GDPR Compliance Pack

Records of Processing, DPIA and Procedures — Aureus IA SPRL (BCE BE 1028.230.781)

1. DPO Designation (Art. 37-39 GDPR)

Aureus Social Pro processes personal data on a large scale including special categories (NISS/SSN, salary data, health data). The designation of a Data Protection Officer is mandatory under Article 37.1.b and c GDPR.

DPO Contact: dpo@aureussocial.be

Belgian DPA notification: https://www.autoriteprotectiondonnees.be

2. Records of Processing Activities (Art. 30 GDPR)

#	Processing	Purpose	Legal Basis	Data Categories	Retention
1	Payroll Management	Salary calculation	Art. 6.1.b+c	Identity, NISS, IBAN, salary	10 years
2	Social Declarations	NSSO obligations	Art. 6.1.c	NISS, services, contributions	10 years
3	Tax Declarations	Tax authority obligations	Art. 6.1.c	Identity, income, withholding	10 years
4	Staff Register	Legal obligation	Art. 6.1.c	Identity, contract, dates	5 years after exit
5	Employee Portal	Payslip/leave access	Art. 6.1.b	Email, payslips, leave balance	Contract + 1 year
6	Occupational Health	Health surveillance	Art. 9.2.b	Health data	40 years
7	Absence Management	Sick/accident tracking	Art. 6.1.b+9.2.b	Certificates, dates	5 years
8	Application Logs	Security, audit	Art. 6.1.f	IP, user-agent, timestamps	1 year
9	Backup	Business continuity	Art. 6.1.f	All data	30 days rolling
10	Marketing	Newsletter, updates	Art. 6.1.a	Email, name	Until consent withdrawal

3. Data Protection Impact Assessment (DPIA) — Art. 35 GDPR

Risk	Likelihood	Severity	Mitigation	Residual Risk
NISS Data Breach	Low	High	AES-256 encryption, Supabase RLS	Low

Risk	Likelihood	Severity	Mitigation	Residual Risk
Unauthorized Access	Low	High	RBAC, 2FA, brute force protection	Low
Data Loss	Very Low	High	Auto backup 24h, JSON export	Very Low
Misuse of Data	Very Low	Medium	Data minimization, Art.30 register	Very Low
Non-compliant Processor	Low	Medium	Signed DPA, EU hosting	Low

4. Technical and Organizational Measures (Art. 32)

Measure	Implementation	Status
Encryption in Transit	TLS 1.3 (HSTS preload)	OK
Encryption at Rest	Supabase AES-256	OK
Access Control	Multi-level RBAC + RLS	OK
Strong Authentication	2FA TOTP available	OK
Brute Force Protection	Rate limiting + 30min block	OK
Audit Trail	All critical actions logged	OK
Backup	Auto 24h + JSON export	OK
Data Minimization	Only necessary data collected	OK
Pseudonymization	NISS masked in logs	OK
Security Testing	Strict CSP, XSS, CSRF	OK

5. Mandatory Procedures

Exercise of Rights (Art. 15-22): Form accessible via the Employee Portal. Response deadline: 30 calendar days.

Breach Notification (Art. 33-34): DPA deadline 72 hours max. Notify data subjects if high risk.

Sub-processing (Art. 28): DPA signed with Supabase Inc. (EU hosting) and Vercel Inc.

Data Portability (Art. 20): Full JSON export available in one click.