DATA PROCESSING AGREEMENT FOR SUPPLIERS

Conversant Group, LLC or one of its affiliates (the applicable entity will be referred to as, "**Conversant**") and Supplier have entered into an agreement (as may be amended from time to time) (the "**Services Agreement**") under which Supplier may process Conversant Personal Data in connection with the provision of Services. This Data Protection Agreement, including the Annexes attached hereto and the Standard Contractual Clauses ("**DPA**") governs Supplier's processing of that data and shall form part of and be incorporated by reference into the Services Agreement with Conversant for providing the Services – PROVIDED THAT any additional promises or protections from Supplier to Conversant in any other portion of the Parties' agreement(s) shall remain in place and are not superseded or waived by Conversant herein. This DPA shall be effective on the effective date of the Services Agreement. At all times, Supplier shall, and shall cause its Subprocessors to, comply with this DPA. Conversant (and its affiliate entering into any agreement with Supplier) and Supplier may each be referred to as a "**Party**" and together as the "**Parties**".

Notwithstanding expiry or termination of the Services Agreement, this DPA will remain in effect until, and will terminate automatically upon, deletion by Supplier and its Subprocessors of all Conversant Personal Data covered by this DPA, in accordance with this DPA.

1. Definitions and Interpretation

"**Affiliate**" means any entity under the control of a party where **"control"** means ownership of, or the power to vote, directly or indirectly, a majority of any class of voting securities of a corporation or limited liability company, or the ownership of any general partnership interest in any general or limited partnership or as otherwise defined in the Services Agreement to which the DPA relates.

"**Authorized Personnel**" means any natural person who Processes Conversant Personal Data on Supplier's behalf, including Supplier's employees, officers, partners, principals, contractors, and Subprocessors.

"**Controller**" means an entity that alone or jointly with others determines the purposes and means of Processing of Personal Data. For the purposes of this DPA, a Controller includes a "business" as such term is defined by the CCPA, or a similar designation under Data Protection Legislation.

"**Conversant Personal Data**" means any Personal Data provided or made available by or on behalf of Conversant to Supplier and/or collected or otherwise obtained by Supplier in connection with Supplier's performance of Services to Conversant and Processed by Supplier as a Processor, as more particularly described in the DPA and **Annex A**.

"**Data Protection Legislation**" means any applicable global laws relating to data protection and privacy and the Processing of Conversant Personal Data that is protected by applicable law in any relevant jurisdiction, including but not limited to: (i) EU/UK Data Protection Law; and (ii) US Data Protection Law.

"**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such Personal Data (General Data Protection Regulation) (the "**GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to have effect by virtue of section 2 of the European Union (Withdrawal) Act 2018, and any other laws in force in the UK applicable (in whole or in part) to the Processing of Personal Data (together, "**UK Data Protection Law**"); (iv) the Swiss Federal Act on Data Protection of

2020 and its Ordinance ("**Swiss FADP**"); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii) and (iv) above; in each case as may be amended, superseded or replaced from time to time.

"**Europe**" means, for the purposes of this DPA, the member states of the European Economic Area, the United Kingdom ("**UK**") and Switzerland.

“**Personal Data**” means all information relating to an identified or identifiable natural person or consumer ("**Data Subject**"), including any data or information that is deemed “personal data”, "personally identifiable information" and/or “personal information” under Data Protection Legislation.

“**Process**,” “**Processes**,” “**Processing**,” “**Processed**” means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, destruction, or creating information from, Personal Data.

"**Processor**" means an entity that Processes Personal Data on behalf, and in accordance with the instructions, of a Controller. For purposes of this DPA, a Processor includes a "service provider" as such term is defined by the CCPA, or any similar or analogous designation under Data Protection Legislation.

"**Restricted Transfer**" means a transfer (directly or via onward transfer) of Personal Data that is subject to EU/UK Data Protection Law to a country outside Europe which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).

"**Security Incident**" means any actual or suspected breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Conversant Personal Data or similar incident involving Conversant Personal Data.

"**Services**" means any product or service provided by Supplier to Conversant pursuant to and as more particularly described in the Services Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission's Implementing Decision 2021/914 of 4 June 2021, as updated or amended from time to time.

"**Subprocessor**" means any third party that has access to Conversant Personal Data and which is engaged directly or indirectly by Supplier to assist in fulfilling Supplier's obligations with respect to providing the Services pursuant to the Services Agreement or the DPA. Subprocessors may include Supplier’s Affiliates but shall exclude Supplier's employees, contractors and consultants who are natural persons.

“**Supervisory Authority**” means any regulatory, supervisory, governmental, state agency, Attorney General or other competent authority with jurisdiction or oversight over compliance with Data Protection Legislation.

"**Supplier**" means the means the party from which Conversant is purchasing solutions and its Affiliates.

"**Term**" means the term of the Services Agreement and any period after the termination or expiry of the Services Agreement during which Supplier and/or its Subprocessors Processes Conversant Personal Data, until Supplier has destroyed or returned such Conversant Personal Data in accordance with the terms of the DPA.

"**UK Addendum**" means the International Data Transfer Addendum to the Standard Contractual Clauses (version B1.0) issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as it is revised under Section 18 therein; as may be amended, superseded or replaced from time to time.

"**US Data Protection Law**" means all relevant U.S. federal and state privacy laws (including any implementing regulations and amendment thereto) effective as of the date of this DPA, including but not limited to (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"); (ii) the Virginia Consumer Data Protection Act ("**CDPA**"); (iii) the Colorado Privacy Act ("**CPA**"); (iv) the Utah Consumer Privacy Act (“**UCPA**”); (v) the Connecticut Data Privacy Act ("**CTDPA**"); in each case as may be amended, superseded or replaced from time to time.

2. Scope of this DPA and Relationship of the Parties

2.1 Supplier as a Processor. For the purposes of the GDPR and similar Data Protection Legislation, the Parties agree that Supplier will Process Conversant Personal Data as a Processor acting on behalf of Conversant (whether a Controller itself or acting on behalf of (a) an Affiliate or (b) a third-party Controller) and only in accordance with Conversant's written instructions, as further described in Annex A attached hereto, and this DPA shall apply accordingly.

2.2 Sale or Sharing of Conversant Personal Data Prohibited. Supplier will not (a) sell Conversant Personal Data to a Subprocessor or any other third parties, as the term "sell" is defined under US Data Protection Law; (b) share Conversant Personal Data to a Subprocessor or any other third parties, as the term “share" is defined by the CCPA; (c) retain, use, disclose or transfer the Conversant Personal Data for any purposes other than for performing Supplier’s obligations under the Services Agreement and this DPA, in particular, the Permitted Purpose (as defined below), including to retain, use or disclose Conversant Personal Data for a commercial purpose other than performing its Services under the Services Agreement and this DPA; (d) retain, use, or disclose the Conversant Personal Data outside the direct business relationship between the Parties; or (e) combine Conversant Personal Data received with Personal Data that Supplier receives from other sources or that it collects from its own interaction with the Data Subject, except as otherwise permitted by the Services Agreement or by US Data Protection Law. The Parties agree that Conversant's transfer of Conversant Personal Data to Supplier is not a sale, and Supplier provides no monetary or other valuable consideration to Conversant in exchange for Conversant Personal Data. Supplier certifies that it understands the restrictions set out in this Section and will comply with them.

2.3 Compliance with Data Protection Legislation. Each Party shall comply with its obligations under Data Protection Legislation with respect to the Processing of Conversant Personal Data. The Parties shall reasonably assist each other in meeting their respective obligations under Data Protection Legislation. Supplier shall not perform its obligations under the Services Agreement or the DPA in such a way as to cause Conversant to breach any of its obligations under Data Protection Legislation. Supplier shall promptly notify Conversant in writing if it believes that it can no longer meet its obligations under any Data Protection Legislation.

2.4 Remediation. Conversant has the right to take reasonable and appropriate steps to ensure that Supplier uses Conversant Personal Data in a manner that is consistent with a business’s obligations under US Data Protection Law and other Data Protection Legislation, which may include asking survey questions or for audits or interviews of appropriate personnel during ordinary business hours.

3. Processing Instructions

3.1 Supplier will Process the Conversant Personal Data as a Processor only in accordance with the written instructions from Conversant and in compliance with Data Protection Legislation. Such instructions may be specific or of a general nature as set out in this DPA, the Services Agreement, an SOW, or as otherwise notified by Conversant to Supplier in writing from time to time.

3.2 Conversant instructs Supplier to Process Conversant Personal Data as a Processor for the following purposes: (a) to provide the Services and all other Processing necessary for Supplier to perform its obligations under the Services Agreement and the DPA; (b) to comply with any other reasonable instructions provided by Conversant (e.g., via email or support tickets) that are consistent with the terms of the Services Agreement and the DPA; (c) to comply with Supplier's legal obligations under applicable law, including Data Protection Legislation; and (d) any other purpose expressly authorised by Conversant under the Services Agreement (collectively and individually the "**Permitted Purpose**").

3.3 Supplier shall not Process Conversant Personal Data for its own or for any other purposes except (i) as otherwise specified in this DPA or (ii) to the extent applicable, as required by Union or Member State law to which the Supplier is subject. If (ii) applies, Supplier shall inform Conversant of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and, where permitted, Supplier shall only Process Conversant Personal Data as strictly necessary to comply with such law. Supplier certifies that it understands the restrictions set out in this Section 3.3 and will comply with them.

3.4 Supplier shall make available to Conversant all information necessary to demonstrate compliance with the obligations laid down in this DPA. Supplier will inform Conversant prior to the Processing of Conversant Personal Data -- unless prohibited by law from doing so -- if it: becomes aware of or believes that any instruction from Conversant violates Data Protection Legislation; and/or is unable to comply with Conversant's instructions for any reason.

4. Security

4.1 Supplier represents and warrants that it has implemented and shall maintain appropriate technical and organisational measures to protect the Conversant Personal Data against Security Incidents and to preserve the security and confidentiality of Conversant Personal Data. These measures shall take into account the current industry standards, state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Without prejudice to the foregoing, such measures shall include, at a minimum, those set out in **Annex B** attached hereto. Supplier may change the measures outlined in **Annex B** hereto so long as it maintains a comparable or better level of security. Material changes must be communicated to Conversant in writing at: LegalNotices@conversantgroup.com. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Conversant Personal Data.

4.2 Supplier shall ensure that any person who Processes Conversant Personal Data on Supplier's behalf: (a) is required to protect and Process Conversant Personal Data in a manner consistent with the terms of the Services Agreement and the DPA; and (b) will receive appropriate training by Supplier regarding the protection of Conversant Personal Data prior to receiving access to Conversant Personal Data.

4.3 Supplier will take reasonable steps to ensure the reliability and competence of any of its and its Subprocessors' Authorized Personnel, including regular training of those with access to Conversant Personal Data in applicable security and data privacy measures. Supplier will ensure that all such Authorized Personnel are subject to a strict legal duty of confidentiality and that they Process the Conversant Personal Data only for the purpose of delivering the Services to Conversant in accordance with this DPA.

5. Subprocessing

5.1 Supplier will not give access to or transfer any Conversant Personal Data to any third party (including any of Supplier's Affiliates, group companies or Subprocessors) without the prior written consent of Conversant. Notwithstanding the foregoing, where Supplier is a Processor, Conversant does consent to Supplier engaging a Subprocessor to Process Conversant Personal Data provided that:

(a) Supplier conducts appropriate due diligence to ensure it retains Subprocessors which present sufficient guarantees in terms of confidentiality, security and data protection in accordance with Data Protection Legislation;

(b) Supplier provides at least 30 days' prior written notice to Conversant of the engagement of any new Subprocessor (including details of the Processing and location) and Supplier shall update the list of all Subprocessors engaged to Process Conversant Personal Data under the DPA and send such updated version to Conversant prior to the engagement of the Subprocessor;

(c) Supplier must ensure the Subprocessor is a "service provider" as such term is defined under US Data Protection Law or any similar or analogous designation under Data Protection Legislation;

(d) Supplier must ensure the reliability and competence of such Subprocessor, and of its Authorized Personnel who may have access to Conversant Personal Data;

(e) Supplier imposes in its contract with such Subprocessor provisions which are at least as protective of Conversant as those in the DPA and the Services Agreement and as required by Data Protection Legislation; and

(f) Supplier is fully liable to Conversant for any breach of the DPA and the Services Agreement caused by an act, error or omission of a Subprocessor including Authorized Personnel.

5.2 If Conversant objects to the engagement of any Subprocessor on data protection grounds, then either Supplier will not engage the Subprocessor to Process Conversant Personal Data or Conversant may elect to immediately suspend or terminate the Services Agreement or the Processing of Conversant Personal Data under the Services Agreement, in each case without penalty.

6. Cooperation

6.1 Supplier will take all reasonable steps to assist Conversant in meeting Conversant's (or its Affiliates) obligations under Data Protection Legislation, including Conversant's obligations: (a) to respond to requests by Data Subjects to exercise their rights with respect to Conversant Personal Data (including its right of access, correction, objection, erasure/deletion and data portability, as applicable); (b) to adhere to data security obligations; and (c) to consult with Supervisory Authorities.

6.2 Supplier will promptly inform Conversant in writing if it receives: (a) a request from a Data Subject concerning any Conversant Personal Data; or (b) a complaint, communication, or request relating to Conversant's obligations under Data Protection Legislation. Supplier shall not respond to such communication without Conversant's express authorization, except to confirm that the request relates to Conversant. Regarding requests from Data Subjects seeking to exercise their rights, Supplier will inform Conversant in writing without undue delay (but in no case longer than five (5) business days) of receiving a request from a Data Subject concerning the Processing of Conversant Personal Data. Where the request concerns Personal Data covered under the CCPA or other US Data Protection Law, Supplier shall inform the requestor that the request cannot be acted upon because the request has been sent to a service provider, as this term is defined under US Data Protection Law, and that the request is or has been referred to Conversant.

6.3 Supplier will provide all reasonable assistance required by Conversant or its Affiliate to conduct a data protection impact assessment, risk assessment, cybersecurity audit or similar under Data Protection Legislation and/or inquiry, complaint or prior consultation with any applicable Supervisory Authorities.

6.4 If Supplier receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other governmental, regulatory or judicial authorities) seeking the disclosure of Conversant Personal Data, Supplier shall not disclose any information but shall immediately notify Conversant in writing of such request, and reasonably cooperate with Conversant if Conversant wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

6.5 Supplier shall have in place, maintain and comply with a policy governing Personal Data access requests from government authorities, which addresses the obligations herein and at minimum prohibits: massive, disproportionate or indiscriminate disclosure of Personal Data relating to Data Subjects in Europe; and disclosure of Personal Data relating to Data Subjects in Europe to a government authority without a subpoena, warrant, writ, decree, summons or other legally binding order that compels disclosure of such Personal Data.

7. Deletion or return

7.1 Supplier acting as a Processor. At the end of the Services, or upon Conversant's request, Supplier will securely destroy or return to Conversant the Conversant Personal Data in Supplier's possession or control (including any Conversant Personal Data Processed by its Subprocessors) that Supplier processes as a Processor.

7.2 The requirements above shall not apply to the extent that Supplier is required by any applicable law to retain some or all of the Conversant Personal Data, in which case Supplier shall isolate and protect the Conversant Personal Data from any further Processing except to the extent required by such law. Supplier shall delete such retained data without undue delay when technically feasible and/or allowed by the applicable law.

7.3 The obligations placed upon Supplier under this DPA shall survive so long as Supplier and/or its Subprocessors Process Conversant Personal Data.

8. Transfers

8.1 International transfers. Supplier shall be entitled to Process and transfer the Conversant Personal Data, including by using Subprocessors, in or to a territory other than the territory in which the Conversant Personal Data was first collected as permitted by and in compliance with Data Protection Legislation and this DPA.

8.2 Restricted Transfers. Supplier shall not conduct a Restricted Transfer of Conversant Personal Data unless it first takes all such measures as are necessary to ensure the Restricted Transfer is in compliance with EU/UK Data Protection Law. Such measures may include (without limitation) transferring Conversant Personal Data to a recipient that: (a) is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for personal data; (b) has achieved binding corporate rules authorization; or (c) has executed with Supplier appropriate Standard Contractual Clauses, including the adoption of supplementary measures, if required to ensure an adequate level of protection; in each case as adopted or approved in accordance with applicable EU/UK Data Protection Law.

8.3 Where Conversant transfers (directly or via onward transfer) Conversant Personal Data to Supplier, the Parties agree to be subject to the Standard Contractual Clauses, which shall be incorporated by reference as form an integral part of this DPA, as follows:

(a) Supplier as a Processor. In relation to Conversant Personal Data that is protected by the EU GDPR and is Processed in accordance with this DPA, the SCCs shall apply completed as follows: (i) Module Two (Controller-to-Processor or Module Three (Processor-to-Processor, as applicable) will apply; (ii) in Clause 7, the optional docking clause will apply, (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 6 (Subprocessing) of this DPA; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the SCCs will be governed by the law of the Netherlands; (vi) in Clause 18(b), disputes shall be resolved before the courts of the Netherlands; (vii) Annex I of the SCCs shall be deemed completed with the information set out in **Annex A** attached hereto; and (viii) subject to Section 5.1 of this DPA, Annex II of the SCCs shall be deemed completed with the information set out in **Annex B** attached hereto.

(b) UK Transfer Mechanism. For the purposes of Conversant Personal Data that is protected by UK Data Protection Law, the SCCs as implemented above will also apply with the following modifications: (i) the SCCs to be deemed amended as specified by Part 2 of the UK Addendum; (ii) tables 1 to 3 in Part 1 of the UK Addendum to be deemed completed respectively with the information set out in Annexes A, B and C attached hereto (as applicable); and (iii) table 4 in Part 1 of the UK Addendum to be deemed completed by selecting "neither party".

(c) Swiss Transfer Mechanism. For the purposes of Conversant Personal Data that is protected by the Swiss FADP, the SCCs as implemented above will also apply with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP; (ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss FADP; (iii) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law"; (iv) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland); (v) Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner; (vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland"; (vii) in Clause 17, the SCCs shall be governed by the laws of Switzerland; and (viii) Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

8.4 Supplier agrees to implement and maintain any additional contractual, technical or organisational measures to supplement the safeguards under the SCCs which are required from time to time by Conversant in order to protect the Conversant Personal Data, so long as such safeguards are consistent with requirements under Data Protection Legislation. If Supplier is unable to implement and maintain such supplementary measures, Conversant may immediately terminate the Services Agreement and the DPA (in whole or in part) without penalty. Supplier shall promptly notify Conversant if it makes a determination that it can no longer meet its obligations under this Section 9, and in such event but without prejudice to any other right or remedy available to Conversant, Supplier shall:

(a) remediate (if remediable) any Processing until such time as the Processing meets the level of protection as is required by Data Protection Legislation and this Section 9; and/or

(b) immediately cease (and require that all Subprocessors immediately cease) Processing such Conversant Personal Data if in Conversant's sole discretion, Conversant determines that Supplier has not or cannot correct any non-compliance with this Section 9 within a reasonable time frame.

8.5 It is not the intention of either Party, nor the effect of the DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail. In no event does the DPA restrict or limit the rights of any Data Subject or of any competent Supervisory Authority.

8.6 The Parties agree that, in the event that a Supervisory Authority and/or EU/UK Data Protection Law no longer allow the lawful transfer of Conversant Personal Data to Supplier and/or requires that Conversant adopt an alternative transfer solution that complies with EU/UK Data Protection Law, Supplier will fully co-operate with Conversant to enter into an amendment to this DPA to remedy such non-compliance and/or cease Processing of Conversant Personal Data. If the Parties, acting in good faith, are unable to agree such changes within thirty (30) days, Conversant may immediately terminate the Services Agreement without any further liability or obligation to Supplier, and Supplier shall refund to Conversant any amounts which were paid for work not yet performed under the Services Agreement.

9. Security Reports and Inspections

9.1 Supplier shall maintain records in accordance with ISO 27001 or similar information security management system standards. On request, Supplier shall provide copies of relevant reports, certifications or any information reasonably requested by Conversant to demonstrate compliance with the obligations set out in the DPA. Supplier shall also respond to Conversant security and compliance questionnaires and address any reasonable follow up questions.

9.2 While it is the Parties' intention ordinarily to rely on Section 10.1 above to demonstrate Supplier's compliance with the DPA (including the Standard Contractual Clauses as applicable) and Data Protection Legislation, where Conversant has reasonable concerns about Supplier's compliance, Supplier will allow Conversant or an Affiliate under the DPA and their respective auditors or authorized agents to conduct audits and inspections during the term of the Services Agreement and for 12 months thereafter. Such inspections shall include, where necessary, providing access to the premises, resources and Authorized Personnel, and provide all reasonable assistance in order to assist Conversant or an Affiliate under the DPA in exercising its audit rights under this Section 10.2. Inspections may only be carried out with reasonable prior notice, during normal business hours.

10. Security Incidents

10.1 If Supplier becomes aware of any Security Incident, it shall:

(a) without undue delay (and in any event no later than 48 hours of discovery) notify Conversant and provide Conversant with: a detailed description of the Security Incident; the type of data that was the subject of the Security Incident; the identity of each affected Data Subjects (if determinable), and the steps Supplier has taken or intends to take in order to mitigate and remediate such Security Incident, in each case as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Conversant may reasonably request relating to the Security Incident);

(b) take action immediately, at its own expense, to investigate the Security Incident and to identify, prevent and mitigate the effects of the Security Incident and, with the prior written approval of Conversant, to carry out any recovery or other action necessary to remedy the Security Incident;

(c) reimburse Conversant for reasonable costs incurred by Conversant (or an Affiliate) to draft, prepare, generate, and send, or otherwise related to, all notifications as required by Data Protection Legislation and, if requested by Conversant, provide credit monitoring and identity theft protection services to affected Data Subjects; and

(d) not release or publish any filing, communication, notice, press release, or report concerning the Security Incident without Conversant's prior written approval (except where it is required to do so by law).

11. Liability and Indemnity

11.1 Notwithstanding anything else to the contrary in the Services Agreement, Supplier agrees that:

(a) it shall be liable for any unauthorized use, exposure or loss of data (including Conversant Personal Data) arising under or in connection with the Services Agreement and the DPA to the extent such loss results from any failure of Supplier (or its Subprocessors) to comply with its obligations under the DPA and/or applicable law or regulation; and

(b) any exclusion of damages or limitation of liability that may apply to limit Supplier’s liability in the Services Agreement shall not apply to Supplier’s liability arising under or in connection with the DPA, howsoever caused, regardless of how such amounts or sanctions awarded are characterized and regardless of the theory of liability, which liability shall be expressly excluded from any agreed exclusion of damages or limitation of liability.

11.2 To the fullest extent permitted by applicable law, Supplier shall indemnify, defend, and hold Conversant, including its Affiliates, and each of its affiliates, partners, principals, officers, directors, employees, subcontractors and agents harmless against any claims, suits, or proceedings and any resulting liabilities, fines, losses, damages, costs and expenses (including reasonable attorney's fees) that Conversant may suffer or incur as a result of any act or omission on the part of Supplier or its subcontractors, or anyone acting on their behalf, that leads to Conversant being liable for breach of Data Protection Legislation or a third-party contract.

11.3 In the event there is any act, error or omission on the part of Supplier and/or its Subprocessors which leads to Conversant being liable for breach of Data Protection Legislation or any third-party contract, then Supplier shall indemnify Conversant for any damages, losses, liabilities, costs, harm or expenses (including reasonable legal fees) suffered by Conversant as a result.

11.4 The Parties acknowledge and agree that any breach by Supplier of the DPA shall constitute a material breach of the Services Agreement, in which event and without prejudice to any other right or remedy available to it, Conversant may elect to immediately terminate the Services Agreement in accordance with the termination provisions in the Services Agreement.

11.5 Nothing in the DPA is intended to limit any Data Subject rights, as third-party beneficiaries, under the Standard Contractual Clauses against any Party arising out of such Party's breach of the Standard Contractual Clauses, where applicable.

12. Documentation and Records of Processing

12.1 Each Party is responsible for its compliance with its documentation requirements, in particular maintaining records of Processing, where required under Data Protection Legislation. Each Party shall reasonably assist the other Party in its documentation requirements, including providing the information the other Party needs from it in a manner reasonably requested by the other Party (such as using an electronic system) in order to enable the other Party to comply with any obligations relating to maintaining records of Processing.

13. General

13.1 The DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Services Agreement, unless and to the extent required otherwise by the Data Protection Legislation or, where applicable, the Standard Contractual Clauses.

13.2 If Supplier accesses, retains, is exposed to, or becomes aware of “Protected Health Information” as defined in 45 C.F.R. § 164.501 in the course of providing service, Supplier and Conversant hereby agree to and Supplier shall comply with the HIPAA US Subcontractor Agreement and the HIPAA Business Associate Agreement, attached as Annex C.

13.3 The Parties acknowledge and agree that the DPA is incorporated into and forms a part of the Services Agreement between Conversant and Supplier. For matters not addressed under the DPA, the terms of the Services Agreement apply. If and to the extent the DPA conflicts with any provision of the Services

Agreement, the DPA shall control and prevail. Conflicts between the terms of the DPA and the Standard Contractual Clauses are addressed in Section 9.5 above, as further subject to Section 9.6 above.

13.4 The Parties acknowledge that either Party may disclose this DPA (and any other relevant privacy terms or agreements entered between the Parties) to the US Department of Commerce, the Federal Trade Commission, European data protection authorities or any other US, EU, Swiss or UK judicial or regulatory body upon their request.

13.5 The Parties acknowledge and agree that any breach by Supplier of the DPA shall constitute a material breach of the Services Agreement, in which event and without prejudice to any other right or remedy available to it, Conversant may elect to immediately terminate the Services Agreement (in whole or in part) in accordance with the termination provisions in the Services Agreement.

Annex A
Description of the Processing Activities / Transfer

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: The Conversant entity executing the Services Agreement and the DPA	**Name:** Supplier as this term is defined in the DPA and/or Services Agreement
Address: As identified in the Services Agreement	**Address:** As identified in the Services Agreement
Contact Person's Name, position and contact details: privacy@Conversant	**Contact Person's Name, position and contact details:** As provided for in the Services Agreement or otherwise Supplier's publicly-available email address for receiving privacy-related notices.
Activities relevant to the transfer: See **Annex 1(B)** below	**Activities relevant to the transfer:** See **Annex 1(B)** below
Role: Controller or Processor	**Role:** Processor

Annex 1(B) Description of transfer:

	Description
Categories of data subjects:	As needed in order for Supplier to perform the Services, which may include: ● Employees and applicants ● Customers and end users ● Suppliers, agents, and contractors
Categories of personal data:	As needed in order for Supplier to perform the Services, which may include: ● Direct identifiers such as first and last name, date of birth, & home address; ● Communications data such as home telephone number, cell telephone number, email address, postal mail, and fax number; ● Family and other personal circumstance information such as age, date of birth, marital status, spouse or partner, and number and names of children; ● Employment information such as employer, work address, work email and phone, job title and function, salary, manager, employment ID, system usernames and passwords, performance information, and CV data; ● Other data such as financial, goods or services purchased, device identifiers, online profiles, and IP address; ● Details of user's interaction with the data importer's systems and with systems for which the data importer provides computing services; ● Information that the data exporter or its users choose to include in files stored on or routed through data importer's applications; and ● Other personal data to which the parties provide to each other in connection with the provision of the Services.
Sensitive data transferred (if applicable) and applied restrictions:	Personal data transferred may include sensitive data such as government identifier, or any other sensitive data necessary to be processed in order to perform the Services.
Frequency of the transfer:	Continuous
Nature of the Processing:	The performance of Services under the Services Agreement and the DPA.
Duration of the Processing:	The term of the Services Agreement and any period after the termination or expiry of the Services Agreement during which Supplier Processes Conversant Personal Data, until Supplier has deleted, destroyed or returned such Personal Data in accordance with the terms of the DPA (the "**Processing Term**").
Purpose(s) of the data transfer and further Processing:	The Permitted Purpose (as defined in the DPA).
Retention period (or, if not possible to determine, the criteria used to determine that period):	The Processing Term.

For transfers to Subprocessors, also specify subject matter, nature and duration of the Processing:	The nature is the provision of the Services as described in the Services Agreement. The subject matter is the personal data as described above. The duration will be in accordance with Section 9 of the DPA.

Annex 1(C) Competent supervisory authority:
The competent supervisory authority, in accordance with Clause 13 of the SCCs, shall be determined in accordance with EU/UK Data Protection Law.

Annex B
Technical and organizational measures

Supplier shall implement the following minimum technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security taking into account the nature, scope, context and purposes of the processing, and the risks for the rights and freedoms of natural persons:

Type of Measure	Implemented Measure
1. Measures of encryption of personal data	● Encryption of the Conversant Personal Data while at rest and in transit consistent with industry standards and at a minimum of 256-bit encryption.
2. Measures for ensuring ongoing confidentiality, integrity and resilience of processing systems and services	● Confidentiality Obligations. Ensure employees are required to sign a confidentiality agreement when accepting a new hire offer and contractors who access the facilities and/or data required to sign a confidentiality or non-disclosure agreement. ● Training. Implement and maintain security and privacy awareness training for all employees and contractors regarding the handling and securing of confidential information and Conversant Personal Data consistent with applicable law (including Data Protection Legislation). ● Background Checks. Supplier shall conduct a criminal background check on each of all employees and contractors with access to Conversant Personal Data. Supplier shall not provide access to Conversant Personal Data to any employee or contractor who: (a) has any felony convictions or misdemeanour convictions involving violence or dishonesty, or its international equivalents; (b) has a restriction (e.g. a court order or restrictive covenant) that would prevent the person from providing services or impose limitations on the services that the person is able to provide to Conversant or a customer of Conversant; (c) may present a higher than normal security risk to Conversant or a customer of Conversant; or (d) do not meet other guidelines specified by Conversant or the customers of Conversant from time to time. ● Remote access to systems must utilize secure applications, i.e., VPN. Access to remote resources must be authenticated using multiple authentication factors (MFA). ● Identify appropriately defined organizational roles for security and incident response. ● Include appropriate controls addressing (A) critical asset identification and asset management; (B) access controls and management; (C) physical and environmental security; (D) communications and operations security and management; (E) systems acquisition, development, and maintenance; (F) third-party risk management; (G) configuration and change management for software systems; (H) incident response, planning, and management, including appropriate maintenance, monitoring and analysis of audit logs; and (I) business continuity management, disaster recovery, and contingency planning/redundancy. ● Segregation of the Conversant Personal Data from all other third-party data. ● Proper user authentication for all employees and contractors with access to the Conversant Personal Data, including, without limitation, by assigning each employee/contractor unique access credentials for access to any system on which the Conversant Personal Data can be accessed and prohibiting

	employees/contractors from sharing such access credentials. ● Restrict and track access to the Conversant Personal Data by only those employees/contractors whose access is necessary to performing the services and implement and maintain logging and monitoring technology to help detect and prevent unauthorized access attempts to networks and production systems. ● Conduct periodic reviews of changes affecting systems' handling authentication, authorization, and auditing, and privileged access to production systems. ● Upon termination of any employee/contractor, ensure the terminated employee/contractor's access to any Conversant Personal Data on Supplier's systems will be immediately revoked. ● If Supplier or any authorized person is granted access to or connects to any computing system, network, platform, facilities or telecommunications or other information system (the "Systems") owned, controlled, or operated by or on behalf of Conversant or any of its Affiliates, then Supplier and any applicable authorized person will be subject to and shall comply with all then-current Conversant policies, including without limitation, all security, privacy, safety, environmental, information technology, legal and business conduct policies. Any such access or connection to the Systems is strictly for the purpose of Supplier's performance of the Services under and in accordance with the Agreement. Supplier agrees that Conversant may perform periodic network assessments and should any such assessment reveal inadequate security by Supplier, Conversant, in addition to other remedies it may have, may suspend Supplier's access to the Systems until such security issue has been eliminated.
3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	● Business Continuity Plan. Maintain internal practices, plans or procedures that are designed to reasonably ensure Supplier's products and services are uninterrupted during the term of the Agreement. ● Maintain: (i) daily backups (including backup encryption) of production file systems and databases; and (ii) a formal disaster recovery plan for the production data center and conduct regular testing on the effectiveness of such plan.
4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	● Section 5 of the DPA. ● Regularly conduct internal security audits and contract annually for external security assessments and penetration tests of Supplier systems including, without limitation, cloud architecture, business processes and procedures, access controls and encryption measures. ● Implement and maintain a risk assessment program to help identify foreseeable internal and external risks to Supplier's information resources and determine if existing controls, policies, and procedures are adequate.
5. Measures for user identification and authorisation	● Proper user authentication for all employees and contractors with access to the Conversant Personal Data, including, without limitation, by assigning each employee/contractor unique access credentials for access to any system on which the Conversant Personal Data can be accessed and prohibiting employees/contractors from sharing such access credentials. ● Restrict and track access to the Conversant Personal Data to only those employees/contractors whose access is necessary to performing the services and implement and maintain logging and monitoring technology to help detect and prevent unauthorized access attempts to networks and production systems. ● Conduct periodic reviews of changes affecting systems' handling authentication, authorization, and auditing; and privileged access to production systems.
6. Measures for protection of	● Encryption at rest. See Section 1 above. ● Multifactor authentication enabled for user access to production environment.

Data during storage	● Not store the Conversant Personal Data on any personal device (e.g., a home computer) or removable storage devices.
7. Measures for ensuring physical security of locations at which personal data are processed	● Establish limits on physical access to information systems and facilities using physical controls (e.g., coded badge access) that provide reasonable assurance that access to data centers is limited to authorized individuals. ● Install camera or video surveillance systems at all external and at critical internal entry points. ● All access logs and cameras shall be monitored 24x7. Alerts to unauthorized access or activities are responded to immediately by a designated incident response team. Record retention shall be maintained for 6 months if permitted under applicable law.
8. Measures for ensuring events logging	● All activities impacting the Conversant Personal Data, the management of this data, and changes to access shall be logged and reviewed on a regular schedule for unauthorized access or activities. These logs shall be securely stored and processed by a security event and incident management system, which shall be configured to alert for suspicious or unauthorized activities 24x7. A designated team shall be responsible to manage and monitor these systems and logs.
9. Measures for ensuring system configuration, including default config	● Implement and maintain policies and procedures for managing changes to production systems, applications and databases, including without limitation, processes for documenting testing and approval of changes into production, security patching, and authentication.
10. Measures for internal IT and IT security governance and management	● Maintain and implement security policies and procedures designed to ensure employees and contractors process the Conversant Personal Data in accordance with the Standard Contractual Clauses, this DPA and Data Protection Legislation. ● Implement and enforce disciplinary measures against employees and contractors for failure to abide by its security policies and procedures.
11. Measures for certification/assurance of processes and products	● Certifications. See Section 4 above. ● All information security roles and responsibilities are defined and allocated. Minimization of opportunities for unauthorized or unintentional modification or misuse of assets and data.
12. Measures for ensuring data minimization and accountability	● Section 3 of the DPA. ● Detailed privacy assessments are performed related to implementation of new products/services and processing of personal data by Supplier and third parties. ● Security measures are in place to provide only the minimum amount of access necessary to perform required functions. ● Data retention time limits restricted.
13. Measures for ensuring data quality	● Exercise of rights. See Section 7 of the DPA. ● Secure development environment. Development environments are protected from malicious or accidental development and update of code that may create vulnerabilities or compromise confidentiality, integrity, and availability of the platform.
14. Measures for ensuring limited data retention	● Section 8 and Annex A of the DPA.
15. Measures for allowing data portability and ensuring erasure	● Sections 7 and 8 of the DPA.

Annex C: HIPAA

US HIPAA BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

Conversant and/or its Affiliates ("Conversant" or "Business Associate") and Supplier, its parent company and its worldwide direct and indirect subsidiaries ("Subcontractor") entered into an agreement pursuant to which Conversant purchases services or products from Supplier and Supplier performs services on Conversant's behalf ("Supplier

Agreement"). This HIPAA Business Associate Subcontractor Agreement ("HIPAA Agreement") is attached to and made a part of the Data Protection Agreement ("DPA") between Conversant and Subcontractor.

1. STATEMENT OF PURPOSE. CONVERSANT IS A BUSINESS ASSOCIATE AS DEFINED BY THE PRIVACY AND SECURITY RULES OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA") AND HAS BEEN ENGAGED TO PROVIDE CERTAIN SERVICES TO ITS CUSTOMERS OR ITS PERSONNEL. IN CONNECTION WITH THESE ENGAGEMENTS, CONVERSANT HAS ENTERED INTO BUSINESS ASSOCIATE AGREEMENTS WITH CERTAIN OF ITS CUSTOMERS OR PERSONNEL AS REQUIRED BY HIPAA. CONVERSANT IS NOW ENTERING INTO THIS HIPAA AGREEMENT WITH SUBCONTRACTOR IN CONNECTION WITH CONVERSANT SUBCONTRACTING ALL OR A PART OF THE PERFORMANCE OF SUCH SERVICES TO SUBCONTRACTOR PURSUANT TO THE SUPPLIER AGREEMENT(S). THE PARTIES ACKNOWLEDGE THAT SUBCONTRACTOR MAY BE RESPONSIBLE FOR FACILITIES OR SYSTEMS THAT HOUSE OR CONTAIN PHI (AS DEFINED BELOW), AND/OR MAY BE EXPOSED TO, CREATE, RECEIVE, MAINTAIN, TRANSMIT OR BECOME AWARE OF PHI IN THE PERFORMANCE OF THE SERVICES UNDER THE SUPPLIER AGREEMENT(S) BETWEEN CONVERSANT AND SUBCONTRACTOR. THIS HIPAA AGREEMENT CONSTITUTES THE WRITTEN ASSURANCES REQUIRED BY THE HIPAA RULES IN CONNECTION WITH SUBCONTRACTOR'S ACTIVITIES UNDER THIS HIPAA AGREEMENT AND THE SUPPLIER AGREEMENT(S).

2. ORDER OF PRECEDENCE. In the event that a provision of this HIPAA Agreement is contrary to a provision of a Supplier Agreement, then in connection with any PHI, the provision of this HIPAA Agreement shall control. Any ambiguity in the terms of this HIPAA Agreement will be resolved to permit Conversant and Conversant's Customers to comply with HIPAA. Nothing in this HIPAA Agreement shall change or modify any terms of the Supplier Agreement(s) that prohibit Subcontractor from retaining subcontractors or agents to assist in the performance of Services for Conversant.

3. DEFINITIONS. Capitalized terms not specifically defined in this HIPAA Agreement have the meanings set forth in the DPA, the NDA, or the applicable Supplier Agreement.

3.1. "Breach" has the meaning set forth in 45 C.F.R. § 164.402.

3.2. "Covered Entity" has the meaning set forth in 45 C.F.R. § 160.103.

3.3. "Customers" means customers of Conversant who are Covered Entities under HIPAA.

3.4. "Data Aggregation" has the meaning set forth in 45 C.F.R. § 164.501.

3.5. "Designated Record Set" has the meaning set forth in 45 C.F.R. Section 164.501.

3.6. "Discovery" means "discovery" as such term is described in 45 C.F.R. § 164.410(a)(2).

3.7. "ePHI" means "Electronic Protected Health Information" as defined in 45 C.F.R. § 160.103 that is created, received, maintained or transmitted by Subcontractor from or on behalf of Conversant or Conversant's Customers or personnel under the Supplier Agreement(s).

3.8. "HIPAA Breach Notification Rule" means the Notification in the Case of Breach of Unsecured PHI, as set forth at 45 C.F.R. Part 164 Subpart D.

3.9. "HIPAA Privacy Rule" means the standards, requirements and specifications promulgated by at 45 C.F.R. Section 160 subparts A and E promulgated under HIPAA.

3.10."HIPAA Security Rule" means the standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Section 164 subpart C promulgated under HIPAA.

3.11."HIPAA Rules" means the HIPAA Privacy Rule, the HIPAA Security Rules, the Breach Notification Rule, as the same may, from time to time, be amended.

3.12."Individual" has the meaning set forth in 45 C.F.R. § 160.103.

3.13."PHI" means "Protected Health Information" as defined in 45 C.F.R. § 164.501 that is created, received, maintained or transmitted by Subcontractor from or on behalf of Conversant or Conversant's Customers or personnel under the Supplier Agreement(s).

3.14."Required by Law" has the meaning set forth in 45 C.F.R. § 164.103.

3.15.”Secretary” has the meaning set forth in 45 C.F.R. § 160.103.

3.16.“Security Incident” has the meaning set forth in 45 C.F.R. § 164.304.

3.17.”Sell” or “Sale” means a disclosure of PHI by Subcontractor where Subcontractor directly or indirectly receives remuneration from or on behalf of the recipient of such PHI in exchange for such PHI, but does not include any disclosure of PHI described in 45 C.F.R. § 164.502(a)(5)(ii)(B)(2).

3.18.”Unsecured PHI” shall have the meaning set forth in 45 C.F.R. § 164.402.

4. OBLIGATIONS OF SUBCONTRACTOR. Subcontractor agrees:

4.1. not to use or further disclose PHI other than as required to carry out its obligations to Conversant under the Supplier Agreement(s) and as expressly permitted or required by this HIPAA Agreement or as Required by Law. Such use, disclosure or request of PHI shall utilize a limited data set if practicable or otherwise the minimum necessary PHI to accomplish the intended purpose of the use, disclosure or request;

4.2. to use reasonable and appropriate safeguards to prevent the use or disclosure of PHI in any manner other than as permitted by this HIPAA Agreement, consistent with the applicable principles and obligations set out in the HIPAA Rules;

4.3. to report to Conversant in writing any use or disclosure of PHI not provided for by this HIPAA Agreement of which it becomes aware within 48 hours of becoming aware of such use or disclosure. In addition, Subcontractor will report to Conversant in writing, within 48 hours following Discovery, any acquisition, access, use, or disclosure of Unsecured PHI, unless such event is excluded from the definition of Breach in 45 C.F.R. § 164.402(1). Any such report shall include the identification (if known) of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed, all other information required by 45 C.F.R. § 164.410€, and any other information reasonably requested by Conversant or the applicable Customer. Upon receipt of such report, Conversant will then conduct, or have Subcontractor conduct at Conversant’s direction, a risk assessment to determine whether such acquisition, access, use, or disclosure compromised the security or privacy of such Unsecured PHI based on the factors specified in the definition of Breach in 45 C.F.R. § 164.402(2). If Subcontractor believes, based on such risk assessment, that any such acquisition, access, use, or disclosure results in a low probability that the Unsecured PHI has been compromised, it shall provide to Conversant all information supporting such conclusion;

4.4. to ensure, in accordance with 164.502(e)(1)(ii) and 164.504(e)(2)(ii)(D), that any agents or subcontractors who create, receive, maintain or transmit PHI agree to provide reasonable assurances, evidenced by written contract, that such agents or subcontractors will comply with substantially the same restrictions and conditions that apply to Subcontractor with respect to such information;

4.5. to the extent (if any) that Subcontractor maintains a Designated Record Set, to make available PHI maintained by Subcontractor in a Designated Record Set to Conversant as required for Conversant’s Customers to comply with their obligation to give an Individual the right of access to inspect and obtain a copy of their PHI as set forth in 45 C.F.R. § 164.524. If specifically requested by Conversant or the applicable Customer, Subcontractor will either (a) transmit copies of the PHI in an electronic format directly to a person the Individual designates., or (b) make copies of the PHI in a paper form and provide such copies directly to a person the Individual designates.

4.6. to the extent (if any) that Subcontractor maintains a Designated Record Set, to make available PHI maintained by Subcontractor in a Designated Record Set to Conversant as required for Conversant or its Customers to comply with their obligation to amend PHI as set forth in 45 CFR 164.526;

4.7. to make available to Conversant information regarding disclosures of PHI by Subcontractor for which an accounting is required under 45 C.F.R. Section 164.528 so Conversant or its Customers can meet their requirements to provide an accounting of disclosures to Individuals in accordance with 45 CFR 164.528;

4.8. to make its internal practices, books and records relating to its compliance with its obligations under this HIPAA Agreement and the use and disclosure of PHI by Subcontractor available to the Secretary for purposes of determining Conversant or Conversant’s Customers’ compliance with the HIPAA Rules, and to provide any such materials to Conversant or Conversant’s Customer upon request;

4.9. in accordance with 45 C.F.R. § 164.502(a)(4)(i), to disclose PHI when required by the Secretary under subpart C of part 160 of HIPAA;

4.10. at termination of this HIPAA Agreement for any reason, return or destroy all PHI that Subcontractor still maintains in any form and to retain no copies of such information, or, if such return or destruction is not feasible, Subcontractor shall (i) provide Conversant with notification of the conditions that make return or destruction infeasible, (ii) extend the protections of this HIPAA Agreement to the PHI, and (iii) limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. If Supplier proceeds with destruction of such PHI, certify to Conversant in writing that such destruction has occurred;

4.11. With respect to ePHI, to: (a) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI, as required by the Security Rule, including the applicable administrative, physical and technical safeguards described in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314 and 45 C.F.R. § 164.316 with respect to ePHI to prevent the use or disclosure of ePHI other than as provided in this HIPAA Agreement; provided, however, Subcontractor shall encrypt ePHI in transit and at rest in accordance with Section 3(f) of the DPA. (b) ensure, in accordance with 45 C.F.R. §§ 164.504(e)(2)(ii)(D), 164.308(b)(2) and (3) and 164.314(a)(2)(iii), that any agent, including a subcontractor, who create, receive, maintain or transmit ePHI agrees, evidenced by written contract, to implement reasonable and appropriate safeguards to protect such ePHI consistent with the requirements described in clause (i) of this Section 3(j); and (c) report to Conversant any Security Incident affecting ePHI of which it becomes aware; 4.12. not to Sell PHI; –

4.13. mitigate, to the extent practicable, any harmful effect that is known to Subcontractor of a use or disclosure of PHI by Subcontractor in violation of this HIPAA Agreement;

4.14. not to perform Data Aggregation activities nor de-identify PHI unless specifically requested in writing by Conversant;

4.15. to reimburse Conversant for the costs it incurs in responding to (including providing notifications and credit monitoring services), remediating, and/or mitigating damages caused by a Breach of Unsecured PHI or a Security Incident caused by Subcontractor's failure to perform its obligations under this HIPAA Agreement, the DPA, the NDA, or the Supplier Agreement or a use of disclosure of PHI by Subcontractor not provided for by this HIPAA Agreement, and the costs Conversant incurs in following up a complaint by an Individual or a regulator related to the foregoing; and

4.16. to comply with any (i) modifications to, restrictions on, defects in, or revocation or other termination of the effectiveness of, any consent, authorization or permission relating to the use or disclosure of PHI; and (ii) agreement that Conversant or the applicable Customer makes or limitations in the applicable privacy practices that either (A) restricts the use or disclosure of PHI pursuant to 45 C.F.R. § 164.522(a) or 45 C.F.R. § 164.520, or (B) requires confidential communication about PHI pursuant to 45 C.F.R. § 164.522(b), in each case under clause (i) or (ii), to the extent any such modification, defect, revocation, termination, restriction, confidential communication obligations or limitations affect Subcontractor's permitted or required uses and disclosures of PHI specified in this HIPAA Agreement (collectively, "Restrictions"), provided that Conversant or the applicable Customer notifies Subcontractor in the Restrictions that Subcontractor must follow.

5. TERM AND TERMINATION. With respect to each Supplier Agreement, the term of this HIPAA Agreement shall be the same as the term of such Supplier Agreement. In the event Conversant determines that Subcontractor may have breached a material term of this HIPAA Agreement, or if Subcontractor's has knowledge of such breach, which Subcontractor shall promptly disclose to Conversant, Conversant may in Conversant's discretion, provide an opportunity for Subcontractor to cure the breach or end the violation within thirty (30) business days of such notification. If Subcontractor fails to cure the breach or end the violation within such time period to the satisfaction of Conversant, or Conversant concludes that it is no longer in Conversant's interests to proceed to use Subcontractor's services, Conversant shall have the right to immediately terminate this HIPAA Agreement and the Agreement(s) that are the subject of such breach upon written notice to Subcontractor. As authorized by law, Subcontractor hereby acknowledges that Conversant shall have the right to report the breach to the Secretary.

6. SUBCONTRACTORS. Subcontractor acknowledges that to the extent required by HIPAA (e.g., 45 C.F.R. §§ 160.102(b), 160.300, 164.104(b), 164.302, and 164.500(c)) the standards and requirements of the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule apply to Subcontractor.

7. INDEMNIFICATION. Subcontractor shall indemnify and defend Conversant and Conversant's directors, officers, employees, representatives, and agents from and against any and all claims, actions, demands, and legal proceedings and all liabilities, damages, losses, judgments, authorized settlements, costs, fines, penalties and expenses including reasonable attorneys' fees arising out of or in connection with, resulting from or relating to the acts or omissions of Subcontractor in connection with a breach of the representations, duties and obligations of Subcontractor under this HIPAA Agreement or Subcontractor's violation of the HIPAA Rules.

BUSINESS ASSOCIATE AGREEMENT

Conversant Group, LLC and/or its Affiliates, acting as Plan Sponsor ("Plan Sponsor") of the Conversant Inc. Comprehensive Welfare Benefits Plan ("Plan") has engaged Supplier to provide certain professional, consulting or other services to the Plan (the "Services") pursuant to an agreement (the "Supplier Agreement"). This Business Associate Agreement ("BAA") is attached to and made a part of the Data Protection Agreement ("DPA") between Conversant and Supplier.

1. STATEMENT OF PURPOSE. Because Supplier may access, retain, be exposed to, or become aware of confidential health information in the performance of the Services, the parties agree to protect the confidentiality of such information in accordance with federal and state laws and regulations including, but not limited to, information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health information Technology for Economic and Clinical Health Act ("HITECH Act"), and the regulations promulgated thereto ("HIPAA Regulations"), including, as amended from time to time, (a) the standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Part 164 subparts A and E ("Privacy Rule"); (b) the security standards published on February 20, 2003 at Fed. Reg. 8334 et. seq. (45 C.F.R. Parts 160, 162 and 164) ("HIPAA Security Rule"); and (c) the breach notification standards, requirements, and specifications enacted by Subtitle D of the HITECH Act and its implementing regulations promulgated by the Secretary at 45 C.F.R. Part 164 Subpart D as part of the final omnibus rule ("Omnibus Rule") (collectively, "Breach Notification Rule"); and (d) the enforcement standards, requirements and specifications promulgated by the Secretary at 45 C.F.R. Part 160 subparts C, D, and E ("Enforcement Rule").

2. DEFINITIONS. Capitalized terms not specifically defined in this BAA have the meanings set forth in the DPA, the applicable Supplier Agreement or the HIPAA Regulations.

2.1. "**Breach**" means the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI, as defined and subject to the exceptions set forth in 45 C.F.R. § 164.402.

2.2. "**Discovery**" in relation to the discovery of a Breach, has the meaning set forth in the HITECH Act or other applicable law, including 45 C.F.R. § 164.410(a)(2).

2.3. "**ePHI**" means "Electronic Protected Health Information" as defined in the HIPAA Security Rule that is created, received, maintained or transmitted by or on behalf of Plan.

2.4. "**HIPAA Security Rule**" means the Security Standards published at 45 C.F.R. Parts 160, 162 and 164 and as may be amended from time to time.

2.5. "**HITECH Act**" means the Privacy Provisions of the Health Information Technology for Economic and Clinical Health Act, Sections 13400 et seq. enacted on February 17, 2009 and the implementing regulations including, but not limited to, the "Breach Notification for Unsecured Protected Health Information" regulations published on August 24, 2009 at 74 Fed. Reg. 42740 et seq. and as may be amended from time to time.

2.6. "**Individual**" has the same meaning as the term "individual" in 45 C.F.R. § 160.103 and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502 (g).

2.7. "**Law**" means all applicable Federal and State Statutes and all relevant regulations thereunder.

2.8. "**PHI**" has the same meaning as the term "Protected Health Information" in 45 C.F.R. § 160.103, limited to the information created, received, maintained, or transmitted by Supplier from or on behalf of Plan.

2.9. "**Secretary**" means the Secretary of the Department of Health and Human Services, or his designee.

2.10."**Subcontractor**" means a person or entity to whom Supplier delegates a function, activity, or service other than in the capacity of a member of the workforce of Supplier.

3. CONFIDENTIALITY. Supplier recognizes the sensitive and confidential nature of the PHI and agrees (a) that such PHI will be used or disclosed, including the uses and disclosures inherent in the performance of the Services, solely as required or permitted under this BAA and in accordance with Law or as required by Law; and (b) that Supplier shall use reasonable safeguards designed to ensure that the transmission, handling, storage, and use of such PHI by Supplier will preserve the confidentiality of the PHI, in accordance with Law including the HIPAA Regulations.

4. RESPONSIBILITIES OF SUPPLIER

4.1. Records. Supplier will maintain accurate records of all transactions made in connection with this BAA. Supplier acknowledges and agrees to comply with its obligations as a Business Associate under the HIPAA Regulations and all other relevant Law.

4.2. Accounting. The Plan acknowledges its obligation as a Covered Entity (as defined in 45 C.F.R. 160.103) under the Privacy Rule to provide an accounting of disclosures to an Individual in accordance with 45 C.F.R. 164.528. Pursuant to this BAA and only with respect to PHI, Supplier agrees to (i) document and make available to Plan upon request all disclosures of PHI that are subject to an accounting under the Privacy Rule and the HITECH Act, (ii) receive and process requests for accountings from Individuals, (iii) provide accountings to Individuals, and (iv) suspend provision of an accounting, when applicable. Supplier will maintain information necessary to provide an accounting for a period of six (6) years from the date of disclosure, unless otherwise required under the HITECH Act and the HIPAA Regulations.

4.3. Disclosure. Supplier agrees to report to Plan within a reasonable time following Discovery of any use or disclosure of information it knows or should know is not permitted in this BAA. To the extent applicable, Supplier shall follow the disclosure requirements found in section 5 of this BAA relating to Breaches of Unsecured PHI.

4.4. Subcontractors. Supplier shall ensure that any agents, including any Subcontractors, who will create, receive, maintain, or transmit any PHI on behalf of Supplier agree in writing to the same restrictions, conditions, and requirements relating to the use or disclosure of PHI as required by this BAA and shall not, in any manner that violates the Privacy Rule or any other applicable provision of law, use or disclose PHI except as set forth in this BAA. Supplier further agrees to ensure that any such agent, including a Subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect such information in accordance with section 4.20of this BAA. In the event that Supplier discovers a pattern of activity or practice of its Subcontractor that constitutes a material breach or violation of the Subcontractor's obligation under its Supplier Agreement, in accordance with 45 C.F.R. § 164.504(e)(1)(iii) and the Omnibus Rule, Supplier must take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, terminate the agreement with the Subcontractor, if feasible.

4.5. Limitations. Supplier agrees to limit any request, use and disclosure of PHI, to the extent practicable, to the Limited Data Set or, if needed, to the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure in compliance with the HITECH Act and any regulations or guidance promulgated pursuant thereto. The parties acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the Privacy Rule, HITECH Act and any guidance issued by the Secretary.

4.6. Amendments. The Plan acknowledges its obligation as a Covered Entity under the Privacy Rule to amend an Individual's PHI in accordance with 45 C.F.R. 164.526. Pursuant to this BAA and with respect to Protected Health Information, Supplier agrees to comply with 45 C.F.R. § 164.526, including but not limited to, granting or denying requests for amendment and making amendments to Protected Health Information, when applicable.

4.7. Subpart E Compliance. To the extent the Supplier is to carry out one or more of Plan's obligations under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to Plan in the performance of such obligations.

4.8. Practices and Records. Supplier agrees to make its internal practices, books and records relating to the use and disclosure of Protected Health Information, including policies and procedures relating to Protected Health Information, received from, or created or received by Supplier on behalf of Plan available to Plan and the Secretary for the sole purpose of determining compliance with the HIPAA Regulations.

4.9. Confidentiality. Supplier and Plan agree that all confidentiality provisions in this BAA shall survive termination of this BAA.

4.10. Data Aggregation. Supplier may provide data aggregation services relating to health care operations of Plan.

4.11.PHI Use. Supplier is not prohibited by this BAA from utilizing PHI for its proper management and administration or to carry out its legal responsibilities, if any. Further, Supplier is not prohibited from disclosing PHI for its proper management and administration or to carry out its legal responsibilities if the disclosure is required by Law or Supplier obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by Law or for the purpose for which it was disclosed to the person. Supplier will further require that the person to whom information is disclosed inform the Supplier of any breach of confidentiality or violation of the HIPAA Regulations with respect to that information. In such event, Supplier will notify Plan of any instances of which it is aware in which the confidentiality of the information has been breached or the Privacy Rule was otherwise violated.

4.12. Reporting. Supplier is not prohibited from using PHI to report violations of law to appropriate Federal and State authorities consistent with the Privacy Rule.

4.13. Access. The Plan acknowledges its obligation as a Covered Entity under the Privacy Rule to provide an Individual with access to that Individual's PHI in accordance with 45 C.F.R. 164.524. Pursuant to this BAA and with respect to Protected Health Information, Supplier agrees to grant or deny requests for access, provide review of denials of access, when required under 45 C.F.R. § 164.524, and provide access to Individuals. In the event Supplier uses or maintains an Electronic Health Record with respect to PHI of an Individual, Supplier shall upon request provide an electronic copy of the PHI either to the Individual or directly to a third party designated by the Individual in accordance with the compliance date as provided in the HITECH Act and any guidance issued thereunder.

4.14. Mitigation. Supplier agrees to mitigate, to the extent practicable, any harmful effect that is known to Supplier resulting from a use or disclosure of PHI by Supplier, or its Subcontractor, in violation of the requirements of this BAA or Applicable Law.

4.15. Plan Availability. Supplier agrees to, within three (3) business days of receiving a request, make available to Plan or, at Plan's request, to Plan Sponsor, PHI that is relevant for Plan to carry out health plan functions under 45 C.F.R. § 164.504(f), provided the disclosures are subject to, and consistent with, the terms of the Supplier Agreement.

4.16. Authorizations. With respect to PHI that Supplier creates, receives, maintains, or transmits on behalf of Plan, Supplier will be responsible for obtaining from an Individual any necessary authorizations to use or disclose that Individual's Protected Health Information, in accordance with 45 C.F.R. § 164.506 or 164.508; provided, however, that Plan Sponsor shall obtain any consent or authorization that may be required under applicable federal or state laws and regulations prior to Plan Sponsor's receipt of Private Health Information from Supplier. Supplier acknowledges that failure to obtain an authorization when necessary prior to disclosure constitutes a violation of this BAA and must be reported to Plan under section 4.3 of this BAA.

4.17. Restriction Requests. With respect to PHI that Supplier creates, receives, maintains, or transmits on behalf of Plan, Supplier will be responsible for receiving requests for restrictions from an Individual in accordance with 45 C.F.R. § 164.522 and for denying or agreeing to abide by any such requests. If Supplier agrees to a restriction, Supplier will be Conversant Confidential Data Protection Agreement Rev. 03312022 Internal Use - Confidential responsible for using and disclosing PHI consistent with that restriction. Failure to act in accordance with an agreedto restriction constitutes a violation of this BAA and must be reported to Plan in accordance with section 4.3 of this BAA. If a request for restriction is made directly to Plan, Plan will refer such request to Supplier for disposition in accordance with this subsection.

4.18. Confidential Communications. With respect to PHI that Supplier creates, receives, maintains, or transmits on behalf of Plan, Supplier will be responsible for receiving and acting upon requests for confidential communications from an Individual in accordance with 45 C.F.R. § 164.522. If Supplier agrees to accommodate a request for confidential communications, Supplier will be responsible for adhering to that accommodation. Failure to act in accordance with an accommodation that has been granted constitutes a violation of this BAA and must be reported to Plan in accordance with section 4.3 of this BAA. If a request for confidential communications is made directly to Plan, Plan will refer Individual to Supplier via customer service.

4.19. De-Identify. Supplier may de-identify any and all PHI provided that Supplier shall de-identify the information in accordance with HIPAA. De-identified information does not constitute Protected Health Information, and may be used by Supplier or an affiliated entity for creating comparative databases, statistical analysis, or other studies.

4.20. Safeguards. Without limiting other provisions of this BAA, Supplier agrees to (i) implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of EPHI that it creates, receives, maintains or transmits on behalf of Plan as required by the HIPAA Security Rule; and (ii) ensure that any Subcontractor to whom it provides EPHI agrees in writing to implement reasonable and appropriate safeguards to protect such information. Supplier shall provide Plan with any such information concerning these safeguards as Plan may from time to time request.

4.21. Security Incidents. Supplier agrees to promptly report to Plan any Security Incident it learns of.

5. RESPONSIBILITIES OF SUPPLIER REGARDING UNSECURED PHI

5.1. Securing PHI. Unless it is not feasible under the circumstances, Business Associate agrees to implement, in a reasonable and appropriate manner, the technologies and methodologies the HITECH Act, the Secretary, or other Law specifies in order to render PHI that Supplier creates, receives, maintains or transmits on behalf of Plan, unusable, unreadable, or indecipherable to unauthorized individuals, thereby making the PHI secure. In addition, unless it is not feasible under the circumstances, Supplier shall ensure that any agent, including, but not limited to, Subcontractors or vendors to whom it provides Plan's PHI will implement, in a reasonable and appropriate manner, the technologies and methodologies the HITECH Act, the Secretary, or other Law specifies with respect to rendering Plan's PHI unusable, unreadable or indecipherable to unauthorized individuals.

5.2. Breach Notification. With respect to any Unsecured PHI, Supplier shall report to Plan any Breach (as defined in the Omnibus Rule) discovered by Supplier, or any of Supplier's Subcontractors, within twenty-four (24) hours of Discovery.

(a) The report must include (or be supplemented on an ongoing basis as information becomes available) with: (i) the identification of all Individuals whose Unsecured PHI was or is believed to have been breached; (ii) a brief description of the Breach, including the type of Breach (e.g, theft, loss, improper disposal, hacking), location of the Breach (e.g., laptop, desktop, paper), how the Breach occurred, the date the Breach occurred, and the date the Breach was discovered; (iii) a description of the type of Unsecured PHI involved (e.g., social security number, diagnosis, EOBs, etc.), including the type of media, but not the Breached PHI itself, unless requested by Plan; (iv) a description of the safeguards in place prior to the Breach (e.g., firewalls, packet filtering, secure browser sessions, strong authentication); (v) a description of the actions taken in response to the Breach (e.g., additional safeguards, mitigation, sanctions, policies, and procedures); (vi) all other information reasonably requested by Plan to enable Plan to perform and document a risk assessment in accordance with the Breach Notification Rule, and (vii) all other information reasonably necessary to provide notice to Individuals, the Secretary and/or the media.

(b) At Plan's sole option, Plan may delegate to Supplier the responsibility for determining (and providing evidence to Plan) that any such incident is not a Breach, including the requirement to perform a risk assessment to determine whether a low probability of compromise has occurred, as provided by the Breach Notification Rule. In the event that Plan delegates this obligation to Supplier, without unreasonable delay, and in any event no later than thirty (30) calendar days after Discovery, Supplier shall provide Plan with written notification of the Breach and a copy of the risk assessment that assesses whether a low probability of compromise occurred.

(c) At Plan's sole option, Plan may delegate to Supplier the responsibility of providing any notifications Plan determines is required by the Breach Notification Rule, including notifications to Individuals, the Secretary and/or the media. Prior to sending out such notifications, Supplier will provide a copy of the template notification letters for approval by Plan. All notifications shall comply with the elements established by the Breach Notification Rule and be sent within timeframes established by the Breach Notification Rule. In the event that Plan delegates these obligations to Supplier and in the event of a Breach, without unreasonable delay, and in any event no later than sixty (60) calendar days after Discovery, Supplier shall provide Plan evidence that all required notifications, including any media or Secretary notifications, have been made.

(d) Supplier shall pay all reasonable costs incurred in relation to the occurrence of a Breach or potential Breach, including, but not limited to, expenses relating to providing any notifications Plan, or as applicable the Supplier, determines necessary under the Breach Notification Rule, regardless of whether Supplier or Plan makes the notifications.

6. RESPONSIBILITIES OF PLAN. Plan agrees to amend Plan documents to include specific provisions to restrict the use or disclosure of PHI and to ensure adequate procedural safeguards and accounting mechanisms for such uses or disclosures, in accordance with the Privacy Rule.

7. TERM AND TERMINATION.

7.1. Term. The term of this BAA shall continue until termination of the Supplier Agreement or until otherwise terminated pursuant to this BAA.

7.2. Termination and Amendment by Operation of Law. This BAA shall terminate immediately in the event that a HIPAA Business Associate Agreement is no longer applicable or required under then current Law. If on the advice of Plan's counsel, Plan reasonably determines that the terms of this BAA likely would be interpreted to violate or not comply with any Applicable Laws, the parties shall negotiate in good faith to amend this BAA to comply with such Laws. If the parties cannot reasonably agree on such amendment, then this BAA and the Supplier Agreement, if one, shall terminate.

7.3. Termination by Plan. Plan may terminate this BAA if it reasonably determines that Supplier has violated a material term of this BAA, the HIPAA Regulations, or any other Applicable Law after providing thirty (30) days for Supplier to cure the breach in cooperation with Plan or end the violation; provided, however, that in the event that termination of this BAA is not feasible in Plan's sole discretion, Supplier hereby acknowledges that Plan shall have the right to immediately terminate this BAA and the Supplier Agreement, if any, and to report the breach to the Secretary, notwithstanding any other provision of this BAA to the contrary.

7.4. Right to Cure. In the event that Supplier breaches this BAA or any provision of the Privacy Rule and fails to cure the breach within thirty (30) days, Plan reserves the right to cure such breach. Supplier will cooperate with any such efforts undertaken by Plan. Cure of breach does not limit Plan's ability to immediately terminate this BAA and the Supplier Agreement, if any.

7.5. Injunctive Relief. Supplier acknowledges and agrees that the terms of this BAA and the HIPAA Regulations are necessarily of a special, unique and extraordinary nature and that the loss arising from a breach thereof cannot reasonably and adequately be compensated by money damage, as such breach will cause Plan to suffer irreparable harm. Accordingly, upon failure of Supplier to comply with the terms of the Supplier Agreement, HIPAA Regulations, or other Applicable Law, and except as otherwise provided herein, Plan or any of its successors or assigns shall be entitled to injunctive or other extraordinary relief and with such injunctive or other extraordinary relief to be cumulative to, but not in limitation of, any other remedies that may be available to Plan, its successors or assigns, such relief to be without the necessity of posting a bond.

7.6. Effect of Termination. Upon termination or expiration of this BAA, Supplier shall either return or destroy all PHI created, received, maintained, or transmitted by Supplier on behalf of Plan that the Supplier maintains in any form and shall retain no copies of such information to the extent that such action is feasible and not prohibited by other Applicable Law. This provision applies to all Subcontractors or agents of Supplier who may possess PHI on behalf of the Supplier and/or Plan. In the event that Plan has ascertained that the return or destruction of such information is not feasible or permissible, Supplier agrees to continue to comply with all provisions of this BAA with regard to its uses, storage, and disclosure of such PHI for as long as Supplier maintains such PHI.

7.7. General Permitted Uses and Disclosures. Except as limited in this BAA, Supplier may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Plan as specified in the Supplier Agreement, provided that such use or disclosure would not violate the HIPAA Regulations or other Law if performed by Plan itself.