kinective

Data Processing Addendum (DPA)

This Data Processing Addendum ("DPA") forms part of, and is incorporated into, the Master Services Agreement or other written agreement (the "Agreement") between Cash Flow Management, LLC. ("Kinective" or "Company") and the customer identified in the signature block below ("Customer") for the provision of Kinective's financial technology services and platform (the "Services"). This DPA reflects the parties' agreement with respect to the Processing of Customer Personal Data.

In the event of any conflict or inconsistency between the terms of this DPA and the Agreement, the terms of this DPA shall control with respect to data protection matters. The terms of any applicable Standard Contractual Clauses shall prevail over any conflicting terms in this DPA.

By executing the Agreement or this DPA, Customer and Kinective agree to be bound by the terms of this DPA.

EFFECTIVE DATE

This DPA is effective as of the date the Agreement is executed or, if executed separately, the date of last signature below ("Effective Date").

1. Definitions

For purposes of this DPA, the following capitalized terms shall have the meanings set forth below. Capitalized terms not defined herein have the meanings given in the Agreement or applicable Data Protection Laws.

- **"Authorized Subprocessor"** means a third-party entity, including Kinective's subsidiaries, affiliates, contractors, and subcontractors, authorized by Kinective to Process Customer Personal Data in connection with the provision of the Services, as listed in Appendix B to this DPA.
- **"CCPA"** means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 ("CPRA"), and all implementing regulations thereunder.
- **"Controller"** means the entity that determines the purposes and means of the Processing of Personal Data.
- **"Customer Personal Data"** means any Personal Data that Kinective Processes on behalf of Customer in the course of providing the Services under the Agreement.
- **"Data Breach"** means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Customer Personal Data transmitted, stored, or otherwise Processed by Kinective or its Authorized Subprocessors.
- **"Data Protection Laws"** means all applicable laws and regulations governing the Processing of Personal Data, including without limitation: (i) the Gramm-Leach-Bliley Act ("GLBA") and implementing regulations; (ii) applicable U.S. state privacy laws including the CCPA/CPRA; (iii) the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"); (iv) the UK GDPR and Data Protection Act 2018; (v) India's Digital Personal Data Protection Act 2023 ("DPDPA"); (vi) applicable Philippine data protection laws including Republic Act No. 10173 (Data Privacy Act of 2012) ("DPA Philippines"); and (vii) all other applicable national, federal, state, and local privacy and data protection laws, in each case as amended or superseded from time to time.
- **"Data Subject"** means the identified or identifiable natural person to whom Personal Data relates.
- **"FFIEC Guidelines"** means the Federal Financial Institutions Examination Council examination guidelines, including the IT Examination Handbook, as updated from time to time.
- **"GLBA"** means the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., and all implementing regulations, including the FTC Safeguards Rule (16 C.F.R. Part 314) and applicable banking agency regulations.

- **"Nonpublic Personal Information ("NPI")"** has the meaning set forth in the GLBA and applicable implementing regulations, and includes personally identifiable financial information and any list, description, or other grouping of consumers derived using such information.
- **"Personal Data"** means any information relating to an identified or identifiable natural person, and includes NPI and any other information that constitutes "personal data," "personal information," or "personally identifiable information" under applicable Data Protection Laws.
- **"Processing"** means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.
- **"Processor"** means the entity that Processes Personal Data on behalf of the Controller, including as applicable a "service provider" as defined under the CCPA.
- **"Restricted Transfer"** means any transfer of Customer Personal Data from a jurisdiction that restricts cross-border data transfers to a country or territory that has not received an adequacy determination under applicable Data Protection Laws.
- **"Standard Contractual Clauses ("SCCs")"** means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or superseded.
- **"Supervisory Authority"** means the competent regulatory authority responsible for overseeing compliance with applicable Data Protection Laws in a given jurisdiction.

2. Roles and Responsibilities

The parties acknowledge and agree that with respect to the Processing of Customer Personal Data under this DPA:

- Customer is the Controller (or, where Customer itself acts as a processor on behalf of its own clients, a Processor) of Customer Personal Data.
- Kinective is the Processor of Customer Personal Data and shall Process Customer Personal Data only on behalf of, and in accordance with the documented instructions of, Customer.
- With respect to the CCPA, Customer is a "Business" and Kinective is a "Service Provider" as those terms are defined under the CCPA with respect to Customer Personal Data.
- With respect to the GLBA, Kinective acknowledges its status as a service provider to Customer and its obligations as a nonaffiliated third party receiving NPI pursuant to applicable GLBA implementing regulations.

3. Scope and Purpose of Processing

Kinective shall Process Customer Personal Data solely: (i) to perform the Services and fulfill its obligations under the Agreement; (ii) in accordance with Customer's documented instructions as set forth in the Agreement and this DPA; (iii) as required by applicable law, in which case Kinective shall promptly notify Customer of such legal requirement prior to Processing (unless prohibited by law); and (iv) as otherwise expressly authorized in writing by Customer.

Kinective shall not: (a) sell Customer Personal Data; (b) retain, use, or disclose Customer Personal Data for any purpose other than performing the Services; (c) combine Customer Personal Data with personal data collected from other sources except as expressly permitted under the Agreement; or (d) Process Customer Personal Data outside the scope of this DPA without Customer's prior written consent.

The subject matter, nature, purpose, duration, categories of Personal Data Processed, and categories of Data Subjects are described in Appendix A (Description of Processing) to this DPA.

4. Customer Instructions

Customer's instructions to Kinective for the Processing of Customer Personal Data consist of: (i) the terms of this DPA and the Agreement; (ii) Customer's configuration and use of the Services; and (iii) any additional written

Processing instructions that Customer provides to Kinective and that Kinective expressly acknowledges and agrees to in writing.

If Kinective reasonably believes that any Customer instruction violates applicable Data Protection Laws, Kinective shall promptly notify Customer. Kinective shall not be required to follow any instruction that would cause it to violate applicable law. The parties shall cooperate in good faith to resolve any such issue.

5. Kinective's Data Protection Obligations

5.1 Confidentiality and Access Limitation

Kinective shall ensure that access to Customer Personal Data is limited to personnel who: (i) have a legitimate need to access such data to perform the Services; (ii) are bound by written confidentiality obligations no less protective than those in the Agreement; and (iii) have received appropriate data protection and information security training. Kinective shall ensure that such confidentiality obligations survive termination of employment or engagement.

5.2 GLBA Safeguards Program

Given that Customer Personal Data may include NPI subject to the GLBA, Kinective shall maintain a comprehensive information security program that complies with the GLBA Safeguards Rule (16 C.F.R. Part 314) and applicable banking agency regulations. Such program shall include, at minimum:

- Designation of a qualified individual responsible for overseeing and implementing Kinective's information security program;
- Risk-based administrative, technical, and physical safeguards appropriate to the size, complexity, and sensitivity of the NPI Processed;
- Regular risk assessments and penetration testing;
- Encryption of NPI in transit and at rest;
- Multi-factor authentication for systems that access NPI;
- A written incident response plan; and
- Annual review and testing of the information security program.

5.3 Technical and Organizational Security Measures

In addition to the GLBA Safeguards Program, Kinective shall implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, alteration, or disclosure as found at www.kinective.io/msa-information-security-and-privacy-standards,. Such measures shall include those described in Appendix C (Security Measures) to this DPA and shall be appropriate to the risks presented by the Processing, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing.

5.4 Regulatory Compliance — Financial Services

Kinective acknowledges that Customer operates as a regulated financial institution subject to oversight by federal and state banking regulators, including the OCC, FDIC, Federal Reserve, NCUA, and applicable state agencies. Kinective shall:

- Cooperate with Customer's regulatory examination and oversight activities;
- Maintain policies and procedures designed to satisfy FFIEC Guidelines applicable to third-party service providers;
- Promptly notify Customer of any regulatory inquiry, examination, or enforcement action that relates to or could affect the Services or the Processing of Customer Personal Data;
- To the extent applicable to the specific Service, maintain SOC 2 Type II certification (or equivalent) and provide Customer with copies of such reports upon written request; and
- Cooperate with Customer's third-party risk management program.

6. Subprocessors and Cross-Border Data Transfers

6.1 Appointment of Subprocessors

Customer acknowledges and agrees that Kinective may engage Authorized Subprocessors to Process Customer Personal Data in connection with the provision of the Services. Kinective's current Authorized Subprocessors, including its India development/engineering operations and Philippine customer support subcontractors, are listed in Appendix B to this DPA.

Kinective shall: (i) enter into a written agreement with each Authorized Subprocessor that imposes data protection obligations at least as protective as those in this DPA; (ii) remain liable for the acts and omissions of its Authorized Subprocessors to the same extent Kinective would be liable if performing the services directly; and (iii) restrict each Authorized Subprocessor's access to Customer Personal Data to only that which is necessary to perform the specific subprocessing activities.

6.2 Notification of New Subprocessors

Before appointment of any new Subprocessor or materially changing the role of an existing Subprocessor, Kinective shall provide Customer with at least thirty (30) days' prior written notice including via the product/services, or by updating our website. If Customer does not object to the appointment of any new Subprocessor within thirty (30) days after notification of such appointment by Kinective, Customer will be deemed as having provided its consent to the new appointment. Should Customer object (acting reasonably) to a new Subprocessor, upon prior written notice, Kinective will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Customer Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If Kinective is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the specific affected Services upon written notice, and Kinective shall refund any prepaid fees for the terminated Services prorated from the termination date.

6.3 India Operations — Development, Engineering, and Testing

Customer acknowledges that Kinective employs development, engineering, and quality assurance personnel in India who may, in the course of their duties, have occasional access to Customer Personal Data. With respect to such Processing:

- Access to Customer Personal Data by India-based personnel shall be on a need-to-know basis only, and shall be subject to role-based access controls and logging;
- India-based personnel are subject to Kinective's global information security policies and written confidentiality obligations;
- To the extent required by applicable Data Protection Laws, Kinective shall implement appropriate transfer mechanisms (including SCCs where applicable) for the transfer of Customer Personal Data to India; and
- Kinective shall comply with India's Digital Personal Data Protection Act 2023 (DPDPA) and applicable implementing regulations with respect to Customer Personal Data Processed in India.

6.4 Philippines Operations — Customer Support Subcontractors

Customer acknowledges that Kinective engages subcontractors in the Philippines who provide customer support services and may have occasional access to Customer Personal Data. With respect to such Processing:

- Philippine-based subcontractors shall access Customer Personal Data only as necessary to respond to customer support requests and shall not retain, copy, or use such data for any other purpose;
- Philippine-based subcontractors are bound by written data processing agreements that comply with this DPA and the Philippines Data Privacy Act of 2012 (Republic Act No. 10173) and its implementing rules;
- Kinective shall be fully liable for the acts and omissions of its Philippine-based subcontractors with respect to Customer Personal Data; and
- Kinective shall implement appropriate transfer mechanisms for any transfer of Customer Personal Data to the Philippines as required by applicable Data Protection Laws.

6.5 Cross-Border Transfer Mechanisms

Where the transfer of Customer Personal Data from the United States or another jurisdiction to Kinective's India or Philippine operations (or any other third country) constitutes a Restricted Transfer under applicable Data Protection Laws, the parties shall implement one or more of the following transfer mechanisms as appropriate:

- Standard Contractual Clauses (EU SCCs), as incorporated by reference into this DPA for transfers subject to the GDPR or UK GDPR;
- The UK International Data Transfer Addendum (UK IDTA) for transfers from the United Kingdom;
- Such other mechanisms as may be recognized under applicable Data Protection Laws as providing adequate safeguards for the transfer of Personal Data; or
- Consent of the Data Subject where permitted under applicable law.

The applicable SCCs (where required) are incorporated by reference into this DPA. For transfers subject to EU GDPR, Module 2 (Controller to Processor) or Module 3 (Processor to Processor) shall apply as determined by Customer's role. The governing law for the SCCs shall be the law of Ireland unless the Agreement designates a different EU Member State.

7. Data Subject Rights

To the extent that Customer Personal Data is subject to Data Protection Laws that confer rights on Data Subjects (including rights of access, correction, deletion, portability, restriction of Processing, and objection to Processing), Kinective shall:

- Promptly notify Customer (and in any event within five (5) business days) upon receiving any request, complaint, or inquiry from a Data Subject relating to Customer Personal Data;
- Provide Customer with reasonable cooperation and assistance, taking into account the nature of the Processing, to enable Customer to respond to Data Subject requests within the timeframes required by applicable Data Protection Laws;
- Not respond directly to any Data Subject request without Customer's prior written authorization, except to inform the Data Subject that the request has been forwarded to Customer; and
- Implement appropriate technical and organizational measures to assist Customer in fulfilling its obligations to respond to Data Subject requests, to the extent such measures are reasonably practicable.

8. Data Breach Notification and Response

8.1 Notification

Kinective shall notify Customer without undue delay, and in no event later than forty-eight (48) hours, after becoming aware of a confirmed Data Breach affecting Customer Personal Data. Such notification shall be provided to Customer's designated security contact and shall include, to the extent then known:

- A description of the nature of the Data Breach, including the categories and approximate number of Data Subjects and records affected;
- The name and contact information of Kinective's data protection or security contact;
- A description of the likely consequences of the Data Breach; and
- A description of the measures taken or proposed to address the Data Breach, including mitigation measures.

Kinective acknowledges that Customer, as a regulated financial institution, may have shorter regulatory notification obligations (including the FDIC/OCC/Federal Reserve 36-hour notification requirement for banking organizations under 12 C.F.R. Part 53 and related rules). Kinective shall aim to cooperate fully with Customer to meet all applicable regulatory notification requirements.

8.2 Remediation

Following any Data Breach, Kinective shall: (i) take reasonable steps to identify and remediate the root cause of the breach; (ii) provide Customer with regular updates on the investigation and remediation efforts; (iii) cooperate with Customer's forensic investigation and any regulatory or law enforcement investigations; and (iv) at Customer's reasonable request, provide written documentation of remediation measures implemented.

8.3 No Admission

Kinective's notification of or response to a Data Breach shall not constitute an admission of fault or liability.

9. Audit Rights and Compliance Demonstration

9.1 Documentation

Kinective shall maintain accurate and up-to-date records of its Processing activities under this DPA and shall make such records available to Customer upon reasonable written request.

9.2 Third-Party Certifications

To the extent applicable to the specific Service, Kinective shall obtain and maintain the following certifications and shall make copies available to Customer upon written request: (i) SOC 2 Type II audit report (or equivalent); and (ii) any other certifications required under applicable Data Protection Laws or regulatory guidance applicable to Kinective's provision of the Services. Kinective shall notify Customer promptly of any material adverse findings in any such audit or certification.

9.3 Customer Audit Rights

Upon Customer's written request, and no more than once per calendar year (unless a Data Breach has occurred or Customer's banking regulator requires an audit), Customer or its designated third-party auditor may conduct an audit or assessment of Kinective's Processing activities and security measures relating to Customer Personal Data. Any such audit shall be:

- Conducted upon at least thirty (30) days' prior written notice (or shorter notice if required by a banking regulator or following a Data Breach);
- Conducted during normal business hours and in a manner that does not unreasonably disrupt Kinective's business operations;
- Subject to reasonable confidentiality obligations; and
- At Customer's expense, except where the audit reveals a material breach of this DPA by Kinective, in which case Kinective shall bear reasonable audit costs.

Customer acknowledges that Kinective operates a multi-tenant environment. Kinective may adapt the scope of any on-site audit to protect the confidentiality of other customers' data and Kinective's proprietary information.

9.4 Regulatory Access

Kinective agrees that Customer's federal and state banking regulators (including the OCC, FDIC, Federal Reserve, NCUA, and applicable state banking departments) shall have the right, upon reasonable notice and in accordance with applicable law, to examine and audit Kinective's records, facilities, and operations to the extent they relate to the Services provided to Customer. Kinective shall cooperate fully with any such regulatory examination.

10. Data Retention and Return

Upon termination or expiration of the Agreement, or upon Customer's written request, Kinective shall, within thirty (30) days: (i) return all Customer Personal Data to Customer in a commonly used machine-readable format; and (ii) securely delete or destroy all copies of Customer Personal Data in Kinective's possession or control (including copies held by Authorized Subprocessors), except to the extent Kinective is required to retain such data by applicable law or regulation.

11. Government and Law Enforcement Requests

If Kinective receives a legally binding request from any government, law enforcement authority, or Public Authority for access to Customer Personal Data, Kinective shall, to the extent legally permitted:

- Notify Customer promptly upon receipt of such request, including a summary of the nature of the request;
- Challenge the request through all available legal means if Kinective concludes, after careful assessment, that there are reasonable grounds to believe the request is unlawful or overbroad;
- Disclose only the minimum amount of Customer Personal Data required to satisfy the request; and

- Provide Customer with information available to Kinective regarding the request to the extent permitted by law.

If Kinective is legally prohibited from notifying Customer, Kinective shall use commercially reasonable efforts to obtain a waiver of such prohibition. Kinective certifies that it has not created, and will not create, any backdoors or mechanisms to facilitate unauthorized government access to Customer Personal Data.

12. Limitation of Liability

Each party's liability under or in connection with this DPA shall be as set forth in the Agreement. For avoidance of doubt, any claims or actions arising out of this DPA shall be governed by the limitations and exclusions as set forth in the Agreement.

13. General Provisions

13.1 Order of Precedence

In the event of any conflict between this DPA and the Agreement: (i) this DPA shall control with respect to the Processing and protection of Customer Personal Data; and (ii) the terms of any applicable SCCs or other mandatory transfer mechanisms shall control over any conflicting provisions of this DPA.

13.2 Amendments

This DPA may be amended only by a written instrument signed by authorized representatives of both parties. The parties agree to negotiate in good faith any amendments necessary to comply with changes in applicable Data Protection Laws.

13.3 Governing Law

This DPA shall be governed by and construed in accordance with the governing law of the Agreement, provided that the SCCs incorporated herein shall be governed by the law of Ireland (for EU transfers) or the law of England and Wales (for UK transfers) unless otherwise required by applicable Data Protection Laws.

13.4 Changes in Law

In the event of (i) any newly enacted Data Protection Laws; (ii) any change to existing Data Protection Laws (including generally-accepted interpretations thereof); (iii) any qualified and informed interpretation of a new or existing Data Protection Law; or (iv) any material new or emerging cybersecurity threat, which individually or collectively requires a change in the manner by which Kinective is providing the Services to Customer, the parties shall work together in good faith to mutually agree upon how Kinective's provision of the Services will be impacted and shall make equitable adjustments to the terms of the Agreement and the Service.

13.5 Severability

If any provision of this DPA is held invalid or unenforceable, such provision shall be modified to the minimum extent necessary to make it enforceable, and the remaining provisions shall continue in full force and effect.

13.6 Entire Agreement

This DPA, together with the Agreement and its exhibits and appendices, constitutes the entire agreement between the parties with respect to the Processing of Customer Personal Data and supersedes all prior agreements, representations, and understandings relating to the same subject matter.

In Witness Whereof, the parties' authorized representatives hereby agree to this DPA as of the Effective Date.

Last Updated: June 3, 2026

APPENDIX A

Description of Processing

This Appendix A describes the subject matter, nature, purpose, duration, categories of Personal Data, and categories of Data Subjects covered by this DPA.

A.1 Subject Matter of Processing

The subject matter of Processing under this DPA is Kinective's provision of financial technology services and platform solutions to Customer, including core processing integration, data analytics, digital banking, and related services as described in the Agreement.

A.2 Nature and Purpose of Processing

Kinective Processes Customer Personal Data for the following purposes:

- Providing, maintaining, and improving the Services contracted by Customer under the Agreement;
- Account management, transaction processing, and financial data analytics;
- Customer support, troubleshooting, and technical assistance;
- Development, engineering, quality assurance, and testing of new and existing features (with production data only where necessary and subject to appropriate masking or anonymization where feasible);
- Security monitoring, fraud detection, and incident response;
- Compliance with applicable legal and regulatory obligations; and
- As otherwise instructed by Customer in writing.

A.3 Duration of Processing

Kinective shall Process Customer Personal Data for the duration of the Agreement, unless otherwise agreed by the parties in writing or required by applicable law. Upon termination, Kinective shall return and/or delete Customer Personal Data in accordance with Section 10 of this DPA.

A.4 Categories of Data Subjects

Category of Data Subject	Description
Customer's End Users	Customers, end users, business partners, vendors (who are natural persons).
Customer's Employees	Personnel of Customer who access or use the Services in the course of their employment.
Customer's Prospective Customers	Individuals who have applied for or inquired about Customer's financial products or services.
Customer's Business Contacts	Representatives of businesses or entities that have a commercial relationship with Customer.

A.5 Categories of Personal Data

Category	Examples of Personal Data Processed
Contact Information	Home and business address, telephone number, email address.
Financial Data (NPI)	Account numbers, routing numbers, transaction history, account balances, credit scores, loan information, investment data, payment card information.
Device and Access Data	IP address, device identifiers, usage data, browser type, access logs, authentication records.
Demographic Data	Occupation, employer, income, and other demographic data submitted by Customer or its end users.
Sensitive Data	Where submitted by Customer: Social Security Numbers and other government identifiers; financial account credentials. Such data is subject to heightened security controls.

A.6 Frequency and Manner of Transfer

Customer Personal Data is transferred to Kinective on a continuous basis through Customer's use of the Services. Transfers to Kinective's India and Philippine operations occur on an as-needed basis for development, support, and engineering activities as described in Section 6 of this DPA.

APPENDIX B

Authorized Subprocessors

This Appendix B sets forth the Authorized Subprocessors that Kinective may engage to Process Customer Personal Data as of the Effective Date. Kinective shall update this Appendix B in accordance with Section 6.2 of this DPA.

B.1 Kinective Affiliates and Internal Operations

1. Cash Flow Management, LLC
2. Orbograph LLC
3. Orbograph Ltd. (Israel)
4. The Compuflex LLC
5. Nexus Software, LLC
6. Integrated Media Management, LLC
7. ESQ Business Services, LLC
8. ESQ, Ltd.
9. Cloudexa Technologies, Inc. (Canada)
10. ESQ Management Solutions Pte. Ltd. (Singapore)
11. ESQ Management Solutions India Private Limited (India)
12. Kinective México, S. de R.L. de C.V.
13. NXTsoft Secure Data Solutions, LLC
14. Epic River Healthcare, Inc.
15. Datava, Inc.
16. Janusea, Inc.
17. Janusea Cuso LLC

B.2 Third-Party Service Providers

Third-party subprocessors below (e.g., cloud infrastructure, analytics, security monitoring providers):

1. Amazon Web Services
2. Microsoft Corporation (Azure)
3. Salesforce Inc.
4. Oracle Corporation
5. Slack Technologies, LLC
6. RyanTech Cloud Services Information Technology
7. ThoughtFocus, Inc.
8. Zoom Video Communications, Inc.

kinective

APPENDIX C

Technical and Organizational Security Measures

The following technical and organizational measures are implemented by Kinective to protect Customer Personal Data, including NPI, against unauthorized or unlawful Processing and against accidental loss, destruction, damage, or disclosure.

Security Domain	Measure Implemented	Standard / Reference
Access Control	Role-based access controls (RBAC); multi-factor authentication (MFA) for all systems accessing Customer Personal Data; privileged access management (PAM); quarterly access reviews.	ISO 27001:2022 Annex A 5.15–5.18
Encryption	AES-256 encryption at rest; TLS 1.2 or higher in transit; encrypted backups; key management procedures.	ISO 27001:2022 Annex A 5.15–5.18
Network Security	Firewalls, intrusion detection/prevention systems (IDS/IPS); network segmentation; DDoS mitigation; regular vulnerability scanning.	ISO 27001:2022 Annex A 8.20–8.22
Incident Response	Written incident response plan; 24/7 security monitoring; forensic investigation capability; defined escalation procedures; annual tabletop exercises.	ISO 27001:2022 Annex A 5.24–5.28
Physical Security	Data center access controls; CCTV monitoring; environmental controls; third-party data center SOC 2 certification required.	SOC 2 Type II
Personnel Security	Background checks for personnel with access to NPI; mandatory annual security awareness training; confidentiality agreements.	ISO 27001:2022 Annex A 6.1–6.6
Vendor Management	Written agreements with all Authorized Subprocessors; annual vendor risk assessments; security review before engagement.	ISO 27001:2022 Annex A 5.19–5.22
Business Continuity	Documented BCP/DR plan; regular backup and recovery testing; recovery time objectives (RTO) and recovery point objectives (RPO) defined.	ISO 27001:2022 Annex A 5.29–5.30
Audit & Logging	Centralized security logging and SIEM; log retention per regulatory requirements; regular audit log review; tamper-evident logging.	ISO 27001:2022
Application Security	Secure software development lifecycle (SDLC); static and dynamic application security testing (SAST/DAST); annual penetration testing by qualified third party.	ISO 27001:2022 Annex A 8.25–8.31

The security measures listed above represent Kinective's current baseline. Kinective shall review and update these measures at least annually and following any material change to its Processing environment. Kinective shall not materially decrease the overall security of the Services during the term of the Agreement without Customer's prior written consent.