# DATA PROTECTION TERMS

## 1. ACCEPTANCE

TrustMotion's Purchase Order ("**PO**"), including these Data Protection Terms ("**DPTs**"), is TrustMotion's offer to Supplier. Upon acceptance by Supplier, either by acknowledgement, commencement of services or shipment of goods, by delivery of any items ordered, or otherwise where Data is processed, TrustMotion's PO, including these DPTs, shall become binding. These DPTs, together with TrustMotion's General Terms and Conditions of Purchase and the PO constitute the entire agreement between TrustMotion and Supplier, "**Agreement**").

These DPTs are intended to satisfy legal requirements under Data Protection Laws. Capitalized terms not defined in these DPTs will have the meanings given to them in the PO or TrustMotion's General Terms and Conditions of Purchase.

## 2. DPTs STRUCTURE

Depending on the Supplier being categorized as Controller or Processor, one of the following sections will apply:

- Where Personal Data is being processed whereby TrustMotion acts as Controller and Supplier as Controller, **APPENDIX A** shall apply.
- Where Personal Data is being processed whereby TrustMotion acts as Controller and Supplier as Processor, **APPENDIX B** shall apply.
- Where Data is being transferred by TrustMotion to Supplier, **APPENDIX C** will apply.

## 3. DEFINITIONS

For the purposes of this document, the following terms shall have the meanings set forth below:

| | |
|---|---|
| **Controller** | the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, and for the purpose of these Data Privacy Terms the Controller is TrustMotion. |
| **Data** | any information transferred by TrustMotion to Supplier, including Personal Data. |

| | |
|---|---|
| **Data Processing Agreement** | applicable agreement describing the purpose, agreed responsibilities and requirements with regards to the processing of Personal Data amongst the parties, as taken up in **APPENDIX B** of these DPTs. |
| **Data Protection Impact Assessment** | an assessment of the impact of the envisaged processing operations on the protection of Personal Data, as may be required under applicable Data Protection Laws. |
| **Data Protection Laws** | all applicable data protection, data privacy, and cybersecurity laws, rules, and regulations anywhere in the world in force from time to time to which the TrustMotion's Personal Data is subject. Data Protection Laws shall include, but are not limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"), the EU General Data Protection Regulation 2016/679 ("**GDPR**"), and the Chinese Personal Protection Law ("**PIPL**"). |
| **Data Subject** | the individual whose personal data is subject to the processing activity. |
| **Party** or **Parties** | the parties to the Agreement. |
| **Personal Data** | any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly. |
| **Processing** | any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. |
| **Processor** | a data processor is a person, company, or other body which processes personal data on the Data Controller's behalf. |
| **SCCs** or **Standard Contractual Clauses** | the clauses as set out in the Commission Implementing Decision (EU)2021/914 for the transfer of Personal Data to countries outside the EEA pursuant to the GDPR, as updated, amended, replaced and superseded from time to time. |
| **Services** | means the services and or goods which Supplier provides pursuant to the PO. |

| | |
|---|---|
| **Sub-Processor** | a sub-processor acts under the instructions of the processor, meaning that they may process individuals' Personal Data on behalf of the Processor. A sub-processor can be a legal person, for example a business, an SME, a public authority, an agency or other body. |
| **Supplier** | Person/organization that provides the Services. |
| **Technical and Organizational Measures** or **TOMs** | is a description of the measures implemented by the Supplier to ensure an appropriate level of security is maintained throughout Processing of Data. |
| **TrustMotion** | the TrustMotion entity listed on the Purchase Order. |

## 4. GENERAL TERMS

### 4.1. Modifications

TrustMotion reserves the right to make modifications, amendments and supplements to these DPTs in case of changes in Data Protection Laws. Should a provision of these DPTs become unenforceable, that provision shall not affect the validity or enforceability of any other provisions of these DPTs.

### 4.2. Termination or Expiration of the Privacy Terms

(a) The terms contained herein shall terminate or expire upon completion or termination of the Service procured under which Personal Data is being processed under the PO.

(b) Within thirty (30) days of termination or expiration of this Agreement, the Supplier shall, unless otherwise agreed, erase all Personal Data, provided there is no duty to preserve records due to statutory retention periods, after which Supplier shall certify to TrustMotion that this has been done. In the case there is a duty to preserve Personal Data due to statutory retention periods, Supplier agrees to be bound by the applicable terms contained herein for the period required by statutory law.

(c) TrustMotion may terminate the Agreement without notice in case of Supplier's breach of the terms of the DPTs or Supplier's breach of Data Protection Laws resulting in a situation where TrustMotion cannot reasonably be expected to continue the Data Processing until termination and/or expiration of the Agreement.

### 4.3. Miscellaneous

(a) In case any of TrustMotion's property rights are at risk in the office premises of the Supplier due to measures taken by third parties (e.g. through seizures or confiscation), insolvency proceedings or any other events, the Supplier shall promptly inform TrustMotion hereof. The Supplier waives the right of lien in respect to storage media and datasets.

(b) If not otherwise stated herein, these DPTs will be governed by, construed, and enforced in accordance with the laws of the Austria as if entered by citizens thereof to be performed wholly within that jurisdiction and without regard to its conflict of laws provision.

(c) Except for actions seeking temporary injunctive relief for a breach or threatened breach of a Party's confidentiality obligations or with respect to trademarks, trade secrets, or other intellectual property claims, all disputes arising out of or in relation to this Agreement will first be attempted by the Parties to be resolved through discussion, negotiation and consultation in good faith and a spirit of cooperation. All such disputes not resolved within 60 days from the date the relevant dispute first arose may be submitted to a court of competent jurisdiction.

(d) **Contact Persons**. In case of any inquiries, and/or concerns, feel free to reach out to TrustMotion's data protection board through contacting the following email address: dataprotection@trustmotion.com.

# APPENDIX A
# TRUSTMOTION AND SUPPLIER ACT AS CONTROLLERS

## 1. STANDARD CONTRACTUAL CLAUSES

When there is a transfer of Personal Data, pursuant to the GDPR, to a Supplier located outside of the European Economic Area whilst there is no adequacy decision or any other transfer mechanism in place, the Standard Contractual Clauses Module 1 will apply. In all other instances, Section 2 of **APPENDIX A** of these DPTs, 'Controller to Controller' will apply.

Specifically, the following deviations to the Model 1 SCCs will apply:

- Clause 7 (Docking Clause): Not Applicable
- Clause 17 (Governing Law): The SCCs shall be governed by the law of The Netherlands.
- Clause 18 (Choice of forum and jurisdiction), sub-section (b): The choice of forum and jurisdiction shall be the courts of The Netherlands.
- ANNEX I.A (List of Parties): Specified in PO.
- ANNEX I.B (Description of Transfer): Specified in PO.
- ANNEX I.C (Competent Supervisory Authority): Austrian Data Protection Authority (Österreichische Datenschutzbehörde - DSB) TrustMotion's headquater is based in Austria.
- ANNEX II (Technical and Organisational Measures): Specified in **APPENDIX C**.

## 2. CONTROLLER TO CONTROLLER

For the performance of the Services each Party will solely be responsible and comply with their respective obligations under Data Protection Laws relating to the Processing of Personal Data in force during the term the Service is being provided. In furtherance of this commitment, the Parties undertake to:

(i) handle Personal Data relating to individuals, only if this Personal Data has been collected and processed fairly and lawfully;

(ii) ensure that they have duly informed the individual whose Personal Data is being processed in accordance with the Data Protection Laws and have established a valid legal basis, in particular with regard to the processing made by the Parties for the purposes of the Service;

(iii) where applicable, ensure individuals whose Personal Data is being processed can exercise their data protection rights;

(iv) process Personal Data only for the purposes strictly necessary for the provisioning of the Service;

(v) if required to share with third parties, to share the Personal Data only with third parties who offer the same guarantees as those defined herein;

(vi) safeguard the transfer of the Personal Data to any other country by means of required data transfer mechanisms, and specifically in the case the Supplier is located within the European Economic Area, to refrain from transferring Personal Data to third parties located outside the European Economic Area unless 1) the Supplier and the third party have entered into the appropriate EU Standard Contractual Clauses, 2) the Parties have implemented binding corporate rules that have received European approval and that cover all Personal Data that Parties will receive in their capacity of Controller, 3) the countries where Parties will process such Personal Data have received a binding adequacy decision by the European Commission, or 4) another validly executed transfer mechanism applies to the transfer of Personal Data to such countries that have not received a binding adequacy decision by the European Commission;

(vii) implement technical and organizational measures to ensure an adequate level of protection of the Personal Data, which are no less protective than those stipulated in **APPENDIX C**; and

(viii) delete the Personal Data when it is no longer necessary for the purposes of the Services, or at the request of the Party which provided it.

# APPENDIX B
# TRUSTMOTION AS CONTROLLER AND SUPPLIER AS PROCESSOR

The terms of this **APPENDIX B** shall be referred to as the Data Processing Agreement (the "DPA") and will apply to the processing of TrustMotion's Personal Data by Supplier acting as the Processor. TrustMotion hereby instructs Supplier to Process TrustMotion's Personal Data solely to the extent necessary to provide the Services to TrustMotion. Supplier is not entitled to Process TrustMotion Personal Data for its own purposes including, without limitation, sharing TrustMotion Personal Data with third parties (other than approved Sub-processors). Supplier will only Process TrustMotion Personal Data on behalf of TrustMotion and solely for the purpose of providing the Services.

When there is a transfer of Personal Data, pursuant to the GDPR, to a Supplier located outside of the European Economic Area whilst there is no adequacy decision or any other transfer mechanism in place, the Standard Contractual Clauses Module 2 will apply. Specifically, the following deviations to the Model 2 SCCs will apply:

- Clause 7 (Docking Clause): Not Applicable.
- Clause 9 (Use of sub-processors): Option 2 "General Written Authorization" is chosen.
- Clause 17 (Governing Law): The SCCs shall be governed by the law of The Netherlands.
- Clause 18 (Choice of forum and jurisdiction), sub-section (b): The choice of forum and jurisdiction shall be the courts of The Netherlands.
- ANNEX I.A (List of Parties): Specified in PO.
- ANNEX I.B (Description of Transfer): Specified in PO.
- ANNEX I.C (Competent Supervisory Authority): ): Austrian Data Protection Authority (Österreichische Datenschutzbehörde - DSB) TrustMotion's headquarter is based in Austria.
- ANNEX II (Technical and Organizational Measures): Specified in **APPENDIX C**.

In all other cases the terms and conditions of this DPA will be applicable.

## 1. Subject of the DPA and Term

The Processor performs Services for the Controller pursuant to the PO which these terms are referenced to.

## 2. Processing Under Instruction of the Controller

2.1. The Controller is responsible for compliance with the relevant Data Protection Laws, in particular for the lawfulness of the Data Processing and for safeguarding the Data Subjects'

statutory rights, as stipulated by the applicable Data Protection Laws. Statutory or contractual liability provisions shall remain unaffected.

2.2. The Processor shall Process the Personal Data disclosed by the Controller solely under the instructions of the Controller and within the scope of the agreed Services and stipulations. Data must only be corrected, erased or blocked subject to the instruction of the Controller.

2.3. The Processor must only Process Data under the Controller's instruction, unless processing of certain Personal Data is required by Data Protection Laws to which the Processor is subject to. In such a case, the Processor shall inform the Controller of that legal requirement prior to Processing, unless that law prohibits such information on important grounds of public interest.

2.4. The instructions of the Controller require no specific form. Verbal instructions may be documented by the Controller. Upon request of the Processor, the Controller shall provide the Processing instructions in writing.

2.5. The Processor shall inform the Controller without undue delay if it believes that an instruction given by the Controller infringes upon applicable Data Protection Laws.

## 3. Technical and Organizational Measures

3.1. The Processor shall implement adequate technical and organizational security measures, as stipulated in **APPENDIX C** of these DPTs for the agreed Data Processing and is obliged to document the implementation of them. These security measures should be appropriate to the risks involved with regards to the specific Personal Data Processing operations.

3.2. The measures as described in **APPENDIX C** of the DPTs may be modified to adapt to future technical and organizational developments. The Processor will carry out these modifications, if they meet at a minimum the previous level of security. The Processor is only required to inform the Controller of substantial changes to the implemented measures, subject to the existence of other regulations to the contrary.

3.3. The Processor shall support the Controller in its compliance with all legal obligations as far as the technical and organizational measures are concerned. The Processor shall, upon request, cooperate in creating and maintaining the Controller's record of Processing activities. The Processor shall cooperate with the creation of a Data Protection Impact Assessment as defined under applicable Data Protection Laws and if necessary, with prior

consultations with supervisory authorities. Upon request, the Processor shall make the required information and documents available to the Controller.

## 4. Obligations of the Processor

4.1. The Processor confirms that it is aware of the relevant Data Protection Laws to which it is subject. The Processor's internal operating procedures shall comply with the specific requirements of effective Data protection management as required under applicable Data Protection Laws.

4.2. The Processor guarantees that it has implemented appropriate technical and organizational measures, in a manner that ensures that its Data Processing is in compliance with the Data Protection Laws and the rights of data subjects.

4.3. The Processor warrants and undertakes that all employees involved in the Personal Data Processing procedures are familiar with the relevant Data Protection Laws. The Processor assures that those employees are bound to maintain confidentiality or are subject to an adequate legal obligation of secrecy. The Processor shall monitor compliance with the applicable Data Protection Laws.

4.4. The Processor may only access the Controller's Personal Data if it is necessary for the purposes of carrying out the Data Processing as required for the purpose of providing the Service.

4.5. Insofar as it is legally required, the Processor shall appoint a data protection officer who is to ensure that its organization Processes the Personal Data of its staff, customers, providers or any other individuals in compliance with the applicable Data Protection Laws.

4.6. The Processor shall support the Controller with appropriate technical and organizational measures in the fulfillment of its obligations to Data Subjects in the exercise of their rights under the applicable Data Protection Laws. Such obligations include but are not limited to: the right to information, the right to rectification and to erasure, the right to restriction of Processing, to Data portability and to object to Data Processing.

4.7. In the event of a Data breach, the Processor shall support the Controller in the fulfillment of any information obligations to which the Controller is subject.

4.8. Information regarding the Data Processing carried out by Processor may only be provided to data subjects or to other third parties with the prior approval of the Controller. If a data

subject exercises his or her data subject's rights in respect to the Processor, the Processor shall forward this request to the Controller without undue delay.

4.9. The Processor will nominate a contact person who will support the Controller in the fulfillment of the applicable legal obligations in connection with the Data Processing and will share this person's contact details with the Controller without undue delay.

## 5. Sub-Processing

5.1. The Sub-Processing relationship shall be established when the Processor appoints another Processor(s) in part or in whole, for the provision of Services agreed upon in this Agreement. Ancillary services that are provided to and on behalf of the Processor by third-party service providers, and which may support the Processor in the exercise of its duties, shall not be regarded as sub-processing within the meaning of this DPA. Such services may include, for example, provision of telecommunication services or facility management.

5.2. The Processor is obliged to guarantee the protection and the security of the Controller's Data in respect to third-party service providers, and to ensure appropriate and legally compliant contractual agreements and supervisory measures are in place.

5.3. The Processor may appoint or change Sub-Processors only after informing the Controller of such intended appointment or change. Upon receipt of such information, the Controller may notify the Processor of any objections (on reasonable grounds) to the proposed appointment or changes.

5.4. A Sub-Processor may only have access to the Personal Data which is the subject to this DPA once the Processor has ensured, by means of a written contract, that the provisions of this DPA are also binding on the Sub-Processor, and in particular adequate guarantees are provided as to the implementation of appropriate technical and organizational measures to ensure that the Processing is compliant with Data Protection Laws.

5.5. The Sub-Processors at the time of signature are deemed to have been approved by the Controller, provided that the Processor has provided the Controller with a copy of the list of Sub-Processors and the Controller has not objected to the use of them.

## 6. Data Transfers

6.1. The Processor will process Personal Data provided to them by the Controller under this DPA exclusively in the territory of the respective country in which it received the Personal Data.

6.2. Processing of Personal Data outside of the respective country requires the explicit prior approval of the Controller and the execution of the required transfer mechanisms and other

legal requirements for such transfer such as, without limitation, the use of Standard Contractual Clauses.

6.3. Processor agrees that its Sub-Processors will be bound by the data transfer restrictions as provided under this section.

## 7. Controller's Audit Rights

7.1. The Processor agrees that the Controller, upon providing prior notice, or a person authorized by the Controller, shall be entitled to monitor Processor's compliance with the Data Protection Laws and other contractual provisions in this DPA using reasonable and appropriate means including requests for relevant documents and information gathering, the inspection of Data Processing systems and processes or by accessing the business premises of the Processor during the designated office hours.

7.2. Proof of proper Data Processing can also be provided by appropriate and valid certificates for IT security (e.g. IT-Grundschutz, ISO 27001, SOC 2 type II), provided that the specific subject and scope of the certification applies to the Data Processing activity being carried out in the specific case.

7.3. The presentation of a relevant certificate does not replace the Processor's duty to document the technical and organizational measures as mentioned in §3 of this DPA.

7.4. Processor agrees that in compliance with its obligations under this DPA, it shall bear the cost of one yearly audit or inspection as mandated by the Controller. Audit or inspections costs arising from further Controller requests shall be borne by the Controller, except in cases of a Data related incident arising from the Processing activities of the Processor. In such cases, the Processor shall bear the costs of such audit.

## 8. Data Protection Violations by the Processor

8.1. The Processor shall notify the Controller without undue delay about any disruption in its operations which results in a risk to the Personal Data provided by the Controller, as well as of any suspicion of Data protection infringements concerning Personal Data provided by the Controller. The same applies if the Processor discovers that his security measures do not satisfy legal requirements.

8.2. The Processor is aware that the Controller is obligated to document all breaches of the security of Personal Data and, where necessary, to inform the supervisory authority and/or

the Data Subjects. The Processor will report such breaches to the Controller without undue delay and will provide, at a minimum, the following information:

(a) a description of the nature of the breach, the categories and approximate number of Data Subjects and Personal Data records concerned,
(b) name and contact details of a contact person for further information,
(c) a description of the likely consequences of the breach, and
(d) a description of the measures taken for the remedy or mitigation of the breach.

# APPENDIX C
# TECHNICAL AND ORGANISATIONAL MEASURES
# ("TOMs")

## 1. Security Policy and Counsellor, Supervision, Inspection and Maintenance

The Supplier puts in place – inter alia – the following measures:

(i) A written policy in relation to data security, giving a precise description of the security strategies and protection features for Data security. The security policy considers the real risks the Data is exposed to. It includes a description of how to manage security incidents, a description of the awareness raising process for the policy within the organization and a description of the various responsibilities and organizational rules. It also specifies the measures foreseen in keeping the security system up to date after installation.

(ii) An approved security policy by the relevant persons in charge and which has been adequately disseminated within the organization. A reassessment of the technical and organizational measures is performed on a regular basis in order to assure that the initial goals and the measures taken remain up to date so that improvements can be made if necessary. In case of reorganization or modification of infrastructure, security controls are updated. The security policy will be adapted where necessary as a result of modifications or reassessment.

(iii) Information classification procedures. Whenever necessary, an inventory can be drawn up and all Data being Processed can be localized, irrespective of the type of data carrier.

## 2. Organization and Human Aspects of Security

The Supplier puts in place – inter alia – the following measures:

(i) Sufficient and adequate organizational, technical and financial resources to organize security.

(ii) A security counsellor appointed by the Supplier, who is in charge of the implementation of the security policy. The security counsellor possesses the necessary competences, is adequately trained and will not be able to discharge any function or take up any responsibility that is incompatible or conflicting with that of a security counsellor.

(iii) Guidelines on Data protection disseminated within the organization in order to ensure that all employees accessing Data are sufficiently informed about their duties and responsibilities during any operations.

(iv) Necessary measures for background verifications and checks before recruiting personnel.

**3. Access Control to Premises and Facilities (Physical)**

The Supplier puts in place – inter alia – the following measures to avoid the access of unauthorized persons or authorities to the carriers of Data and computer systems by which the Data is accessed or used:

(i) By formal/technical access procedures, the access to the premises and facilities involving data centers is regulated.

(ii) All persons or authorities have to identify themselves in front of the security staff to gain access to a premise and facility or to certain areas of the premise and facility. This requires an identity card issued by the Supplier. There are documented processes for the issuance of identity cards by the Supplier. The ownership and the return of this identity card is followed and examined according to the defined process.

(iii) Records of visitors are made. Visitors are provided with temporary identity cards and have to be accompanied by an employee of the Supplier to gain access to areas behind the reception area of a premise and facility.

(iv) Only authorized employees and contracting parties who are constantly employed in the premise and facility have the right to get electronic access cards for these institutions.

(v) The standardized security measures which also exist and are carried out in each premise and facility are composed of known technologies and follow generally recognized "best practices" of the sector. Electronic access control systems by card access, alarm systems, cameras for the interior and the exterior and security staff are part of this. The equipment is inspected on a regular basis.

**4. Access Control to Systems and Data (Logical)**

The Supplier puts in place – inter alia – the following measures to avoid the use by unauthorized persons or authorities of equipment by which Data could be accessed:

(i) Secured access connections and technologies for the authentication control are implemented to regulate the access to the systems and internal support-tools.

(ii) Technics for encryption are used to secure user authentications.

(iii) A formal process is followed to permit the access to the resources or to deny it. Unique login names, strong passwords and periodic examinations of the access lists are existent to guarantee the appropriate use of user accounts. For critical systems, passwords for one use and/or accounts for only one use are applied.

(iv) All groups which have access to the services are controlled by a regular examination. All named measures are described in a formalized concept of authorization.

(v) The Supplier ensures (i) Data in the systems can only be accessed by authorized individuals according to their access privileges and (ii) that the unauthorized reading, copying, printing, change or deletion of Data is excluded during use, Processing or after the storing of Data.

(vi) The granting of access rights is based on the job responsibilities of the user and on a need-to-know basis and has to be authorized and granted by the corresponding supervisor of the person who makes a request for it.

(vii) The access to production systems is only granted to users who are periodically trained and authorized for performing administrative action. The access to production systems is also immediately withdrawn in case of a termination of the contract of employment or in case of an assignment of a different task.

**5. Network Security**

The Supplier puts in place – inter alia – the following measures to guarantee that Data is not read, copied, altered or removed during the process of electronic transmission, during the transport or storage of data-on-data carriers:

(i) The systems/resources are protected against the risk of intrusion with the help of suitable software and hardware which effectiveness is checked periodically and updated accordingly.

(ii) The routers/firewalls are appropriately configurated to secure internal network from unauthorized external connections and to secure that computer connections and data flow do not breach the logical access adjustment control of the systems.

(iii) Amendments on the hardware-based network components or on their configurations need the acceptance of the designated person in charge and are subject to a change management process.

(iv) The organization has a firewall configuration regulation which defines acceptable ports. Only used ports and services are open. The access for the amendment of the firewall configuration is restricted to an internal team of security experts. Such team regularly examines critical firewall regulations.

**6. Input control (Data Quality)**

The Supplier puts in place – inter alia – the following measures to guarantee that it can be examined and determined subsequently if and by whom the Data has been entered into, removed from, or altered in the Data Processing systems:

(i) Effective input control is applied to ensure that Data cannot be read, copied, modified or re-modified without authorization in the course of Processing or use and after storage. All access requests are logged, and their compliance is monitored because detection data are also Data, any operation performed on these Data is submitted to adequate security measures.

## 7. Job control

The Supplier shall ensure that the functions and obligations of every individual with access to the Data are clearly defined, updated and documented. Measures are adopted to make staff familiar and periodically trained with respect to the specific rules applicable to their functions and the consequences of any breach of these rules.

## 8. Availability control and Business Continuity Management

The Supplier puts in place – inter alia – the following measures to ensure that Data is protected against damage by accident or loss:

(i) Data is protected from accidental destruction or loss through effective retrieval systems, disaster recovery and business continuity planning. The procedures laid down for making backup copies and for recovering Data ensure that can be reconstructed to the state in which they were at the time they were last backed up.

(ii) At least annually executed perform drills for Business Continuity and Disaster Recovery (BC-DR) purposes which is then stored or shared as evidence.

(iii) The organization must take steps to perform a Business Impact Assessment (BIA/) to identify and mitigate potential threats and attacks.

(iv) Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for all their applications and resources, and a formal verification and validation process of the defined measures should be in place. Necessary evidence for audit purpose to be shared with the Customer.

## 9. IT and Security operation

The Supplier puts in place – inter alia – the following measures to ensure that Data is protected against external threats:

(i) A formalized process to be defined regarding the acquisition and development of systems which incorporates the assessment on the adequacy of security measures.

(ii) Secure system development using (i) frameworks to build secure software and address security issues, and (ii) separating development, test and production environment.

(iii) Reducing the surface of vulnerability by hardening of systems according to their exposure and sensitivity.

(iv) Implementing Patch & Vulnerability Management to timely detect and resolve any known vulnerabilities which could result in exploits.

(v) Assess the exploitability of the IT environment by performing penetration testing and cyber-attack testing addressing the attack surface and vulnerability of the systems to external cyber-attack, including readiness testing assessing levels of preparedness and capability.

(vi) Implementation of Endpoint & Network Protection to evade malicious attacks and intrusions.

## 10. Security Incident Management

The Supplier puts in place – inter alia – the following measures to respond and recover from security incident:

(i) The security policy contains a precise description of the steps to be taken when a security incident relating to Data is detected, as well as of the persons in charge of dealing with the incident, in order to return to the normal situation as quickly as possible.

(ii) The procedure for reporting and managing security incidents includes a record of each incident, the time at which it occurred, the person reporting it, to whom it was reported and the effects thereof.

(iii) The circumstances of any incident are to be analyzed in order to elaborate preventive measures or make adaptations so as to avoid a repetition of this type of incident.

## 11. Security Monitoring and Governance

The Supplier puts in place – inter alia – the following measures to detect malicious events which compromise the security of the Data:

(i) Implementation of security event monitoring to timely detect anomalies in the behavior of users and systems. These events logs are maintained for at least a period of 6 months for audit reasons.

(ii) Establishment of a security function (SOC – Security Operation Center) to govern the detection of malicious events to initiate response and recovery actions.

(iii) Enabling of logging of network activities, transaction data, configuration changes and security events according to the defined policies and guidelines. Logs may be collected locally.

(iv) Implementation of Data Leakage Prevention Policy and methods to prevent and / or detect breach or Data leaks.

## 12. Segregation control

The Supplier puts in place – inter alia – the following measures to separate the processing of collected data for different purposes:

(i) Each Data Processing is made on server systems which are separated by a system of logical and physical access controls in the network. The Data Processing is only made in accordance with the Data Processing Agreement.

## 13. Documentation

The Supplier puts in place – inter alia – the following measures to have the following Information Security Management System (ISMS) document measures to be in place:

(i) Centralized documentation relating to security, which is complete and formalized, proportional to security needs, up to date at any time and accompanied by a directory at the disposal of properly authorized persons whenever necessary.

Such documentation should at least contain the following elements: the identity of the security counsellor, the security policy, the implementation of security measures, an inventory of the Data being Processed, their localization and the operations performed on them, a nominative list of the bodies or appointees having access to the Data; the system and network configuration, technical documentation about the security controls that were introduced, a schedule of planned operations, the detection policy, security control test plans, incident reports, audit reports, if any.

## 14. Encryption

The Supplier puts in place – inter alia – the following measures for encryption of Data at rest (e.g., hard disk, flash drives) and Data in transit (e.g., Bluetooth devices, Internet, e-commerce):

(i) Data transmission / transfer (data-in-transit) to and from the organizations network and / or solution it encrypted used industry best practice encryption technologies, such as SSL/TLS.

(ii) Data encryption of Data at rest e.g., BitLocker, Sophos on both user endpoint and system processing and/or storing Data.

(iii) Industry best practices of encryption algorithms, key length and key management should be implemented which are considered effective in protection (Confidentiality, Integrity and Availability) of Data-at-rest and in-transit.

(iv) Pseudonymization is a means of protecting the Data. Pseudonymization can be established by methods like encryption, tokenization or hashing.

## 15. Data Minimization / Retention

The Supplier puts in place – inter alia – the following measures so that only the necessary or minimal Data is shared:

(i) The processed/shared Data is either destroyed or stored with appropriate security measures for a defined period of time.

(ii) The Data received from the TrustMotion will be destroyed/deleted/handed over to TrustMotion or a party designated by TrustMotion on termination of the PO unless agreed otherwise for legitimate reason. During the course of the Processing activities, the Supplier needs to destroy all the copies of the Processed and validated Data once shared with the TrustMotion using a standard operating procedure or statement of work, unless agreed otherwise. If both Supplier and TrustMotion agree on a certain retention period of Data, then it should be clearly documented in the PO and justified by a legal reasoning. The Supplier will upon request of TrustMotion provide evidence of maintaining necessary Data according to TrustMotion's data retention policy; this should at least include a policy for deletion or erasure of records after termination or expiration of the PO.

(iii) The Supplier may store the necessary Data for the duration necessary for the performance of the PO and will ensure appropriate data deletion techniques (NIST standards) are used to delete the TrustMotion Data.

## 16. Data Portability & Right to Erasure

The Supplier puts in place – inter alia – the following measures:

(i) The Supplier ensures the employees of the TrustMotion have the possibility of accessing the Processed Data at any given point in time. If need be, an employee can share his/her information with another third party for further processing. e.g., tax slips or pay slip.

(ii) On the request of the TrustMotion / TrustMotion's employee, the Supplier will adhere to deletion of certain Data values/ fields which may no longer be deemed necessary to continue with the assigned work, where is illegally collected, if the consent is withdrawn, when there is an objection raised for sharing Data and also in compliance with law.

## 17. Certifications

Supplier holds one or more of the certifications specified below on their ISMS in relation to the implementation of technical and organizational measures:

- SOC 2 type II;
- ISO 27001, together with a statement of applicability including data privacy in scope.

If Supplier does not hold one or more of the certifications specified below Supplier will inform TrustMotion without undue delay and will be required to complete the Security Assessment Questionnaire initiated by TrustMotion.

Supplier will for the term of providing the Service to TrustMotion and at a minimum for an additional six (6) months afterwards:

(i) maintain such certification;

(ii) provide yearly or upon request and in a format acceptable to TrustMotion the updated certificates and/or reports evidencing maintenance of such certification;

(iii) provide all information on maintenance and implementation of such certification as reasonably requested by TrustMotion;

(iv) immediately identify to TrustMotion any deficiencies discovered during self-assessments of such certifications and/or reported by independent auditors in relation to such certifications;

(v) remedy identified deficiencies within a timeframe acceptable to TrustMotion;

(vi) implement additional procedures requested by TrustMotion within a period specified by TrustMotion; and

(vii) ensure for onward transfers to other parties, the above mentioned technical and organizational measures are implemented by such other parties.