DATA PROCESSING ADDENDUM

For Convergint Customers

This Data Processing Addendum ("**Addendum**") forms part of the agreement that references and incorporates this Addendum ("**Agreement**") entered into between the Convergint entity ("**Convergint**") and the customer specified in the Agreement ("**Customer**"). This Addendum, together with all appendices, annexes, exhibits, attachments, and amendments hereto, reflects the parties' agreement regarding the Processing of Personal Data (as defined below) by Convergint in connection with providing services described in the Agreement. This Addendum applies solely to the extent of such Processing, and if no such Processing takes place, this Addendum does not apply.

In the event of a conflict between the Agreement and this Addendum, the terms and conditions of this Addendum will prevail. If Customer and Convergint enter into EU SCCs (defined below) in relation to the same subject matter as this Addendum, in the event of a conflict, the EU SCCs shall prevail over both the Addendum and the Agreement.

1. DEFINITIONS AND INTERPRETATION

1.1 **Affiliate** means any entity directly or indirectly controlling, controlled by, or under common control with Convergint.

1.2 **Business Contact Information** means Personal Data that a Party collects from the other Party's personnel for the purpose of maintaining a business relationship with that Party (e.g., contracting, billing, general relationship inquiries).

1.3 **Data Controller** means the entity responsible for determining the purposes and the means of Processing Personal Data. The term "Data Controller" includes entities that assume the role of "Data Controller" (*e.g.*, under GDPR), "Business" (*e.g.*, under CCPA / CPRA), or other analogous roles in applicable Data Protection Laws.

1.4 **Data Processor** means the entity that Processes Personal Data on behalf of the Data Controller. The term "Data Processor" includes entities that assume the role of "Data Processor" (*e.g.,* under GPDR), "Service Provider" (*e.g.*, under CCPA / CPRA), or other analogous roles in applicable Data Protection Laws.

1.5 **Data Protection Laws** means all laws and regulations relating to data privacy, information security, data protection, cross-border data flows, security and protection of Personal Data, and Personal Data rights, including without limitation the California Consumer Privacy Act ("CCPA"), the California Privacy Rights Act ("CPRA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, the Connecticut Data Privacy Act, state and federal data breach notification laws, the implementing legislation and regulations of the European Union member states under the European Union General Data Protection Regulation (EU) 2016/679 ("GDPR"), and the Brazilian General Data Protection Law No. 13,709/2018 ("LGPD").

1.6 **Data Subject** means an identified or identifiable natural person whose Personal Data is Processed by Convergint under the Agreement.

1.7 **Personal Data** means information relating to an identified or identifiable natural person or otherwise considered "personal data" or "personal information" under applicable Data

Protection Laws, and that Convergint "Processes" (defined below) on behalf of Customer under this Agreement.

1.8 **Data Incident(s)** means a breach of security in Convergint's systems or facilities and/or Convergint's Sub-processors' systems or facilities that results in the accidental, unlawful, or unauthorized destruction, loss, alteration, damage, disclosure, access to, or use of Personal Data transmitted, stored, or otherwise Processed by or on behalf of Convergint.

1.9 **Processing or Process** mean one or more of the following activities: collection; recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction performed on the Personal Data;

1.10 **EU SCCs** means the EU Standard Contractual Clauses set forth in EU Decision 2021/915 (June 2021), as well as the UK Addendum (to the extent applicable), with Controller-to-Processor (Module 2) selected in all applicable locations; and

1.11 **Sub-Processors** means any thirdparty services providers Convergint engages for Processing (whether in part or in full) of Personal Data processed under this Agreement.

2. GENERAL PROCESSING TERMS

2.1 The Parties agree that Customer is the Data Controller in relation to the Personal Data and that Customer appoints Convergint as the Data Processor to Process Personal Data on Customer's behalf.[1] Such Processing shall solely be for the purposes necessary for the fulfilment of services described under the Agreement as well as any accepted SOWs, Purchase Orders, or other instruments executed under the Agreement (collectively, "SOWs"). Convergint shall Process Personal Data only on documented instructions from Customer, which may be set forth directly in the Agreement, this Addendum, any accepted SOWs, or other written instructions that are acknowledged and confirmed by Convergint. Convergint shall not disclose Personal Data to another entity except as otherwise provided in this Addendum.

2.2 Convergint is not the manufacturer or developer ("OEM") of certain products ("Third Party Products") delivered or serviced by Convergint, and such OEMs are not Convergint subprocessors. Notwithstanding anything to the contrary, Convergint's obligations regarding privacy and information security exclude Third Party Products except to the extent of processing performed directly by Convergint or its subcontractors.

2.3 Each Party shall be responsible for compliance with applicable Data Protection Laws related to the performance of its obligations under the Agreement, and Customer represents and warrants that it has the necessary rights and permissions to provide the Personal Data for processing as contemplated under the Agreement. Convergint shall promptly notify Customer if Convergint makes a determination that it can no longer meet its obligations under applicable Data Protection Laws and/or if Convergint believes an instruction from Customer violates applicable Data Protection Laws.

2.4 All Convergint personnel authorized to Process Personal Data shall be bound to a duty of confidentiality regarding such Personal Data.

2.5 Convergint is a global company and may store, access or transfer Personal Data across borders to other jurisdictions and may transfer Personal Data to other Convergint Affiliates.

[1] As an exception to the foregoing, each Party is the Data Controller of the Business Contact Information it receives related to the personnel of the other party. Business Contact Information may only be used for the business purpose of maintaining the business relationship and it must be protected using appropriate technical and organizational measures in accordance with Data Protection Laws.

When it does so, Convergint will comply with applicable Data Protection Laws regarding such transfers (including, where appropriate, EU SCCs or the UK Addendum 2022 executed among Convergint Affiliates).

2.6 Upon request, Convergint shall assist Customer in performing any risk assessment that is designed to identify and analyze whether processing of Data Subject personal information presents significant risk to Data Subject's privacy or security ("Data Protection Impact Assessments") where required under the Data Protection Laws.

3. REQUESTS AND INQUIRIES

3.1 Convergint shall within 5 business days inform Customer in writing of any request, inquiry or complaint by a data protection supervisory authority or regulatory body and/or Data Subject that it receives in relation to the Processing of Personal Data.

3.2 At Customer's request, Convergint shall provide assistance as reasonably necessary to comply with any request or inquiry Customer or Convergint has received from a Data Subject or data protection supervisory authority or regulatory body in relation to the Processing of Personal Data.

3.3 Convergint shall not disclose or report any information to any Data Subject, data protection supervisory authority, or regulatory body in relation to the Processing of Personal Data without the prior written consent of Customer unless required by Data Protection Laws.

4. DATA SECURITY

4.1 Convergint shall implement administrative, technical and organizational measures to ensure a level of confidentiality, integrity, availability and resilience of the Personal Data, including processes and procedures appropriate to the data protection risks of such Personal Data, including those set forth in the Convergint Information Security Addendum, available on https://www.convergint.com/terms.

4.2 Convergint shall have in place a plan and program to manage the consequences of Data Incidents. Upon the occurrence of a Data Incident, Convergint shall:

(a) Notify Customer of the Data Incident without undue delay of Convergint having knowledge of such Data Incident, with such notification to include a reasonably detailed description of the Data Incident (*e.g.*, where information is available, the nature of the breach, including categories and approximate number of data subjects and personal data records concerned; likely consequences of the breach; and measures taken to address the breach)

(b) Take prompt steps to mitigate the consequences of such Data Incident;

(c) Investigate the Data Incident;

(d) Assess the risks and potential adverse consequences of the Data Incident;

(e) Collaborate closely and without delay with Customer to determine the appropriate response and action, including where applicable, notification to the relevant Data Subjects or data protection supervisory authorities; and

(f) Assist Customer upon request with responses and actions to carry out as a result of the Data Incident.

4.3 Convergint shall not report any Data Incident to any data protection supervisory authority, regulatory body or Data Subjects without Customer's prior written consent unless required by Data Protection Laws.

5. SUB-PROCESSING AND THIRD PARTIES

5.1 Customer hereby grants Convergint general authorization to use Sub-Processors (and onward Sub-processors) to Process Personal Data in accordance with this Addendum. Prior to engaging any Sub-Processors in the context of provisioning services under this Agreement, Convergint will provide Customer with at least fifteen (15) days' advanced notice and an opportunity to object. If Customer provides no objection during this notice period, Customer shall be deemed to have provided authorization for use of such Sub-Processor. In the event Customer objects, the Parties shall cooperate to address Customer's concerns and/or select an alternative, mutually agreeable Sub-Processor. All Sub-Processors listed in Appendix 1 shall be deemed as authorized unless specifically objected to in writing.

5.2 Convergint shall ensure that its Sub-Processors are contractually bound to meet obligations as required by Data Protection Laws and Convergint shall remain responsible for all acts and omissions of its Sub-Processors with respect to the Personal Data.

6. RECORDS AND AUDITS

6.1 Processor Records

(a) Convergint shall keep and maintain (and shall require its Sub-Processors keep and maintain), during this Agreement and for applicable retention periods after its termination or expiry, complete and accurate records of the Processing activities in a manner compliant with applicable Data Protection Laws.

6.2 Audit

(a) Upon request, Convergint will supply a summary copy of security audit report(s) ("Report") to Customer demonstrating its technical and organizational measures to ensure a level of confidentiality, integrity, availability and resilience of the Personal Data. Convergint shall also respond to any reasonable written audit questions submitted to it by Customer that are relevant to Convergint's compliance with Data Protection Laws with respect to its handling of the Personal Data, provided that Customer shall not exercise this right more than once per year.

(b) Customer shall be entitled to conduct audits to validate Convergint's compliance with this Addendum, provided that such audits shall be at Customer's expense, limited to one audit every 12 months (except in the event of a data breach), conducted upon at least 30 days' notice, conducted during normal business hours and in a manner that does not interfere with Convergint's business activities, limited to systems and facilities relevant to Customer data, and subject to an appropriate confidentiality agreement. Network audits or tests (including penetration or vulnerability tests) shall be conducted only upon prior notice to and consent from Convergint (such consent not to be unreasonably withheld) regarding the scope and parameters of such audit or test.

(c) International Data Transfers

6.3 Convergint shall comply with Data Protection Laws in connection with any international transfer of Personal Data.

6.4 Any transfer of Personal Data located in the European Economic Area by Customer to Convergint to a country located outside the European Economic Area not deemed to have adequate protection under Data Protection Laws shall be legitimized through implementation of EU SCCs along with any other supplemental measures adopted by the Parties. To the extent applicable to the Agreement given the nature of the services, the EU SCCs are set forth in Appendix 2.

6.5 Any transfer of Personal Data located in the United Kingdom by Customer to Convergint to a country located outside the United Kingdom not deemed to have adequate protection under Data Protection Laws shall be legitimized through implementation of the UK Addendum 2022 along with any other supplemental measures adopted by the Parties. To the extent applicable to the Agreement given the nature of the services, the UK Addendum 2022 is set forth in Appendix 2.

6.6 To the extent Personal Data is being transmitted from Switzerland to a country located outside Switzerland not deemed to have adequate protection under Data Protection Laws, the Parties agree and acknowledge that the EU SCCs apply to such transfers, references to the GDPR are to be understood as references to the FADP, the competent supervisory under Annex I.C is the Swiss FDPIC, and the term 'member state' as used in the EU SCCs does not exclude data subjects in Switzerland.

6.7 In relation to Personal Data protected under any other Data Protection Laws, where a transfer safeguard is required in addition to the terms of this Addendum, the Parties agree the EU SCCs will apply and adapted for local purposes as follows:

(a) references to the EU, EU Member States and EU Member State law shall mean the originating country protecting the transfer;

(b) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the originating country's law;

(c) under Clause 18(c) of the EU SCCs, data subjects in the originating country shall have the right to sue for their rights at their place of habitual residence and the local courts shall be the applicable courts;

(d) references to the GDPR in the EU SCCs shall include the reference to any equivalent provisions of the originating country's Data Protection Laws; and

(e) the competent supervisory authority under the originating country's Data Protection Laws shall have regulatory authority for the purposes of the EU SCCs.

7. DELETION OR RETURN OF PERSONAL DATA

7.1 At Customer's request upon termination of this Agreement, Convergint will promptly return or delete any Personal Data and all copies thereof, except where prohibited by applicable data retention laws or other legal obligations. Convergint shall provide, upon Customer's request, written confirmation of compliance with this provision.

8. CUSTOMER OBLIGATIONS

8.1 Except for Services specifically requested of Convergint pursuant to this Agreement, Customer is solely responsible for the information security of its systems, which includes Third Party Products. If applicable based on the requested services, Convergint may access Customer's information systems. Convergint is not responsible for losses or harms caused by Customer's own systems, by following Customer's instructions, by third party or Customer-specified remote access software, or that are otherwise not due to the fault of Convergint, and Customer remains responsible for the overall security of its information systems. Except as provided by this Addendum, Customer is responsible for the security of its own systems (hardware, software, networks, *etc.*).

9. GENERAL PROVISIONS

9.1 **Duration**. The term of this Addendum will end simultaneously and automatically at the later of (i) the termination of the Agreement, or (ii) when all Personal Data is deleted from Convergint's and each and all of its Sub-Processors' systems.

9.2 **Regulatory Changes.** Customer agrees to reasonably cooperate with Convergint to implement changes to this Addendum or the Processing of Personal Data as necessary to comply with changes in applicable Data Protection Laws.

9.3 All other provisions of the Agreement remain in full force and effect.

Appendix 1

Summary of Data Processing Activities

1. Subject matter / business purpose of the Personal Data processing	Systems integration services as further specified in the Agreement and applicable SOWs
2. Nature of the processing	Convergint provides installation, configuration, and maintenance services for Third Party Products on infrastructure managed by our customers or their service providers. The exact nature of processing will be determined based on customer requirements and specifications and/or Third Party Product capabilities or specifications.
3. Category of data subjects whose data will be processed	End users of Customer systems being integrated or serviced by Convergint or as otherwise specified in the Agreement or associated statements of work, such end users typically including employees, contractors, and visitors to Customer premises.
4. Type of personal data subject to processing	Data utilized for access management, identity management, security-related surveillance, alarm monitoring, and/or such other data types as processed by Customer systems being installed, integrated, or serviced by Convergint, as specified in the Agreement or applicable statements of work. Data types are governed by customer specifications and/or Third Party Product capabilities or specifications.
5. Duration of processing	During term of Agreement unless otherwise requested by Customer, plus such additional period of time as required for compliance with applicable data retention periods and archival or backup purposes
6. Frequency of data transfer	As agreed in the Agreement and as otherwise requested
7. Sub-processors being used by Convergint	See “Convergint Subprocessor Disclosure”, available at convergint.com/terms.

Appendix 2

EU SCCs

Standard Contractual Clauses (Decision 2021/914/EU)
For use when Personal Data in European Economic Area (EEA) is transferred outside of EEA

Controller to Processor (Module 2)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in

Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records

concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the

representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has

become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public

authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii)

Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*
Name: As described in Agreement
Address: As specified in Agreement
Contact person's name, position and contact details: As specified in Agreement
Activities relevant to the data transferred under these Clauses: As described in Agreement
Signature and date: Signature in Agreement constitutes acceptance of EU SCCs
Role (controller/processor): CONTROLLER

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*
Name: Convergint
Address: One Commerce Drive, Schaumburg, IL 60173
Contact person's name, position and contact details: Shubham Mukherjee, DPO, dataprotectionofficer@convergint.com
Activities relevant to the data transferred under these Clauses: As described in Agreement
Signature and date: Signature in Agreement constitutes acceptance of EU SCCs
Role (controller/processor): PROCESSOR

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

See Appendix 1

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

See Appendix 1

Nature of the processing

See Appendix 1

Purpose(s) of the data transfer and further processing

See Appendix 1

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Duration of Agreement subject to applicable data retention laws

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Appendix 1

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Ireland Data Protection Commission

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

See Convergint Information Security Addendum, available on convergint.com/terms.

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses for the transfer of personal data outside the UK

Part 1 - Tables

Table 1: Parties

Start date	The start date shall be the earlier of the date of execution of the Parties' underlying commercial agreement or the date of execution of these SCCs	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See EU SCCs Annex I.A	See EU SCCs Annex I.A
Key Contact	See EU SCCs Annex I.A	See EU SCCs Annex I.A
Signature (if required for the purposes of Section 2)	See signature block of Agreement	See signature block of Agreement

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: See accompanying EU SCCs Reference (if any): EU SCCs Other identifier (if any):

Table 3 – Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See EU SCCs
Annex 1B: Description of Transfer: See EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): See EU SCCs

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: □ Importer □ Exporter ☒ neither Party

Alternative Part 2 - Mandatory Clauses:

Mandatory Clauses (Part 2) are incorporated in this Addendum

Mandatory Clauses means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.