Data Processing Addendum (“Addendum”)

Between _____ ("**Company**“)

and **TestMonitor**

(“**TestMonitor**” meaning the legal entity with which the **Company** has a contractual relationship according to the Framework Agreement, as defined below. Company and TestMonitor also referred to as a “**Party**” and collectively as the “**Parties**”)

1. Background

The Parties have agreed to the Terms of Service posted at https://www.testmonitor.com/terms-of-service (“**Framework Agreement**”) according to which TestMonitor has agreed to provide certain services to Company (hereinafter the “**Services**”).

When providing the Services, TestMonitor may collect, process, and gain access to personal data of individuals on behalf of Company. From a data protection perspective, Company will be the data controller, and TestMonitor will be the data processor.

This Data Processing Addendum specifies the data protection obligations of the Parties under the Framework Agreement. It applies to all activities performed by TestMonitor in connection with the Framework Agreement in which TestMonitor, its staff, or a third party acting on behalf of TestMonitor encounters personal data of individuals.

If there is a conflict between the terms of the Framework Agreement and those of this Data Processing Addendum, the provisions of this Addendum will prevail.

2. TestMonitor’s Obligations

1. TestMonitor will collect and process personal data in connection with the Framework Agreement only for the purpose of fulfilling the Framework Agreement. TestMonitor will carry out the data processing operations in accordance with the Framework Agreement as well as any written instructions received from Company that does not conflict with the provisions of this Data Processing Addendum or the Framework Agreement.

2. Personal data to which TestMonitor may receive access concern the following data subjects (“**Data Subjects**”):
    i. Company’s software testing data, like requirements, risks, use cases, test cases, test results, issues, IP address and payment data.
    ii. Any third party with whom TestMonitor interacts or is requested to interact in connection with the provision, operation, or maintenance of the Services on behalf of Company.
    iii. Any other individuals for which Company enters personal data or information into the Service.

    TestMonitor will not have any knowledge or control over the categories or identities of the Data Subjects whose Personal Data Company may elect to record or upload into the Service, except as provided in the Framework Agreement.

3. The data processing activities will generally include the following categories of personal data ("**Personal Data**"):
    i. Name, street address, email address, phone number, other contact information, company name, title;
    ii. Customer history;
    iii. Contract billing and bank data;
    iv. IP Addresses;

    TestMonitor will not have any knowledge or control over the categories or nature of the Personal Data that Company may elect to record or upload into the Service, except as provided in the Framework Agreement.

4. TestMonitor will not collect, process, or use any Personal Data made available to it for any purposes other than for the performance of the Services and anonymously for academic research. Copies or duplicates of any Personal Data made available hereunder may only be compiled with the approval of Company or as permitted under the Framework Agreement.

5. TestMonitor will grant to Company and its designees during the term of the Data Processing Addendum all requested information and access rights strictly in accordance with TestMonitor's security policy to verify TestMonitor's compliance with the Framework Agreement, this Data Processing Addendum and with applicable data protection law. Company may determine TestMonitor's compliance with the agreed technical and organizational measures (see **Exhibit 1** of this Data Processing Addendum) at TestMonitor's facilities. If and to the extent Company engages third parties to conduct the audit, such third parties have to be bound to confidentiality obligations similar to those agreed for TestMonitor under this Data Processing Addendum.

6. TestMonitor will notify Company without undue delay if TestMonitor is of the opinion that a written instruction received from Company is in violation of applicable data protection law and/or in violation of contractual duties under the Framework Agreement.

7. TestMonitor will notify Company without undue delay (within 24 hours) if TestMonitor becomes aware that TestMonitor's employees have violated any data protection law, or the provisions of the Framework Agreement if the violation occurs in the course of the processing of the data by TestMonitor. Furthermore, if TestMonitor is of the opinion that Personal Data has been or might have been illegally transferred or otherwise illegally disclosed to or accessed by a third party, TestMonitor will notify Company thereof without undue delay in accordance with applicable data protection laws, including Regulation (EU) 2016/679. In case of any loss of, or unauthorized access to Personal Data stored on the Service, TestMonitor will inform Company without undue delay, and assist Company in fulfilling its statutory obligations under applicable data protection laws, including Regulation (EU) 2016/679.

8. Company grants TestMonitor a general authorization in line with Article 28 (2) of Regulation (EU) 2016/679 to engage processors for the purposes of providing the TestMonitor Services. TestMonitor will inform Company of changes in such processors in the Framework Agreement in accordance with the procedure of modifying the Framework Agreement.

9. TestMonitor may only engage Subcontractors for providing the Services under the Framework Agreement if TestMonitor (i) communicates the name, address and contact details of the subcontractor and the tasks of the subcontractor prior to engaging the subcontractor, (ii) has in place or concludes prior to engaging the subcontractor a sub-processing agreement between TestMonitor and the subcontractor that is no less protective with respect to

Company's interest and protection of Personal Data than this Data Processing Addendum, (iii) ensures that an adequate level of data protection for subcontractors that are located outside of the EU/EEA exists or is created (e.g., by concluding EU Standard Contractual Clauses) (iv) has sufficient rights against the subcontractor to enforce a claim or request of Company in the context of the Services provided by the subcontractor and (v) provides copies of documentation evidencing (ii) to (iv) above before engaging the subcontractor.

10. TestMonitor will keep confidential and will not make available any Personal Data received in connection with the Framework Agreement to any third party except as required by applicable law.

11. TestMonitor will support Company in fulfilling the rights of the Data Subject, regarding the correction, blocking, deletion, and provision of Personal Data. If so, instructed by Company, and if feasible, TestMonitor will correct, block, or delete Personal Data in accordance with Company's written instructions. If a Data Subject contacts TestMonitor directly to have his or her data corrected, deleted, or blocked, TestMonitor will forward such request to Company without undue delay after receipt of such request. TestMonitor will assist Company in ensuring compliance with the obligations pursuant to Articles 32-36 of Regulation (EU) 2016/679 considering the nature of processing and the information available to TestMonitor.

12. TestMonitor will adopt adequate technical and organizational measures to ensure the security of its network and data center operations for the purposes of providing the Services to Company in accordance with **Exhibit 1**.

13. TestMonitor will use reasonable efforts to fully cooperate and to comply with any instructions, guidelines, and orders received from the relevant supervisory authority when such instructions, guidelines, or orders pertain to the Personal Data.

14. Upon termination of the Framework Agreement or, if applicable, an agreed exit phase, upon written instruction from Company, TestMonitor will return all media provided by Company regarding the Framework Agreement containing Personal Data and will destroy any other Personal Data within six months of termination of the Framework Agreement.

15. TestMonitor will use qualified personnel with data protection training to provide the Services.

16. TestMonitor will oblige its employees to process and use the Personal Data only in accordance with the Framework Agreement, this Data Processing Agreement, including its exhibits, and any written instructions received from Company.

3. Obligation of confidentiality

1. When processing data on behalf of the Controller, the Processor shall be obliged to maintain confidentiality of data which he receives or obtains in connection with the data processing order. The Processor shall undertake to comply with the same confidentiality regulations as those incumbents for the Controller. The Controller is obliged to inform the Processor of any specific confidentiality regulations.
2. The Processor warrants that applicable data protection regulations are known to him, and that the Processor is familiar with their application. The Processor also warrants that the employees working on the data have been made known to applicable regulations of data protection and that they are bound to maintain data confidentiality. Furthermore, the Processor warrants that he has undertaken to maintain confidentiality, in particular regarding the

employees involved in carrying out the work and has informed them of the instructions of the Controller.
3. Proof for such an obligation for the employees pursuant to paragraph 2 must be presented to the Controller on request (not more than once a year).

4. Supervisory powers

1. The Controller has the right to monitor compliance with statutory laws regarding data protection and/or compliance of the regulations agreed between the Parties and/or compliance with the instructions of the Controller by the Processor at any time to the extent necessary.
2. The Processor shall be obliged to provide the Controller with information to the extent necessary to carry out an inspection in the meaning of paragraph 1.
3. Pursuant to paragraph 1, the Controller shall be permitted to control the premises of the Processor, upon prior timely notification, during regular business hours. The Controller shall thereby ensure that the inspections are carried out only to the extent necessary in order to not interfere with the Processor's business operations.

5. Obligations of Company

1. Company will be responsible for the evaluation of the admissibility of the data processing and for ensuring the rights of the data subjects concerned.

2. Company will be entitled to issue written instructions regarding the scope and the procedure of the data processing.

6. Technical and Organizational Measures

TestMonitor will implement the technical and organizational security measures as set forth in **Exhibit 1** to this Data Processing Addendum. The technical and organizational security measures will be aimed at protecting the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, and against all other unlawful forms of processing. Every year TestMonitor will be audited ISO27001 by a third-party.

7. Term

This Data Processing Addendum will become effective when signed by the Parties (“**Effective Date**”) and will run for the same term as the Framework Agreement.

8. Choice of Law

The Data Processing Addendum is governed by the law indicated as the governing law in the respective provisions of the Framework Agreement.

9. Liability

For the purposes of this Addendum, the liability between controller and processor will be allocated pursuant to Article 82 of the GDPR.

	TestMonitor
Data Controller	Data Processor
	R. Ceelen
Name	Name
	CEO
Position	Position
	2022-02-24
Date	Date
	
Signature	Signature

EXHIBIT 1 to Data Processing Addendum

Technical and Organizational Measures
Description of the technical and organizational security measures implemented by TestMonitor according to Sec. 4 of the Data Processing Addendum:

1. Access Control of Processing Areas
TestMonitor will implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers, and related hardware) where the Personal Data are processed or used. This will be accomplished by:

- establishing security areas;
- protection and restriction of access paths;
- securing the data processing equipment, and personal computers;
- establishing access authorizations for employees and third parties, including the respective documentation;
- regulations on passwords;
- all access to the data center where personal data are hosted is logged, monitored, and tracked;
- the data center where personal data are hosted is secured by a security alarm system and other appropriate security measures.

2. Access Control to Data Processing Systems
TestMonitor will implement suitable measures to prevent its data processing systems from being used by unauthorized persons. This will be accomplished by:

- identification and password required; SSO; 2FA
- identification of the terminal user to the data importers systems.
- automatic time-out user ID when several erroneous passwords are entered.

3. Access Control to Use Specific Areas of Data Processing Systems
TestMonitor will ensure that the persons entitled to use the TestMonitor data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization). TestMonitor will ensure that Personal Data cannot be read, copied or modified, or removed without authorization. This will be accomplished by:

- ISO27001 certification and training
- employee policies and training in respect of each employee's access rights to the personal data.
- effective and measured disciplinary action against individuals who access personal data without authorization.
- release of data to only authorized persons.
- control of files, controlled and documented destruction of data; and
- policies controlling the retention of back-up copies.

4. Transmission Control
TestMonitor will implement suitable measures to prevent the Personal Data from being read, copied, altered, or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This will be accomplished by:

- use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels.
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

5. Input Control
TestMonitor will implement suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This will be accomplished by:

- an authorization policy for the reading, alteration, and deletion of stored data.
- authentication of the authorized personnel.
- protective measures for the reading, alteration, and deletion of stored data.
- utilization of user codes (passwords); and
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked.

6. Job Control
TestMonitor will implement suitable measures to ensure that the Personal Data is processed strictly in accordance with the instructions of Company. This will be accomplished by:

- ensuring clear instructions to TestMonitor regarding the scope of any processing of Personal Data. This will be limited to specific system development and database management requirements of Company (for example, the creation of new reporting templates, where the processing of data is necessary in order to test those reporting templates); and
- granting regular access and control rights to Company, on appropriate notice and in accordance with Company's security policies and accompanied by TestMonitor.

7. Availability Control
TestMonitor will implement suitable measures to ensure that Personal Data is protected from accidental destruction or loss. This will be accomplished by:

- infrastructure mirroring: clustered database servers will be used for storing the data;
- extra backup is stored off-site and available for restore in case of failure of the database server.

8. Separation of Processing for different Purposes
TestMonitor will implement suitable measures to ensure that data collected for different purposes can be processed separately. This will be accomplished by:

- access to data will be separated through application security for the appropriate users.
- modules within TestMonitor's database will separate which data is used for which purpose, i.e., by functionality and function.
- at the database level, data will be stored in different normalized tables, separated per module or function they support; and
- interfaces, batch processes, and reports will be designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

9. Subcontractor

We use subcontractors to provide our Service. Listed below are entities with whom we share customer data.

Subcontractor	Type of Service	Data	Hosting Region	EU/ SCC
Transip	Cloud computing provider	Database	The Netherlands	EU
Mailgun Technologies, Inc.	Email notification services	Email users	United States	SCC