Sembi Affiliates Data Processing Terms

(for the Customer-Facing DPA)

Details of Processing of Xblend Software, LDA

a. **Address: –**
   Rua Cidade de Córdova, n.º 2 A, Alfragide, 2610 038 AMADORA, Portugal
b. **Type of Services provided by the Sembi Affiliate involving the Processing of Customer Personal Data: –**
   i. Xray is a market-leading test management solution for Jira users, providing an intuitive and comprehensive test management experience that is customizable for a user's specific QA needs.
   ii. Xporter is a reporting app for Jira that exports single or multiple issues to Word, Excel, and PDF for ad hoc or scheduled instances. Exports are based on a specific issue or predetermined Jira filters with the ability to customize reports or utilize an extensive range of templates.
c. **Data Protection Officer (DPO) Details: –**
   VeraSafe, LLC
   experts@verasafe.com
   100 M Street S.E., Suite 600, Washington, D.C . 20003 USA
d. **EU Data Protection Representative: –**
   n/a
e. **UK Data Protection Representative: –**
   VeraSafe United Kingdom Ltd.
   37 Albert Embankment London SE1 7TL United Kingdom
   Contact form: https://verasafe.com/public-resources/contact-data-protection-representative
f. **Subject matter and duration: –**
   The subject matter and duration of the Processing of Customer Personal Data are set forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.
g. **Nature and Purpose of Processing: –**
   The nature and purpose of the Processing of Customer Personal Data are set forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.

h. **Further Processing: –**
   No further Processing of Customer Personal Data beyond the Processing necessary for the provision of the Services is allowed.

i. **Categories of Data Subjects: –**
   Data subjects may include Customer's representatives, such as employees, contractors, collaborators, partners. Data subject may also include individuals attempting to communicate or transfer Customer Personal Data to users of the Services.

j. **Categories of Customer Personal Data: –**
   The Categories of Customer Personal Data that Customer authorizes and requests that Xblend Processes include but are not limited to: Personal contact information such as full name, address, mobile number, email address, details including employer name, job title and function, Atlassian account identifiers and business contact details, goods or services provided, test cases and their execution, user's full name and email address when the In-App Chat Support feature is accessed, IP addresses, and interest data.

k. **Special Categories of Customer Personal Data to be Processed (if applicable) and the applied restrictions to the Processing of these Special Categories of Customer Personal Data: –**
   n/a

l. **Categories of third-party recipients to whom the Customer Personal Data may be disclosed or shared by Sembi: –**
   Subprocessors; and other Sembi Affiliates, if applicable.

m. **Frequency of the Transfer of Customer Personal Data: –**
   The frequency of the transfer of Customer Personal Data is determined by the Customer. Customer Personal Data is transferred each time that the Customer instructs Xblend to Process Customer Personal Data.

n. **Maximum data retention periods, if applicable: –**
   The retention period of the Customer Personal Data is generally determined by the Customer, and is subject to the term of the DPA and the Main Agreement, respectively, in the context of the contractual relationship between Xblend and the Customer.

o. **The basic Processing activities to which Customer Personal Data will be subject include, without limitation: –**
   Collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Services to Customer in accordance with the terms of the Main Agreement

p. **The following is deemed an instruction by the Customer to Xblend to Process Customer Personal Data: –**
   i. Processing in accordance with the Main Agreement.

ii. Processing initiated by Data Subjects in their use of the Services.

iii. Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Main Agreement.

q. **List of Xblend's Subprocessors available at** https://www.ideracorp.com/Legal/XBlend/Subprocessors

r. **Description of technical and organizational security measures implemented by the Xblend: –**

i. Measures of pseudonymization and encryption of Customer Personal Data:

a. Encryption of the transferred Customer Personal Data in transit using the Transport Layer Security (TLS) protocol version 1.2 or higher with a minimum of 128-bit encryption;

ii. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:

a. Restriction of logical access to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access;

b. Active monitoring and logging of network and database activity for potential security events, including intrusion;

c. Regular scanning and monitoring of any unauthorized software applications and IT systems for vulnerabilities of Xblend;

d. Firewall protection of external points of connectivity in Data Importer's network architecture; and

e. Expedited patching of known exploitable vulnerabilities in the software applications and IT systems used by Xblend.

iii. Measures for ensuring the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident:

a. Services are hosted on Amazon Web Services to ensure high availability and scalability;

b. Monitoring checks are made in order to detect performance and availability issues; and

c. Backups are made every three hours and there is documentation to restore systems.

iv. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing

a. Compliance program to track security controls;

b. Private bug bounty program exists, and penetration tests are being done regularly; and

    c. Vulnerabilities are being addressed as they are being discovered.

v. Measures for user identification and authorization:
    a. The applications are using JWT (JSON Web Tokens) to authenticate and authorize users; and
    b. Access controls are guaranteed by Atlassian permissions and custom application permissions.

vi. Measures for the protection of data during transmission:
    a. Connections from public networks to Xblend services are encrypted using TLS 1.2 with a minimum 128-bit encryption.

vii. Measures for the protection of data during storage:
    a. Data is stored using a leading service that ensures high performance, scalability, availability and security by default; and
    b. Access is role based and reviewed regularly.

viii. Measures for ensuring physical security of locations at which Customer Personal Data are processed:
    a. Restriction of physical to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access; and
    b. Physical security is part of the service provided by Amazon Web Services and DigitalOcean.

ix. Measures for ensuring events logging:
    a. Active monitoring and logging of network and database activity for potential security events, including intrusion.

x. Measures for ensuring system configuration, including default configuration:
    a. Applications are using standard configurations and they are scanned against best practices and vulnerabilities.

xi. Measures for internal IT and IT security governance and management:
    a. Users are created with only required permissions and access roles;
    b. Permissions are reviewed and removed regularly; and
    c. Users are required to use MFA and secure services.

xii. Measures for certification/assurance of processes and products:
    a. Xblend currently holds a SOC 2 Type 2 certification.

xiii. Measures for ensuring data minimization:
    a. Data minimization is guaranteed during the design and implementation processes.

xiv. Measures for ensuring data quality:

a. Customer is responsible for data quality and accuracy since the data is provided by the Customer; and
b. Form validations are made to validate some fields.

xv. Measures for ensuring limited data retention:
a. Different policies can apply depending on the type of data;
b. Temporary data is automatically deleted using a TTL (Time to live); and
c. Automated process to ensure data retention no more than 60 days after the uninstallation.

xvi. Measures for ensuring accountability:
a. Documentation about how personal data is processed.

xvii. Measures for allowing data portability and ensuring erasure:
a. In-product feature to allow data portability that securely transmits the data structured in a readable format; and
b. A process for deleting Customer Personal Data by making a support request.

xviii. Other:
a. Internal policies establishing that

xix. Where Xblend is prohibited by law from notifying Data Exporter of an order from a public authority for transferred Customer Personal Data, Xblend shall take into account the laws of other jurisdictions and use best efforts to request that any confidentiality requirements be waived to enable it to notify the competent Supervisory Authorities;

xx. Xblend must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred Customer Personal Data;

xxi. Xblend shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid; and

xxii. If Xblend is legally required to comply with an order, it will respond as narrowly as possible to the specific request.