GUVRIX DATA PROCESSING AGREEMENT

Effective Date: September 23, 2026
Last Updated: September 23, 2026

This Data Processing Agreement ("DPA") forms part of the agreement between Guvrix LLC ("Guvrix") and the business, organization, government entity, nonprofit, association, or other legal entity using the Guvrix Services ("Customer").

This DPA applies where Guvrix processes Personal Data on behalf of Customer in connection with Customer's use of the Guvrix website, software platform, applications, subscriptions, and related services (collectively, the "Services").

This DPA supplements the Guvrix Terms of Service, applicable order form or subscription agreement, and Guvrix Privacy Policy (collectively, the "Agreement").

If there is a conflict between this DPA and the Agreement concerning the processing of Customer Personal Data, this DPA will control to the extent of that conflict.

1. Definitions

For purposes of this DPA:

1.1 "Applicable Data Protection Law"

means privacy, data-protection, and information-security laws applicable to the processing of Customer Personal Data under the Agreement, which may include, where applicable:

- Regulation (EU) 2016/679 ("GDPR");
- applicable European Economic Area data-protection laws;
- United Kingdom data-protection law, including the UK GDPR as applicable;
- Israel's Privacy Protection Law and applicable regulations;
- Kenya's Data Protection Act and applicable regulations;
- applicable United States federal and state privacy laws; and
- other applicable privacy or data-protection requirements.

1.2 "Controller"

means the person or organization that determines the purposes and means of processing Personal Data, or the equivalent term under Applicable Data Protection Law.

1.3 "Customer Personal Data"

means Personal Data processed by Guvrix on behalf of Customer in connection with Customer's use of the Services.

Customer Personal Data does not include Personal Data for which Guvrix independently determines the purposes and means of processing, such as certain account administration, billing, security, fraud prevention, or legal-compliance activities, as described in the Guvrix Privacy Policy.

1.4 "Data Subject"

means an identified or identifiable natural person to whom Personal Data relates.

1.5 "Personal Data"

means any information relating to an identified or identifiable natural person, or information otherwise defined as personal information, personal data, or an equivalent term under Applicable Data Protection Law.

1.6 "Personal Data Breach"

means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

1.7 "Process," "Processed," or "Processing"

means any operation performed on Personal Data, including collection, recording, organization, structuring, storage, modification, retrieval, consultation, use, disclosure, transmission, restriction, deletion, or destruction.

1.8 "Processor"

means a person or organization that processes Personal Data on behalf of a Controller, or the equivalent term under Applicable Data Protection Law.

1.9 "Subprocessor"

means a third party engaged by Guvrix to process Customer Personal Data on behalf of Customer in connection with the Services.

1.10 "Supervisory Authority"

means a governmental, regulatory, or data-protection authority with jurisdiction over processing covered by this DPA.

2. Roles of the Parties

For Customer Personal Data processed through the Services:

Customer is the Controller and Guvrix is the Processor, except where Applicable Data Protection Law provides otherwise.

Customer determines:

- what Personal Data is submitted to Guvrix;
- the purposes for which the Personal Data is processed;
- which individuals may access the Personal Data;
- the lawful basis for processing;
- how the Customer uses information produced through Guvrix; and
- when Customer Personal Data should be retained or deleted, subject to the Agreement and applicable law.

Guvrix processes Customer Personal Data on behalf of Customer to provide the Services and in accordance with Customer's documented instructions.

Nothing in this DPA prevents Guvrix from acting as an independent Controller for Personal Data that Guvrix processes for its own legitimate business purposes, including account administration, security, fraud prevention, legal compliance, billing administration, and operation of its business, where permitted by law.

3. Customer Instructions

Customer instructs Guvrix to process Customer Personal Data as reasonably necessary to:

- provide the Services;
- operate Customer's Guvrix account;
- perform governance and compliance assessments;
- calculate assessment results and risk indicators;
- identify potential governance or compliance gaps;
- provide guidance and suggested controls;
- generate reports;
- provide AI-assisted features requested by Customer;
- generate Customer-requested templates, checklists, documents, or other materials;
- store Customer information;
- provide support;
- maintain security and availability;
- prevent abuse or unauthorized access; and
- otherwise perform Guvrix's obligations under the Agreement.

The Agreement, Customer's configuration and use of the Services, and instructions submitted through authorized users constitute Customer's documented instructions to Guvrix.

Guvrix will not process Customer Personal Data for purposes materially inconsistent with those instructions unless required by applicable law.

If applicable law requires Guvrix to process Customer Personal Data contrary to Customer's instructions, Guvrix will notify Customer before processing unless prohibited from doing so by law.

If Guvrix reasonably believes an instruction violates Applicable Data Protection Law, Guvrix may inform Customer and suspend the affected processing until the parties resolve the issue.

4. Customer Responsibilities

Customer represents and warrants that:

- it has the right and authority to provide Customer Personal Data to Guvrix;
- its processing instructions comply with Applicable Data Protection Law;
- it has provided required privacy notices;
- it has obtained any required consents or other lawful basis for processing;
- use of the Services will comply with Applicable Data Protection Law;
- it will not instruct Guvrix to process Personal Data unlawfully; and
- it will not intentionally submit Personal Data that is unnecessary for the intended governance or compliance purpose.

Customer is responsible for determining whether particular categories of Personal Data are appropriate for use with Guvrix.

5. Data Minimization

Guvrix is designed primarily to evaluate organizational governance, compliance, risk, and operational practices rather than to create extensive profiles of identifiable individuals.

Customers should provide organizational information rather than personally identifiable information whenever possible.

Customer should avoid entering unnecessary:

- health information;
- biometric information;
- financial-account information;
- government identification numbers;
- information concerning children;
- information regarding race, ethnicity, religion, political beliefs, sexual orientation, or other sensitive characteristics;
- passwords or authentication credentials;
- criminal-history information; or
- other highly sensitive Personal Data,

unless such processing has been expressly authorized, is necessary for Customer's legitimate use of the Services, and complies with Applicable Data Protection Law.

6. Confidentiality

Guvrix will ensure that personnel authorized to process Customer Personal Data:

- access such information only where reasonably necessary to perform their responsibilities;
- are subject to appropriate confidentiality obligations; and
- receive appropriate privacy and security instructions or training relevant to their responsibilities.

Guvrix will not disclose Customer Personal Data except as permitted by this DPA, the Agreement, Customer instructions, or applicable law.

7. Security Measures

Guvrix will maintain reasonable and appropriate technical and organizational measures designed to protect Customer Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure.

Security measures will be appropriate to the nature and risk of the processing and may include, as applicable:

- access controls;
- authentication controls;
- role-based access;
- least-privilege principles;
- encryption in transit;
- encryption at rest where appropriate;
- password and credential protections;
- system logging;
- security monitoring;
- backups;
- vulnerability management;
- security patching;
- malware protection;
- network and infrastructure safeguards;
- secure development practices;
- incident-response procedures;
- business continuity and recovery measures;
- personnel confidentiality requirements;
- vendor and Subprocessor security requirements; and
- periodic review of relevant security controls.

Additional information concerning Guvrix's technical and organizational security measures is provided in Schedule 2.

Guvrix may update its security controls as technologies, risks, and the Services evolve, provided that Guvrix will not materially reduce the overall level of protection for Customer Personal Data during a subscription term.

8. Personal Data Breaches

Guvrix will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data.

To the extent reasonably available, the notification will include information concerning:

- the nature of the Personal Data Breach;
- categories of Customer Personal Data involved;
- categories of affected Data Subjects;
- approximate number of affected records or individuals, where known;
- likely consequences of the breach;
- measures taken or proposed to address the breach; and
- measures taken to reduce potential harm.

Guvrix may provide information in phases if complete information is not initially available.

Guvrix will take reasonable steps to contain, investigate, mitigate, and remediate a Personal Data Breach within its control.

Guvrix's notification of a Personal Data Breach does not constitute an admission of fault or liability.

Unless Applicable Data Protection Law requires otherwise, Customer remains responsible for determining whether notification must be provided to Data Subjects, Supervisory Authorities, customers, employees, or other parties.

Guvrix will provide reasonable assistance to Customer concerning such notifications where required by Applicable Data Protection Law.

9. Data Subject Requests

Taking into account the nature of the processing, Guvrix will provide reasonable assistance to Customer in responding to requests by Data Subjects exercising applicable privacy rights, including, where required:

- access;
- correction;
- deletion;
- restriction;
- objection;
- portability; and
- withdrawal of consent.

If Guvrix receives a request directly from a Data Subject concerning Customer Personal Data, Guvrix may direct the individual to Customer unless Guvrix is legally required to respond directly.

Guvrix will not independently respond to a Data Subject request concerning Customer Personal Data except:

- on Customer's instructions;
- where necessary to identify the applicable Customer; or
- where required by law.

10. Assistance with Customer Compliance

Taking into account the nature of processing and information reasonably available to Guvrix, Guvrix will provide reasonable assistance to Customer concerning applicable obligations relating to:

- information security;
- Personal Data Breaches;
- Data Subject rights;
- data-protection impact assessments;
- regulatory consultations; and
- other Processor-assistance obligations imposed by Applicable Data Protection Law.

Customer remains responsible for determining its own legal obligations.

Assistance that requires substantial resources beyond the normal operation of the Services may be subject to reasonable fees, provided Guvrix informs Customer beforehand where practicable.

11. Subprocessors

11.1 General Authorization

Customer provides Guvrix with general written authorization to engage third-party subprocessors where reasonably necessary to provide, support, secure, maintain, or improve the Services.

Guvrix will require each subprocessor that processes Customer Personal Data on Guvrix's behalf to be subject to appropriate contractual obligations regarding data protection, confidentiality, and security that are consistent with Guvrix's obligations under this DPA and Applicable Data Protection Law.

11.2 Subprocessor Information

Guvrix maintains a current list of subprocessors that may process Customer Personal Data in connection with the Services.

For security, confidentiality, commercial, and vendor-management reasons, Guvrix does not make its detailed subprocessor list publicly available.

An authorized representative of a Customer may request the current subprocessor list where reasonably necessary for the Customer's data protection, information security, regulatory compliance, procurement, audit, or vendor due-diligence obligations.

Requests must be submitted to Guvrix through the contact method designated by Guvrix and must identify the requesting organization and authorized representative.

Guvrix may require reasonable verification of the requester's identity, authority, and Customer relationship before providing the information. Guvrix may also require that non-public subprocessor information be treated as Confidential Information under the Agreement or an applicable confidentiality agreement.

Guvrix may decline requests that are unrelated to a legitimate Customer compliance or due-diligence purpose, are excessive or repetitive, seek information beyond what is reasonably necessary to evaluate Guvrix's processing of Customer Personal Data, or are submitted by unauthorized third parties.

11.3 Information Provided

Where reasonably required under Applicable Data Protection Law, the information provided may include:

- the identity of the subprocessor;
- the services or processing activities performed by the subprocessor;
- the general categories of Customer Personal Data processed;
- the applicable processing or hosting location or geographic region, where relevant; and
- other information reasonably necessary for the Customer to evaluate the subprocessor's role in processing Customer Personal Data.

Guvrix is not required to disclose confidential commercial terms, pricing, security credentials, proprietary configurations, internal security information, or other information that could reasonably create a security or commercial risk, except where disclosure is required by Applicable Data Protection Law.

11.4 Changes to Subprocessors

Where required by Applicable Data Protection Law, Guvrix will provide Customers with reasonable advance notice of any intended addition or replacement of a subprocessor that will process Customer Personal Data.

Customer may object to the proposed subprocessor on reasonable and documented data-protection or information-security grounds within the period specified in the notice.

The parties will work in good faith to address a valid objection. If a reasonable solution cannot be reached, Guvrix may, where commercially and technically feasible, modify the affected Services or Customer may discontinue the affected portion of the Services in accordance with the Agreement.

An objection does not provide Customer with a general right to control Guvrix's selection of service providers or subprocessors.

11.5 Payment and Independent Service Providers

Third parties such as payment processors, merchants of record, financial institutions, or other providers that process Personal Data as independent controllers are not subprocessors merely because they provide services relating to a Customer transaction.

Their status will be determined according to the nature of the processing and Applicable Data Protection Law.

12. Payment Providers

Guvrix may use payment and commerce providers including Stripe, PayPal, Paddle, or other providers.

To the extent such providers process information independently for payment processing, fraud prevention, regulatory compliance, taxation, chargebacks, merchant-of-record functions, or similar purposes, they may act as independent Controllers rather than Subprocessors of Guvrix.

Such independent processing is governed by the applicable provider's own privacy terms and is not Customer Personal Data processing performed by Guvrix as Processor under this DPA.

If a payment provider processes Customer Personal Data solely on Guvrix's behalf in a Processor capacity, that processing will be subject to the applicable Subprocessor requirements of this DPA.

13. Artificial Intelligence Providers

Guvrix may use third-party artificial intelligence or machine-learning providers to support AI-assisted Services.

Where an AI provider processes Customer Personal Data on behalf of Guvrix, Guvrix will treat that provider as a Subprocessor where required by Applicable Data Protection Law.

Guvrix will take reasonable measures to ensure that Customer Personal Data provided to such services is:

- limited to information reasonably necessary for the requested functionality;

- subject to appropriate contractual protections;
- protected through reasonable security measures; and
- processed consistently with this DPA.

Guvrix will not permit Customer Personal Data to be used to train or improve a third-party provider's general-purpose AI models unless Customer has expressly authorized such use.

Guvrix may use de-identified or aggregated information to improve its own Services where such information no longer reasonably identifies Customer or a Data Subject and such use is permitted under the Agreement and Applicable Data Protection Law.

14. International Transfers

Customer acknowledges that Guvrix and its authorized Subprocessors may process Customer Personal Data in countries other than the country in which Customer or Data Subjects are located.

Guvrix will ensure that international transfers of Customer Personal Data are made in accordance with Applicable Data Protection Law.

Where a legally recognized transfer mechanism is required, the parties will use an appropriate mechanism, which may include:

- an adequacy decision;
- Standard Contractual Clauses;
- an approved addendum to Standard Contractual Clauses;
- another approved contractual mechanism;
- another legally recognized transfer arrangement; or
- another lawful basis for transfer.

Where necessary, Guvrix will implement supplementary technical, organizational, or contractual safeguards appropriate to the circumstances.

15. European Economic Area Transfers

If Customer Personal Data subject to the GDPR is transferred to a country that does not benefit from an applicable European Commission adequacy decision and no other lawful transfer mechanism applies, the parties agree that the applicable European Commission Standard Contractual Clauses may be incorporated into this DPA as necessary.

Unless otherwise agreed, the appropriate controller-to-processor module will apply where Customer is a Controller and Guvrix is a Processor.

The parties will complete any information reasonably necessary to give effect to those clauses.

If the Standard Contractual Clauses conflict with this DPA regarding an international transfer governed by those clauses, the Standard Contractual Clauses will control.

16. United Kingdom Transfers

Where Customer Personal Data subject to United Kingdom data-protection law is transferred internationally and a legally recognized transfer mechanism is required, the parties will use an applicable UK-approved transfer mechanism, including an applicable UK International Data Transfer Addendum or successor mechanism where appropriate.

17. Other International Transfers

Where Customer Personal Data is subject to Israeli, Kenyan, United States, or other applicable international-transfer requirements, the parties will comply with legally required transfer restrictions and safeguards applicable to their respective roles.

Customer is responsible for identifying any Customer-specific transfer restriction not reasonably apparent from Customer's ordinary use of the Services and notifying Guvrix where additional measures are required.

18. Government and Law-Enforcement Requests

If Guvrix receives a legally binding request from a government authority for Customer Personal Data, Guvrix will, to the extent legally permitted:

- review the request for validity;
- limit disclosure to information legally required;
- notify Customer before disclosure where permitted; and
- reasonably cooperate with Customer regarding an appropriate response.

Nothing in this section requires Guvrix to violate applicable law or a binding governmental or judicial order.

19. Data Retention

Guvrix will retain Customer Personal Data only for as long as reasonably necessary to provide the Services, meet contractual obligations, maintain appropriate backups, resolve disputes, protect security, or meet applicable legal requirements.

Customer may delete or modify certain Customer Personal Data through functionality made available within the Services.

Specific retention periods may vary according to the nature of the information and the Services.

20. Return and Deletion of Customer Personal Data

Upon expiration or termination of the Services, Customer may request return or export of Customer Personal Data where reasonably supported by the Services.

Following expiration of the applicable data-export or retention period, Guvrix will delete or render inaccessible Customer Personal Data within its control unless:

- continued retention is required by law;
- the information exists in secured backups that cannot reasonably be individually deleted immediately; or
- continued retention is otherwise authorized under the Agreement.

Customer Personal Data retained in backups will remain protected under this DPA and will not be restored for ordinary business use except as required for system recovery or legal compliance.

21. Audits and Compliance Information

Upon reasonable written request, Guvrix will make available information reasonably necessary to demonstrate compliance with its obligations under this DPA.

Where available and appropriate, Guvrix may satisfy an audit request by providing:

- security documentation;
- privacy documentation;
- policies;
- certifications;
- questionnaires; or
- other relevant compliance information.

If such information is insufficient to satisfy a legally required audit obligation, Customer may request an additional audit.

Any audit must:

- occur no more than once per twelve-month period unless required following a material security incident or by a Supervisory Authority;
- be conducted during normal business hours;
- provide reasonable advance notice;
- avoid unreasonable interference with Guvrix operations;
- protect Guvrix confidential information and information belonging to other customers;
- be limited to matters relevant to Customer Personal Data; and
- comply with reasonable security requirements established by Guvrix.

Customer will bear its audit costs unless Applicable Data Protection Law requires otherwise or the audit identifies a material breach of this DPA by Guvrix.

22. Regulatory Inquiries

If a Supervisory Authority contacts Guvrix regarding Customer's processing of Customer Personal Data, Guvrix may notify Customer where legally permitted.

The parties will reasonably cooperate regarding relevant regulatory inquiries to the extent required by Applicable Data Protection Law.

Each party remains responsible for its own regulatory compliance and interactions with Supervisory Authorities concerning matters within its control.

23. Records of Processing

Guvrix will maintain records of processing activities where required by Applicable Data Protection Law.

Customer will provide information reasonably necessary for Guvrix to maintain legally required records concerning Customer's processing activities.

24. Data Protection Impact Assessments

Where Customer is legally required to conduct a data-protection impact assessment relating to its use of the Services, Guvrix will provide reasonable information within its possession necessary to assist Customer.

Customer remains responsible for determining whether an impact assessment is required and for completing that assessment.

25. Children's Personal Data

The standard Guvrix Services are designed for organizational and professional users and are not intended to collect children's Personal Data directly.

If Customer uses Guvrix in a context involving children or minors, Customer is responsible for determining whether such processing is lawful and for obtaining required permissions, notices, parental consent, safeguarding measures, or other protections.

Customer should not submit children's Personal Data unless necessary for an authorized purpose and permitted by Applicable Data Protection Law.

26. Special Categories and Sensitive Personal Data

Customer must determine whether its use of Guvrix involves sensitive or special-category Personal Data and whether additional legal requirements apply.

Customer should minimize such processing wherever reasonably possible.

If Customer intends to use Guvrix systematically to process substantial quantities of sensitive Personal Data, Customer should notify Guvrix so that the parties can determine whether additional contractual or security measures are appropriate.

27. Sale of Personal Data

Guvrix does not sell Customer Personal Data to third parties for monetary consideration.

Guvrix will not disclose Customer Personal Data to advertising companies or data brokers for their independent commercial use unless Customer expressly authorizes such disclosure or the practice is otherwise expressly disclosed and lawfully permitted.

28. Limitation of Liability

The limitations, exclusions, and allocation of liability stated in the Agreement apply to this DPA unless prohibited by Applicable Data Protection Law.

Nothing in this DPA excludes or limits liability to the extent such liability cannot lawfully be excluded or limited.

29. Term

This DPA becomes effective when Customer becomes subject to the Agreement and Guvrix begins processing Customer Personal Data on Customer's behalf.

It remains effective for as long as Guvrix processes Customer Personal Data on behalf of Customer.

Obligations relating to confidentiality, security, deletion, and protection of retained Customer Personal Data survive termination to the extent reasonably necessary.

30. Changes to this DPA

Guvrix may update this DPA where reasonably necessary to:

- comply with changes in Applicable Data Protection Law;
- implement new regulatory requirements;
- update transfer mechanisms;
- reflect changes to the Services; or
- improve privacy or security protections.

Guvrix will not materially reduce the protections afforded to Customer Personal Data during an existing subscription term without a legitimate legal, regulatory, security, or operational reason.

Where legally required, Guvrix will notify Customer of material changes.

31. Governing Law

Unless mandatory Applicable Data Protection Law requires otherwise, this DPA will be governed by the governing-law provision in the Agreement.

Where Standard Contractual Clauses or another legally required data-transfer mechanism specifies a different governing law for matters covered by that mechanism, that specified law will govern those matters.

32. Order of Precedence

In the event of a conflict among documents concerning Customer Personal Data, the following order of precedence applies:

1. mandatory Applicable Data Protection Law;
2. applicable Standard Contractual Clauses or other mandatory international-transfer mechanism;
3. this DPA;
4. a separately executed Customer agreement or Order Form, unless it expressly states that it overrides this DPA;
5. the Guvrix Terms of Service; and
6. the Guvrix Privacy Policy.

33. Customer Details and Execution

Where this DPA is incorporated into the Agreement between Guvrix and Customer, the identity and contact details of the Customer and Guvrix will be those specified in the applicable Subscription/Order Agreement, account registration, order form, or other agreement governing the Customer's use of the Services.

This DPA forms part of the Agreement and does not require a separate signature unless Guvrix and Customer agree otherwise or a separate execution is required by Applicable Data Protection Law.

If a separately executed DPA is required, Guvrix may provide an execution version containing appropriate signature blocks and Customer-specific information.

SCHEDULE 1

DETAILS OF PROCESSING

1. Subject Matter

Processing Customer Personal Data as necessary to provide the Guvrix governance, compliance, risk-management, assessment, reporting, guidance, and related SaaS Services.

2. Duration

For the duration of Customer's subscription and any limited post-termination retention period, unless longer retention is required by law.

3. Nature and Purpose of Processing

Processing may include:

- collection;
- recording;
- organization;
- storage;
- retrieval;
- analysis;
- consultation;
- calculation;
- classification;
- generation of assessment results;
- generation of recommendations;
- generation of reports and documents;
- AI-assisted analysis where requested;
- transmission;
- support;
- security monitoring;
- backup;
- correction;
- export; and
- deletion.

The purpose is to provide, secure, maintain, support, and improve the Services provided to Customer.

4. Categories of Data Subjects

Depending upon Customer's use of Guvrix, Data Subjects may include:

- Customer employees;
- officers;
- directors;
- owners;
- managers;
- contractors;
- consultants;
- authorized users;
- customers or clients of Customer;
- vendors or suppliers;
- business contacts; and
- other individuals whose Personal Data Customer lawfully submits to Guvrix.

5. Categories of Personal Data

Depending upon Customer use, Customer Personal Data may include:

- name;
- business contact information;
- job title;
- role;
- organizational affiliation;
- account information;
- governance responsibilities;
- questionnaire responses;
- comments;
- corrective-action assignments;
- compliance-related information;
- uploaded information;
- documents;
- system activity; and
- other Personal Data submitted by Customer.

6. Sensitive Personal Data

Guvrix does not require Customers to provide sensitive Personal Data as part of ordinary use of the Services.

Depending upon Customer use, sensitive information could nevertheless be submitted by Customer.

Customer is responsible for determining whether such processing is appropriate and lawful.

7. Processing Frequency

Continuous or intermittent during Customer's use of the Services.

8. Geographic Scope

Processing may occur in locations where Guvrix or authorized Subprocessors operate, subject to Section 14 of this DPA and Applicable Data Protection Law.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Guvrix maintains technical and organizational measures appropriate to the nature and risk of Customer Personal Data processed through the Services.

Measures may include the following, as applicable to Guvrix's systems and infrastructure.

1. Access Management

- User authentication
- Unique user accounts
- Role-based permissions where applicable
- Administrative access restrictions
- Least-privilege principles
- Procedures for removing access when no longer required

2. Data Protection

- Encryption of network communications using appropriate industry-standard protocols
- Encryption of stored data where appropriate
- Controlled access to production systems
- Segregation of Customer information where technically appropriate

3. Infrastructure Security

- Secure hosting environments
- Network protections
- System monitoring
- Security configuration
- Patch and update management
- Malware and threat protections where applicable

4. Application Security

- Secure development practices
- Change-management controls
- Vulnerability identification and remediation

- Testing appropriate to significant system changes
- Protection against unauthorized application access

5. Logging and Monitoring

- Logging of appropriate system and security activity
- Monitoring for abnormal or unauthorized activities where appropriate
- Retention of relevant security records

6. Business Continuity

- Backup procedures
- Restoration capabilities
- Business-continuity planning appropriate to the Services
- Recovery procedures following significant technical incidents

7. Incident Management

- Security incident reporting procedures
- Investigation and containment processes
- Escalation procedures
- Remediation and lessons-learned activities where appropriate

8. Personnel Security

- Confidentiality obligations
- Access based upon role and business need
- Privacy and security awareness appropriate to personnel responsibilities

9. Third-Party Management

- Reasonable due diligence for material service providers
- Contractual privacy and security requirements where appropriate
- Oversight proportionate to the services and risks involved

10. Security Review

Guvrix periodically reviews its security measures and may modify them as technology, risk, legal requirements, and the Services evolve.

SCHEDULE 3

SUBPROCESSORS

Guvrix maintains its current Subprocessor List separately from this DPA.

The current list is not published publicly and is available to authorized Customers upon reasonable request in accordance with Section 11 of this DPA.

Subprocessor information provided by Guvrix that is designated as confidential will be treated as Confidential Information under the Agreement.