snap+ DATA PROTECTION DOCUMENTS

Version control

Version: **1.0** | Effective date: **13 July 2026** | Owner: Conferma Legal

Applies to: any snap+ Agreement with a Commencement Date on or after the effective date of this version.

Supersedes: all previous versions (retained in, and available from, the Conferma Trust Centre archive). Published at: the Conferma Trust Centre (https://trust.conferma.com/)

Incorporation and applicable version

These Data Protection Documents are incorporated by reference into, and form part of, the snap+ Agreement (comprising the Order Form and the Terms and Conditions) (the "Agreement"). The version of these Data Protection Documents that applies to a given Agreement is the version specified in the Order Form and in force as at the Commencement Date. Conferma may issue updated versions of these Data Protection Documents from time to time; any updated version shall apply prospectively only, shall be notified to the Customer, and shall not materially reduce the protection afforded to the Customer or to data subjects during the Term without the Customer's prior written agreement.

Interpretation

These Data Protection Documents contain their own definitions of the core data protection terms used in them, set out in the Definitions section below, and those definitions apply throughout these Data Protection Documents. Any other capitalised term used but not defined in these Data Protection Documents (including "Agreement", "Order Form", "Commencement Date", "Customer", "Conferma", "Services" and "Term") has the meaning given to it in the Agreement (including Schedule A (Definitions and Interpretation) to the Terms and Conditions). Where a term is defined both in these Data Protection Documents and elsewhere in the Agreement, the definition in these Data Protection Documents applies for the purposes of these Data Protection Documents and in respect of data protection matters. References to "this Agreement" are to the Agreement into which these Data Protection Documents are incorporated. In the event of conflict, the priority provisions of the Order Form apply.

DEFINITIONS

Affiliates	In relation to a Party, a business entity now or hereafter controlled by, controlling or under common control with that Party. Control exists when an entity owns or controls directly or indirectly at least fifty percent (50%) plus one share of the outstanding equity representing the right to vote for the election of directors or other managing authority of another entity.
Applicable Law	Means: (i) in respect of Conferma, any laws, regulations, statutes and codes in the Territory which apply to the provision of snap+, the

© 2026 Conferma Limited

	Services and/or the performance of this Agreement; and (ii) in respect of Customer, any laws, regulations, statutes and codes in the Territory which apply to the receipt of snap+, the Services and/or the performance of this Agreement.
Approved Addendum	The ICO's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, issued under section 119A of the Data Protection Act 2018 and in force from 21 March 2022, as revised or replaced from time to time.
Business Day	A day, excluding Saturdays and Sundays, on which banks are generally open in London, England, for the transaction of normal banking business.
Commencement Date	The date specified as such in the Order Form or, if none is specified, the date on which the Order Form is last signed by the Parties.
Confidential Information	In relation to a Party, any information relating to such Party's business, customers, subscribers, personnel, research, development, finances, technologies, marketing plans, business opportunities, financial or other affairs, including trade secrets and other proprietary, non-public information relating to such Party's snap+ plans, designs, costs, prices and snap+ names, or know-how but excluding information that (a) is or becomes generally known or available by publication, commercial use or otherwise through no fault or negligence of the receiving Party; (b) is known and has been reduced to tangible form by the receiving Party at the time of disclosure and is not subject to restriction; (c) is independently developed by the receiving Party or learned by the receiving Party from third parties with no access to the information disclosed; (d) is lawfully obtained from a third party that has the right to make such disclosure; or (e) is made generally available by the disclosing Party without restriction on disclosure, and includes without limitation the contents of this Agreement.
Controller, Processor, Data Subject, Personal Data Breach and "processing" (and "process)	Have the meanings given to those terms (or their nearest equivalents) in the Privacy Laws.
Customer Personal Data	Any Personal Data comprised in the transaction data (or any other data) provided by the Customer.
Data Protection Documents	Conferma's snap+ Data Protection Documents published by Conferma at the Trust Centre at https://trust.conferma.com/ (or such other URL as Conferma notifies to the Customer), in the

© 2026 Conferma Limited

	version specified in the Order Form, which include Conferma's data privacy terms, data processing particulars, security measures, international data transfer mechanisms and United States state privacy terms, together with any other data protection schedules or modules they contain from time to time, and which are incorporated into and form part of this Agreement.
DPA 2018	The Data Protection Act 2018 (and regulations made thereunder).
EU SCCs	The standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended, replaced or superseded from time to time.
FAFDP	The Swiss Federal Act on Data Protection of 25 September 2020 (SR 235.1) and the Ordinance on Data Protection (SR 235.11), each as amended from time to time.
FDPIC	The Swiss Federal Data Protection and Information Commissioner.
GDPR	Means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and includes the UK implementation of Regulation (EU) 2016/679 under section 3 of the UK European Union (Withdrawal) Act 2018.
IDTA	The ICO's International Data Transfer Agreement, version A1.0, in force from 21 March 2022, as revised or replaced from time to time.
Order Form	The order form signed by the Parties which sets out the commercial particulars of the Agreement (including the Service Tier(s), fees, Territory, currency, Commencement Date and Initial Term) and which incorporates these Terms and Conditions and the Data Protection Documents by reference.
Party	A party to this Agreement and 'Parties' means both of them.
Personal Data	Any and all personal data protected by and within the scope of the Privacy Laws.
Privacy Laws	All applicable international, federal, state, provincial, and local laws, rules, regulations, directives and governmental requirements relating in any way to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: (a) the GDPR, (b) the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder) ("**DPA 2018**"), the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426), (c) the Australian Privacy Act 1988 (Cth) No. 119 1988 (as amended), (d) the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, et seq. and all implementing regulations

© 2026 Conferma Limited

	promulgated by the California Attorney General to date, as amended from time to time), (e) the Singaporean Personal Data Protection Act 2012 For avoidance of doubt, each Party will be subject only to the laws, rules, regulations, directives and governmental requirements applicable to it.
Regulator	Means any supervisory authority, regulator or other governmental body with responsibility for the enforcement of the Privacy Laws (including the Information Commissioner's Office ("ICO")).
Restricted Transfer	A transfer of Customer Personal Data that is subject to the transfer restrictions in Chapter V of the GDPR, Chapter V of the UK GDPR or the equivalent provisions of any other applicable Privacy Laws.
Security Incident	An occurrence that could reasonably be considered by a Party to have potential substantial security implications to a system or its environment in relation to any Account Data of Customer or its Affiliates, including any loss, damage, alteration, destruction, unauthorised disclosure, misuse or theft of such data (whether accidental or deliberate). In the context of PCI DSS, security incidents identify suspicious or anomalous activity.
Services	Support services and professional services required to provide, maintain and support the Customer's access to and use of snap+.
Service Analysis	Statistical and other information related to the performance, operation and use of the Services and use data from the Services environment in aggregated form.
snap+	snap+ and services to be provided by Conferma to Customer pursuant to this Agreement as set out in the Order Form (together with all updates, modifications and new versions of such snap+ released by Conferma for general sale from time to time) and any Order Forms.
Sub-processor	Any processor engaged by Conferma to process Customer Personal Data on Conferma's behalf in connection with the Services.
Transfer Risk Assessment	An assessment of the risks associated with a Restricted Transfer, as required by the applicable Privacy Laws (including the "data protection test" introduced by the DUAA for UK transfers).
UK GDPR	Has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

© 2026 Conferma Limited

DATA PRIVACY TERMS

1.1 The Parties acknowledge that, for the purposes of the Privacy Laws, the Customer shall be the controller and Conferma shall be the processor for Customer Personal Data.

1.2 Customer warrants and represents that it has obtained all necessary consents from and given all necessary notices to the Affiliates and cardholders (including under Applicable Law) to enable lawful transfer of the Customer Personal Data and/or lawful collection of the Customer Personal Data by Conferma on behalf of the Customer and the subsequent processing by Conferma in accordance with this Agreement for the duration of this Agreement.

1.3 The Data Processing Particulars set out the scope, nature and purpose of processing by Conferma, the duration of the processing and the types of Personal Data and categories of Data Subject.

1.4 Conferma shall:

(a) process Customer Personal Data solely for the purposes of and in accordance with Customer's documented instructions set out in this Agreement, unless required by Applicable Laws to otherwise process the Personal Data. Where Conferma is relying on Applicable Laws as the basis for Processing Personal Data, Conferma shall promptly notify the Customer of this before performing the processing required by Applicable Laws unless those Applicable Laws prohibit Conferma from so notifying the Customer;

(b) promptly inform the Customer if, in Conferma's opinion, an instruction given by the Customer in respect of the Processing of Customer Personal Data infringes the Privacy Laws and, where reasonably required, provide an explanation of the reasons for that opinion, and the Parties shall co-operate reasonably to resolve the matter, provided that Conferma shall not be obliged to carry out any independent legal review of the Customer's instructions;

(c) taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures, including those measures set out in the Security Measures, to ensure a level of security in relation to Customer Personal Data appropriate to the risk;

(d) ensure that all personnel who have access to and/or process Personal Data are contractually obliged to keep the Personal Data confidential or are under an appropriate statutory obligation of confidentiality;

(e) ensure that any Affiliates and Sub-processors who collect, process or store Customer Personal Data for Conferma do so in accordance with the relevant provisions of this Agreement and the Privacy Laws, and Conferma shall remain liable to Customer for any Affiliates' and Sub-processors' compliance with them;

© 2026 Conferma Limited

(f) ensure that Customer Personal Data that originates from within the United Kingdom is only transferred to Affiliates and Sub-processors outside the United Kingdom: (i) if the territory is determined by a relevant authority to ensure an adequate level of protection in accordance with the relevant Privacy Laws; (ii) if the transfer is governed by appropriate safeguards in accordance with the relevant Privacy Laws (such as binding corporate rules, standard data protection clauses adopted by a relevant authority or a certification mechanism approved by a relevant authority), and

(i) the Customer or Conferma has provided appropriate safeguards in relation to the transfer;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) Conferma complies with its obligations under the Privacy Laws by providing an adequate level of protection to any Customer Personal Data that is transferred; and

(iv) Conferma complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Customer Personal Data;

(g) promptly notify Customer if it receives a request about any Customer Personal Data from a data subject under any Privacy Laws, and provide such reasonable cooperation and information as is reasonably necessary to assist Customer to respond to such request. Conferma shall not respond directly to any such request but shall promptly provide the Customer with a copy of it. Any assistance provided by Conferma to the Customer in responding to such a request shall be at the Customer's cost;

(h) assist the Customer in ensuring compliance with its obligations under the Privacy Laws with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(i) notify the Customer without undue delay on becoming aware of a Personal Data Breach;

(i) at the written direction of the Customer, delete or return Customer Personal Data and copies thereof to the Customer on termination of the Agreement, unless required by Applicable Laws to store the Personal Data, provided that Conferma may retain a copy of such Customer Personal Data where reasonably necessary for the establishment, exercise and defence of legal claims;

(j) maintain complete and accurate records to demonstrate its compliance with this clause 1.4 and provide such reasonable cooperation and information as is reasonably necessary to assist Customer to verify Customer's compliance with its obligations under any Privacy Laws taking into account the nature of processing and the information available to Conferma; and

© 2026 Conferma Limited

(j) provide such reasonable cooperation and information to Customer as is reasonably necessary to demonstrate compliance with this clause 1.4 or as required by a Regulator PROVIDED THAT:

(i) Customer shall give Conferma as much advance written notice of an audit request as reasonably possible (and in any event at least fourteen (14) days advance notice except where it is prevented from doing so by a Regulator);

(ii) Customer shall use reasonable endeavours to minimise the frequency of audit requests and the disruption to Conferma (including its business operations and other customers) in complying with audit requests; and

(iii) the provision of any cooperation and/or information shall be subject to any obligations of confidentiality or non-disclosure owed by Conferma to a third party or under Applicable Laws.

1.5 The Customer consents to Conferma appointing the categories of Sub-processors of Customer Personal Data under this Agreement described in the Data Processing Particulars, provided that it enters into with any Sub-processor a written agreement incorporating terms which are substantially similar to those set out in this clause 1 and which Conferma confirms reflect and will continue to reflect the requirements of the Privacy Laws. As between the Customer and Conferma, Conferma shall remain fully liable for all acts or omissions of any Sub-processor appointed by it pursuant to this clause 1.5.

1.6 Conferma shall inform the Customer of any intended changes concerning the addition or replacement of Sub-processors (which notification may be given via Conferma's Trust Centre) and shall allow the Customer a reasonable period to raise any reasonable objection to such change. The Parties shall co-operate reasonably to resolve any concerns the Customer may have about any such proposed change.

1.7 The Parties acknowledge that Conferma may compile and use Service Analysis to create statistical analysis, for security and operations management, for research and development purposes and for marketing purposes. Service Analysis will be anonymised so that they do not incorporate Customer Personal Data, Account Data, or Confidential Information in a form that could identify or serve to identify Customer or any data subject. Conferma retains all intellectual property rights in Service Analysis.

1.8 For any transfers of Customer Personal Data under this Agreement to countries which do not ensure an adequate level of data protection within the meaning of Privacy Laws of the foregoing territories, to the extent such transfers are subject to such Privacy Laws, and are:

(a) from the European Union, the European Economic Area and/or their member states, then the EU SCCs, Module 2 (Controller to Processor) and, where applicable, Module 3 (Processor to Processor) apply and are incorporated by reference to this Agreement, with the Annex information deemed completed as follows:

© 2026 Conferma Limited

(i) The information of the contracting parties to this Agreement shall form Annex I.A;

(ii) The contents of the Data Processing Particulars shall form Annex I.B;

(iii) The supervisory authority listed in Annex I.C. shall be that determined under Part A (EU Standard Contractual Clauses), clause 3.3, of the International Data Transfer Mechanisms; and

(iv) The contents of the Security Measures shall form Annex II.

(v) From the UK, then the UK SCCs apply, and are incorporated by reference to this Agreement.

(vi) From Switzerland, then the EU SCCs as recognised under the Swiss Federal Act on Data Protection (FADP) shall apply mutatis mutandis, with references to the GDPR replaced by references to the FADP and references to the competent supervisory authority replaced by the Swiss Federal Data Protection and Information Commissioner, and the EU SCCs shall be deemed amended accordingly.

© 2026 Conferma Limited

DATA PROCESSING PARTICULARS

Processing, Personal Data and Data Subjects

1. Processing Operations

The Personal Data transferred or Processed will be subject to the following processing activities:

- Scope: Conferma shall process the Personal Data to the extent necessary to provide the Product and Services pursuant to and in accordance with the terms of the Agreement.
- Nature: Conferma shall process the Personal Data as necessary to provide the Services. Such Personal Data may also be used for reporting and analysis purposes in connection with the Services.
- Purpose of processing: to provide the Product and Services to the Customer in accordance with the Agreement.
- Duration of the processing: for the Term and for such period thereafter as is required pursuant to Applicable Laws and/or as reasonably required by Conferma for the purpose of the establishment, exercise or defence of legal claims.

2. Data Subjects

The Personal Data transferred or Processed concern the following categories of Data Subjects:

- Cardholders
- Travellers
- Customer employees or authorised users

3. Categories of Data

The Personal Data transferred or Processed concern the following categories of data:

- Names
- Addresses
- Telephone numbers
- Email addresses
- Payment information (including credit card numbers)

4. International Transfer

If Customer agrees: Personal Data may be transferred to a country/recipient outside the EU/EEA/UK/Switzerland as follows:

- South Africa
- United States of America

© 2026 Conferma Limited

Authorised Sub-processors

Conferma intends to use the service of the following Sub-processors for Processing of Personal Data:

Name of Sub-processor	Address	Task to be performed	Location of Processing
Iomart PLC	Data Protection Officer, iomart Group PLC 6 Atlantic Quay 55 Robertson Street Glasgow G2 8JD	Physical data centre hosting and firewall management.	UK
Cloudflare	Cloudflare, Ltd. County Hall/The Riverside Building Belvedere Road London, SE1 7PB Attention: Data Protection Officer privacyquestions@cloudflare.com	Edge hosting, WAF, DDoS, Firewall, CDN, TLS Certificate management	UK
Upland Interfax	Data Protection Officer privacy@uplandsoftware.com	Fax provider used to send data to merchant companies requiring fax documents	US – No access to PII or PCI data; data is sent encrypted and sent on to intended recipient.
Concord	Data Protection Officer privacy@concord.net	Fax provider used to send data to merchant companies requiring fax documents.	Belgium (EU)
Fortra	Fortra LLC 11095 Viking Drive, Suite 100, Eden Prairie, MN 55344 Attention Data Protection Officer: privacy@fortra.com	MSSP for the SOC and Managed, hosted SIEM service	UK
ServiceNow	Data Protection Officer privacy@servicenow.com For written enquiries, please contact: ServiceNow, Inc. Attn: Privacy 2225 Lawson Lane Santa Clara, CA 95054	Customer Service	UK/EU
Microsoft	If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or EU Data Protection Officer, please	Email, Teams, Telephony (including voicemail),	UK data centres

© 2026 Conferma Limited

	contact Microsoft by using their web form. For more information about contacting Microsoft, including Microsoft Ireland Operations Limited, see the *"How to contact us section"* of their privacy statement.	documentation (e.g. contract) storage.	
Microsoft Azure	If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or EU Data Protection Officer, please contact Microsoft by using their web form. For more information about contacting Microsoft, including Microsoft Ireland Operations Limited, see the *"How to contact us section"* of their privacy statement.	Cloud Computing	UK data centres (current); EU data centres (planned)
WNS	Data Protection Officer Office Address: 2 Heron Cres, Century City, Cape Town, 7441, South Africa Attention: Data Protection Officer privacy@wns.com	Overflow customer service centre	UK (storage) / South Africa (view/access)
DerbySoft	Headquarters: 14800 Landmark Blvd Suite 640, Dallas, TX 75254 Email: privacy@derbysoft.net	AI Voice Agent - automating outbound calls to hotels	US - No access to PCI data; data is sent encrypted and sent on to intended recipient.

Approval. The Customer's approval of the use of the above Sub-processors and of the international transfer of Personal Data (if applicable) is given by the Customer in the Order Form to the Agreement.

© 2026 Conferma Limited

SECURITY MEASURES

Conferma has implemented and will maintain appropriate technical and organisational measures, internal controls and information security routines intended to protect Personal Data. These include:

1. Access controls – policies, procedures and physical and technical controls:

(a) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorised persons;
(b) to ensure that all members of its workforce who require access to Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access;
(c) to ensure that Conferma's assigned administrators retain sole responsibility for granting access to Personal Data; to authenticate and permit access only to authorised individuals; and to prevent members of its workforce from providing Personal Data to unauthorised individuals;
(d) to provide a process by which employee and other user accounts are created and deleted in a secure and timely fashion, and to ensure that such process includes appropriate leadership approval, an auditable history of all changes, and an annual review of access authorisation and excess access remediation; and
(e) to encrypt and decrypt Personal Data where appropriate.

2. Security incident procedures – policies and procedures to detect, respond to, and otherwise address suspected or known security incidents, including procedures to:

(a) monitor systems and detect actual and attempted attacks on or intrusions into Personal Data or the systems that contain it;
(b) mitigate harmful effects of security incidents; and
(c) document security incidents and their outcomes.

3. Contingency planning – policies and procedures for responding to an emergency or other occurrence (for example, pandemic, fire, vandalism, system failure and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan.

4. Device and media controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain Personal Data into and out of a Conferma facility and the movement of these items within a Conferma facility, including:

(a) policies and procedures to address the final disposition of Personal Data and the hardware or electronic media on which it is stored, and
(b) procedures for removal of Personal Data from electronic media before the media are made available for re-use.

© 2026 Conferma Limited

Conferma shall ensure that no Personal Data is downloaded or otherwise stored on laptops or other portable devices.

5. Audit controls – hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use Personal Data, including appropriate logs and reports concerning these security requirements and compliance therewith.

6. Data integrity – policies and procedures to ensure the confidentiality, integrity and availability of Personal Data and to protect it from improper disclosure, alteration or destruction.

7. Storage and transmission security – technical security measures to guard against unauthorised access to Personal Data transmitted over an electronic communications network, including a mechanism to encrypt Personal Data in electronic form while in transit and, where required by Applicable Law or PCI DSS, in storage on networks or systems.

8. Assigned security responsibility – designation of a security official responsible for the development, implementation and maintenance of its information security program.

9. Testing – regular testing of the key controls, systems and procedures of the information security program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the information security program.

10. Patching – deployment as quickly as reasonably possible of all necessary security patches to all systems that process, store or otherwise support the services described in the Agreement, including operating system, open source and application software.

11. Storage media – an auditable program of disposal and destruction requirements for all storage media containing Personal Data, including procedures that require Personal Data to be irreversibly deleted before assigning, allocating or reallocating storage media that contained Personal Data, or before permanently removing storage media from a facility, so that the media contains no residual data. If necessary, this program should involve physically destroying the storage media so that it is impossible to recover any portion of data.

12. Program violations – documented consequences for violations of the information security program, and any other privacy, data protection, information security or confidentiality policies.

13. Training – information security training to all individuals authorised to have access to Personal Data.

© 2026 Conferma Limited

INTERNATIONAL DATA TRANSFER MECHANISMS

1. INTERPRETATION AND APPLICATION

1.1 This document sets out the transfer mechanisms that apply to any restricted transfer of Customer Personal Data made under this Agreement. It supplements the Data Privacy Terms, the Data Processing Particulars and the Security Measures and is incorporated into this Agreement.

1.2 The Part of this document that applies to a given transfer is determined by the origin of the Customer Personal Data:

(a) Part A (EU Standard Contractual Clauses) applies to transfers originating from the European Union or the European Economic Area;
(b) Part B (UK Addendum and IDTA) applies to transfers originating from the United Kingdom;
(c) Part C (Swiss FADP Addendum) applies to transfers originating from Switzerland;
(d) Part D (Singapore Personal Data Protection Act 2012) applies to transfers originating from Singapore;
(e) Part E (Australia Privacy Act 1988, Australian Privacy Principle 8) applies to transfers originating from Australia;
(f) Part F (Japan Act on the Protection of Personal Information) applies to transfers originating from Japan;
(g) Part G (India Digital Personal Data Protection Act 2023) applies to transfers originating from India;
(h) Part H (China Personal Information Protection Law 2021) applies to transfers originating from mainland China; and
(i) Part I (Global Residual Framework) applies to transfers originating from any other jurisdiction where local law restricts or imposes conditions on international transfers of personal data.

1.3 Where a transfer originates from more than one of the territories referred to in clause 1.2, each applicable Part shall apply to the relevant Customer Personal Data.

1.4 Terms used in this document and not otherwise defined have the meanings given to them in the Agreement or in the applicable transfer instrument.

PART A - EU STANDARD CONTRACTUAL CLAUSES

1. INCORPORATION

1.1 Where Part A applies, the EU SCCs are incorporated into this Agreement by reference and form part of it, with the selections set out in this Part A and the annex information completed as set out in clause 3 of this Part A.

1.2 As between the parties:

© 2026 Conferma Limited

(a) where the Customer is a controller of the relevant Customer Personal Data, Module Two (Controller to Processor) applies, with the Customer as data exporter and Conferma as data importer; and

(b) where the Customer is itself a processor of the relevant Customer Personal Data, Module Three (Processor to Processor) applies, with the Customer as data exporter and Conferma as data importer.

1.3 Where there is any conflict between the EU SCCs and any other provision of this Agreement, the EU SCCs prevail in respect of the relevant Restricted Transfer.

2. MODULE SELECTIONS

2.1 Clause 7 (Docking clause) applies.

2.2 In Clause 9 (Use of sub-processors), Option 2 (general written authorisation) applies. Conferma shall inform the Customer of any intended addition or replacement of Sub-processors in accordance with the Sub-processor change provisions of the Data Privacy Terms, and the minimum period for prior notice shall be fourteen (14) days.

2.3 In Clause 11 (Redress), the optional wording permitting data subjects to lodge a complaint with an independent dispute resolution body is not included.

2.4 In Clause 17 (Governing law), the EU SCCs are governed by the law of the EU Member State in which the data exporter is established. Where the data exporter is not established in an EU Member State, the EU SCCs are governed by the law of Ireland.

2.5 In Clause 18 (Choice of forum and jurisdiction), disputes shall be resolved before the courts of the EU Member State whose law governs under clause 2.4 of this Part A.

2.6 The optional wording in Clause 8.9 (audits carried out by an independent auditor) and any other optional wording not expressly selected in this Part A is not included, save where required by the applicable Privacy Laws.

3. ANNEX COMPLETION

3.1 Annex I.A (List of Parties) is completed with the details of the parties set out in the Order Form. The Customer is the data exporter; Conferma is the data importer.

3.2 Annex I.B (Description of the transfer) is completed as set out in the Data Processing Particulars, including the categories of data subjects, the categories of Customer Personal Data, the nature and purpose of processing, and the duration of processing.

3.3 Annex I.C (Competent supervisory authority) is determined in accordance with Clause 13 of the EU SCCs, namely: (a) where the Customer, as data exporter, is established in an EU or EEA Member State, the supervisory authority of that Member State; (b) where the Customer is not so established but has appointed a representative under Article 27 of the GDPR, the supervisory authority of the Member State in which that representative is established; or (c) failing (a) and (b),

© 2026 Conferma Limited

the supervisory authority specified in the Order Form or, absent such specification, the Irish Data Protection Commission.

3.4 Annex II (Technical and organisational measures) is completed as set out in the Security Measures.

3.5 Annex III (List of sub-processors), where applicable under Module Three, is completed as set out in the list of authorised Sub-processors in the Data Processing Particulars.

PART B - UK ADDENDUM AND INTERNATIONAL DATA TRANSFER AGREEMENT

1. INCORPORATION

1.1 Where Part B applies, the Approved Addendum is incorporated into this Agreement by reference and applies to the relevant Restricted Transfer, together with the EU SCCs as incorporated and completed under Part A (as amended by the Approved Addendum).

1.2 Alternatively, where the parties agree in the Order Form to use a standalone mechanism for a UK-only transfer, the IDTA applies in place of the Approved Addendum, with its Tables completed consistently with this Part B and its Mandatory Clauses unchanged.

1.3 Where there is any conflict between the Approved Addendum (or the IDTA) and any other provision of this Agreement, the Mandatory Clauses of the Approved Addendum (or the IDTA) prevail in respect of the relevant Restricted Transfer.

2. ADDENDUM TABLE COMPLETION

2.1 Table 1 (Parties) is completed with the details of the parties set out in the Order Form. The Customer is the “Exporter” and Conferma is the “Importer”.

2.2 Table 2 (Selected SCCs, Modules and Selected Clauses) is completed on the basis that the version of the EU SCCs to which the Approved Addendum is appended is that incorporated under Part A, together with the module and clause selections set out in Part A.

2.3 Table 3 (Appendix Information) is completed by reference to the annex information set out in clause 3 of Part A (which in turn refers to the Data Processing Particulars, the Security Measures and the Order Form).

2.4 Table 4 (Ending this Addendum when the Approved Addendum changes) is completed on the basis that neither party may end the Approved Addendum in the circumstances described in Section 19 of the Mandatory Clauses, except to the extent necessary to maintain valid appropriate safeguards for the relevant Restricted Transfer.

2.5 The Mandatory Clauses of the Approved Addendum apply unchanged.

© 2026 Conferma Limited

3. DUAA AND UPDATED INSTRUMENTS

3.1 The parties acknowledge that the DUAA applies a "data protection test" to Restricted Transfers made in reliance on appropriate safeguards, and that the ICO has indicated it will issue updated versions of the IDTA and the Approved Addendum.

3.2 Each party shall act reasonably and proportionately in assessing whether the level of protection for data subjects under a Restricted Transfer is not materially lower than under the UK GDPR.

3.3 Where the ICO issues a revised or replacement IDTA or Approved Addendum, the parties shall adopt the updated instrument in accordance with clause 4 of the Common Provisions in this document.

PART C - SWISS FADP ADDENDUM

1. INCORPORATION

1.1 Where Part C applies, the EU SCCs as incorporated and completed under Part A apply to the relevant Restricted Transfer, subject to the amendments set out in this Part C as recognised by the FDPIC.

1.2 Where there is any conflict between the EU SCCs (as amended by this Part C) and any other provision of this Agreement, the EU SCCs (as so amended) prevail in respect of the relevant Restricted Transfer.

2. AMENDMENTS RECOGNISED BY THE FDPIC

2.1 The competent supervisory authority in Annex I.C and for the purposes of Clause 13 is the FDPIC, to the extent the transfer is governed by the FADP.

2.2 References in the EU SCCs to the "GDPR" or "Regulation (EU) 2016/679" are to be read as references to the FADP in respect of transfers governed by the FADP.

2.3 The EU SCCs protect the personal data of legal entities until the entry into force of any amendment to the FADP that removes such protection, to the extent the FADP so requires.

2.4 References to a "Member State" and to "EU Member State" must not be interpreted so as to exclude data subjects in Switzerland from the possibility of enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

2.5 Where the transfer is governed exclusively by the FADP, the EU SCCs are governed by, and disputes are to be resolved before the courts of, Switzerland; and any reference to the law and courts of an EU Member State in Clauses 17 and 18 is amended accordingly.

© 2026 Conferma Limited

PART D - SINGAPORE PERSONAL DATA PROTECTION ACT 2012

1. APPLICATION

1.1 Part D applies to any transfer of Customer Personal Data to a recipient outside Singapore where the Customer Personal Data relates to individuals in Singapore or is otherwise subject to the PDPA.

1.2 In this Part D: "ASEAN MCCs" means the ASEAN Model Contractual Clauses for Cross Border Data Flows endorsed by the PDPC, as updated from time to time; "APEC CBPR" means the APEC Cross-Border Privacy Rules System; "PDPA" means the Personal Data Protection Act 2012 (Singapore) (No. 26 of 2012), as amended from time to time, together with subsidiary legislation, regulations and binding guidance issued thereunder; "PDPC" means the Personal Data Protection Commission of Singapore; "Transfer Limitation Obligation" or "TLO" means the obligation under section 26 of the PDPA to ensure that personal data transferred outside Singapore receives a standard of protection comparable to that under the PDPA.

2. TRANSFER LIMITATION OBLIGATION

2.1 Where Part D applies, Conferma shall comply with the TLO and shall not transfer Customer Personal Data to a recipient outside Singapore unless it has taken reasonable steps to ensure that the recipient protects the Customer Personal Data to a standard comparable to that required under the PDPA.

2.2 The parties agree that Conferma's obligations under the Data Privacy Terms, the Data Processing Particulars and the Security Measures, taken together with the terms of this Part D, are designed to provide a standard of protection for Customer Personal Data that is comparable to the PDPA.

3. CONTRACTUAL MECHANISM

3.1 As the primary mechanism for satisfying the TLO, Conferma shall ensure that any onward transfer of Customer Personal Data to a Sub-processor or other third party outside Singapore is made only pursuant to a binding written agreement requiring the recipient to: (a) protect the Customer Personal Data to a standard comparable to the PDPA; (b) not transfer the Customer Personal Data to any further third party without the prior written consent of Conferma and equivalent contractual protections on the further recipient; and (c) notify Conferma promptly of any breach or suspected breach of data protection obligations relating to the Customer Personal Data.

3.2 The ASEAN MCCs may be used as a recognised contractual mechanism for transfers within the ASEAN region. Conferma shall notify the Customer if it adopts the ASEAN MCCs for any such transfer.

© 2026 Conferma Limited

4. APEC CBPR CERTIFICATION

4.1 Where an overseas recipient of Customer Personal Data holds valid APEC CBPR System or Privacy Recognition for Processors (PRP) System certification, Conferma may rely on such certification as an alternative mechanism for satisfying the TLO in respect of transfers to that recipient.

5. SUPERVISORY AUTHORITY

5.1 The supervisory authority for the purposes of Part D is the PDPC (www.pdpc.gov.sg).

PART E - AUSTRALIA PRIVACY ACT 1988 (AUSTRALIAN PRIVACY PRINCIPLE 8)

1. APPLICATION

1.1 Part E applies to any disclosure of Customer Personal Data to an overseas recipient where the Customer Personal Data relates to individuals in Australia or is otherwise subject to the Privacy Act.

1.2 In this Part E: "APP" means an Australian Privacy Principle set out in Schedule 1 to the Privacy Act; "APP Entity" means an entity to which the APPs apply under the Privacy Act; "OAIC" means the Office of the Australian Information Commissioner; "Privacy Act" means the Privacy Act 1988 (Cth), as amended from time to time, including as amended by the Privacy and Other Legislation Amendment Act 2024 (Cth).

2. ACCOUNTABILITY AND REASONABLE STEPS

2.1 Where Part E applies, Conferma shall, before disclosing Customer Personal Data to an overseas recipient, take reasonable steps to ensure that the recipient will not act in a way that would breach the APPs (other than APP 1) in relation to that information.

2.2 As the primary means of taking reasonable steps under clause 2.1, Conferma shall enter into a binding contractual agreement with each overseas recipient requiring the recipient to: (a) handle the Customer Personal Data in a manner that would not breach the APPs (other than APP 1) if the recipient were itself an APP Entity; (b) not disclose the Customer Personal Data to any further third party without first taking reasonable steps to ensure that further third party will not breach the APPs; and (c) cooperate with any investigation by the OAIC relating to the Customer Personal Data.

2.3 The parties acknowledge that under APP 8.1, an APP Entity that discloses personal information to an overseas recipient remains accountable for any act or practice of that recipient that would breach the APPs, even where the APP Entity has taken the reasonable steps in clause 2.2. Conferma shall take commercially reasonable steps to monitor overseas recipients' compliance with their contractual obligations.

© 2026 Conferma Limited

3. 2024 ACT AMENDMENTS

3.1 The parties acknowledge that the Privacy and Other Legislation Amendment Act 2024 (Cth), which commenced on 11 December 2024, amended APP 8 by introducing new subclauses 8.2(aa) and 8.3, which create an additional exception to the requirement in APP 8.1 to take reasonable steps. Conferma shall assess whether reliance on any such exception is appropriate in the circumstances of a given disclosure, having regard to OAIC guidance.

4. EXCEPTIONS

4.1 The obligation in clause 2.1 does not apply where: (a) the overseas recipient is subject to a law or binding scheme that, in the reasonable assessment of Conferma, is substantially similar to the APPs and under which the individual can enforce that protection; (b) the individual has been expressly informed by the Customer that APP 8.1 will not apply to the disclosure and has consented to the disclosure in those circumstances; or (c) the disclosure is required or authorised by or under an Australian law or a court or tribunal order.

5. SUPERVISORY AUTHORITY

5.1 The supervisory authority for the purposes of Part E is the OAIC (www.oaic.gov.au).

PART F — JAPAN ACT ON THE PROTECTION OF PERSONAL INFORMATION (APPI)

1. APPLICATION

1.1 Part F applies to any provision of Customer Personal Data by Conferma to a third party located outside Japan where that Customer Personal Data relates to individuals in Japan or is otherwise subject to the APPI.

1.2 In this Part F: “APPI” means the Act on the Protection of Personal Information (Act No. 57 of 2003, Japan), as amended with effect from 1 April 2022 and as further amended from time to time; “Equivalent System” means a system that continuously implements measures for the protection of personal data equivalent to those required of business operators under the APPI, as determined in accordance with guidelines issued by the PPC; “PPC” means the Personal Information Protection Commission of Japan; “White-listed Country” means a country or region designated by the PPC as having a personal information protection system equivalent to Japan’s standards, which as at the date of this Agreement includes the EU/EEA Member States and the United Kingdom.

2. GENERAL RULE — CONSENT

2.1 As a general rule under the APPI, the provision of Customer Personal Data to a third party in a foreign country requires the prior, informed consent of the data subject. Where consent is required, Conferma shall inform the Customer promptly so that the Customer can take steps to obtain the required consent before the transfer proceeds.

© 2026 Conferma Limited

3. EXCEPTIONS — WHITE-LISTED COUNTRIES AND EQUIVALENT SYSTEMS

3.1 Consent under clause 2.1 is not required where: (a) the recipient is located in a White-listed Country; or (b) the recipient has established an Equivalent System.

3.2 Where Conferma relies on the Equivalent System exception under clause 3.1(b), it shall: (a) obtain confirmation from the recipient that it maintains an Equivalent System prior to the transfer; (b) maintain records of that confirmation; and (c) promptly suspend the relevant transfer and notify the Customer upon becoming aware that the recipient has ceased to maintain an Equivalent System.

3.3 Conferma shall maintain records of any provision of Customer Personal Data to overseas third parties and the basis on which each provision was made, in accordance with the APPI and PPC rules.

4. REGULATORY DEVELOPMENTS

4.1 The parties note that a bill amending the APPI was approved by the Japanese Cabinet on 7 April 2026 and, if enacted, is expected to take full effect by 2028. Amendments include proposed relaxations on consent requirements for statistical and AI development purposes. The parties shall cooperate in good faith to assess and give effect to any amendments to the APPI as they come into force.

5. SUPERVISORY AUTHORITY

5.1 The supervisory authority for the purposes of Part F is the PPC (www.ppc.go.jp).

PART G — INDIA DIGITAL PERSONAL DATA PROTECTION ACT 2023

1. APPLICATION

1.1 Part G applies to any transfer of Customer Personal Data outside India where that Customer Personal Data relates to individuals in India or is otherwise subject to the DPDP Act.

1.2 In this Part G: “Data Protection Board” means the Data Protection Board of India established under section 18 of the DPDP Act; “DPDP Act” means the Digital Personal Data Protection Act 2023 (India) (Act No. 22 of 2023), as amended from time to time; “DPDP Rules” means the Digital Personal Data Protection Rules 2025, notified by the Ministry of Electronics and Information Technology on 14 November 2025, as amended from time to time; “MeitY” means the Ministry of Electronics and Information Technology of India; “Restricted Country” means any country notified by the Central Government of India under section 16(1) of the DPDP Act as a country to which transfers of personal data are restricted.

2. CURRENT TRANSFER POSITION

2.1 The DPDP Act adopts a blacklist approach to cross-border data transfers: personal data may generally be transferred outside India unless the Central Government designates a specific country as a Restricted Country by notification under section 16(1).

© 2026 Conferma Limited

2.2 As at the date of this Agreement, the Central Government has not notified any Restricted Countries. Conferma shall monitor MeitY and Data Protection Board publications for any section 16(1) notifications and shall notify the Customer promptly if any country to which Customer Personal Data is transferred or stored is designated as a Restricted Country.

3. IMPLEMENTATION STATUS

3.1 The parties acknowledge that: (a) the DPDP Rules were notified on 14 November 2025 and operationalise the DPDP Act, including requirements for consent management and the establishment of the Data Protection Board; and (b) certain provisions of the DPDP Act and DPDP Rules are expected to become fully effective by approximately May 2027. The parties shall keep this Part G under review and cooperate in good faith to address any new obligations as they take effect.

4. CONTRACTUAL SAFEGUARDS

4.1 Without prejudice to the current transfer position in clause 2, Conferma shall implement the following contractual safeguards in respect of Customer Personal Data subject to the DPDP Act: (a) bind any overseas Sub-processor by contractual obligations equivalent to those in the Data Privacy Terms and the Security Measures; (b) on request from the Customer, provide evidence of the contractual safeguards in place for transfers of Customer Personal Data outside India; and (c) on becoming aware of any Restricted Country designation that affects an existing transfer, immediately suspend that transfer and notify the Customer.

5. DATA FIDUCIARY AND PROCESSOR ROLES

5.1 The parties acknowledge that for the purposes of the DPDP Act, the Customer is the "Data Fiduciary" and Conferma is the "Data Processor". Conferma shall assist the Customer in meeting its obligations as Data Fiduciary, including in relation to data principal (data subject) rights, breach notification and responding to the Data Protection Board.

6. SUPERVISORY AUTHORITY

6.1 The supervisory authority for the purposes of Part G is the Data Protection Board of India. Contact and guidance are available at www.meity.gov.in.

PART H — CHINA PERSONAL INFORMATION PROTECTION LAW 2021 (PIPL)

1. APPLICATION

1.1 Part H applies to any outbound provision of Customer Personal Data from mainland China to a recipient outside mainland China, where that Customer Personal Data relates to individuals in China or is otherwise subject to the PIPL.

1.2 In this Part H: "CAC" means the Cyberspace Administration of China; "CAC Standard Contract" means the government-prescribed standard contractual clauses issued by the CAC pursuant to the Measures on Standard Contract for Cross-Border Transfer of Personal

© 2026 Conferma Limited

Information (effective 1 June 2023), as updated from time to time, which must be used in the prescribed form and filed with the relevant provincial CAC office; "CIIO" means a Critical Information Infrastructure Operator as defined under the Regulations on the Security Protection of Critical Information Infrastructure (effective 1 September 2021); "Important Data" means data that, if tampered with, destroyed, leaked or illegally acquired or used, may endanger national security, the operation of the economy, social stability, or public health and safety, as designated by the relevant competent authorities; "Certification Measures" means the Measures for the Certification of Cross-Border Transfer of Personal Information (effective 1 January 2026); "PIPL" means the Personal Information Protection Law of the People's Republic of China (effective 1 November 2021), as amended from time to time; "PIPIA" means a Personal Information Protection Impact Assessment required under Article 55 of the PIPL; "Security Assessment" means the mandatory outbound data security assessment carried out through the CAC under the Measures for the Security Assessment of Outbound Data Transfer (effective 1 September 2022) and the Provisions on Facilitating and Regulating Cross-border Data Flows (effective 22 March 2024).

2. TRANSFER PATHWAYS AND THRESHOLDS

2.1 Before transferring any Customer Personal Data outside mainland China, Conferma shall determine the applicable transfer pathway based on the following thresholds (as updated by the Provisions on Facilitating and Regulating Cross-border Data Flows, effective 22 March 2024):

(a) Security Assessment (mandatory) where Conferma: is a CIIO; transfers Important Data; within a calendar year transfers personal information of one million (1,000,000) or more individuals (excluding sensitive personal information); or within a calendar year transfers sensitive personal information of ten thousand (10,000) or more individuals.

(b) CAC Standard Contract where Conferma is not a CIIO, does not transfer Important Data, and within a calendar year transfers personal information of 100,000 to 999,999 individuals (excluding sensitive personal information) or fewer than 10,000 individuals' sensitive personal information. The CAC Standard Contract must be executed in the CAC-prescribed form, completed with the required annexes, and filed with the relevant provincial CAC office within ten (10) Business Days of taking effect.

(c) Certification as an alternative to the CAC Standard Contract pathway, where Conferma obtains personal information protection certification from a CAC-accredited institution in accordance with the Certification Measures (effective 1 January 2026), subject to meeting the applicable eligibility criteria.

(d) Below thresholds: where Conferma's annual transfers fall below 100,000 individuals (excluding sensitive personal information) and below 10,000 individuals' sensitive personal information, and Conferma is not a CIIO and does not transfer Important Data, no prescribed pathway is mandatory under the PIPL. Conferma shall nonetheless implement the contractual safeguards in clause 3.

© 2026 Conferma Limited

2.2 Conferma shall monitor its transfer volumes on a rolling calendar-year basis and shall notify the Customer promptly if it approaches or exceeds any threshold in clause 2.1 so that the parties can agree and implement the appropriate pathway without delay.

3. OBLIGATIONS APPLICABLE TO ALL PATHWAYS

3.1 Regardless of the applicable pathway, Conferma shall before making any outbound transfer: (a) conduct a PIPIA in accordance with Article 55 of the PIPL, covering the lawfulness of the processing purpose and method, the impact on individual rights and interests, and the security measures in place; (b) retain a record of the PIPIA and make it available to the Customer on request; and (c) ensure that any overseas recipient contractually agrees to: (i) process the Customer Personal Data only for the agreed purposes; (ii) implement technical and organisational security measures equivalent to those required by the PIPL; (iii) not further transfer the Customer Personal Data to any third party without Conferma's prior written consent and equivalent obligations on the further recipient; and (iv) cooperate with any investigation or inquiry by the CAC.

4. EXEMPTIONS

4.1 The pathway requirements in clause 2.1 do not apply to transfers that fall within the following exemptions, subject to any conditions prescribed by the CAC: (a) transfers strictly necessary for the conclusion or performance of a contract to which the individual is a party; (b) transfers strictly necessary for cross-border human resources management pursuant to employment contracts or applicable regulations; and (c) transfers necessary to protect an individual's life, health or property in an emergency.

4.2 Conferma shall document its reliance on any exemption under clause 4.1.

5. GOVERNMENT-PRESCRIBED CONTRACT NOTE

5.1 The parties acknowledge that the CAC Standard Contract is a government-prescribed instrument that must be used in its prescribed form and is not the same as, or interchangeable with, the EU SCCs incorporated under Part A of this document. Where the CAC Standard Contract pathway applies, the parties shall execute the CAC-prescribed document separately and Conferma shall complete the required filing with the relevant provincial CAC office.

6. HONG KONG SAR AND MACAU SAR

6.1 Hong Kong SAR and Macau SAR each have separate data protection frameworks (the Personal Data (Privacy) Ordinance (Cap. 486) (Hong Kong) and Law 8/2005 on Personal Data Protection (Macau) respectively) and are not subject to the PIPL. Where Conferma transfers Customer Personal Data from Hong Kong or Macau, it shall comply with the applicable local framework and shall implement equivalent contractual safeguards to those in this Part H.

© 2026 Conferma Limited

7. SUPERVISORY AUTHORITY

7.1 The supervisory authority for the purposes of Part H is the CAC (www.cac.gov.cn). Filings for CAC Standard Contracts are submitted to the relevant provincial CAC office.

PART I — GLOBAL RESIDUAL FRAMEWORK

1. PURPOSE AND SCOPE

1.1 Part I applies to any transfer of Customer Personal Data originating from a jurisdiction not otherwise covered by Parts A to H of this document, where the laws of that jurisdiction restrict or impose conditions on the international transfer of personal data.

1.2 Part I also applies on a supplementary basis to transfers covered by Parts A to H, to the extent that a particular transfer gives rise to obligations under a jurisdiction not otherwise addressed in those Parts.

1.3 The jurisdictions anticipated as most relevant to this Part I as at the date of this Agreement include: (a) Brazil (Lei Geral de Proteção de Dados Pessoais (LGPD), Law No. 13,709/2018); (b) Canada - Personal Information Protection and Electronic Documents Act (PIPEDA) (S.C. 2000, c. 5) and applicable provincial privacy legislation (including Quebec's Law 25 (Act 25 modernising legislative provisions on the protection of personal information)); (c) United Arab Emirates - Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (UAE Federal DPL); DIFC Law No. 5 of 2020 on Data Protection; and ADGM Data Protection Regulations 2021; (d) South Africa - Protection of Personal Information Act No. 4 of 2013 (POPIA); (e) South Korea - Personal Information Protection Act (PIPA), as amended from time to time, but Part I extends to any other jurisdiction with applicable data transfer restrictions.

2. GENERAL OBLIGATIONS

2.1 Where Part I applies, Conferma shall: (a) assess whether the law of the jurisdiction of origin of the Customer Personal Data imposes restrictions on the transfer of personal data to the destination country or requires specific safeguards; (b) implement appropriate contractual, technical and organisational measures to ensure that Customer Personal Data receives in the destination country a standard of protection not materially lower than that required by the law of the jurisdiction of origin; (c) enter into a binding written agreement with any overseas recipient requiring the recipient to protect the Customer Personal Data to an equivalent standard; and (d) notify the Customer promptly if Conferma identifies that a proposed or existing transfer does not, or may not, comply with applicable local data transfer restrictions.

3. JURISDICTION SPECIFIC NOTES

3.1 Brazil (LGPD): transfers of personal data from Brazil require adequate protection in the destination country or the use of specific safeguards recognised by the Brazilian National Data Protection Authority (ANPD), including standard contractual clauses, binding corporate rules, specific guarantees, or approved seals and certifications. Conferma shall use ANPD-approved

© 2026 Conferma Limited

contractual clauses or equivalent recognised safeguards for any transfer of personal data originating in Brazil.

3.2 Canada (PIPEDA and provincial law): Canada does not prohibit cross-border transfers of personal information but requires organisations to remain accountable for personal information they transfer to Sub-processors, including overseas processors. Conferma shall bind any overseas recipient of Canadian personal information by contractual obligations providing equivalent protection to PIPEDA and, where applicable, Quebec's Law 25 (including its privacy impact assessment requirement for certain transfers outside Quebec).

3.3 UAE (Federal DPL, DIFC and ADGM): the following regime-specific requirements apply: (a) UAE Federal (DPL 45/2021): transfers outside the UAE to countries not recognised by the UAE Data Office as providing adequate protection require binding contractual arrangements ensuring equivalent protection and, where applicable, registration or notification to the UAE Data Office; (b) DIFC (DP Law 5/2020): transfers outside the DIFC require either an adequacy finding by the DIFC Commissioner of Data Protection or an approved transfer contract or other appropriate safeguard; (c) ADGM (DP Regulations 2021): equivalent adequacy or contractual safeguard requirement to the DIFC. Conferma shall identify the applicable UAE regime for any transfer of Customer Personal Data from a UAE jurisdiction and implement the appropriate safeguard.

3.4 South Africa (POPIA): transfers of personal data outside South Africa require the recipient to be subject to a binding law, binding corporate rules, or a binding agreement that provides an adequate level of protection substantially similar to POPIA. Conferma shall ensure such binding protections are in place for any transfer of South African personal data.

3.5 South Korea (PIPA): transfers of personal data outside South Korea generally require the data subject's consent or the use of standard contractual clauses issued by the Personal Information Protection Commission (PIPC) of Korea, unless the destination country has been designated as adequate by the PIPC. Conferma shall use the PIPC-issued standard clauses or obtain the required consent for any transfer of South Korean personal data where no adequacy designation applies.

4. COOPERATION AND JURISDICTION-SPECIFIC INSTRUMENTS

4.1 Where a jurisdiction covered by this Part I introduces or updates a government-prescribed transfer instrument (such as standard contractual clauses, binding corporate rules or an approved certification scheme), the parties shall cooperate in good faith to adopt that instrument within a reasonable period of its coming into effect.

4.2 The Customer shall notify Conferma in reasonable time of any transfer covered by this Part I that requires a specific regulatory approval, filing or notification, so that the parties can cooperate to ensure compliance.

© 2026 Conferma Limited

5. NO DUPLICATION

5.1 Where a transfer is covered by a more specific Part of this document (Parts A to H), that Part governs the transfer and this Part I applies only to the extent it addresses obligations not covered by the more specific Part.

COMMON PROVISIONS

1. TRANSFER RISK ASSESSMENTS

1.1 Before making, and periodically during, any Restricted Transfer relying on the mechanisms in this document, Conferma shall carry out and maintain a Transfer Risk Assessment appropriate to the transfer, taking into account the circumstances of the transfer, the laws and practices of the destination country, and any supplementary measures required to ensure a level of protection consistent with the applicable Privacy Laws.

1.2 Conferma shall, on the Customer's reasonable written request, provide a summary of the relevant Transfer Risk Assessment and details of any supplementary measures implemented, subject to any obligations of confidentiality owed to third parties.

2. SUPPLEMENTARY MEASURES

2.1 Where a Transfer Risk Assessment identifies that the transfer mechanism alone does not ensure an adequate level of protection, Conferma shall implement appropriate supplementary technical, organisational or contractual measures, or shall not make (or shall suspend) the relevant Restricted Transfer.

3. PRIORITY AND SEVERANCE

3.1 In the event of any conflict or inconsistency between this document and the body of this Agreement or the Data Privacy Terms, the mandatory clauses of the applicable transfer instrument prevail to the extent required to maintain valid appropriate safeguards, and thereafter this document prevails over the body of this Agreement in respect of the relevant Restricted Transfer.

3.2 If any transfer mechanism in this document is held to be invalid or ceases to provide a lawful basis for a Restricted Transfer, the parties shall, without undue delay, implement an alternative lawful transfer mechanism, and the remaining provisions of this document shall continue in full force and effect.

4. ADOPTION OF UPDATED INSTRUMENTS

4.1 Where the European Commission, the ICO, the FDPIC or any other competent supervisory authority referred to in this document issues a revised, updated or replacement version of any transfer instrument referred to in this document, that revised instrument shall apply to the relevant Restricted Transfers from the date it takes effect (or such later date as it specifies), and the parties shall complete any additional information reasonably required to give effect to it.

© 2026 Conferma Limited

4.2 Each party shall promptly take such steps and execute such documents as are reasonably necessary to give effect to this clause 4.

5. ADEQUACY

5.1 Nothing in this document requires the parties to implement a transfer mechanism where, and for so long as, the relevant transfer is covered by an adequacy decision, adequacy regulations or an equivalent recognition of adequate protection under the applicable Privacy Laws that lawfully permits the transfer without additional safeguards.

US STATE PRIVACY TERMS

1. APPLICATION AND INTERPRETATION

1.1 This section applies where, and to the extent that, one or more United States state privacy laws apply to Conferma's Processing of Customer Personal Data under this Agreement. As at the effective date of these Data Protection Documents, this section addresses the California Consumer Privacy Act; it is intended to accommodate other United States state privacy laws (including those of Virginia, Colorado, Connecticut, Utah and Texas) which impose comparable service provider or processor contract requirements, and Conferma may add corresponding terms for such laws from time to time.

1.2 In this section, "CCPA" means the California Consumer Privacy Act of 2018 (Cal. Civ. Code section 1798.100 et seq.), as amended by the California Privacy Rights Act of 2020 and all implementing regulations promulgated by the California Privacy Protection Agency and the California Attorney General, each as amended from time to time.

1.3 This section addresses Conferma's obligations as a service provider (or equivalent) in respect of the Processing of Customer Personal Data. It is not an international data transfer mechanism, and the Common Provisions of the International Data Transfer Mechanisms that relate specifically to Restricted Transfers (namely Transfer Risk Assessments, supplementary measures and adequacy) do not apply to this section.

1.4 In the event of any conflict between this section and the other Data Protection Documents in respect of Personal Data subject to a United States state privacy law, this section prevails.

2. CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

2.1 Terms used in this clause 2 that are defined in the CCPA (including "Business", "Service Provider", "Sell", "Share", "Business Purpose", "Commercial Purpose", "Consumer" and "Deidentified") have the meanings given to them in the CCPA. For the purposes of this clause 2, the Customer is the Business and Conferma is the Service Provider.

2.2 Conferma shall Process Customer Personal Data only: (a) for the Business Purposes specified in this Agreement and the Data Processing Particulars, or as otherwise permitted for a Service Provider under the CCPA; and (b) on behalf of the Customer and in accordance with the Customer's documented instructions.

© 2026 Conferma Limited

2.3 Conferma shall not: (a) Sell or Share Customer Personal Data; (b) retain, use or disclose Customer Personal Data for any purpose other than the Business Purposes specified in this Agreement, or as otherwise permitted under the CCPA; (c) retain, use or disclose Customer Personal Data outside the direct business relationship between the parties, except as permitted under the CCPA; or (d) combine Customer Personal Data with personal information that Conferma receives from, or on behalf of, any other person, or collects from its own interaction with the Consumer, except as permitted under the CCPA.

2.4 Conferma shall provide the same level of privacy protection in respect of Customer Personal Data as is required of Businesses by the CCPA.

2.5 Conferma shall notify the Customer promptly, and in any event without undue delay, after it makes a determination that it can no longer meet its obligations under the CCPA.

2.6 The Customer may, on reasonable notice, take reasonable and appropriate steps to stop and remediate any unauthorised use of Customer Personal Data by Conferma, and to help ensure that Conferma uses Customer Personal Data in a manner consistent with the Customer's obligations under the CCPA.

2.7 Deidentified data. Where Conferma receives or creates Deidentified data, it shall: (a) take reasonable measures to ensure that the data cannot be associated with a Consumer or household; (b) Process such data only in a Deidentified form; (c) not attempt to re-identify the data, except as permitted under the CCPA; and (d) contractually obligate any recipient of such data to comply with this clause 2.7.

2.8 Customer obligations. The Customer shall: (a) inform Conferma of any Consumer request made under the CCPA with which Conferma must assist or comply; and (b) provide the information reasonably necessary for Conferma to comply with, or assist the Customer in complying with, such request.

2.9 Sub-processors. Conferma may engage Sub-processors to assist in providing the Services, provided that Conferma enters into a written agreement with each such sub-processor that imposes obligations substantially equivalent to those set out in this clause 2, consistent with the requirements of the CCPA for engagements of onward Service Providers or Contractors.

© 2026 Conferma Limited