Annex 4 – Data Processing Agreement

SECTION I

1. PURPOSE AND SCOPE

a) The purpose of these Standard Contractual Clauses (the "**Clauses"**) is to ensure compliance with article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR"**).

b) The controllers and processors listed in Appendix I have agreed to these Clauses in order to ensure compliance with article 28(3) and (4) of GDPR.

c) These Clauses apply to the processing of personal data as specified in Appendix II.

d) Appendices I to III are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of GDPR.

2. INTERPRETATION

a) Where these Clauses use the terms defined in GDPR, those terms shall have the same meaning as in that regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of GDPR.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

3. HIERARCHY

In the event of a contradiction between these Clauses and the provisions of the Contract, these Clauses shall prevail.

SECTION II – OBLIGATIONS OF THE PARTIES

4. DESCRIPTION OF THE PROCESSING(S)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Appendix II.

5. OBLIGATIONS OF THE PARTIES

5.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless

the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe GDPR or the applicable Union or Member State data protection provisions.

5.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Appendix II, unless it receives further instructions from the controller.

5.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Appendix II.

5.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Appendix III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach).

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.6 Documentation and compliance

a) The parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all reasonable information to demonstrate compliance with the obligations that are set out in these Clauses. At the controller's request, the processor shall also permit the controller to perform audits at most once a year or in case of personal data breach. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor, being agreed that the auditor may not have directly or indirectly activities competing with the processor. Audits appropriate, be carried out with reasonable prior written notice. The controller undertakes to bear the costs of the audit and to cover all costs incurred by the processor in carrying out the audit. The controller will pay these costs upon presentation of an invoice.

5.7 Use of sub-processors

a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 7 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s).

b) The agreements shall impose on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses.

c) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its agreement with the processor.

d) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor agreement and to instruct the sub-processor to erase or return the personal data.

5.8 International transfers

a) The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V GDPR, the processor and the sub-processor can ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of article 46(2) of GDPR.

6. ASSISTANCE TO THE DATA CONTROLLER

a) The processor shall without undue delay notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing.

c) In addition to the processor's obligation to assist the controller pursuant to Clause 7(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

7. NOTIFICATION OF PERSONAL DATA BREACH

In the event of a personal data breach as defined by GDPR concerning data processed by the controller, the processor shall notify the controller, without undue delay after the processor has become aware of it.

1) The processor shall assist the controller in obtaining the information concerning the measures taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

SECTION III – FINAL PROVISIONS

a) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data unless otherwise agreed by the Parties or if the processor irreversibly anonymizes the personal data.

APPENDIX I – List of parties

1. **Controller**

The Client, whose contact details are specified in the Order Form.

2. **Processor**

Name	Formance SAS
Address	9 rue des Colonnes, Paris (75002)
Name, position and contact details of the contact person	Marie Tran Head of Corporate Services marie@formance.com

<u>APPENDIX II –</u> Description of the processing

Categories of data subjects whose personal data is processed	Only personal data relating to individuals who are registered or otherwise use the Formance platform is processed. This includes, but is not limited to, the Client's employees, clients, consultants, contractors, and/or agents actively using the platform. Additionally, depending on the data submitted by the Client via configurable fields (such as metadata or custom attributes), other categories of data subjects may be processed. The Client remains solely responsible for the nature and scope of the data it uploads to the platform, including the identification of relevant data subjects.
Categories of personal data processed	Depending on the specific use of the platform and the data submitted by the Client, the following categories of personal data may be processed: • Identification and contact details: name, email address, job title, username; • Technical metadata: IP address; • Any other personal data submitted by the Client through configurable fields such as metadata or custom attributes.

	The Client is solely responsible for the nature of the data it uploads to the platform, including ensuring that no unnecessary or sensitive data is provided unless strictly required and compliant with applicable laws.
Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	The Client shall not submit, and is expressly prohibited from submitting, any sensitive personal data or special categories of data as defined under applicable data protection laws (including, but not limited to, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or sex life, or criminal convictions and offences) to the Company through the use of the platform. The Company does not require, expect or process such categories of data as part of the services. Should the Client nevertheless transmit such data, the Client remains solely responsible for ensuring that all legal requirements (including obtaining valid consent or providing appropriate safeguards) are fulfilled.
Nature of the processing	Receiving data, including collection, accessing, retrieval, recording, and data entry Holding data, including storage, organization, and structuring Sharing data, including disclosure to subprocessors as permitted in this DPA Erasing data, including destruction and deletion
Purpose(s) for which the personal data is processed on behalf of the controller	Provision of the Services to the Client
Duration of the processing	Duration of the Contract with Client

Processing by sub-processors

The list of sub-processors engaged by Formance, including details of their services, locations and whether data is transferred internationally, is available at:

https://trust.formance.com/subprocessors

This list is kept up to date and may be modified in accordance with the terms set forth in this DPA regarding the appointment and replacement of sub-processors.

APPENDIX III – Technical and organisational measures including technical and organisational measures to ensure the security of the data

1. Infrastructure Security

Access Control & Authentication

- Multi-factor authentication enforced for all production systems
- Privileged access to encryption keys restricted to authorized users only
- Role-based access control (RBAC) implemented across all systems
- Access control procedures documented for adding, modifying, and removing users

Network Security

- Network segmentation implemented to protect customer data
- Remote access only permitted via approved encrypted connections
- Production network access restricted to authorized personnel

2. Data Protection

Encryption

- Data at rest encrypted using AES-256 encryption
- Data in transit encrypted using TLS 1.2+ protocols
- Encryption keys access restricted to authorized personnel

Data Management

- Formal data retention and disposal procedures established
- Customer data deleted upon service termination

3. Operational Security

System Security

- Anti-malware technology deployed and routinely updated
- Log management tools for security event monitoring

- Vulnerability management procedures established
- Configuration management system for consistent deployments

Change Management

- System changes communicated to authorized users
- Critical changes notified to customers
- Configuration management procedures in place

4. Organizational Measures

Personnel Security

- Background checks performed on all new employees
- Security awareness training within 30 days of hire and annually
- Code of Conduct acknowledged by all employees
- Performance evaluations conducted annually
- Access revoked upon termination per documented checklists

Governance & Compliance

- ISO 27001:2022 certified
- SOC 2 Type II certified
- Risk assessments performed annually
- Control self-assessments conducted annually

5. Incident Management

Detection & Response

- Incident response plan tested annually
- Security incident procedures documented
- Breach notification within regulatory timelines

6. Business Continuity

Resilience Measures

- Business Continuity and Disaster Recovery plans established
- BC/DR plans tested annually
- Backup and recovery procedures documented
- Data backup policy implemented

7. Third-Party Management

Subprocessor Controls

- Written agreements with all vendors including confidentiality commitments

- Vendor management program established
- Critical vendor inventory maintained

8. Compliance & Audit

Testing & Validation

- Annual penetration testing
- Quarterly access reviews conducted
- External audits for SOC 2 and ISO 27001
- CyberSecurity insurance

Monitoring

- Continuous security monitoring via Vanta
- Vulnerability scanning and remediation
- Security metrics and reporting

9. Additional Measures

Development Security

- Secure development practices
- Code review processes
- Dependency vulnerability monitoring

Communication

- External support system for incident reporting
- Responsible disclosure policy published
- GDPR rights portal available at gdpr.formance.com