DATA PROCESSING ADDENDUM

BETWEEN:

Customer (hereinafter to be referred to as the “Data Controller”),

AND

HCL Technologies Limited, a company duly organized and existing under the laws of India and having its registered offices at 806 Siddharth, 96 Nehru Place, New Delhi-110019 (hereinafter to be referred to as the “Data Processor”).

This Data Processing Addendum is entered into between the above entities and forms part of the agreement between the parties (“Agreement”) for the provision of standard software, software support and related services (collectively, “Services”).

HEREBY AGREE AS FOLLOWS:

1. Subject matter of this Data Processing Addendum

1.1 In the course of providing Services to Data Controller pursuant to the Agreement, Data Processor may process Personal Data that is subject to the European Union’s General Data Protection Regulation 2016/679 (“GDPR”) or other applicable Data Protection Laws. This Data Processing Addendum reflects the parties’ agreement with regard to the processing of such Personal Data.

1.2 “Data Protection Law” means any legislative or regulatory regime enacted by a recognized government, governmental or administrative entity with the purpose of protecting the privacy rights of individuals, including the GDPR and supplementing data protection law of the European Union Member States, Canada’s Personal Information Protection and Electronic Documents Act (“PIPEDA”), Brazil’s LGPD, and the California Consumer Privacy Act (“CCPA”) of 2018.

1.3 Terms such as “Processing,” “Personal Data,” “Data Controller,” “Data Subject,” and “Processor” shall have the meaning ascribed to them in the GDPR or the applicable Data Protection Law.

1.4 Insofar as the Data Processor will be processing Personal Data subject to the applicable 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 Addendum shall apply. An overview of the categories of Personal Data, the types of Data Subjects, duration and purposes for which the Personal Data are being processed is provided in Annex 2.

2. The Data Controller and the Data Processor

2.1. The Data Processor will only process the Personal Data for the purposes of performing the Services under the Agreement and for the purposes set out in Annex 2 or under any other documented instructions from Data Controller, or as required to comply with a legal obligation to which the Data Processor is subject. These instructions are as indicated in the Agreement and the schedules thereto. If the Data Processor must process Personal Data to comply with a legal obligation in a manner not instructed by Data Controller or otherwise permissible hereunder, 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 the Regulation.

2.2. The Parties have entered into this Data Processing Addendum 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 discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Addendum and applicable Data Protection Law.

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 it has obtained all necessary data subject consents to this Processing, 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 by Data Processor.

3. Confidentiality

3.1 Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as confidential and shall inform all its employees, agents and/or approved subprocessors 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

4.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, duration, context and purposes of processing as well as the varying likelihood and severity of the risk of harm to the rights and freedoms of individuals, 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. These measures shall include as appropriate:

4.1.1 measures to limit access to Personal Data to authorized personnel for the purposes set forth in Annex 2 of these Data Processing Addendums;

4.1.2 the encryption of personal data;

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

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

4.1.5 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;

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

4.1.7 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 the measures set forth in Clause 4.1 of this Data Processing Addendum. At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to Clause 4 of these Data Processing Addendums to allow the Data Controller to audit and test such measures, per Clause 4.3 of this Data Processing Addendum.

4.3 Audit rights

4.3.1 Subject to this section 4.3, Data Processor shall:

a) make available to the Data Controller on the provision of not less than thirty (30) days written notice, all relevant information necessary to demonstrate compliance with this Agreement, or

b) allow for and contribute to an audit, by the Data Controller, or an auditor mandated by the Data Controller, in relation to the processing of the Personal Data in accordance with the Agreement.

4.3.2 Any audit under 4.3.1(b) will be subject to the following conditions:

a) The scope, content and timing of the proposed audit such shall be agreed between the parties in advance;

b) any third party auditor appointed by Data Controller must be independent of the parties and not be a competitor of HCL;

c) auditors must be bound by a confidentiality agreement provided by HCL;

d) the cost of any audit will be borne by the Data Controller; and

Audits will not take place more frequently than once within a 12 month period or as otherwise expressly agreed between the parties in response to a breach or other data privacy incident.

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 Clause 4 of this Data Processing Addendum on an ongoing basis and will tighten, supplement and improve these measures in order to maintain compliance with the requirements set out in Clause 4 of this Data Processing Addendum. 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 Laws 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 hereby notifies the Data Controller of, and the Data Controller hereby consents to, transfers of Personal Data to entities in countries outside of the European Economic Area without an adequate level of protection as listed in Annex 4. The Data Controller hereby consents to the Data Processor executing the Standard Contractual Clauses on behalf of the Data Controller with the subprocessors 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. Incidents. When the Data Processor becomes aware of a successful incident that impacts the Processing of the Personal Data that is the subject of the Agreement, it shall notify the Data Controller about the incident without undue delay after confirmation of 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 Clause 7.1 of this Data Processing Addendum shall be understood to mean in any case:

7.2.1.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. This may include a request from a governmental entity for access to Data Controller's Personal Data.

7.2.2.any unauthorized or accidental access, processing, deletion, loss or any form of unlawful processing of the Personal Data;

7.2.3.any breach of the security and/or confidentiality as set out in Clause 3 and 4 of this Data Processing Addendum leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data;

7.2.4.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 such an incident.

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

7.4.1.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;

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

7.4.3.a description of the likely consequences of the incident; and

7.4.4.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.

7.5. Data Subject Request. If Data Processor receives a request from a data subject to exercise his or her right of access, right to rectification, restriction of processing, erasure, data portability objection to further processing or the right not to be subject to automated individual decision making , or any other rights provided to individuals under applicable Data Protection Laws, the Data Processor will, to the extent legally permitted, promptly forward such request to the Data Controller. Except to the extent required by applicable Data Protection Law, Data Processor shall not respond to any such request without Data Controller's explicit instruction, except to confirm that the request relates to Data Controller.

8. Contracting with Subprocessors

8.1. The Data Controller authorizes the Data Processor to engage subprocessors in Annex 5. Data Processor may make changes to the subprocessors upon prior reasonable notice to the Data Controller. If Data Controller wishes to object to a new subprocessor, Data Controller shall contact the Data Controller's account manager at Data Processor within thirty (30) days of being notified of such change in subprocessors.

8.2. The Data Processor shall ensure that each subprocessor is bound by the same or similar data protection obligations of the Data Processor under this Data Processing Addendum.

9. Returning or Destruction of Personal Data

9.1. At the Data Controller's written request, within thirty (30) days of termination or expiration of the applicable Agreement and fulfillment of the purposes agreed in the context of the Services (or as otherwise agreed by the parties) the Data Processor shall either delete, destroy or return all Personal Data to the Data Controller and destroy or return any existing copies. Consideration shall be taken at such time as to whether there is any legitimate need to retain the Personal Data so as not to disrupt any operations or otherwise interfere with the Services provided hereunder. Notwithstanding the above, Personal Data shall not be retained for longer than permitted under applicable Data Protection Laws.

9.2. Upon such deletion in accordance with Clause 9.1 above, the Data Processor shall notify third parties to whom it has provided access to Personal Data and request that the Personal Data be deleted from any third parties platforms, including any subprocessors' platforms.

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 Clause 4 (Security) of this Data Processing Addendum 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. This Data Processing Addendum 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 this Data Processing Addendum shall not discharge the Data Processor from its confidentiality obligations pursuant to Clause 3 of this Data Processing Addendum.

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 Data Processor acknowledges that it will be deemed to be a "Service Provider" under the California Consumer Privacy Act of 2018 ("CCPA") with respect to the processing of any personal information of a California resident hereunder.

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

12.3 Data Processor is prohibited from: (i) selling Personal Data, as defined under the CCPA; or (ii) retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services.

13. Miscellaneous

13.1. In the event of any inconsistency between the provisions of this Data Processing Addendum and the provisions of the Agreement, the provisions of this Data Processing Addendum 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. Each party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' or similar provision of the Agreement governing the applicable Services.

13.4. This Data Processing Addendum 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 Addendum 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 Controller:

The primary contact as provided by the Data Controller.

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

Chief Privacy Officer

HCL Technologies Limited
Axon Centre, Church Road
Egham, TW20 9QB
England, UK
privacy@hcl.com

Annex 2

Personal Data that will be processed in the scope of and for the duration of the Agreement and the purposes for which the Personal Data will be processed.

Personal Data shall be used for the purpose of providing the Services set forth in the Agreement.

The following set of data is collected by Support for the purpose of resolving customer report product problems which may contain Personal Data.

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 case 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

HCL Software (HCL SW) has implemented various technical and organizational security measures to comply with the data processor requirements of various geographies. HCL SW has documented and implemented data privacy policies and procedures. The Data Privacy Organization structure is a part of overall Risk & Compliance Governance Structure in HCL. There is a nominated chief privacy officer who oversees data protection at the organizational level.

The HCL privacy statement can be found on our website

Description of the technical and organisational security measures implemented by the data processor:

Information Security Organization & Compliance

- HCL SW has an identified Information Security organization structure which oversees information security related processes and activities for HCL SW.
- HCL has defined and documented data privacy policies and processes addressing access to personal data.
- HCL has defined, documented and implemented a Risk Management framework to identify risks related to security, privacy and other contractual requirements.
- Mandatory Information Security awareness training is provided through a country-wide e-Learning module.
- All incidents reported are analyzed for root cause and impact. The remedial actions are initiated by the process owners. The key incidents along with their root causes and impact are reported to HCL management.
- HCL SW Data Centers are ISO 27001 certified.

Physical & Environmental Security

- Physical access to Data Processor offices and processing area(s) is controlled by access control mechanism.
- Access to the datacenter is strictly controlled and any change is approved by the Data Processor technical team.
- Access is provided on need basis only and reviewed periodically
- Visitor entry is monitored and recorded. Visitors are allowed to visit only on prior approval basis.
- Visitors are provided Visitor badges.
- All critical areas are CCTV covered and recordings are maintained for at least 30 days.
- Security guards are deployed on 24X7 basis.

- Security guards are trained to challenge any individual with suspicious movements/ without appropriate identification card.
- Operational area is equipped with fire and smoke detectors and alarms with Fire extinguishers.
- Fire drills including evacuation drills are conducted on predefined frequency.
- Power supply to all the computers and other equipment in the building are provided with UPS and generators
- Temperature and humidity inside the server room is monitored regularly.

Laptops, Desktops, Servers and Networking equipment

- Operating systems and application patches are recommended by the vendor is tested and applied regularly to the desktops, laptops, Servers and networking equipment.
- Default IDs are changed and disabled. Their passwords are changed after initial installation. Manufacturers default passwords shall not be used.
- If sharing of files/directories from a server to other computers is required, then it has to be enabled in such a way that only users who have need to know is having the access to the share and the principle of least privilege is followed.
- Remote Diagnostics dial in ports of servers and networking equipment is normally disabled. It is only enabled for diagnostics and troubleshooting purposes only for the duration of diagnostic activity. Appropriate authorization is obtained before enabling these ports and when enabled access is given to authorized personnel only. These activities are also logged and monitored.
- Systems clocks of all the servers and networking equipment is synchronized and they are set to the time of the time zone of the location of the server/equipment. Only authorized personnel are having the privilege to change or reset system clock time.
- Administrative accounts are set with strong passwords and privileges are given to only identified persons.
- Antivirus software is installed on all desktops and servers.
- Antivirus signatures are updated on daily basis and any deviations/ exceptions are tracked.
- Unauthorized software’s are not allowed on laptops, desktops and servers.
- Backups are taken and restoration checks are done for identified systems based on agreed upon frequencies.
- Only company owned laptops are permitted inside the facility.
- For the Data Center, Visitor laptops and other media devices are permitted only on approval basis and for required purposes only.

Logical Access Controls

- Every HCL employee requires a unique ‘User ID’ and password to access the IT systems in the enterprise.

- Every user ID has a password and users are required to set and change their passwords as per HCL password policy.
- User IDs are created as per defined process and with adequate authorizations.
- User IDs are disabled on separation day based on information provided.

Email Security

- All emails are scanned for virus or malicious codes at gateway level.
- Email systems are configured to restrict identity spoofing, spamming and relaying to protect against the same.

Other Security controls

- Firewalls and routers are configured in such a way that only authorized traffic is allowed.
- HCL SW IT environment is regularly monitored for security related issues and incidents are reported on timely basis, once detected.
- All secured communications at HCL follows the encryption standard.
- DLP is installed on all end user machines

Annex 4

Support may be located in, but is not limited to, the follow list of countries:

Name	Reason For Processing	Country where data exporters data is processed
HCL Software Products Ltd.	To provide technical support to HCL Software customers	United States
HCL Technologies Canada Inc	To provide technical support to HCL Software customers	Canada
HCL Technologies Ltd.	To provide technical support to HCL Software customers	France
HCL Technologies Germany GmbH	To provide technical support to HCL Software customers	Germany
HCL Technologies BV	To provide technical support to HCL Software customers	Netherlands
HCL Technologies Italy S.P.A	To provide technical support to HCL Software customers	Italy
HCL Great Britain Ltd	To provide technical support to HCL Software customers	United Kingdom
HCL Technologies Sweden AB	To provide technical support to HCL Software customers	Sweden
HCL Technologies Philippines Inc	To provide technical support to HCL Software customers	Philippines
HCL Japan Ltd	To provide technical support to HCL Software customers	Japan
HCL Technologies Beijing Co. Ltd.	To provide technical support to HCL Software customers	China

HCL Australia Services Pty. Ltd.	To provide technical support to HCL Software customers	Australia
HCL Technologies Ltd	To provide technical support to HCL Software customers	India
HCL (Brazil) Tecnologia da informacao Ltda.	To provide technical support to HCL Software customers	Brazil

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
Microsoft Azure	Global	Cloud hosting services
Google Cloud Platform	Global	Cloud hosting services used to reproduce customer reported problems
IBM	Global	Level 2/Level 3 support for escalations of IBM-related products

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 the data exporting organisation:...

Address:..

Tel.:.. ; fax: .... ; e-mail:....................................

Other information needed to identify the organisation:

....

(the data **exporter**)

And

Name of the data importing organisation: ....

Address:..

Tel.: ....; fax: ....; e-mail: ....

Other information needed to identify the organisation:

....

(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.

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, namely…………………………………………………………………………

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, namely……

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 the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

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 procure Support for software products that are licensed from the data importer. 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, HCL Technologies Limited, is a provider of Services as defined in the Clause 1.1 of Data Processing Addendum to the data exporter. 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):

- Data exporter's employees
- End users of the application associated with the software product
- Any other users as defined by data exporter based on the business use cases which utilize the software product

Categories of Data

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

- Contact details (includes but is not limited to Contact name, business phone number, business email address, Contact's timezone, etc.)
- Profile details (includes but is not limited to business details such as job title, location, etc. required to interact with the software product)
- Any other data as defined by data exporter based on the business use cases which utilize the software product

Special Categories of Data (*if appropriate*)

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

N/A

Processing Operations

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

- **Customer Contact Information:** To communicate with the data exporter regarding their product support cases, the data importer maintains a record of Company and Customer Contact details.

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

- **Diagnostic data:** The diagnostic data would be shared by the data exporter to the data importer in order to troubleshoot the reported issue in the support case. Such data could include configuration files, log data, or any other piece of relevant data for such investigation.

FOR DATA IMPORTER – [__________]

Name: ………………………………………………………………… ………………………………

Authorized
Signature: ……………………………………………………………… …………

FOR DATA EXPORTER – ___________

Name: ………………………………………………………………… ………………………………

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 organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

HCL SW has implemented various technical and organizational security measures to comply with the data processor requirements of various geographies. HCL SW has documented and implemented data privacy policies and procedures. The Data Privacy Organization structure is a part of overall Risk & Compliance Governance Structure in HCL. There is a nominated chief privacy officer who oversees data protection at the organizational level.

The HCL privacy statement can be found on our website

Description of the technical and organisational security measures implemented by the data processor:

Information Security Organization & Compliance

- HCL SW has an identified Information Security organization structure which oversees information security related processes and activities for HCL SW.
- HCL has defined and documented data privacy policies and processes addressing access to personal data.
- HCL has defined, documented and implemented a Risk Management framework to identify risks related to security, privacy and other contractual requirements.
- Mandatory Information Security awareness training is provided through a country-wide e-Learning module.
- All incidents reported are analyzed for root cause and impact. The remedial actions are initiated by the process owners. The key incidents along with their root causes and impact are reported to HCL management.
- HCL SW Data Centers are ISO 27001certified.

Physical & Environmental Security

- Physical access to Data Processor offices and processing area(s) is controlled by access control mechanism.
- Access to the datacenter is strictly controlled and any change is approved by the Data Processor technical team.
- Access is provided on need basis only and reviewed periodically

- Visitor entry is monitored and recorded. Visitors are allowed to visit only on prior approval basis.
- Visitors are provided Visitor badges.
- All critical areas are CCTV covered and recordings are maintained for at least 30 days.
- Security guards are deployed on 24X7 basis.
- Security guards are trained to challenge any individual with suspicious movements/ without appropriate identification card.
- Operational area is equipped with fire and smoke detectors and alarms with Fire extinguishers.
- Fire drills including evacuation drills are conducted on predefined frequency.
- Power supply to all the computers and other equipment in the building are provided with UPS and generators
- Temperature and humidity inside the server room is monitored regularly.

Laptops, Desktops, Servers and Networking equipment

- Operating systems and application patches are recommended by the vendor is tested and applied regularly to the desktops, laptops, Servers and networking equipment.
- Default IDs are changed and disabled. Their passwords are changed after initial installation. Manufacturers default passwords shall not be used.
- If sharing of files/directories from a server to other computers is required, then it has to be enabled in such a way that only users who have need to know is having the access to the share and the principle of least privilege is followed.
- Remote Diagnostics dial in ports of servers and networking equipment is normally disabled. It is only enabled for diagnostics and troubleshooting purposes only for the duration of diagnostic activity. Appropriate authorization is obtained before enabling these ports and when enabled access is given to authorized personnel only. These activities are also logged and monitored.
- Systems clocks of all the servers and networking equipment is synchronized and they are set to the time of the time zone of the location of the server/equipment. Only authorized personnel are having the privilege to change or reset system clock time.
- Administrative accounts are set with strong passwords and privileges are given to only identified persons.
- Antivirus software is installed on all desktops and servers.
- Antivirus signatures are updated on daily basis and any deviations/ exceptions are tracked.
- Unauthorized software's are not allowed on laptops, desktops and servers.
- Backups are taken and restoration checks are done for identified systems based on agreed upon frequencies.
- Only company owned laptops are permitted inside the facility.

- For the Data Center, Visitor laptops and other media devices are permitted only on approval basis and for required purposes only.

Logical Access Controls

- Every HCL employee requires a unique ‘User ID’ and password to access the IT systems in the enterprise.
- Every user ID has a password and users are required to set and change their passwords as per HCL password policy.
- User IDs are created as per defined process and with adequate authorizations.
- User IDs are disabled on separation day based on information provided.

Email Security

- All emails are scanned for virus or malicious codes at gateway level.
- Email systems are configured to restrict identity spoofing, spamming and relaying to protect against the same.

Other Security controls

- Firewalls and routers are configured in such a way that only authorized traffic is allowed.
- HCL SW IT environment is regularly monitored for security related issues and incidents are reported on timely basis, once detected.
- All secured communications at HCL follows the encryption standard.
- DLP is installed on all end user machines