DSGVO-Konformitatspaket

Verzeichnis der Verarbeitungstatigkeiten, DSFA und Verfahren — Aureus IA SPRL (ZBE BE 1028.230.781)

1. Benennung des DSB (Art. 37-39 DSGVO)

Aureus Social Pro verarbeitet personenbezogene Daten in grossem Umfang, einschliesslich besonderer Kategorien (INSZ, Gehaltsdaten, Gesundheitsdaten). Die Benennung eines Datenschutzbeauftragten ist gemaess Art. 37.1.b und c DSGVO verpflichtend.

Kontakt DSB: dpo@aureussocial.be

Belgische Datenschutzbehorde: https://www.autoriteprotectiondonnees.be

2. Verzeichnis der Verarbeitungstatigkeiten (Art. 30 DSGVO)

#	Verarbeitung	Zweck	Rechtsgrundlage	Datenkategorien	Aufbewahrung
1	Lohnverwaltung	Gehaltsberechnung	Art. 6.1.b+c	Identitat, INSZ, IBAN, Gehalt	10 Jahre
2	Sozialmeldungen	LSS-Verpflichtungen	Art. 6.1.c	INSZ, Leistungen, Beitrage	10 Jahre
3	Steuererklarungen	FOD-Verpflichtungen	Art. 6.1.c	Identitat, Einkommen, QS	10 Jahre
4	Personalregister	Gesetzliche Pflicht	Art. 6.1.c	Identitat, Vertrag, Daten	5 Jahre nach Austritt
5	Mitarbeiterportal	Zugang Gehaltszettel	Art. 6.1.b	Email, Gehaltszettel, Urlaub	Vertragsdauer + 1 Jahr
6	Arbeitsmedizin	Gesundheitsuberwachung	Art. 9.2.b	Gesundheitsdaten	40 Jahre
7	Abwesenheitsverwaltung	Krankheit/Unfall	Art. 6.1.b+9.2.b	Bescheinigungen, Daten	5 Jahre
8	Anwendungsprotokolle	Sicherheit, Audit	Art. 6.1.f	IP, User-Agent, Zeitstempel	1 Jahr
9	Backup	Geschaftskontinuitat	Art. 6.1.f	Alle Daten	30 Tage rollierend
10	Marketing	Newsletter, Updates	Art. 6.1.a	Email, Name	Bis Widerruf

3. Datenschutz-Folgenabschatzung (DSFA) — Art. 35 DSGVO

Risiko	Wahrscheinlichkeit	Schwere	Massnahme	Restrisiko
INSZ-Datenleck	Gering	Hoch	AES-256, Supabase RLS	Gering
Unbefugter Zugriff	Gering	Hoch	RBAC, 2FA, Brute-Force-Schutz	Gering
Datenverlust	Sehr gering	Hoch	Auto-Backup 24h, JSON-Export	Sehr gering
Missbrauch	Sehr gering	Mittel	Datenminimierung, Register Art.30	Sehr gering
Nicht-konformer Auftragnehmer	Gering	Mittel	DPA unterzeichnet, EU-Hosting	Gering

4. Technische und organisatorische Massnahmen (Art. 32)

Massnahme	Implementierung	Status
Verschlusselung im Transit	TLS 1.3 (HSTS preload)	OK
Verschlusselung im Ruhezustand	Supabase AES-256	OK
Zugriffskontrolle	Mehrstufige RBAC + RLS	OK
Starke Authentifizierung	2FA TOTP verfugbar	OK
Brute-Force-Schutz	Rate Limiting + 30min Sperre	OK
Audit-Trail	Alle kritischen Aktionen protokolliert	OK
Backup	Auto 24h + JSON-Export	OK
Datenminimierung	Nur notwendige Daten	OK
Pseudonymisierung	INSZ in Logs maskiert	OK
Sicherheitstests	CSP strict, XSS, CSRF	OK

5. Pflichtverfahren

Ausubung der Rechte (Art. 15-22): Formular uber das Mitarbeiterportal zuganglich. Antwortfrist: 30 Kalendertage.

Meldung von Verletzungen (Art. 33-34): Frist Datenschutzbehorde maximal 72 Stunden. Benachrichtigung der Betroffenen bei hohem Risiko.

Unterauftragsverarbeitung (Art. 28): DPA unterzeichnet mit Supabase Inc. (EU-Hosting) und Vercel Inc.

Datenubertragbarkeit (Art. 20): Vollstandiger JSON-Export mit einem Klick verfugbar.