A

Aureus Social Pro

Rapport d'audit technique complet

Date : 1er mars 2026

Version : v20.3 — Sprint 37+

Auteur : Aureus IA SPRL

Classification : Confidentiel

URL : https://app.aureussocial.be

SAAS PAIE & SECRETARIAT SOCIAL — BELGIQUE

Table des matières

1. Vue d'ensemble du projet

Aureus Social Pro est un logiciel SaaS de gestion de paie et de secrétariat social pour la Belgique, développé par Aureus IA SPRL. Il couvre le calcul des salaires, les déclarations ONSS (DmfA, Dimona), la fiscalité belge (précompte professionnel, Belcotax), la gestion RH, et la conformité RGPD/SOC2/ISO27001.

106	27	27	23 120
MODULES REACT	ROUTES API	LIBRAIRIES MÉTIER	LIGNES (MONOLITHE)

2.9 MB	362 KB	4	55+
MODULES TOTAUX	LIBRAIRIES	DÉPENDANCES NPM	PROCÉDURES RH

2. Stack technique

COUCHE	TECHNOLOGIE	VERSION	STATUT
Framework	Next.js (App Router)	15.1.0	OK
UI	React + React DOM	19.0.0	OK
Langage	JavaScript pur (pas de TypeScript)	ES2020+	CHOIX
CSS	Inline styles + responsive.css	—	OK
Backend / BDD	Supabase (PostgreSQL + Auth + Realtime)	2.47.0	OK
Auth	Supabase Auth + MFA TOTP	—	OK
Déploiement	Vercel	—	OK
PWA	Service Worker + manifest.json	—	OK
CI/CD	GitHub Actions (test-paie + OWASP ZAP)	—	OK
IA	Anthropic Claude (agent juridique)	—	OK
Email	Resend API	—	CONFIG
Chiffrement	AES-256-GCM + PBKDF2	—	OK

3. Audit des modules (106 fichiers — 2.9 MB)

Modules principaux par catégorie

CATÉGORIE	MODULE	TAILLE	STATUT
Paie	PayrollHub.js	49 KB	ACTIF
	PrimesAvantagesV2.js (56 types de primes)	131 KB	ACTIF
	SimulateurNetBrut.js	7 KB	ACTIF
Déclarations	DeclarationsFiscalV2.js	45 KB	ACTIF
	CommissionsModule.js	47 KB	ACTIF
	BaremesCP.js	54 KB	ACTIF
Absences / Contrats	AbsencesContratsV3.js	60 KB	ACTIF
	AbsencesContratsReportingV2.js	38 KB	ACTIF
Sécurité	SecurityDashboard.js	40 KB	ACTIF
	AccessManagement.js	20 KB	ACTIF
Portails	PortalSystem.js	58 KB	ACTIF
	OnboardingHub.js	32 KB	ACTIF
Juridique / IA	FloatingLegalAgent.js	64 KB	ACTIF
	TransversalCP.js	69 KB	ACTIF
Admin	AutoAdminV3.js (RBAC)	54 KB	ACTIF
Ops	SmartOpsCenter.js	50 KB	ACTIF
Documents	DocumentForms.js (C4, C131, Belcotax)	28 KB	ACTIF
RGPD	GDPRPortal.js + DPODashboard.js	24 KB	ACTIF

Procédures RH (55+ fichiers spécialisés)

PROCÉDURE	FICHIER	STATUT
Premier engagement	ProceduresRH_PremierEngagement.js (56 KB)	COMPLET
Maladie / incapacité	ProceduresRH_Maladie.js	COMPLET
Maternité / paternité	ProceduresRH_Maternite.js	COMPLET
Licenciement / préavis	ProceduresRH_LicenciementPreavis.js	COMPLET
Crédit-temps	ProceduresRH_CreditTemps.js	COMPLET

PROCÉDURE	FICHIER	STATUT
ACTIVA (aide à l'emploi)	ProceduresRH_Activa.js (64 KB)	COMPLET
Flexi-Job	ProceduresRH_FlexiJob.js	COMPLET
Intérimaire	ProceduresRH_Interimaire.js	COMPLET
Art. 60 §7	ProceduresRH_Art60.js	COMPLET
Temps partiel	ProceduresRH_TempsPartiel.js	COMPLET
Congé parental	ProceduresRH_CongeParental.js	COMPLET
Handicap	ProceduresRH_Handicap.js	COMPLET
Étudiant	ProceduresRH_Etudiant.js	COMPLET
Alternance	ProceduresRH_Alternance.js	COMPLET
Fin de carrière	ProceduresRH_CreditTempsFinCarriere.js	COMPLET

4. Librairies métier (27 fichiers — 362 KB)

FICHIER	LIGNES	RÔLE	CRITICITÉ
`calc-paie.js`	1 911	Moteur de calcul brut→net (loi belge)	CRITIQUE
`lois-belges.js`	509	Constantes légales belges 2026	CRITIQUE
`calc-pp.js`	196	Précompte professionnel	CRITIQUE
`xml-generators.js`	452	XML DmfA, Dimona, SEPA, Belcotax	CRITIQUE
`onss-client.js`	510	Client ONSS & déclarations	HAUTE
`crypto.js`	73	AES-256 (NISS, IBAN)	HAUTE
`persistence.js`	81	localStorage + Supabase sync	HAUTE
`csv-parsers.js`	397	Import CSV employés / paie	MOYENNE
`pdf-export.js`	223	Export PDF fiches de paie	MOYENNE
`backup.js`	145	Backup JSON + CSV + auto-backup	MOYENNE
`i18n.js`	368	Internationalisation FR/NL	MOYENNE
`agent-simulateur.js`	352	Agent IA juridique (Claude)	MOYENNE
`module-registry.js`	164	Registre modules + lazy loading	MOYENNE
`api-security.js`	85	Sécurité API (auth, validation)	HAUTE
`failover.js`	116	Failover & résilience	MOYENNE

5. Routes API (27 endpoints)

ROUTE	MÉTHODES	RÔLE	SÉCURITÉ
`/api/v1/payroll`	GET, POST	Calculs de paie	AUTH + RLS
`/api/v1/employees`	GET, POST, PUT	CRUD employés	AUTH + RLS
`/api/v1/declarations`	GET, POST	Déclarations sociales	AUTH + RLS
`/api/v1/docs`	GET, POST	Documents	AUTH + RLS
`/api/onss`	POST	Déclarations ONSS	AUTH
`/api/onss/dimona`	POST	Dimona (entrée/sortie)	AUTH
`/api/onss/status`	GET	Statut ONSS	AUTH
`/api/agent`	POST	Agent IA juridique	AUTH
`/api/send-email`	POST	Envoi emails (Resend)	

ROUTE	MÉTHODES	RÔLE	SÉCURITÉ
			AUTH
`/api/baremes`	GET	Barèmes salariaux	AUTH
`/api/bce`	GET	Banque-Carrefour Entreprises	AUTH
`/api/dms`	GET, POST	Gestion documentaire	AUTH
`/api/esign`	POST	Signature électronique	AUTH
`/api/scan-paie`	POST	OCR fiches de paie	AUTH
`/api/webhooks`	POST	Webhooks entrants	HMAC
`/api/health`	GET	Health check	PUBLIC
`/api/cron`	POST	Tâches planifiées	IP + KEY
`/api/monitoring`	GET	Monitoring applicatif	AUTH

6. Sécurité & conformité

16/16	100%	AES-256	3
CONTRÔLES SÉCURITÉ OK	SCORE SÉCURITÉ	CHIFFREMENT	CERTIFICATIONS VISÉES

Checklist sécurité

- ✅ **HTTPS strict (HSTS)**
  Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
- ✅ **Content Security Policy (CSP)**
  CSP strict avec whitelist Supabase + CDN
- ✅ **Rate limiting**
  60 req/min général, 10 req/min auth endpoints
- ✅ **Brute force protection**
  5 tentatives max → blocage 30 min par IP
- ✅ **MFA / 2FA (TOTP)**
  Authentification multi-facteurs activée
- ✅ **Chiffrement NISS/IBAN**
  AES-256-GCM + PBKDF2 100K itérations
- ✅ **Row Level Security**
  Isolation multi-tenant au niveau PostgreSQL
- ✅ **Audit trail**
  Journal d'activité + timestamp + utilisateur
- ✅ **OWASP ZAP automatisé**
  Scan hebdomadaire + sur chaque PR
- ✅ **Backup automatique**
  Supabase quotidien + backup.js JSON/CSV
- ✅ **IP Whitelist CIDR**
  Middleware + interface admin pour gérer les IP autorisées
- ✅ **Protection SSRF**
  Blocage IP privées + metadata AWS sur webhooks

Conformité réglementaire

NORME	DOCUMENTATION	AVANCEMENT
RGPD (Règlement UE 2016/679)	docs/rgpd/ + GDPRPortal + DPODashboard	90%
ISO 27001	docs/iso27001/ (7 documents)	85%
SOC 2 Type II	docs/soc2/ + docs/compliance/	80%

7. Tests & CI/CD

FICHIER	LIGNES	COUVERTURE	STATUT
`test-paie.js`	726	Moteur de paie (brut→net, ONSS, PP, bonus)	PASS
`test-api-routes.js`	419	27 routes API (auth, CORS, status codes)	PASS
`test-lib-extracts.js`	545	Extraction librairies depuis monolithe	PASS
`extracted-logic.js`	2 263	Logique métier extraite	PASS

Pipelines CI/CD

WORKFLOW	TRIGGER	ACTIONS
`test-paie.yml`	Push/PR sur main	Node 20 → `node tests/test-paie.js`
`owasp-zap.yml`	Push/PR + hebdo lundi 3h	Baseline scan + API scan → rapport HTML

8. Ce qui a été réalisé (session courante)

Session du 1er mars 2026 — Fonctionnalité de sauvegarde manuelle des données

Fichiers modifiés

FICHIER	MODIFICATION	STATUT
`app/lib/backup.js`	**+4 fonctions ajoutées :** • `downloadFile()` — Téléchargement fichier via Blob/URL • `exportEmployeesCSV()` — Export CSV 14 colonnes (nom, NISS, IBAN, brut, CP...) • `exportPayrollCSV()` — Export CSV 9 colonnes (période, brut, ONSS, PP, net...) • `exportAllData()` — Export combiné JSON + CSV employés + CSV paie	FAIT
`app/modules/SecurityDashboard.js`	**Nouvel onglet "Backup données"** ajouté dans la barre d'onglets • 4 boutons d'export (JSON, CSV employés, CSV paie, tout exporter) • Section restauration de backup JSON • Indicateur de backup automatique Supabase	FAIT
`app/modules/SprintComponents.js`	**Section "Sauvegarde manuelle"** ajoutée dans le composant `SecuriteData` • 4 boutons export identiques (JSON, CSV employés, CSV paie, tout) • C'est la page visible via le menu sidebar "Securite Donnees"	FAIT

Commits réalisés

HASH	MESSAGE	FICHIERS
`8d34d34`	feat: ajouter export manuel des données (JSON + CSV employés + CSV paie)	backup.js, SecurityDashboard.js
`6f14e3e`	feat: ajouter boutons export dans la page Securite Donnees	SprintComponents.js

Build & déploiement

✅ **npm run build**
Build production Next.js — SUCCÈS (pas d'erreur)

✅ **git push**
Poussé sur la branche claude/claude-md-mm6l1kr0dfps1nkm-su7i4

9. Ce qu'il reste à faire

Priorité haute (avant mise en production fiduciaire)

#	TÂCHE	DÉTAIL	EFFORT	STATUT
1	**Connexion ONSS réelle**	Intégrer les credentials ONSS (DmfA, Dimona) via le portail socialsecurity.be — actuellement en mode simulation	3-5j	À FAIRE
2	**Connexion Belcotax réelle**	Intégration fiscale SPF Finances pour les fiches 281.10 / 325	2-3j	À FAIRE
3	**Configuration email (Resend)**	Activer l'envoi réel d'emails (fiches de paie, notifications, invitations)	0.5j	CONFIG
4	**Tests end-to-end**	Ajouter des tests Playwright/Cypress pour les parcours critiques (login, calcul paie, déclaration)	3-5j	À FAIRE
5	**DPO désigné**	Nommer un DPO si traitement de >250 travailleurs (obligation RGPD)	—	À VÉRIFIER
6	**Contrats DPA sous-traitants**	Vérifier/signer les Data Processing Agreements avec Vercel et Supabase	—	À VÉRIFIER

Priorité moyenne (amélioration continue)

#	TÂCHE	DÉTAIL	EFFORT	STATUT
7	**Refactoring monolithe**	Découper AureusSocialPro.js (23 120 lignes) selon le plan ARCHITECTURE.js	5-10j	EN COURS
8	**Sauvegarde USB / dossier personnalisé**	Implémenter l'API File System Access pour permettre l'export direct vers clé USB	1j	À FAIRE
9	**Signature électronique avancée**	Intégrer un fournisseur eIDAS (Connective, Itsme) pour les contrats de travail	3-5j	À FAIRE
10	**Import comptable réel**	Tester et valider les connecteurs BOB50, Winbooks, Exact Online	2-3j	À TESTER
11	**Multi-langue NL/DE**	Compléter les traductions néerlandais et allemand (i18n.js en place)	3-5j	PARTIEL
12	**Dashboard analytics avancé**	Graphiques D3/Recharts pour les KPIs paie, absence, coût employeur	2-3j	À FAIRE
13	**App mobile / PWA améliorée**	Optimiser l'expérience offline et les notifications push	2-3j	PARTIEL

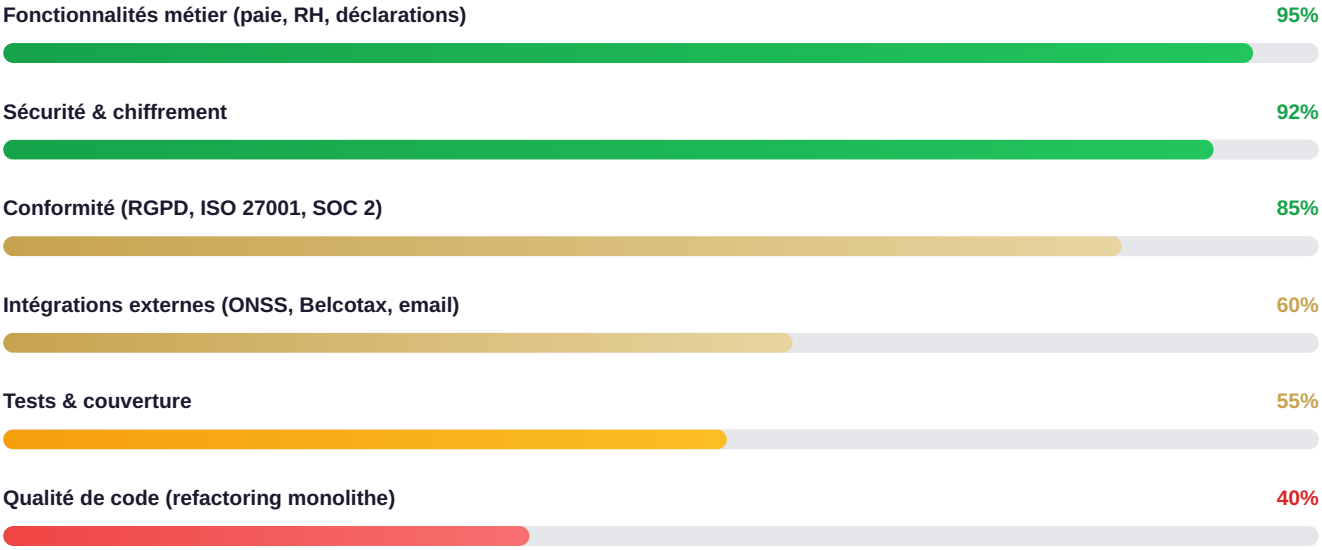
Priorité basse (nice-to-have)

#	TÂCHE	DÉTAIL	EFFORT
14	Migration TypeScript	Ajouter progressivement des types pour sécuriser le code	10-15j
15	Linter / Prettier	Configurer ESLint + Prettier pour la qualité de code	1j
16	Storybook composants	Documenter visuellement les composants UI	3-5j

#	TÂCHE	DÉTAIL	EFFORT
17	API versioning v2	Préparer la v2 de l'API REST avec pagination, filtres avancés	3-5j
18	Multi-région failover	Activer le failover Supabase multi-région (doc 06 prête)	2j

10. Recommandations & priorisation

Avancement global du projet



Points forts

✅ **Architecture minimale & performante**
Seulement 4 dépendances npm — réduction drastique de la surface d'attaque

✅ **Couverture fonctionnelle exceptionnelle**
106 modules couvrant la quasi-totalité des besoins d'un secrétariat social belge

✅ **Sécurité de niveau enterprise**
AES-256, MFA, RLS, IP whitelist, OWASP ZAP, audit trail, HSTS preload

✅ **Conformité réglementaire avancée**
Documentation ISO 27001, SOC 2, RGPD + modules DPO et GDPR Portal intégrés

✅ **55+ procédures RH belges**
Premier engagement, maladie, maternité, licenciement, crédit-temps, flexi-job, ACTIVA, etc.

Points d'attention

1. Monolithe AureusSocialPro.js (23 120 lignes) — Le refactoring est entamé (modules extraits) mais le fichier central reste très volumineux. Risque : maintenance difficile, temps de build.

2. Intégrations ONSS/Belcotax en simulation — Les déclarations XML sont générées mais pas encore envoyées au portail réel. Bloquant pour la mise en production.

3. Tests limités au moteur de paie — Pas de tests E2E ni de tests unitaires pour les modules UI. Risque de régressions lors des mises à jour.

Roadmap recommandée

PHASE	OBJECTIF	DÉLAI ESTIMÉ
Phase 1	Connexion ONSS + Belcotax réels + email Resend + DPA sous-traitants	2 semaines
Phase 2	Tests E2E + sauvegarde USB + dashboard analytics	2 semaines
Phase 3	Refactoring monolithe + multi-langue NL/DE	3-4 semaines
Phase 4	Signature eIDAS + connecteurs comptables + API v2	3-4 semaines

Aureus Social Pro — v20.3

Rapport généré le 1er mars 2026 — Aureus IA SPRL — Confidentiel