

GDPR Conformiteitspakket

Register van verwerkingen, GEB en procedures — Aureus IA SPRL (KBO BE 1028.230.781)

1. Aanstelling DPO (Art. 37-39 AVG)

Aureus Social Pro verwerkt persoonsgegevens op grote schaal van bijzondere categorieën (INSZ, loongegevens, gezondheidsgegevens). De aanstelling van een Functionaris voor Gegevensbescherming is verplicht conform Artikel 37.1.b en c AVG.

Contact DPO: dpo@aureussocial.be

Melding GBA: <https://www.gegevensbeschermingsautoriteit.be>

2. Register van verwerkingen (Art. 30 AVG)

#	Verwerking	Doel	Rechtsgrond	Gegevens	Bewaartermijn
1	Loonbeheer	Berekening verloning	Art. 6.1.b+c	Identiteit, INSZ, IBAN, loon	10 jaar
2	Sociale aangiften	Verplichtingen RSZ	Art. 6.1.c	INSZ, prestaties, bijdragen	10 jaar
3	Fiscale aangiften	Verplichtingen FOD	Art. 6.1.c	Identiteit, inkomsten, BV	10 jaar
4	Personeelsregister	Wettelijke verplichting	Art. 6.1.c	Identiteit, contract, data	5 jaar na uitdiensttreding
5	Werknemersportaal	Toegang loonfiches	Art. 6.1.b	Email, fiches, verlofsaldo	Duur contract + 1 jaar
6	Arbeidsgeneeskunde	Gezondheidstoezicht	Art. 9.2.b	Gezondheidsgegevens	40 jaar
7	Afwezigheidsbeheer	Opvolging ziekte/AO	Art. 6.1.b+9.2.b	Attesten, data	5 jaar
8	Applicatielogs	Beveiliging, audit	Art. 6.1.f	IP, user-agent, timestamps	1 jaar
9	Backup	Bedrijfscontinuïteit	Art. 6.1.f	Alle gegevens	30 dagen rollend
10	Marketing	Nieuwsbrief, updates	Art. 6.1.a	Email, naam	Tot intrekking toestemming

3. Gegevensbeschermingseffectbeoordeling (GEB) — Art. 35 AVG

Risico	Waarschijnlijkheid	Ernst	Maatregel	Restrisico
Lek van INSZ	Laag	Hoog	Versleuteling AES-256, RLS Supabase	Laag
Ongeoorloofde toegang	Laag	Hoog	RBAC, 2FA, brute force bescherming	Laag
Gegevensverlies	Zeer laag	Hoog	Auto backup 24u, JSON-export	Zeer laag
Oneigenlijk gebruik	Zeer laag	Gemiddeld	Minimalisatie, register Art.30	Zeer laag
Niet-conforme onderaannemer	Laag	Gemiddeld	DPA ondertekend, EU-hosting	Laag

4. Technische en organisatorische maatregelen (Art. 32)

Maatregel	Implementatie	Status
Versleuteling in transit	TLS 1.3 (HSTS preload)	OK
Versleuteling in rust	Supabase AES-256	OK
Toegangscontrole	RBAC meerdere niveaus + RLS	OK
Sterke authenticatie	2FA TOTP beschikbaar	OK
Brute force bescherming	Rate limiting + blokkering 30min	OK
Auditspoor	Kritieke acties gelogd	OK
Backup	Auto 24u + JSON-export	OK
Minimalisatie	Enkel noodzakelijke gegevens	OK
Pseudonimisering	INSZ gemaskeerd in logs	OK
Beveiligingstests	CSP strict, XSS, CSRF	OK

5. Verplichte procedures

Uitoefening van rechten (Art. 15-22): Formulier beschikbaar via het Werknemersportaal. Antwoordtermijn: 30 kalenderdagen.

Melding van inbreuken (Art. 33-34): Termijn GBA maximaal 72 uur. Melding aan betrokkenen bij hoog risico.

Onderaanneming (Art. 28): DPA ondertekend met Supabase Inc. (EU-hosting) en Vercel Inc.

Gegevensoverdraagbaarheid (Art. 20): Volledige JSON-export beschikbaar met een klik.