# Master Subscription Agreement

# Data Protection Appendix

**THIS DATA PROTECTION APPENDIX FORMS PART OF THE MASTER SUBSCRIPTION AGREEMENT THAT GOVERNS THE SUPPLY OF THE EMAINT ONLINE SERVICE INCLUDING OFFLINE COMPONENTS**

## 1. DATA PROTECTION

### 1.1. Processor/Controller

1.1.1. The parties agree that, for the Protected Data, the Customer shall be the Data Controller and eMaint shall be the Data Processor.

### 1.2. Compliance with Data Protection Laws and obligations

1.2.1. eMaint shall process Protected Data in compliance with:

(a) the obligations of Data Processors under Data Protection Laws, in respect of the performance of its obligations under this Agreement; and

(b) this Agreement.

1.2.2. The Customer shall comply with:

(a) all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

(b) this Agreement.

1.2.3. The Customer warrants, represents and undertakes, that:

(a) with respect to data being provided to or accessed by eMaint for the performance of the Services under this Agreement, such data shall have been sourced by the Customer in all respects in compliance with Data Protection Laws, including in terms of its collection, storage and processing, which for the avoidance of doubt includes the Customer providing all required fair processing information to, and obtaining all necessary consents from, Data Subjects in order that eMaint can lawfully process and transfer such data in accordance with this Agreement;

(b) all instructions given by it to eMaint in respect of Protected Data shall at all times be in accordance with Data Protection Laws;

(c) it has undertaken due diligence in relation to eMaint's processing operations, and it is satisfied that:

(i) eMaint's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage eMaint to process the Protected Data; and

(ii) eMaint has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

(d) it will not, and shall cause its users to not, upload, store or process any sensitive or special category personal data in the Service, or any other personal data that is not necessary for the purpose or intended use of the Services

1.2.4. The Customer shall not unreasonably withhold, delay or condition its agreement to any Change requested by eMaint in order to ensure the Services and eMaint (or any Sub-Processor) can comply with Data Protection Laws, and no longer than 1 month.

1.3. **Details of processing and instructions**

1.3.1. Insofar as eMaint processes Protected Data on behalf of the Customer, eMaint:

(a) unless required to do otherwise by applicable law, shall, and shall take steps to ensure each person acting under its authority shall, process the Protected Data only on and in accordance with (a) the Customer's documented instructions as set out in Schedule 2 to this Appendix (*Data Processing Details*), as updated from time to time, and (b) the Customer's instructions via its configuration of the Services ("**Processing Instructions**");

(b) if applicable law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data unless applicable law prohibits such information on important grounds of public interest; and

(c) shall inform the Customer if eMaint becomes aware of a Processing Instruction that, in eMaint's opinion, infringes Data Protection Laws:

(i) provided that doing so shall be without prejudice to clauses 1.2.2 and 1.2.3; and

(ii) it being agreed that to the maximum extent permitted by mandatory law, eMaint shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Processing Losses) arising from or in connection with any processing in accordance with the Customer's Processing Instructions following eMaint informing the Customer of an infringing Processing Instruction.

1.4. **Technical and organisational measures**

1.4.1. eMaint shall implement and maintain, at its cost and expense, the technical and organisational measures:

(a) in relation to the processing of Protected Data by eMaint, as set out in and substantially in compliance with schedule 2 (*Data Processing Details*) and the Security Measures per schedule 1; and

(b) taking into account the nature of the processing, to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data.

1.4.2. Any additional technical and organisational measures requested by the Customer shall be at the Customer's cost and expense and only to the extent reasonably possible to be implemented.

1.5. **Security of processing**

1.5.1. eMaint shall, in respect of the Protected Data processed by it under this Agreement comply with the requirements regarding security of processing set out in Data Protection Laws as applicable to Data Processors and in this Appendix including clause 1.4.

1.6. **Using staff and other processors**

1.6.1. Customer agrees that eMaint may engage Sub-Processors to perform processing activities in respect of Protected Data on behalf of Customer, as is necessary for the provision of the Services. The Sub-Processors currently appointed by eMaint are listed in schedule 2. eMaint will inform the Customer of any addition to or change of the appointed Sub-Processors by giving no less than thirty (30) days' advance notice, and the Customer will have fourteen (14) days after such notice to object to such addition or change. In the case of an objection from the Customer, eMaint may choose from the following options to cure the objection:

(a) eMaint will cancel its plans to use the objectionable Sub-Processor(s) with regard to Protected Data or will offer an alternative to provide the Services without such Sub-Processor(s); or

(b) eMaint will take the corrective steps requested by the Customer in its objection (which remove the Customer's objection) and proceed to use the objectionable Sub-Processor(s) with regard to Protected Data; or

(c) eMaint may cease to provide or the Customer may agree not to use (temporarily or permanently) the particular aspect of the Services that would involve the use of the objectionable Sub-Processor(s) with regard to Protected Data, subject to an agreement of eMaint and the Customer to adjust the Fees, considering the reduced scope of the Services.

If none of the above options are reasonably available and the objection has not been resolved to the mutual satisfaction of the Customer and eMaint within 30 days after eMaint's receipt of the Customer's objection, either party may terminate this Agreement and the Customer will be entitled to a pro-rata refund of pre-paid fees for the Services not performed as of the date of termination.

1.6.2. eMaint shall engage Sub-Processors under a written contract containing materially the same obligations as this clause 1, including without limitation clause 1.8 below.

1.6.3. eMaint shall take reasonable steps to ensure that all of eMaint's personnel who have access to personal data are reliable and that all of eMaint's personnel authorised to process Protected Data are subject to a binding written contractual obligation with eMaint to keep the Protected Data confidential except where disclosure is required in accordance with applicable law, in which case eMaint shall, where practicable and not prohibited by applicable law, notify the Customer of any such requirement before such disclosure.

1.7. **Assistance with the Customer's compliance and Data Subject rights**

1.7.1. eMaint shall refer all Data Subject Requests it receives to the Customer within three Business Days of actual receipt of the request, and the Customer shall pay eMaint reasonable expenses, as set out in the Price List for recording and referring the Data Subject Requests in accordance with this clause 1.7.1.

1.7.2. eMaint shall provide such reasonable assistance as the Customer reasonably requires, taking into account the nature of processing performed by and the information available to eMaint, to comply with the Customer's obligations under Data Protection Laws with respect to the Services as they relate to:

(a) security of processing;

(b) DPIAs;

(c) prior consultation with a Supervisory Authority regarding high risk processing; and

(d) notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Protected Data Breach,

provided the Customer shall pay eMaint's Charges, per eMaint's Price List, for providing assistance under this clause 1.7.2.

1.8. **International data transfers**

1.8.1. The Customer agrees that eMaint may transfer Protected Data outside the UK, EEA or Switzerland, or to any international organisation(s) (individually or collectively, an "International Recipient"), provided all transfers by eMaint of Protected Data to an International Recipient and any onward transfer shall to the extent required under Data Protection Laws be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The foregoing sentence shall constitute Customer instructions with respect to international data transfers for the purposes of clause 1.3.1.

1.8.2. eMaint may engage Sub-Processors who are International Recipients using the Standard Contractual Clauses to ensure compliance with clause 2.8.1. At Customer's request, eMaint shall provide a copy of such Standard Contractual Clauses redacted to the extent necessary to protect business secrets or other confidential information, including personal data.

1.9. **Records, information and audit**

1.9.1. eMaint shall maintain, in accordance with Data Protection Laws binding on eMaint, written records of all categories of processing activities carried out on behalf of the Customer.

1.9.2. eMaint shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate eMaint's compliance with the obligations of Data Processors under Data Protection Laws, and allow for and contribute to audits, including inspections, by the Customer or another auditor mandated by the Customer for this purpose, subject to the Customer:

(a) giving eMaint reasonable prior notice of such information request, audit or inspection being required by the Customer;

(b) ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential, save for disclosure to the Supervisory Authority or as otherwise required by applicable law;

(c) ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to eMaint's business, a Sub-Processor's business, or the business of other Customers of eMaint; and

(d) paying eMaint's reasonable costs, a pre-estimate of which is set out in the Price List, for assisting with the provision of information and allowing for and contributing to inspections and audits.

1.10. **Notification of Protected Data Breaches and Complaints**

1.10.1. In respect of any Protected Data Breach involving Protected Data, eMaint shall, without undue delay:

(a) notify the Customer of the Protected Data Breach; and

(b) provide the Customer with details of the Protected Data Breach.

1.10.2. Each party shall promptly, and in any event within three Business Days, inform the other if it receives a Complaint and provide the other party with full details of such Complaint.

1.11. **Deletion or return of Protected Data and copies**

eMaint shall, at the Customer's written request, either delete or return all the Protected Data to the Customer within a reasonable time after the end of the provision of the relevant Services related to processing, and delete any other existing copies thereof unless storage of any data is required by applicable law and, where this is the case, eMaint shall inform the Customer of any such requirement.

1.12. **Liability, indemnities and compensation claims**

1.12.1. The Customer shall indemnify and keep indemnified eMaint in respect of all Data Processing Losses suffered or incurred by, awarded against or agreed to be paid by, eMaint and any Sub-Processor arising from or in connection with any:

(a) non-compliance by the Customer with the Data Protection Laws;

(b) processing carried out by eMaint or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

(c) breach by the Customer of any of its obligations under this clause 1,

except to the extent eMaint is liable under clause 1.12.2.

1.12.2. eMaint shall be liable for Data Processing Losses howsoever arising, whether in contract, tort (including negligence) or otherwise under or in connection with this Agreement:

(a) only to the extent caused by the processing of Protected Data under this Agreement and directly resulting from eMaint's breach of this clause 1; and

(b) in no circumstances for any portion of the Data Processing Losses (or the circumstances giving rise to them) contributed to or caused by any breach of this Agreement by the Customer (including a breach of clause 1.3.1(c)(ii)).

1.12.3. If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim, and each party shall:

(a) make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party, which consent shall not be unreasonably withheld, conditioned or delayed; and

(b) consult fully with the other party in relation to any such action, but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under this Agreement for paying the compensation.

1.12.4. The parties agree that the Customer shall not be entitled to claim back from eMaint any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify eMaint in accordance with clause 1.12.1.

1.12.5. This clause 1.12 is intended to apply to the allocation of liability for Data Processing Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

(a) to the extent not permitted by applicable law (including Data Protection Laws); and

(b) that it does not affect the liability of either party to any Data Subject.

# SCHEDULE 1

## SECURITY MEASURES

### Description of Technical and Organizational Security Measures Implemented by eMaint

| Technical Measures to Ensure Security of Processing | |
|---|---|
| **1. Inventory and Control of Hardware Assets** | Actively manage all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access. |
| **2. Inventory and Control of Software Assets** | Actively manage all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution. |
| **3. Continuous Vulnerability Management** | Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. |
| **4. Controlled Use of Administrative Privileges** | Maintain processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, applications, and data. |
| **5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** | Implement and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |
| **6. Maintenance, Monitoring, and Analysis of Audit Logs** | Collect, manage, and analyse audit and security logs of events that could help detect, understand, or recover from a possible attack. |
| **7. Email and Web Browser Protections** | Deploy automated controls to minimise the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems or content. |
| **8. Malware Defenses** | Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action. |

| | |
|---|---|
| **9. Limitation and Control of Network Ports, Protocols, and Services** | Manage (track, control, correct) the ongoing operational use of ports, protocols, services, and applications on networked devices in order to minimise windows of vulnerability and exposure available to attackers. |
| **10. Data Recovery Capabilities** | Maintain processes and tools to properly back up personal data with a proven methodology to ensure the confidentiality, integrity, availability, and recoverability of that data. |
| **11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches** | Implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |
| **12. Boundary Defenses** | Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data. |
| **13. Data Protection** | Maintain processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the confidentiality and integrity of personal data. |
| **14. Controlled Access Based on the Need to Know** | Maintain processes and tools to track, control, prevent, and correct secure access to critical or controlled assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical or controlled assets based on an approved classification. |
| **15. Wireless Access Control** | Maintain processes and tools to track, control, prevent, and correct the secure use of wireless local area networks (WLANs), access points, and wireless Customer systems. |
| **16. Account Monitoring and Control** | Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimise opportunities for unauthorised, inappropriate, or nefarious use. |

| **Organisational Measures to Ensure Security of Processing** | |
|---|---|
| **1. Implement a Comprehensive Information Security Programme** | Through the implementation of a Comprehensive Information Security Programme (CISP), maintain various administrative safeguards to protect personal data. These measures are designed to ensure:<br>• security, confidentiality and integrity of personal data<br>• protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud<br>• that employees, contractors, consultants, temporaries, and other workers who have access to personal data only process such data on instructions from the data controller. |
| **2. Implement a Security Awareness and Training Programme** | For all functional roles (prioritizing those mission critical to the business, its security, and the protection of personal data), identify the specific knowledge, skills and abilities needed to support the protection and defense of personal data; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programmes. |
| **3. Application Software Security** | Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. |
| **4. Incident Response and Management** | Protect the organisation's information, including personal data, as well as its reputation, by developing and implementing an incident response infrastructure (*e.g.*, plans, defined roles, training, communications, management oversight, retainers, and insurance) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the organisation's network and systems. |
| **5. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises** | Test the overall strength of the organisation's defense (the technology, processes, and people) by simulating the objectives and actions of an attacker; as well as, assess and validate the controls, policies, and procedures of the organisation's privacy and personal data protections. |
| **6. Physical Security and Entry Control** | Require that all facilities meet the highest level of data protection standards possible, and reasonable, under the circumstances relevant to the facility and the data it contains, process, or transmits. |

# SCHEDULE 2

## DATA PROCESSING DETAILS

### 2. SUBJECT-MATTER OF PROCESSING

eMaint processes Personal Data to provide the Services to the Customer in accordance with this Agreement.

### 3. DURATION OF THE PROCESSING

Duration of the provision of the Services or as per Customer's instructions.

### 4. NATURE AND PURPOSE OF THE PROCESSING

eMaint processes data in order to provide the Services to the Customer and its users in accordance with this Agreement, including:

1. To provide the Services, including to provide the Customer's users with access to the Services;
2. To provide the Customer's users with the option to use the email features and QR codes that form part of the Services;
3. To provide remote implementation and setup services to the Customer's admin and power users;
4. To provide technical support to the Customer's users who access the Services;
5. To maintain and upgrade the Services; and
6. To provide the Customer's users with invitations to educational webinars and training sessions.

### 4. TYPE OF PERSONAL DATA

1. User ID, password, workstation name, IP address, geolocation information, cookie identifiers;
2. First and last name, contact details (email, telephone, address) and/or professional, business title or trade;
3. Employer (Customer: name, company number, address); and
4. Any other Personal Data that is collected by the Customer or its users or is inputted into the Services based on the Customer's own configuration of the Services and marked by Customer as Personal Data.

### 5. CATEGORIES OF DATA SUBJECTS

The Personal Data processed by eMaint concern the following categories of Data Subjects:

(i) prospective, current and former employees and contractors of the Customer, its affiliates and end customers;

(ii) prospective, current and former employees and contractors of the Customer's service providers and contractors; and

(iii) any categories of data subject in relation to which the Customer or its users configure the Services to collect.

### 6. TECHNICAL AND ORGANIZATIONAL MEASURES

See schedule 1, which shall form a part of this schedule 2.

## 7. APPROVED SUB-PROCESSORS

The following Sub-Processors are affiliated companies of eMaint and may process personal data as set out in this Schedule for the purposes described in Points 3. to 6. (inclusive) of Section 3 "NATURE AND PURPOSE OF PROCESSING":

1. eMaint Enterprises LLC, 3181 N Bay Village Ct, Bonita Springs, FL 34135, United States
2. eMaint EMEA Limited, The Old Distillery Building, Beresford Street, Smithfield, Dublin 7, Ireland
3. Fluke Deutschland GmbH, In den Engematten 14, 79286 Glottertal, Germany
4. Fluke Europe B.V., BIC 1, 5657 BX Eindhoven, Netherlands
5. Fluke Nederland B.V., BIC 1, 5657 BX Eindhoven, Netherlands
6. Fluke do Brasil Ltda., Av. Maria Coelho Aguiar, 215, Bloco F, Piso Panamby – loja 84c, Jardim São Luis, São Paulo 05805-000, Brazil
7. Prüftechnik-Wibrem sp.z.o.o, UL. Tyniecka 17, Wroclaw 52407, Poland
8. Prüftechnik Technology sp.zo.o, UL. Tyniecka 17, Wroclaw 52407, Poland

eMaint has additionally appointed the following Sub-Processors:

9. Fluke Corporation, 6920 Seaway Blvd, Everett WA 98204, U.S.A
    a. An affiliated company of eMaint
    b. Activities: Point 6. of Section 3 "NATURE AND PURPOSE OF PROCESSING".
10. Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A and Amazon Web Services EMEA SARL, 5 rue Plaetis, L-2338 Luxembourg and their sub-processors listed at https://aws.amazon.com/compliance/sub-processors/, as updated from time to time by them.
    a. A service provider of eMaint
    b. Processing occurs in Germany, or, where agreed with the customer, in the United States or UK, depending on the Customer's site location.
    c. Activities: Cloud-based service eMaint, providing hosting for personal and other data and infrastructure services that is used to provide the Services.
11. GuideCX, Inc., 392 E 12300 S, Draper, UT 84020
    a. A service provider of eMaint
    b. Activities: GuideCX processes data related to customer onboarding that is used to provide the Services. This includes organizational data and some personal data for the Customer and/or their Users involved in the onboarding process.

## Data Protection Appendix (CCPA)

eMaint shall process Personal Data only as necessary for the specific limited purposes of performing the Services under this Agreement on behalf of Customer and for any business purpose permitted by the California Consumer Privacy Act ("CCPA").

In addition, eMaint shall not (i) sell or share (as those terms are defined by the CCPA) any Personal Data received from Customer; or (ii) retain, use, or disclose the Personal Data provided by or collected on behalf of Customer for any purpose other than for the specific purpose of performing the services specified in the Agreement and for any business purpose, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the services specified in this Agreement and as permitted by the CCPA; (iii) retain, use, or disclose the Personal Data provided by or collected on behalf of Customer outside of the direct business relationship between eMaint and Customer; or (iv) combine the Personal Data provided by or collected on behalf of Customer with Personal Data Fluke receives from or on behalf of any other customer or person, except to the extent such combination is required by the Services under this Agreement or to perform any business purpose under the CCPA or regulations adopted pursuant to the CCPA.

eMaint further agrees: (i) to comply with its CCPA obligations and provide the same level of privacy protection as required by CCPA; (ii) to permit Customer to take reasonable and appropriate steps to help to ensure that eMaint uses the Personal Data in a manner consistent with Customer's obligations under CCPA; (iii) to notify Customer if eMaint determines it can no longer meet its CCPA obligations; and (iv) to permit Customer, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer's Personal Data.