Mesures de sécurité

Mesures techniques et organisationnelles du service Formia. Situation documentée au 13 novembre 2026.

Accès au service

Les deux adresses publiques, avec et sans www, utilisent HTTPS et un certificat valide. La délégation DNSSEC du domaine a été vérifiée le 13 novembre. La base et les pièces principales sont hébergées en Irlande ; la connexion SSL à la base est exigée dans la configuration relevée. La création d'un compte requiert une adresse e-mail confirmée. Le minimum serveur relevé est de 15 caractères pour le mot de passe ; l'authentification anonyme est désactivée. Le 13 novembre, un compte témoin a suivi un lien reçu dans Gmail, a été confirmé puis s'est connecté sur www.monformia.fr.

Séparation des organismes et accès aux documents

Les contrôles serveur vérifient l'organisme, le rôle et, selon l'action, l'affectation à une session. La base applique des règles d'accès par ligne. Les pièces sont stockées dans un espace privé avec contrôle du type de fichier et une limite de 5 Mio par pièce. Les liens de participation et de partage sont à remettre aux seuls destinataires concernés. En recette hébergée, des organismes fictifs ont servi à vérifier la séparation des dossiers et le refus de 57 fonctions après révocation de l'accès. La recette sur téléphone partagé a distingué deux signataires successifs. Ces observations portent sur les versions et les parcours testés.

Accès d'administration

La double authentification a été constatée sur les comptes d'administration Supabase, Cloudflare et Brevo examinés en novembre 2026. Cloudflare impose la double authentification aux membres du compte contrôlé. Sur Supabase, elle a été constatée pour le propriétaire. Les personnes, accès techniques et moyens de relais doivent être revus à chaque changement d'exploitant.

Ce que gère l'organisme

Nommer un représentant habilité et un contact joignable en cas d'incident. Attribuer les rôles aux personnes qui en ont besoin et retirer les accès au départ d'un intervenant. Vérifier destinataire et pièce avant envoi. Protéger les téléphones partagés et les fichiers exportés ; appliquer les durées propres au financement et aux obligations de l'organisme.

Politique de confidentialité · Annexe de traitement

Sauvegardes, incidents et sortie

Portée des contrôles et conditions d'exploitation à convenir pour l'organisme.

Copies chiffrées et capacité

Une tâche quotidienne prépare les copies, les chiffre puis les dépose dans un espace Cloudflare R2 privé situé en Union européenne. Le préfixe de production prévoit une expiration à 30 jours et un verrou de 7 jours. Les contrôles des 11, 12 et 13 novembre attestent la réussite des copies et la fraîcheur des manifestes.

Capacité testée pour le premier organisme

Le plafond de sauvegarde est de 128 Mio de pièces cumulées, avec 5 Mio par pièce et 1 000 pièces au maximum. Le 13 novembre, un test sur deux bases PostgreSQL locales a restauré 201 PDF fictifs, dont 200 pour un organisme de 20 sessions (100 Mio) et une pièce témoin (5 Mio). Tous ont été rouverts et comparés par empreinte SHA-256. Les échanges avec le stockage distant ont été reproduits localement. Le plafond distant reste de 8 Gio. La couverture contractuelle de GitHub Actions reste à confirmer.

Restitution, effacement et reprise

L'organisme indique dans l'annexe son choix de sortie, le périmètre, le destinataire, le canal et la date. Formia dispose d'une procédure privée de restitution et d'effacement. L'export disponible dans l'application peut nécessiter une restitution complémentaire des pièces ou historiques. Une recette sur données fictives a vérifié qu'après restauration les accès restent fermés pendant le rejeu des suppressions et que les fichiers du second organisme sont conservés. Une reprise complète en production à la volumétrie du client reste à démontrer. Les copies anciennes ou de date incertaine doivent être vérifiées avant réouverture.

Traçabilité et durées

La règle retenue pour les échanges utiles de support est de 12 mois après clôture, et de 6 mois après l'événement pour les traces de sécurité maîtrisées par Formia, sous réserve d'une exception documentée. Les pièces de diagnostic sont à retirer dès résolution. Le tri effectif sur les sources, les tickets et les copies reste à démontrer. La traçabilité disponible varie selon les services et les offres.

Signalement et suivi d'un incident

Écrire à christophe.sanier@gmail.com en indiquant l'organisme, la date et le symptôme. Formia vérifie le périmètre, contient l'incident et, en cas de violation de données confiées, informe l'organisme sans retard injustifié avec les éléments connus et les complète ensuite. L'organisme décide des notifications qui lui incombent. Le contact d'urgence figure page 5 de l'annexe.

Contact et hébergement · RGPD, articles 32 à 34