Dynabudget

Application locale de gestion de budget, dépenses et échéanciers

Rapport d'audit de sécurité et de conformité RGPD

Version de l'application : v65
Date du rapport : 20/11/2026

Ce document décrit les mesures de sécurité mises en œuvre dans l'application et la manière dont les données personnelles y sont traitées. Il ne contient aucune donnée financière ou personnelle.

1. Audit de sécurité

Un audit complet de l'application a été réalisé sur les points suivants : injection dans les pages (XSS), requêtes base de données, falsification de requêtes (CSRF), envois de fichiers, en-têtes HTTP, sessions et contrôle d'accès. Le tableau ci-dessous résume les mesures en place.

Domaine	Mesures en place
Injection XSS	Toutes les données saisies (rubriques, libellés, notes, noms) sont échappées avant affichage. La politique CSP bloque tout script non prévu.
Requêtes SQL	100 % des requêtes utilisent des paramètres liés — aucune valeur saisie n'est concaténée dans le SQL.
CSRF	Cookie de session SameSite=Lax + vérification de l'en-tête Origin/Referer sur toutes les écritures : un site tiers ne peut pas agir à votre place.
Envois de fichiers	Images OCR : taille maxi 15 Mo et signature du format vérifiée. Imports CSV : 5 Mo maxi. Restauration : signature SQLite, contrôle d'intégrité et copie de secours automatique.
En-têtes HTTP	Content-Security-Policy stricte, anti-détournement de cadre (X-Frame-Options), nosniff, Referrer-Policy, HSTS en HTTPS. Appliqués à toutes les réponses.
Sessions	Identifiant de session aléatoire, cookie HttpOnly (illisible par les scripts), Secure dès que le site est en HTTPS, durée 30 jours.
Mots de passe	Hachage PBKDF2 (jamais stockés en clair), 8 caractères minimum, verrouillage temporaire du compte après échecs répétés.
Anti-brute-force	Verrouillage par compte + limitation par adresse IP sur connexion (30/10 min) et demandes publiques (8/h).
Droits admin	Les fonctions d'administration sont refusées côté serveur à tout compte non administrateur — pas seulement masquées dans le menu.
Isolation des données	Chaque compte possède sa propre base SQLite ; une session ne peut lire que sa base. Restauration réservée au titulaire.

2. Conformité RGPD

Données traitées

L'application traite, pour chaque compte :

- l'identifiant de connexion et le nom affiché (obligatoires) ;
- l'adresse e-mail (facultative, uniquement pour la réinitialisation du mot de passe) ;
- le mot de passe sous forme hachée (jamais en clair) ;
- les données budgétaires saisies : rubriques, montants prévus et réels, échéanciers, sources de paiement, patrimoine ;
- les scans de tickets analysés à la demande (archivés, jamais détruits automatiquement).

Finalité et base légale

La seule finalité est la gestion du budget personnel ou familial des utilisateurs du compte. Il s'agit d'un usage domestique (exonération « foyer » du RGPD) ; les bonnes pratiques du règlement sont néanmoins appliquées par principe. Aucune donnée n'est transmise à un tiers, revendue ou utilisée à des fins statistiques ou publicitaires.

Localisation des données

Toutes les données restent sur la machine ou le serveur qui héberge l'application :

- comptes et sessions : data/auth.db ;
- données de chaque utilisateur : data/users/<identifiant>.db ;
- sauvegardes automatiques et scans : sous-dossiers de data/.

Aucun service externe n'est contacté par l'application, hormis le serveur SMTP configuré par l'administrateur pour les

e-mails de réinitialisation.

Cookies et stockage local

L'application dépose un unique cookie :

- budg_session — cookie de session technique, strictement nécessaire à l'authentification (HttpOnly, SameSite=Lax).

Conformément aux lignes directrices de la CNIL, les cookies strictement nécessaires sont exemptés de recueil du consentement : une simple mention d'information est affichée sur l'écran de connexion. Aucun cookie de suivi, de mesure d'audience ou publicitaire n'existe. Le stockage local du navigateur (localStorage) ne conserve que des préférences d'affichage (thème, année consultée, ordre du menu).

Droits des personnes

Chaque utilisateur peut :

- consulter l'intégralité de ses données (pages de l'application et export complet de sa base via « Sauvegarde ») ;
- rectifier toute information saisie (opérations, rubriques, patrimoine) ;
- demander à l'administrateur la suppression de son compte : sa base est alors archivée puis peut être détruite ;
- changer son mot de passe à tout moment, et le réinitialiser par e-mail si une adresse est renseignée.

Sécurité et conservation

- **mots de passe hachés (PBKDF2) et sessions aléatoires ;**
- **bases isolées par compte, sauvegardées automatiquement (30 copies glissantes par profil) ;**
- **les comptes supprimés voient leur base archivée — la destruction définitive relève de l'administrateur ;**
- **aucune durée d'effacement automatique : les données sont conservées tant que le compte existe.**

Bonnes pratiques pour l'administrateur

- **servir l'application en HTTPS (nécessaire pour le cookie Secure, HSTS et l'installation PWA) ;**
- **conserver les dossiers data/ hors de tout partage public ;**
- **restreindre l'accès réseau au cercle voulu (LAN, VPN) ;**
- **supprimer ou archiver les comptes inutilisés.**