DATA PROCESSING TERMS

BETWEEN:

Customer (hereinafter to be referred to as: the "**Data Controller**"),

AND

HCL Technologies Ltd. & its Affiliates, ("Affiliate" has the meaning given in the Master License Agreement (hereinafter to be referred to as: the "**Data Processor**").

HEREBY AGREE AS FOLLOWS:

1. Subject matter of these Data Processing Terms

1.1. These Data Processing Terms apply exclusively to the processing of personal data that is subject to EU Data Protection Law[i] in the scope of the agreement effective [date] between the parties for the [provision of services] ("Services") (hereinafter to be referred to as: the "Agreement") and is hereby incorporated by reference into the Agreement and governed by the Agreement.

1.2. The term EU Data Protection Law shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.3. Terms such as "Processing", "Personal Data", "Data Controller" and "Processor" shall have the meaning ascribed to them in the EU Data Protection Law.

1.4. Insofar as the Data Processor will be processing Personal Data subject to EU Data Protection Law on behalf of the Data Controller in the course of the performance of the Agreement with the Data Controller the terms of this Data Protection Agreement shall apply. An overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed as provided in Annex 2.

[i] Although an EU model is presumed here, other applicable laws may apply depending on where Services are provided.

2. The Data Controller and the Data Processor

2.1. The Data Processor will only process the Personal Data as set forth in Data Controller's written instructions except as required to comply with a legal obligation to which the Data Processor is subject. These instructions are as indicated in the Master License Agreement and the schedules thereto. If, the Data Processor must process Personal Data to comply with a legal obligation, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Data Controller. The Data Processor shall promptly inform the Data Controller if, in its opinion, an instruction infringes this Regulation.

2.2. The Parties have entered into Agreement in order to benefit from the expertise of the Processor in securing and processing the Personal Data for the purposes set out in Annex 2. The Data Processor shall be allowed to exercise its own direction in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of these Data Processing Terms.

2.3. Data Controller warrants that it has all necessary rights to provide the Personal Data to Data Processor for the Processing to be performed in relation to the Services. To the extent required by Applicable Data Protection Law, Data Controller is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the data subject, Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and Data Processor remains responsible for implementing any Data Controller instruction with respect to the further processing of that Personal Data. If Data Processor receives a data subject request, the Data Processor will promptly forward to the Data Controller.

3. Confidentiality

3.1. Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security[ii] [iii]

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, without prejudice to any other security standards agreed upon by the Parties, the Data Controller and Data Processor shall implement appropriate technical and organizational measures to ensure a level of security of the processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

(a) measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in Annex 2 of these Data Processing Terms;

(b) in assessing the appropriate level of security, account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;

(c) the encryption of personal data;

(d) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(e) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

(f) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data;

(g) measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Data Controller;

(h) the measures agreed upon by the Parties in Annex 3.

4.2. The Data Processor shall at all times have in place an appropriate written security policy with respect to the processing of Personal Data, outlining in any case the measures set forth in Article 4.1.

4.3. At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to this Article 4 to allow the Data Controller to audit and test such measures, per the terms of the Agreement.

[ii] GDPR Article 32(3): Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

[iii] Processor may demonstrate compliance by sharing certifications

5. Improvements to Security

5.1. The Parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Article 4. The Parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction.

5.2. Where an amendment to the Agreement is necessary in order to execute a Data Controller instruction to the Data Processor to improve security measures as may be required by changes in applicable data protection law from time to time, the Parties shall negotiate an amendment to the Agreement in good faith.

6. Data Transfers

6.1. The Data Processor shall hereby notify the Data Controller of, and the Data Controller hereby consents to transfers of Personal Data to countries outside of the European Economic Area without an adequate level of protections listed in Annex 4. The Data Controller hereby consents to the Data Processor executing the Standard Contractual Clauses (hereby incorporated as Exhibit 1) on behalf of the Data Controller with the third parties listed in Annex 5.

6.2. To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

7. Information Obligations and Incident Management

7.1. When the Data Processor becomes aware of a successful incident that impacts the Processing of the Personal Data that is the subject of the Services Agreement, it shall promptly notify the Data Controller about the incident, shall at all times cooperate with the Data Controller, and shall follow the Data Controller's instructions with regard to such incidents, in order to enable the Data Controller to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident.

7.2. The term "incident" used in Article 7.1 shall be understood to mean in any case:

(a) a complaint or a request with respect to the exercise of a data subject's

rights under EU Data Protection Law;

(b) an investigation into or seizure of the Personal Data by government officials, or a specific indication that such an investigation or seizure is imminent; subject to HCL permitted to disclose such investigation.

(c) any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;

(d) any breach of the security and/or confidentiality as set out in Articles 3 and 4 of these Data Processing Terms leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place;

(e) where, in the opinion of the Data Processor, implementing an instruction received from the Data Controller would violate applicable laws to which the Data Controller or the Data Processor are subject.

7.3. The Data Processor shall at all times have in place written procedures which enable it to promptly respond to the Data Controller about an incident. Where the incident is reasonably likely to require a data breach notification by the Data Controller under applicable EU Data Protection Law, the Data Processor shall implement its written procedures in such a way that it is in a position to notify the Data Controller no later than 72 hours of having confirmed of such an incident.

7.4. Any notifications made to the Data Controller pursuant to this Article 7 shall be addressed to the employee of the Data Controller whose contact details are provided in Annex 1 of these Data Processing Terms, and shall contain:

(a) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;

(c) a description of the likely consequences of the incident; and

(d) a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

8. Contracting with Sub-Processors

The Data Controller authorizes the Data Processor to engage sub-processors in Annex 5. If Data Controller wishes to object to a sub-processor, Data Controller shall contact the Data Controller's account manager at Data Processor within xx days of being notified of such

change in sub-processors.

8.1. The Data Processor shall ensure that the sub-processor is bound by the same data protection obligations of the Data Processor under these Data Processing Terms.

9. Returning or Destruction of Personal Data

9.1. Upon the Data Controller's written request, the Data Processor shall either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies.

9.2. The Data Processor shall delete the Personal Data upon written request and delete from third party's platform or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

10. Assistance to Data Controller

10.1. Taking into account the nature of the processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under the GDPR.

10.2. The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Section 4 (Security) and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data.

10.3. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Processor's obligations and allow for and contribute to audits, per the terms of the Agreement.

11. Duration and Termination

11.1. These Data Processing Terms shall come into effect as of the effective date of the applicable Agreement that governs the support and maintenance and/or professional services provided by Data Processor to Data Controller.

11.2. Termination or expiration of the Agreement and these Data Processing Terms shall not discharge the Data Processor from its confidentiality obligations pursuant to Article 3.

11.3. The Data Processor shall process Personal Data until the date of termination of the agreement, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on instruction of the Data Controller.

12. California Consumer Privacy Act of 2018

12.1. To the extent that Personal Data of California citizens is in scope, "California Consumer Privacy Act," or "CCPA" means Assembly Bill 375 of the California House of Representatives, an Act to add title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, related to privacy and approved by the California Governor on June 28, 2018.

12.2. Data Processor is a "Service Provider" as defined in CCPA Section 1798.140(v).

12.3. Data Controller discloses Personal Data to Data Processor solely for: (i) a valid business purpose; and (ii) Data Processor to perform the Services.

12.4. Data Processor is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Data outside of the Agreement between Smartsheet and Customer.

12.5. Data Processor understands the prohibitions outlined in Section 12.3.

13. Miscellaneous

13.1. In the event of any inconsistency between the provisions of these Data Processing Terms and the provisions of the Service Agreement, the provisions of these Data Processing Terms shall prevail.

13.2. Data Controller shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Data Processor to protect the Data Processor against additional risks associated. If Data Controller proposes any other variations to this Addendum which Data Controller reasonably considers to be necessary to address the requirements of any Data Protection Law, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

13.3. Data Processor shall promptly notify Data Controller if Data Processor receives a request from a Data Subject under any Data Protection Law in respect of the Data Subject's Personal Data; and ensure that the Contracted Processor does not request except on the documented instructions of Customer or the relevant Customer Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Data Processor shall to the extent permitted by Applicable Laws inform Data Controller of that legal requirement before Data Processor responds to the request.

13.4. These Data Processing Terms is governed by the laws of the applicable Member State where the Personal Data is processed. Any disputes arising from or in connection with this Data Processing Terms shall be brought exclusively before the competent court of

the applicable Member State where the Personal Data is processed.

13.5. The Parties agree to execute the below addenda as required.

Annex 1:

Contact information of the [data protection officer/compliance officer] of the Data Controller:

[Contact Information]

Contact information of the [data protection officer/compliance officer] of the Data Processor:

Chief Privacy Officer
HCL Technologies Ltd.
Axon Centre, Church Road
Egham, TW20 9QB
England, UK
privacy@hcl.com

Annex 2:

Personal data that will be processed in the scope of the Agreement and the purposes for which these data will be processed

The following set of data is collected by Support for the purpose of resolving customer report product problems.

Customer Contact Information: To communicate with our customers, HCL Software Support maintains a record of Company and Contact details that include, but is not limited to, Company Name, Company address, Contact Name, email address, and telephone number.

Case data including Customer Contact data: The communication data would be any information that the customer enters in the support portal itself during the lifetime of the case (i.e. description of their problem, communication back and forth with HCL support team to troubleshoot the issue).

Diagnostic data: To work on customer support queries, information between the customer and HCL Support needs to be shared. Customers may upload data, like log and configuration files, for Support to use in troubleshooting reported problems.

Annex 3:

Security measures

Case data including Customer Contact data: HCL Support keeps Customer Support related information in our Ticketing System, which is hosted by an accredited external company on servers in Canada. The communication is done via HTTPS and uses the protocol supported is TLS 1.2. This backend database is encrypted.

Diagnostic data: The data is sent via SFTP or HTTPS and is encrypted once on HCL servers. The database encryption algorithm is AES (Advanced Encryption Standard 360bit).

Annex 4:

Transfers to countries outside the European Economic Area without a suitable level of protection for which the Data Controller has granted its authorization:

Case data including Customer Contact data: We keep Customer Support related information in our Ticketing System, which is hosted by an accredited external company on servers in Canada.

Diagnostic data: HCL Support diagnostic data is housed in what we call the Customer Data Repository. This is hosted in Bangalore, India.
HCL Support standard data analysis environments are hosted in data centers across US, India, and Italy and are used by our worldwide support engineers.

Annex 5:

The following Subprocessors may be used to provide services in connection with the

Agreement:

Subprocessor	Country	Subprocessing Activities
Amazon AWS	USA	Cloud hosting services used to reproduce customer reported problems
ServiceNow	Canada	Cloud hosting service used for ticketed management system

EXHIBIT 1

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of data exporting organization:	
Address:	
Email:	

(**the data exporter**)

and

Name of data importing organization:	
Address:	
Email:	

(**the data importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law***'** means the legislation protecting the fundamental rights and

freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected

having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary

description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties agree that the liability of either party arising under or in connection with these Clauses shall be subject to the limitations and exclusions of liability set out in Clause [XX] of the [Principal Agreement]. For purposes of both the [Principal Agreement] and these Clauses, the limitation on liability in sub-Clause [xx] is a single, aggregate limitation applicable to liability arising under the [Principal Agreement] and/or under these Clauses, and references in Clause [XX] to the parties to the [Principal Agreement] shall include the data exporter and the data importer. Nothing in this Clause 6(4) limits the liability of either party to a data subject under these Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.
5. The data exporter consents to the appointment of sub-processors by the data importer. The data importer shall inform the data exporter of any changes in the sub-processors appointed by the data importer under these Clauses, including the addition or replacement of any such sub-processors.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

3. The parties agree that any audit carried out by the data exporter under Clause 5(f) or Clause 12(2) of the Clauses shall be carried out in accordance with the audit provisions in Clause [XX] of the [Principal Agreement]. Nothing in this clause 12(3) limits any audit carried out by a supervisory authority.

On behalf of data exporting organization	
Address	
Signature	
Name	
Position	

On behalf of data importing organization	
Address	
Signature	
Name	
Position	

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter, _____, is a provider of_____. The data exporter has appointed the data importer to provide [describe services]. To facilitate the provision of these services, the data exporter may provide to the data importer access to the personal data described below.

Data importer
The data importer, [Company Name], is a provider of [describe services]. The data importer will be the recipient of personal data which is exported by the data exporter to the data importer as described below.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

[Whose data will be transferred (e.g. riders, drivers, employees)?]

Categories of data
The personal data transferred concern the following categories of data (please specify):

[What types of data will be transferred (e.g. name, email, phone number, UUID, device ID)?]

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

[What special types of data will be transferred (e.g. race, gender, political affiliation, sexual orientation), if any?]

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

[How will the data be used or processed?]

FOR DATA IMPORTER – **[_____]**	FOR DATA EXPORTER – _____
Name:	Name: ....
Authorized Signature:	Authorized Signature: .....

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The following measures will be implemented: