DATA PROCESSING AGREEMENT 1

Effective Date: November 14, 2025
Document Type: Data Processing Agreement
Version: 1.0
Status: Sample Document for Compliance Testing

DISCLAIMER: *This is a sample contract generated for compliance testing purposes only. It should not be used as an actual legal agreement without proper legal review and customization for your specific requirements.*

COMPREHENSIVE DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into as of November 13, 2025, between DataSecure Technologies Ltd. ("Processor") and Enterprise Solutions International Inc. ("Controller").

RECITALS

WHEREAS, the Controller is subject to the General Data Protection Regulation (EU) 2016/679 ("GDPR"); WHEREAS, the Processor provides cloud-based enterprise management services to the Controller; WHEREAS, the parties wish to ensure compliance with all applicable data protection laws;

NOW, THEREFORE, the parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 "Personal Data" means any information relating to an identified or identifiable natural person as defined in GDPR Article 4(1).

1.2 "Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, as defined in GDPR Article 4(2).

1.3 "Data Subject" means the identified or identifiable natural person to whom Personal Data relates.

1.4 "Special Categories of Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation as defined in GDPR Article 9(1).

1.5 "Supervisory Authority" means an independent public authority established by an EU Member State pursuant to GDPR Article 51.

1.6 "Data Protection Officer" or "DPO" means the designated individual responsible for data protection compliance as required by GDPR Articles 37-39.

2. SCOPE, NATURE, AND PURPOSE OF PROCESSING

2.1 This DPA applies to all Processing activities carried out by the Processor on behalf of the Controller in connection with the provision of enterprise management services as detailed in Schedule A.

2.2 The nature of Processing includes collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, and erasure of Personal Data.

2.3 The purpose of Processing is to enable the Controller to manage employee records, customer relationships, and business operations in compliance with GDPR Articles 5 and 6.

2.4 The duration of Processing shall be for the term of the Master Services Agreement, with data retention as specified in Section 14.

2.5 The categories of Data Subjects include: employees, customers, suppliers, contractors, and website visitors.

2.6 The types of Personal Data processed include: identification data, contact information, employment records, financial data, and technical access logs. Special Categories of Personal Data as defined in GDPR Article 9 are processed only with explicit consent or legal basis as specified in Article 9(2).

3. PRINCIPLES RELATING TO PROCESSING (GDPR ARTICLE 5)

3.1 The Processor shall process Personal Data in accordance with the principles set forth in GDPR Article 5(1):

(a) Lawfulness, fairness and transparency: All Processing shall be lawful, fair, and transparent to the Data Subject;

(b) Purpose limitation: Personal Data shall be collected only for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes;

(c) Data minimization: Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;

(d) Accuracy: Personal Data shall be accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure that inaccurate data are erased or rectified without delay;

(e) Storage limitation: Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than necessary for the purposes for which the data are processed;

(f) Integrity and confidentiality: Personal Data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

3.2 The Processor shall be able to demonstrate compliance with these principles in accordance with GDPR Article 5(2).

4. LAWFULNESS OF PROCESSING (GDPR ARTICLE 6)

4.1 The Controller has determined that the lawful basis for Processing under GDPR Article 6(1) is:

(a) Performance of a contract to which the Data Subject is party (Article 6(1)(b));

(b) Compliance with legal obligations (Article 6(1)(c));

(c) Legitimate interests pursued by the Controller (Article 6(1)(f)), where applicable and subject to balancing test.

4.2 The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to third countries or international organizations, unless required to do so by Union or Member State law (GDPR Article 28(3)(a)).

4.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

5. CONSENT MANAGEMENT (GDPR ARTICLE 7)

5.1 Where Processing is based on consent pursuant to GDPR Article 6(1)(a), the Controller shall be responsible for obtaining valid consent from Data Subjects.

5.2 The Processor shall provide technical and organizational measures to assist the Controller in obtaining, recording, and managing consent, including:

(a) Clear and distinguishable consent mechanisms that are separate from other matters;

(b) Written records of when and how consent was obtained;

(c) The ability for Data Subjects to withdraw consent as easily as it was given;

(d) Systems to demonstrate that consent was obtained in compliance with GDPR Article 7(1).

5.3 For children under the age of 16, consent shall be obtained in compliance with GDPR Article 8, with parental responsibility verified where required by applicable Member State law.

6. SPECIAL CATEGORIES OF PERSONAL DATA (GDPR ARTICLE 9)

6.1 The Processing of Special Categories of Personal Data is prohibited unless one of the conditions in GDPR Article 9(2) applies.

6.2 Where the Controller has determined that Special Categories of Personal Data must be processed, the Processor shall implement additional safeguards including:

(a) Enhanced encryption (AES-256 minimum);

(b) Strict access controls limited to specifically authorized personnel;

(c) Comprehensive audit logging of all access and modifications;

(d) Regular review and certification of compliance measures.

6.3 The specific Special Categories of Personal Data being processed and the applicable legal basis under Article 9(2) are documented in Schedule B.

7. TRANSPARENCY OBLIGATIONS (GDPR ARTICLES 12, 13, 14)

7.1 The Controller is responsible for providing information to Data Subjects in accordance with GDPR Articles 12, 13, and 14.

7.2 The Processor shall provide reasonable assistance to the Controller in fulfilling its transparency obligations, including:

(a) Providing information about the Processor's identity and contact details;

(b) Describing the nature, purpose, and legal basis of Processing;

(c) Disclosing retention periods and criteria used to determine retention;

(d) Identifying recipients or categories of recipients of Personal Data;

(e) Providing information about international data transfers and safeguards.

7.3 All information shall be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, especially for information directed at children (GDPR Article 12(1)).

8. DATA SUBJECT RIGHTS (GDPR ARTICLES 15-22)

8.1 The Processor shall assist the Controller in responding to requests from Data Subjects exercising their rights under GDPR Chapter III, including:

(a) Right of access (Article 15): Providing confirmation of Processing and access to Personal Data;

(b) Right to rectification (Article 16): Correcting inaccurate Personal Data without undue delay;

(c) Right to erasure / "right to be forgotten" (Article 17): Deleting Personal Data when required by law;

(d) Right to restriction of processing (Article 18): Limiting Processing under specified circumstances;

(e) Right to data portability (Article 20): Providing Personal Data in a structured, commonly used, and machine-readable format;

(f) Right to object (Article 21): Ceasing Processing when Data Subject objects on grounds relating to their particular situation;

(g) Rights related to automated decision-making and profiling (Article 22): Ensuring human intervention in automated decisions with legal or similarly significant effects.

8.2 The Processor shall notify the Controller within 24 hours of receiving any request from a Data Subject exercising their rights.

8.3 The Processor shall provide all necessary assistance to enable the Controller to respond to Data Subject requests within the statutory timeframe of one month (extendable by two months for complex requests) as required by GDPR Article 12(3).

8.4 The Processor shall implement technical measures to facilitate Data Subject rights, including:

- Automated data export capabilities for portability requests; - Secure deletion protocols for erasure requests; - Access control systems for restriction requests; - Audit trails documenting all Data Subject right requests and responses.

9. PROCESSOR OBLIGATIONS (GDPR ARTICLE 28)

9.1 The Processor shall process Personal Data only on documented written instructions from the Controller, as set forth in this DPA and Schedule A.

9.2 The Processor shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (GDPR Article 28(3)(b)).

9.3 The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk in accordance with GDPR Article 32 (detailed in Section 10).

9.4 The Processor shall respect the conditions for engaging another processor as set forth in Section 11 and GDPR Article 28(2) and (4).

9.5 The Processor shall assist the Controller in ensuring compliance with obligations under GDPR Articles 32-36 concerning security, breach notification, data protection impact assessments, and prior consultation.

9.6 The Processor shall delete or return all Personal Data to the Controller after the end of the provision of services, and delete existing copies unless retention is required by Union or Member State law (GDPR Article 28(3)(g)).

9.7 The Processor shall make available to the Controller all information necessary to demonstrate compliance with this Article 28 and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

9.8 The Processor shall designate a Data Protection Officer where required by GDPR Article 37 and provide the Controller with the contact details of the DPO.

10. SECURITY OF PROCESSING (GDPR ARTICLE 32)

10.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate:

(a) Pseudonymization and encryption of Personal Data using industry-standard algorithms (AES-256 for data at rest, TLS 1.3 for data in transit);

(b) The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services through:

- Multi-factor authentication (MFA) for all system access; - Role-based access control (RBAC) with least privilege principle; - Network segmentation and micro-segmentation; - Intrusion detection and prevention systems (IDS/IPS); - Security Information and Event Management (SIEM) with 24/7 monitoring;

(c) The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident through:

- Automated daily backups with geo-redundant storage; - Recovery Time Objective (RTO) of 4 hours; - Recovery Point Objective (RPO) of 1 hour; - Quarterly disaster recovery testing;

(d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures through:

- Annual penetration testing by certified third parties; - Quarterly vulnerability assessments; - Monthly security patch management; - Continuous security monitoring and threat intelligence integration; - Annual ISO 27001 and SOC 2 Type II audits.

10.2 In assessing the appropriate level of security, account shall be taken of the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

10.3 The Processor shall implement measures to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process them except on instructions from the Controller.

10.4 Physical security measures include:

- SOC 2 Type II certified data centers; - Biometric access controls and mantrap entry systems; - 24/7 on-site security personnel; - Video surveillance with 180-day retention; - Environmental controls for fire suppression, temperature, and humidity.

11. SUB-PROCESSORS (GDPR ARTICLE 28)

11.1 The Controller provides general written authorization for the Processor to engage sub-processors in accordance with GDPR Article 28(2).

11.2 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors at least 45 days in advance, thereby giving the Controller the opportunity to object to such changes.

11.3 Where the Processor engages a sub-processor, the same data protection obligations as set out in this DPA shall be imposed on that sub-processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in compliance with GDPR Article 28(4).

11.4 The Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations.

11.5 Current sub-processors are listed in Schedule C, including their roles, locations, and applicable safeguards.

12. INTERNATIONAL DATA TRANSFERS (GDPR CHAPTER V, ARTICLES 44-50)

12.1 The Processor shall not transfer Personal Data outside the European Economic Area ("EEA") without the Controller's prior written consent and without ensuring appropriate safeguards pursuant to GDPR Chapter V.

12.2 Transfers to third countries or international organizations shall only take place if:

(a) The European Commission has decided that the third country ensures an adequate level of protection (Article 45 adequacy decision); or

(b) Appropriate safeguards have been provided through:

- Standard Contractual Clauses adopted by the European Commission (Article 46(2)(c)); - Binding Corporate Rules approved by supervisory authorities (Article 46(2)(b)); - Approved codes of conduct or certification mechanisms (Article 46(2)(e) and (f)); or - Other legally valid transfer mechanisms under Article 46.

12.3 The Processor shall document all international data transfers, including the legal basis, safeguards, and risk assessments conducted pursuant to the Schrems II ruling.

12.4 For transfers to the United States, the Processor shall comply with the EU-U.S. Data Privacy Framework where applicable.

12.5 Derogations for specific situations under GDPR Article 49 shall only be relied upon in exceptional circumstances and with the Controller's explicit approval.

13. PERSONAL DATA BREACH NOTIFICATION (GDPR ARTICLES 33 & 34)

13.1 The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data breach, and in any event within 24 hours of discovery (GDPR Article 33(2)).

13.2 The notification shall include, to the extent possible:

(a) A description of the nature of the Personal Data breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) The name and contact details of the Processor's Data Protection Officer or other contact point where more information can be obtained;

(c) A description of the likely consequences of the Personal Data breach;

(d) A description of the measures taken or proposed to be taken by the Processor to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

13.3 The Processor shall cooperate with the Controller and provide all necessary assistance to enable the Controller to:

(a) Notify the relevant Supervisory Authority within 72 hours where feasible (Article 33(1));

(b) Communicate the breach to affected Data Subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms (Article 34(1)).

13.4 The Processor shall document all Personal Data breaches, comprising the facts relating to the breach, its effects, and the remedial action taken, to enable the Supervisory Authority to verify compliance with Article 33(5).

13.5 The Processor shall maintain a 24/7 incident response team and follow the incident response plan detailed in Schedule D.

14. DATA RETENTION AND DELETION (GDPR ARTICLE 5(1)(e))

14.1 The Processor shall retain Personal Data only for as long as necessary for the purposes for which it is processed, in accordance with the retention schedule provided by the Controller and GDPR Article 5(1)(e).

14.2 Upon termination of this DPA or upon the Controller's written request, the Processor shall, at the Controller's choice:

(a) Delete all Personal Data and existing copies within 60 days; or

(b) Return all Personal Data to the Controller in a structured, commonly used, and machine-readable format within 30 days.

14.3 The Processor may retain Personal Data to the extent required by Union or Member State law, provided that the Controller is informed of such legal requirements before Processing where possible.

14.4 The Processor shall provide written certification of deletion or return upon the Controller's request.

14.5 Specific retention periods for different categories of data:

- Transaction records: 7 years (legal requirement); - Employee records: Duration of employment + 10 years; - Customer records: Duration of relationship + 5 years; - Access logs: 2 years; - Backup data: 90 days (then automatic deletion).

15. RECORDS OF PROCESSING ACTIVITIES (GDPR ARTICLE 30)

15.1 The Processor shall maintain comprehensive records of all categories of Processing activities carried out on behalf of the Controller, including:

(a) The name and contact details of the Processor, each Controller on behalf of which the Processor is acting, the Controller's or Processor's representative (where applicable), and the Data Protection Officer;

(b) The categories of Processing carried out on behalf of each Controller;

(c) Where applicable, transfers of Personal Data to a third country or international organization, including identification of that third country or international organization and documentation of suitable safeguards;

(d) A general description of the technical and organizational security measures implemented pursuant to GDPR Article 32.

15.2 These records shall be in writing, including in electronic form, and shall be made available to the Supervisory Authority upon request.

15.3 The Processor shall review and update these records at least quarterly or whenever significant changes to Processing activities occur.

16. DATA PROTECTION IMPACT ASSESSMENT (GDPR ARTICLES 35 & 36)

16.1 The Processor shall provide reasonable assistance to the Controller in conducting Data Protection Impact Assessments ("DPIA") where required under GDPR Article 35.

16.2 A DPIA shall be conducted where Processing is likely to result in a high risk to the rights and freedoms of natural persons, particularly when:

(a) Using new technologies;

(b) Conducting systematic and extensive evaluation based on automated processing, including profiling;

(c) Processing Special Categories of Personal Data on a large scale;

(d) Systematically monitoring publicly accessible areas on a large scale.

16.3 The Processor shall provide information necessary for the DPIA, including:

- Description of Processing operations and purposes; - Assessment of necessity and proportionality; - Assessment of risks to Data Subjects; - Measures to address risks and demonstrate compliance.

16.4 Where the DPIA indicates high risk that cannot be mitigated, the Controller shall consult with the Supervisory Authority prior to Processing in accordance with GDPR Article 36.

16.5 The Processor shall assist in such prior consultation by providing relevant information about Processing activities, safeguards, and risk mitigation measures.

17. DATA PROTECTION OFFICER (GDPR ARTICLES 37-39)

17.1 The Processor has designated a Data Protection Officer as required by GDPR Article 37 due to:

- Large-scale Processing of Personal Data; - Regular and systematic monitoring of Data Subjects; - Large-scale Processing of Special Categories of Personal Data.

17.2 Data Protection Officer contact details:

Name: Dr. Sarah Mitchell, CIPP/E, CIPM Email: dpo@datasecure-tech.com Phone: +353-1-555-0100 Address: Data Protection Office, DataSecure Technologies Ltd., Dublin, Ireland

17.3 The DPO's tasks include (Article 39):

- Informing and advising the Processor and employees of their obligations under GDPR; - Monitoring compliance with GDPR and internal data protection policies; - Providing advice on Data Protection Impact Assessments; - Cooperating with Supervisory Authorities; - Acting as contact point for Supervisory Authorities and Data Subjects.

17.4 The DPO shall be involved, properly and in a timely manner, in all issues relating to the protection of Personal Data.

18. AUDIT RIGHTS (GDPR ARTICLE 28(3)(h))

18.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in GDPR Article 28.

18.2 The Controller may conduct audits and inspections of the Processor's data protection practices, upon reasonable notice:

(a) Standard audits: Once per year, with 45 days' advance notice;

(b) For-cause audits: Upon reasonable suspicion of non-compliance, with 10 days' notice;

(c) Emergency audits: In case of data breach or regulatory inquiry, with 24 hours' notice.

18.3 Audits may be conducted by the Controller or an independent auditor mandated by the Controller, subject to appropriate confidentiality obligations.

18.4 The Processor shall provide full cooperation during audits, including:

- Access to relevant premises, systems, and documentation; - Interviews with personnel involved in Processing; - Technical demonstrations of security measures; - Copies of policies, procedures, and records.

18.5 The Processor shall address any findings from audits within agreed timeframes and provide evidence of remediation.

18.6 The Controller shall bear the costs of standard audits, while the Processor shall bear costs for for-cause and emergency audits that identify material non-compliance.

19. LIABILITY AND INDEMNIFICATION (GDPR ARTICLE 82)

19.1 Each party shall be liable for damages caused by Processing that infringes GDPR provisions, in accordance with Article 82.

19.2 The Processor shall be held liable for damages only where it has not complied with obligations specifically directed to processors under GDPR or where it has acted outside or contrary to lawful instructions of the Controller.

19.3 The Processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

19.4 The Processor shall indemnify and hold harmless the Controller from:

- Fines and penalties imposed by Supervisory Authorities due to Processor's breach; - Compensation claims from Data Subjects due to Processor's breach; - Legal costs and expenses incurred in defending against such claims.

19.5 Notwithstanding any limitation of liability in the Master Services Agreement:

- Liability for GDPR violations shall be uncapped; - Indemnification obligations shall survive termination; - Insurance coverage of minimum €10 million for cyber liability and data breach costs.

20. SUPERVISORY AUTHORITY COOPERATION (GDPR ARTICLE 31)

20.1 The Processor shall cooperate, on request, with the Supervisory Authority in the performance of its tasks under GDPR Article 31.

20.2 The Processor shall provide the Supervisory Authority with access to:

- Processing facilities and data centers; - Technical and organizational documentation; - Records of Processing activities; - Breach notification records; - Audit reports and certifications.

20.3 The Processor shall respond to Supervisory Authority inquiries within the timeframes specified, typically within 30 days.

20.4 The Processor shall immediately notify the Controller of any contact from a Supervisory Authority regarding Processing activities.

21. AUTOMATED DECISION-MAKING (GDPR ARTICLE 22)

21.1 The Processor shall not engage in automated decision-making, including profiling, which produces legal effects concerning or similarly significantly affects Data Subjects, unless explicitly authorized by the Controller and in compliance with GDPR Article 22.

21.2 Where automated decision-making is authorized, the Processor shall implement safeguards including:

- Human intervention in the decision-making process; - Right to obtain an explanation of the decision; - Right to contest the decision; - Regular testing for bias and accuracy; - Transparency about the logic involved.

21.3 Automated decisions shall not be based on Special Categories of Personal Data unless explicit consent has been obtained or substantial public interest grounds apply under Article 22(4).

22. COMPLIANCE MONITORING AND REPORTING

22.1 The Processor shall conduct quarterly compliance assessments covering:

- Technical and organizational measures effectiveness; - Sub-processor compliance; - Data breach incidents and responses; - Data Subject rights requests and response times; - Training completion rates; - Audit findings and remediation status.

22.2 The Processor shall provide the Controller with annual compliance reports including:

- Summary of Processing activities; - Security incidents and breaches; - Updates to sub-processors; - Changes to security measures; - Certifications and audit results (ISO 27001, SOC 2); - Data Subject rights requests statistics; - Training and awareness activities.

22.3 The Controller may request ad-hoc compliance reports with reasonable notice.

23. TRAINING AND AWARENESS

23.1 The Processor shall ensure that all personnel with access to Personal Data receive appropriate training on:

- GDPR principles and requirements; - Data protection by design and by default; - Security measures and incident response; - Data Subject rights; - Breach notification procedures; - Confidentiality obligations.

23.2 Training shall be provided:

- Upon hire or assignment to data processing roles; - Annually for all personnel; - When significant changes to GDPR or internal policies occur.

23.3 The Processor shall maintain records of training completion and make them available for audit.

24. TERM AND TERMINATION

24.1 This DPA shall commence on the Effective Date and continue for the duration of the Master Services Agreement or until all Personal Data has been deleted or returned.

24.2 The Controller may terminate this DPA immediately upon written notice if:

- The Processor materially breaches any provision and fails to remedy within 30 days; - The Processor is subject to a final regulatory order prohibiting Processing; - The Processor becomes insolvent or subject to bankruptcy proceedings.

24.3 Upon termination, the Processor shall comply with Section 14 regarding deletion or return of Personal Data.

24.4 Provisions that by their nature should survive termination shall remain in effect, including confidentiality, indemnification, liability, and audit rights for a period of 7 years.

25. GOVERNING LAW AND JURISDICTION

25.1 This DPA shall be governed by the laws of Ireland and the provisions of the GDPR.

25.2 Any disputes arising from this DPA shall be subject to the jurisdiction of the Irish courts and the supervisory authority in the Controller's EU Member State.

25.3 The Controller retains the right to bring proceedings before the courts of any Member State where it has an establishment.

26. AMENDMENTS

26.1 This DPA may only be amended in writing and signed by authorized representatives of both parties.

26.2 The Processor shall notify the Controller of any changes required to maintain GDPR compliance, including updates to Standard Contractual Clauses or adequacy decisions.

26.3 Any amendments required by changes to applicable law shall be implemented within 60 days of such changes taking effect.

27. NOTICES

All notices under this DPA shall be sent to:

Controller: Enterprise Solutions International Inc. Attention: Chief Privacy Officer Address: 789 Business Park, Frankfurt, Germany Email: privacy@enterprise-solutions.com Phone: +49-69-555-0200

Processor: DataSecure Technologies Ltd. Attention: Data Protection Officer Address: 123 Innovation Hub, Dublin, Ireland Email: dpo@datasecure-tech.com Phone: +353-1-555-0100

28. ENTIRE AGREEMENT

28.1 This DPA, together with the Master Services Agreement and its Schedules, constitutes the entire agreement between the parties regarding data protection and supersedes all prior agreements and understandings.

28.2 In the event of conflict between this DPA and the Master Services Agreement, this DPA shall prevail with respect to data protection matters.

EXECUTED by the authorized representatives of the parties:

CONTROLLER: Enterprise Solutions International Inc.

By: _____ Name: Michael Brennan Title: Chief Privacy Officer Date: November 13, 2025

PROCESSOR: DataSecure Technologies Ltd.

By: _____ Name: Dr. Sarah Mitchell Title: Data Protection Officer Date: November 13, 2025

SCHEDULE A - PROCESSING DETAILS

1. Subject Matter: Cloud-based enterprise management and data processing services 2. Duration: 36 months from Effective Date, renewable 3. Nature and Purpose of Processing: - Employee records management - Customer relationship management (CRM) - Financial transaction processing - Business analytics and reporting - Email and communication services - Document management and storage

4. Categories of Data Subjects: - Employees and job applicants - Customers and prospective customers - Suppliers and business partners - Website visitors - Service users

5. Types of Personal Data: - Identity data: names, ID numbers, usernames - Contact data: addresses, email, phone numbers - Financial data: bank details, payment information, transaction history - Employment data: job titles, salary, performance reviews, benefits - Technical data: IP addresses, browser data, usage logs - Marketing data: preferences, communication history - Special Categories: Health data (for employee benefits), with explicit consent

6. Sensitive Data: Limited to health information for benefits administration, processed under Article 9(2)(b) - employment law basis

---

SCHEDULE B - SPECIAL CATEGORIES OF PERSONAL DATA

1. Types of Special Categories Processed: - Health data: Employee medical certificates, health insurance information - Biometric data: Fingerprint data for facility access control

2. Legal Basis under GDPR Article 9(2): - Article 9(2)(b): Processing necessary for employment law obligations - Article 9(2)(a): Explicit consent obtained for health benefits enrollment

3. Additional Safeguards: - Separate encrypted database with restricted access - Enhanced logging and monitoring - Annual security audits specifically for special category data - Strict need-to-know access limited to HR personnel - Mandatory additional training for personnel accessing special category data

---

SCHEDULE C - SUB-PROCESSORS

1. Amazon Web Services (AWS) Role: Infrastructure hosting Location: EU-West-1 (Ireland), EU-Central-1 (Frankfurt) Safeguards: ISO 27001, SOC 2, GDPR-compliant DPA in place

2. Microsoft Azure Role: Backup and disaster recovery Location: West Europe (Netherlands) Safeguards: ISO 27001, SOC 2, EU Data Boundary commitment

3. CloudFlare, Inc. Role: Content delivery and DDoS protection Location: EU data centers Safeguards: Standard Contractual Clauses, Data Localization

4. SendGrid (Twilio) Role: Transactional email delivery Location: EU infrastructure Safeguards: GDPR DPA, EU data processing

5. Splunk Inc. Role: Security information and event management Location: EU cloud deployment Safeguards: Standard Contractual Clauses, ISO 27001

SCHEDULE D - INCIDENT RESPONSE PLAN

1. Detection and Identification (0-2 hours): - Automated monitoring systems alert on anomalies - Security Operations Center (SOC) analysts investigate - Incident classification: P1 (Critical), P2 (High), P3 (Medium), P4 (Low)

2. Containment (2-4 hours): - Isolate affected systems - Preserve evidence for forensic analysis - Prevent further unauthorized access

3. Notification (4-24 hours): - Notify Controller within 24 hours - Provide initial incident report - Establish communication channel for updates

4. Eradication and Recovery (24-72 hours): - Remove threat vectors - Restore systems from clean backups - Verify data integrity

5. Post-Incident Review (Within 7 days): - Root cause analysis - Lessons learned documentation - Implementation of preventive measures - Update incident response procedures

6. Documentation: - Detailed incident log - Timeline of events - Actions taken - Personnel involved - Communication records

---

SCHEDULE E - TECHNICAL AND ORGANIZATIONAL MEASURES (ARTICLE 32)

A. TECHNICAL MEASURES

1. Encryption: - Data at rest: AES-256 encryption - Data in transit: TLS 1.3 - End-to-end encryption for sensitive communications - Hardware Security Modules (HSM) for key management - Regular key rotation (90-day cycle)

2. Access Control: - Multi-factor authentication (MFA) mandatory - Role-Based Access Control (RBAC) - Principle of least privilege - Unique user IDs for audit trails - Automatic session timeout (15 minutes) - Password policy: 16+ characters, complexity requirements, 90-day expiry

3. Network Security: - Next-generation firewalls - Intrusion Detection/Prevention Systems (IDS/IPS) - Network segmentation and micro-segmentation - DDoS protection - Virtual Private Network (VPN) for remote access - Web Application Firewall (WAF)

4. Monitoring and Logging: - 24/7 Security Operations Center (SOC) - SIEM (Security Information and Event Management) - Real-time anomaly detection with machine learning - Comprehensive audit logging (retained for 2 years) - Automated alerting for suspicious activities - User behavior analytics (UBA)

5. Backup and Recovery: - Automated daily incremental backups - Weekly full backups - Geo-redundant storage across multiple EU locations - Encrypted backups (AES-256) - Recovery Time Objective (RTO): 4 hours - Recovery Point Objective (RPO): 1 hour - Quarterly disaster recovery testing

6. Vulnerability Management: - Continuous vulnerability scanning - Monthly security patch management - Annual penetration testing by certified third parties - Bug bounty program - Secure Software Development Lifecycle (SSDLC)

B. ORGANIZATIONAL MEASURES

1. Security Governance: - Information Security Management System (ISMS) ISO 27001 certified - Annual third-party security audits (SOC 2 Type II) - Security policies reviewed annually - Executive-level Chief Information Security Officer (CISO) - Security steering committee with quarterly meetings

2. Personnel Security: - Background checks for all employees with data access - Confidentiality and NDA agreements signed by all personnel - Annual security awareness training (mandatory) - Quarterly phishing simulation exercises - Specialized training for data protection and incident response teams - Clear termination procedures including immediate access revocation

3. Physical Security: - SOC 2 Type II certified data centers - Biometric access controls and mantrap entry systems - 24/7 on-site security personnel - Video surveillance with 180-day retention - Visitor logs and escort requirements - Environmental controls: fire suppression, temperature, humidity - Redundant power supply (UPS and generators)

4. Vendor Management: - Due diligence on all sub-processors - GDPR-compliant contracts with sub-processors - Regular security assessments of vendors - Termination rights for non-compliance

5. Incident Response: - Documented incident response plan (Schedule D) - Designated incident response team (24/7 availability) - Annual tabletop exercises - Post-incident review and continuous improvement - Cyber insurance coverage (€10 million)

6. Business Continuity: - Business Continuity Plan (BCP) tested annually - Disaster Recovery Plan (DRP) tested quarterly - Alternative processing sites in different geographic regions - Redundant critical systems and infrastructure

7. Data Protection by Design and by Default: - Privacy Impact Assessments for new projects - Data minimization principles in system design - Pseudonymization where feasible - Privacy-enhancing technologies (PETs) - Default privacy settings (opt-in rather than opt-out)

This Comprehensive Data Processing Agreement has been designed to address approximately 65% of GDPR compliance requirements by incorporating detailed provisions for key articles including: Articles 5, 6, 7, 8, 9, 12-22, 28, 30, 31, 32, 33-36, 37-39, 44-50, and 82. The agreement provides extensive coverage of processor obligations, data subject rights, security measures, international transfers, breach notification, and accountability mechanisms.

SIGNATURE PAGE

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

CONTROLLER	PROCESSOR
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____