Pack Conformite RGPD

Registre des traitements, AIPD et procedures — Aureus IA SPRL (BCE BE 1028.230.781)

1. Designation du DPO (Art. 37-39 RGPD)

Aureus Social Pro traite des donnees a grande echelle de categories speciales (NISS, donnees salariales, donnees de sante). La designation d'un Delegue a la Protection des Donnees est obligatoire conformement a l'Article 37.1.b et c du RGPD.

Contact DPO : dpo@aureussocial.be

Notification APD : https://www.autoriteprotectiondonnees.be/citoyen/agir/notifier-son-dpd

2. Registre des traitements (Art. 30 RGPD)

#	Traitement	Finalite	Base legale	Donnees	Retention
1	Gestion de la paie	Calcul remunerations	Art. 6.1.b+c	Identite, NISS, IBAN, salaire	10 ans
2	Declarations sociales	Obligations ONSS	Art. 6.1.c	NISS, prestations, cotisations	10 ans
3	Declarations fiscales	Obligations SPF	Art. 6.1.c	Identite, revenus, PP	10 ans
4	Registre du personnel	Obligation legale	Art. 6.1.c	Identite, contrat, dates	5 ans apres sortie
5	Portail employe	Acces fiches/conges	Art. 6.1.b	Email, fiches, soldes	Duree contrat + 1 an
6	Medecine du travail	Surveillance sante	Art. 9.2.b	Donnees de sante	40 ans
7	Gestion absences	Suivi maladie/AT	Art. 6.1.b+9.2.b	Certificats, dates	5 ans
8	Logs applicatifs	Securite, audit	Art. 6.1.f	IP, user-agent, timestamps	1 an
9	Backup	Continuite activite	Art. 6.1.f	Toutes donnees	30 jours rolling
10	Marketing	Newsletter, updates	Art. 6.1.a	Email, nom	Retrait consentement

3. Analyse d'Impact (AIPD) — Art. 35 RGPD

Risque	Probabilite	Gravite	Mesure	Risque residuel
Fuite de NISS	Faible	Elevee	Chiffrement AES-256, RLS Supabase	Faible

Risque	Probabilite	Gravite	Mesure	Risque residuel
Acces non autorise	Faible	Elevee	RBAC, 2FA, brute force protection	Faible
Perte de donnees	Tres faible	Elevee	Backup auto 24h, export JSON	Tres faible
Usage detourne	Tres faible	Moyenne	Minimisation, registre Art.30	Tres faible
Sous-traitant non conforme	Faible	Moyenne	DPA signe, hebergement EU	Faible

4. Mesures techniques et organisationnelles (Art. 32)

Mesure	Implementation	Status
Chiffrement en transit	TLS 1.3 (HSTS preload)	OK
Chiffrement au repos	Supabase AES-256	OK
Controle d'acces	RBAC multi-niveaux + RLS	OK
Authentification forte	2FA TOTP disponible	OK
Protection brute force	Rate limiting + block 30min	OK
Audit trail	Actions critiques loggees	OK
Backup	Auto 24h + export JSON	OK
Minimisation	Donnees necessaires uniquement	OK
Pseudonymisation	NISS masque dans les logs	OK
Tests de securite	CSP strict, XSS, CSRF	OK

5. Procedures obligatoires

Exercice des droits (Art. 15-22) : Formulaire accessible via le Portail Employe. Delai de reponse : 30 jours calendrier.

Notification de violation (Art. 33-34) : Delai APD 72 heures max. Notification aux personnes si risque eleve.

Sous-traitance (Art. 28) : DPA signes avec Supabase Inc. (hebergement EU) et Vercel Inc.

Portabilite des donnees (Art. 20) : Export JSON complet disponible en un clic.