DATA PROCESSING

AND

CONFIDENTIALITY AGREEMENT

TABLE OF CONTENT

ABOUT THE DATA PROCESSING AGREEMENT

As of today, the Parties have entered into this data processing agreement (hereinafter called "**the Agreement**" or "**this Agreement**" pursuant to § 42 (2) of the Danish Act on Processing of Personal Data[1] and Section 28(3)(4) of the General Data Protection Regulation[2].

THE PARTIES

The Data Controller (Customer/MSP)

and

Panorama9 ApS
Flaesketorvet 28, 1st Floor
1711 Copenhagen V
Denmark
CVR: 33396880

Subsidiary Of
Panorama9 Inc.
789 Folsom Street
San Francisco
CA 94107
USA
(Hereinafter called "**the Data Processor**")

1 BACKGROUND, OBJECTIVE AND SCOPE

1.1. The Data Controller is responsible for the processing of personal data covered by this Agreement.

1.2. The Data Processor processes personal data covered by this Agreement, as the Data Processor is given access to personal data from the Data Controller in connection with the service provided to the Data Controller by the Data Processor.

1.3. When the Data Controller and the Data Processor are jointly mentioned in this Agreement, the name "**the Parties**" shall also apply.

1.4. This Agreement determines the requirements for processing and security set out by the Data Controller to the Data Processor, when the Data Processor processes personal data exclusively covered by this Agreement and exclusively upon directions from the Data Controller.

[1] Act No. 429 of 31 May 2000 on the processing of personal data, as amended.

[2] Regulation (EC) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

2 DATA PROCESSING

2.1 The processing of personal data from the Data Controller takes place through the Panorama9 offered service(s) provided by the Data Processor when the Data Processor needs to have access to personal data from the Data Controller.

When processing this data, the Data Processor receives three (3) types of data, as described below.

- Application Configuration Data
    - Application configuration data contains the customer specific configuration of the Panorama9 service. Data within this category is not classified as Customer Data.
- Document Metadata
    - Document Metadata contains information regarding public IP address of the device communicating with Panorama9, timestamps and User Agent information. Data within this category may contain personal data.
- Document Content
    - Document content is the actual content a device is submitting to Panorama9, or receiving from a Panorama9 service. This type of Customer Data may contain personal data.

2.2 In this connection, the Data Processor has access to the following categories of personal data:

– General personal data[3] such as document content that any given device is submitting to Panorama9.

2.3 The Data Processor processes personal data of the following categories of persons:

– The Data Controller's employees.

– The Data Controller's customers employees.

2.4 The Data Controller shall retain all rights, ownership and copyright to the personal data and other information made available for the Data Processor in accordance with this Agreement or relating to the performance of the Agreement by the Data Processor, unless otherwise expressly agreed in writing.

[3] Ordinary personal data means information subject to article 6 and, therefore, not falling under the scope of article 9 and 10 of the Regulation.

3 TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES, SECTORS IN THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

3.1 Personal data shall not be transferred to a third country, specific sectors in a third country or an international organization without necessary legal basis provided for in the legislation in force at any time regarding processing of personal data.

3.2 However, the Data Processor may transfer personal data to a third country, specific sectors in a third country or an international organization. The Data processor may engage with Sub-data processors such as CRM, ERP, CSM services and exchange personal data such as email address. The data controller is always entitled to receive a current list of used third party providers by the Data Processor. Please see 4.3.

4 OBLIGATIONS OF THE DATA PROCESSOR

4.1 Instructions for processing:

4.1.1 The Data Processor shall only process personal data according to instructions from the Data Controller and not for own, independent purposes.

4.1.2 The Data Processor shall be obliged to perform appropriate technical and organizational measures in such a way that the processing meets the requirements of the legislation in force at any time and ensures protection of the rights of the data subjects.

4.2 Confidentiality:

4.2.1 The Data Processor shall be obliged to ensure that the persons authorized to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.

4.3 Use of other Data Processors and Sub-Data Processors

4.3.1 The Data Processor cannot be replaced with another Data Processor without prior written consent from the Data Controller.

4.3.2 By entering this Agreement, the Data Controller authorizes the use of Sub-Data Processors by the Data Processor.

4.3.3 If the Data Processor uses a Sub-Data Processor, the Data Processor shall be obliged to ensure that an agreement is made with the Sub-Data Processor (Data Processing and Confidentiality Agreement), which, as a minimum, shall meet the requirements of the Agreement and the legislation in force at any time on the processing of personal data.

4.3.4 The Data Controller may at any time require existing agreements between the Data Processor and any Sub-Data Processor.

4.3.5 In accordance with article 28 (4) of the General Data Protection Regulation, the Data Processor shall be fully responsible to the Data Controller for the failure of the Sub-Data Processor to comply with the requirements of this Agreement.

4.4 **Security:**

4.4.1 The Data Processor shall take the appropriate technical and organizational measures against accidental or illegal destruction, forfeiture or deterioration of personal data and against unauthorized disclosure of data, misuse or treatment otherwise in violation of legislation.

4.4.2 Specifically, the Data Processor shall be obliged to take appropriate technical and organizational measures as referred to in Annex 1 (security appendix) to this Agreement.

4.4.3 Any Sub-Data Processors of the Data Processor shall also be obliged to take appropriate technical and organizational measures.

4.5 **Security breach:**

4.5.1 In the event of a security breach at the Data Processor, where personal data is leaked, compromised or has otherwise come to the knowledge of unauthorized persons, the Data Processor shall be obliged, from the time at which the Data Processor becomes aware of the breach, to immediately notify the Data Controller of the breach.

4.5.2 Notification to the Data Controller shall be made to the Person using the e-mail address for signing up to the service of Panorama9.

4.5.3 In the event of a security breach at the Data Processor, where personal data is leaked, compromised or has otherwise come to the knowledge of unauthorized persons, the Data Processor shall also be obliged to conduct a detailed investigation of the security breach, including the causes of the breach, and to assist the Data Controller in limiting the impact of the breach.

4.5.4 In the event of a security breach at the Data Processor, where personal data is leaked, compromised or has otherwise come to the knowledge of unauthorized persons, the Data Processor shall, as far as possible and in consideration of the nature of the processing, be obliged to assist the Data Controller in notifying the relevant Data Protection Agency no later than 72 hours after the Data Processor has become aware of the breach.

4.5.5 In the event of a security breach at the Data Processor, where personal data is leaked, compromised or has otherwise come to the knowledge of unauthorized persons, the Data Processor shall, as far as possible and in consideration of the nature of the processing, be obliged to assist the Data Controller in notifying the data subjects.

4.5.6 In case of security breaches at the Data Processor, every party shall bear own costs in connection with the performance of the obligations under this agreement, section 4.5.1-4.5.6.

4.6 **Other obligations:**

4.6.1 In consideration of the nature of the processing and the information available to the Data Processor, and only if necessary, the Data Processor shall, to the extent possible, be obliged to assist the Data Controller in meeting the obligation of the Data Controller to respond to requests for exercise of the rights of the data subjects as laid down in the General Data Protection Regulation, chapter III. In order to enable the Data Processor to comply with the requests, the Data Controller must immediately forward any requests involving the assistance of the Data Processor.

4.6.2 In consideration of the nature of the processing and the information available to the Data Processor, and only if necessary, the Data Processor shall, to the extent possible, be obliged to assist the Data Controller in meeting the obligations of the Data Controller under the General Data Protection Regulation, article 32-36.

4.6.3 In accordance with the choice of the Data Controller, the Data Processor shall delete – and, if possible, return – all personal data to the Data Controller, as well as delete existing copies, unless European Union law or national law of the member states provides for storage of the personal data. The data shall be deleted – and, if possible, be returned – immediately after the request of the Data Controller.

4.6.4 The Data Processor shall, at own expense, be obliged to make all information necessary available to the Data Controller to demonstrate compliance with the requirements of the legislation in force at any time concerning the processing of personal data and allow for and contribute to audits, including inspections carried out by the Data Controller or another auditor or expert authorized by the Data Controller.

4.6.5 If the Data Processor considers an instruction from the Data Controller to be inconsistent with the General Data Protection Regulation or other relevant legislation, the Data Processor shall immediately, in writing, inform the Data Controller hereof.

4.6.6 The Data Processor shall be obliged to indemnify and defend the Data Controller against all requirements, legal claims and any liability, losses, fines, costs and expenses connected hereto as a result of an infringement of this Agreement by the Data Controller, committed by the Data Processor, the employees or representatives of the Data Processor in connection with the provision of services, execution of the Agreement, or as otherwise agreed between the Parties.

4.6.7 Thus, the Data Processor shall be directly liable to the Data Controller, regardless of whether the infringements of this Agreement are caused by the suppliers or representatives of the Data Processor in connection with the provision of services.

5 CONTROL

5.1 The Data Controller may at any time make announced inspections at the Data Processor to verify that the data processing takes place in accordance with applicable law and with adequate IT security measures. The Data Processor shall in this connection make all relevant information and physical facilities available for the inspection to be carried out on an informed basis.

5.2 Each Party bear own costs related to any data audit.

6 DURATION, AMENDMENTS, TERMINATION AND BREACH

6.1 This Agreement between the Data Controller and the Data Processor shall be valid until it is terminated or lapses for any other reason.

6.2 This agreement may be amended at any time by mutual written agreement between the Parties, or if such amendment is necessary in order to comply with the legislation in force at any time, or if changes must be made to relevant Agreement(s) relating to the provision of service/services between the Parties, which may necessitate an amendment to this Agreement. An amendment of this Agreement shall, however, always meet the minimum requirements for a Data Processing Agreement of the legislation in force at any time on the processing of personal data.

6.3 Upon termination of this Agreement, the Data Processor will delete all personal data and delete any copies no later than 30 days after termination of this Agreement upon request.

6.4 If the Data Processor does not have the necessary organizational and technical security measures in place as mentioned this Agreement, section 4.4 and annex 1, and the Data Processor has not, within a reasonable time after having been made aware hereof, implemented the necessary security measures, this represents a material breach.

6.5 A security breach at the Data Processor, which entails that personal data has been compromised, leaked or has otherwise come to the knowledge of unauthorized persons, constitutes a breach. If, on the basis of a security breach at the Data Processor, adequate technical and organizational measures are not implemented immediately hereafter to partly reduce the damage caused by the breach and partly deal with similar events, this represents a material breach.

6.6 If the Data Processor at the request of the Data Controller does not provide access for the Data Controller to personal data, including preventing the Data Controller or a representative of the Data Controller from conducting inspections and audits, this represents a material breach.

6.7 If the Data Processor uses personal data for own purposes beyond the purposes for which the Data Processor may process personal data pursuant to this Agreement, this shall be considered a material breach.

6.8 If the Data Processor, with any Sub-data Processors, fails to enter into Data Processing agreements which meet the requirements of this Agreement and the legislation in force at any time on the processing of personal data, this shall be considered a material breach.

6.9 This Agreement, section 6.1-6.9, also applies to any Sub-Data Processors of the Data Processor.

6.10 In the event of termination of this Agreement, regardless of the legal basis for this, the Data Processor shall provide the necessary transitional services to the Data Controller. The necessary transitional services include, inter alia, that the Data Processor shall continue to act on the instructions of the Data Controller, including the instruction to return or delete personal data. The cost for providing the necessary transitional services is borne by the Data Controller.

6.11 The Data Processor shall be obliged to, loyally and as quickly as possible, contribute to the transfer of execution of services to another supplier, or to transfer these back to the Data Controller. The Data Processor shall immediately upon request modify, transfer or delete personal data processed by the Data Processor for the Data Controller.

6.12 Regardless of the formal period of the Agreement, the Agreement shall apply as long as the Data Processor processes personal data for the Data Controller.

6.13 Neither the Data Controller nor the Data Processor shall be deemed liable to the other Party for any circumstances beyond the control of the Party, which the Party upon entering this Agreement could not have taken into consideration, avoided or overcome. Circumstances at a sub-contractor shall only be considered force majeure, if an obstacle is present at the sub-contractor which is subject to this item, and which the Party could not have avoided or overcome.

7 PRIORITY, DISPUTES, APPLICABLE LAW AND PLACE OF JURISDICTION

7.1 In the event of any discrepancy between this Agreement and other agreements between the Parties, this Agreement shall prevail.

7.2 This Agreement (including any questions about the validity of the Agreement) is governed by the laws of the country in which the Data Controller is established.

7.3 Any dispute which may arise under this Agreement shall be brought before the District Court of Copenhagen, Denmark.

Appendix 1 – The Security Appendix

The purpose of this security appendix is to define the technical and organizational security measures that the Processor is obliged to implement under this Agreement.

1. ORGANISATION OF THE INFORMATION SECURITY
    a. The Processor shall take adequate technical and organizational measures to protect data from accidental or unlawful destruction, loss or deterioration and from unauthorized access, exploitation or processing by other means in contravention of applicable law.

    b. More specifically, the Processor shall take the technical and organizational measures specified in this security appendix.

2. INTERNAL SECURITY GUIDELINES
    a. The Processor shall establish and implement internal risk-based guidelines on secure processing of personal data in compliance with the rules on processing of personal data applicable at any time.

    b. The Processor shall also implement a data protection policy in accordance with Section 24(2) of the General Data Protection Regulation (GDPR).

    c. The Processor's relevant internal guidelines shall be reviewed once a year at a minimum with a view to ensuring that they are comprehensive and reflect the facts.

3. PERSONAL DATA PROCESSING BY EMPLOYEES
    a. All personal data shall be treated confidentially. The Processor's employees shall be subject to confidentiality for the processing of any personal data to which they gain access as part of data processing.

    b. All of the Processor's employees with access to the Controller's data need security clearance under the Controller's standard procedure for granting such clearance.

    c. The Processor shall draw up an explicit list of the Processor's employees with security clearances and authority to access or receive the Controller's data.

4. PHYSICAL SECURITY AND IT SECURITY
    a. Security measures shall be taken to prevent unauthorized access to personal data which are processed by the Processor pursuant to this Agreement.

    b. If the Processor's employees work from a home office when processing personal data, the Supplier shall guarantee that the internal security measures are complied with on how to use home offices.

5. SECURING OF EQUIPMENT

    a. In connection with the repairing, servicing or destruction of equipment and media containing personal data which are subject to this Agreement, measures shall be taken to prevent unauthorized access to personal data.

6. TRANSFER OF DATA THROUGH THE INTERNET

a. When connecting to the Internet or other open networks, measures shall be taken to prevent unauthorized access to the Processor's internal network(s).

b. When transferring personal data through the open Internet (such as an email), the Processor shall meet the following minimum requirements:
    - Any transfer of confidential, personal data must be subjected to careful encryption, based on an acceptable algorithm (AES or the like).
    - The authenticity of the sender's and the recipient's identities shall be ensured as required when using, for example, digital signatures or personal, confidential passwords.

7. DELETION OF PERSONAL DATA
    a. Hard copy documentation shall be shredded when it is no longer necessary to keep the personal data on file. Personal data stored electronically shall be deleted in an acceptable manner when it is no longer necessary to keep them on file.

8. LOGGING
    a. Any transaction involving confidential, personal data shall be logged, and the log shall state:
        - Time,
        - User,
        - Usage

    b. The log shall be kept for twelve (12) months, following which it shall be deleted.

    c. The Processor shall also be obliged to make available print-outs/grant access to logs for the Controller upon request by the Controller's Chief Security Officer.

9. ACCESS CONTROL
    a. Only employees with the Processor authorized to access personal data shall have access to personal data. Access rights for personal data shall not be granted where such rights exceed the user's work-related need for such access.

    b. User access to confidential, personal data shall be reassessed annually.

    c. The employee's passwords shall be of adequate complexity.

    d. Rejected login attempts shall be checked, and further attempts shall be blocked.

    e. The Processor shall not use any software and hardware configurations containing known weaknesses and vulnerabilities which can be exploited to gain access to personal data.