conduit à corriger, et cœur cryptographique ouvert en MIT.
Certifications (ISO 27001, SOC 2, HDS)	Aucune.	Non revendiquées, nulle part.

Bases légales retenues

Traitement	Base légale
Fourniture du service, authentification, stockage du coffre chiffré	Exécution du contrat (art. 6.1.b)
Transmission / héritage : invitations, notifications, surveillance du dispositif	Exécution du contrat (art. 6.1.b), à l'initiative et sur désignation du titulaire

Traitement	Base légale
E-mails transactionnels (vérification d'adresse, alertes de sécurité)	Exécution du contrat (art. 6.1.b)
Journaux de sécurité, limitation de débit, lutte contre l'abus	Intérêt légitime (art. 6.1.f) — sécurité du service
Preuve de consentement aux documents contractuels (version, date, adresse IP)	Obligation légale et intérêt légitime probatoire
Abonnement et facturation	Exécution du contrat (art. 6.1.b) et obligations comptables

Aucun traitement du service ne repose sur le consentement au sens de l'article 6.1.a : il n'y a ni publicité, ni pistage, ni revente, ni profilage. Aucun cookie autre que le stockage local strictement nécessaire à la session et aux préférences.

Droits des personnes

Accès, rectification, effacement, limitation, portabilité, opposition. Réponse dans les délais légaux, en principe sous trente jours, à contact@libertyshield.app.

Deux particularités tiennent à l'architecture et sont énoncées telles quelles :

- **L'effacement est réel et immédiat.** La suppression du compte est irréversible, exige le mot de passe maître, purge les fichiers chiffrés du stockage objet et efface en cascade l'intégralité des données liées. Détail à la section « Politique de conservation et d'effacement ».
- **La portabilité du contenu ne passe pas par l'éditeur.** L'utilisateur exporte lui-même son coffre, en clair ou chiffré, depuis son appareil. L'éditeur ne peut pas produire ce contenu à sa place : il ne l'a jamais lisible.

Réclamation possible auprès de l'autorité de protection des données du pays de résidence.

Registre des activités de traitement — article 30 du RGPD

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier. Aucune autre pièce du dossier ne répète ces informations.

Le registre décrit les traitements **réellement en production**, tels qu'on peut les lire dans le schéma de base et le code du service. Chaque rubrique nomme les données au niveau du champ.

T1 — Gestion du compte et authentification

Finalité. Créer un compte, authentifier son titulaire, maintenir sa session, permettre le recouvrement d'accès par la feuille de secours. **Base légale.** Exécution du contrat. **Personnes concernées.** Utilisateurs titulaires d'un compte.

Données traitées. Adresse e-mail ; nom affiché ; rôle et statut du compte ; date de vérification de l'adresse ; niveau d'offre ; sel et paramètres de dérivation Argon2id ; empreinte d'authentification **re-hachée côté serveur** ; clé de compte **enveloppée** ; clé publique X25519 ; clé privée X25519 **enveloppée** ; éléments de secours (sel, clé enveloppée, empreinte re-hachée) ; dates de création et de mise à jour.

Ce qui n'est pas traité. Aucun mot de passe, aucune clé en clair, aucune empreinte d'authentification exploitable en l'état. La clé maître est dérivée sur l'appareil et **n'est jamais transmise**.

Destinataires. Hébergeur applicatif et base de données (voir la section « Sous-traitants et transferts internationaux »).

Conservation. Durée du compte, puis effacement immédiat — voir la section « Politique de conservation et d'effacement ».

T2 — Sessions et appareils

Finalité. Maintenir une session, permettre sa révocation, reconnaître un appareil enrôlé en biométrie. **Base légale.** Exécution du contrat ; intérêt légitime pour la partie sécurité.

Données traitées. Empreinte du jeton de rafraîchissement (jamais le jeton), agent utilisateur, adresse IP, dates d'expiration et de révocation. Pour un appareil enrôlé : nom donné par l'utilisateur, identifiant et clé publique de l'authentificateur WebAuthn, compteur de signature, date de dernière utilisation.

Point notable. Les éléments de déverrouillage rapide — code PIN et clé biométrique — **ne sont jamais transmis au serveur** : ils vivent dans le stockage local de l'appareil. Le scellé du code PIN combine le code et une sortie non extractible de l'enclave sécurisée de l'appareil.

Conservation. Jeton d'accès : 1 heure. Session de rafraîchissement : 30 jours, révocable à tout moment.

T3 — Contenu des coffres

Finalité. Stocker et synchroniser le contenu du coffre entre les appareils du titulaire. **Base légale.** Exécution du contrat.

Données traitées. Blocs chiffrés (ciphertext + nonce), clés d'éléments **enveloppées**, type d'élément, marqueurs de statut non sensibles (épinglé, privé), versions antérieures chiffrées, horodatages. Pièces jointes : blob chiffré en stockage objet, métadonnées de fichier (nom, type MIME) **chiffrées côté client**, taille en octets en clair.

Ce que le serveur voit. Un type d'élément, une taille, une date. **Jamais un titre, un identifiant, un mot de passe, une seed, un nom de fichier.**

Destinataires. Hébergeur de base de données ; stockage objet pour les pièces jointes. **Conservation.** Durée du compte. Effacement en cascade à la suppression, y compris purge des blobs du stockage objet.

T4 — Partage et coffre familial

Finalité. Permettre à un titulaire de partager un élément ou un coffre commun avec une personne de son choix. **Base légale.** Exécution du contrat, à l'initiative du titulaire. **Personnes concernées.** Titulaires et destinataires d'un partage.

Données traitées. Lien entre deux comptes, clé d'élément ou de coffre **scellée** vers la clé publique du destinataire, permission (lecture / édition), horodatage. Pour une invitation en attente : adresse e-mail invitée et statut.

Garde-fou en place. Une adresse e-mail non vérifiée n'est ni consultable dans l'annuaire, ni éligible à un partage. Avant le premier scellement vers une personne, la clé publique du destinataire est vérifiée hors bande par une empreinte de six mots, puis épinglée dans le coffre chiffré du vérificateur.

T5 — Transmission / héritage

Finalité. Organiser l'accès technique aux informations du titulaire au profit de personnes qu'il désigne, en cas de décès ou d'incapacité durable. **Base légale.** Exécution du contrat, sur désignation expresse du titulaire. **Personnes concernées.** Titulaires ; bénéficiaires et exécuteurs désignés par eux.

Données traitées. Pour chaque personne désignée : adresse e-mail, civilité, prénom, nom, étude ou cabinet, rôle, statut, indication du port d'un fragment, dates d'acceptation et d'accusé de réception. Note privée du titulaire sur la personne et message qui lui est destiné : **chiffrés**, illisibles du serveur. Paramètres du dispositif : intervalle de signal de vie, délai de grâce, fenêtre de refus, seuils. Legs : bloc chiffré, seuil d'ouverture, nombre d'entrées.

Ce que le serveur voit. Qui a été désigné et sous quel rôle. **Jamais** le contenu du legs, ni les fragments de clé, qui ne lui sont jamais transmis.

Information des personnes désignées. Chaque personne reçoit un e-mail nommant le titulaire et le rôle proposé, et doit créer un compte puis accepter expressément. Rien ne lui est imposé. **Conservation.** Durée du dispositif ; effacement explicite à la suppression du compte du titulaire.

T6 — Surveillance du dispositif de transmission

Finalité. Détecter qu'un dispositif de transmission est devenu inopérant, et en avertir le seul titulaire tant qu'il peut corriger. **Base légale.** Exécution du contrat.

Données traitées. Comparaison du nombre de porteurs confirmés au seuil d'ouverture, ancienneté des accusés de réception du canal, indicateur de legs périmé, date et motif du dernier rappel envoyé.

Limites en place. Le calcul porte sur des **métadonnées seules**. Les rappels ne partent qu'au titulaire, au maximum une fois par mois et par motif, et uniquement tant qu'aucune libération n'est engagée.

T7 — Multisig du niveau Sanctuaire

Finalité. Subordonner le déverrouillage du niveau le plus sensible à l'accord d'un nombre choisi de détenteurs. **Base légale.** Exécution du contrat, sur activation expresse du titulaire.

Données traitées. Seuil ; lien entre la configuration et le compte de chaque détenteur ; part SLIP-39 **scellée** vers la clé publique du détenteur ; étiquette libre non sensible ; demandes de déverrouillage avec demandeur, statut et expiration ; approbations avec part re-scellée.

T8 — E-mails transactionnels

Finalité. Vérifier une adresse, notifier une invitation, un signal de vie manqué, une fenêtre de refus ouverte, un legs libéré, un rappel de santé du dispositif, une alerte de facturation. **Base légale.** Exécution du contrat. **Données transmises au prestataire.**

Adresse e-mail du destinataire, objet, corps du message. **Aucun secret, aucun fragment, aucun contenu de coffre ne transite par e-mail. Destinataire.** Prestataire d'envoi établi dans l'Union européenne — voir la section « Sous-traitants et transferts internationaux ».

T9 — Preuve de consentement aux documents contractuels

Finalité. Établir qu'une version déterminée des conditions générales et de la politique de confidentialité a été acceptée, et à quelle date. **Base légale.** Obligation légale et intérêt légitime probatoire. **Données traitées.** Type de document, version, date d'acceptation, adresse IP.

Point notable. L'adresse IP enregistrée est celle ajoutée par le proxy d'infrastructure, non celle annoncée par le client : une preuve de consentement ne doit pas pouvoir être choisie par la personne qu'elle engage. **Conservation.** Durée du compte, puis effacement avec lui.

T10 — Abonnement et facturation

Finalité. Encaisser un abonnement, en suivre le statut, relancer en cas d'échec de paiement. **Base légale.** Exécution du contrat ; obligations comptables. **Données traitées.** Identifiants client et abonnement du prestataire de paiement, statut, référence tarifaire, fin de période, date de début d'impayé, nombre de relances. **Point notable.** **Aucune donnée de carte bancaire n'est reçue ni stockée par l'éditeur** : la saisie et la conservation relèvent entièrement du prestataire de paiement.

T11 — Journalisation

Finalité. Sécurité du service, diagnostic, traçabilité des actions sensibles pour le titulaire lui-même. **Base légale.** Intérêt légitime. **Données traitées.** Identifiant du compte, libellé d'action, métadonnées associées, horodatage. Le journal est **consultable par le titulaire** dans l'application.

Mesures de sécurité communes

Elles sont décrites en détail, avec leur modèle de menace, dans le whitepaper sécurité publié (voir la section 1).

- Chiffrement de bout en bout côté client : XChaCha20-Poly1305 en chiffrement authentifié, Argon2id pour la dérivation, X25519 pour les scelllements, hiérarchie de clés à quatre niveaux.
- Empreinte d'authentification re-hachée côté serveur et comparée en temps constant.
- Politique de sécurité de contenu stricte interdisant l'exfiltration vers un domaine tiers.
- Limitation de débit sur la connexion, le rafraîchissement de jeton, la recherche d'annuaire et les routes d'administration ; protection contre l'énumération des comptes.
- Vérification obligatoire de l'adresse e-mail avant tout partage, part de Sanctuaire ou acceptation de legs.
- Vérification hors bande des clés publiques par empreinte de six mots, épinglée dans le coffre chiffré de l'utilisateur.
- Déverrouillage rapide scellé par l'enclave sécurisée de l'appareil ; aucun élément de déverrouillage rapide côté serveur.
- Mot de passe maître exigé pour les opérations irréversibles : suppression de compte, régénération de la feuille de secours, export en clair.
- Double sauvegarde, dont une copie indépendante chiffrée une seconde fois chez un fournisseur distinct — voir la section « Plan de continuité et de reprise ».

Procédure de violation de données — articles 33 et 34 du RGPD

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier.

Ce qu'une violation peut être ici, et ce qu'elle ne peut pas être

L'architecture de Shield borne la gravité de tout incident : **le contenu des coffres n'est pas exposable par une compromission de l'infrastructure**, puisque le serveur n'en détient aucune clé. Une base entière exfiltrée donne des blocs opaques, dont l'ouverture exige un secret dérivé sur l'appareil de chaque titulaire.

La procédure ne s'en déduit pas plus courte : elle se concentre sur ce qui est réellement exposable — les **métadonnées** — et sur ce qui serait réellement grave — une **atteinte au code servi**, seul scénario capable de capter un secret avant chiffrement.

Qualification et délais

Le délai de 72 heures de l'article 33 court à **compter de la connaissance** de la violation, c'est-à-dire du moment où un fait établi, et non un simple soupçon, indique une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de données à caractère personnel.

Étape	Délai visé
Consignation initiale dans le registre des violations	Immédiate, dès le signalement
Qualification : est-ce une violation ? quel niveau ?	24 heures
Notification à l'autorité de contrôle, si risque	72 heures à compter de la connaissance
Information des personnes concernées, si risque élevé	Dans les meilleurs délais
Rapport de clôture et mesures correctrices	30 jours

Une notification incomplète est envoyée dans les délais puis **complétée**, plutôt que retardée — l'article 33.4 le permet expressément.

Niveaux de gravité

Niveau	Définition	Exemples	Conduite
N1 — Sans risque	Aucune donnée à caractère personnel n'est atteinte, ou uniquement des données chiffrées dont les clés ne sont pas compromises.	Exfiltration de blocs chiffrés sans compromission d'appareil ; perte d'une sauvegarde chiffrée dont la clé est restée hors du système.	Consignation au registre. Analyse des causes. Pas de notification ; la position et son raisonnement sont écrits, datés et conservés.
N2 — Risque	Des métadonnées sont exposées : adresses e-mail, noms affichés, liens entre comptes, identités de bénéficiaires ou d'exécuteurs.	Accès non autorisé à la base ; fuite de journaux contenant des adresses ; erreur d'adressage d'un envoi d'e-mails.	Notification à l'autorité de contrôle sous 72 h. Information des personnes si le risque le justifie.

Niveau	Définition	Exemples	Conduite
N3 — Risque élevé	Un secret en clair a pu être capté, ou l'intégrité du code servi est en cause.	Code de l'application altéré ; compromission d'une clé de signature ou de déploiement ; chaîne de distribution de l'extension compromise.	Notification à l'autorité et information individuelle des personnes concernées, sans délai. Mise hors ligne immédiate si nécessaire.

Qui fait quoi

L'éditeur est une structure à effectif réduit : la procédure le dit plutôt que de décrire une organisation qui n'existe pas.

Rôle	Titulaire	Mission
Point de contact et décideur	Le dirigeant de l'entité responsable (voir bloc « Identité »)	Qualifie, décide de notifier, signe les notifications
Suppléance	Désignée par écrit en cas d'indisponibilité prolongée du décideur	Mêmes pouvoirs, sur le seul périmètre de l'incident
Réception des signalements	contact@libertyshield.app, surveillé quotidiennement	Consigne et alerte le décideur

Aucune décision de ne pas notifier n'est prise oralement. Elle est écrite, motivée et datée dans le registre des violations.

Déroulé

1. **Signaler et consigner.** Tout signalement — interne, utilisateur, chercheur, prestataire — est inscrit au registre avec sa date et son heure de réception.
2. **Contenir.** Révocation des accès et des jetons concernés, rotation des secrets d'infrastructure, mise hors ligne du composant si l'intégrité du code est en cause.
3. **Qualifier.** Nature de la violation, catégories et volume approximatif de personnes et d'enregistrements, conséquences probables, niveau N1 / N2 / N3.
4. **Notifier.** À l'autorité de contrôle compétente si N2 ou N3, sous 72 heures, selon le modèle ci-dessous. Aux personnes concernées si N3, en clair et sans jargon.
5. **Corriger et clore.** Correctif, vérification, rapport de clôture sous 30 jours. Si l'incident révèle une affirmation inexacte dans un document public, **ce document est corrigé.**

Registre des violations

Tenu que la violation soit notifiable ou non — c'est une obligation autonome de l'article 33.5.

Colonnes : identifiant ; date et heure de la connaissance ; source du signalement ; description des faits ; systèmes et données concernés ; catégories et nombre approximatif de personnes ; niveau retenu ; **motivation écrite** de la décision de notifier ou non ; date et référence de la notification à l'autorité ; date et forme de l'information des personnes ; mesures de confinement ; mesures correctrices ; date de clôture.

Modèle de notification à l'autorité de contrôle

Objet — Notification d'une violation de données à caractère personnel (article 33 du RGPD)

1. Responsable du traitement. Voir le bloc « Identité » du dossier de conformité. Contact : contact@libertyshield.app. Représentant au sens de l'article 27 : statut indiqué au même endroit.

2. Date et heure de la connaissance. [date, heure, fuseau]

3. Nature de la violation. [confidentialité / intégrité / disponibilité] — [description factuelle des faits, sans spéculation]

4. Catégories de données concernées. [métadonnées de compte / données de transmission / journaux / blocs chiffrés]. Préciser, le cas échéant : *les données concernées sont chiffrées de bout en bout et les clés correspondantes ne sont pas détenues par le responsable de traitement.*

5. Catégories et nombre approximatif de personnes concernées. [nombre] — [utilisateurs titulaires / personnes désignées comme bénéficiaires ou exécuteurs]

6. Conséquences probables. [analyse motivée]

7. Mesures prises ou proposées. [confinement, correctif, information des personnes, mesures préventives]

8. Information des personnes concernées. [faite le ... / non requise, motif]

9. Point de contact pour toute information complémentaire. contact@libertyshield.app

Modèle d'information aux personnes concernées

Objet — Information relative à un incident de sécurité

Bonjour,

Nous vous informons d'un incident survenu le [date] et affectant [description en langage clair].

Ce qui est concerné : [liste explicite]. **Ce qui ne l'est pas :** le contenu de votre coffre est chiffré sur votre appareil, sous une clé que nous ne détenons à aucun moment. [Adapter si ce n'est pas le cas — ne jamais écrire cette phrase si elle est inexacte.] **Ce que nous avons fait :** [mesures]. **Ce que nous vous recommandons de faire :** [actions concrètes, dans l'ordre].

Pour toute question : contact@libertyshield.app.

Maxime

Divulcation responsable

Un chercheur en sécurité peut signaler une vulnérabilité à contact@libertyshield.app. Engagements : accusé de réception sous 72 heures, aucune poursuite pour une recherche de bonne foi respectant la vie privée des utilisateurs, correctif coordonné, mention du chercheur s'il le souhaite. Un signalement est traité comme un incident tant que son absence d'impact n'est pas établie.

Accord de traitement des données — modèle

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier. Modèle prêt à signer, conforme à l'article 28.3 du RGPD. Il est conclu **sur demande** à contact@libertyshield.app par tout client agissant en qualité de responsable de traitement.

Préambule — qui est quoi

Pour un particulier utilisant Shield à titre personnel, cet accord est sans objet : l'éditeur est responsable de traitement pour les métadonnées nécessaires au service, et la relation est régie par les conditions générales et la politique de confidentialité.

Le présent accord s'applique lorsqu'une organisation — cabinet, étude, family office, employeur — déploie Shield pour ses propres clients ou collaborateurs. Elle est alors **responsable de traitement** ; l'éditeur agit comme **sous-traitant** pour les métadonnées qu'il traite pour son compte.

Particularité à ne pas perdre de vue. Le contenu des coffres est chiffré de bout en bout, sous des clés que l'éditeur ne détient à aucun moment. Pour ce contenu, l'éditeur n'est pas en mesure d'exécuter une instruction de lecture, de rectification ou d'extraction, **quelle qu'en soit l'origine**. La sous-traitance porte donc sur les métadonnées énumérées à l'annexe 1, et sur elles seules.

Article 1 — Objet et durée

L'éditeur traite pour le compte du responsable de traitement les données décrites à l'annexe 1, aux seules fins de fournir le service Shield, pour la durée de l'abonnement et pendant la période de restitution et d'effacement prévue à l'article 9.

Article 2 — Instructions documentées

L'éditeur ne traite les données que sur instruction documentée du responsable de traitement, y compris pour les transferts hors Union européenne. Le contrat de service et le présent accord constituent l'instruction initiale complète.

L'éditeur informe immédiatement le responsable de traitement s'il estime qu'une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données.

Lorsqu'une obligation légale de l'État du siège de l'éditeur impose un traitement, l'éditeur en informe le responsable de traitement avant de l'exécuter, **sauf interdiction légale de le faire**. Il est expressément rappelé qu'une injonction de produire le contenu d'un coffre ne peut, en fait comme en droit, aboutir qu'à la remise de données chiffrées inexploitable par l'éditeur.

Article 3 — Confidentialité

Toute personne autorisée à traiter les données est soumise à une obligation de confidentialité contractuelle et ne dispose d'un accès que dans la mesure strictement nécessaire à sa mission. La liste des personnes autorisées est tenue à jour et communiquée sur demande.

Article 4 — Sécurité (article 32)

Les mesures techniques et organisationnelles en vigueur sont décrites dans le registre (la section « Registre des activités de traitement », rubrique « Mesures de sécurité communes ») et, dans le détail de leur modèle de menace, dans le whitepaper sécurité publié. Elles comprennent notamment le chiffrement de bout en bout côté client, une dérivation de clé à coût mémoire élevé, l'absence structurelle d'accès de l'éditeur au contenu, la limitation de débit, la vérification obligatoire des adresses e-mail et une double sauvegarde dont une copie indépendante chiffrée une seconde fois.

L'éditeur n'oppose aucune certification qu'il ne détient pas : au 18 septembre 2026, **aucun audit de sécurité tiers n'a été réalisé et aucune certification n'est revendiquée**. L'état réel est celui décrit dans la section 1, rubrique « Écarts assumés ».

Article 5 — Sous-traitance ultérieure

Le responsable de traitement autorise le recours aux sous-traitants ultérieurs listés à la section « Sous-traitants et transferts internationaux ». L'éditeur informe le responsable de traitement de tout ajout ou remplacement **au moins trente jours à l'avance**, par e-mail à l'adresse de contact désignée au contrat. Le responsable de traitement peut s'y opposer par écrit et motivé dans ce délai ; à défaut d'accord, il peut résilier sans pénalité la part du service concernée.

L'éditeur impose à chaque sous-traitant ultérieur, par contrat, des obligations de protection au moins équivalentes à celles du présent accord, et demeure pleinement responsable de leur exécution.

Article 6 — Assistance aux droits des personnes

L'éditeur assiste le responsable de traitement, par des mesures techniques et organisationnelles appropriées, dans la réponse aux demandes d'exercice des droits. En pratique :

- **Accès, rectification, effacement des métadonnées** : exécutés par l'éditeur sur demande, dans les délais convenus.
- **Portabilité et accès au contenu** : exécutés par la personne elle-même depuis son appareil, au moyen des fonctions d'export du produit. L'éditeur ne peut pas s'y substituer, ne détenant pas les clés.

Article 7 — Assistance aux obligations des articles 32 à 36

L'éditeur assiste le responsable de traitement dans le respect des obligations de sécurité, de notification de violation et d'analyse d'impact, compte tenu de la nature du traitement et des informations dont il dispose. Sa procédure de violation est documentée à la section « Procédure de violation de données ».

Article 8 — Notification des violations

L'éditeur notifie au responsable de traitement toute violation de données à caractère personnel le concernant **dans les meilleurs délais et au plus tard 48 heures après en avoir eu connaissance**, avec les éléments énumérés à l'article 33.3 du RGPD, afin que le responsable de traitement puisse tenir son propre délai de 72 heures.

Article 9 — Sort des données en fin de contrat

Au terme du contrat, au choix du responsable de traitement exprimé par écrit : restitution ou effacement. À défaut de choix exprimé dans les trente jours, **l'effacement s'applique**. Les copies de sauvegarde sont purgées selon le cycle décrit à la section « Plan de continuité et de reprise ». Un certificat d'effacement est délivré sur demande.

Article 10 — Audit

L'éditeur met à disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de l'article 28, et permet la réalisation d'audits, y compris d'inspections, par le responsable de traitement ou un auditeur qu'il mandate, dans la limite d'un audit par an sauf incident, avec un préavis raisonnable et dans des conditions préservant la sécurité des autres clients.

Article 11 — Transferts internationaux

Les transferts hors Union européenne, leurs destinataires et leur encadrement sont décrits à la section « Sous-traitants et transferts internationaux ». Les clauses contractuelles types de la Commission européenne, dans leur version en vigueur, s'appliquent lorsque la réglementation l'exige.

Annexe 1 — Périmètre du traitement

Objet. Fourniture d'un service de coffre-fort numérique chiffré de bout en bout, incluant le partage, la transmission et le déverrouillage à seuil. **Durée.** Durée de l'abonnement, augmentée de la période d'effacement. **Nature des opérations.** Collecte, enregistrement, conservation, consultation, transmission aux destinataires désignés par la personne, effacement. **Catégories**

de personnes concernées. Utilisateurs titulaires d'un compte ; personnes désignées par eux comme bénéficiaires, exécuteurs ou détenteurs d'une part.

Catégories de données traitées pour le compte du responsable de traitement :

- Identifiants de compte : adresse e-mail, nom affiché, rôle, statut, dates.
- Données d'authentification non réversibles : sels, paramètres de dérivation, empreintes re-hachées, clés enveloppées ou scellées.
- Métadonnées techniques : sessions, agent utilisateur, adresse IP, appareils enrôlés.
- Métadonnées relationnelles : liens de partage, désignations de bénéficiaires et d'exécuteurs, appartenance à un coffre familial, détention d'une part.
- Métadonnées d'abonnement : identifiants du prestataire de paiement, statut, échéances.
- Preuve de consentement : type de document, version, date, adresse IP.
- Journaux d'activité et de sécurité.

Catégories de données expressément exclues du périmètre de sous-traitance, faute d'accès : le contenu des coffres, les pièces jointes, les noms de fichiers, les notes privées, le contenu des legs, les fragments de clé et tout élément de déverrouillage rapide — tous chiffrés sur l'appareil ou conservés hors du serveur.

Aucune catégorie particulière de données au sens de l'article 9 n'est traitée par l'éditeur. L'utilisateur peut en placer dans son coffre ; elles y sont chiffrées avant tout envoi et demeurent hors de portée de l'éditeur.

Annexe 2 — Signatures

Responsable de traitement	Sous-traitant
Entité	Voir bloc « Identité »
Représenté par	
Qualité	
Date	
Signature	

Gouvernance des métadonnées

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier.

Pourquoi ce document existe

Un coffre chiffré de bout en bout déplace le risque : il ne le supprime pas. Le contenu devient inatteignable, y compris pour l'éditeur ; ce qui reste visible, ce sont les **métadonnées** — l'existence d'un compte, l'identité de ses correspondants, le rythme de ses connexions.

Ce document énumère ce que le serveur voit réellement, ce qu'il ne voit jamais, et ce qui est fait pour réduire le reste. Il est écrit pour être opposable : chaque ligne correspond à une colonne existante de la base.

Ce que le serveur ne voit jamais

Élément	Où il est protégé
Titres, identifiants, mots de passe, seeds, notes, codes 2FA	Chiffrés sur l'appareil avant tout envoi (XChaCha20-Poly1305)
Noms et types des fichiers joints	Métadonnées de fichier chiffrées côté client
Contenu des pièces jointes	Blob chiffré, la clé ne quitte pas l'appareil
Contenu du legs et instructions aux bénéficiaires	Chiffré par une clé de legs découpée en fragments physiques jamais transmis
Notes privées du titulaire sur une personne désignée	Chiffrées pour le titulaire seul
Messages scellés vers un bénéficiaire, un exécuteur, un détenteur de part	Scellés vers la clé publique du destinataire ; l'éditeur ne peut pas les ouvrir
Parts SLIP-39 du Sanctuaire et fragments de legs	Scellés vers leur détenteur, ou jamais transmis du tout
Code PIN, clé biométrique, scellés de déverrouillage rapide	Ne quittent jamais l'appareil
Mot de passe maître, clé maître, phrase du Sanctuaire	Jamais transmis ; seule une empreinte dérivée l'est, elle-même re-hachée à l'arrivée

Conséquence. Une réquisition judiciaire, une compromission de l'hébergeur ou un employé malveillant ne peuvent produire que du chiffré. Ce n'est pas une promesse de bonne conduite : c'est une propriété de l'architecture, vérifiable dans le code client publié en open source.

Ce que le serveur voit

Métadonnée	Pourquoi elle existe	Ce qu'elle révèle
Adresse e-mail, nom affiché	Authentifier, notifier, permettre d'être trouvé pour un partage	Identité déclarée
Dates de création, de mise à jour, de dernière session	Fonctionnement, sécurité	Rythme d'usage
Adresse IP et agent utilisateur des sessions	Révocation, détection d'abus	Localisation approximative, appareil
Type d'élément (mot de passe, carte, wallet, note...) et nombre d'éléments	Affichage, quotas, statistiques du titulaire	Nature générale de l'usage, jamais son contenu
Taille des pièces jointes	Quotas, facturation du stockage	Ordre de grandeur
Liens de partage entre deux comptes	Faire fonctionner le partage	Qui connaît qui

Métadonnée	Pourquoi elle existe	Ce qu'elle révèle
Désignations de bénéficiaires et d'exécuteurs : e-mail, nom, rôle, étude	Invitations, notifications, déclenchement	Le cercle de confiance et une intention successorale
Détention d'une part de Sanctuaire	Faire fonctionner le seuil	Lien de confiance renforcé
Statut d'abonnement	Facturation	Niveau d'offre
Preuve de consentement : version, date, adresse IP	Obligation probatoire	Acceptation datée
Journal d'activité	Sécurité, transparence envers le titulaire	Suite d'actions

La ligne la plus sensible du tableau est le graphe relationnel : partages, bénéficiaires, exécuteurs, détenteurs de parts. C'est la seule donnée du service dont la divulgation aurait, en elle-même, une portée intime — elle dessine un cercle de confiance et, pour la transmission, une intention. Elle est traitée comme telle ci-dessous.

Mesures de réduction en place

- **Aucune donnée de contenu n'entre jamais dans un e-mail.** Les notifications nomment le titulaire et le rôle, jamais un secret, jamais un fragment.
- **L'annuaire est fermé.** Une adresse non vérifiée n'y est pas consultable ; les routes de recherche sont limitées en débit et protégées contre l'énumération.
- **Les notes du titulaire sur une personne sont chiffrées pour lui seul.** Le serveur connaît le fait de la désignation, jamais son motif.
- **La surveillance du dispositif de transmission ne lit que des compteurs** : un nombre de porteurs, un seuil, des dates d'accusé de réception. Elle n'ouvre rien et n'écrit à personne d'autre qu'au titulaire.
- **Les identités internes sont opaques.** Les identifiants techniques ne portent ni horodatage ni séquence exploitable.
- **L'adresse IP de consentement est celle du proxy d'infrastructure**, non celle annoncée par le client : elle est une preuve, elle ne doit pas être choisie par la personne qu'elle engage.
- **Le journal d'activité appartient au titulaire** : il le consulte dans l'application. La transparence est d'abord due à celui dont on journalise les actions.
- **Aucune publicité, aucun pistage, aucun cookie tiers, aucun profilage, aucune revente.** Ni maintenant ni sous condition.

Ce qui n'est pas réduit, et pourquoi

Le graphe relationnel ne peut pas être chiffré sans perdre la fonction qu'il sert : le serveur doit savoir à quelle adresse envoyer une invitation, et quel compte a le droit de télécharger un legs libéré. Le chiffrer reviendrait à supprimer la transmission et le partage.

La position retenue est donc celle-ci, énoncée sans détour : **cette donnée existe, elle est nécessaire, elle est minimisée, et elle est effacée avec le compte.** Un utilisateur qui souhaite ne pas la produire dispose d'un moyen simple : utiliser Shield sans partage ni transmission. Le coffre fonctionne entièrement seul.

Réquisitions et demandes d'autorités

Toute demande d'autorité est examinée au regard du droit applicable et de sa proportionnalité. L'éditeur ne peut remettre que ce qu'il détient : des métadonnées et des blocs chiffrés. Il ne détient aucune clé permettant d'ouvrir un coffre, et **il n'existe aucun mécanisme de séquestre, aucune porte dérobée, aucun compte de secours administrateur.** Une modification de cette architecture serait un changement majeur du produit, annoncé comme tel.

Lorsque la loi ne l'interdit pas, la personne concernée est informée de la demande la visant.

Politique de conservation et d'effacement

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier. Les durées ci-dessous sont celles **appliquées par le code en production**, non des intentions.

Principe

Une donnée est conservée tant qu'elle sert la finalité qui l'a fait naître, puis elle est effacée. Shield n'a ni archive commerciale, ni base d'anciens utilisateurs, ni conservation « au cas où ».

Durées par catégorie

Donnée	Durée	Mécanisme
Compte et éléments d'authentification	Durée du compte	Effacement immédiat à la suppression
Contenu chiffré des coffres, versions antérieures	Durée du compte	Effacement en cascade
Pièces jointes chiffrées en stockage objet	Durée du compte	Suppression explicite des blobs avant l'effacement du compte
Jeton d'accès	1 heure	Expiration intrinsèque au jeton
Session de rafraîchissement	30 jours	Expiration ; révocable à tout moment par l'utilisateur
Jeton de vérification d'adresse e-mail	Jusqu'à expiration	Purge automatique toutes les heures
Jeton de changement d'adresse e-mail	Jusqu'à expiration	Purge automatique toutes les heures
Jeton d'habilitation à usage unique	15 minutes, non jouable	Purge automatique toutes les heures
Données de transmission : personnes désignées, paramètres, legs	Durée du dispositif	Effacement explicite à la suppression du compte du titulaire
Données de multisig Sanctuaire	Durée de la configuration	Effacement en cascade
Preuve de consentement	Durée du compte	Effacement avec le compte
Journal d'activité	Durée du compte	Effacement en cascade
Abonnement	Durée du compte, sous réserve des obligations comptables du prestataire de paiement	Effacement en cascade côté éditeur
Sauvegardes	Voir la section « Plan de continuité et de reprise »	Rotation ; une donnée effacée disparaît des sauvegardes au terme du cycle

Suppression du compte

Elle est **définitive, irréversible, et à la main du seul titulaire**. Aucun administrateur ne peut la déclencher à sa place.

1. **Le mot de passe maître est exigé.** Un jeton d'accès valide ne suffit pas : un appareil ouvert et abandonné ne doit pas permettre de détruire un coffre.
2. **Les pièces jointes sont purgées du stockage objet**, une par une, avant toute autre opération. Un blob orphelin ne bloque pas la suite, mais la tentative est faite pour chacun.
3. **Les données sans lien de cascade sont effacées explicitement** : configuration et personnes de la transmission, legs déposé, demandes de changement d'adresse, jetons de vérification d'adresse et jetons d'habilitation. Ces tables portent un identifiant de compte sans relation formelle : sans effacement explicite, elles survivraient. Elles ne survivent pas.
4. **Le compte est supprimé**, entraînant en cascade coffres, éléments, versions, pièces jointes, habilitations de clé, invitations, partages, bénéficiaires, documents, appareils, sessions, consentements, journal, abonnement et données de multisig.

Aucune corbeille, aucune période de rétention, aucune restauration possible — y compris par l'éditeur.

Ce qui survit, et pour combien de temps

Les sauvegardes. Une donnée effacée reste présente dans les sauvegardes antérieures jusqu'à leur rotation. C'est inhérent à toute politique de continuité et cela doit être dit : le délai réel d'effacement complet est celui du cycle de rotation décrit à la section « Plan de continuité et de reprise ». Les sauvegardes indépendantes sont chiffrées sous une clé conservée hors du système sauvegardé.

Les données détenues par le prestataire de paiement relèvent de ses propres obligations comptables et fiscales, et de sa politique de conservation. L'éditeur n'en dispose pas.

Ce qui a été remis à un tiers sur instruction de l'utilisateur — un fragment papier confié à un porteur, un élément partagé avec un proche, un legs téléchargé après libération — est hors de portée de l'éditeur, par construction. Le produit le dit à l'utilisateur au moment où il le fait.

Effacement à la demande

Une demande adressée à contact@libertyshield.app est traitée dans les délais légaux, en principe sous trente jours. Lorsque la demande porte sur des métadonnées de transmission concernant une personne désignée par un tiers, l'éditeur informe cette personne de la demande et la traite en distinguant ce qui relève du titulaire du dispositif et ce qui relève de la personne désignée.

Plan de continuité et de reprise

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier.

Le risque propre à un coffre chiffré

Le zero-knowledge protège la confidentialité. Il ne protège pas, en lui-même, contre la **disparition** des données — et il aggrave même une forme de risque : personne ne peut reconstituer un contenu perdu, puisque personne d'autre que l'utilisateur ne peut le lire.

Les deux risques sont donc traités séparément, et celui-ci l'est sur trois plans : la sauvegarde de l'infrastructure, une copie totalement indépendante de cette infrastructure, et une voie de récupération qui ne dépend d'aucun serveur.

Les trois lignes de défense

1. Sauvegarde native de l'hébergeur

La base PostgreSQL est protégée par pgBackRest, en archivage continu vers un dépôt objet dédié, distinct du stockage applicatif :

- un segment de journal de transactions est poussé **chaque minute** (compression zstd) ;
- une sauvegarde **différentielle** est prise **chaque jour** ;
- une sauvegarde **complète** est prise périodiquement ;
- le dépôt conserve les **quatre dernières sauvegardes complètes et quatorze différentielles**, les plus anciennes expirant automatiquement ;
- la présence d'une sauvegarde complète exploitable dans le dépôt est **vérifiée toutes les heures**.

La restauration à un instant précis est donc possible à la minute près, sur une fenêtre de plusieurs semaines.

Couvre : panne matérielle, corruption de base, erreur opérationnelle, suppression accidentelle. **Ne couvre pas** : un incident affectant l'hébergeur lui-même — perte du compte, indisponibilité prolongée de la plateforme, incident de région.

2. Copie indépendante, chiffrée une seconde fois

Une fois par jour, le service exporte l'intégralité des tables PostgreSQL, **chiffre l'export une seconde fois côté serveur** en AES-256-GCM, et le dépose chez un fournisseur de stockage objet **distinct de l'hébergeur principal**.

- La clé de ce second chiffrement vit dans l'environnement de déploiement de l'application, **hors de la base sauvegardée et hors du fournisseur de stockage**. Sans elle, la copie est illisible, y compris pour ce fournisseur. Ce que cette couche protège est donc précis, et vaut d'être dit sans exagération : elle neutralise une compromission **du fournisseur de sauvegarde**. Elle ne protège pas d'une compromission de l'hébergeur principal, qui donnerait accès à la base et à la clé.
- Le contenu des coffres y est donc chiffré **deux fois** : une première fois sur l'appareil de l'utilisateur, une seconde fois avant l'envoi.
- L'export couvre l'ensemble des modèles persistants, y compris les configurations et parts scellées du multisig Sanctuaire. Les seules tables volontairement exclues sont éphémères et purgées à expiration : jetons de vérification d'adresse et jetons d'habilitation à usage unique. Elles n'ont aucune valeur de restauration.
- Un échec d'export est journalisé et **retenté au cycle suivant** plutôt que reporté d'un jour.

Les pièces jointes suivent le même chemin. Les blobs des pièces jointes vivent dans le stockage objet principal ; chaque cycle en dépose chez le second fournisseur, sous un préfixe dédié, ceux qui n'y sont pas encore. Ils ne reçoivent pas de second chiffrement, à la différence de l'export : un blob de pièce jointe est **déjà opaque** — son contenu est chiffré sur l'appareil, et son nom comme son type MIME sont chiffrés et conservés en base, jamais dans le blob. Il n'y a aucun clair à protéger, et un second chiffrement interdirait la reprise incrémentale. La règle de cycle de vie du dépôt ne porte que sur les exports : un blob copié correspond à une pièce jointe vivante et n'a pas à disparaître au bout de trente jours.

Couvre : la perte de l'hébergeur principal, quelle qu'en soit la cause, et celle du stockage objet.

3. Récupération sans serveur

Le legs de transmission est ouvrable par un **décrypteur autonome**, page statique publiée en open source, fonctionnant hors ligne. Les bénéficiaires n'ont besoin ni du service, ni d'un compte, ni d'une connexion : les fragments physiques et le fichier de legs suffisent.

Couvre : la disparition définitive de l'éditeur.

Ce qui n'est pas couvert, et doit être dit

Situation	Conséquence	Position
Perte du secret de l'utilisateur	Un mot de passe maître oublié sans feuille de secours rend le coffre définitivement inaccessible. Aucune restauration n'y change quoi que ce soit.	Conséquence assumée du zero-knowledge, énoncée dans le produit, la documentation et le whitepaper. Le produit impose la génération d'une feuille de secours et encourage sa mise à l'abri.
Perte de la clé de chiffrement des sauvegardes	Les copies indépendantes deviennent illisibles.	La clé est détenue hors de la base sauvegardée ; sa perte ne détruit pas les données, la chaîne pgBackRest restant disponible.
Destruction volontaire des copies indépendantes	Les objets déposés chez le fournisseur de sauvegarde sont remplaçables et supprimables par qui détient la clé d'accès au dépôt. Un attaquant ayant pris le contrôle de l'environnement de déploiement pourrait donc effacer la chaîne indépendante.	Écart connu. La parade est l'immuabilité côté stockage (verrouillage d'objet en écriture unique sur la durée de rétention), identifiée comme travaux à venir. La chaîne pgBackRest, qui utilise des identifiants distincts et un autre fournisseur, ne tombe pas avec elle.
Échec silencieux de la copie indépendante	Sans surveillance, une interruption prolongée de l'export passerait inaperçue : un échec ne laisse qu'une ligne de journal.	Couvert. Une veille horaire surveille non pas les erreurs mais l' absence de réussite — ce qui détecte aussi le cas où la tâche ne s'exécute plus du tout. Au-delà de 48 heures sans dépôt abouti, une alerte nommant la dernière réussite et la dernière erreur est envoyée au responsable, au maximum une fois par jour, et un message de rétablissement ferme la boucle dès qu'un dépôt réussit. L'état est consultable à tout moment sur une route d'administration.

Objectifs de reprise

Ces objectifs sont des **cibles déclarées**, non des mesures issues d'un exercice de restauration grandeur nature. Cette distinction est volontaire : un plan de continuité qui présente des cibles comme des résultats éprouvés n'est pas un document de conformité.

Scénario	RPO — perte de données maximale	RTO — délai de remise en service
Corruption ou suppression accidentelle en base	Quelques minutes (restauration à un instant précis)	4 heures

Scénario	RPO — perte de données maximale	RTO — délai de remise en service
Indisponibilité de l'application, infrastructure saine	Nul	1 heure (redéploiement depuis le dépôt)
Perte de l'hébergeur principal	24 heures (dernière copie indépendante)	72 heures (reconstruction de l'infrastructure et restauration)
Perte du stockage objet	24 heures (dernier cycle de miroir)	24 heures, pièces jointes comprises

Engagement de vérification. Un exercice de restauration de la copie indépendante vers une base vierge est réalisé **au moins une fois par an**, et son compte rendu — daté, avec le temps réellement constaté — est ajouté ci-dessous.

Exercice du 18 septembre 2026

Premier exercice complet, mené sur une base PostgreSQL vierge provisionnée pour l'occasion puis détruite.

Étape	Résultat
Objet restauré	Copie indépendante du 18 septembre 2026, 15 h 55 UTC, 2,12 Mo
Déchiffrement AES-256-GCM	Réussi et authentifié — le tag d'intégrité valide l'intégralité du contenu
Lecture	JSON intègre, exploitable
Couverture du schéma	26 modèles persistants sur 26 présents dans la copie
Reconstruction des types	13 comptes : clés enveloppées et horodatages reconstruits sans perte
Reconstitution du schéma	30 secondes
Réinsertion des données	2 770 lignes sur 14 tables peuplées, en moins d'une minute
Contrôle final	Chaque table restaurée contient exactement le nombre de lignes attendu — aucun écart

Ce que l'exercice établit. La copie indépendante est réellement exploitable : elle se déchiffre, se lit et se recharge intégralement dans une base neuve. Ce n'était, jusqu'à cette date, qu'une hypothèse.

Ce qu'il n'établit pas. Il mesure la reconstitution des **données**, pas une reprise complète après sinistre — laquelle comprend aussi le provisionnement de l'infrastructure, la redirection des noms de domaine et le sort des pièces jointes, qui ne figurent pas dans cette copie. Les délais du tableau ci-dessus restent donc des cibles pour ces volets ; seule la restauration des données est désormais mesurée.

Prérequis de restauration, constatés à l'exercice. Une base vierge n'a pas de tables : la restauration commence par reconstituer le schéma, comme le fait le démarrage du service. Et l'outil qui réinsère les données doit être généré à partir de la **même version de schéma** que celle ayant produit la copie — une version antérieure rejette les colonnes qu'elle ne connaît pas. Ces deux points sont désormais vérifiés par le script d'exercice, qui s'interrompt avec la marche à suivre plutôt que sur une erreur technique.

Procédure de reprise

Une sauvegarde restaurable ne suffit pas s'il faut inventer, le jour de l'incident, l'ordre des opérations. La procédure tient en cinq étapes, dans cet ordre.

1. Reconstituer l'hébergement. Créer un projet chez un hébergeur, y provisionner une base PostgreSQL et un service applicatif branché sur le dépôt Git du produit. Le code n'a pas à être sauvegardé : le dépôt Git **est** sa sauvegarde, et il est répliqué chez l'hébergeur du dépôt comme sur chaque poste de travail l'ayant cloné.

2. Reposer les variables d'environnement. C'est le seul élément qui ne vit ni dans le dépôt Git, ni dans les sauvegardes — délibérément, puisqu'il s'agit de secrets. Leur inventaire figure ci-dessous ; leurs valeurs sont conservées par le responsable dans un gestionnaire de secrets, hors de l'infrastructure décrite ici.

3. Restaurer les données. Au choix selon l'incident : restauration à un instant précis depuis la chaîne d'archivage continu si elle est intacte, sinon rechargement du dernier export indépendant. Le schéma se reconstitue au démarrage du service ; le rechargement de l'export est décrit et outillé par le script d'exercice (voir « Exercice du 18 septembre 2026 »).

4. Restaurer les pièces jointes. Recopier les blobs du préfixe dédié du dépôt de sauvegarde vers le stockage objet, sous leur clé d'origine — la clé d'un blob est enregistrée en base, donc restaurée à l'étape précédente.

5. Repointer les noms de domaine. Trois enregistrements, décrits ci-dessous.

Inventaire des variables d'environnement

Les noms et leur rôle, jamais les valeurs. Une variable absente empêche le service de démarrer ou désactive silencieusement la fonction qu'elle gouverne — la colonne « conséquence si absente » est donc la plus utile des trois.

Variable	Rôle	Conséquence si absente
DATABASE_URL	Connexion à la base	Le service ne démarre pas
SESSION_SECRET	Signature des jetons de session	Le service ne démarre pas
APP_URL	Adresse publique, utilisée dans les e-mails	Liens d'e-mail erronés
R2_ACCOUNT_ID, R2_ACCESS_KEY_ID, R2_SECRET_ACCESS_KEY, R2_BUCKET	Stockage objet des pièces jointes	Pièces jointes indisponibles
BACKUP_B2_ENDPOINT, BACKUP_B2_KEY_ID, BACKUP_B2_APPLICATION_KEY, BACKUP_B2_BUCKET_NAME	Dépôt de la copie indépendante	Plus aucune copie indépendante, silencieusement jusqu'à l'alerte de veille
BACKUP_ENCRYPTION_KEY	Second chiffrement de la copie indépendante (32 octets en base64)	Copie indépendante désactivée
BREVO_API_KEY, MAIL_FROM_EMAIL, MAIL_FROM_NAME	E-mails transactionnels	Aucune notification : invitations, signal de vie, alertes
STRIPE_SECRET_KEY, STRIPE_WEBHOOK_SECRET, STRIPE_PRICE_SHIELD_MONTHLY, STRIPE_PRICE_SHIELD_YEARLY	Abonnements	Souscription et renouvellement inopérants
ADMIN_SERVICE_KEY	Routes d'administration serveur à serveur	Routes d'administration inaccessibles
OPS_ALERT_EMAIL	Destinataire des alertes d'exploitation	Repli automatique sur le premier compte administrateur

À retenir sur BACKUP_ENCRYPTION_KEY. Sans elle, les copies indépendantes sont illisibles — y compris pour le responsable. Elle doit être conservée **hors de l'infrastructure qu'elle protège**, et sa perte transforme une sauvegarde en fichier inerte. C'est le seul secret de cette liste dont la perte détruit une ligne de défense entière.

Noms de domaine

Nom	Destination	Rôle
libertyshield.app	Service applicatif	Application et interface publique
docs.libertyshield.app	Service de documentation	Documentation et tutoriels
assets.libertyshield.app	Stockage objet public	Whitepaper, dossier de conformité, ressources

La zone est hébergée chez un opérateur DNS **distinct de l'hébergeur applicatif** : une panne de l'hébergement ne fait pas tomber la zone, et un repointage reste possible depuis un autre poste. Les enregistrements applicatifs sont maintenus à **durée de vie courte** afin qu'un basculement se propage en minutes plutôt qu'en heures.

Le point de défaillance qu'aucune sauvegarde ne couvre

Les deux comptes — celui de l'hébergeur et celui de l'opérateur DNS — commandent l'ensemble. Qui prend l'un des deux fait plus de dégâts qu'aucune panne matérielle : il peut détruire l'infrastructure, ou détourner les noms de domaine vers un serveur qu'il contrôle.

Mesures, et elles n'ont rien de technique :

- **Second facteur matériel** sur les deux comptes, et sur le compte du dépôt Git.
 - **Moyen de récupération indépendant de l'appareil principal** : des codes de secours imprimés, ou une seconde clé physique rangée ailleurs. Un second facteur perdu avec son téléphone devient un sinistre à lui seul.
 - **Verrou de transfert** chez le bureau d'enregistrement du nom de domaine, renouvellement automatique actif, et adresse de contact de renouvellement valide et relevée. Un nom de domaine perdu pour non-renouvellement ne se récupère pas toujours.
-

Rotation et effacement des sauvegardes

Une copie indépendante est déposée par jour, sous une clé d'objet datée. Une **règle de cycle de vie** appliquée au dépôt de sauvegarde masque chaque objet 29 jours après son dépôt et le supprime définitivement le lendemain : la **rétenion effective est de 30 jours**, appliquée par le stockage lui-même et non par le code. Elle est active depuis le 18 septembre 2026.

Conséquence à retenir pour le droit à l'effacement : une donnée supprimée à la demande d'une personne disparaît des systèmes actifs immédiatement, et des sauvegardes **au plus tard au terme de cette période de 30 jours**. C'est la durée réelle de l'effacement complet ; elle est indiquée comme telle à la section « Politique de conservation et d'effacement ».

Continuité du service en cas de disparition de l'éditeur

Le point est traité de front parce qu'un acheteur institutionnel le posera : que deviennent les coffres si l'éditeur cesse son activité ?

- Le **décrypteur hors-ligne** et le **module de chiffrement client** sont publiés en open source sous licence MIT. Ils ne dépendent d'aucun serveur et continueront de fonctionner.
- Le **kit de legs** — coffre chiffré et décrypteur — est téléchargeable par le titulaire et archivable chez lui ou chez son exécuter. C'est la voie prévue lorsque le service n'existe plus.
- Le produit **recommande explicitement** cet archivage dans son tutoriel de transmission, plutôt que de laisser croire à une pérennité qui ne dépendrait pas de l'utilisateur.

Sous-traitants et transferts internationaux

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier. Cette liste est **exhaustive** au jour de la version. Elle est celle publiée dans la politique de confidentialité, version 1.2 du 18 septembre 2026, et communiquée sur demande.

Liste

Sous-traitant	Rôle	Données reçues	Pays de traitement
Railway	Hébergement de l'application et de la base PostgreSQL	L'ensemble des données du service : métadonnées en clair, blocs chiffrés	États-Unis
Cloudflare R2	Stockage objet des pièces jointes	Blobs chiffrés , clés d'objet opaques. Aucune métadonnée de fichier lisible : nom et type MIME sont chiffrés côté client	États-Unis
Brevo — Sendinblue SAS	Envoi des e-mails transactionnels	Adresse e-mail du destinataire, objet, corps du message. Aucun secret, aucun fragment, aucun contenu de coffre	France / Union européenne
Stripe	Encaissement des abonnements	Identité de facturation et données de paiement, collectées et conservées par Stripe seul . L'éditeur ne reçoit que des identifiants techniques et un statut d'abonnement, jamais un numéro de carte	Irlande / États-Unis
Backblaze B2	Copie de sauvegarde indépendante	Export complet de la base, chiffré une seconde fois en AES-256-GCM avant l'envoi, sous une clé conservée hors du système. Illisible par le fournisseur	États-Unis

Aucun autre destinataire. Pas de régie publicitaire, pas d'outil d'analyse d'audience, pas de traceur tiers, pas de plateforme de support intégrée, pas de revente ni de mise à disposition à des tiers à quelque titre que ce soit.

Ce que chaque sous-traitant peut réellement voir

Le tableau ci-dessus dit ce qui est transmis. Voici ce qui en découle, ce qui est le seul point utile à un comité de conformité :

- **Railway** est le seul sous-traitant en position de voir l'ensemble des métadonnées. C'est l'exposition la plus large de la chaîne, et elle est inhérente à toute externalisation d'hébergement. Le contenu des coffres lui reste inaccessible : il est chiffré avant d'arriver.
- **Cloudflare R2, Brevo, Stripe et Backblaze** ne voient chacun qu'un fragment étroit : des blobs chiffrés, des adresses e-mail, des données de facturation, un export doublement chiffré. Aucun d'eux ne peut, seul ou en se rapprochant d'un autre, reconstituer le contenu d'un coffre.

- **Aucun sous-traitant ne détient de clé de déchiffrement des coffres.** Il n'en existe pas hors des appareils des utilisateurs.
-

Transferts hors Union européenne

Les traitements ont lieu aux États-Unis pour l'hébergement, le stockage objet et la sauvegarde indépendante, et en Irlande ou aux États-Unis pour l'encaissement. L'envoi d'e-mails est traité dans l'Union européenne.

Lorsque la réglementation l'exige, ces transferts sont encadrés par des **garanties appropriées** au sens du chapitre V du RGPD : clauses contractuelles types de la Commission européenne dans leur version en vigueur, ou mécanisme équivalent tel que l'adhésion du destinataire à un cadre de protection reconnu.

Élément spécifique à Shield, et qui change la portée réelle du transfert. Les données transférées sont, pour le contenu des coffres, **chiffrées de bout en bout sous des clés que ni l'éditeur ni aucun sous-traitant ne détient**. Un accès par une autorité étrangère au sens de la jurisprudence *Schrems II* ne peut produire, pour ce contenu, que des blocs inexploitable. Le chiffrement n'est pas ici une mesure complémentaire ajoutée après coup pour répondre à une objection : c'est la structure même du produit, antérieure à la question.

Le transfert conserve toutefois une portée réelle sur les **métadonnées**, qui transitent en clair vers l'hébergeur. Elles sont énumérées et justifiées à la section « Gouvernance des métadonnées ».

Gestion des évolutions

Tout ajout ou remplacement de sous-traitant est notifié aux clients professionnels **au moins trente jours à l'avance**, avec droit d'opposition motivée, selon l'article 5 du modèle d'accord de traitement (la section « Accord de traitement des données »). La liste publique et le présent document sont mis à jour à la même date.

Chaque sous-traitant est lié par ses propres engagements contractuels de protection des données, au moins équivalents à ceux souscrits par l'éditeur.

Analyse d'impact relative à la protection des données — décision motivée

LIBERTY Shield — version 1.0, 18 septembre 2026. Entité responsable, coordonnées et statut de représentation : voir le bloc « Identité » de la section 1 du présent dossier.

Question posée

L'article 35 du RGPD impose une analyse d'impact lorsqu'un traitement est **susceptible d'engendrer un risque élevé** pour les droits et libertés des personnes. La question se pose sérieusement ici : Shield conserve, pour le compte de ses utilisateurs, ce qu'ils ont de plus sensible.

Elle mérite donc d'être tranchée par écrit, et non éludée.

Examen au regard des critères de l'article 35.3

Critère	Applicable ?	Motif
Évaluation ou notation systématique, y compris profilage (a)	Non	Aucun profilage, aucun score, aucune évaluation automatisée des personnes.
Décision automatisée produisant des effets juridiques (b)	Partiellement, et encadré	Le déclenchement de la transmission est automatisé et produit un effet réel : la mise à disposition d'un legs. Voir ci-dessous.
Surveillance systématique à grande échelle (c)	Non	Aucune observation des personnes. Les seuls contrôles automatiques portent sur des compteurs du dispositif de transmission, au bénéfice du titulaire lui-même.
Traitement à grande échelle de données sensibles (art. 9) ou d'infractions (d)	Non pour l'éditeur	L'éditeur ne traite aucune donnée de l'article 9. L'utilisateur peut en placer dans son coffre ; elles y sont chiffrées avant tout envoi et demeurent hors de sa portée.
Croisement ou combinaison d'ensembles de données (e)	Non	Aucun croisement, aucun enrichissement, aucune source externe.
Données de personnes vulnérables (f)	Non	Service réservé aux personnes majeures.
Usage innovant ou application de nouvelles technologies (g)	Oui, au sens large	Chiffrement de bout en bout, partage à seuil, transmission post-mortem automatisée.
Empêchement d'exercer un droit ou de bénéficier d'un service (h)	Non	Aucun refus de service fondé sur un traitement automatisé de données personnelles.
Transferts hors Union européenne	Oui	Traité à la section « Sous-traitants et transferts internationaux ».

Décision

Une analyse d'impact complète n'est pas requise au titre de l'article 35 dans la configuration actuelle du produit. Deux critères seulement sont atteints — l'usage innovant et le transfert hors Union — et aucun des critères de masse, de sensibilité, de surveillance ou de profilage.

Cette décision s'appuie sur trois constats de fait :

1. **L'éditeur n'a pas accès au contenu.** Le risque le plus élevé qu'un coffre puisse porter — la divulgation de son contenu — n'est pas un risque que l'éditeur soit en mesure de réaliser, ni volontairement, ni par négligence, ni sous contrainte.
2. **Aucun traitement de masse.** Les métadonnées sont minimisées, énumérées champ par champ dans le registre, et ne font l'objet d'aucune exploitation secondaire.
3. **Aucune décision automatisée sur les personnes** au sens de l'article 22 : aucun refus, aucune restriction, aucune évaluation.

Le point qui a réellement été analysé : le déclenchement automatisé de la transmission

C'est le seul mécanisme du produit qui produise, sans intervention humaine, un effet significatif : au terme d'une procédure, un legs devient téléchargeable par des tiers désignés. Un déclenchement à tort porterait atteinte à la vie privée d'une personne **vivante**.

Il a donc fait l'objet d'une analyse spécifique, dont les mesures suivantes sont en production :

Risque	Mesure en place
Déclenchement par erreur pendant une absence du titulaire	Signal de vie périodique, puis délai de grâce, puis fenêtre de refus — trois délais cumulés, tous réglables par le titulaire, avant toute libération.
Déclenchement malveillant par une seule personne désignée	Fenêtre de refus portée à 30 jours minimum lorsqu'un seul demandeur est à l'origine de la procédure, quelle que soit la valeur configurée.
Titulaire non informé de la procédure en cours	Notification par e-mail nommant les demandeurs et la date d'échéance , pour que le refus soit un geste informé. Le titulaire peut annuler à tout moment, autant de fois que nécessaire, par un simple signal de vie.
Personne désignée à son insu	Chaque personne est informée par e-mail, doit créer un compte et accepter expressément son rôle. Une adresse non vérifiée n'est pas éligible.
Usurpation d'une adresse e-mail de personne désignée	Vérification obligatoire de l'adresse avant toute acceptation de rôle.
Libération d'un legs exploitable par un seul tiers	La libération ne donne qu'un fichier chiffré . Son ouverture exige la réunion d'un seuil de fragments physiques, remis en main propre, que l'éditeur ne détient jamais.
Dispositif devenu inopérant sans que personne ne s'en aperçoive	Surveillance continue du seuil, de la fraîcheur du legs et de la joignabilité des porteurs, avec alerte au seul titulaire tant qu'il est en mesure de corriger.

Conclusion de ce point. Le risque résiduel est jugé faible et, surtout, il est **réversible tant que le titulaire est vivant et joignable** — la fenêtre de refus est précisément conçue pour cela. La mesure la plus protectrice n'est pas technique : c'est le fait que la personne qui pourrait être lésée soit prévenue, nommément et à l'avance.

Réexamen

Cette décision est réexaminée, et une analyse d'impact complète engagée, si l'une des situations suivantes survient :

- ouverture du service à des personnes mineures ;
- traitement par l'éditeur de données relevant de l'article 9, hors contenu chiffré des coffres ;
- introduction d'un profilage, d'une notation ou d'une décision automatisée concernant les personnes ;
- déploiement institutionnel de grande ampleur — banque, assurance, gestion de patrimoine — modifiant l'échelle du traitement ;

- introduction de tout mécanisme de recouvrement détenu par l'éditeur, qui remettrait en cause le constat fondant la présente décision.

Ce dernier point est le plus important du document : **c'est l'absence d'accès de l'éditeur qui fonde la décision**. Si cette propriété disparaissait, l'analyse serait à refaire de zéro.