DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) forms part of the Master Subscription Agreement (the “**Agreement**”) between Customer and Aigoritma Inc. (”**Octai**”).

1. Subject Matter and Duration

1.1 Subject Matter. This DPA is designed to control how the Customer provides and how Octai processes Customer Personal Data, as outlined in the Agreement. All terms in uppercase that aren't explicitly defined in this DPA are understood as they're defined in the Agreement. In cases where the wording in this DPA or its attachments contradicts the Agreement, this DPA will prevail.

1.2 Duration and Survival. This DPA will be in effect from the Agreement's effective date and will last until either the Agreement ends, or the Customer Personal Data is returned or deleted as per Section 8.1, whichever occurs later.

2. Definitions

The following terms and those defined within the body of this DPA apply for the purposes of this DPA.

“**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. and any associated regulations and amendments, including the California Privacy Rights Act amendments.

“**Controller**” means the person who, alone or jointly with others, determines the purposes and means of the Processing of personal data; for purposes of this DPA, the term "Controller" shall also include "business" as such term is defined under the CCPA.

“**Customer Personal Data**” means Customer Data that is “personal data” or “personal information” under applicable Data Protection Law.

“**Data Protection Law(s)**” means all worldwide data protection and privacy laws and regulations applicable to Customer Personal Data, including, where applicable, EU/UK Data Protection Law, PDPL and the CCPA.

"**EEA**" means the European Economic Area.

"**EU/UK Data Protection Law**" means: (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) (the "EU GDPR"); (ii) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (collectively, the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) and Personal Data Protection Law numbered 6698 (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii) or (iv); in each case as may be amended or superseded from time to time;

“**Process**” or “**Processing**” means any operation or set of operations which is performed on Customer Personal Data or sets of Customer Personal Data, whether or not by automated 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.

“**Processor**” means the person who, alone or jointly with others, Processes personal data on behalf of the Controller; for purposes of this DPA, the term "Processor" shall also include "service provider" as such term is defined under the CCPA.

“**PDPL**” means the Personal Data Protection Law numbered 6698.

"**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018, in case whether such transfer is direct or via onward transfer. Where the PDPL no 6698 applies, a transfer of personal data from Turkey to any other country that is not deemed adequate under Article 9 of the PDPL, regardless of whether such transfer is direct or via onward transfer.

"**SCCs**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses for processors adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("**UK SCCs**").

“**Security Incident(s)**” means any unauthorized or unlawful breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction loss, alteration, unauthorized disclosure or access to any Customer Data processed under or in connection with the Agreement, including but not limited to Customer Personal Data.

“**Subprocessor(s)**” means a third party including Octai’s affiliates engaged by Octai to Process Customer Personal Data under the Agreement.

3. Data Use and Processing

3.1 Data Processing Relationship. The Customer is either in control of the Customer Personal Data or processes Customer Personal Data as a Processor on behalf of a third party (such as the Customer's end client). Regardless of the scenario, both parties recognize and agree that the Customer has appointed Octai to Process the Customer Personal Data as a Processor (or sub-Processor as needed) on the Customer's behalf. If the Customer is acting as a Processor on behalf of a third-party Controller, the Customer will ensure that any Processing instructions it gives to Octai under this DPA align with the Controller's directives given to the Customer.

3.2 Documented Instructions. Octai is tasked with Processing Customer Personal Data exclusively: (1) to meet its commitments to the Customer under the Agreement, which includes this DPA; (2) on behalf of the Customer; and (3) in accordance with Data Protection Laws. The Processing of Customer Personal Data by Octai will strictly adhere to the business purpose(s)

agreed upon between the parties and outlined in the Agreement, this DPA, and any written instructions mutually agreed upon by the parties (collectively referred to as the "**Business Purpose(s)").** The Customer will avoid instructing Octai to Process Customer Personal Data in a manner that contradicts applicable laws (including Data Protection Law(s)). Octai has no responsibility to oversee the legality of the Customer's utilization of the Services (including adherence to Data Protection Law(s)) and will not be held liable for any harm or damages arising from Octai's compliance with unlawful Instructions given by the Customer. Nevertheless, unless legally restricted, Octai will (i) notify the Customer in writing if it reasonably thinks there's a conflict between the Customer's instructions and applicable law (including Data Protection Law(s)) or attempts to Process Customer Personal Data in a way that contradicts the Customer's instructions, and (ii) in any such situation, halt all Processing of the relevant Customer Personal Data (except for mere storage and security maintenance of the affected Customer Personal Data) until the Customer issues new instructions that Octai can comply with. If this clause is invoked, Octai will not be accountable to the Customer under the Agreement for non-performance of the Services until such time as the parties agree on new instructions. The Customer maintains the right, upon notification, to implement reasonable and suitable measures to prevent and rectify unauthorized use of Customer Personal Data, including any use of Customer Personal Data not authorized in this DPA.

3.3 Service provider certification. Octai shall not: (a) "sell" Customer Personal Data (as such term in quotation marks is defined in the CCPA), (b) "share" or Process Customer Personal Data for purposes of "cross-context behavioral advertising" or "targeted advertising" (as such terms in quotation marks are defined in the CCPA); (c) retain, use, or disclose Customer Personal Data for any purpose other than for the Business Purpose(s), including to retain, use, or disclose the Customer Personal Data for a commercial purpose other than performing its Services under the Agreement; (d) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between Customer and Octai. Octai (i) will not attempt to re-identify any pseudonymized, anonymized, aggregate, or de-identified Customer Personal Data without Customer's express written permission; and (iii) will comply with any applicable restrictions under Data Protection Laws on combining the Customer Personal Data with personal data that Octai receives from, or on behalf of, another person or persons. Octai certifies that it understands the restrictions set out in this Section 3.3 and will comply with them.

3.4 Authorization to Use Subprocessors. Customer hereby authorizes Octai to engage affiliates and other Subprocessors including Octai affiliates to Process Customer Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Customer acknowledges and agrees that Octai's use of such Subprocessors satisfies the requirements of this DPA.

3.5 Octai and Subprocessor Compliance. Octai agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Customer Personal Data that imposes on such Subprocessors data protection requirements for Customer Personal Data that are consistent with this DPA; and (ii) remain responsible to Customer for Octai's Subprocessors' failure to perform their obligations with respect to the Processing of Customer Personal Data.

3.7 Confidentiality. Octai will ensure that any person whom Octai authorizes to Process Customer Personal Data on its behalf is subject to confidentiality obligations in respect of that Customer Personal Data.

3.8 Customer Personal Data Inquiries and Requests. To the extent Customer, in Customer's use of the Services, does not have the ability to address a request from a data subject exercising their rights under applicable Data Protection Laws (e.g., access, deletion, etc.), Octai shall, upon Customer's request, use commercially reasonable efforts to assist Customer in responding to such data subject request. If a request relating to Customer Personal Data is sent directly to Octai, Octai shall use commercially reasonable efforts to promptly notify Customer within five (5) business days of receiving such request and shall not respond to the request unless Customer has authorized Octai to do so. To the extent legally permitted, Customer shall be responsible for any non-negligible costs arising from Octai's provision of assistance under this Section. Customer acknowledges that Octai is reliant on Customer for direction as to the extent to which Octai is entitled to Process Customer Personal Data on behalf of Customer in performance of the Services. Consequently, Octai will not be liable under the Agreement for any claim brought by a data subject arising from any action or omission by Octai, to the extent that such action or omission resulted from Customer's instructions or from Customer's failure to comply with its obligations under applicable law.

3.9 Data Protection Impact Assessment and Prior Consultation. Where and to the extent required by Data Protection Law(s), Octai agrees to provide Customer reasonable assistance to and cooperation for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Protection Laws, and at Customer's reasonable expense.

3.10 Limitation on Disclosure of Customer Personal Data. Restrictions on Distributing Customer Personal Data. As far as it is legally possible, Octai shall: (i) promptly notify the Customer in written form when it receives an order, subpoena, demand, legal request, or any other documentation which seems to call for, obligate, or require the release of Customer Personal Data to any third party apart from the data subject. This includes but is not limited to regulatory entities and the United States government for surveillance or other purposes; and (ii) abstain from exposing Customer Personal Data to the third party, providing the Customer with a minimum of forty-eight (48) hours' advance notice, enabling the Customer to utilize any rights it might have under applicable laws to prevent, contest, or limit such exposure to the extent permitted by the relevant laws. If Octai is prohibited by applicable Data Protection Laws from disclosing details of a government request to the Customer, Octai will inform the Customer of its inability to abide by the Customer's instructions under this DPA without providing additional details, and await further instructions from the Customer. Octai will utilize all available and reasonable legal resources to resist any demands for data access received through a national security process, along with any associated non-disclosure conditions.

4. Cross-Border Transfers of Customer Personal Data

4.1 Cross-Border Transfers of Customer Personal Data. Customer authorizes Octai and its Subprocessors to transfer Customer Personal Data across international borders, including from the EEA, Turkey, and/or the United Kingdom to the United States.

4.2 Standard Contractual Clauses. The parties agree that, when the transfer of Customer Personal Data from Customer to Octai is a Restricted Transfer, it shall be subject to the appropriate SCCs as follows:

4.2.1. in relation to Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

1. Module Two will apply (where Customer is the Controller of Customer Personal Data), otherwise Module Three will apply (where Customer is a Processor of Customer Personal Data), as appropriate;
2. in Clause 7, the optional docking clause will apply;
3. in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 3.5 of this DPA;
4. in Clause 11, the optional language will not apply;
5. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;
6. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
7. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this DPA;
8. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA;

4.2.2. in relation to Restricted Transfers of Customer Personal Data protected by UK GDPR, the UK IDTA will apply completed as follows:

1. the IDTA will apply the EU SCCs (completed as set out in paragraph 4.2.1) to Restricted Transfers of Customer Personal Data from the UK;
2. Tables 1 – 3 of the UK IDTA shall be deemed completed with the relevant information set out in this DPA and the EU SCCs (completed as set out in paragraph 4.2.1 above);
3. Table 1 of the UK IDTA shall be deemed signed by Customer and Octai upon the entry into force of this DPA, and the start date specified in Table 1 of the UK DPA shall be deemed completed with the date of entry into force of this DPA;
4. In Table 4, the option “Importer” shall be deemed selected.

4.2.4. in the event that any provision of this DPA contradicts the SCCs (directly or indirectly), the SCCs shall prevail.

4.2.5. The parties agree that, in the event where Data Protection Laws no longer allows the lawful transfer of Customer Personal Data to Octai and/or requires an alternative transfer solution that complies with Applicable Privacy Law(s), Octai will make an amendment to this DPA available to Customer to remedy such non-compliance and/or cease processing of Customer Personal Data without penalty.

5. Information Security Program

5.1 Security Measures. Octai shall implement and maintain commercially reasonable administrative, technical, and physical measures designed to protect Customer Personal Data. Octai regularly monitors compliance with these measures. Octai will not materially decrease the overall security of the Service during any Subscription Term.

6. Security Incidents.

6.1 Notice. Upon gaining knowledge of a Security Incident, Octai commits to notify the Customer in writing without unnecessary delay. Such a notification does not constitute an admission of guilt or liability. To the extent possible, this notice will encompass all details known to Octai and required under Data Protection Law(s) for Customer to meet Customer’s own reporting responsibilities to regulatory authorities or individuals impacted by the Security

Incident. This may include, where relevant and if known, the cause of the Security Incident, the categories and approximate number of data subjects involved, the categories and approximate number of Customer Personal Data records affected, the anticipated repercussions of the Security Incident, and the actions Octai has taken or proposes to take to manage the Security Incident, including measures to mitigate its potential adverse effects, if suitable. Octai will employ commercially reasonable efforts to: (i) investigate and identify the source of such Security Incident; (ii) rectify or alleviate the potential adverse impacts of such Security Incidents, and (iii) diminish the likelihood that such Security Incident repeats. Octai will not evaluate the contents of Customer Personal Data to pinpoint information subject to any specific legal necessities or to assess the applicability of any specific privacy, data protection, or cybersecurity requirement to such information. Customer bears sole responsibility for abiding by Security Incident notification requirements applicable to Customer and for meeting any third-party notification obligations related to any Security Incident. Provided that, upon Customer's written request and subject to Customer covering Octai's reasonable fees (at current rates) and expenses, Octai will offer assistance reasonably needed to enable Customer to report relevant security breaches to the competent data protection authorities and/or affected data subjects, should Customer be required to do so under Data Protection Law(s).

7. Audits

7.1 Third-Party Audit Reports. Upon request from the Customer, and subject to the confidentiality obligations outlined in the Agreement and the enactment of specific non-disclosure agreements, Octai shall make accessible to the Customer (or Customer's independent, reputable, third-party auditor) information related to Octai's adherence to the duties stated in this DPA by sharing summaries of the most recent third-party audit report. All such summaries, unless made generally publicly accessible by Octai on its website, are considered Octai's Confidential Information.

7.2 Audit of Octai. Should Data Protection Laws grant the Customer the right to audit, the Customer (or Customer's independent, reputable, third-party auditor) may contact Octai in accordance with the "Notices" Section of the Agreement to request an audit of Octai's policies, procedures, and records pertaining to the Processing of Customer Personal Data. Such an audit is aimed at verifying Octai's compliance with this DPA, as long as such matters are under Octai's control and Octai is not prohibited from disclosure by applicable law, a confidentiality obligation, or any other duty owed to a third party. Customer shall compensate Octai for its costs and expenditures, including any time invested associated with such an audit at Octai's then-current rates, which will be provided to the Customer upon request. Prior to the initiation of any such audit, Customer and Octai shall mutually agree on the audit's scope, timing, and duration, in addition to the reimbursement rate for which Customer will be accountable. All reimbursement rates shall be reasonable, reflecting the resources utilized by Octai. In no instance will Octai be obligated, in relation to any of its duties under this DPA or otherwise, to reveal information it is barred from disclosing by applicable law, a confidentiality obligation, or any other obligation owed to a third party. Any audit must be: (i) conducted during Octai's regular business hours; (ii) with reasonable advance notice to Octai; (iii) undertaken in a way that minimizes disruption to Octai's operations; and (iv) subject to reasonable confidentiality procedures. Furthermore, any audit shall be restricted to once per year, unless directed by a government authority with appropriate jurisdiction. Customer shall promptly notify Octai of any alleged non-compliance with this DPA identified during an audit, and Octai shall employ commercially reasonable efforts to rectify any confirmed non-compliance.

8. Data Deletion

8.1 Data Deletion. Upon termination or expiration of the Agreement, Octai shall, upon Customer's request, and subject to the limitations described in the Agreement, return to Customer (or make available for export in accordance with the Agreement) all Customer Personal Data in Octai' possession, or securely destroy such Customer Personal Data (excluding any back-up or archival copies which shall be deleted in accordance with Octai' data retention schedule), except where Octai is required to retain copies under applicable laws, in which case Octai will limit its processing of such Customer Personal Data except to the extent required by applicable laws.

9. Processing Details.

9.1 Subject Matter. The subject matter of the Processing is the Services pursuant to the Agreement.

9.2 Duration. Customer Personal Data will be Processed for the duration of the Agreement, including any post-termination retention period specified therein, subject to Section 8.1 of this DPA.

9.3 Categories of Data Subjects. Data subjects whose Customer Personal Data will be Processed pursuant to the Agreement may include Employees, Suppliers, Customers, Job Applicants, Consultants, and/or Contractors.

9.5 Types of Customer Personal Data. Customer represents and warrants to Octai that Customer Personal Data does not and will not contain, and Customer has not and will not otherwise provide or make available to Octai for Processing any sensitive personal data, including but not limited to financial information (e.g. credentials to any financial accounts or tax return data); health information (e.g. protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental, or physical condition, or medical treatment or diagnosis by a health care professional, health insurance information, or genetic information); biometric information; government IDs or other government-issued identifiers (e.g. social security numbers); passwords for online accounts (other than passwords necessary to access the Services); credit reports or consumer reports; any payment card information or cardholder data subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, or similar laws, or the regulations promulgated thereunder; information subject to restrictions under applicable law governing personal data of children, including, without limitation, all information about children under 16 years of age; or any information that falls within any special categories of data (as defined under the EU/UK Data Protection Law or otherwise interpreted under the implementing laws of the EEA member states).

Annex I - Data Processing Description

This Annex I forms part of the DPA and describes the processing that Octai (as the Processor or Subprocessor, as applicable) will perform on behalf of the Customer (as the Controller or Processor, as applicable).

A. LIST OF PARTIES

Controller(s) / **Data exporter(s)**: [*Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: *Customer listed in the applicable Octai Master Subscription Agreement.*

Address: *Address listed in the applicable Octai Master Subscription Agreement.*

Contact person's name, position and contact details: *Contact person listed in the applicable Octai Master Subscription Agreement***.**

Activities relevant to the data transferred under these Clauses: *Processing to carry out the Services pursuant to the Octai Master Subscription Agreement entered into between Customer and Octai.*

Signature and date: *This Annex I shall automatically be deemed executed when Customer agrees to the Octai Master Subscription Agreement*

Role (controller/processor): *Controller or Processor, as applicable*

Processor(s) / **Data importer(s)**: *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

Name: *Octai, Inc.*

Address: *3 Germany Dr., Unit 4 #1430 Wilmington, Delaware 19804, USA*

Contact person's name, position and contact details: *Octai Legal Team - legal@octai.com*

Activities relevant to the data transferred under these Clauses: *Processing to carry out the Services pursuant to the Octai Master Subscription Agreement entered into between Customer and Octai.*

Signature and date: *This Annex I shall automatically be deemed executed when Customer agrees to the Octai Master Subscription Agreement.*

Role (controller/processor): *Controller or Processor, as applicable*

B. DESCRIPTION OF PROCESSING/ TRANSFER

EU SCC Module: *C2P (Module 2)*

Categories of Data Subjects: *The personal data transferred may concern the following categories of data subjects set forth in Section 9.3 of the DPA:*

Employees, Suppliers, Customers, Job Applicants, Consultants, and Contractors

Purpose(s) of the data transfer and further processing/ processing operations: *The purpose of the transfer is the performance of the Services pursuant to the Agreement.*

Categories of Personal Data: *The personal data transferred concerns any category of personal data submitted by Customer to Octai pursuant to the Agreement, except for any personal data covered by Section 9.5 of the DPA.*

Sensitive data transferred (if applicable) and applied restrictions or safeguards: *As set forth in Section 9.5 of the DPA, sensitive data are expressly excluded from the scope of the Services.*

Frequency of the transfer: *Continuous*

Subject matter of the processing: *The subject matter of the Processing is Octai's Processing of Customer Personal Data to provide the Services pursuant to the Octai Master Subscription Agreement.*

Nature and subject matter of the processing: *The nature and purpose of the transfer is the performance of the Services pursuant to the Octai Master Subscription Agreement.*

Duration of the processing: *The duration of the data processing under this DPA is until the termination of the Octai Master Subscription Agreement in accordance with its terms.*

Retention period (or, if not possible to determine, the criterial used to determine the period): *For the duration of the Octai Master Subscription Agreement. Upon termination of the Agreement, Customer Personal Data shall be returned or destroyed in accordance with Section 8.1 of the DPA.*

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs):

Where the EU GDPR applies, the supervisory authority is the EU Member State in which the Customer (or, if the Customer does not have an establishment in the EU, its representative) is established. Otherwise, if the Customer does not have an EU establishment nor an EU representative, the Irish Data Protection Commission.

Where the UK GDPR applies, the UK Information Commissioner's Office.

Where the PDPL applies, the Turkish Data Protection Authority.

Annex II - Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the Processor(s) / Data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

1. **Measures of pseudonymisation and encryption of personal data**

   Octai has implemented robust pseudonymisation and encryption measures for personal

data. This ensures that sensitive information is protected and cannot be directly linked to individuals. All personal data is encrypted both during transmission and storage, providing an additional layer of security.

2. **Measures for Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience of Processing Systems and Services:**

   Octai employs a comprehensive set of measures to ensure the continuous confidentiality, integrity, availability, and resilience of its processing systems and services. These measures include:

   a. Access Control: Production systems are regulated through VPN and utilize unique accounts and role-based access. Authorization requests for access are logged and tracked regularly. Employee access is revoked upon termination or change of role.

   b. Multi-Factor Authentication (MFA): Critical and production resources require MFA for access, enhancing the security of user accounts.

   c. Strong Password Policies: Strong passwords are mandated, never stored in clear text, and encrypted during transmission and storage.

   d. Mandatory Security Training: Employees are required to undergo regular security training covering data protection, confidentiality, social engineering, password policies, and overall security responsibilities.

   e. Confidentiality Requirements: Strict confidentiality requirements are imposed on employees, and third-party vendors are bound by Non-Disclosure Agreements (NDAs).

   f. Network Segmentation: Networks are segregated based on trust levels, reducing the risk of unauthorized access.

3. **Measures for Ensuring the Ability to Restore Availability and Access to Personal Data in a Timely Manner:**

   Octai has established processes to maintain ongoing confidentiality, availability, and resilience during security incidents. This includes a robust incident response plan that helps restore timely access to personal data following an incident.

4. **Processes for Regularly Testing, Assessing, and Evaluating the Effectiveness of Technical and Organisational Measures:**

   Octai conducts annual penetration tests for all components of its services, including web and mobile applications. Additionally, the company maintains security incident management policies and procedures and promptly notifies impacted customers of any unauthorized disclosure of Customer Data as required by law.

5. **Measures for User Identification and Authorization:**

Octai's Services support SAML for Customers, ensuring secure and reliable user identification and authorization. Access by Octai personnel to systems is uniquely identifiable, logged, and monitored. Back-end infrastructure access requires multiple layers of authentication, including unique identifiers and Multi-Factor Authentication.

6. **Measures for the Protection of Data During Transmission and Storage:**

Octai employs end-to-end encryption for Customer Data during transit, ensuring data remains secure while being transmitted between the user's browser and the Services. Customer instances are logically separated, preventing unauthorized access to data, and unauthorized actors are barred from accessing data from other customers.

7. **Measures for Ensuring Physical Security of Processing Locations:**

Octai's subprocessors are contractually obligated to maintain physical security measures at data centers. These measures include restricted access for authorized personnel only, around-the-clock guards, two-factor access screening, escort-controlled access, and on-site backup generators to mitigate the impact of power failures.

8. **Measures for Ensuring Events Logging:**

Octai logs authorization requests to privileged spaces and user activities, including logins, configuration changes, deletions, and updates. These logs are internally available and can be accessed for security investigations upon request.

9. **Measures for Ensuring System Configuration and Default Configuration:**

Octai monitors changes to its systems to ensure compliance with the Change Management Policy. Changes are tracked in a change management system to mitigate the risk of undetected changes to production systems.

10. **Measures for Internal IT and IT Security Governance and Management:**

Octai has internal information security policies and procedures communicated to all employees upon hire and annually thereafter. Information Security training is provided to employees to ensure they are aware of their responsibilities. The Information Security function reports to the Legal department, which is authorized by senior leadership to establish, implement, and manage Octai's Information Security Program.

11. **Measures for Certification/Assurance of Processes and Products:**

Octai undergoes annual audits by reputable third-party auditors to verify the implementation of controls and safeguards. The company holds industry-standard certifications, demonstrating its commitment to safeguarding the confidentiality and privacy of information stored and processed on its service.

12. **Measures for Ensuring Data Minimisation and Data Quality:**

Octai collects and processes data strictly in line with its stated purposes, and access is provisioned based on roles and job responsibilities. The company provides self-service

functionality to customers to update their personal data, ensuring data quality.

13. Measures for Ensuring Limited Data Retention:

To enforce data retention limitations, Octai deletes data based on retention periods. Terminated customer accounts are maintained in an inactive status for a limited period before securely overwriting account data from production. Backup data is deleted within a set timeframe after account termination.

14. Measures for Ensuring Accountability:

Octai maintains Records of Processing Activities and conducts Privacy Impact Assessments, where applicable, to ensure compliance with data protection requirements.

By implementing these comprehensive technical and organisational security measures, Octai ensures the protection of personal data and upholds the privacy rights of individuals. These measures, combined with regular testing and evaluation, demonstrate the company's commitment to maintaining a high level of data security and privacy.