EU GDPR DATA PROTECTION IMPACT ASSESSMENT

DeepShield Systems, Inc.

Assessment Date: January 11, 2024

Document Reference: DPIA-2024-001

1. EXECUTIVE SUMMARY

This Data Protection Impact Assessment ("DPIA") has been conducted in accordance with Article 35 of the General Data Protection Regulation (EU) 2016/679 ("GDPR") to evaluate the data protection implications of DeepShield Systems' Industrial Control System (ICS) Security Platform and associated services.

2. PROCESSING ACTIVITIES OVERVIEW

1. The primary processing activities assessed include:

- Collection and analysis of industrial network traffic data
- Processing of user authentication credentials
- Monitoring of operational technology (OT) system behaviors
- Storage of incident response and threat detection logs
- Processing of customer organization personnel data

2. Data Categories Processed:

- Network telemetry data
- System log data
- User authentication credentials
- Industrial process parameters
- Employee contact information
- Security incident reports

3. NECESSITY AND PROPORTIONALITY ASSESSMENT

1. Legal Basis for Processing:

- Article 6(1)(b) GDPR: Performance of Contract
- Article 6(1)(f) GDPR: Legitimate Interests

- Article 9(2)(g) GDPR: Substantial Public Interest (Critical Infrastructure Protection)

2. Data Minimization Measures:

- Automated data retention policies
- Purpose-specific data collection
- Regular data purging protocols
- Pseudonymization of personal data where feasible

4. RISK ASSESSMENT

1. Identified Risks:

Risk Category	Likelihood	Impact	Mitigation Measures
Unauthorized Access	Medium	High	Multi-factor authentication, encryption
Data Breach	Low	High	Network segmentation, access controls
Cross-border Transfer	Medium	Medium	SCCs, technical safeguards
Function Creep	Low	Medium	Regular audit, access reviews

2. Technical Security Measures:

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Role-based access control (RBAC)
- Regular penetration testing
- Automated threat detection
- Secure development lifecycle

5. DATA SUBJECT RIGHTS

1. Mechanisms in place to ensure:

- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing

- Right to data portability
- Right to object

2. Response Procedures:

- Dedicated data protection team
- 72-hour breach notification process
- Subject access request handling
- Regular staff training

6. INTERNATIONAL TRANSFERS

1. Transfer Mechanisms:

- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules
- EU-US Data Privacy Framework compliance

2. Geographic Data Storage:

- Primary: EU (Ireland)
- Backup: EU (Germany)
- Disaster Recovery: EU (Netherlands)

7. CONSULTATION

1. Internal Stakeholders Consulted:

- Chief Security Architect
- Data Protection Officer
- Legal Department
- IT Security Team
- Operations Management

2. External Consultation:

- EU Data Protection Authority (where required)
- External Data Protection Counsel
- Customer Data Protection Officers

8. RECOMMENDATIONS AND ACTIONS

1. Required Actions:

- Implementation of additional encryption for OT data
- Enhancement of audit logging capabilities
- Regular review of access controls
- Updated privacy notices

2. Timeline for Implementation:

- Q1 2024: Technical measures
- Q2 2024: Procedural updates
- Q3 2024: Training and awareness
- Q4 2024: Review and assessment

9. APPROVAL AND REVIEW

This DPIA has been reviewed and approved by:

Data Protection Officer:

Name: Dr. Maria Schmidt

Date: January 11, 2024

Signature: _

Chief Security Architect:

Name: Dr. Elena Rodriguez

Date: January 11, 2024

Signature: _

Chief Technology Officer:

Name: Sarah Blackwood

Date: January 11, 2024

Signature: _

10. REVIEW SCHEDULE

This DPIA shall be reviewed:

- Annually as part of regular compliance review
- Upon significant changes to processing activities
- Following major security incidents
- Upon material changes to applicable regulations

Next scheduled review date: January 11, 2025
