Sembi Affiliates Data Processing Terms
(for the Customer-Facing DPA)

Details of Processing of Gurock Software GmbH

a. **Address: –**
Südliche Ringstraße 175, 63255 Langen (Hessen), Germany

b. **Type of Services provided by the Sembi Affiliate involving the Processing of Customer Personal Data: –**
   i. TestRail by Gurock is a comprehensive web-based (i.e. Software as a Service) test case management tool used by leading development teams in the Fortune 500. TestRail allows users to efficiently manage, track, and organize software testing efforts to boost testing productivity and increase the spd and soundness of software development.

c. **Data Protection Officer (DPO) Details: –**
VeraSafe, LLC, a Delaware limited liability company.
experts@verasafe.com

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 unless required under applicable law.

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 Gurock 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, identification numbers and business contact details; goods or services provided; 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 Gurock 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 Gurock 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 Gurock 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 Gurock's Subprocessors available at**
https://www.ideracorp.com/Legal/Gurock/Subprocessors

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

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

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

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

    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. Advanced Backup System (Tenant Backups/Restores. RDS Backups/Snapshot/Restores.)

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 consisting of internal and external (independent third-party) audits to track data privacy and security controls;

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

v. Measures for user identification and authorization:

       a. Users are provided passwords to enter the application and these passwords are stored hashed inside the database

       b. There is a custom application permission system to guarantee that users have access only to data that is appropriate to their access level

vi. Measures for the protection of data during transmission:

       a. SSL

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.

       c. Annual risk assessment is performed for all vendors with access to Customer Personal Data.

viii. Measures for ensuring physical security of locations at which Customer Personal Data are processed:

       a. Annual risk assessment is performed for all vendors with access to Customer Personal Data.

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

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 use 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 using the principle of least privilege with only required permissions and access roles;
  b. Permissions are reviewed and removed regularly.
xii. Measures for certification/assurance of processes and products:
  a. Gurock is SOC-2 Type 2 certified.
  b. Gurock performs an annual penetration test with an independent third-party assessor.
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. Data is retained only for as long as the customer agreement is active, unless otherwise requested by customer.
xvi. Measures for ensuring accountability:
  a. Documentation about how personal data is processed.
  b. Annual reviews and testing to ensure policies and procedures are operating effectively.
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 formal Compliance process for deleting Customer Personal Data by making a request to compliance@gurock.io.