DATA PROCESSING ADDENDUM

For Use With Convergint's Subcontractors (Subprocessors)

This Data Processing Addendum ("**Addendum**") forms part of any underlying commercial agreements and/or the agreement that references and incorporates this Addendum ("**Agreement**") entered into between Convergint Technologies, LLC and its Affiliates ("**Convergint**") and the supplier specified in the Agreement ("**Company**"). This Addendum, together with all appendices, annexes, exhibits, attachments, and amendments hereto, reflects the parties' agreement regarding Company's Processing of Protected Information in connection with providing products and services described in the Agreement. In the event of a conflict between the Agreement and this Addendum, the terms and conditions of this Addendum will prevail. If Convergint and Company 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 Company.

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 applicable data and/or privacy laws, rules or regulations in connection with all use and processing of Protected Information including Personal Data, including laws, rules or regulations of any applicable country from which such data originated, including laws, rules or regulations that relate to the security and protection of personally-identifiable information, data privacy, trans-border data flow or data protection.

1.6 **Data Subject** means the individual(s) whose Personal Data is Processed by Company under this Agreement.

1.7 **Harmful Code** means vulnerabilities, viruses, worms, time bombs, key-locks, Trojan horses and other malicious code, files, scripts, agents or programs that could disrupt or interfere with the operation of the Products or equipment upon which the Products operate.

1.8 **Information Systems** means all hardware, software, networks, and associated services that relate to or enable any of the features or functionality of the Products and/or that store, transmit, enable access to, or Process Protected Information.

1.9 **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.

1.10 **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;

1.11 **Products** means those products or services, including related documentation, that are sold or supplied by Company to Convergint.

1.12 **Protected Information** means information provided by, about, or pertaining to Convergint, information pertaining to or created by Convergint's use of the Products, and information that is considered confidential to Convergint pursuant to the Agreement or that Company should understand to be confidential based on the circumstances. Protected Information also includes Personal Data.

1.13 **Security Incident(s)** means any potential, suspected, or actual unauthorized disclosure, loss, destruction, compromise, damage, alteration, access or theft of an Information System and/or Protected Information.

1.14 **EU SCCs** means the EU standard Contractual Clauses set forth in EU Decision 2021/915 (June 2021), with Processor-to-Processor (Module 3) selected in all applicable locations; and

1.15 **UK Addendum 2022** means the International Data Transfer Addendum that came into force on March 21, 2022.

1.16 **Sub-Processors** means any third party service providers that a Processor engages for further Processing (whether in part or in full) of Personal Data processed under this Agreement.

2. GENERAL PROCESSING TERMS

2.1 The Parties agree that Convergint's customer is a Data Controller in relation to Personal Data being Processed under the Agreement, Convergint is a Data Processor in relation to such Personal Data, and Convergint appoints Company as a Sub-Processor to Process such Personal Data on Convergint's behalf.[1] Processing of Protected Information shall solely be for the purposes necessary for the fulfilment of services described under this Agreement as well as any accepted SOWs, accepted Purchase Orders, or other instruments executed under this Agreement. Company shall Process Protected Information only on documented instructions from Convergint, which may be set forth directly in the Agreement, this Addendum, any accepted SOWs, accepted Purchase Orders, or other accepted instruments executed under this Agreement, and/or other written instructions that are acknowledged and confirmed by Company. Company shall not Process Protected Information for any purposes other than those specified in this Section, and Company shall not disclose, sell, or share Protected Information to another entity except as otherwise provided in this Addendum. Company shall not combine or update Protected Information collected pursuant to this Addendum with any personal information received from another source or collected from Company's own interactions with a Data Subject. Company hereby certifies that it understands the restrictions in this Addendum and will comply with them.

[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.

2.2 Each Party shall comply with applicable Data Protection Laws related to the performance of its obligations under the Agreement, and provide the same level of privacy protection as required by applicable Data Protection Laws. Convergint represents and warrants that it has the necessary rights and permissions to provide the Protected Information for processing as contemplated under the Agreement. Company shall promptly notify Convergint if Company makes a determination that it can no longer meet its obligations under applicable Data Protection Laws, if Company believes an instruction from Convergint violations applicable Data Protection Laws, or if Company believes any Protected Information has been processed in a manner not authorized by Convergint or in violation of this Addendum.

2.3 All Company personnel authorized to Process Protected Information shall be bound to a duty of confidentiality regarding such Protected Information.

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

2.5 Company shall retain in confidence all Protected Information and shall not disclose such Protected Information to anyone, except to its employees or approved Sub-processors that have a need to know such information in furtherance of executing Convergint's instructions.

2.6 Company shall comply with all privacy or data protection policies or procedures of the applicable Data Controller, including any data processing addendums or information security requirements that are part of any upstream contracts between Convergint and the Data Controller, and any Convergint or Data Controller policies and procedures related to privacy or data protection. To the extent Company accesses any of the applicable Data Controller's information systems, Company shall: (1) only access such information systems upon authorization of Convergint or the applicable Data Controller; (2) implement and follow technical, administrative, and organizational measures sufficient to ensure that Company does not compromise the security of such information systems or the confidentiality, integrity, or availability of any of Convergint's or the applicable Data Controller's data; (3) comply with all applicable Data Protection Laws; and (4) comply with all privacy or data protection provisions of the applicable Data Controller, including any associated data processing addendums or information security requirements, and any Convergint or Data Controller policies and procedures related to information security.

3. REQUESTS AND INQUIRIES

3.1 Company shall within 5 business days inform Convergint 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 Protected Information.

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

3.3 Company shall not disclose or report any information to any Data Subject or data protection supervisory authority or regulatory body in relation to the Processing of Protected Information without the prior written consent of Convergint and the applicable Data Controller unless such disclosure is required by Data Protection Laws.

3.4 In the event that Company is required or requested by law, court order, warrant, subpoena, or other legal judicial process to disclose any Protected Information to any person other than Convergint, Company will promptly notify Convergint, unless and to the extent prohibited by law. Company also shall use all reasonable endeavors, including judicial remedies, to seek to defend against any disclosure of Protected Information and use all reasonable endeavors to assist Convergint and the applicable Data Controller in defending against any disclosure of Protected Information, as permitted by applicable law. Should Company be unable to challenge an order of disclosure of Protected Information, it will seek measures to mitigate the effects of the order until the court's decision. Should Company be unable to withdraw from disclosing the Protected Information without being in breach of the applicable laws, Company undertakes to disclose only that portion which is legally required, and will exercise reasonable effort to obtain reliable assurance that confidential treatment will be accorded to such Protected Information.

4. DATA SECURITY

4.1 Company shall implement administrative, technical and organizational measures to ensure a level of confidentiality, integrity, availability and resilience of the Protected Information and Company systems, processes and procedures that involve the Processing of Protected Information appropriate to the data protection risks of such Protected Information. Company shall validate the effectiveness of such measures at least annually. Such measures shall include at least those set forth in Appendix 2 to this Addendum.

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

(a) Notify Convergint of the Security Incident within 24 hours, with such notification to include a detailed description of the Security Incident, including the nature of the breach; 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) Utilize best efforts and take immediate steps to contain the Security Incident and mitigate its consequences, including restore to the last available backup of any Protected Information that may have been lost, damaged or destroyed as a result of the Security Incident;

(c) Investigate the Security Incident;

(d) Assess the risks and potential adverse consequences associated with the Security Incident;

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

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

4.3 Company shall not report any Security Incident to any data protection supervisory authority, regulatory body or Data Subjects without Convergint's or the applicable Data Controller's prior written consent unless such disclosure is required by Data Protection Laws.

4.4 Company acknowledges that the applicable Data Controller may have the right to, in its sole discretion, disclose the Security Incident, the circumstances of the Security Incident, and any relevant

information or documents as may be appropriate to affected individuals or entities, law enforcement authorities, regulators, data protection or supervisory authorities, affiliated entities, and other representatives and agents, in accordance with applicable Data Protection Laws or otherwise at its discretion.

5. SUB-PROCESSING AND THIRD PARTIES

5.1 Convergint hereby grants Company general authorization to use further Sub-Processors as necessary for the provision of services under this Agreement. Prior to engaging any Sub-Processors in the context of provisioning services under this Agreement, Company will provide Convergint with at least fifteen (15) days' advanced notice and an opportunity to object. If Convergint provides no objection during this notice period, Convergint shall be deemed to have provided authorization for use of such Sub-Processor. In the event Convergint objects, the Parties shall cooperate to address Convergint's concerns and/or select an alternative, mutually agreeable Sub-Processor.

5.2 Company warrants that it maintains a security evaluation process to conduct commercially reasonable due diligence prior to utilizing any Subcontractor to Process Protected Information, and shall obligate each such party to meet or exceed its own information security policies and standards as well as all requirements of this Addendum and applicable Data Protection Laws. Company is, and shall at all times remain, responsible for all acts and omissions of any and all of its employees and Subcontractors.

5.3 Company shall ensure that its Sub-Processors and employees are contractually bound to meet obligations no less strict than those expressed under this Agreement.

6. RECORDS AND AUDITS

6.1 Processor Records

(a) Convergint shall have the right to take reasonable and appropriate steps to ensure that Company uses the Protected Information that it collected pursuant to this Addendum in a manner consistent with the applicable Data Protection Laws. Company grants Convergint the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Protected Information.

(b) Company 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.

(c) Company shall allow (and shall require its Sub-Processors to allow) Convergint during this Agreement to access, inspect, audit and, in respect of electronic or paper documents, take copies of the above-mentioned records during normal business hours provided the Convergint has given Company a seven-day prior written notice.

6.2 Audit

(a) During Company's regular business hours, Convergint may, at its sole expense, perform a confidential audit of documentation, systems, devices, networks, and other materials reasonably necessary to demonstrate Company's compliance with this Agreement. Any onsite audit shall be conducted during regular business hours on a date that shall not be sooner than thirty (30) calendar days after Company's receipt of Convergint's written request for such audit, except that in the event of a Security Incident only one (1) day written notice shall be required. Such audits shall be limited to documentation, systems, devices, networks, and other materials reasonably necessary to show Company's compliance with this

Agreement and/or to understand the circumstances related to a Security Incident. Convergint may conduct the audit directly or via an independent auditor, at its discretion. If engaging an independent auditor, the independent auditor must execute prior to commencement of the audit a confidentiality and non-disclosure agreement, as presented by and for the benefit of Company. Company shall provide Convergint assistance as reasonably necessary for initiation and performance of the audit.

(b) Convergint or its designated representative may conduct a vulnerability test or pentest of Company with prior notice after: (i) any Security Incident; (ii) any adverse assessment, scan or audit of Company systems; or (iii) if Convergint discovers or reasonably suspects that Company may not be implementing, maintaining, or enforcing its compliance with this Addendum. Such vulnerability test or pentest shall be conducted on a mutually agreed date, which shall not be sooner than thirty (30) calendar days after Company's receipt of Convergint's written request, except that in the aftermath of a Security Incident only three (3) days' written notice shall be required.

(c) When conducting audits, vulnerability tests, or pentests, Convergint shall comply with Company's reasonable directions to minimize disruption to Company's business and to safeguard the confidentiality of Company's other confidential information.

6.3 Audit Report and Findings

(a) Where an audit, vulnerability test, or pentest reveals a data security risk that may have an impact on the security of Protected Information, or reveals any breach or non-compliance of this Agreement, Company shall promptly develop a remediation plan to remedy the risk or breach of the Agreement.

(b) Such plan shall be submitted to Convergint for information and Convergint shall have the right to request any reasonable further rectification steps. Company shall comply with the remediation plan and provide written evidence of completed remediation to Convergint. Convergint shall have the right to take reasonable and appropriate steps to remedy unauthorized uses of Protected Information.

7. International Data Transfers

7.1 Company shall comply with Data Protection Laws in connection with any international or cross-border transfer of Protected Information.

7.2 Any transfer of Protected Information located in the European Economic Area by Convergint to Company 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 3.[2]

7.3 Any transfer of Protected Information located in the United Kingdom by Convergint to Company 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 3.

[2] 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.

8. Deletion Or Return Of Protected Information

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

9. Survival

9.1 The rights and obligations of the Parties under this Addendum survive the termination, cancellation, or expiration of any other agreement entered into by the Parties for so long as Company has access to Protected Information.

Appendix 1

Summary of Data Processing Activities

1. Business purpose / nature of services / nature and purpose of the Personal Data processing	Systems integration or related services as further specified in the Agreement
2. Category of data subjects whose data will be processed	End users of Data Controller systems being integrated / 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 Data Controller premises.
3. 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 Data Controller 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.
4. 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
5. Frequency of data transfer	For installation, configuration, and servicing: On an as-needed basis For ongoing maintenance and support: As agreed in the Agreement and as otherwise requested
6. Sub-processors being used by Company	As separately notified to Convergint

Appendix 2

Information Security Measures

1. Information Security Measures

1.1. General. Company shall implement appropriate administrative, technical, physical, and organizational measures to ensure the security, confidentiality, integrity, availability, and resilience of all Information Systems, Products, and Protected Information.

1.2. Governance. Company shall create, implement and maintain an enterprise information security program that governs the Information Systems and the Products, that meets or exceeds industry best practices, that meets the requirements of all Data Protection Laws, and that includes without limitation appropriate policies, governance structures, staffing, monitoring and assessment procedures. Company shall maintain and follow a reasonable and appropriate written data security policy that includes technological, physical, administrative and procedural controls to protect the confidentiality, integrity and availability of Protected Information, and that meets or exceed prevailing industry standards or an applicable third-party security assurance standard such as ISO 27001 or Statement on Standards for Attestation Engagements No. 18 Type II ("SSAE 18") (SOC 2 Type II).

1.3. Product Security and Testing. Company shall test all Products prior to making them available to ensure such Products do not contain Harmful Code and meet or exceed industry best practices for information security. Company shall engage qualified security representatives, either internal or external, to perform penetration, vulnerability, or other applicable forms of testing on the Products at least annually.

1.4. Software Development. Company shall create, implement and maintain a secure software development lifecycle (SDLC) program that meets or exceeds industry best practices for all software, applications, or code applicable to the Products, including documented secure coding standards that are referenced and followed for all development activities. Company shall evaluate and document the risk of each application security issue identified. Company shall remediate identified application security issues utilizing a risk based approach within a reasonable timeframe in accordance with industry best practices.

1.5. System Administration. Company shall create, implement, and maintain system administration procedures for its Information Systems that meet or exceed industry best practices for information security, including without limitation, system hardening, event logging, firewall protection, malware protection, system and device patching and proper anti-virus installation. Hardening guides for Products shall be furnished upon request.

1.6. Access Controls. Company shall manage access rights to the Information Systems and Protected Information on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, and shall maintain a record of privilege levels. Company shall create, implement and maintain controls protecting access to the Information Systems and Protected Information that meet or exceed industry best practices, including at least unique user IDs, changing default passwords, multi-factor authentication, and a password policy that adopts prevailing industry standard for length, character type, complexity, expiry, re-use, and lock-outs, along with a review of user and privileged user access rights at least annually. Company shall maintain strict operating standards and guidelines for privileged user status, including but not limited to training and monitoring.

1.7. Encryption. Company shall ensure that all Protected Information is, at all times, encrypted using encryption mechanisms that meet or exceed industry standards while in transit (including but not limited to on public networks, email systems, or within Company's internal network) and while at rest (including without limitation where it is stored on servers, computers, smart phones / tablets, or removable media).

1.8. Data Segregation. Company shall create, implement, and maintain logical or physical data segregation that meets or exceeds industry standards to ensure Protected Information is not accessible by unauthorized users and not commingled with data from other end users or customers.

1.9. Logging. Company shall create, implement, and maintain security and system event logging procedures for the Information Systems and Products designed to meet or exceed industry standards in the detection, investigation and response to suspicious activity in a timely manner, including retention of event logs for at least twelve (12) months.

1.10. Patch Management. Company shall implement and maintain patch management procedures for the Information Systems and Products that meet or exceed industry best practices and that require patches to be prioritized, tested, and installed based upon criticality according to timelines that meet or exceed industry best practices. Company shall have a process for identifying and disclosing known vulnerabilities related to the products or services provided to its end users or customers. Upon request, Company shall provide the status of remediation efforts for vulnerabilities determined to present material risks to the Products or Information Systems. Company shall

have the relevant patch installed within seven (7) days of patch release for vulnerabilities prioritized as “Critical,” within thirty (30) days of patch release for vulnerabilities prioritized as “High,” and within a commercially reasonable period of time (not to exceed ninety (90) days) for all other vulnerabilities.

1.11. Network Security. Company shall create, implement and maintain internal and external network security policies and procedures for the Information Systems that meet or exceed industry best practices, and Company shall actively monitor the Information Systems for suspicious activity.

1.12. Endpoint Security. Company shall ensure all devices used by its Personnel are configured with security software including multi-factor authentication, anti-virus, anti-malware, and encryption; that each user account is associated with a specific, individual user; that each device is configured to the maximum extent possible for automatic security updates; that each device includes endpoint detection and response software and capabilities, and that each deice is configured to meet or exceed industry best practices for automatic locking, passwords, scanning for Harmful Code, and website or content filtering.

1.13. Physical Security. Company shall create, implement and maintain physical security policies and procedures for all facilities that contain or allow access to the Information Systems or Protected Information.

1.14. Testing. Company shall conduct at least quarterly vulnerability testing and annual penetration testing (both internal and external) for all the Information Systems and Products, and complete timely identification, tracking, and resolution of all findings using a risk-based approach in accordance with industry best practices. Upon request, Company shall provide a copy or summary of findings from such testing. For the avoidance of doubt, the testing conducted in accordance with this Section shall not limit Convergint’s right to conduct testing as otherwise authorized by this Exhibit.

1.15. Incident Response. Company shall create, implement, and maintain cyber incident response plans and procedures and shall test such plans and procedures at least annually. Company shall make available such incident response plans, or at a minimum summary forms of such incident response plans.

1.16. Compliance. Company shall comply with its obligations pursuant to all Data Protection Laws.

1.17. Remote Access. To the extent Company accesses (including remotely accesses) any of Convergint’s information systems, Company shall: (1) only access such information systems upon authorization of Convergint; (2) implement and follow technical, administrative, physical, and organizational measures sufficient to ensure that Company does not compromise the security of such information systems or the confidentiality, integrity, or availability of any Protected Information; and (3) comply with all Data Protection Laws. Company shall create, implement, and maintain remote access policies and procedures that meet or exceed industry best practices, ensure access to Convergint’s information systems require multi-factor authentication, and retain logs detailing activity conducted during each session for twelve (12) months.

1.18. Assessments and Audits. Upon request at any time, in the event of a Security Incident, or where required by applicable Laws, Company shall complete any reasonable information security assessments or questionnaires submitted by Convergint. Convergint may, at its sole expense and in its sole discretion, perform a confidential audit of documentation, systems, devices, networks, and other materials reasonably necessary to demonstrate Supplier’s compliance with this Exhibit. Such audit may be conducted directly or via an independent auditor (subject to appropriate confidentiality obligations), at Convergint’s discretion. Convergint or its independent auditor may conduct vulnerability tests or pentests of the Information Systems with reasonable prior notice to Company. Supplier shall provide Convergint or its independent auditor assistance as reasonably necessary for initiation and performance of such audits or tests. When conducting audits, vulnerability tests, or pentests, Convergint shall comply with Company’s reasonable directions to minimize disruption to Company’s business and to safeguard the Information Systems and Confidential Information. Company shall in a timely fashion and consistent with industry best practices track and resolve all findings arising out of any audits, vulnerability tests, or pentests, and confirm in writing such resolutions upon request.

1.19. Incident Notification and Response. Company agrees to promptly and without undue delay (but in any event within 24 hours of becoming aware of it) notify Convergint (with a copy to dataprotectionofficer@convergint.com) of any Security Incident. Such notice shall summarize in reasonable detail the type of data that was subject to the Security Incident, the identity of each affected data subject, the effect on Convergint, if known, of the Security Incident, the corrective actions taken or to be taken by Company, and any other information Convergint may reasonably request and provide sufficient information to enable Convergint to meet its obligations under Data Protection Laws. Company shall utilize best efforts and take immediate steps to investigate, contain, and mitigate the consequences of the Security Incident, including to restore the last available backup of any protected Information that may have been lost, damaged, or destroyed. Company shall promptly take such

reasonable and commercial steps as requested by Convergint to cooperate in the investigation, notification, mitigation, and remediation of any Security Incident at Company's own expense.

1.20. Employee Screening. Company shall create, implement and maintain policies and procedures that meet or exceed industry best practices regarding the background screening of all Company personnel, including without limitation and to the extent permitted by applicable law a criminal history screening that covers a period of seven (7) years. To the extent Company provides professional services Convergint, Company shall comply with reasonable requirements for background screening of Company personnel. Company shall ensure its personnel's access to the Information Systems and Protected Information is revoked immediately upon termination or when access is no longer required.

1.21. Training. Company shall create, implement and maintain a security awareness program for Company Personnel, which provides initial education and on-going awareness on at least an annual basis of information security best practices, privacy compliance, incident notification procedures, and adherence to Company's information security policies.

1.22. Business Continuity. Company shall create, implement, and maintain business continuity and disaster recovery plans (including creation of ongoing backups of applicable Information Systems) that meet or exceed industry best practices to enable prompt recovery of all Information Systems and Protected Information in the event of an unforeseen outage. Upon request, Company shall make such plans (or summaries of such plans) available to Convergint. Company shall implement its business continuity and disaster recovery plans as required to ensure Company continues to function through an operation interruption, and: (i) continues to provide the Services within 24 hours (RTO); and (ii) maintains data that is no less than 8 hours from point of outage (RPO). The Customer shall test business continuity and disaster recovery plans on at least an annual basis to determine the effectiveness of the plan and the organizational readiness to execute the plan.

1.23. Backups. Company shall maintain backup plans, procedures, and infrastructure to ensure that Company can quickly and efficiently restore compromised or disabled Information Systems, including availability and access to all associated Protected Information.

1.24. Data Destruction. Company shall destroy or return Protected Information to Convergint subsequent to the term of this Agreement and applicable retention periods. Destruction shall be carried out in accordance with industry best practices.

1.25. Service Providers / Subcontractors. If Company utilizes service providers or subcontractors in its provisioning of Products or services, Company shall: (a) obtain Convergint's express, written permission; and (b) shall ensure such service providers or subcontractors comply with all provisions of this Exhibit. Company shall be liable for any failure of its service providers or subcontractors to comply with all provisions of this Exhibit.

1.26. Cloud. Where Company is leveraging cloud-based services, Company shall ensure its cloud service provider maintains at all times an up-to-date certification under ISO 27001 or can provide an up-to-date, unqualified SOC 2 Type II report, in each case dated within the past 12 months. Company shall create, implement, and maintain security practices which meet or exceed industry best practices governing the information security of the cloud services utilized. Company shall create, implement and maintain a formal program to track and report end users with access to cloud systems that support the Products. Company shall gain appropriate assessment rights at any utilized cloud service provider sufficient to allow Convergint to audit the cloud platform. For any cloud service providers that will not agree to assessment rights, Company shall ensure that appropriate independent audit testing occurs annually and the resulting reports (e.g. SSAE 16 SOC2, ISO 27001, etc.) are reviewed and subsequently shared with Converging upon request. Company shall maintain all Protected Information in the original country of origin absent express authorization from Convergint (as applicable). Company shall establish controls to know the location of all Protected Information at all times.

Appendix 3

EU SCCs

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

Processor to Processor (Module 3)

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 personal 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(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(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 exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ([2]).

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([3]) (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 of Regulation (EU) 2016/679;

(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 or the controller 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 controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) 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.

(g) 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 controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. ([4]) 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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 and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by 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 ([5]);

(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). The data exporter shall forward the notification to the controller.

(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, if appropriate in consultation with the controller. 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 controller or 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.

The data exporter shall forward the notification to the controller.

(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.). The data exporter shall forward the information to the controller.

(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 minimization

(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. The data exporter shall make the assessment available to the controller.

(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 and the controller 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 _____ (*specify Member State*).

(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.

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: The Convergint entity that is named in the Agreement.
Address: As provided in the Agreement
Contact person's name, position and contact details: Shubham Mukherjee, Senior Counsel & Data Protection Officer, dataprotectionofficer@convergint.com
Activities relevant to the data transferred under these Clauses: See Appendix 1, above
Signature and date: Signature or acceptance of 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: As described in Agreement
Address: As provided in the Agreement
Contact person's name, position and contact details: To be communicated by Company
Activities relevant to the data transferred under these Clauses: See Appendix 1, above
Signature and date: Signature or acceptance of 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 Data Security provision of Addendum.

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] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

[3] 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 purposes of these Clauses.

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

[5] 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.