Resonata

Resonata Data Processing Addendum

LAST UPDATED: JUNE 25, 2026

This Resonata Data Processing Addendum ("DPA") is incorporated into and subject to the terms and conditions of the Agreement between Resonata and the Customer entity that is a party to the Agreement. All capitalized terms not defined in this DPA have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the "Agreement" include this DPA, including the Standard Contractual Clauses where applicable.

1. Definitions

1.1 "Affiliate" means any legal entity directly or indirectly controlling, controlled by, or under common control with a party, where control means ownership of a majority share of the stock, equity, or voting interests of such entity.

1.2 "Agreement" means Resonata's Master Services Agreement, Order Form, Statement of Work, or other written or electronic agreement that governs Customer's access to and use of the Services.

1.3 "AI Tools" means artificial intelligence, machine learning, speech-to-text, text-to-speech, natural language processing, large language model, summarization, classification, routing, analytics, or similar technology used by Resonata to provide, maintain, secure, support, or improve the Services.

1.4 "Controller", "Processor", "Data Subject", "Personal Data", "Processing" and "Process" have the meanings given to them under applicable Data Protection Laws, and if not defined thereunder, the GDPR.

1.5 "Customer" means the non-Resonata party to both the Agreement and this DPA that has access to or uses the Services.

1.6 "Customer Data" means Personal Data that Resonata Processes on behalf of Customer through the Services, including guest, caller, reservation, communication, transcript, recording, and account data, as further described in Annex A.

1.7 "Data Protection Laws" means all data protection, privacy, electronic communications, and data security laws and regulations applicable to a party's Processing of Customer Data under the Agreement, including, where applicable, European Data Protection Laws and Non-European Data Protection Laws.

1.8 "Europe" means the European Economic Area and its member states, Switzerland, and the United Kingdom.

1.9 "European Data Protection Laws" means all data protection laws and regulations applicable to Europe, including the GDPR, the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, Directive 2002/58/EC, and applicable national implementing laws, each as amended or superseded.

1.10 "Non-European Data Protection Laws" means United States Data Protection Law, Canadian privacy laws including PIPEDA, and other non-European data protection laws applicable to the Processing of Customer Data.

1.11 "Resonata" means Resonata, Inc., Resonata, LLC, or the applicable Resonata contracting entity identified in the Agreement. If no specific entity is identified, "Resonata" means the Resonata entity providing the Services to Customer.

1.12 "SCCs" or "Standard Contractual Clauses" means the standard contractual clauses adopted by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced from time to time, and as applicable to the relevant transfer.

1.13 "Security Incident" means an unauthorized or unlawful breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data on systems managed or controlled by Resonata.

1.14 "Sensitive Data" means social security number, tax identification number, passport number, driver's license number, payment card number other than truncated values, financial account credentials, health information, biometric information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, criminal record information, account passwords, or other data treated as special category, sensitive, or highly regulated data under Data Protection Laws.

1.15 "Services" means Resonata's voice AI reservations, guest communications, call handling, call routing, booking assistance, analytics, integrations, dashboard, support, and related services provided to Customer under the Agreement.

1.16 "Sub-processor" means any Processor engaged by Resonata or its Affiliates to Process Customer Data on behalf of Customer in connection with the Services. Sub-processors may include third-party service providers and Affiliates of Resonata, but exclude Resonata employees, contractors, and consultants.

1.17 "UK Addendum" means the International Data Transfer Addendum issued by the UK Information Commissioner's Office under section 119A of the UK Data Protection Act 2018, as updated or amended from time to time.

1.18 "United States Data Protection Law" means applicable comprehensive state privacy and data protection laws in the United States, including the California Consumer Privacy Act as amended by the California Privacy Rights Act, and similar state privacy laws as amended or superseded from time to time.

2. Roles and Responsibilities

2.1 Parties' roles. Where Data Protection Laws apply to Processing of Customer Data, the parties acknowledge that Customer is the Controller or Processor, as applicable, and Resonata is a Processor or Sub-processor Processing Customer Data on behalf of Customer. Resonata does not determine the purposes and means of Processing Customer Data except as expressly permitted by the Agreement, this DPA, or applicable law.

2.2 Purpose limitation and permitted Processing. Resonata shall Process Customer Data only for the following purposes: (i) to provide, operate, support, secure, maintain, and improve the Services; (ii) as initiated by Customer or Customer's authorized users through use or configuration of the Services; (iii) to comply with Customer's documented instructions; (iv) as necessary to comply with applicable law; and (v) as otherwise agreed in writing (collectively, "Permitted Purposes").

2.3 Complete instructions. The Agreement, this DPA, Customer's use and configuration of the Services, Customer's written instructions, and applicable Order Forms constitute Customer's complete instructions to Resonata regarding Processing of Customer Data. Processing outside those instructions requires prior written agreement unless required by law.

2.4 Prohibited and Sensitive Data. Customer shall not provide Resonata with Sensitive Data unless the parties have expressly agreed in writing that such data may be Processed through the Services. Resonata does not intentionally request or require Sensitive Data to provide the Services. Because voice conversations may include unsolicited information, Customer acknowledges that callers may voluntarily disclose Sensitive Data or other regulated information during calls. Resonata will handle such incidental disclosures in accordance with this DPA, but Customer remains responsible for determining whether the Services are appropriate for the categories of data Customer permits to be Processed.

2.5 Customer compliance. Customer represents and warrants that it has provided and will continue to provide all notices, obtain all consents, establish all lawful bases, and secure all rights necessary for Resonata to Process Customer Data for the Permitted Purposes. Customer is responsible for the accuracy, quality, legality, and lawful acquisition of Customer Data.

2.6 Call recording, AI disclosure, and communications compliance. Customer is responsible for determining and implementing any notices, consents, scripts, signage, privacy disclosures, and other requirements applicable to call recording, call monitoring, AI-assisted interactions, SMS, email, and other guest communications under applicable law. Resonata may assist Customer with configurable disclosures or scripts where available, but Customer remains responsible for approving and deploying legally sufficient notices for its properties and jurisdictions.

2.7 Lawfulness of instructions. Customer will ensure that Resonata's Processing of Customer Data in accordance with Customer's instructions does not violate applicable law. Resonata shall promptly notify Customer, unless prohibited by law, if Resonata becomes aware or believes that an instruction violates applicable Data Protection Laws.

2.8 Customer as Processor. Where Customer acts as Processor on behalf of a third-party Controller, Customer warrants that its instructions to Resonata and authorizations for Sub-processors have been authorized by the relevant Controller. Customer shall serve as the sole point of contact for Resonata with respect to such third-party Controller unless otherwise agreed in writing.

3. Sub-processing

3.1 Authorization. Customer generally authorizes Resonata to engage Sub-processors to Process Customer Data on Customer's behalf for the Permitted Purposes. Resonata shall maintain a current list of Sub-processors at a publicly available webpage or make such list available to Customer upon request. The list will identify the Sub-processor, the nature of Processing, and the general location of Processing where reasonably available.

3.2 Notice of changes. Resonata shall provide notice of new or replacement Sub-processors at least ten (10) days before authorizing such Sub-processor to Process Customer Data, by updating its Sub-processor list, providing email notice, or other reasonable means. Customer may object to a new Sub-processor as set forth in Annex C where applicable.

3.3 Sub-processor obligations. Resonata shall enter into a written agreement with each Sub-processor imposing data protection obligations that provide at least the same level of protection for Customer Data as this DPA, to the extent applicable to the nature of services provided by such Sub-processor. Resonata remains responsible for each Sub-processor's compliance with those obligations and for acts or omissions of such Sub-processor that cause Resonata to breach this DPA.

3.4 Sub-processor categories. Sub-processors may include providers of cloud hosting, telephony, call routing, speech-to-text, text-to-speech, large language models, AI orchestration, monitoring, logging, analytics, customer support, email, SMS, payment-link infrastructure, data storage, security, and property management system or central reservation system integrations.

4. Security

4.1 Security Measures. Resonata shall implement and maintain appropriate technical and organizational measures designed to protect Customer Data against Security Incidents and to preserve the confidentiality, integrity, availability, and resilience of the Services. The current Security Measures are described in Annex B.

4.2 Confidentiality. Resonata shall ensure that personnel authorized to Process Customer Data are subject to appropriate confidentiality obligations, whether contractual, statutory, or professional.

4.3 Updates. Customer acknowledges that the Security Measures are subject to technical progress and development. Resonata may update or modify the Security Measures from time to time,

provided that such updates and modifications do not materially reduce the overall security of the Services.

4.4 Security Incident response. Upon becoming aware of a Security Incident, Resonata shall: (i) notify Customer without undue delay and, where feasible, within forty-eight (48) hours after awareness; (ii) provide timely information relating to the Security Incident as it becomes known or as reasonably requested by Customer; and (iii) take reasonable steps to contain, investigate, and remediate the Security Incident. Resonata's notification of or response to a Security Incident shall not be construed as an admission of fault or liability.

4.5 Customer responsibilities. Customer is responsible for secure use of the Services, including managing authorized users, account credentials, configuration choices, integration permissions, phone routing settings, and the security of Customer systems that connect to the Services.

5. Security Reports and Audits

5.1 Information. Resonata shall make available information reasonably necessary to demonstrate compliance with this DPA, including security documentation, responses to reasonable security questionnaires, and other documentation reasonably requested by Customer.

5.2 Audit process. Customer may request information to confirm Resonata's compliance with this DPA no more than once per calendar year unless required by a supervisory authority or following a Security Incident. Requests should be sent to privacy@resonata.io or another privacy contact identified by Resonata. Resonata may satisfy audit obligations by providing security reports, certifications, policies, summaries, questionnaire responses, or other reasonable documentation. On-site audits require reasonable advance notice, mutual agreement on scope, and appropriate confidentiality protections.

5.3 Third-party reports. To the extent Resonata obtains SOC 2, ISO 27001, penetration test summaries, or similar reports, Resonata may provide them to Customer under confidentiality terms instead of duplicative audit activities.

6. International Transfers

6.1 Processing locations. Customer acknowledges that Resonata and its Sub-processors may Process Customer Data in the United States and other countries where Resonata, its Affiliates, or Sub-processors maintain operations. Resonata shall ensure that such transfers are made in accordance with applicable Data Protection Laws and this DPA.

6.2 EEA transfers. To the extent Customer Data protected by GDPR is transferred to Resonata in a country that is not recognized as providing an adequate level of protection, the parties agree that the SCCs are incorporated into this DPA and apply to such transfer as the applicable transfer mechanism.

6.3 Data Privacy Framework. As of this version of the DPA, Resonata is not relying on certification under the EU-U.S. Data Privacy Framework, the UK Extension, or the Swiss-U.S. Data Privacy Framework as its primary transfer mechanism unless Resonata separately identifies such certification in writing. If Resonata later obtains and maintains such certification, Resonata may rely on the applicable framework for covered transfers, with the SCCs or other lawful mechanisms available as fallback or supplemental mechanisms where appropriate.

6.4 SCC optional provisions. Where the SCCs apply, the following selections apply unless otherwise agreed in writing: (a) Clause 7, Docking Clause, is omitted; (b) Clause 9(a), Option 2, general written authorization for Sub-processors, applies with the notice process in Section 3; (c) Clause 11(a), optional redress language, does not apply; (d) Clause 13 identifies the competent supervisory authority as the supervisory authority responsible for Customer's compliance with GDPR for the relevant transfer; (e) Clause 17 is governed by the laws of the Netherlands unless another EU member state law is required or agreed; and (f) Clause 18 identifies the courts of the Netherlands unless another forum is required or agreed.

6.5 UK transfers. For transfers subject to UK Data Protection Laws, the SCCs apply as amended by the UK Addendum. The UK Addendum is incorporated into this DPA. Tables 1 through 3 are deemed completed with the information in Annex A and Annex B, and Table 4 is deemed completed by selecting "neither party" unless otherwise agreed.

6.6 Swiss transfers. For transfers subject to the Swiss Federal Act on Data Protection, the SCCs apply with references to the GDPR interpreted as references to Swiss data protection law, references to EU member states interpreted as references to Switzerland where applicable, and the Swiss Federal Data Protection and Information Commissioner identified as the competent supervisory authority where required.

6.7 Alternative mechanisms. To the extent Resonata adopts another lawful transfer mechanism that complies with applicable Data Protection Laws, such alternative mechanism may apply to the relevant transfer in place of or in addition to the mechanisms described in this Section 6.

7. Return and Deletion of Customer Data

7.1 Deletion upon termination. Upon termination or expiration of the Agreement, Resonata shall delete or return Customer Data in its possession or control in accordance with the Agreement and Resonata's retention policies, except to the extent retention is required by applicable law, necessary for legal, tax, security, fraud prevention, backup, or dispute resolution purposes, or retained in archived backups that are securely isolated and deleted according to Resonata's standard backup lifecycle.

7.2 Retention configuration. Where the Services provide retention settings for call recordings, transcripts, logs, or analytics data, Customer is responsible for selecting and maintaining retention settings appropriate for Customer's legal obligations and operational needs. If no specific retention

setting is agreed, Resonata may retain Customer Data for the duration necessary to provide the Services and for a reasonable period thereafter as described in its policies or the Agreement.

7.3 Deletion certification. Upon Customer's written request, Resonata shall provide reasonable written confirmation of deletion of Customer Data, subject to the exceptions in this Section 7.

8. Data Subject Rights and Cooperation

8.1 Data subject requests. Taking into account the nature of the Processing, Resonata shall provide commercially reasonable assistance to Customer to enable Customer to respond to requests from Data Subjects to access, correct, delete, restrict, port, or object to Processing of Customer Data. If a Data Subject submits a request directly to Resonata concerning Customer Data, Resonata shall not respond except to direct the Data Subject to Customer or as legally required.

8.2 DPIAs and consultations. To the extent required by Data Protection Laws, Resonata shall provide reasonably requested information regarding the Services to assist Customer with data protection impact assessments or prior consultations with supervisory authorities. Resonata may satisfy this obligation by providing the Agreement, this DPA, security documentation, subprocessors information, and other reasonable documentation.

8.3 Assistance costs. Resonata may charge reasonable fees for assistance under this Section 8 where the request is excessive, repetitive, requires disproportionate effort, or falls outside standard functionality, unless prohibited by applicable law.

9. Voice AI, Guest Communications, and Payment Workflows

9.1 Voice AI interactions. Customer acknowledges that the Services may use AI Tools to conduct or support voice conversations with callers, answer property and reservation questions, collect booking information, route or transfer calls, summarize interactions, classify call outcomes, and generate analytics. Resonata shall Process Customer Data generated by such interactions only for the Permitted Purposes and in accordance with this DPA.

9.2 Call recordings and transcripts. The Services may create, store, analyze, and display call recordings, transcripts, summaries, metadata, and call outcome classifications. Customer is responsible for determining whether calls should be recorded, whether notices or consents are required, and how long recordings and transcripts should be retained.

9.3 SMS and email communications. Where Customer enables SMS, email, or other guest communications through the Services, Customer is responsible for ensuring that the content, timing, consent, opt-out handling, and deployment of such communications comply with applicable law. Resonata will Process related Customer Data as necessary to provide the enabled communication functionality.

9.4 Payment workflows. The Services may facilitate booking completion by sending secure payment links or directing callers to Customer-approved payment processes. Unless expressly agreed in writing, Customer shall not provide Resonata with full payment card numbers, CVV codes, bank account credentials, or other regulated payment authentication data. Resonata may Process payment-link metadata, truncated payment identifiers, booking status, or confirmation information as necessary to provide the Services.

9.5 Human handoff. The Services may transfer callers to Customer personnel, call centers, or other systems based on Customer configuration, caller intent, AI confidence, legal or policy constraints, or operational requirements. Customer remains responsible for the actions of Customer personnel and third-party systems outside Resonata's control.

10. Jurisdiction-Specific Terms

To the extent Resonata Processes Customer Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex C, the terms in Annex C apply in addition to the terms of this DPA. In the event of conflict or ambiguity, the applicable jurisdiction-specific terms control only to the extent of their applicability.

11. Limitation of Liability

11.1 Each party's and its Affiliates' aggregate liability arising out of or related to this DPA, including the SCCs, is subject to the exclusions and limitations of liability set forth in the Agreement.

11.2 Claims against Resonata or its Affiliates under or in connection with this DPA may be brought only by the Customer entity that is a party to the Agreement, except where Data Protection Laws require otherwise.

11.3 Nothing in this DPA limits any liability that cannot be limited under applicable Data Protection Laws.

12. Relationship with the Agreement

12.1 This DPA remains in effect for as long as Resonata Processes Customer Data on behalf of Customer or until all Customer Data has been returned or deleted in accordance with Section 7.

12.2 This DPA supersedes any prior data processing agreement or similar document between the parties in connection with the Services.

12.3 In the event of conflict between this DPA and the Agreement, the following order of precedence applies: (i) the SCCs where applicable; (ii) this DPA; and (iii) the Agreement, unless the Agreement expressly states that a specific provision overrides this DPA.

12.4 Except for the modifications made by this DPA, the Agreement remains unchanged and in full force and effect.

12.5 This DPA is governed by the governing law and jurisdiction provisions in the Agreement unless required otherwise by applicable Data Protection Laws.

Annex A — Details of Data Processing

(a) Categories of Data Subjects

- Customer personnel, administrators, authorized users, and support contacts who access or configure the Services.
- Hotel guests, prospective guests, callers, and individuals who contact Customer properties by phone or through related communication channels.
- Individuals whose information is included in reservation inquiries, booking records, call recordings, transcripts, SMS messages, emails, payment-link workflows, or property management system records made available to the Services.
- Customer representatives, front desk agents, reservation agents, managers, or call center personnel involved in call handling, transfers, configuration, or review of call outcomes.

(b) Categories of Personal Data

- **Account and user data:** name, business email address, business phone number, role, login credentials or authentication metadata, permissions, user activity logs, and support communications.
- **Guest and caller contact data:** name, phone number, email address, mailing address if provided, language preference, and communication preferences.
- **Reservation and booking data:** stay dates, number of guests, room type preferences, rate or package interest, special requests, loyalty information if provided, booking status, confirmation details, cancellation or modification requests, and information related to accommodations or ancillary services such as dining, spa, parking, activities, or property amenities.
- **Voice and communication data:** call recordings, call audio, transcripts, AI-generated summaries, call classifications, call outcomes, transfer history, sentiment or intent signals, SMS content, email content, and metadata associated with communications.
- **Technical and usage data:** IP address, device or browser metadata for dashboard users, timestamps, call metadata, routing logs, system logs, integration logs, and analytics generated through use of the Services.
- **Payment-link and booking completion metadata:** payment link status, booking status, truncated payment identifiers where applicable, and confirmation information. Full payment card numbers, CVV codes, and bank account credentials are not intended to be Processed unless expressly agreed in writing.

(c) Sensitive Data Processed, If Applicable

Resonata does not intentionally request or require Sensitive Data to provide the Services. Because callers may voluntarily disclose information during voice conversations, Customer Data may incidentally include Sensitive Data or other regulated information. Customer shall not intentionally configure the Services to collect Sensitive Data unless the parties expressly agree in writing and appropriate controls are implemented.

(d) Duration of Processing

Resonata will Process Customer Data for the term of the Agreement and thereafter as necessary to provide the Services, comply with legal obligations, resolve disputes, maintain security, prevent fraud or abuse, and complete deletion or backup lifecycle activities as described in Section 7.

(e) Nature and Purpose of Processing

- Providing a voice AI reservations agent for hospitality customers.
- Answering property, availability, amenity, policy, rate, and reservation-related questions.
- Collecting information needed to assist with reservations, booking completion, follow-up, or human transfer.
- Sending or facilitating SMS and email communications, including booking or payment links where enabled.
- Creating, storing, transcribing, summarizing, classifying, and analyzing calls and guest communications.
- Providing dashboards, analytics, reporting, call outcome categorization, quality assurance, and customer support.
- Integrating with property management systems, central reservation systems, telephony systems, payment-link systems, and other Customer-approved systems.
- Monitoring, debugging, securing, improving, and optimizing the Services, including model prompts, workflows, accuracy, reliability, latency, fraud prevention, and service quality.
- Complying with applicable law and Customer's documented instructions.

(f) Frequency of Processing

Processing occurs on a continuous basis during the term of the Agreement as Customer and its guests, callers, personnel, and systems use or interact with the Services.

Annex B — Security Measures

1. Governance and Policies. Resonata maintains internal security and privacy policies appropriate to the nature of the Services and the stage of the company, including policies or procedures for

access control, acceptable use, incident response, vendor management, data retention, and confidentiality.

2. System Access Controls. Resonata uses reasonable measures designed to prevent unauthorized access to systems Processing Customer Data, which may include unique user accounts, strong passwords, multi-factor authentication where appropriate, access approval workflows, least-privilege access, periodic access reviews, and prompt removal of access when no longer required.

3. Data Access Controls. Resonata restricts access to Customer Data to authorized personnel and Sub-processors who require access for the Permitted Purposes. Direct database access is limited to authorized personnel. Application permissions are designed so users can access only the Customer Data they are authorized to access.

4. Encryption. Resonata uses encryption in transit for Customer Data transmitted over public networks using industry-standard protocols. Resonata uses encryption at rest for production systems, databases, storage services, and backups where supported by the relevant infrastructure provider.

5. Network and Infrastructure Security. Resonata uses cloud infrastructure and related security controls designed to protect production systems, including logical network segmentation where appropriate, secure configuration, firewalls or security groups, managed infrastructure controls, and monitoring of production services.

6. Logging and Monitoring. Resonata maintains logs for production systems, access events, errors, integration activity, and security-relevant events where appropriate. Logs are used for monitoring, troubleshooting, fraud prevention, incident investigation, and service reliability.

7. Vulnerability and Change Management. Resonata uses reasonable vulnerability management and change management practices, which may include dependency review, patching, code review, testing, deployment controls, and remediation of identified vulnerabilities based on risk.

8. Secure Development. Resonata applies secure development practices appropriate to the Services, including review of material changes, environment separation, secrets management, and controls designed to reduce unauthorized access, data leakage, and service disruption.

9. Personnel Security and Confidentiality. Resonata personnel with access to Customer Data are subject to confidentiality obligations. Resonata provides security and privacy guidance appropriate to personnel roles and responsibilities.

10. Sub-processor Diligence. Resonata evaluates Sub-processors based on the nature of services provided and requires Sub-processors to maintain appropriate security and privacy obligations. Resonata remains responsible for Sub-processor Processing as described in Section 3.

11. Backup and Resilience. Resonata uses reasonable backup, replication, and recovery measures designed to support availability and integrity of the Services. Backup retention and deletion follow Resonata's standard backup lifecycle unless otherwise agreed.

12. Payment Data Handling. Unless expressly agreed in writing, Resonata does not intend to Process full payment card numbers, CVV codes, or bank account credentials. Payment workflows should use Customer-approved secure payment links, payment processors, or tokenized systems. Resonata may Process payment-link metadata and booking status information as necessary to provide the Services.

13. Incident Response. Resonata maintains incident response procedures designed to identify, investigate, contain, remediate, and communicate Security Incidents as required by this DPA.

Annex C — Jurisdiction-Specific Terms

Europe

1. Objection to Sub-processors. Where European Data Protection Laws apply, Customer may object in writing to Resonata's appointment of a new Sub-processor within five (5) calendar days after receiving notice, provided that the objection is based on reasonable grounds relating to data protection. The parties shall discuss the objection in good faith. If no commercially reasonable resolution is available, Resonata may choose not to appoint the Sub-processor for Customer or permit Customer to suspend or terminate the affected Services in accordance with the Agreement.

2. Government data access requests. Resonata does not voluntarily provide government agencies or law enforcement with access to Customer Data except as required by valid legal process or applicable law. If Resonata receives a compulsory request for Customer Data, Resonata will, where legally permitted and reasonably practicable: (i) review the legality of the request; (ii) attempt to redirect the requesting authority to Customer; (iii) notify Customer; and (iv) disclose only the minimum amount of information reasonably required. Resonata is not required to provide notice where legally prohibited or where Resonata has a good-faith belief that urgent disclosure is necessary to prevent imminent serious harm.

3. EU Representative. Resonata will identify an EU representative if required by European Data Protection Laws and applicable to Resonata's Processing activities. Until Resonata identifies such representative in writing, Customer should direct privacy inquiries to privacy@resonata.io.

4. International transfer assessments. Where required by European Data Protection Laws, the parties shall reasonably cooperate in connection with transfer impact assessments or similar assessments related to transfers of Customer Data.

United States

- For purposes of United States Data Protection Law, the terms Controller, Processor, Personal Data, and Data Subject shall include equivalent terms such as Business, Service Provider, Contractor, Personal Information, and Consumer as applicable.
- Resonata shall Process Customer Data for the Permitted Purposes, to provide the Services, in accordance with Customer's documented instructions, as otherwise permitted for service

providers or processors under United States Data Protection Law, or as required by applicable law.

- Resonata shall not Sell or Share Customer Data as those terms are defined under applicable United States Data Protection Law. Resonata shall not retain, use, or disclose Customer Data outside the direct business relationship with Customer except as permitted by this DPA, the Agreement, or applicable law.
- Resonata may de-identify, anonymize, or aggregate Customer Data in accordance with applicable law and may use such de-identified, anonymized, or aggregated data for analytics, benchmarking, service improvement, security, product development, and other lawful business purposes, provided that Resonata does not attempt to re-identify such data except to test or validate de-identification controls or as permitted by law.
- Resonata shall provide reasonable assistance to Customer with consumer rights requests under applicable United States Data Protection Law as described in Section 8.

Canada

- Resonata shall use contractual and organizational measures designed to require Sub-processors Processing Customer Data subject to Canadian privacy laws to protect such data in a manner substantially consistent with this DPA.
- Resonata will implement technical and organizational measures as set forth in Section 4 and Annex B.

Annex D — Resonata AI Use Policy

This AI Use Policy supplements the DPA and provides specific instructions regarding Processing of Customer Data through AI Tools. In the event of conflict between this AI Use Policy and the DPA, this AI Use Policy controls solely with respect to AI-specific operational use cases and data training permissions, provided that it shall not reduce Resonata's security obligations or individual privacy rights under the DPA or Data Protection Laws.

1. Use of AI Tools. Customer acknowledges that Resonata may use AI Tools to provide, support, secure, and improve the Services. AI Tools may be used for voice AI conversations, speech-to-text transcription, text-to-speech voice generation, natural language understanding, call routing, call summarization, reservation assistance, guest inquiry handling, outcome classification, analytics, debugging, quality assurance, and service reliability.

2. No foundation model training on raw Customer Data. Resonata will not use raw Customer Data to train or fine-tune any internal or third-party foundation model except with Customer's prior written authorization. Resonata may use Customer Data to provide, maintain, evaluate, debug, secure, and improve the Services for Customer, including prompt, workflow, classification, and quality improvements, subject to the Agreement and this DPA.

3. De-identified and aggregate data. Resonata may create and use de-identified, anonymized, or aggregate data derived from Customer Data for analytics, benchmarking, quality improvement, model evaluation, product development, and operational purposes, provided such data does not reasonably identify Customer, Customer properties, or an individual Data Subject, and provided Resonata maintains safeguards required by applicable law.

4. Third-party AI providers. Some AI functionality may be powered by third-party providers acting as Sub-processors. Customer authorizes Resonata to engage such providers in accordance with Section 3. Resonata will maintain a Sub-processor list and apply contractual restrictions appropriate to the nature of the Processing, including restrictions on unauthorized use of Customer Data for provider model training where commercially available and applicable.

5. AI outputs. Outputs generated by AI Tools from Customer Data, including transcripts, summaries, suggested responses, classifications, and analytics, are treated as Customer Data for purposes of the DPA to the extent they contain or are derived from Personal Data. As between the parties, Customer retains ownership of Customer Data, and Resonata retains ownership of the Services, underlying technology, models, prompts, workflows, and generalized know-how, subject to Customer's rights in Customer Data.

6. Human oversight and accuracy. AI Tools are not human and may generate inaccurate, incomplete, delayed, or inappropriate outputs. Customer is responsible for configuring the Services, approving property-specific content, reviewing outputs where appropriate, determining escalation rules, and maintaining human oversight suitable for Customer's operations and legal obligations. Resonata is responsible for providing the Services in accordance with the Agreement.

7. Restricted inputs. Customer shall not intentionally use the Services to collect Sensitive Data, full payment card information, medical information, emergency service information, or other data requiring specialized regulatory controls unless expressly agreed in writing. Customer should configure disclosures, scripts, routing rules, and human handoff procedures to reduce unnecessary collection of Sensitive Data.

8. Call recordings and transcripts. Call recordings, transcripts, summaries, and related analytics may be used by Resonata to provide, support, debug, secure, monitor, and improve the Services, subject to this DPA. Customer is responsible for determining whether callers must receive notice or provide consent before recording, transcription, AI processing, or follow-up communications.

Annex E — Sub-processor Schedule

Resonata will maintain a current Sub-processor list at resonata.io/subprocessors, another webpage identified by Resonata, or by providing the list to Customer upon request. Until a public Sub-processor page is available, the following categories describe the types of Sub-processors Resonata may use to provide the Services:

- Cloud infrastructure and data hosting providers.

- Telephony, voice routing, and communications platform providers.
- Speech-to-text, text-to-speech, natural language processing, and large language model providers.
- SMS, email, notification, and guest communication providers.
- Monitoring, observability, logging, error tracking, and security providers.
- Customer support, ticketing, CRM, and operations providers.
- Payment-link, booking completion, or payment workflow providers where enabled by Customer.
- Property management system, central reservation system, channel manager, CRM, or hospitality integration providers where enabled by Customer.

Customer may request the then-current list of specific Sub-processors by contacting privacy@resonata.io.
