HOW TO EXECUTE THIS DATA PROCESSING AGREEMENT (DPA):

To complete this DPA, Customer must:

- Complete the information in the signature box and sign the DPA;
- Send the completed and signed DPA to Camunda by email at privacy@camunda.com, if applicable, please indicate also the Product Tier you are subscribed to and the Use Case;
- Camunda will provide you with a countersigned copy.

Data Processing Agreement

This Data Processing Agreement ("DPA") is entered into between Camunda Services GmbH, Camunda Ltd or Camunda Inc, as applicable and the Customer and forms an integral part of the Agreement. For the purpose of this DPA, the entity acting as Camunda hereunder is the entity acting as Camunda under the Agreement, as designated in accordance with the Section "Contracting Party, Governing Law and Venue" of the Agreement.

The DPA is effective upon acceptance or signing of the Agreement or upon signing of this DPA by both Parties. It supplements, and does not supersede or cancel, the Agreement, which remains in full force and effect according to its terms. In the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will apply.

This DPA consists of two parts: the main body of the DPA, and Appendix 1, 2 and 3.

Terms not otherwise defined herein, including but not limited to the terms "controller" "data subject", "Personal Data", "processing", "personal data breach" and "supervisory authority" shall have the meaning as set forth in the Agreement or the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("General Data Protection Regulation" or "GDPR").

1. Definitions

Applicable Law means all laws, rules and regulations applicable to each Party in its use of or provisioning of the Software or any Services, including but not limited to those applicable to the processing of Personal Data. This means, in particular, the GDPR and all national laws validly amending the applicable rules for the processing of Personal Data, or in relation to the United Kingdom or Switzerland, the respective laws applicable in these countries.

Personal Service Data means any Personal Data that is part of Service Data and which Camunda or Camunda's Affiliates, employees or agents may process on behalf of Customer in providing the Software or any Services in accordance with this Agreement. This may include the Personal Data of any of Customer's employees or end-customers which is submitted to and processed within the Software or the Services by Customer. For the avoidance of doubt, Personal Service Data does not include (i) the sign up information of Customer's employees, which may include Personal Data (such as email, name, password, job title, company, localization data); (ii)

Telemetry Data, and (iii) Personal Data about visitors to the Camunda Website (as further set for in the Privacy Policy).

SCC means the EU Standard Contractual Clauses pursuant to European Commission Decision of 4 June 2021.

Service Data means any information processed or transmitted by or on behalf of Customer in the Software or in connection with performance of the Services during the Subscription. All Service Data processed under the terms of this Agreement will remain the property of Customer.

Sub-processor means a third party subcontractor engaged by Camunda that performs Camunda's obligations under this DPA on behalf of Camunda. Customer hereby consents to Camunda's use of Sub-processors. A list of current Sub-processors can be found in Appendix 3.

2. Scope of the DPA and roles of the Parties

2.1 This DPA applies to any and all activities associated with the Agreement, in whose scope Customer's Personal Service Data is submitted to and processed within the Software or any Services by Camunda, Camunda's employees or agents as per the instructions of Customer as a controller and the GDPR being applicable to such processing. Unless provided for otherwise in the Agreement, the processing will be limited to the storage or processing of certain limited Personal Service Data on a server and incidental access to such data when providing the Software or the Services pursuant to the Agreement. This DPA details the Parties' obligations in relation to the protection of Personal Service Data. For the avoidance of doubt, Camunda does not act as a Data Processor or Service Provider when it collects any data which is not Personal Service Data.

2.2 Customer shall be the "controller" in accordance with Art. 4 no. 7 GDPR and Camunda shall be "processor" in accordance with Art. 4 no. 8 GDPR.

3. Nature and Purpose, Duration and Specification of Processing Operations

3.1 The nature and purpose of the data processing under this DPA is the provision of the Services and providing the Software and/or the Services to Customer and the performance of Camunda's obligations under the Agreement and this DPA (or as otherwise agreed by the Parties).

3.2. The categories of Personal Data and data subjects which may be subject to the processing within the scope of this DPA are listed in Appendix 1. Appendix 1 can be amended by written notice to Camunda, provided that Camunda confirms the receipt of such notice in writing.

3.3 The duration of the processing shall correspond to the Agreement Term.

4. Responsibilities

4.1 Within the scope of this DPA, Customer shall be solely responsible for compliance with Applicable Laws including but not limited to the lawfulness of disclosing Personal Data to Camunda and the lawfulness of having Personal Data processed on behalf of Customer.

4.2 Customer's individual instructions on data processing shall, initially, be as detailed in the Agreement. Customer shall subsequently be entitled to modify, amend or replace such individual instructions in writing or in a machine-readable format (e.g. via email) by issuing such instructions to the point of contact designated by Camunda. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the Agreement and will only be effective if documented in a written addendum which is signed by both Parties. Customer shall, without undue delay, confirm in writing or by email any oral instruction given.

5. Camunda´s obligations

5.1 Except where expressly permitted by Art. 28 para. 3 lit. a) GDPR, Camunda shall process Personal Service Data only within the scope of the Agreement and the documented instructions issued by Customer, unless required to do so by Applicable Law to which Camunda is subject to. In such case, Camunda shall inform Customer of that legal requirement before processing, unless Applicable Law prohibits such information from being shared on important grounds of public interest.

5.2 If Camunda believes that an instruction would be in breach of Applicable Law, Camunda will notify Customer of such belief without undue delay. Camunda is entitled to not perform the relevant instruction until Customer confirms that it complies with Applicable Law or modifies such instruction.

5.3 Camunda shall, within Camunda's scope of responsibility, organize Camunda's internal organization so that it satisfies the specific requirements of the Applicable Law. Camunda shall, in particular, taking into account the nature of the Personal Service Data and the risks involved in the processing of any such Personal Service Data, maintain reasonable and appropriate technical and organizational measures designed to ensure the adequate protection of Customer's Personal Service Data, which will fulfil the requirements of the GDPR and specifically its obligations under Art. 32 GDPR. The measures implemented at the time of establishing this DPA are set forth in Annex 2 to this DPA. Customer is familiar with these technical and organizational measures, and is responsible for determining that such measures ensure a level of security appropriate to the risk associated with Personal Service Data. Camunda reserves the right to modify the measures and safeguards implemented, provided that the level of security shall not be less protective than initially agreed.

5.4 Camunda shall implement a data protection management procedure according to Art. 32 para 1 lit. d) GDPR, for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to reasonably ensure the security of the processing. Camunda will further, by way of regular self-audits, reasonably ensure that the processing of Personal Service Data conforms with the provisions according to Customer's instructions or as agreed with Customer.

5.5 Taking into account the nature of the processing, Camunda shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising data subjects' requests, as laid down in chapter III of the GDPR. Camunda shall assist Customer in ensuring compliance with the obligations pursuant to Art. 32 to 36 GDPR taking into account the nature of the processing and the information available to Camunda.

5.6 Camunda ensures that (i) any person entitled to process Personal Service Data on behalf of Customer as the controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy and all such secrecy obligations shall survive the termination or expiration of such data processing, and (ii) all employees authorized to process Personal Service Data and other such persons as may be involved in data processing within Camunda's scope of responsibility is prohibited from processing Personal Service Data outside the scope of the instructions.

5.7 Camunda shall notify Customer, without undue delay, if Camunda becomes aware of a personal data breach within Camunda's scope of responsibility. In the event of any breach, Camunda shall implement the measures necessary to secure Personal Service Data and mitigate potential negative consequences for the affected data subjects. Camunda shall coordinate such efforts with Customer without undue delay. Camunda shall notify Customer of the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

5.8 Camunda shall correct or erase Personal Service Data if so, instructed by Customer and where covered by the scope of the instructions if this is permissible. Where an erasure consistent with data protection requirements or a corresponding restriction of processing is impossible, Camunda will, based on Customer's instructions, and unless otherwise agreed in the Agreement, destroy all carrier media and other material or return the

same to Customer in compliance with data protection requirements. In specific cases designated by Customer, such Personal Service Data will be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.

5.9 Camunda shall, upon termination of the data processing and upon Customer's instruction, return all Personal Service Data, carrier media and other materials to Customer or delete the same. In case of testing and discarded material, no instruction shall be required.

5.10 Customer shall bear any extra cost caused by deviating requirements in returning or deleting data.

5.11 Where a data subject asserts any claims against Customer in accordance with Art. 82 GDPR, Camunda will support Customer in defending against such claims to the extent they arise in connection with the processing of Personal Service Data by Camunda within the scope of this DPA only, and to the extent this is possible. Camunda reserves the right to a reasonable compensation for such support.

6. Customer's obligations

6.1 Customer shall notify Camunda in sufficient detail and without undue delay of any defect or irregularity detected by Customer in Camunda's provision of the Software or the Services concerning data protection.

6.2 Section 5.11 of this DPA shall apply, mutatis mutandis, to claims asserted by data subjects against Camunda in accordance with Art. 82 GDPR.

6.3 Customer shall notify Camunda of the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

6.4 Customer shall notify Camunda in writing of the names of the persons who are entitled to issue instructions to Camunda. Unless otherwise specified at a later date, the point of contact designated in the Agreement or during the onboarding process shall be entitled to issue instructions. If no point of contact has been designated, the managing directors and designated Data Protection Officer of the Customer shall be entitled to issue instructions to Camunda.

7. Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure (deletion), restriction (blocking), transmission or access against Camunda, and where Camunda is able to correlate the data subject to Customer based on the information provided by the data subject, Camunda shall refer such data subject to Customer. Camunda shall forward the data subject's claim to Customer without undue delay. Camunda shall support Customer, to a reasonable extent and at Customer's expense, and based upon Customer's instructions. Camunda shall not be liable in cases where Customer fails to respond to the data subject's request or fails to do so correctly and/or in a timely manner.

8. Options for documentation and audits

8.1 Camunda shall document and make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA. Customer shall have the right to assess Camunda's compliance with the obligations agreed upon in this DPA by appropriate measures.

8.2 Where, in individual cases, audits and inspections by Customer or an auditor appointed by Customer are required at Camunda's working premises and allowable under applicable law to determine Camunda's compliance with this DPA, to the extent that such information is within Camunda's control and Camunda is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party, such audits and inspections will be conducted during regular business hours, and without interfering

with Camunda's operations and upon prior notice of at least 30 days. Camunda shall be entitled to reject auditors that (i) are competitors of Camunda, (ii) are not sufficiently qualified to conduct such an audit, or (iii) are not independent. At least one employee of Camunda may accompany the auditors at any time. Camunda may memorialize the results of the audit in writing which shall be confirmed by Customer.

8.3 Customer hereby consents to the appointment of a competent, independent external auditor by Camunda if Camunda so chooses, provided that Camunda provides a copy of the audit report to Customer.

8.4 Camunda may also determine that any audits and inspections require the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organizational measures and safeguards implemented. In this case, execution of such a confidentiality undertaking will be a prerequisite for any audit or inspection.

8.5 Camunda reserves the right to charge a reasonable fee for Camunda's support in conducting inspections based on Camunda's reasonable costs. Camunda's time and effort for such inspections shall be limited to one day per calendar year, unless agreed upon otherwise.

8.6 Where a data protection supervisory authority or another supervisory authority with statutory competence for Customer conducts an inspection, Section 7.2 of this DPA above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations the breach of which is sanctionable under the applicable criminal code.

8.7 Camunda shall audit its Sub-processors (as defined below) on a regular basis and will upon Customer's request confirm their compliance with Applicable Law and the obligations set upon the Sub-processors according to the data processing agreement concluded with them. If Customer provides reasoned, adequately detailed justifications for further audits and Camunda (acting reasonably) considers such justifications to be valid, Customer may instruct Camunda to conduct further audits, which Camunda will conduct to the extent permitted.

9. Sub-processor

9.2 Camunda shall conclude with such Sub-processors the contractual instruments necessary to ensure an appropriate level of data protection and information security in accordance with Art. 28 para. 4 GDPR. Where Camunda commissions Sub-processors, Camunda is responsible for ensuring that every Sub-processor is subject to obligations regarding the processing of Personal Data that are no less protective than those to which Camunda is subject under this DPA.

9.3 If Camunda intends to instruct additional Sub-processors in the future, Camunda will notify Customer thereof in writing (email to the email address(es) provided in accordance with Section 5.3 of this DPA shall be sufficient) and will give Customer the opportunity to object to the engagement of the new Sub-processor within 10 business days after being notified. The objection must be based on reasonable grounds (e.g. if Customer proves that Sub-processor does not act in compliance with this DPA and the Applicable Law and, therefore, significant risks for the protection of its Personal Data exist at the Sub-processor). If Camunda and Customer are unable to resolve such an objection, either Party may terminate the Agreement by providing written notice to the other Party. Customer shall not be entitled to any refund of Fees unless the objection is based on justified reasons of non-compliance with Applicable Law, in which case it is entitled to receive a pro-rata refund of any Fees paid.

9.4 If Customer does not object to the engagement of a third party in accordance with this Section within 10 business days after notice is given by Camunda, the Sub-processor shall be deemed a Sub-processor to which Customer consented for the purposes of this DPA.

9.5 Where a Sub-processor refuses to be bound by the same data protection obligations as the ones under this DPA, Customer may consent to such other terms whereby such consent shall not be unreasonably withheld if, upon request of the Customer, Camunda can demonstrate Sub-processor's compliance with Applicable Law.

9.6 Camunda is entitled to engage a Sub-processor located outside the EEA, the United Kingdom and Switzerland. If so, Camunda shall implement appropriate contractual and technical safeguards to ensure compliance with the requirements under Art. 44 et seq. GDPR on international data transfers. For compliance with international data transfers, Customer authorizes Camunda on its behalf to enter into the SCC. Camunda may amend or replace the SCC by other appropriate safeguards as required under Applicable Law for transfers of Personal Data to third countries once made available by the European Commission or once further guidance about the use of the SCC and accompanying supplementary measures becomes available. Camunda will conduct a transfer impact assessment prior to the engagement of any new Sub-processor located outside the EEA, the United Kingdom and Switzerland.

9.7 For the Services provided by Camunda and its Sub-processors, Customer may be able to select between several data centers worldwide (e.g. within the EEA, the United Kingdom, the United States of America or other countries). If an outside the EEA location is selected, Customer is solely liable for compliance with Applicable Law in relation to the international transfer of personal data.

10. SCC

If Customer is a Controller located outside the EEA, enters into this Agreement including a DPA with Camunda Services GmbH, and chooses a data location within the EEA, Camunda and Customer hereby agree that Module 4) of the SCC (Controller to Processor) apply and Camunda shall be acting a Data Exporter and Customer acting as Data Importer within the meaning of the SCC.

11. Safeguards and Support for international data transfers

Camunda undertakes to provide reasonable support to Customer to ensure compliance with the requirements imposed on the transfer of Personal Data to third countries with respect to data subjects located in the EEA, United Kingdom and Switzerland. Camunda will do so, in particular, by providing information to Customer which is reasonably necessary for Customer to complete a TIA. Customer warrants that it will have successfully completed an appropriate TIA prior to any processing under the DPA if required.

12. Liability and damages

The provisions on the Parties' liability contained in the Agreement shall apply to any liability relating to data processing, unless otherwise agreed in this DPA.

13. Modifications

The Parties may modify or supplement this DPA, with notice to the other Party, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Art 40, 42 and 43 of the GDPR. The informed Party shall notify the modifying Party if it does not agree to a modification, in which case the informed Party may terminate this DPA and the Agreement with two (2) weeks' prior written notice. Customer shall not be entitled to any refund of Fees unless the objection to the modifications are based on justified reasons of non-compliance with Applicable Law, in which case it is entitled to receive a pro-rata refund of any Fees paid.

14. Obligations to inform, mandatory written form, choice of law

14.1 Where the Personal Service Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by Third Parties while in Camunda's control, Camunda shall notify Customer of such action without undue delay. Camunda shall, without undue delay, notify all pertinent Parties in such action that any data affected thereby is in Customer's sole property and area of responsibility, that data is at Customer's sole disposition, and that Customer is the responsible body in the sense of the GDPR.

14.2 No modification of this DPA and/or any of its components – including, but not limited to, Camunda's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this DPA. The foregoing shall also apply to any waiver or modification of this mandatory written form.

14.3 In case of any conflict, the data protection regulations of this DPA shall take precedence over the provisions of the Agreement. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

14.4 This DPA is governed by the laws of the Federal Republic of Germany and the place of jurisdiction shall be Berlin unless and to the extent required otherwise by applicable data protection and privacy laws.

Camunda	**Customer**
Signature:	**Signature:**
Name:	**Name:**
Date:	**Date:**

Appendix 1 – Specifications of the Processing

1. Types of personal data

Personal Data being processed by Camunda on behalf of Customer could contain the types of Personal Data that Customers provide in process instances of their automated processes, including but not limited to personal data, that Customers store in order to bring about decisions in the respective process instances. Examples could include risk classification, references to personal data in third-party systems, identity data, contact details, professional data, meta data (i.e. data containing information on characteristics of other data) and purchase data.

2. Categories of data subjects

Personal Data being processed by Camunda on behalf of Customer could refer to any category of data subject that Customers provide in process instances of their automated processes, including but not limited to Customer's customers and potential customers, employees, suppliers and other Customer contacts.

3. Data Exporter

Customer is the Data Exporter.

4. Data Importer

Camunda is the Data Importer, an online service provider that offers process automation services through its SaaS Platform.

Appendix 2 - Technical and Organizational Measures

1. Pseudonymization (Art.32 para. 1 lit. a) GDPR; Art. 25 para. 1 GDPR) (Measures suited to ensure the Personal Service Data cannot be associated with a specific Data Subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures):

    - For support tickets no Personal Service Data is required by Camunda; Customer may pseudonymize his Personal Service Data before sending it to the support team.

2. Confidentiality, Integrity, Availability and Resilience (Art. 32 para. 1 lit. a) GDPR; Art. 25 para. 1 GDPR)
    a. Confidentiality (Art. 32 para. 1 lit. b) GDPR)

    - Physical Access Control (Measures to prevent unauthorised access to data processing equipment with which Personal Service Data may be processed and used):

        - No unauthorized access to Personal Service Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems.
        - An effective and documented procedure exists to assign, alter and withdraw access rights, incl. the return of the means of access.
        - Visitors in security zones are accompanied by authorised staff
        - Data related to support inquiries is currently stored at a data center in Frankfurt, Germany (https://www.leaseweb.com/de/node/3377) operated by Camunda.
        - Camunda Platform SaaS is hosted at an external cloud service provider (currently Google Cloud Platform), with whom Camunda has a data processing agreement in place.

    - Electronic Access Control (Measures to prevent unauthorized use of data processing systems):

        - Access is secured via a firewall, with strong encryption and by two-factor authentication mechanisms.
        - Secure passwords are used and default passwords of systems and applications are changed as a matter of principle. Their structure and handling is in accordance with a documented password guideline.
        - An effective and documented access control policy exists.
        - The access control policy is assessed at least once per year.
        - All staff are instructed to lock their workplaces when they leave them. Workplaces are configured with an automatic lock as standard.
        - The access control policy defines the issuance and withdrawal of access rights, as well as their approval for internal and external staff.

    - Internal Access Control (Measures ensuring that authorized persons only have access to the Personal Service Data covered by their access authorization, and that prevent unauthorized reading, alteration or erasure during processing, use and storage):

- Release of Personal Service Data only to authorized persons, including allocation of differentiated access rights and roles.
- Access rights are adjusted if the tasks carried out in the business processes change and/or are withdrawn if they are no longer needed.

b. Integrity (Art. 32 para. 1 lit. b) GDPR)

- Data Transfer Control (Measures that prevent unauthorized reading, alteration or erasure during processing, use and storage of Personal Service Data during electronic transfer, storage on data media or during transportation):

    - Use of adequate encryption technologies
    - No physical transport of the Personal Service Data (e.g. via data carriers)
    - Use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the Personal Service Data travels.

- Data Entry Control (Measures that are suited to verify whether any by whom Personal Service Data been entered into, altered in or removed from data processing systems):

    - Plausibility is guaranteed via the Login functions of the Camunda Platform SaaS.
    - Log systems and logging information are protected against unauthorised access, alteration and erasure, and are regularly evaluated.
    - The clocks of all critical systems are synchronised using a reliable, agreed time server.

- Order Control (Measures that are suited for ensuring that the commissioned processing of personal data complies with the guidelines of the contracting Party):

    - Camunda has data processing agreements with the sub-processors who process Personal Service Data on Camunda's behalf in place.
    - External service-providers are evaluated before being contracted.

- Separation rule (Measures that are suited for ensuring that data that has been collected for different purposes can be kept separate during processing):
    - Access to Personal Service Data is separated through application security for the appropriate Customers.
    - Personal Service Data that have been collected for different purposes are kept apart in such a way (physically or logically) that they are separated, processed, stored and erased in a manner appropriate to the purpose.
    - Development, testing and production environments are separated.

c. Availability and Resilience (Art. 32 para. 1 lit. b) GDPR) (Measures to prevent accidental or willful destruction or loss):

- Camunda uses redundant power supplies and independent power generators in data centres and monitors availability

- All Personal Service Data processed by Camunda Platform Saas is stored on servers from our Cloud Service Provider (currently Google Cloud Platform)
    - High availability via redundant servers can be determined by Customer.

d. Incident-response-management (Measures suited to ensure that data breaches are recognised and reported quickly):

- A process has been established which ensures that security incidents are identified, assessed and dealt with appropriately.
- Escalation procedures and organisational interfaces are defined with all relevant parties, including the data protection officer.
- Staff who are responsible for the management of IT systems/applications are trained to recognise, classify and report security incidents.
- A process has been established which ensures information security for all critical business processes, even during a crisis or catastrophe.
- Processes and responsibilities have been defined in case of an emergency or crisis, and appropriate tests are held.

e. Regular testing, assessment and evaluation processes (Art. 32 Paragraph 1 Point d) GDPR) (Measures guaranteeing that the data protection requirements are implemented):

- Relevant staff are trained and familiarised with data protection and placed under an appropriate obligation.
- The IT operation procedures (e.g. user management, backup, network management) are comprehensibly documented, regularly checked and altered where necessary.
- Identification, provision and testing of updates are a part of standard operation.
- Regulations exist for information security and data protection.
- The regulations for information security and data protection, as well as the security measures, are tested regularly for compliance and effectiveness.

Appendix 3 - Camunda Sub-processors

Sub-processors processing Personal Data Personal Service Data uploaded by Customer or its Customers to the Camunda Platform SaaS Offerings.

Sub-processor	**Purpose**	**Location (by country)**
AWS	Continuity and disaster recovery plan	Germany
Google Cloud Platform LLC	Camunda Platform SaaS Infrastructure	Belgium USA
Cloudflare	Web Application Firewall for Camunda Platform SaaS	worldwide (depending on Customer's location)