

Revinata Data Processing Addendum

v1.7 updated July 26, 2023

This Revinata Data Processing Addendum (“DPA”) is incorporated into, and is subject to the terms and conditions of, the Agreement (defined below) between Revinata and the Customer entity that is a party to the Agreement.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the “Agreement” shall include this DPA (including the SCCs (where applicable), as defined herein).

1. Definitions

For the purposes of this DPA:

1.1 “Affiliate(s)” has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term means any legal entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership of a majority share of the stock, equity or voting interests of such entity.

1.2 “Agreement” means Revinata’s Master Services Agreement, or other written or electronic agreement, which governs the provision of the Services to Customer, as such terms or agreement may be updated from time to time.

1.3 “Controller,” “Processor,” “Data Subject,” “Personal Data,” “Processing” and “Process” (whether or not capitalized) have the meanings given to them under applicable Data Protection Laws or if not defined thereunder, the GDPR, and “Process”, “Processes” and “Processed”, with respect to any Customer Data shall be interpreted accordingly.

1.4 “Customer” means the non-Revinata party to both the Agreement and this DPA that has access to the Services.

1.5 “Customer Data” means any Personal Data that Revinata processes on behalf of Customer via the Services, as more particularly described in this DPA.

1.6 “Data Protection Laws” means all data protection 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.

1.7 “Europe” means, for the purposes of this DPA, the European Economic Area and its member states (“EEA”), Switzerland and the United Kingdom (“UK”).

1.8 “European Data Protection Laws” means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (“GDPR”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable

national implementations of (i) and (ii); (iv) the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, “UK Data Protection Laws”); and (v) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance, and the new Federal Act on Data Protection effective as of September 1, 2023 (“Swiss DPA”).

1.9 “Non-European Data Protection Laws” means US Data Protection Law and the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”).

1.10 “Revinatē” means the Revinatē entity that is a party to both the Agreement and this DPA, which may be Revinatē, LLC, a Delaware limited liability corporation, or a Revinatē Affiliate as applicable.

1.11 “SCCs” or “Standard Contractual Clauses” means (i) the Standard Contractual Clauses between Controllers and Processors adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021 (the “2021 Controller-to-Processor Clauses”); or (ii) the Standard Contractual Clauses between Processors adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021 (the “2021 Processor-to-Processor Clauses”), set out at https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en (or such other URL as the European Commission may designate); as applicable in accordance with Section 6.3.

1.12 “Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Customer Data on systems managed or otherwise controlled by Revinatē.

1.13 “Sensitive Data” means (a) social security number, tax file number, passport number, driver’s license number, or similar identifier; (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of “special categories of data” under applicable Data Protection Laws.

1.14 “Sub-processor” means any Processor engaged by Revinatē or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of Revinatē, but shall exclude Revinatē’s employees, contractors, or consultants.

1.15 “UK Addendum” means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner’s Office under S.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.

1.16 “US Data Protection Law” means the California Privacy Rights Act (“CPRA”); Colorado Privacy Act; Connecticut Personal Data Privacy and Online Monitoring Act; Indiana Consumer Data Protection Act (effective 1 Jan. 2026); Iowa Consumer Data Protection Act (effective 1 Jan. 2025); Montana Consumer Data Privacy Act (effective 1 Jan. 2024); Oregon Consumer Privacy Act; Tennessee Information Protection Act (effective 1 July 2025); Texas Data Privacy and Security Act (effective 1 July 2024); Utah Consumer Privacy Act; Virginia Consumer Data Protection Act; and all applicable comprehensive state data protection laws and regulations that are or are not yet in effect as of the date of this DPA; in each case as may be amended or superseded from time to time.

2. Roles and Responsibilities

2.1 Parties' roles. If European Data Protection Laws apply to either party's Processing of Customer Data, the parties acknowledge and agree that with regard to the Processing of Customer Data, Revinate is a Processor acting on behalf of Customer (whether itself a Controller or a Processor). For the avoidance of doubt, this DPA shall not apply to instances where Revinate is the Controller (as defined by European Data Protection Laws) unless otherwise described in Annex C (Jurisdiction-Specific Terms) of this DPA.

2.2 Purpose limitation. Revinate shall Process Customer Data, as further described in Annex A (Details of Data Processing) of this DPA, only in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing ("Permitted Purposes"). The parties agree that the Agreement, including this DPA, along with the Customer's configuration of or use of any settings, features, or options in the Services (as the Customer may be able to modify from time to time) constitute the Customer's complete and final instructions to Revinate in relation to the Processing of Customer Data (including for the purposes of the SCCs), and Processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

2.3 Prohibited Data. Customer will not provide (or cause to be provided) any Prohibited Data to Revinate for Processing under the Agreement, and Revinate will have no liability whatsoever for Prohibited Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to Prohibited Data.

2.4 Customer compliance. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its Processing of Customer Data and any Processing instructions it issues to Revinate and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Revinate to Process Customer Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Customer Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any campaigns or other content created, sent, or managed through the Services, including those relating to obtaining consents (where required) to send messages, the content of the messages and its message deployment practices.

2.5 Lawfulness of Customer's instructions. Customer will ensure that Revinate's Processing of the Customer Data in accordance with Customer's instructions will not cause Revinate to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Revinate shall promptly notify Customer in writing, unless prohibited from doing so under European Data Protection Laws, if it becomes aware or believes that any data Processing instruction from Customer violates European Data Protection Laws. Where Customer acts as a Processor on behalf of a third-party Controller (or other intermediary to the ultimate Controller), Customer warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Revinate for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall serve as the sole point of contact for Revinate and Revinate need not interact directly with (including to provide notifications to or seek authorization from) any third-party Controller other than through regular provision of the Services to the extent required under the Agreement. Customer shall be

responsible for forwarding any notifications received under this DPA to the relevant Controller, where appropriate.

3. Sub-processing

3.1 Authorized Sub-processors. Customer agrees that Revinate may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by Revinate and authorized by Customer are listed at Revinate's Sub-processor web page: <https://www.revinate.com/subprocessors>. Revinate shall notify Customer if it adds or removes Sub-processors at least 10 days prior to any such changes if Customer opts in to receive such notifications from Revinate.

3.2 Sub-processor obligations. Revinate shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-processor; and (ii) remain responsible for such Sub-processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Revinate to breach any of its obligations under this DPA. Customer acknowledges and agrees that, where applicable, Revinate fulfills its obligations under Clause 9 of the 2021 Controller-to-Processor Clauses and 2021 Processor-to-Processor Clauses (as applicable) by complying with this Section 3, and that Revinate may be prevented from disclosing Sub-processor agreements to Customer due to confidentiality restrictions but Revinate shall, upon request, use reasonable efforts to provide Customer with all relevant information it reasonably can in connection with Sub-processor agreements.

4. Security

4.1 Security Measures. Revinate shall implement and maintain appropriate technical and organizational security measures that are designed to protect Customer Data from Security Incidents and designed to preserve the security and confidentiality of Customer Data in accordance with Revinate's security standards described in Annex B ("Security Measures") of this DPA.

4.2 Confidentiality of processing. Revinate shall ensure that any person who is authorized by Revinate to process Customer Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 Updates to Security Measures. Customer is responsible for reviewing the information made available by Revinate relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Revinate may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Customer.

4.4 Security Incident response. Upon becoming aware of a Security Incident, Revinate shall: (i) notify Customer without undue delay, and where feasible, within 48 hours of awareness; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain and investigate any Security Incident. Revinate's notification of or response to a Security Incident under this Section 4.4 shall not be construed as an acknowledgment by Revinate of any fault or liability with respect to the Security Incident.

4.5 Customer responsibilities. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

5. Security Reports and Audits

5.1 Audit rights. Revinate shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA (including this Section 5.1 and where applicable, the SCCs) and any audit rights granted by Data Protection Laws, by instructing Revinate to comply with the audit measures described in Section 5.2 below.

5.2 Security due diligence. Revinate shall respond to all reasonable requests for information made by Customer to confirm Revinate's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Customer's written request to support+privacy@revinate.com, provided that Customer shall not exercise this right more than once per calendar year.

6. International Transfers

6.1 Data center locations. Subject to Section 6.2, Customer acknowledges that Revinate may transfer and process Customer Data to and in the United States and anywhere else in the world where Revinate, its Affiliates or its Sub-processors maintain data processing operations. Revinate shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

6.2 EEA Data Transfers. To the extent that Revinate is a recipient of Customer Data protected by GDPR in a country outside of EEA that is not recognized as providing an adequate level of protection for personal data (as described in applicable European Data Protection Laws), the parties agree to abide by and process such Customer Data in compliance with the SCCs, which shall be incorporated into and form an integral part of this DPA.

6.3 UK Data Transfers. With respect to transfers to which the UK Data Protection Laws apply, the SCCs shall apply and shall be deemed amended as specified by the UK Addendum. The UK Addendum shall be deemed executed by the parties and incorporated into and form an integral part of this DPA. In addition: Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annexes I and II of the relevant SCCs; and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

6.4 Swiss Data Transfers. With respect to transfers to which the Swiss DPA apply, the SCCs shall apply in accordance with Section 6.2 with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA; (ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA; (iii) references to "EU", "Union" and "Member State law" shall be replaced with "Switzerland"; (iv) Clause 13(a) and Part C of Annex II shall be deleted; (v) references to the "competent supervisory authority" and "competent

courts" shall be replaced with "the Swiss Federal Data Protection and Information Commissioner" and "relevant courts in Switzerland"; (vi) Clause 17 shall be replaced to state "The Clauses are governed by the laws of Switzerland"; and (vii) Clause 18 shall be replaced to state "Any dispute arising from these Clauses shall be resolved by the applicable courts of Switzerland. The parties agree to submit themselves to the jurisdiction of such courts".

6.5 Compliance with the SCCs. The parties agree that if Revinate cannot ensure compliance with the SCCs, it shall promptly inform Customer of its inability to comply. If Customer intends to suspend the transfer of European Data and/or terminate the affected parts of the Services, it shall first provide notice to Revinate and provide Revinate with a reasonable period of time to cure such non-compliance, during which time Revinate and Customer shall reasonably cooperate to agree what additional safeguards or measures, if any, may be reasonably required. Customer shall only be entitled to suspend the transfer of data and/or terminate the affected parts of the Services for non-compliance with the SCCs if Revinate has not or cannot cure the non-compliance within a reasonable period.

6.6 Alternative transfer mechanism. To the extent Revinate adopts an alternative lawful data transfer mechanism for the transfer of European Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable European Data Protection Laws and extends to the countries to which European Data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer European Data (within the meaning of applicable European Data Protection Laws), Revinate may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of European Data.

7. Return or Deletion of Data. Upon termination or expiration of the Agreement, Revinate shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, except that this requirement shall not apply to the extent Revinate is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which Customer Data Revinate shall securely isolate, protect from any further processing and eventually delete in accordance with Revinate's deletion policies, except to the extent required by applicable law. The parties agree that the certification of deletion of Customer Data described in Clause 8.5 and 16(d) of the 2021 Controller-to-Processor Clauses and 2021 Processor-to-Processor Clauses (as applicable) shall be provided by Revinate to Customer only upon Customer's written request.

8. Data Subject Rights and Cooperation

8.1 Data subject requests. As part of the Services, Revinate provides Customer with a number of self-service features, that Customer may use to retrieve, correct, delete, or restrict the use of Customer Data, which Customer may use to assist it in connection with its (or its third-party controller's) obligations under the Data Protection Laws with respect to responding to requests from data subjects via Customer's account at no additional cost. In addition, Revinate shall, considering the nature of the processing, provide reasonable additional assistance to Customer to the extent possible to enable Customer (or its third-party controller) to comply with its data protection obligations with respect to data subject rights under Data Protection Laws. In the event that any such request is made to Revinate directly, Revinate shall not respond to such communication directly except as appropriate (for example, to direct the data subject to contact Customer) or legally required, without Customer's prior authorization. If Revinate is required to

respond to such a request, Revinate shall, where the Customer is identified or identifiable from the request, promptly notify Customer and provide Customer with a copy of the request unless Revinate is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) shall restrict or prevent Revinate from responding to any data subject or data protection authority requests in relation to personal data for which Revinate is a controller.

8.2 Data protection impact assessment. To the extent required under applicable Data Protection Laws, Revinate shall (considering the nature of the processing and the information available to Revinate) provide all reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws. Revinate shall comply with the foregoing by: (i) complying with Section 5 (Security Reports and Audits); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

9. Jurisdiction-Specific Terms. To the extent Revinate processes Customer Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Annex C, then the terms specified in Annex C with respect to the applicable jurisdiction(s) ("Jurisdiction-Specific Terms") apply in addition to the terms of this DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and any other terms of this DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms' applicability to Revinate.

10. Limitation of Liability

10.1 Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

10.2 Any claims made against Revinate or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

10.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

11. Relationship with the Agreement

11.1 This DPA shall remain in effect for as long as Revinate carries out Customer Data processing operations on behalf of Customer or until termination of the Agreement (and all Customer Data has been returned or deleted in accordance with Section 7 above).

11.2 The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Services.

11.3 In the event of any conflict or inconsistency between this DPA and Revinate's General Terms and Conditions, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the General Terms and Conditions.

11.4 Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.

11.5 No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.

11.6 This DPA shall be governed by and construed in accordance with 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:

The categories of data subjects whose Personal Data is Processed include (i) individual end users who work for Customer and set up user accounts on Revinate's Services, and (ii) guests who stay at or otherwise visit Customer's property(ies).

(b) Categories of Personal Data:

Revinate will Process (i) the names and email addresses of Customer personnel who log in to the Revinate Services, and (ii) data related to a guest's stay at or visit to Customer's property(ies), including:

- Name
- Email address
- Physical address
- IP-address and other online identifiers
- Date of birth
- Telephone/mobile number
- Location Data
- Information related to a guest's booking for accommodations or ancillary services (e.g., spa, golf, dining, etc.) at the Customer's hotel property

In addition, Revinate will Process the categories of Personal Data provided by Customer. If Customer's property management system captures special categories of data, including, without limitation, factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity, and Customer chooses to make those categories available to Revinate, Revinate may Process them.

(c) Sensitive data processed (if applicable): Revinate does not want to, nor does it intentionally, collect or Process any Sensitive Data in connection with the provision of the Services.

(d) Duration of Processing: Revinate will process Customer Data as outlined in Section 7 (Return or Deletion of Data) of this DPA.

(e) Nature and Purpose of Processing: Revinate processes Personal Data in order to provide its Services to hospitality customers as described at www.revinate.com. Revinate shall only Process Customer Data for the Permitted Purposes, which shall include: (i) processing as necessary to provide the Services in accordance with the Agreement; (ii) Processing initiated by Customer in its use of the Services; and (iii) Processing to comply with any other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement.

Annex B – Security Measures

The following describes Revinate’s Technical and Organizational Security Measures.

1. System Access Controls: Revinate shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

2. Data Access Controls: Revinate shall take reasonable measures to (i) provide that Personal Data is accessible and manageable only by properly authorized staff, (ii) direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and (iii) that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.

3. Auditing. Revinate will cooperate with any audit(s) requested by Customer pursuant to Section 5.2 of the DPA.

Annex C - Jurisdiction-Specific Terms

Europe:

- 1. Objection to Sub-processors.** Customer may object in writing to Revinate's appointment of a new Sub-processor within five (5) calendar days of receiving notice in accordance with Section 3.1 of the DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Revinate will, at its sole discretion, either not appoint such Sub-processor, or permit Customer to suspend or terminate the affected Services in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).
- 2. Government data access requests.** As a matter of general practice, Revinate does not voluntarily provide government agencies or authorities (including law enforcement) with access to or information about Revinate's accounts (including Customer Data). If Revinate receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to or information about a Revinate account (including Customer Data) belonging to a Customer whose primary contact information indicates the Customer is located in Europe, Revinate shall: (i) review the legality of the request; (ii) inform the government agency that Revinate is a Processor of the data; (iii) attempt to redirect the agency to request the data directly from Customer; (iv) notify Customer via email sent to Customer's primary contact email address of the request to allow Customer to seek a protective order or other appropriate remedy; and (v) provide the minimum amount of information permissible when responding to the agency or authority based on a reasonable interpretation of the request. As part of this effort, Revinate may provide Customer's primary and billing contact information to the agency. Revinate shall not be required to comply with this paragraph 2 if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or Revinate's property, the Revinate Site, or Services, but where Revinate is legally prohibited from notifying Customer of requests it shall use its best efforts to obtain a waiver of the prohibition.

United States:

- 1.** Except as described otherwise, the terms Controller, Processor, Personal Data and data subject shall mean "Business", "Service Provider" "Personal Information", and "Consumer" under CPRA, and shall include equivalent terms under other US Data Protection Laws.
- 2.** For this "section of Annex C only, "Permitted Purposes" shall include Processing Customer Data only for the purposes described in this DPA and in accordance with Customer's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for "Service Providers" under US Data Protection Law.
- 3.** Revinate's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, extend to rights requests under US Data Protection Law.

4. Notwithstanding any use restriction contained elsewhere in this DPA, Revinate shall Process Customer Data to perform the Services, for the Permitted Purposes and/or in accordance with Customer's documented lawful instructions, or as otherwise permitted or required by applicable law.
5. Notwithstanding any use restriction contained elsewhere in this Annex C, Revinate may de-identify or aggregate Customer Data as part of performing the Services specified in this DPA and the Agreement.
6. Where Sub-processors Process the Personal Information of Customer contacts, Revinate takes steps to ensure that such Sub-processors are Service Providers under US Data Protection Law with whom Revinate has entered into a written contract that includes terms substantially similar to this Section of Annex C or are otherwise exempt from the CCPA's definition of "sale". Revinate conducts appropriate due diligence on its Sub-processors.
7. Revinate shall not Sell or Share (as defined in US Data Protection Laws), disclose, release, transfer, make available or otherwise communicate any Customer Data to another business or third party without Customer's prior written consent unless and to the extent that such disclosure is made to a Sub-processor for a business purpose. Notwithstanding the foregoing, nothing in this DPA shall restrict Revinate's ability to disclose Customer Data to comply with applicable laws; provided that if such disclosure is required, Revinate will promptly notify Customer of the request for disclosure unless such notification is prohibited by applicable law or a legally binding order.

Canada:

1. Revinate takes steps to ensure that Revinate's Sub-processors, as described in Section 3 (Sub-processing) of the DPA, are third parties under PIPEDA, with whom Revinate has entered into a written contract that includes terms substantially similar to this DPA. Revinate conducts appropriate due diligence on its Sub-processors.
2. Revinate will implement technical and organizational measures as set forth in Section 4 (Security) of the DPA.