

## **DATA PROTECTION ADDENDUM**

This Data Protection Addendum (“DPA”) supplements the agreement (the “Agreement”) between your firm (referred to herein as “Customer”) and Orion Advisor Solutions, Inc. (“OAS”), in which OAS and/or its Affiliates (including, without limitation, Orion Advisor Technology, LLC, BasisCode Compliance LLC (dba Orion Compliance), Advizr, Inc. (dba Orion Planning), GxWorks, LLC (dba Orion Risk Intelligence), Summit Wealth Systems, Inc., and Redtail Technology, Inc., collectively “Orion”) are providing you with the services (“Services”) set forth in such agreement. Customer and Orion may be referred to in this DPA collectively as the “Parties” or individually as a “Party.”

By signing the Agreement, Customer enters into this DPA on behalf of itself and its Authorized Affiliates. This DPA is binding on the Parties only to the extent applicable Data Protection Laws govern the Processing of Customer Personal Data in performance of the Services. This DPA is fully incorporated into and made a part of the Agreement. This DPA replaces any previously agreed-to or otherwise existing terms, exhibits, schedules, appendices, addendums, or other attachments related to the Processing of Customer Personal Data unless otherwise expressly stated in this DPA. In the event of any inconsistency between the terms of this DPA and any terms of the Agreement with respect to the Processing of Customer Personal Data, the terms of this DPA will govern and control.

Capitalized terms used but not otherwise defined in this DPA have the same meanings as set out in the Agreement.

### **I. Definitions**

“Affiliate” means, with respect to Orion or Customer, any legal entity directly or indirectly controlling, controlled by or under common control with such subject entity.

“Authorized Affiliates” means any of Customer’s Affiliate(s) that are (a) permitted to use the Service pursuant to the Agreement and are not “Customer” (or such substantially equivalent term) as defined under the Agreement or this DPA or (b) directly or indirectly controlling, controlled by or under common control with a subject entity.

“CCPA” means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018), as the same may be supplemented or amended, including the California Privacy Rights Act of 2020 and any implementing regulations, as may be amended or superseded from time to time (“CPRA”). The terms “business,” “consumer,” “personal information,” and “service provider” shall have meaning under CCPA.

“Customer Personal Data” means any “personal information,” including sensitive personal information (as such terms are defined under applicable Data Protection Laws) relating to a Data Subject that is subject to protection under applicable Data Protection Laws and which is shared with Orion by the Customer for the purposes of performing the services set forth in the Agreement.

“Data Controller” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Processor” means the entity which Processes Personal Data on behalf of the Data Controller.

“Data Protection Laws” means any applicable laws and regulations relating to data the Processing of Personal Data in question under the Agreement, including (where applicable) the General Data Protection Regulation (“GDPR”), the United Kingdom General Data Protection Regulation (“UK GDPR”), the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”), the Australian Privacy Act of 1988, Switzerland’s Federal Act on Data Protection, the CCPA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, the Texas Data Privacy and Security Act, and the Oregon Consumer Privacy Act.

“Data Subject” means the identified or identifiable natural person to which the Personal Data relates.

“Personal Data” or “Personal Information” means any information relating to a Data Subject and is protected as personal data, including the terms “personally identifiable information,” or “nonpublic personal information” under applicable Data Protection Laws.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Sub-Processor” means any Processor engaged by Orion or its Affiliates to Process Personal Data on Orion’s or its Affiliates’ behalf. As used herein, Sub-Processor does not include third-party integration partners and/or service providers that the Customer uses to Process, and/or provides access to, Personal Data held in Orion systems or databases (“Customer Engaged Processors”).

## **II. Roles, Responsibilities, and Representations Regarding Personal Data**

### *A. Party Roles.*

1. To the extent Orion Processes Customer Personal Data in performance of the Services, the Parties agree that Customer is the Data Controller (or a Data Processor conveying direction on behalf of the ultimate Data Controller), and Orion is the Data Processor acting on behalf and at the direction of Customer.
2. With respect to Customer Personal Data subject to CCPA, when Processing Customer Personal Data in accordance with Customer’s instructions, the parties acknowledge and agree that Customer is a Business and Orion is a Service Provider, as those terms are defined in CCPA.

### *B. Orion Responsibilities.*

1. Orion shall Process the Personal Data in connection with its Services only on documented instructions from Customer, unless otherwise required by applicable Data Protection Laws.
2. Orion shall ensure that personnel authorized by Orion to Process Customer Personal Data have committed themselves to confidentiality.
3. To the extent required by applicable Data Protection Laws, Orion will immediately inform Customer if, in Orion’s opinion based on the information available to Orion, any Customer instruction would violate applicable Data Protection Laws.

4. Customer may request amendments to Customer's instructions, where such amendments are required to ensure that Customer complies with applicable Data Protection Laws and Customer cannot achieve Customer's compliance with applicable Data Protection Laws unless Orion implements such instructions ("Modified Instructions"). If Orion notifies Customer that it is infeasible or impracticable to implement any Modified Instructions, Customer may terminate the applicable Service by providing Orion with written notice within thirty (30) days of Orion's notification.

5. If Orion receives a valid request or legal process (such as a subpoena or court order) for Customer Personal Data, Orion will attempt to redirect the governmental entity or third-party requester to request Customer Personal Data directly from Customer. If compelled to disclose Customer Personal Data to a governmental entity or third party requester, then Orion will give (to the extent legally permissible) Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Orion is legally prohibited from doing so.

6. With respect to Customer Personal Data subject to CCPA, Orion will Process Customer Personal Data as a Service Provider strictly for the purpose of performing the Services under the Agreement (the "Business Purpose"). Consistent with our privacy policy, Orion will not (a) sell or share (as such terms are defined under the CCPA) the relevant Customer Personal Data; (b) retain, use, or disclose the relevant Customer Personal Data for a commercial purpose other than to perform the Business Purpose specified in this Addendum or as otherwise permitted by the CCPA; or (c) retain, use, or disclose the relevant Customer Personal Data outside of the direct business relationship between Customer and Orion, such as by combining or updating Customer Personal Data, unless expressly permitted by the CCPA.

7. With respect to Customer Personal Data subject to CCPA, the limited and specified Business Purposes for which Orion will Process Customer Personal Data include: (i) performing Services on behalf of Customer including maintaining or servicing client database(s) and performing ancillary services, or enabling Customer to utilize ancillary services in connection therewith (including the preparation of performance evaluations, calculation of billing and advisory fees, the maintenance of investment models, and similar activities), providing customer service, processing or fulfilling orders and transactions, processing payments, or providing any of the following: compliance, analytics Services, storage, or similar Services on behalf of Customer; (ii) assisting to ensure security and integrity to the extent the use of the consumer's Personal Data is reasonably necessary and proportionate for these purposes; (iii) short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with Customer, provided that the consumer's Personal Data is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with Customer; (iv) de-bugging to identify and repair errors that impair existing intended functionality; (v) undertaking activities to verify or maintain the quality or safety of a service or device that is owned or controlled by Customer, and to improve, upgrade, or enhance the service or device that is owned or controlled by Customer; (vi) undertaking internal research for technological development; or (vii) providing advertising and marketing Services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider shall not combine the Personal Data of an opted-out consumer that the service provider receives from, or on behalf of, another person, or collection from its own interaction with consumers.

### *C. Customer Responsibilities.*

1. Customer shall: (i) ensure the ongoing accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data; (ii) comply with all necessary

transparency and lawfulness requirements under applicable Data Protection Law for the collection and use of Customer Personal Data, including, but not limited to, obtaining any necessary consents and authorizations from Data Subjects; (iii) ensure it has the right to transfer, or provide access to, Customer Personal Data to Orion for Processing in accordance with the terms of the Agreement (including this DPA); and (iv) ensure that its instructions to Orion regarding the Processing of Personal Data are lawful and comply with, and do not cause Orion to violate, applicable laws, including the Data Protection Laws. Customer shall promptly inform Orion if any of the foregoing representations are no longer accurate.

2. Customer acknowledges and agrees that Orion does not have a means to verify any of the following: (i) the residency of each Data Subject, (ii) specific data identifiers that are provided to Orion by Customer in connection with each request by Customer to Process such Customer Personal Data, nor (iii) the location of third parties that Customer chooses to exchange Customer Personal Data through the Service. Accordingly, it shall be sole the responsibility of the Customer to identify and verify, as necessary, the relevant Data Protection Law(s) that may apply to such Customer Personal Data.

3. With respect to Customer Personal Data subject to CCPA, Customer acknowledges that its use of the Services will not violate the rights of any individual to whom such Customer Personal Data relates that has opted-out from sales or other disclosures of Personal Information, to the extent applicable under the CCPA.

### **III. Data Subject Requests**

A. Orion will promptly notify Customer if Orion receives a request from a Data Subject to exercise his or her rights under applicable Data Protection Laws with respect to Customer Personal Data (“Data Subject Requests”). Customer shall be solely responsible for responding to any such Data Subject Requests or communications involving Customer Personal Data.

B. Orion will provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Personal Data, which Customer may use to assist it in connection with its obligations under Data Protection Laws. To the extent Customer is unable to independently address a Data Subject Request through the Service, then upon Customer’s written request Orion shall, to the extent legally required, provide reasonable assistance to Customer to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. At Orion’s request, Customer shall reimburse Orion for the commercially reasonable costs arising from this assistance.

### **IV. Security**

Both parties shall maintain appropriate technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

### **V. Personal Data Incidents**

In accordance with applicable Data Protection Laws, each party shall notify the other party, without undue delay and as soon as reasonably possible, upon becoming aware (but not later than 72 hours after becoming aware) of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data maintained and Processed in Orion’s systems (a “Personal Data Incident”). Each party shall make reasonable efforts to identify the cause of a Personal

Data Incident and take those steps as deemed necessary and reasonable in order to remediate the cause of such Personal Data Incident, to the extent that the remediation is within such party's reasonable control. Orion's obligations set forth herein shall not apply to Personal Data Incidents that are caused directly or indirectly by Customer or a non-Orion Processor engaged by Customer.

## **VI. Retention, Return, and Deletion of Personal Data**

During the term of the Agreement, Orion will provide Customer with the capability to obtain a copy of Customer Personal Data Processed by Orion and in Orion's possession, as set forth in the Agreement. Unless otherwise required or contemplated by the Services, as set forth in the Agreement, upon termination of the Agreement, Orion will within one (1) year securely delete, return, or provide Customer with a commonly-used, structured, electronic, and machine-readable format and allow Customer to obtain a copy of or delete all Customer Personal Data. All such copies of the Customer Personal Data shall be provided to Customer in accordance with the specific provisions set forth in the Agreement. Notwithstanding anything to the contrary herein, Orion may retain copies of Personal Data as necessary to comply with legal, regulatory, judicial, audit, or internal compliance requirements for as long as required to achieve the processing purpose for which the Personal Data was collected, in accordance with applicable Data Protection Laws.

## **VII. Audits**

If required by applicable Data Protection Laws, Orion shall make available to Customer (upon its written request), any applicable information reasonably necessary to demonstrate compliance with applicable Data Protection Laws. Upon thirty (30) days written notice from Customer, Orion shall allow for audits, including inspections, conducted by Customer or another reputable auditor selected by Customer and reasonably approved by Orion, provided that Customer shall not exercise this right more than once per calendar year, unless necessary to comply with governmental or regulatory requirements.

## **VIII. Sub-Processors**

Customer authorizes and agrees that (a) Orion's Affiliates may be retained as Sub-Processors; and (b) Orion and Orion's Affiliates respectively may engage third-party Sub-Processors in connection with Orion's performance of the Agreement, each as detailed at <https://orion.com/subprocessors>.

1. If and to the extent Orion engages third-party Sub-Processors to Process Customer Personal Data on Orion's behalf, Orion will impose data protection terms on those Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. Orion will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Orion to breach any of its obligations under this DPA, except as otherwise set forth in the Agreement.

2. Orion will provide electronic notification of a new third-party Sub-Processor to be engaged solely by Orion. Customer agrees to register at <https://orion.com/subprocessors> to receive any such electronic notifications and to review any updates. Customer may object to Orion's engagement of such new Sub-Processor by notifying Orion in writing within ten (10) business days after receipt of Orion's notification. In the event Customer objects to a new Sub-Processor, the parties will work in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Orion will, at its sole discretion, choose to either not appoint the new Sub-Processor, or permit Customer to suspend or

terminate the affected portion of the Services to be performed by such new Sub-Processor with respect only to those aspects which cannot be provided by Orion without the use of the objected-to new Sub-Processor by providing written notice to Orion.

3. Notwithstanding anything herein to the contrary, Orion shall not be responsible for Customer Engaged Processors or other third-party Processors engaged by Customer, and the Customer is solely responsible for ensuring such Customer Engaged Processors and third-party Processors comply with applicable Data Protection Laws.

#### **IX. Authorized Affiliates**

A. The parties agree that, by executing the DPA, Customer enters into the DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Orion and each such Authorized Affiliate. Each Authorized Affiliate shall be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, all access and use of the Services by Authorized Affiliate(s) shall comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Customer.

B. Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under applicable Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Orion directly by itself.

C. Customer represents and warrants that Authorized Affiliates may access Customer Personal Data, and any instructions received from Authorized Affiliates will be treated by Orion as if they come from Customer, except in such case as Orion receives potentially contradictory instructions from Customer and Authorized Affiliate, in which case Orion will implement instructions from Customer.

#### **X. Data Protection Impact Assessments and Consultation with Supervisory Authorities**

To the extent that information is reasonably available to Orion, and Customer does not otherwise have access to the required information, Orion will provide reasonable assistance to Customer with any data protection impact assessments and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by Data Protection Laws.

#### **XI. Cross-Border Data Transfers**

A. Customer acknowledges that in connection with the performance of the Services by Orion, Orion may be a recipient of Customer Personal Data from residents of countries outside of the United States, if so directed by Customer. Orion and its Affiliates are based in the U.S. If Customer engages directly with U.S. companies for products and services, transfers of Customer Personal Data may be made as necessary for the performance of our contract with Customer or the implementation of pre-contractual measures taken at Customer's request or, as circumstances may require, Customer's consent.

B. Orion endeavors to keep Customer Personal Data in the jurisdiction where it was collected, but for some services and in some circumstances, Orion may need to transfer Customer Personal Data to other jurisdictions or receive Personal Data from Customer in other jurisdictions. In those situations, Orion shall not transfer Personal Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data unless it takes such measures as necessary to ensure the transfer is in compliance with applicable Data Protection Laws. Such measures may include, without limitation,

transferring such data to a recipient that has implemented binding corporate rules in accordance with applicable Data Protection Laws or to a recipient that has executed appropriate EU Standard Contractual Clauses adopted or approved by the European Commission. Where necessitated by Data Protection Law, a transfer of Customer Personal Data shall be conducted pursuant to the EU Standard Contractual Clauses.

C. Where Customer, as a Data Controller or a Data Processor acting on behalf or at the direction of a Data Controller, transfers or directs the transfer of Customer Personal Data from the European Union to Orion, as Data Processor, in the United States, the Parties agree to be deemed executed by the Parties and incorporated into this DPA the EU Standard Contractual Clauses, as follows:

- a. Incorporate the language/provisions of the EU Standard Contractual Clauses under Module Two: Transfer controller to processor or, if applicable, Module Three: Transfer processor to processor;
- b. Customer shall be the “Data Exporter” and Orion shall be the “Data Importer” under both Module Two and Module Three;
- c. With respect to Clause 7, the Parties choose not to include the optional docking clause;
- d. With respect to Clause 11, the Parties choose not to include the optional language relating to the use of independent dispute resolution body;
- e. With respect to Clause 9, the data importer has the data exporter’s general authorization to engage sub-processors from the list in Annex III, which list may be amended from time to time by Orion with 5 business days advanced notice to Customer (as provided in Section VIII above);
- f. With respect to Clause 13 and Annex I.C, the competent Data Protection Authority is Republic of Ireland;
- g. With respect to Clause 17, the EU Standard Contractual Clauses shall be governed by the laws of Republic of Ireland;
- h. With respect to Annex I.A of the Appendix, the Name and Contact Information of the Controller shall be that of the Customer as set forth in the Agreement or other relevant documentation, and the Name and Contact Information of the Processor shall be that of Orion as set forth in the Agreement or other relevant documentation.

The Personal Data Processing activities in Annex I to the Appendix to the EU Standard Contractual Clauses will be such activities as necessary for Orion to perform the Services for Customer, as fully described in the Agreement. The categories of Data Subjects and categories of Personal Data in Annex I to the EU Standard Contractual Clauses will be those provided by Customer to Orion pursuant to the Services as set forth in Agreement and this DPA. The data security measures in Annex II to the EU Standard Contractual Clauses will be those identified in Annex II to the Appendix (Information Security Program) of this DPA. The list of appointed Sub-Processors will be identified in Annex III to the Appendix, as updated from time to time pursuant to Section VIII hereof.

D. Where Customer, as a Data Controller or a Data Processor acting on behalf or at the direction of a Data Controller, transfers or directs the transfer of Customer Personal Data from the United Kingdom to Orion, as Data Processor, in the United States, the Parties agree to be bound by and incorporate to this DPA and the EU Standard Contractual Clauses by reference any additional modifications and amendments required by the UK Transfer Addendum. The information set forth in the Agreement and the Annexes shall be used to complete Parts 1 and 3 of the UK Transfer Addendum. In accordance with Section 19 of the UK Transfer Addendum, neither the data exporter or data importer may terminate the UK Transfer Addendum for convenience.

E. Where Customer, as a Data Controller or a Data Processor acting on behalf or at the direction of a Data Controller, transfers or directs the transfer of Customer Personal Data from Switzerland to Orion, as Data Processor, in the United States, the EU Standard Contractual Clauses as set forth in paragraph C above,

will apply to the transfer in a manner compliant with the Federal Act on Data Protection.

## **XII. General Provisions**

A. *Precedence.* This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. Except as specifically set forth in this DPA, the terms of the underlying Agreement shall remain unmodified and in full force and effect. In the event of a conflict between the terms of the Agreement and the terms of this DPA, the terms of this DPA shall prevail.

B. *Amendments.* This DPA may be updated by Orion from time to time as reasonably required in accordance with Data Protection Laws following notice to Customer. Customer's continued use of the services pursuant to the Agreement shall signify acceptance of such revised terms.

C. *Severability.* If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

## **APPENDIX**

### **ANNEX I: DESCRIPTION OF THE PROCESSING**

#### **A. LIST OF PARTIES**

Data exporter: The name and contact information of the Data Exporter shall be that of the Customer, as set forth in the Agreement or other relevant documentation.

Data importer: The name and contact information of the Data Importer shall be that of Orion, as set forth in the Agreement or other relevant documentation.

#### **B. DESCRIPTION OF TRANSFER**

The Personal Data Processing activities will be such activities as necessary for Orion to perform the Services for Customer, as described in the Agreement. The categories of Data Subjects and categories of Personal Data will be provided by Customer to Orion pursuant to the Services as set forth in the Agreement.

#### **C. COMPETENT SUPERVISORY AUTHORITY**

In accordance with Clause 13, the competent supervisory authority is the Republic of Ireland.

## **ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

*Description of the technical and organizational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data.*

All data, including personal data, is encrypted while at rest and in transit. Wherever possible, information is redacted to remove personal data. For data at rest, Orion encrypts the data at AES-256. For data in transit, Orion encrypts the data at TLS 1.2 and above.

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.*

Orion processing systems and services are implemented and managed in accordance with NIST guidance and ISO 27001 requirements to ensure confidentiality, integrity and availability.

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.*

Orion has a BCP/DR plan in place to ensure our system resiliency and availability and access to personal data. These plans are tested at least annually to ensure they provide the desired physical and technical redundancies and meet Recovery Time and Recovery Point Objectives.

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.*

Orion performs both internal and independent third party testing on a continuing basis to ensure the effectiveness of technical and organizational controls with regard to the confidentiality, availability and integrity of systems and processing.

*Measures for user identification and authorization.*

Orion uses appropriate identification access management methods to determine user identification and authorization of all our system users.

*Measures for the protection of data during transmission.*

All data, including personal data, is encrypted at rest and in transit. Wherever possible, information is redacted to remove personal data.

*Measures for the protection of data during storage.*

All data, including personal data, is encrypted at rest and in transit. Wherever possible, information is redacted to remove personal data.

*Measures for ensuring physical security of locations at which personal data are processed.*

Appropriate processes and controls are in place to ensure the security of personal data stored at physical locations. Controls are reviewed and validated both internally and by independent third parties on at least an annual basis.

*Measures for ensuring events logging.*

Orion uses commercially available solutions for log aggregation of all critical systems. Information Security team members regularly use and confirm that events are logged within these solutions.

*Measures for ensuring system configuration, including default configuration.*

Orion has policy on baseline images for systems. The policy also dictates that Information Security notification and approval is required to build a system outside of the baseline image.

*Measures for internal IT and IT security governance and management.*

Orion follows NIST guidance and the ISO framework to govern internal information security policy. This policy and framework undergoes an annual internal audit and an annual 3<sup>rd</sup> party external audit. Our ISO certificate is available online or by request.

*Measures for certification/assurance of processes and products.*

Orion maintains an ISO certification to assure we are complying with the ISMS and ISO standards.

*Measures for ensuring data minimisation.*

Wherever possible, information is redacted to remove personal data. Only required data is collected and stored.

*Measures for ensuring data quality.*

Appropriate processes and controls are in place to ensure the confidentiality, availability and integrity of data. Data quality validation takes place on a continuing basis.

*Measures for ensuring limited data retention.*

Orion retains Customer data during the term of the Agreement. Following the expiration or termination of the Agreement, Orion will within one (1) year securely delete, return, or provide Customer with a commonly-used, structured, electronic, and machine-readable format and allow Customer to obtain a copy of or delete all Customer Personal Data. All such copies of the Customer Personal Data shall be provided to Customer in accordance with the specific provisions set forth in the Agreement. Active Customer databases are not retained by Orion following termination of the Agreement, but rather are archived within a reasonable time period following the expiration or termination of the Agreement. Orion may retain copies of Personal Data as necessary to comply with legal, regulatory, judicial, audit, or internal compliance requirements for as long as required to achieve the processing purpose for which the Personal Data was collected, in accordance with applicable Data Protection Laws.

*Measures for ensuring accountability.*

Orion uses appropriate identification access management methods to determine user identification and authorization of all our system users.

Any detected incidents of non-compliance are logged and appropriate enforcement actions are taken.

*Measures for allowing data portability and ensuring erasure.*

Orion will comply with authorized requests to amend, transfer, or delete personal information in a timely manner. Orion has comprehensive data destruction policies and processes in place, and reviews and tests such policies and processes on a regular basis.

*For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller.*

*Description of the specific technical and organizational measures to be taken by the processor to be able to provide assistance to the controller.*

Orion contractually requires its sub-processors to maintain substantially similar technical and organizational measures to those described above.

**ANNEX III: LIST OF SUB-PROCESSORS****Authorized Third-Party Sub-Processors**

<u>Subprocessor</u>	<u>Category</u>	<u>Location</u>
<u>6sense</u>	<u>Customer Engagement and Marketing Analytics</u>	<u>United States</u>
<u>Amazon Web Services</u>	<u>Hosting, computing, storage, and other application services</u>	<u>United States</u>
<u>Amazon Web Services (Amazon Bedrock)</u>	<u>AI model provider for certain services and/or features that utilize generative artificial intelligence. The AI models available to Orion through the Amazon Bedrock service can be found <a href="#">here</a>.</u>	<u>United States</u>
<u>Confluent</u>	<u>Data streaming services</u>	<u>United States</u>
<u>Conga Composer</u>	<u>Document generation tool</u>	<u>United States</u>
<u>DataBricks</u>	<u>ETL Tool</u>	<u>United States</u>
<u>Datadog, Inc.</u>	<u>Observability and monitoring platform for logs, usage data, and troubleshooting</u>	<u>United States</u>
<u>Fiserv, Inc.</u>	<u>Payment processing</u>	<u>United States</u>
<u>Flyer Financial Technologies</u>	<u>Cloud-based trading provider</u>	<u>United States</u>
<u>Fullstory, Inc.</u>	<u>Session replay and usage analytics to support customer service, troubleshooting, and issue resolution</u>	<u>United States</u>
<u>Gainsight</u>	<u>In-application communications service</u>	<u>United States</u>
<u>Glia</u>	<u>Digital communications provider</u>	<u>United States</u>
<u>Global Relay</u>	<u>Compliance books &amp; records</u>	<u>United States</u>
<u>HighSpot</u>	<u>Sales enablement and content management platform</u>	<u>United States</u>
<u>Iron Mountain</u>	<u>Data backup &amp; storage</u>	<u>United States</u>
<u>LearnUpon Limited</u>	<u>Education tool platform</u>	<u>United States</u>
<u>Microsoft Corporation</u>	<u>Hosting, email, and data storage provider, MFA</u>	<u>United States</u>

<u>Momentive.io</u>	<u>Survey tool</u>	<u>United States</u>
<u>Nylas</u>	<u>Email, calendar, and contact sync technology provider</u>	<u>United States</u>
<u>Okta Inc.</u>	<u>Identity and access management provider for authentication and authorization</u>	<u>United States</u>
<u>OwnBackup</u>	<u>Data backup &amp; storage</u>	<u>United States</u>
<u>Pendo.io, Inc.</u>	<u>In-app guide platform and product usage analytics to support onboarding, feature adoption, and user engagement</u>	<u>United States</u>
<u>Proofpoint</u>	<u>Email security</u>	<u>United States</u>
<u>Salesforce</u>	<u>Cloud-based customer CRM</u>	<u>United States</u>
<u>Sisense</u>	<u>Business analytics</u>	<u>United States</u>
<u>Smartsheet</u>	<u>Work management platform</u>	<u>United States</u>
<u>Tata Consultancy Services Limited</u>	<u>Data Reconciliation Operations; Client Support; QA; Devops; and Business Intelligence functions</u>	<u>India</u>
<u>Twilio</u>	<u>Multi-factor authentication and messaging</u>	<u>United States</u>
<u>UiPath, Inc.</u>	<u>Robotic process automation platform provider</u>	<u>United States</u>
<u>Workday</u>	<u>Cloud-based employee and accounting CRM; supplier sourcing/procurement workflows</u>	<u>United States</u>

### **Authorized Orion Affiliates**

<u>Affiliate</u>	<u>Category</u>	<u>Location</u>
<u>Orion Advisor Technology, LLC</u>	Provision of technical services, support services, and supporting the provision, management, and maintenance of the Services.	<u>United States</u>
<u>BasisCode Compliance LLC (dba Orion Compliance)</u>		<u>United States</u>
<u>Advizr, Inc. (dba Orion Planning)</u>		<u>United States</u>

GxWorks, LLC (dba  
Orion Risk  
Intelligence)

United States

Redtail Technology,  
Inc.

United States

Summit Wealth  
Systems, Inc.

United States