Security & Data Protection Whitepaper

GloPros Platform BV

Version 1.0 | March 2026 | Public Transparency Statement

Executive Summary

At GloPros Platform BV, security is not an afterthought; it is foundational to how we operate. As an AI-powered recruitment platform, we handle some of the most sensitive professional and personal data in the market: candidate profiles, hiring decisions, client workforce strategies, and employment records. The trust our clients and candidates place in us demands nothing less than the highest standards of information security.

This whitepaper describes GloPros's security posture, governance framework, and ongoing commitments to protecting data for the benefit of our enterprise clients, prospective partners, and the candidates we serve.

1. About GloPros

GloPros Platform BV is an Amsterdam-based AI recruitment platform specialising in sourcing and placing technology talent across the globe. Our platform leverages artificial intelligence to match candidates with enterprise clients quickly, precisely, and with integrity.

As a technology-forward firm operating at the intersection of AI and human capital, GloPros recognises that data security and client confidentiality are core differentiators - not merely compliance obligations.

2. Our Security Governance Framework

2.1 ISO/IEC 27001:2022 Certification

GloPros maintains an **ISO/IEC 27001:2022 certified Information Security Management System (ISMS),** the internationally recognised standard for information security management. Our certification demonstrates independent third-party validation of our security practices and commitment to continuous improvement. This framework governs how we identify, assess, treat, and monitor information security risks across our organisation.

Certification Details:

- Certification Body: **INCERCERT**
- Certificate Number: **IC-IS-2411180**
- Certification Date: **November 20, 2024**
- Next Surveillance Audit: **November 19, 2026**
- Certificate available upon request for prospective clients

Our ISMS covers:

- **Organisational security controls** - policies, roles, responsibilities, and supplier management
- **People security controls** - background screening, security awareness training, and acceptable use
- **Physical & environmental controls** - secure office facilities and device management
- **Technological controls** - access control, encryption, vulnerability management, and secure development

ISO 27001:2022 introduced a significantly modernised control set (Annex A, 93 controls across 4 domains), and GloPros has implemented and maintains certification against this updated structure as the baseline for our control implementation. Our ISMS undergoes regular internal audits, management reviews, and external surveillance audits to ensure ongoing compliance and continuous improvement.

2.2 Security Leadership & Accountability

GloPros has designated an **Information Security function** responsible for:

- Maintaining and continuously improving the ISMS
- Conducting periodic internal audits and management reviews
- Managing security incidents and coordinating responses
- Ensuring vendor and third-party security compliance

Security governance is reviewed quarterly by senior management, ensuring that information security remains a board-level priority.

3. Data Classification & Handling

GloPros classifies all data it processes into four tiers:

Classification	Description	Examples
Public	Freely shareable	Marketing content, job postings
Internal	For GloPros staff only	Internal policies, process docs

Confidential	Restricted; need-to-know	Client contracts, hiring briefs
Restricted	Highest sensitivity; strictly controlled	Candidate PII, salary data, assessment results

All **Restricted** and **Confidential** data is subject to encryption at rest and in transit, strict access controls, and formal data retention and disposal policies.

4. Candidate & Client Data Protection

4.1 Data Minimisation

We collect only the data necessary to deliver our recruitment services. Candidate information is never repurposed for unrelated activities, and data is retained only as long as required by legal obligation or legitimate business need.

4.2 Encryption

- All candidate and client data is encrypted **in transit** using TLS 1.3 as standard (with TLS 1.2 fallback for compatibility).
- Sensitive data is encrypted at rest using industry-standard algorithms.

4.3 Access Control

Access to personal and confidential data follows the principle of **least privilege** - users are granted only the access necessary for their role. Access rights are reviewed regularly, and all privileged access is subject to additional controls and logging.

4.4 Third-Party & Supplier Security

GloPros evaluates all third-party vendors and technology partners against our security requirements prior to engagement. Contracts with suppliers who process personal data include appropriate security and confidentiality obligations, consistent with **ISO 27001:2022** Annex A control requirements for supplier relationships.

4.5 Profile Anonymization & Privacy by Design

GloPros implements a three-tier profile anonymization system as a core privacy protection mechanism. Every professional profile on the platform exists in three variants (Full Profile, Semi-anonymized Profile, and Strongly-anonymized Profile), each revealing progressively less personally identifiable information. The system dynamically determines which variant to display based on user permissions, candidate preferences, and context, ensuring that sensitive data is exposed only when necessary and authorized. This privacy-by-design approach serves multiple purposes: it protects candidate confidentiality, reduces unconscious bias in initial screening, supports GDPR data minimisation principles, and enables privacy-sensitive searches for confidential recruiting scenarios. The anonymization

system operates transparently to users while providing robust technical controls over personal data visibility.

5. Data Privacy & GDPR Compliance

GloPros Platform BV is registered in the Netherlands and operates under the European Union's General Data Protection Regulation (GDPR). We are committed to the highest standards of data privacy and transparency in how we process personal data of candidates and client representatives.

6. AI Security & Machine Learning Governance

6.1 Our AI-Powered Platform

Artificial intelligence is fundamental to the GloPros platform — not a supplementary feature, but the core technology enabling our unique value proposition. Our AI systems power intelligent candidate-vacancy matching through advanced embedding models, automate resume and job description parsing, and drive the proactive recommendations that differentiate GloPros from traditional recruitment platforms. Because AI is central to our service delivery and processes sensitive professional and personal data, we treat AI security and governance as a critical security domain requiring specialised controls. This section describes how GloPros secures its AI integrations and services, protects the sensitive data processed by AI systems, ensures transparency and auditability of AI-driven decisions, and actively mitigates risks, including third-party AI service dependencies, algorithmic bias, privacy leakage through AI inference, and prompt injection vulnerabilities in AI-powered features.

6.2 AI Processing and Data Protection

We utilise leading third-party AI services, specifically including models from OpenAI and AWS Bedrock. Our data protection protocols ensure that all information processed by these models is handled with strict confidentiality. A critical security control is our contractual agreement that client and candidate data is kept completely private and not used for training newer models by our third-party providers. We ensure AI service integration security by enforcing data encryption in transit and at rest, and applying strict access controls consistent with the principle of least privilege (section 4.3) across all AI interactions.

6.3 Transparency, Auditability, and Fairness

GloPros upholds high standards for AI decision transparency and auditability. Any output generated or assisted by AI within the platform is clearly marked with a transparency notice, indicating that the result was generated by AI. We advise users that the results may vary and that they should verify any AI-generated information before making critical decisions. For compliance and governance, we maintain comprehensive logging and audit trails of AI-driven decisions, allowing for detailed, post-hoc review and explanation of outcomes. Furthermore, we commit to mitigating bias and ensuring fairness through continuous

monitoring of our algorithms for potential bias. Our Profile Anonymization & Privacy by Design system (section 4.5) is a foundational privacy control that also serves to reduce unconscious bias during initial screening processes.

5. Cloud & Infrastructure Security

GloPros's technology infrastructure is hosted on **Amazon Web Services (AWS)**, leveraging AWS's globally recognised security controls and certifications (including ISO 27001, SOC 2, and PCI DSS compliance at the cloud layer).

Our infrastructure security practices include:

- **Network segmentation** - production environments are isolated from development and test environments
- **Role-based access control (RBAC)** - enforced at both application and infrastructure layers
- **Container security** - workloads running on Amazon EKS follow Kubernetes security best practices, including runtime security monitoring and image vulnerability scanning
- **Infrastructure as Code (IaC)** - all infrastructure changes are version-controlled and subject to security review before deployment
- **Audit logging** - comprehensive logs are maintained for all access to sensitive systems and reviewed for anomalous activity

6. Vulnerability & Patch Management

GloPros operates a formal vulnerability management programme:

- Systems are scanned regularly for known vulnerabilities using industry-recognised tooling.
- Critical and high-severity vulnerabilities are remediated within defined SLA windows.
- Application dependencies are monitored for newly disclosed CVEs.
- Security patches are applied through a controlled change management process to minimise operational risk while maintaining a strong security posture.

7. Security Awareness & Training

Every GloPros employee undergoes security awareness training upon joining and at regular intervals thereafter. Training covers:

- Phishing and social engineering awareness
- Data handling and classification responsibilities
- Incident reporting procedures
- Acceptable use of company systems and data

Personnel with elevated access privileges receive role-specific security training aligned to their responsibilities.

---

8. Incident Management & Business Continuity

8.1 Incident Response

GloPros maintains a documented **Security Incident Response Plan** that defines how potential security events are detected, reported, triaged, and resolved. Our incident response process ensures that affected clients and relevant authorities are notified promptly and transparently in the event of a confirmed incident.

8.2 Business Continuity

Critical systems and data are backed up regularly, and recovery procedures are tested periodically to ensure service continuity in the event of a disruption. GloPros maintains a **Business Continuity Plan (BCP)** aligned with the operational risk profile of our services.

9. Our Commitment to Continuous Improvement

ISO 27001:2022 is built on the **Plan–Do–Check–Act (PDCA)** cycle of continuous improvement. GloPros embraces this philosophy - security is not a one-time project but an ongoing discipline.

We commit to:

- Conducting formal **risk assessments** at least annually and whenever significant changes occur
- Performing regular **internal audits** of ISMS controls
- Reviewing security objectives at **management review** meetings
- Tracking and closing **corrective actions** arising from audits, incidents, and risk treatments
- Staying current with the evolving threat landscape relevant to AI-powered recruitment platforms

10. Contact & Transparency

GloPros believes that transparency builds trust. If you are a client, candidate, or partner with questions about our security practices or data handling, we welcome the conversation.

Security enquiries: security@glopros.com **General contact:** www.glopros.com **Registered office:** GloPros Platform BV, Prinsengracht 769, Amsterdam, The Netherlands

---

This whitepaper is published as a public transparency statement and is reviewed annually. Last reviewed: March 2026.

GloPros Platform BV - Connecting AI Talent with Purpose, Securely.