Appendix A Customer Data Processing

This Appendix is incorporated by reference and is an integral part of the Partner Agreement between Tektronix, or its named affiliate (referred to as "Tektronix" in this Appendix), and the Partner. All definitions used in this Appendix are the same as provided in the Agreement unless explicitly provided herein.

1. **Role of the Parties**

1.1. Appointment of Partner as Processor. Tektronix appoints Partner to process Personal Data on its behalf as is necessary for the performance of the terms and objectives of this Agreement, as further detailed in Schedule 1 – Partner Data Processing Obligations to this Appendix. The Parties agree that in relation to such processing, Tektronix shall be the Data Controller and the Partner (and each permitted subcontractor or third party pursuant to this Agreement) shall be the Data Processor. Such processing shall be subject to Schedule 1 – Partner Data Processing Obligations.

1.2 Partner Acting as Independent Controller. If and to the extent that the Partner uses Tektronix Personal Data to make sales directly to customers in the Partner's own name or otherwise than according to Tektronix's instructions or the provisions in Schedule 1 to this Appendix, the Partner shall be the Data Controller of any Personal Data Processed in connection with such customers and shall be responsible for its own compliance with Data Protection Laws.

1.3 Lead Generation Activities. If and to the extent that the Partner provides Tektronix with Personal Data it has sourced and collected independently of any instructions from Tektronix or the provisions in Schedule 1 to this Appendix, unless the Parties have agreed otherwise in writing, each Party is an independent Data Controller and shall be responsible for its own compliance with Data Protection Laws. Partner shall adhere to the terms and conditions of Schedule 2 – Partner Lead Generation to this Appendix when providing Lead Data (as defined in Schedule 2) to Tektronix under this Agreement.

Schedule 1

Customer Data Processing Obligations

DEFINITIONS AND INTERPRETATION

1.1 **Definitions**

"**Data Protection Laws**" means any law, enactment, regulation, regulatory policy, by law, ordinance or subordinate legislation relating to the processing, privacy, and use of Personal Data, as applicable to Tektronix, the Partner and/or the Services, including:

(a) in EEA countries: the General Data Protection Regulation ((EU) 2016/679) ("EU GDPR") and the ePrivacy Directive;

(b) in the UK: the Data Protection Act 2018, the "UK GDPR" (as defined by section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018), the Privacy and Electronic Communications Regulations 2003 and the Council Directive 2002/58/EC ("ePrivacy Directive")(collectively referred to as "UK Data Protection Laws");

(c) in Korea: the Personal Information Protection Act (**PIPA**) of 2011, as amended, and any laws or regulations of the Personal Information Protection Commission (**PIPC**) giving effect to or corresponding with PIPA;

(d) in Switzerland: the Federal Act on Data Protection ("FADP");

(e) California Consumer Protection Act ("CCPA"); and

(f) all applicable relevant laws or regulations and giving effect or corresponding to the above laws and any judicial or administrative interpretation of any of the above, and any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority.

Data Processing Losses " means all liabilities and amounts, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, charges, costs (including legal costs), claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (including relating to material or non-material damage, which includes emotional distress);

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(ii) compensation paid to a Data Subject; and

(iii) the reasonable costs of compliance with investigations by a Supervisory Authority; and

(c) the costs of loading Tektronix data and replacement of Tektronix materials and equipment, to the extent the same are lost, damaged or destroyed, and any loss or corruption of Tektronix data, including the costs of rectification or restoration of Tektronix data;

"**Data Subject Request**" means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

"**Complaint**" means a complaint or request relating to either party's obligations under Data Protection Laws relevant to this agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

"**DPIA**" means a data protection impact assessment or privacy impact assessment (as defined or used in the Data Protection Laws, including relevant guidance from Supervisory Authorities);

"**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

"**Protected Data**" means Personal Data received from or made available or accessible by or on behalf of Tektronix, or otherwise obtained in connection with the performance of the Partner's obligations under this agreement;

"**Protective Measures**" means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

"**Security Measures**" means Tektronix's security policies and measures (including IT policies and measures) for the protection of Personal Data issued to Partner by Tektronix from time to time, which as at the date hereof are as specified in Exhibit 1.

"**Sub-Processor**" means another Data Processor engaged by the Partner for carrying out processing activities in respect of the Protected Data on behalf of Tektronix, and authorised by Tektronix in accordance with clause;

"**Supervisory Authority**" means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

1.2 Interpretation

In this agreement:

1.2.1 <="" span="" style="box-sizing: border-box;">"**Data Controller**" (or "controller"), "**Data Processor**" (or "processor"), "**Data Subject**", "**international organisation**", "**Personal Data**" and **processing**" and all have the meanings given to those terms in Data Protection Laws (and related terms such as "**process**" have corresponding meanings);

1.2.2 references to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting

or consolidating such Applicable Law and the equivalent terms defined in such Applicable Laws, once in force and applicable;

1.2.3 clause 1 (below) (Data Protection) shall survive termination (for any reason) or expiry of this agreement (or of any of the Services).

1. Data protection

1.1 Data Controller and Appointment of Data Processor

The parties agree that, for the Protected Data, Tektronix shall be the Data Controller and the Partner shall be the Data Processor.

1.2 Compliance with Data Protection Laws and obligations

The Partner shall comply with 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.

The Partner shall procure that any Sub-Processor that has access to Protected Data shall comply with the Partner's obligations under this clause

. Tektronix shall comply with all Data Protection Laws in respect of the performance of its obligations under this agreement.

1.3 Details of processing and instructions

The processing to be carried out by the Partner under this agreement shall comprise the processing set out in Schedule (*Data Processing Details*), as updated from time to time by Tektronix.

Insofar as the Partner processes Protected Data on behalf of Tektronix, the Partner:

unless required to do otherwise by Applicable Law, shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with Tektronix's documented instructions as set out in this clause and Schedule 1.3.1 *(Data Processing Details)*, and as updated from time to time by the written agreement of the parties ("**Processing Instructions**");

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

shall immediately inform Tektronix in writing if, in the Partner's reasonable opinion, a Tektronix instruction infringes Data Protection Laws and explain the reasons for such opinion

1.4 **Technical and organisational measures**

The Partner shall implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the processing of Protected Data by the Partner:

such that the processing will meet the requirements of Data Protection Laws and ensure the protection of the rights of Data Subjects;

so as toensure a level of security in respect of Protected Data processed by it appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data transmitted, stored or otherwise processed; and

<="" span="" style="box-sizing: border-box; font: 7pt "Times New Roman";">without prejudice to clause, insofar as is possible, to assist Tektronix in the fulfilment of Tektronix's obligations to respond to Data Subject Requests relating to Protected Data.

1.5 **Security of processing**

Without prejudice to clause 1.4.1(b), the Partner shall, in respect of all Protected Data processed by it, comply with the requirements regarding security of processing set out in Data Protection Laws and in this agreement and all relevant Tektronix Policies. The Partner shall ensure that the Security Measures are the minimum security standards governing Partner's processing of the Protected Data.

1.6 **Using other Sub-Processors**

The Partner shall not engage any third party to process the Protected Data without Tektronix's prior written consent.

If Tektronix gives its consent for such third party to act as a Sub-Processor, the Partner shall, prior to any processing of Protected Data by the Sub-Processor, appoint the Sub-Processor under a binding written contract, with enforceable data protection obligations on the same terms, or terms more onerous than those, that apply to the Partner under this clause 1 ("**Processor Contract**"), including in particular that the Sub-Processor:

provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Data Protection Laws; and

must obtain Tektronix's prior written consent and comply with the conditions referred to in this clause1.6 for engaging another Data Processor.

The Partner shall:

promptly upon request by Tektronix provide the relevant details of any such Processor Contract to Tektronix;

& where that Sub-Processor fails to fulfil its data protection obligations in accordance with the Processor Contract, remain fully liable to Tektronix for the performance of that Sub-Processor's obligations;and

immediately cease using a Sub-Processor to process Protected Data upon receiving written notice from Tektronix requesting that the Sub-Processor ceases processing Protected Data for security reasons or concerns about the Sub-Processor's ability to carry out the relevant processing in compliance with Data Protection Laws or this agreement.

1.7 **Personnel requirements**

The Partner shall:

ensure that Partner Personnel (and shall procure that Sub-Processor personnel) processing Protected Data have entered into a binding contractual obligation with the Partner to keep the Protected Data confidential (except where disclosure is required by Applicable Law, in which case the Partner shall, where practicable and not prohibited by such Applicable Law, notify Tektronix of any such requirement before such disclosure); and

ensure the reliability of the Partner Personnel processing Protected Data and further ensure that the Partner Personnel processing Protected Data receive adequate training on compliance with this clause 1 and the Data Protection Laws applicable to the processing.

1.8 **Data Subject rights**

The Partner shall:

at no cost to Tektronix, record and then refer all Data Subject Requests which the Partner receives to Tektronix within three days of receipt of the Data Subject Requests;

at its cost and expense, provide such information and cooperation and other assistance as Tektronix requests in relation to a Data Subject Request within the timescales reasonably required by Tektronix ; and

not respond to any Data Subject Request without Tektronix's prior written authorisation.

1.9 **Assistance with Tektronix's compliance**

The Partner shall, at its own cost and expense, provide such information, cooperation and other assistance as Tektronix requests ensure Tektronix's compliance with its obligations under Data Protection Laws, including with respect to:

<=”" span="" style="box-sizing: border-box; font: 7pt "Times New Roman";">security of processing;

any remedial action and notifications to be taken in response to any Personal Data Breach or Complaint, including (subject in each case to Tektronix's prior written authorisation) regarding notification of the Personal Data Breach to Supervisory Authorities and/or communication to affected Data Subjects, including in accordance with clause 1.13;

DPIAs, by promptly providing such information and cooperation as Tektronix may reasonably require for the purpose of assisting Tektronix in carrying out a DPIA, and periodic reviews to assess if the processing of Protected Data is performed in compliance with the outcomes of the DPIA;

prior consultation with a Supervisory Authority regarding high risk processing, by promptly and in consultation with Tektronix :

providing such information and cooperation as Tektronix or a Supervisory Authority requests for the purpose of assisting in any consultation by Tektronix with the Supervisor Authority; and

complying with any advice by a Supervisory Authority concerning the Partner's processing activities related to this agreement

1.10 **International data transfers**

The Partner shall not (and shall procure that any Sub Processor or subcontractor shall not) transfer, or allow the onward transfer of, any Protected Data to any country outside of Korea or to any international organisation (individually and collectively, an "**International Recipient**") without Tektronix's prior written consent.

If Tektronix consents to the transfer of Protected Data to an International Recipient, the Partner shall ensure that such transfer (and any subsequent onward transfer):

is pursuant to a written contract including equivalent or more onerous obligations on the Sub-Processor in respect of the Protected Data (in particular relating to security and confidentiality) as apply to the Partner under this clause 1;

is effected by way of Protective Measures, the form of which being subject to Tektronix's prior written approval which shall not be unreasonably withheld or delayed);

complies with clause 1.2.1 and any requirements specified in Schedule 1.3.1 including the Security Measures; and

otherwise complies with Data Protection Laws

1.11 **Records**

The Partner shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of Tektronix, containing such information as Tektronix may reasonably require, including:

<="" span="" style="box-sizing: border-box; font: 7pt "Times New Roman";">the name and contact details of the Data Processor(s) and of each Data Controller on behalf of which the Data Processor is acting, and of the Partner's representative and data protection officer (if any);

the categories of processing carried out on behalf of each Data Controller;

where applicable, details of transfers of Protected Data to an International Recipient, including the identification of that International Recipient and the relevant countries to which such data is transferred, and details of the Protective Measures used; and

a general description of the technical and organisational security measures referred to in clause 1.4.1(b).

1.12 **Compliance, information and audit**

The Partner shall (and shall procure that its Sub-Processors) make available to Tektronix on request in a timely manner (and in any event within three days):

copies of the records under clause 1.11; and

such other information as Tektronix reasonably requires to demonstrate the Partner's compliance with its obligations under Data Protection Laws and this agreement, including sufficiently detailed information about the technical and organisational measures that are implemented and maintained by the Partner.

The Partner shall (and shall procure that its Sub-Processors shall) allow for and contribute to audits, including inspections, conducted by Tektronix or another auditor mandated by Tektronix for the purpose of demonstrating compliance by the Partner with its obligations under Data Protection Laws and under this clause 1 including allowing reasonable access for Tektronix or such other auditor to:

<="" span="" style="box-sizing: border-box; font: 7pt "Times New Roman";">the facilities, equipment, premises and sites on which Protected Data and/or the records referred to

in clause 1.11 are held, and to any other equipment or facilities used in the provision of the Services (in each case whether or not owned or controlled by the Partner); and

the Partner Personnel,

provided that Tektronix shall, where practicable, give the Partner reasonable prior notice of such audit and/or inspection and conduct the same during normal business hours.

If any audit or inspection reveals a material noncompliance by the Partner with its obligations under Data Protection Laws or a breach by the Partner of its data protection obligations under this agreement, the Partner shall promptly on request:

pay the reasonable costs of Tektronix or its mandated auditors for the audit or inspection; and

resolve (and shall procure that its Sub-Processors likewise resolve), at its own cost and expense, all instances of data protection or security noncompliance discovered by Tektronix and reported to the Partner that reveal a breach or potential breach by the Partner (or a Sub-Processor) of its obligations under this clause 1.

Tektronix may share any notification, details, records or information provided by or on behalf of the Partner under this clause 1.12 or clause 1.13 with its respective affiliates, professional advisors, and any Supervisory Authority.

If the Partner (or a Sub-Processor) is in breach of its obligations under this clause 1, Tektronix may suspend the transfer of Protected Data to the Partner until the breach is remedied.

1.13 **Notification of Personal Data Breaches and Complaints**

In respect of any actual or suspected Personal Data Breach involving the Partner or a Sub-Processor, the Partner shall:

notify Tektronix of the Personal Data Breach without undue delay, but in no event later than twelve hours after becoming aware of such Persona Data Breach; and

provide Tektronix without undue delay, wherever possible no later than twenty-four hours after becoming aware of such Personal Data Breach, with such details as Tektronix require regarding:

the nature of such Personal Data Breach, including the categories and approximate numbers of Data Subjects and Persona Data records concerned;

any investigations into such Personal Data Breach;

the likely consequences of such Personal Data Breach; and

any measures taken, or that the Partner recommends to take, to address such Personal Data Breach, including to mitigate its possible adverse effects and prevent the re-occurrence of such Personal Data Breach or a similar breach,

provided that, without prejudice to the above obligations, if the Partner cannot provide all these details within the aforesaid timeframe, it shall in any event before the end of said timeframe provide Tektronix with its reasons for the delay and an expectation for when it reasonably expects to be able to provide Tektronix with such details

The Partner shall promptly and in any event within two days inform Tektronix if it receives a Complaint and provide Tektronix with full details of such Complaint.

1.14 **Deletion or return of Protected Data and copies**

The Partner shall without delay:

at Tektronix's written request, either securely delete or securely return all the Protected Data to Tektronix in such form as Tektronix reasonably requests, after the earlier of:

the end of the provision of the relevant Services related to processing; or

once processing by the Partner of any Protected Data is no longer required for the purpose of the Partner's performance of its relevant obligations under this agreement; and

securely delete all other existing copies of the Protected Data, except only for those copies that are required to be stored by Applicable Law and, in which case, the Partner shall inform Tektronix of any such requirement; and

upon full performance of its obligations unde this clause 1.14, provide Tektronix with a written declaration of such performance.

1.15 **Liability and indemnities**

The Partner shall indemnify and keep indemnified Tektronix in respect of all Data Processing Losses suffered or incurred by, awarded against or agreed to be paid by, Tektronix or any affiliate thereof, arising from or in connection with:

any breach by the Partner of its obligations under this clause1 or of Data Protection Laws; or

the Partner (or any person acting on its behalf) acting outside or contrary to the lawful Processing Instructions ofTektronix in respect of the processing of Protected Data.

This clause 18 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

to the extent not permitted by Applicable Law (including Data Protection Laws);and

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

Exhibit 1 to Schedule 1
Security Measures

Technical Measures to Ensure Security of Processing	
1. Inventory and Control of Hardware Assets	**Actively manage all hardware devices on the network so and unauthorised and unmanaged devices are found and**
2. Inventory and Control of Software Assets	**Actively manage all software on the network so that onl execute, and that unauthorised and unmanaged softwar execution.**
3. Continuous Vulnerability Management	**Continuously acquire, assess, and take action on new inf remediate, and minimize the window of opportunity for**
4. Controlled Use of Administrative Privileges	**Maintain processes and tools to track, control, prevent, a configuration of administrative privileges on computers,**
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	**Implement and actively manage (track, report on, correc laptops, servers, and workstations using a configuration order to prevent attackers from exploiting vulnerable se**

6. Maintenance, Monitoring, and Analysis of Audit Logs -	**Collect, manage, and analyse audit and security logs of e recover from a possible attack.**
7. Email and Web Browser Protections	**Deploy automated controls to minimise the attack surfa manipulate human behaviour through their interaction v** -
8. Malware Defences -	**Control the installation, spread, and execution of malicio while optimising the use of automation to enable rapid u corrective action.** -
9. Limitation and Control of Network Ports, Protocols, and Services -	**Manage (track, control, correct) the ongoing operational applications on networked devices in order to minimise to attackers.** -
10. Data Recovery Capabilities -	**Maintain processes and tools to properly back up perso the confidentiality, integrity, availability, and recoverabil** -
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches -	**Implement, and actively manage (track, report on, corre infrastructure devices using a configuration managemen attackers from exploiting vulnerable services and setting** -
12. Boundary Defences -	**Detect, prevent, and correct the flow of information tra focus on personal data.** -
13. Data Protection -	**Maintain processes and tools used to prevent data exfilt and ensure the confidentiality and integrity of personal** -
14. Controlled Access Based on the Need to Know -	**Maintain processes and tools to track, control, prevent, a assets (e.g. information, resources, systems) according t**

	computers, and applications have a need and right to ac an approved classification.
15. Wireless Access Control	Maintain processes and tools to track, control, prevent, a networks (WLANs), access points, and wireless client sys
16. Account Monitoring and Control	Actively manage the life cycle of system and application deletion in order to minimise opportunities for unautho

Organizational Measures

Organisational Measures to Ensure Security of Processing	
1. Implement a Comprehensive Information Security Programme	Through the implementation of a Comprehensive Information S administrative safeguards to protect personal data. These measu security, confidentiality and integrity of personal data protection against unauthorized access to or use of (stored) pers risk of identity theft or fraud that employees, contractors, consultants, temporaries, and othe 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 b personal data), identify the specific knowledge, skills and abilitie

	of personal data; develop and execute an integrated plan to asse organisational planning, training, and awareness programmes.
3. Application Software Security	**Manage the security life cycle of all in-house developed and acq correct security weaknesses.**
4. Incident Response and Management	**Protect the organisation's information, including personal data, implementing an incident response infrastructure (e.g., plans, de management oversight, retainers, and insurance) for quickly disc containing the damage, eradicating the attacker's presence, and network and systems.**
5. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises	**Test the overall strength of the organisation's defence (the techn objectives and actions of an attacker; as well as, assess and valid organisation's privacy and personal data protections.**
6. Physical Security and Entry Control	**Require that all facilities meet the highest level of data protectio circumstances relevant to the facility and the data it contains, pr**

Exhibit 2 to Schedule 1
Data Processing Details

1. Subject Matter of Processing

The Partner will be processing personal data in the course of providing the Services.

2. Duration of the processing

The processing will be carried out for the term of this Agreement.

3. **Nature and Purpose of the Processing**

The data is processed in order to perform the terms and objectives of this Agreement, including but not limited to following-up on and qualifying sales leads on behalf of Tektronix, lead generation activity on behalf of Tektronix.

4. **Type of Personal Data**

The data processed includes, but is not limited to, name, address, telephone number, email address, application, industry, job function and Products or possible products of affiliated companies purchased.

5. **Special categories of personal data and description of applied restrictions or safeguards**

N/a

6. **Categories of Data Subjects**

Data subjects include individuals being or representing existing customers using Tektronix products, past customers of Tektronix products and prospects that are potential customers for Tektronix products.

7. **Approved Sub-processors**

n/a.

8. **Additional Instructions**

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

Schedule 2 – Partner Lead Generation

1. **Lead Data.** In connection with the Agreement, the Partner may provide Tektronix with lead generation data (collectively, "**Lead Data**") as described in and for the limited and specified purposes identified in Exhibit 1 ("Data Processing Details") to this Schedule.

2. **Lead Data requirements.** Partner represents and warrants that the Lead Data provided to Tektronix will be accurate, up-to-date, free of errors and will not include:
   i. Special categories of personal data or sensitive data as defined under Applicable Privacy Laws (as defined below); or

ii. information about data subjects who are under the age of majority, are located outside of the Geographical scope indicated in Exhibit 1 to this Appendix or who have requested deletion of their data, or have otherwise opted-out from the sale, sharing, or disclosure of their data.

Lead Data shall only be collected from leads who have expressly opted-in to receive marketing communications regarding Tektronix products and services.

3. **Compliance with applicable law; privacy policy**

Each Party represents and warrants that, with respect to the Lead Data, such party shall comply with and provide the same level of protection required by all applicable international, foreign, federal, state, provincial, and local laws, executive orders, rules, regulations, ordinances, codes, orders, and decrees of all governments or agencies of any U.S. or applicable foreign jurisdictions, including but not limited to (where applicable) anti-spam regulation, data brokerage regulation, marketing and advertising regulations, the U.S. Telephone Consumer Protection Act, the California Consumer Privacy Act, the General Data Protection Regulation, and anti-corruption laws such as the US Foreign Corrupt Practices Act and UK Bribery Act 2010 (collectively, "**Applicable Privacy Laws**").

Partner further represents and warrants that (i) its processing (including collection and disclosure) of Lead Data shall comply with all applicable industry best practices; (ii) Partner will maintain and at all times act in accordance with a publicly-accessible privacy policy on its mobile applications and websites that is available via a prominent link in compliance with the requirements of Applicable Privacy Laws; and (iii) Partner's provision of the Lead Data to Tektronix does not violate any agreement or obligation between Partner and a third party. Partner (i) shall notify Tektronix in the event that it makes a determination that it is no longer able to meet the requirements under this Section; and (ii) shall have the right, solely where and to the extent afforded by Applicable Privacy Law, to take reasonable and appropriate steps to ensure the other party meets its obligations under this Appendix and to discontinue and remediate any unauthorized processing of Lead Data hereunder.

4. **Data collection; data handling.** Partner represents and warrants that:

i. Requisite rights. Partner has all requisite rights and has provided and/or obtained all data subject notices and/or consents required under Applicable Privacy Laws sufficient to allow Tektronix to (i) receive and use the Lead Data pursuant to the Agreement with no further action required on Tektronix's part and (ii) transfer Lead Data internationally, including to the United States or other regions as may be required.

ii. Records of consent and notice. Partner will create, retain, and make available to Tektronix, upon request, full records of all consents obtained, and notices provided in connection with the Lead Data processed pursuant to the Agreement. Such records shall be sufficient to prove the validity of the consents and notices under applicable law and shall include, without limitation: (i) the specific source of the consent (e.g., website), (ii) the form of request of consent, (iii) the date and time consent was obtained, and (iv) any and all unsubscribe or opt out requests and

actions. This obligation shall survive the termination of the Agreement for a period of three years.

iii. Notice and cooperation. To the extent applicable, Partner will provide Tektronix with immediate notice of and provide Tektronix with reasonable cooperation in responding to:

i. any notice, inquiry, complaint, or claim made by any individual or third Parties (including any government or regulatory authority) in connection with the Lead Data;

ii. any opt-out, withdrawal of consent, request for deletion, or related request in connection with Lead Data; or

iii. any breach by Partner of its obligations hereunder.

iv. Security of data. Partner will implement and maintain commercially reasonable administrative, technical and physical safeguards which at a minimum: (i) are reasonable and appropriate, given the nature of the data, to protect such data from unauthorized or illegal access, destruction, use, modification, or disclosure; and (ii) comply with requirements under Applicable Privacy Laws to safeguard the Lead Data.

v. Roles of the Parties. With respect to the Lead Data, the Parties will act as independent controllers or Business (as defined under California Consumer Privacy Act (CCPA)) (collectively "controller") under Applicable Privacy Laws.

5. **Tektronix Personal Data, data enrichment and related services.** For the avoidance of doubt, the rights and obligations set forth under this Schedule 2 do not apply to personal data which Partner processes on behalf of Tektronix in the role of a data processor (or substantially similar term under Applicable Privacy Laws) including, without limitation, any data provided to Partner (directly or indirectly) for the purposes of data enrichment or related services (collectively, "**Tektronix Personal Data**").