# RFP Vendor Security Questions

Please fill this to comply with Acme Inc security

**Vendor Name:**

**Date:   
Contact Name:   
Email:   
Address:**

**Data Processing and Privacy Compliance**

1. How does your product ensure compliance with global privacy requirements, including GDPR, when processing Customer Data?

Instabase ensures compliance with global privacy requirements, including GDPR, when processing Customer Data through several measures: 1. \*\*Data Processing Roles\*\*: Instabase predominantly acts as a Data Processor, meaning it processes data under the instructions of its Customers, who control the data. However, in certain situations, such as responding to support requests or processing personal data for marketing activities, Instabase may act as a Data Controller. 2. \*\*Data Processing Addendum (DPA)\*\*: Instabase provides GDPR-ready terms in its Data Processing Addendum, which includes the EU's Standard Contractual Clauses (SCCs) and the UK International Data Transfer Addendum to address data transfer requirements. 3. \*\*Security Practices\*\*: Instabase reviews its security practices to ensure that Customer Data is adequately protected through appropriate technical and organizational measures in accordance with GDPR. This includes encryption of data in transit and at rest using industry-standard algorithms. 4. \*\*Privacy by Design\*\*: Instabase embeds privacy by design principles within the organization through formal processes. 5. \*\*Sub-processor Due Diligence\*\*: Instabase conducts appropriate due diligence on Sub-processors and updates contracts with them to ensure they are GDPR-compliant. 6. \*\*Data Subject Rights\*\*: Instabase ensures that users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of their personal data. Requests can be made via email or mail. 7. \*\*Data Transfer Impact Assessment\*\*: Instabase has implemented appropriate safeguards to ensure that Customer Personal Data remains protected whenever it is processed by Affiliates and Subprocessors, including entering into data processing agreements and transfer mechanisms such as the SCCs. 8. \*\*Certifications and Compliance\*\*: Instabase maintains third-party validations to demonstrate its commitment to information security and compliance with privacy requirements. 9. \*\*Incident Response\*\*: Instabase has an incident response plan in place to inform Customers without undue delay, and within 72 hours, upon becoming aware of a Customer Data Breach. These measures collectively ensure that Instabase complies with global privacy requirements, including GDPR, when processing Customer Data.

**Data Security Measures**

1. What technical and organizational security measures has your product implemented to protect Customer Data from unauthorized access, use, or disclosure?

Instabase has implemented a range of technical and organizational security measures to protect Customer Data from unauthorized access, use, or disclosure. These measures are detailed in several documents, including the Information Security Addendum, Customer Data Protection Agreement, and other related policies. Here are the key measures: ### Technical Security Measures: 1. \*\*Encryption\*\*: - Data at rest in production datastores is encrypted using AES-256. - Data in transit between Customers and Instabase is encrypted using TLS version 1.2. - Cryptographic standards are reviewed periodically, with technologies and ciphers updated according to assessed risk and market acceptance. 2. \*\*Access Controls\*\*: - Industry best practices for authenticating and authorizing personnel access. - Use of third-party secrets management services for managing accounts. - Network security policies and firewalls configured for least-privilege access. - Services' logs are monitored for security and availability. 3. \*\*Virtual Machine/Container Hardening\*\*: - Virtual assets are deployed through code to ensure consistent configuration. - Established configuration baselines are reviewed and approved. - Changes to the configuration baseline must follow the approved change management process. 4. \*\*Physical Security\*\*: - Physical barrier controls including locked doors and gates. - 24-hour on-site security guard staffing. - 24-hour video surveillance and alarm systems. - Access control systems requiring photo-ID badges for entry. - Visitor identification and sign-in protocols. - Logging of facility exits and entries. ### Organizational Security Measures: 1. \*\*Security Certifications and Attestations\*\*: - SOC 2 Type 2 (Trust Service Principles: Security, Availability, and Confidentiality). - Health Insurance Portability and Accountability Act (HIPAA) - Attestation of Compliance. 2. \*\*Policies and Procedures\*\*: - Implementation of appropriate technical and organizational measures designed to protect Customer Personal Data from breaches. - Regular security and vulnerability testing, including third-party penetration tests. - Continuous updates to the security program and strategy to address evolving security threats. 3. \*\*Incident Response\*\*: - Procedures to inform customers without undue delay, and within 72 hours, upon becoming aware of a Personal Data Breach. - Measures to remediate breaches and provide timely information about the nature of the breach. 4. \*\*Data Protection Impact Assessments\*\*: - Cooperation and assistance to comply with obligations under applicable data protection laws, including conducting data protection impact assessments. 5. \*\*Training and Awareness\*\*: - Security and Safety training for vendors working on premises as part of the induction and at a minimum every 12 months. These measures collectively ensure that Instabase maintains a robust security posture to protect Customer Data from unauthorized access, use, or disclosure.

**Data Transfer Mechanisms**

1. Can you provide details on the safeguards your product has in place for cross-border data transfers, particularly in jurisdictions without an adequacy decision by the European Commission?

Instabase has implemented several safeguards for cross-border data transfers, particularly to jurisdictions without an adequacy decision by the European Commission. These safeguards include: 1. \*\*Standard Contractual Clauses (SCCs)\*\*: Instabase uses SCCs approved by the European Commission and the British Information Commissioner's Office for the transfer of personal data. Depending on the circumstances, they use the appropriate SCC module(s) for Controller-Controller, Controller-Processor, or Processor-Processor data transfers. These SCCs are available upon request. 2. \*\*Technical, Organizational, and Contractual Measures\*\*: Instabase has implemented a comprehensive security program designed to protect customer data. This includes rigorous contractual commitments to security, confidentiality of processing, international data transfers, and cooperation with data subject rights. 3. \*\*Internal Policies and Procedures\*\*: Instabase has robust internal policies and procedures to address government access requests and ensure that customer data remains protected wherever it is processed. 4. \*\*Data Processing Addendum (DPA)\*\*: Instabase's DPA incorporates the European Commission's SCCs for transfers of customer data from the EEA and Switzerland, and the SCCs and UK International Data Transfer Addendum for transfers from the UK. 5. \*\*Transfer Impact Assessments (TIAs)\*\*: In light of the "Schrems II" decision, Instabase assists customers in conducting TIAs to ensure that data continues to be afforded an essentially equivalent level of protection to that guaranteed by the GDPR. This involves assessing the recipient country's laws and practices, particularly regarding surveillance. These measures collectively ensure that personal data receives an adequate level of security regardless of the country in which it is processed.

**Subprocessor Management**

1. How does your product manage its subprocessors to ensure they provide a similar level of data protection and information security? Can you provide a list of current subprocessors and their compliance certifications?

### Management of Subprocessors Instabase ensures that its subprocessors provide a similar level of data protection and information security through several measures: 1. \*\*Written Agreements\*\*: Subprocessors are bound by written agreements that include data protection and security measures no less protective than those in the agreement between Instabase and its customers. (Customer Data Protection Agreement, Section 4.6(a)) 2. \*\*Liability\*\*: Instabase remains liable for any breach of the Data Protection Agreement caused by its subprocessors, ensuring accountability. (Customer Data Protection Agreement, Section 4.6(b)) 3. \*\*Notification and Objection\*\*: Customers are notified in advance of any intended additions or replacements to subprocessors. Customers have the right to object to new subprocessors based on reasonable data protection concerns. (Customer Data Protection Agreement, Section 4.6(c)) 4. \*\*Vendor Security Assessments\*\*: All third-party vendors undergo a formal vendor assessment process maintained by Instabase's Security team. This includes periodic reviews in light of Instabase's security and business continuity standards. (Questionnaire History, Page 17) 5. \*\*Continuous Monitoring\*\*: Instabase aggregates system logs for security and general observability from a range of systems to facilitate detection and response. (Questionnaire History, Page 17) ### List of Current Subprocessors and Their Compliance Certifications Instabase utilizes the following subprocessors: 1. \*\*Amazon Web Services, Inc.\*\* - \*\*Purpose\*\*: Cloud Service Provider - \*\*Entity Country\*\*: United States, European Union, and United Kingdom - \*\*Security and Compliance Validations\*\*: - ISO 9001 - ISO 27001 - ISO 27017 - ISO 27018 - SOC 1/ISAE 3402 - SOC 2 - SOC 3 - FISMA - DIACAP - FedRAMP - PCI DSS Level 1 - \*\*Additional Details\*\*: [AWS Security and Compliance](https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html) For more detailed and updated information, customers can refer to Instabase's subprocessors list available at [Instabase Subprocessors](https://instabase.com/trust/subprocessors).

**Data Retention and Deletion**

1. What are your product’s policies regarding the retention and deletion of Customer Data? How can customers request the deletion of their data?

Instabase's policies regarding the retention and deletion of Customer Data are as follows: ### Retention of Customer Data: 1. \*\*General Retention Periods\*\*: - \*\*Business contact information, account log-in credentials, payment information, marketing information, inquiries and feedback\*\*: Data is deleted upon request. - \*\*Log data, usage data, location data\*\*: For SaaS, data is retained for one year from the creation date. For customer-hosted environments, retention is managed by the customer. - \*\*Customer Content (identification and contact data, financial data, health data)\*\*: If the customer leverages Instabase-provided storage, the default retention period is defined by the customer. For customer-hosted environments, retention is managed by the customer. 2. \*\*Administrative Data\*\*: - Administrative data required for legitimate business purposes (e.g., billing records, audit logs, taxes) may be retained even after a deletion request. 3. \*\*Backup Data\*\*: - Backups of customer data must be retained for no longer than 90 days, after which they must be destroyed unless an exception applies. ### Deletion of Customer Data: 1. \*\*Customer Requests\*\*: - Customers can request the deletion of their data by emailing privacy@instabase.com. Upon such a request, Instabase will purge the Customer Data from its systems, except for administrative data required for legitimate business purposes. 2. \*\*Post-Termination\*\*: - Upon a customer's request following the termination or expiry of the agreement, Instabase will return or delete all Customer Personal Data in its possession or control, except where retention is required by **applicable law. Instabase will issue a certificate of deletion upon the customer's request. ### How Customers Can** Request Deletion: - Customers can request the deletion of their data by emailing privacy@instabase.com. Instabase will respond to these requests in accordance with their obligations under applicable privacy and data protection laws. For more detailed information, customers are encouraged to refer to the Data Retention and Disposal Policy and the Customer Data Protection Agreement (DPA).

**Access Control**

1. Who within your company has access to Customer Data, and for what purposes? How does Instabase ensure that access is appropriately controlled and monitored?

### Access to Customer Data \*\*Who within Instabase has access to Customer Data and for what purposes:\*\* 1. \*\*Customer Administrators:\*\* - \*\*Purpose:\*\* - Modify and control certain administrative information. - Provision customer's account. - Understand customer's use of product and functionality. - Train and improve machine learning models and algorithms for customers' benefit. 2. \*\*Instabase Personnel:\*\* - \*\*Purpose:\*\* - Billing/invoicing. - Supporting the service in accordance with Instabase's data access and security controls process. - Understand customer's use of product and functionality. - Train and improve machine learning models and algorithms for customers' benefit. ### Ensuring Controlled and Monitored Access \*\*How Instabase ensures that access to Customer Data is appropriately controlled and monitored:\*\* 1. \*\*Principle of Least Privilege:\*\* - Access to services follows the principle of least privilege, meaning only personnel whose job function involves supporting the delivery of services are credentialed to the services environment. 2. \*\*Access Authorization:\*\* - Data access is authorized only to personnel whose job function requires such access. 3. \*\*Logging and Auditing:\*\* - All activities of Instabase personnel at the services layer, including its infrastructure, are logged and auditable. 4. \*\*Access Reviews:\*\* - Access reviews are conducted quarterly by the system owner and the security team to ensure continuous compliance. This helps maintain a technology environment where employees and contingent workers have minimum access based on specific business needs and security requirements. 5. \*\*Encryption:\*\* - Data at rest in production datastores is encrypted using AES-256. - Data in transit between customers and Instabase is encrypted using TLS version 1.2. 6. \*\*Endpoint Management:\*\* - Endpoint management of corporate workstations and personnel-owned mobile devices via industry-standard services and associated policies. - Automatic application of security configurations to workstations. 7. \*\*Password and Security Policies:\*\* - Password requirements for workstations align with CIS MacOS Benchmark, including minimum length, complexity, and forced changes of password. - Use of Okta as an IDP to manage access permissions, applications, and policies across all vendors that Instabase uses, with MFA enforced through Okta. 8. \*\*Support Access:\*\* - By default, Instabase does not have access to the services. If the customer requires support or assistance, they can either request a screen-sharing session or provision Instabase's authorized personnel with access via the customer's identity provider. 9. \*\*Vendor Security Assessments:\*\* - All third-party vendors undergo a formal vendor assessment process maintained by Instabase's Security team, including periodic reviews in light of Instabase's security and business continuity standards. These measures collectively ensure that access to customer data is controlled and monitored effectively.

**Incident Response**

1. What is your company’s protocol for responding to data breaches or security incidents involving Customer Data?

Instabase's protocol for responding to data breaches or security incidents involving Customer Data is detailed in several documents. Here are the key points: 1. \*\*Notification\*\*: - Instabase will inform the customer without undue delay, and in any event within 72 hours, upon becoming aware of a Personal Data Breach (Customer Data Protection Agreement, Section 4.4; Instabase Data Privacy Sheet, Page 11). - Instabase will provide timely information about the nature of the breach as soon as it becomes known or available (Customer Data Protection Agreement, Section 4.4; Instabase Data Privacy Sheet, Page 11). 2. \*\*Remediation\*\*: - Instabase will take necessary and reasonable measures to remediate the breach (Customer Data Protection Agreement, Section 4.4; Instabase Data Privacy Sheet, Page 11). 3. \*\*Cooperation\*\*: - Instabase will provide reasonable cooperation and assistance to enable the customer to comply with its obligations under applicable data protection laws, including notifying relevant supervisory authorities and/or affected data subjects (Customer Data Protection Agreement, Section 4.4; Instabase Data Privacy Sheet, Page 11). 4. \*\*Incident Response Plan\*\*: - Instabase maintains a Security Incident Response Plan that provides a systematic process for responding to and resolving security incidents (Questionnaire History, Page 21; Security Incident Response Plan, Page 12). - The plan includes steps for internal analysis, customer communication, containment, remediation, and post-incident review (Security Incident Response Plan, Pages 16-17). 5. \*\*Post-Breach Response\*\*: - Any post-breach response, including external and internal communications, notifications, and further inquiries, will depend on the assessment and priority of the security incident (Security Incident Response Plan, Page 12). - The final phase involves reviewing and identifying lessons learned to update or expand the incident response plan or relevant playbooks (Security Incident Response Plan, Page 13). 6. \*\*Retention\*\*: - Documentation related to a security investigation will be retained as long as required by applicable laws and regulations (Security Incident Response Plan, Page 12). These protocols ensure that Instabase responds promptly and effectively to data breaches or security incidents involving Customer Data, while also complying with legal requirements and maintaining transparency with customers.

**Data Portability**

1. How can your company export their data from Instabase's systems? What formats and methods are available for data export?

To export data from Instabase's systems, your company can utilize an Application Program Interface (API). This capability allows the export of all Customer Data stored in Instabase's system. The specific formats and methods for data export are not detailed in the provided documents, but the use of an API suggests that the data can be programmatically accessed and exported, which typically supports various data formats depending on the API's design and the data types involved. For more detailed information on the exact formats and additional methods available, it would be best to consult Instabase's technical documentation or contact their support team directly.

**Support and Troubleshooting**

1. What types of data does Instabase collect and process in connection with support queries? How is this data used to diagnose and resolve issues?

Instabase collects and processes the following types of data in connection with support queries: 1. \*\*Business Contact Information\*\*: User's name, job title, organization, email address, and company. 2. \*\*Account Log-in Credentials\*\*: User's email or username and password. 3. \*\*Troubleshooting and Support Data\*\*: Information provided in connection with support queries, including the content of communications with Instabase. 4. \*\*Log Data\*\*: Information stored in log files, such as IP address, browser or device type, operating system, domain name, device identifiers, and referring website addresses. 5. \*\*Usage Data\*\*: Data related to how the services are used. 6. \*\*Location Data\*\*: Information about the geographical location of the user. This data is used to diagnose and resolve issues in the following ways: - \*\*Understanding, Diagnosing, and Resolving Issues\*\*: The data helps Instabase understand the nature of the problem, diagnose the root cause, and resolve issues with the services. - \*\*Analyzing Usage and Trends\*\*: By analyzing usage patterns and trends, Instabase can identify opportunities for improvement and development of the services. - \*\*Developing New Features\*\*: Personal information, in a de-identified form, may be used to develop new features, capabilities, or products. - \*\*Communicating with Users\*\*: Instabase uses the data to communicate with users, respond to inquiries, and provide updates about the services. These processes ensure that Instabase can effectively support its users and continuously improve its services.

**Marketing and Communication**

1. How does your company handle Customer Data for marketing purposes? What options do customers have to manage their marketing preferences and opt-out of communications?

### Handling Customer Data for Marketing Purposes Instabase processes customer data for marketing purposes under specific conditions. The data processed includes business contact information, account log-in credentials, payment information, marketing information, inquiries and feedback, log data, usage data, and location data. The purposes for processing this data include: - Sending marketing communications in accordance with customer preferences. - Conducting marketing research to improve the effectiveness of marketing campaigns. - Displaying advertising and relevant offers on third-party websites based on customer activities and interests. - Conducting research, contests, surveys, and sweepstakes. ### Managing Marketing Preferences and Opting Out Customers have several options to manage their marketing preferences and opt-out of communications: 1. \*\*Opt-Out of Marketing Communications\*\*: Customers can opt-out of receiving marketing communications by following the instructions provided in the communications or by contacting Instabase directly. 2. \*\*Cookie Management\*\*: Customers can manage their cookie preferences, which may include opting out of certain types of cookies used for targeted advertising. This can be done through browser settings or by using tools provided by third-party advertising partners. 3. \*\*Data Subject Rights\*\*: Customers have the right to access, correct, delete, or object to the processing of their personal information. They can also withdraw consent for processing where consent is the legal basis. These rights can be exercised by contacting Instabase at privacy@instabase.com. 4. \*\*California Residents\*\*: Under the CCPA and CPRA, California residents have additional rights, including the right to opt-out of the sale of their personal information. Instabase does not sell personal data, but residents can exercise their rights by contacting Instabase via email or mail. For more detailed information, customers can refer to the Services Privacy Policy and the Data Privacy Sheet available on the Instabase Trust Center