Sigilbase Data Processing Agreement

Effective Date: [Effective Date]

This Data Processing Agreement (the **Agreement**) forms part of the agreement for the Services between:

1. **Sigilbase Ltd**, a company registered in England and Wales under company number **17332548**, whose registered office is at **66 Paul Street, London, EC2A 4NA, United Kingdom**, and registered with the Information Commissioner's Office under number **ZC265849** (**Sigilbase**); and
2. **[Customer legal name]**, a company or other legal entity organised under the laws of **[jurisdiction]**, with its registered office or principal place of business at **[address]** (**Customer**).

Each is a **Party** and together they are the **Parties**.

1. Definitions and interpretation

1.1 In this Agreement:

- **Applicable Data Protection Law** means the UK GDPR, the Data Protection Act 2018, regulations made under them, and any other applicable UK laws and regulations concerning the processing of Personal Data, in each case as amended or replaced from time to time.
- **Controller**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Processor**, **processing** and **supervisory authority** have the meanings given to them in Applicable Data Protection Law.
- **Customer Personal Data** means Personal Data processed by Sigilbase on behalf of Customer in providing the Services, including Personal Data contained in Events.
- **Documented Instructions** means Customer's documented instructions under this Agreement, including the instructions in clause 3 and Schedule 1, as supplemented by Customer's use and configuration of the Services.
- **Event** means a record submitted to the Services, including its actor, action, payload, timestamp and associated metadata.
- **Sealed History** means the append-only record of accepted Events, including the event data, hash chain, Merkle checkpoints, signatures and associated metadata.
- **Services** means Sigilbase's audit-log ingestion, storage, hashing, chaining, sealing, verification, retention and export services, together with related features provided to Customer.
- **Sub-processor** means a Processor engaged by Sigilbase to process Customer Personal Data on Customer's behalf.

1.2 References to legislation include amendments, replacements and subordinate legislation in force from time to time. If a provision of this Agreement conflicts with Applicable Data Protection Law, Applicable Data Protection Law prevails.

1.3 The Schedules form part of this Agreement.

2. Roles and application

2.1 For Customer Personal Data, Customer acts as Controller and Sigilbase acts as Processor, unless clause 2.2 applies.

2.2 Customer may itself act as a Processor on behalf of another Controller. In that case, Customer appoints Sigilbase as its sub-processor for the relevant Customer Personal Data. Customer shall ensure that its appointment of Sigilbase is authorised by the relevant Controller and that Customer's instructions to Sigilbase are consistent with the Controller's instructions and Applicable Data Protection Law. Customer shall promptly provide relevant Controller instructions that affect Sigilbase's processing.

2.3 This Agreement applies to processing of Customer Personal Data by Sigilbase in connection with the Services. It does not govern Personal Data that Sigilbase processes as an independent Controller for its own purposes, including account administration, fraud prevention, service security, billing administration and compliance with its legal obligations. Billing information processed by a payment provider acting as merchant of record may also be subject to that provider's own privacy terms.

2.4 Customer is responsible for determining its role and the roles of any third parties in relation to Customer Personal Data and for ensuring that the required notices, permissions, contracts and lawful bases are in place.

3. Subject matter, duration and instructions

3.1 The subject matter, nature and purposes of processing, duration, categories of Data Subjects and types of Customer Personal Data are described in Schedule 1.

3.2 Customer instructs Sigilbase to process Customer Personal Data only as necessary to provide, secure, maintain and support the Services, and in accordance with this Agreement, Customer's use and configuration of the Services, and any further written instructions that Sigilbase accepts.

3.3 Customer's Documented Instructions expressly include submitting Events to the Services and processing those Events through ingestion, storage, hashing, chaining, sealing, verification, retention and export. Customer acknowledges that the Services are append-only by design and instructs Sigilbase to retain Sealed History indefinitely on every plan, including a free plan, irrespective of billing status, subject to clauses 8 and 9 and Applicable Data Protection Law.

3.4 Sigilbase shall not process Customer Personal Data for purposes unrelated to the Services, except where required by law. If law requires processing other than on Customer's instructions, Sigilbase shall inform Customer of that legal requirement before processing, unless the law prohibits such notice.

3.5 Sigilbase shall promptly inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. Sigilbase may suspend the affected processing while the Parties clarify or amend the instruction, but shall not be required to assess the lawfulness of Customer's instructions beyond this obligation to notify.

4. Customer obligations

4.1 Customer shall:

a. ensure that it has a lawful basis for processing and for instructing Sigilbase to process Customer Personal Data; b. provide Data Subjects with information required by Applicable Data Protection Law, including information about the nature and intended retention of Events; c. ensure that its instructions, including its instruction to retain Sealed History indefinitely, are lawful, necessary and proportionate for its purposes; d. limit Customer Personal Data in Events to what is relevant and necessary, and not submit Personal Data that it has no right to record or process; e. configure and use the Services in a manner consistent with its obligations as Controller or Processor; f. establish appropriate access controls for its accounts, API keys and credentials, and promptly revoke credentials that are compromised or no longer required; and g. notify Sigilbase promptly of any request, complaint, instruction or regulatory communication that may affect Sigilbase's processing of Customer Personal Data.

4.2 Customer shall not submit special category Personal Data, criminal-offence data, or Personal Data relating to children unless doing so is lawful, necessary for Customer's purposes, covered by suitable safeguards and specifically documented with Sigilbase in writing.

4.3 Customer remains responsible for the accuracy, lawfulness and content of Events. Sigilbase does not determine whether an Event is true, accurate, fair or lawful.

5. Sigilbase's processor obligations

5.1 Sigilbase shall:

a. process Customer Personal Data only on Documented Instructions, unless required by law; b. ensure that persons authorised to process Customer Personal Data are bound by appropriate confidentiality obligations; c. implement and maintain the technical and organisational measures described in Schedule 2, taking account of the nature, scope, context and purposes of processing and the risks to Data Subjects; d. provide reasonable assistance to Customer in responding to requests from Data Subjects and in meeting Customer's obligations under Articles 32 to 36 of the UK GDPR, taking into account the nature of processing and information available to Sigilbase; e. notify Customer without undue delay, and in any event within 48 hours after becoming aware of a Personal Data Breach affecting Customer Personal Data, in accordance with clause 6; f. make available information reasonably necessary to demonstrate compliance with this Agreement and allow audits in accordance with clause 10; g. inform Customer if Sigilbase believes that an instruction infringes Applicable Data Protection Law, in accordance with clause 3.5; and h. maintain records of processing activities to the extent required of a Processor by Applicable Data Protection Law.

5.2 Sigilbase shall not sell Customer Personal Data or use it for advertising or profiling unrelated to the provision of the Services.

5.3 Sigilbase may use Customer Personal Data in aggregated or anonymised form for service analytics, security, capacity planning and improvement only where the information is no longer Personal Data under Applicable Data Protection Law.

6. Personal Data Breaches

6.1 Sigilbase shall notify Customer of a Personal Data Breach affecting Customer Personal Data without undue delay and, in any event, within 48 hours after becoming aware of it.

6.2 The notification shall, to the extent information is then available:

a. describe the nature of the Personal Data Breach, including, where possible, the categories and approximate numbers of affected Data Subjects and Personal Data records; b. provide the name and contact details of a contact point from whom further information may be obtained; c. describe the likely consequences of the Personal Data Breach; and d. describe measures taken or proposed to address the Personal Data Breach and mitigate its possible adverse effects.

6.3 If Sigilbase cannot provide all information at once, it may provide information in phases without undue further delay.

6.4 Sigilbase shall reasonably cooperate with Customer's investigation and response. Customer is responsible for deciding whether and how to notify Data Subjects, a supervisory authority or other persons, unless applicable law requires Sigilbase to make a notification directly.

6.5 Notification of a Personal Data Breach is not an admission of fault or liability.

7. Data Subject requests and regulatory assistance

7.1 Sigilbase shall promptly notify Customer if it receives a request from a Data Subject concerning Customer Personal Data, unless prohibited by law. Sigilbase shall not respond to the request except on Customer's documented instructions or where required by law.

7.2 Taking account of the nature of the processing, Sigilbase shall provide reasonable assistance to enable Customer to respond to requests for access, rectification, erasure, restriction, objection, portability or other rights under Applicable Data Protection Law.

7.3 Customer acknowledges that the append-only design may prevent ordinary editing or deletion of accepted Events. Assistance may therefore include identifying affected records and implementing, where technically available and legally appropriate, a measure described in clause 9. Sigilbase is not required to alter or falsify the Sealed History.

7.4 Sigilbase shall provide reasonable assistance with data protection impact assessments and prior consultation with a supervisory authority, to the extent the relevant information is available to Sigilbase and the processing requires such assistance.

7.5 Sigilbase may charge reasonable, documented costs for assistance that is manifestly unfounded or excessive, or that goes materially beyond the assistance required by Applicable Data Protection Law, provided that Sigilbase first explains the basis for the charge.

8. Retention and append-only design

8.1 Customer acknowledges that accepted Events cannot be edited or deleted from the Sealed History by Customer or Sigilbase without undermining the integrity and verifiability of the record. Customer gives the express instruction described in clause 3.3 to retain Sealed History indefinitely as an inherent feature of the Services.

8.2 This instruction does not override Applicable Data Protection Law. Customer remains responsible for determining whether the submission and continued retention of Personal Data in an Event is lawful, necessary and proportionate, and for establishing and documenting an appropriate legal basis and retention rationale. The Parties shall cooperate in good faith where a Data Subject right or legal obligation requires Personal Data to be rectified, erased, restricted or otherwise made unavailable.

8.3 Sigilbase shall not stop ingestion or delete Sealed History solely because of a change in Customer's billing status. If Customer's account is restricted for non-payment under the applicable service terms, processing and retention described in this Agreement continue as instructed, subject to Applicable Data Protection Law.

8.4 On termination of the Services, Customer may export its data. Unless Customer gives a lawful instruction requiring a different outcome under clause 9, Customer instructs Sigilbase to continue retaining Sealed History indefinitely, in accordance with clause 8.1.

9. Rectification, erasure and deletion

9.1 If Customer determines that Personal Data in an Event must be rectified, erased, restricted or otherwise made unavailable, Customer shall provide Sigilbase with sufficient details to identify the relevant data and the requested outcome. The Parties shall cooperate promptly to determine and implement an appropriate lawful measure that preserves the integrity of the Sealed History to the extent possible.

9.2 Depending on the data, the Service architecture and the legal requirement, measures may include:

a. redacting or suppressing Personal Data at the Services' read layer so that it is not returned or displayed through the Services; b. destroying or disabling a cryptographic key used to make encrypted payload data intelligible, where the relevant payload is encrypted in a manner that permits targeted key destruction; c. removing or replacing data in any unsealed or separately mutable copy, where technically available and appropriate; or d. another effective technical or organisational measure agreed by the Parties.

9.3 Sigilbase shall document the measure implemented and its effect, including any residual information that remains in the Sealed History, backups, hashes, checkpoints, signatures or previously export-

ed evidence bundles. Where a measure cannot be implemented as instructed, Sigilbase shall explain the technical or legal limitation and the Parties shall consider an alternative.

9.4 Customer acknowledges that redaction at the read layer does not alter the underlying sealed record or change the result of verifying its integrity. It does not remove Personal Data from copies or evidence bundles already exported by Customer or any other recipient, or from systems outside Sigilbase's control. Customer is responsible for addressing such copies where required by Applicable Data Protection Law.

9.5 The Parties shall assess whether a measure makes the relevant Personal Data unavailable or unintelligible in the circumstances and whether any residual data, including hashes or metadata, remains Personal Data. No measure under this clause shall be treated as satisfying a legal obligation merely because it has been implemented; the Parties shall cooperate to achieve an outcome that meets the applicable requirement.

9.6 Nothing in this Agreement requires Sigilbase to falsify, rewrite or break the cryptographic integrity of Sealed History. Nothing in this clause limits a Data Subject's rights or a Controller's obligations under Applicable Data Protection Law.

10. Audits and compliance information

10.1 On Customer's reasonable written request, Sigilbase shall make available information reasonably necessary to demonstrate its compliance with this Agreement, including relevant security documentation and available third-party attestations or audit reports.

10.2 If that information is insufficient to demonstrate compliance, Customer or an independent auditor appointed by Customer may conduct an audit or inspection, subject to:

a. reasonable advance written notice, ordinarily at least 30 days; b. the auditor being bound by confidentiality obligations and not being a competitor of Sigilbase; c. the audit being conducted during normal business hours and in a manner that minimises disruption; d. the audit being limited to systems, records and processes relevant to Customer Personal Data; and e. appropriate protections for the security, confidentiality and Personal Data of Sigilbase and its other customers.

10.3 Audits shall be conducted remotely where reasonably sufficient. An on-site audit may be conducted where the nature of the concern or Applicable Data Protection Law reasonably requires it. Customer shall bear its own audit costs and Sigilbase's reasonable, documented costs of providing assistance, except to the extent an audit identifies a material breach of this Agreement by Sigilbase.

10.4 Sigilbase may satisfy a request by providing a relevant independent audit report or certification, where that reasonably addresses the requested information. This shall not remove Customer's audit rights under this clause.

10.5 Nothing in this clause limits the powers of a supervisory authority or any audit rights that cannot lawfully be limited.

11. Sub-processors

11.1 Customer gives Sigilbase general authorisation to engage Sub-processors for the processing of Customer Personal Data, subject to this clause. The current Sub-processors and their processing activities are listed in Schedule 3 and on **https://sigilbase.io/security/**.

11.2 Sigilbase shall impose on each Sub-processor, by written contract, data protection obligations that are materially equivalent to the obligations imposed on Sigilbase under this Agreement, to the extent applicable to the processing performed by that Sub-processor. Sigilbase remains responsible to Customer for the performance of each Sub-processor's data protection obligations, subject to this Agreement and Applicable Data Protection Law.

11.3 Sigilbase shall give Customer at least 30 days' notice by email before adding or replacing a Sub-processor that will process Customer Personal Data, and shall update the Sub-processor list on the security page. Where advance notice is not reasonably practicable because of an urgent security, legal or operational requirement, Sigilbase shall give notice as soon as reasonably practicable and explain the circumstances.

11.4 Customer may object to a proposed Sub-processor on reasonable data protection grounds by giving written notice within 30 days after receiving notice under clause 11.3. The Parties shall discuss the objection in good faith and seek a reasonable alternative. If they cannot resolve the objection, either Party may terminate the affected Services by written notice, without penalty for the affected Services, subject to payment of fees accrued up to termination. Sigilbase may suspend the affected processing where necessary to avoid an unlawful transfer or processing operation.

11.5 A payment provider acting as merchant of record may process billing information under its own terms and as an independent Controller. To the extent such provider processes Customer Personal Data on Sigilbase's documented instructions, it shall be treated as a Sub-processor under this clause.

12. International transfers

12.1 Sigilbase shall not transfer Customer Personal Data to a country or territory outside the United Kingdom, or permit access to it from such a place, unless the transfer complies with Applicable Data Protection Law.

12.2 Where a destination is covered by UK adequacy regulations in force at the time of transfer, Sigilbase may rely on those regulations for the transfer.

12.3 Where an adequacy regulation does not apply and a transfer is a restricted transfer under Applicable Data Protection Law, Sigilbase shall ensure that an appropriate transfer safeguard is in place before the transfer, including, as applicable:

a. the UK International Data Transfer Agreement issued by the Information Commissioner; b. the UK Addendum to the European Commission's Standard Contractual Clauses, completed and executed as required; or c. another safeguard authorised by Applicable Data Protection Law.

The relevant transfer instrument shall be completed with the required parties, transfer details, modules and annexes and shall be incorporated into the Parties' arrangements for that transfer. This Agreement does not, by itself, replace a transfer instrument that must be separately completed or executed.

12.4 Where required, Sigilbase shall conduct or support a transfer risk assessment and implement supplementary measures appropriate to the transfer. Sigilbase shall provide Customer with relevant transfer information on reasonable request, subject to confidentiality and security restrictions.

12.5 Sigilbase shall notify Customer if it becomes aware that a transfer safeguard is no longer effective or that a change in law or circumstances may require additional measures. The Parties shall cooperate to implement appropriate measures, suspend the relevant transfer or use an alternative arrangement as required by Applicable Data Protection Law.

12.6 If Customer is subject to the EU GDPR or another data protection regime that requires additional transfer safeguards, the Parties shall enter into the relevant standard contractual clauses or other lawful transfer mechanism for the relevant transfer.

13. Return, termination and deletion

13.1 This Agreement applies for as long as Sigilbase processes Customer Personal Data on Customer's behalf in connection with the Services.

13.2 Termination of the Services does not end this Agreement while Sigilbase continues to process Customer Personal Data. During that period, Sigilbase shall continue to process the data only in accordance with this Agreement and the Documented Instructions.

13.3 On termination, Customer may export Customer Personal Data using the available export functionality. Customer's instruction is that Sigilbase shall continue to retain Sealed History indefinitely, subject to clauses 8 and 9, unless the Parties agree a lawful alternative or Applicable Data Protection Law requires otherwise.

13.4 Personal Data outside the Sealed History that is not required for ongoing service operation, security, legal compliance or the documented retention instruction shall be deleted or returned in accordance with Customer's lawful instructions and Sigilbase's applicable retention practices. Sigilbase shall delete or render inaccessible such data when it is no longer required for the relevant purpose, subject to legal retention requirements.

13.5 If Sigilbase is required by law to retain Customer Personal Data after termination, it shall notify Customer unless prohibited by law, restrict processing to the legally required purpose and retain the data only for the legally required period.

13.6 Copies of Customer Personal Data in routine backups may remain until overwritten in accordance with Sigilbase's ordinary backup cycle, provided they remain protected, are not restored or

otherwise processed except for recovery, security or legal purposes, and are deleted or overwritten in the ordinary course.

14. Liability

14.1 The liability provisions of the applicable Terms of Service or other governing services agreement apply to liability arising under this Agreement, to the extent they are lawful and effective. If those terms contain no applicable liability limit or are otherwise unenforceable, liability shall be determined under applicable law.

14.2 Nothing in this Agreement limits or excludes any liability that cannot lawfully be limited or excluded, or any rights or remedies available to Data Subjects under Applicable Data Protection Law.

14.3 Each Party's liability to a Data Subject under Article 82 of the UK GDPR shall be determined in accordance with that Article and Applicable Data Protection Law.

14.4 Nothing in this Agreement makes one Party responsible for the other Party's independent failure to comply with its obligations as a Controller or Processor.

15. General

15.1 **Order of precedence.** In the event of conflict:

a. any applicable UK IDTA, UK Addendum or other transfer instrument prevails in relation to the relevant international transfer; b. this Agreement prevails over the Terms of Service, an order form or other service terms in relation to the processing of Customer Personal Data; and c. the Terms of Service or other service terms continue to apply to all other matters.

15.2 **Incorporation and acceptance.** This Agreement is incorporated into the agreement governing Customer's use of the Services when Customer signs this Agreement, accepts it electronically, or uses the Services after being given access to it. Where Customer's use of the Services is governed by an existing Terms of Service, this Agreement supplements those terms.

15.3 **Amendments.** An amendment to this Agreement must be in writing and agreed by both Parties, except that Sigilbase may update its Sub-processor list in accordance with clause 11. A change required by law or to maintain an effective transfer safeguard may be made on notice to Customer to the extent reasonably necessary.

15.4 **Severability.** If any provision of this Agreement is held invalid or unenforceable, the remaining provisions shall continue in effect. The Parties shall replace the affected provision with a valid provision that most closely reflects its original purpose.

15.5 **Notices.** Notices under this Agreement must be in writing and sent to the relevant Party's account contact or the email addresses set out below, or to any replacement address notified in writing.

15.6 **Governing law and jurisdiction.** This Agreement and any non-contractual obligations arising out of or in connection with it are governed by the laws of England and Wales. The courts of England and Wales shall have exclusive jurisdiction, subject to any mandatory rights of a Data Subject or supervisory authority.

Schedule 1 — Details of processing

1. Subject matter

Processing of Customer Personal Data through the Sigilbase audit-log service.

2. Nature and purpose of processing

Processing necessary to receive Events submitted by or on behalf of Customer; store and organise them; hash and chain them using SHA-256; seal them into Merkle checkpoints signed with Ed25519 keys; support verification; provide access and export functionality; retain Sealed History; and maintain, secure and support the Services.

3. Duration

For the term of the Services and thereafter for as long as Customer instructs Sigilbase to retain Sealed History, including indefinitely, subject to clauses 8, 9 and 13 and Applicable Data Protection Law. Other Customer Personal Data shall be retained only for as long as needed for the applicable service, security, legal or operational purpose.

4. Categories of Data Subjects

Depending on Customer's use of the Services:

- Customer's end users, customers and business contacts;
- Customer's employees, contractors, administrators and authorised users;
- individuals identified as actors in Events;
- individuals whose actions or decisions are recorded in Events;
- individuals interacting with automated systems or AI agents whose inputs, outputs or decisions are recorded; and
- any other individuals whose Personal Data Customer chooses to include in an Event.

5. Types of Personal Data

Depending on Customer's use of the Services:

- names, email addresses and other contact details;
- user, account, organisation, device, transaction and other identifiers;
- actor identifiers, role or affiliation information;
- timestamps and related event metadata;
- action and event descriptions;

- Personal Data contained in an Event payload, including any information Customer chooses to record; and
- technical or audit metadata associated with an Event.

Customer shall not submit special category Personal Data, criminal-offence data or Personal Data relating to children except as permitted under clause 4.2 and documented with Sigilbase.

6. Processing operations

Collection, receipt, recording, structuring, storage, adaptation, retrieval, consultation, hashing, chaining, sealing, verification, disclosure by transmission or export at Customer's direction, restriction, read-layer suppression, backup and deletion or return where applicable.

7. Documented Instructions

Customer instructs Sigilbase to process Customer Personal Data to provide the Services described in this Agreement, including indefinite retention of Sealed History as an append-only record, subject to the lawful measures and limitations in clauses 8, 9 and 13.

Schedule 2 — Technical and organisational measures

Sigilbase shall maintain technical and organisational measures appropriate to the risk, including measures consistent with the following:

1. **Encryption in transit and at rest.** Protect Personal Data during transmission using encryption and protect stored Personal Data using encryption at rest, including encrypted backups.
2. **Access controls.** Restrict access to systems and Customer Personal Data to authorised personnel with a business need, using appropriate authentication and access-management controls.
3. **Payload access restrictions.** Redact Event payload contents from operator tooling, except where access is specifically required and authorised for support, security or legal purposes.
4. **Cryptographic integrity.** Hash Events using SHA-256, chain each Event to the preceding Event, and seal batches in Merkle checkpoints signed using Ed25519 keys.
5. **Signing-key management.** Restrict access to signing keys, protect them against unauthorised use, and maintain appropriate key-management procedures, including procedures for key rotation or revocation where applicable.
6. **Availability and resilience.** Maintain appropriate backup and recovery measures, including encrypted backups, and procedures intended to restore access to the Services following an incident.
7. **Security monitoring and incident response.** Maintain procedures to identify, assess, manage and respond to security incidents affecting Customer Personal Data.
8. **Confidentiality and training.** Require personnel authorised to process Customer Personal Data to be subject to confidentiality obligations and receive appropriate security and data protection guidance.

9. **Sub-processor controls.** Conduct appropriate due diligence and impose contractual data protection and security obligations on Sub-processors.
10. **Data minimisation and retention controls.** Process Customer Personal Data in accordance with Customer's Documented Instructions and the append-only retention design, and support read-layer redaction or other agreed measures where technically available and legally appropriate.

Schedule 3 — Current Sub-processors

The following providers are identified in Sigilbase's current public Sub-processor information. Their precise processing locations and functions may vary by service configuration and are maintained on **https://sigilbase.io/security/**.

Provider	Function and processing
OVHcloud	Hosting of the Services in the United Kingdom and encrypted backups in the United Kingdom and France.
Bunny.net	DNS, TLS and content delivery; may process technical connection data required to deliver and protect the Services.
Sweego	Transactional and support email processing, including contact details and message information required to send or respond to service communications; processing in France.
Paddle.com	Payment processing and merchant-of-record services. Paddle may process billing information, such as billing name, email address, plan and invoice status. Paddle is not authorised to process Event payloads under this Agreement unless separately notified and authorised as a Sub-processor. Where Paddle acts as an independent Controller for its merchant-of-record activities, its own terms and privacy information apply.

Sigilbase shall notify Customer of changes to this list in accordance with clause 11.3. Relevant processing locations and transfer safeguards shall be provided on the security page or on reasonable request.

Signatures

The Parties agree to this Agreement as of the Effective Date.

For Sigilbase Ltd

Name: [Name]
Title: [Title]

Signature: _____
Date: [Date]
Notice email: [Email address]

For [Customer legal name]

Name: [Name]
Title: [Title]
Signature: _____
Date: [Date]
Notice email: [Email address]