APICA DATA PROCESSING AGREEMENT

Last Updated: October 21, 2021

This Data Processing Agreement (**DPA**) creates the legal framework, between the Customer as the ***data controller*** and Apica AB as the ***data processor***, for processing of personal data in a manner compliant with EU General Data Protection Regulation 2016/679 (GDPR). The Customer (the data controller) is the subscriber of the Service, and Apica AB (the data processor) will, on behalf of the Customer, process Personal Data selected, collected, and submitted by the Customer, and/or third parties designated by the Customer, and stored and used within the Service. The terms of this DPA only apply together with an active subscription to the Service. Non-English translations of the DPA are provided for convenience only. In the event of any ambiguity or conflict between translations, the English version is authoritative and controls.

By actively agreeing to be bound by this DPA, the Customer agrees to be bound by this DPA with Apica AB, including all its Affiliates, a Swedish corporation with an address at Malmskillnadsgatan 32, 111 51, Stockholm, Sweden. The DPA constitutes a legally binding contract between Apica AB and the Customer with respect to processing of Personal Data, in relation to access and use of the Service.

1. Definitions

All capitalized terms used in this DPA shall have the meanings given to them below:

Account - A specific named Customer, which may be an individual or a company.

Affiliate - Any entity controlling or controlled by or under common control with a Party where control is ownership of more than 50 % of the equity or voting rights of such entity.

Cloud Entity - Entities added to the DC's account to which Personal Data may be associated and/or processed.

Data Controller or **DC** - Has the meaning given in GDPR (and, for the purpose of this DPA, means the party licensing and using the Service).

Data Processor, DP or **Apica** - Has the meaning given in GDPR (and, for the purposes of this DPA, Apica AB, including all its Affiliates, a Swedish corporation with headquarters at Malmskillnadsgatan 32, 111 51, Stockholm.

Data Security Breach - Has the meaning set forth in Section 4.

Data Subject - An individual who is the subject of Personal Data.

Data Subject Request - Has the meaning set forth in Section 4.

Data Transfer - A transfer of Personal Data from the DC to the DP, or an onward transfer of Personal Data from the DP to a Sub-Processor, or between two establishments of a DP; in each case, where such transfer would be prohibited by EU Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of EU Data Protection Laws).

DPA - This Data Processing Agreement together with its annexes, as supplemented and amended from time to time.

EEA - The European Economic Area.

EU Data Protection Laws - Refers to all privacy and personal data legislation applicable to the personal data processing that is carried out under this DPA.

GDPR - EU General Data Protection Regulation 2016/679 and any national laws adopted pertaining to this regulation. The term includes binding guidelines, opinions, recommendations and decisions from supervisory authorities, courts, or other authority.

Party - Either DC or DP.

Parties - DC and DP.

Personal Data - Any information relating to an identified or identifiable natural person, where an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier.

Processing - Any operation or set of operations which is performed upon Personal Data or sets of

Personal Data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Service - Apica's software-as-a-service (SaaS) and cloud-based services and products for ASM and ALT via hosted online web services, and any subsequent updates, upgrades, bug fixes, work around, and other services and/or products delivered or made accessible to the Customer by or on behalf of Apica to the Customer in connection with the Service. The Service is made available online by Apica, via the applicable Customer login link and other web pages designated by Apica, including, individually and collectively, the applicable software, updates, Applications (**App**), API, Documentation, and all applicable Associated Service that Customer has licensed, purchased, or deployed (**Deployed Associated Service**) that are provided by Apica subject to the SA and supplemental license terms and conditions. The Service does not include licenses for (i) Third-Party Services and Third-Party Materials, and (ii) any Additional Features or Associated Service that are not provided under the SA.

Service Data - Any electronic data, text, messages, communications, or other materials submitted to and stored within the Service by Customer in connection with use of the Service, which may include, without limitation, Personal Data.

Sub-Processor - Any third-party data processor engaged by DP who receives Personal Data from DP or DC for Processing on behalf of DC.

Subscription Agreement or **SA** - The agreement created by Customer and Apica, by the Customer completing the required registration process for use of the Service and actively agreeing to be bound by applicable Subscription Form, and any amendments and supplements thereto, that sets forth the terms and conditions for subscription/use of the Service.

Supervisory Authority - Any Data Protection Supervisory Authority with competence over DC, DP, and any Sub-Processor Processing of Personal Data.

Third-Party Services - Any services, products, gateways, links, or other functionality that may be included in or linked to the Service and that allows the Customer to access Third-Party services, for example connectivity- and mobile network services.

2. Purpose

The DC has concluded a SA pursuant to which DC is granted a license to access and use the Service, and the DP will, on behalf of the DC, Process Personal Data selected, collected, and submitted by the DC, and/or third parties designated by the DC with whom DC transacts using the Service, and such Personal Data is stored and used within the Service. For the avoidance of doubt, the terms of this DPA shall only apply to the DC with an active license to the Service.

The Parties are entering into this DPA to ensure that the Processing by the DP of Personal Data, within the Service, is done in a manner compliant with GDPR and its requirements regarding the collection, use and retention of Personal Data.

To the extent that any terms of the SA conflict with the substantive terms of this DPA (as they relate to the protection of Personal Data and the Parties' respective obligations and liabilities), the terms of this DPA shall take precedence.

3. Ownership

All Service Data Processed within the Service shall remain the property of the DC. Under no circumstances will the DP act, or be deemed to act, as a data controller of the Service Data Processed within the Service under GDPR.

4. Data Processor's Obligations

The Parties agree that the subject-matter and duration of Processing performed by the DP under this DPA and the SA, including the nature and purpose of Processing, the type of Personal Data, and categories of Data Subjects, shall be as described in the Processing Instructions attached to this DPA as Annex 1.

The DP undertakes to process Personal Data under this DPA in accordance with applicable EU Data Protection Laws and guidance from the Supervisory Authority and relevant trade associations (*Sw.*

branschorganisationer).

As part of the DP providing the Service to the DC under the SA, DP shall comply with the obligations imposed upon it under GDPR Articles 28 - 32 and agrees and declares as follows:

(a) The DP shall process Personal Data in accordance with the instructions set forth in this DPA;

(b) the DP shall ensure that all staff and management of the DP are fully aware of their responsibilities to protect Personal Data in accordance with this DPA and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in accordance with GDPR Article 28(3)(b);

(c) the DP shall implement and maintain appropriate technical and organizational measures to protect Personal Data in accordance with GDPR Article 32 against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (**Data Security Breach**), provided that such measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, so as to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, including data security consistent with Apica's Data Security Standards attached to this DPA as Annex 2;

(d) the DP shall notify the DC in accordance with GDPR Article 33(2), without undue delay after becoming aware of a Data Security Breach affecting the DC's Service Data and to cooperate with the DC as necessary to mitigate or remediate the Data Security Breach. Further, the DP shall cooperate with the DC and take such commercially reasonable steps as are directed by the DC to assist in the investigation, mitigation and remediation of any such Data Security Breach under GDPR;

(e) the DP shall comply with the requirements of Section 5 when engaging a Sub-Processor;

(f) considering the nature of the Processing, the DP shall assist the DC (including by appropriate technical and organizational measures), insofar as it is commercially reasonable, to fulfil DC's obligation to respond to requests from Data Subjects to exercise their rights under GDPR (a **Data Subject Request**). In the event the DP receives a Data Subject Request directly from a Data Subject, it shall (unless prohibited by law) direct the Data Subject to the DC. However, in the event the DC is unable to address the Data Subject Request, taking into account the nature of the Processing and the information available to the DC, the DP, shall, on the DC's written request and the DC's instruction to the DP, and at the DP's reasonable expense (scoped prior to the DP's response to the Data Subject Request), address the Data Subject Request, as required under GDPR;

(g) upon request, the DP shall provide the DC with commercially reasonable information and assistance, taking into account the nature of the Processing and the information available to the DP, to help the DC to conduct any data protection impact assessment or Supervisory Authority consultation it is required to conduct under GDPR;

(h) upon termination of the DC's access to and use of the Service, the DP shall comply with the requirements of Section 9;

(i) the DP shall comply with the requirements of Section 6 to make available to the DC information that demonstrates the DP's compliance with this DPA; and

(j) the DP shall appoint a security officer who will act as a point of contact for the DC, and coordinate and control compliance with this DPA.

The DP shall immediately inform the DC if, in its opinion, the DC's processing instructions infringe any law or regulation. In such event, the DP is entitled to refuse Processing of Personal Data that it believes to be in violation of law or regulation.

5. Use of Sub-Processors

The DC hereby confirms its general written authorisation for the DP's use of the Sub-Processor(-s) listed in accordance with GDPR Article 28, to assist it in providing the Service and Processing Personal Data provided that such Sub-Processor(-s),

(a) agree to act only on the DP's instructions when Processing the Personal Data (which instructions

shall be consistent with the DC's Processing instructions to the DP), and

(b) agree to protect the Personal Data to a standard consistent with the requirements of this DPA, including by implementing and maintaining appropriate technical and organizational measures to protect the Personal Data they Process consistent with Apica's Data Security Standards attached to this DPA as Annex 2.

The DP is currently processing and storing data in DP's servers situated in the DP's data centers located in Germany, Ireland, Sweden, United Kingdom and USA.

The DP agrees and warrants to remain liable to the DC for the Processing services of any of its Sub-Processor(-s) under this DPA. The DP shall maintain an up-to-date list of the names and locations of all Sub-Processor(-s) used for the Processing of Personal Data under this DPA at www.apica.io/sub-processors. The DP shall update the list on its website of any Sub-Processor to be appointed at least 30 days prior to the date on which the Sub-Processor shall commence processing Personal Data. The DC shall receive email notification of any such changes.

If the DC objects to the Processing of its Personal Data by any newly appointed Sub-Processor, as described in this Section 5, the DC shall inform the DP within 30 days following the update of its online policy above. In such event, the DP will instruct the Sub-Processor to cease any further processing of the DC's Personal Data and this DPA shall continue unaffected.

In addition, and as stated in the SA, the Service requires integrations and combinations with Third-Party Services. If the DC elects to enable, access or use such Third-Party Services, its access and use of such Third-Party Services is governed solely by the terms and conditions and privacy policies of such Third-Party Services, and the DP does not endorse, is not responsible or liable for, and makes no representations as to any aspect of such Third-Party Services, including, without limitation, their content or the manner in which they handle Service Data (including Personal Data) or any interaction between the DC and the provider of such Third-Party Services. The DP is not liable for any damage or loss caused or alleged to be caused by or in connection with the DC's enablement, access or use of any such Third-Party Services, or the DC's reliance on the privacy practices, data security processes or other policies of such Third-Party Services. A provider of a Third-Party Service shall not be deemed a Sub-Processor for any purpose under this DPA.

6. Audit

Subject to this Section 6, the DP shall make available to the DC on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the DC or an auditor mandated by the DC in relation to the Processing of Personal Data by the DP and any Sub-Processor.

Information and audit rights of the DC only arise under Section 6 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of GDPR.

7. International Data Transfers

Except as requested by the DC and as explicitly approved by the DP, the DP and its Sub-Processors will maintain Processing operations in USA – Amazon Web Services (AWS) data centres and servers that are outside of the EU/EEA.

If Personal Data processed in the Service is transferred and/or processed in a country outside the EU/EEA, the DP shall ensure that such transferred and/or processed Personal Data are adequately protected.

The DC is aware and approves that the Processor is using AWS managed services for data processing and data storage, in AWS (Amazon Web Services) servers in the USA and West Europe (Sweden, Ireland, Germany and USA). However, AWS' processing and storage procedures may include that Personal Data may be transferred outside of the EU/EEA within the DP's use of the service. In the light of recent case law and guidance regarding transfer of Personal Data outside of the EU/EEA, the DC and the DP agree to collaborate to ensure that Personal Data is transferred with protection essentially equivalent to that guaranteed within the EU/EEA.

8. Data Controller's Obligations

As part of the DC receiving the Service under the SA, the DC agrees to abide by its obligations under

GDPR and declares and warrants as follows.

(a) That the DC is solely responsible for how Personal Data is acquired and used by the DC, including instructing Processing by the DC in accordance with the provisions of the SA and this DPA, is and shall continue to be in accordance with all the relevant provisions of GDPR, particularly with respect to the security, protection, and disclosure of Personal Data,

(b) that if collection by DP involves any 'special' or 'sensitive' categories of Personal Data (as defined in GDPR), the DC is acquiring and transferring such Personal Data in accordance with GDPR,

(c) that that DC will inform its Data Subjects (if applicable);

- about its general use of data processors to Process their Personal Data, including the DP, and
- that their Personal Data is be Processed outside of the EU/EEA,

(d) that, upon instructions from the DP, it shall respond in reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data by the DP, and to give appropriate instructions to the DP in a timely manner, and

(e) that, upon instructions from the DP, it shall respond in a reasonable time to enquiries from a Supervisory Authority regarding the Processing of relevant Personal Data by DP.

9. Return & Destruction of Personal Data

Upon the termination of the DC's access to and use of the Service, the DP will up to 30 days following such termination at the choice of the DC either;

(a) permit the DC to export its Personal Data, or

(b) delete all Personal Data in accordance with the capabilities of the Service in accordance with GDPR Article 28(3)(g).

10. Duration

This DPA will remain in force for as long as the DP Processes Personal Data on behalf of the DC under the SA and for the Service.

11. Liability

As between the DC and the DP, this DPA shall be subject to the limitations of liability set forth in this Section below, and in applicable SA for the Service licensed by the DC.

The DP does not accept any liability under this DPA or GDPR for any Third-Party Services, including acts and omissions.

The limitation of liability set forth in this Section 11 shall not be construed as limiting the liability of either Party with respect to claims by Data Subjects.

12. Miscellaneous

This DPA may not be amended or modified except by a writing signed by both Parties hereto. This DPA may be executed in counterparts, provided however that the DP shall be entitled to from time to time make non-material functional changes and updates to the DPA (not changing the Parties' respective rights and responsibilities in this DPA) by giving the DC 30 days' notice. Also, should European Parliament and/or the Council pass new regulations and/or issue any guidelines which contains terms that conflict with those used in this DPA, the Parties hereby agree that such terms in this DPA shall primarily be changed or secondarily be interpreted and applied strictly in accordance with any such new regulation and guideline.

Subject to the foregoing restrictions, this DPA will be fully binding upon, inure to the benefit of and be enforceable by the Parties and their respective successors and assigns.

This DPA constitutes the entire understanding between the Parties with respect to the subject matter herein, and shall supersede any other arrangements, negotiations or discussions between the Parties

relating to that subject-matter.

13. Governing Law & Jurisdiction

This DPA and the rights and obligations of the Parties pursuant thereto will be governed by the laws of Sweden, without regard to conflicts of law principles. The Parties irrevocably agree that, subject as provided below, the courts of Sweden shall have exclusive jurisdiction in relation to any claim, dispute or difference concerning this DPA (including the right to possible appeal), and any matter arising therefrom and irrevocably waive any right that they may have to object to an action being brought in those courts, or to claim that the action has been brought in an inconvenient forum, or that those courts do not have jurisdiction.

Annex 1

Processing Instructions

Capitalized terms utilized in this document and not defined shall have the meaning set forth in the Data Processing Agreement (DPA).

1. Data Processor

The DP (where applicable) operates a Software-as-a-Service and (as applicable) Cloud Sourcing services for registering Apica LoadTest™ (ALT) and Apica Synthetic Monitoring (ASM).

2. Data Controller

The DC is the Customer of the Service and will collect and process Personal Data for registering Apica LoadTest™ (ALT) and Apica Synthetic Monitoring (ASM).

3. Duration of Processing

The processing of Personal Data shall endure for the duration of the license term in the relevant SA for the Service.

4. Data Subjects

The DC may, at its sole discretion, collect and submit Personal Data to the Service, which may include, but is not limited to, the following categories of Data Subjects (all of whom are natural persons) of the DC and any natural person(s) authorized by the DC to use the Service:

- **Customers**
- **Employees and consultants of customers and potential customers (contact persons and admin)**
- **Employees and consultants (contact persons and admin)**
- **Relatives of employees**
- **Employees and consultants of business partners**
- **End-customers**

5. Categories of Personal Data

The DC may, at its sole discretion, submit, process and collect Personal Data to the Service which may include, but is not limited to, the following categories of data related to the Data Subjects:

- **First name**
- **Last name**
- **Mobile telephone number**
- **Customer Specified Transaction Data**

6. Processing Operations

The subject matter of the Processing of the Personal Data:

The DP (where applicable) will host, and process Personal Data obtained by the DC using, or third-party using, the Service, while providing and as a technical prerequisite for the DP to provide the Service, the Software-as-a-Service and (as applicable Cloud sourcing services).

With the support of the balance of interests according to the Data Protection legislation, the DC can save logs for other purposes. Logging and saving information about transactions may be justified for technical maintenance and troubleshooting or if a property, for example, has been exposed to disturbances, significant damage or extensive theft. Regarding passages and sometimes visitor registration, the purposes are, in addition to safety and security, for example a crime investigation, and

to keep statistics and optimize the use of the provided Services.

The DP processes Personal Data on behalf on the DC for the following purposes:

- **Provide and administrate the provided service.**
- **Keep statistics and optimize the use of the provided services.**
- **Uphold safety and security while using the services.**
- **Establish and defend legal claims.**
- **Investigate, prevent, or act on illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of agreement.**
- **Comply with legal obligations.**
- **Response to lawful requests by public authorities, including to meet national security or law enforcement requirements.**

7. Contact Details

For Personal Data queries arising from or in connection with this Processing and this DPA, please write to support@apicasystems.com

Annex 2

Data Security Standards

This Data Security Standard policy (**Policy**) sets forth Apica AB's, a Swedish corporation with address Malmskillnadsgatan 32, 111 51, Stockholm, Sweden (**Apica**) technical and organizational security measures for the processing of Customer Data and Personal Data to ensure a level of security appropriate to risks (**Security Standards**). These Security Standards apply to all Personal Data that Apica receives and process using the Apica operated services (**Service**) and Apica's App. This Policy is also part of the legal framework for Apica's processing of personal data, as further outlined in the Data Processing Agreement. Capitalized terms utilized in this Policy and not defined shall have the meaning set forth in the Data Processing Agreement

1. Pseudonymization and Encryption

Personal Data handled by Apica shall be encrypted and pseudonymized. When laptops are used for Personal Data processing, encryption should always take place on fixed and removable storage media.

2. Access and Access Control

Apica has a technical system for access control to the system; to give the right person the right level and scope of access to the system. Apica has procedures for how access permissions to the system are granted and removed. All granted access rights are checked at intervals. Apica has strong authentication checks and routines. All usernames are unique and personal. Apica's password management rules ensure a high password quality. All authentication information is stored securely.

3. Physical Access Controls

Apica takes reasonable measures to;

(a) prevent physical access, such as security personnel and secured buildings, and

(b) prevent unauthorized persons from gaining access to Personal Data or ensure third parties operating data centres on its behalf are adhering to such controls.

4. System Access Controls

Apica takes reasonable measures to prevent Personal Data from being used without authorization. These measures vary based on the nature of the Processing undertaken and may include, among other;

(a) controls,

(b) authentication via passwords and/or two-factor authentication,

(c) documented authorization processes,

(d) documented change management processes, and/or

(e) log of access on several levels.

5. Data Access Controls

Apica takes reasonable measures to provide that;

(a) Personal Data is accessible and manageable only by properly authorized staff,

(b) direct database query access is restricted, and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and

(c) Personal Data cannot be read, copied, modified, or removed without authorization while Processing.

6. Transmission Controls

Apica takes reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Customer Data cannot be read, copied, modified, or removed without authorization during electronic transmission or

transport.

7. Input Controls

Apica use commercial best efforts to provide that it is possible to check and establish whether and by whom Customer Data has been entered into data processing systems, modified, or removed.

Apica takes reasonable measures to ensure that;

(a) the Personal Data source is under the control of the Data Controller, and

(b) Personal Data integrated into the Service is managed by secured transmission from Apica for interactions with Apica's User Interface (UI) or Application Programming Interface (API).

8. Protection Against Malicious Software

Apica has active and updated antivirus solutions on the devices used in personal data processing. Apica performs continuous monitoring of protection against malicious software.

9. Data Backup

Back-ups of the databases in the Service are taken on a regular basis, are secured and to ensure that Personal Data is protected against accidental destruction or loss. Apica has documented procedures for recovery. Testing of restoration of personal data is carried out at intervals and the results documented. Apica has documented procedures for deleting obsolete or old Personal Data.

10. Log

Apica is logging events that takes place during all processing activities of the Personal Data. Apica has documented procedures for handling security logs and a system for protecting logs.

11. Logical Separation

Personal (Service) Data from different Licensees and their respective Licensee is logically segregated on systems managed by Apica to ensure that Personal Data that is collected by different Licensees is segregated from one another.

12. Physical Safety

Equipment, portable data media and the like that are not under the supervision of the personal data tree are locked to be protected against unauthorized use, influence, and theft.

13. Procedures for Investigation

Apica has both technical and practical prerequisites for investigating suspicions of unauthorized access and other forms of unauthorized use of the Personal Data.

14. Equipment Repairs and Service

In the event of repair and service of computer equipment used for processing the Personal Data and performed by someone other than Apica, Apica will enter into a special confidentiality agreement with the service provider. At the service provider's visit, service must be done under the supervision of Apica.