DATA PROCESSING AGREEMENT
Last Updated September 1st, 2022

This Data Processing Agreement reflects the requirements of the European Data Protection Regulation ("**GDPR**") as it comes into effect on May 25, 2018. Cintoo´s services offered in the European Union are GDPR ready and this DPA provides you with the necessary documentation of this readiness.

This DATA PROCESSING AGREEMENT ("**DPA**") is an addendum to the Terms of Service (hereafter, the "**Agreement**") between Cintoo SAS. ("**Cintoo**") and the Customer ("**Customer**"), pursuant to which Cintoo provides services purchased by Customer from Cintoo (the "**Services**") to Customer. All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

To carry out its obligations under the Agreement, Cintoo may have access to and be required to process certain personal data controlled by Customer (hereafter "**Customer Personal Data**").

Customer and Cintoo desire to incorporate this Addendum into the Agreement in order to ensure compliance with the European Union General Data Protection Regulation 2016/679 (GDPR) and related national regulations. This DPA is based on provisions of article 28 of the GDPR.

This DPA applies where and only to the extent that Cintoo processes Customer Personal Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

IF YOU DO NOT AGREE TO BE BOUND BY THIS DPA, AND YOU HAVE NOT SEPARATELY AGREED WITH CINTOO ON TERMS REGARDING THE PROCESSING OF PERSONAL DATA OF DATA SUBJECTS, DO NOT ACCESS CINTOO'S SERVICES FOR THE PROCESSING OF PERSONAL DATA OF DATA SUBJECTS.

BY ACCESSING OR USING CINTOO SERVICES, YOU ARE ACCEPTING THIS DPA ON BEHALF OF YOURSELF OR THE ENTITY THAT YOU REPRESENT, AND YOU REPRESENT AND WARRANT THAT YOU HAVE THE RIGHT, AUTHORITY, AND CAPACITY TO ENTER INTO THIS DPA (ON BEHALF OF YOURSELF OR THE ENTITY THAT YOU REPRESENT AND ITS AFFILIATES).

THE PARTIES AGREE AS FOLLOWS:

1 Definitions

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1.1 "Affiliate" means an entity that directly or indirectly controls, is controlled by or is under the common control with an entity. For the purposes of this DPA, "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question.

1.2 "Cintoo" means Cintoo SAS engaged in the processing of Customer Personal Data.

1.3 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union

or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

1.4 "Customer Data" means any data that the Cintoo Group processes on behalf of Customer, its Affiliates and/or its End-Users, in the course of providing the Services under the Agreement.

1.5 "Customer Personal Data" means Personal Data contained with Customer Data.

1.6 "Data Protection Laws" means all data protection and privacy laws and regulations in particular European Data Protection Laws, applicable to the processing of Personal Data under the Agreement.

1.7 "Data Subject" means an identified or identifiable natural person.

1.8 "European Data Protection Laws" means laws and regulations of the European Union, the EEA and their member states, and the Regulation 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation ("GDPR") regarding the processing of Personal Data and protection of privacy.

1.9 "EEA" means the European Economic Area.

1.10 "End-Users" means any employee, business partner, contractor, agent who is registered or permitted by Customer to use the Services, any customer or potential customer of the Customer.

1.11 "Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

1.12 "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

1.13 **"**Processing" means any operation or set of operations which is performed on personal data or on sets of 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.

1.14 "Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.15 "Sub-processor" means any Processor engaged by Cintoo SAS to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

1.16 "Supervisory authority concerned**"** means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority.
(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
(c) a complaint has been lodged with that supervisory authority.

2 Processing of Customer Personal Data

2.1 **Role of the Parties**. If the GDPR applies to the processing of Customer's Personal Data, the parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller of Customer Personal Data and Cintoo is Processor of that Customer Personal Data on behalf of Customer. Each party will comply with the obligations applicable to it under the European Data Protection Laws with respect to the processing of that Customer Personal Data.

2.2 **Cintoo as a Controller.** Notwithstanding anything to the contrary in this DPA and in the Agreement, Cintoo will have the right to process data relating to and/or obtained in connection with the operation, support and/use of the Services for its legitimate business purposes, such as billing, account management, technical support and sales and marketing. To the extent that such data is Personal Data, Cintoo is the Controller of such data and shall process such Personal Data in accordance with GDPR and as explained in the Services Privacy Policy.

2.3 **Customer Processing of Personal Data**. Customer shall, in its use of the Services, only submit Personal Data or transfer such Personal Data to Cintoo, in accordance with the requirements of GDPR. For the avoidance of doubt, Customer's instructions for the processing of Customer Personal Data shall also comply with Data Protection Laws. In addition, Customer shall have sole responsibility for the accuracy, quality and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Customer shall also have sole responsibility for establishing a lawful data process and for collecting Data Subjects consents and requests. Customer also acknowledges and agrees that there is, and will be throughout the term of the Agreement, a legal basis for the processing by Cintoo of Customer Personal Data on behalf of Customer in accordance with this DPA and the Agreement (including Customer's instructions).

2.4 **Cintoo Processing of Personal Data**. Cintoo shall only process Customer Personal Data under this DPA and the Agreement upon Customer's documented instructions. Cintoo shall notify Customer, within a reasonable time, in writing if, in Cintoo's reasonable opinion, the Customer's instructions violate the provisions of GDPR. This DPA and the Agreement are Customer's complete and final instructions to Cintoo for the processing of Customer Personal Data. Any additional instructions must be agreed upon separately. Customer instructs Cintoo (and authorizes Cintoo to instruct each sub-processor) to process Customer Personal Data for the purposes described in Exhibit A.

3 Description of Processing

The subject matter and details of processing are described in Exhibit A.

4 Cintoo Personnel

4.1 Confidentiality of Processing. Throughout the term of this DPA, Cintoo shall ensure that its personnel engaged in the processing of Customer Personal Data are informed of the confidential nature of such Customer Personal Data, have received appropriate training on their responsibilities and have executed **confidentiality agreements**. This obligation to confidentiality shall continue after the termination of this DPA.

4.2 Reliability. Cintoo shall take commercially reasonable steps to ensure the reliability of any Cintoo personnel engaged in the processing of Customer Personal Data.

4.3 Limitation of Access. Cintoo shall limit its access to Personal Data to those personnel who require such access to perform the Agreement.

4.4 Data Protection Officer. Members of Cintoo have appointed a data protection officer. The appointed person may be reached at privacy@cintoo.com.

5 Data Deletion

5.1 **Data deletion during Term**. To the extent that Customer, in its use of the Services, does not have the ability to delete Customer Personal Data as instructed in Cintoo's privacy policies, Cintoo shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Cintoo is legally permitted to do so and has reasonable access to the Customer Personal Data. This request will constitute an instruction to Cintoo to delete the relevant Customer Personal Data from Cintoo's systems in accordance with applicable law.

5.2 **Data deletion on Term Expiry**. On expiration of the applicable Term, Customer instructs Cintoo to delete all Customer Personal Data from Cintoo's systems in accordance with applicable law. Cintoo will comply with this instruction as soon as reasonably practicable and within a maximum period of 15 days, unless storage of such Customer Personal Data is required by law. Without prejudice to Section 12, Customer acknowledges and agrees that Customer will be responsible for exporting, before the applicable Term expires, any Customer Personal Data it wishes to retain afterwards.

6 Data Security

6.1 **Cintoo Security Measures**. Cintoo implements and maintains technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access such as described in Exhibit B (the "**Security Measures**"). These Security Measures include measures to help ensure ongoing confidentiality, integrity, availability and resilience of Cintoo's systems and Services; to help restore timely access to Personal Data following a data breach and for regular testing of effectiveness. Cintoo may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. Customer acknowledges and agrees that it has reviewed and assessed the Security Measures and deems them appropriate for the protection of Customer Personal Data.

6.2 **Cintoo Security Assistance**. Customer agrees that Cintoo will (taking into account the nature of the processing of Customer Personal Data and the information available to Cintoo) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of Personal Data and Personal Data breaches, including, if applicable, Customer's obligations pursuant to Articles 32 to 34 of the GDPR, by: (a) implementing and maintaining the Security Measures in accordance with Section 6.1; and (b) complying with the procedures for **Personal Data Breach** in accordance with Section 7 below.

7 Personal Data Breach

7.1 **Data Breach Notification**. If Cintoo becomes aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data processed by Cintoo or its Sub-Processors ("**Data** Breach"), Cintoo will notify Customer of the Data Breach without undue delay providing Customer sufficient information to allow the

Customer to meet any obligations to report or inform Data Subjects under Data Protection Laws.

7.2 **Delivery of Notification.** Notification(s) of any Data Breach(s) will be delivered to the appropriate notification email address or, at Cintoo's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the notification email address is current and valid.

7.3 **No Assessment of Customer Data by Cintoo**. Cintoo will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Without prejudice to Cintoo's obligations under this Section 7, Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breach (s).

7.4 No Acknowledgement of Fault by Cintoo. Cintoo's notification of or response to a Personal Data Breach under this Section 7 will not be construed as an acknowledgement by Cintoo of any fault or liability with respect to the Personal Data Breach.

8 Customer's Responsibilities

Within the scope of this DPA, Customer agrees to:

(i) determine the purposes and general means of Cintoo's processing of Customer Personal Data in accordance with this DPA. Customer shall inform Cintoo without undue delay and comprehensively about any errors or irregularities related to the statutory provisions on the processing of Personal Data and;

(ii) comply with its protection, security and other obligations with respect to Customer Personal Data prescribed by Data Protection Laws for Data Controllers. Customer is solely responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Customer Personal Data, securing the account authentication credentials, devices Customer uses to access the Services, and retaining copies of its Customer Personal Data, and;

(iii) ensure that Customer's instructions (as described in Section 2.4 above) are compliant with Data Protection Laws;

(iv) be solely responsible for the accuracy, quality and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data (as described in Section 2.3 above), and;

(v) be sole responsible for establishing a lawful data process and for collecting Data Subjects consents and requests (as described in Section 2.3 above)

9 Reports and Customer's Audit Rights

9.1 **Reports** : Subject to the provisions of Section 9.3 below, at Customer's written request, Cintoo shall provide Customer (on a confidentiality basis) all information necessary to demonstrate compliance with this DPA (including but not limited to records of Cintoo Security Measures). Cintoo shall further provide written responses to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires, that Customer considers necessary to confirm Cintoo's compliance with this DPA, provided that Customer shall not exercise this right more than once a year.

9.2 **Audits and Compliance :** In order to comply with article 28 of the GDPR, Cintoo will allow, at any time during the term of the DPA, Customer and/or an independent third-party auditor appointed by Customer, to conduct audits (including inspections) of Cintoo in order to verify Cintoo's compliance with its obligations under this DPA and especially with the Security Measures. The Customer and/or an independent third-party auditor may request an on-site audit, in which case Customer and/or the independent third-party auditor shall exercise this right by giving prior written notice at least thirty (30) calendar days prior to any audit or inspection, unless such on-site audit is required by a Supervisory Authority. Cintoo shall ensure that Customer is able to conduct an audit in accordance with this Section 9 and undertakes to assist the Customer in the execution of such inspections and audits. In the event of an audit request directly from a relevant Supervisory Authority, Cintoo shall assist the Customer in answering the request and organizing the audit. As described in Section 9.1 below, Customer shall not exercise this audit right more than once a year. Customer shall reimburse Cintoo for any time expended for such on-site audit at its then-current professional services rate, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, the Parties shall mutually agree upon the scope, timing and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. Customer shall promptly notify Cintoo with information regarding any non-compliance discovered during the course of an audit.

10 Data Protection Impact Assessment and Prior Consultation with Supervisory Authorities

10.1 **Data Protection Impact Assessment**. Upon Customer's request and Customer's cost, Cintoo shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation to carry out a data protection impact assessment related to Customer's use of the Services, to the extent that Customer does not otherwise have access to the relevant information, and to the extent that such information is available to Cintoo.

10.2 **Prior Consultation**. Upon Customer's request and Customer's cost, Cintoo shall provide reasonable assistance to Customer with any prior consultations to any Supervisory Authority or other competent data privacy authorities, which Customer reasonably considers to be required under the GDPR, in each case solely in relation to the processing of Customer Personal Data, and to the extent that Customer does not otherwise have access to the relevant information and to the extent that such information is available to Cintoo.

11 Data Subjects Rights

11.1 **Access, Correction, Blocking, Deletion and Portability**. During the term of the Agreement, Cintoo shall comply with any commercially reasonable request by Customer to access, amend, block, delete or retrieve Customer Personal Data, as required under the GDPR, to the extent Cintoo is legally permitted to do so.

11.2 **Data Subject Requests**. The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Personal Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from Data Subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Cintoo shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. Cintoo will provide reasonable assistance, including by appropriate technical and

organizational measures and considering the nature of the Processing, to enable Customer to respond to any request from Data Subjects seeking to exercise their rights under any Data Protection Law with respect to Customer Personal Data ("**Data Subject Request**"), to the extent permitted by the law. Under the GDPR, Customer has thirty (30) days to respond to a Data Subject Request. As a result, when Customer requires the assistance of Cintoo to respond to any Data Subject Request, Customer shall contact Cintoo within five (5) days of the receipt by Customer of the Data Subject Request. Customer remains solely responsible to respond to a Data Subject Request within the 30-days period and Cintoo shall not be held liable if Customer cannot respond to a Data Subject Request within this 30-days period if Customer required the assistance of Cintoo after the 5-days period mentioned here above. If such request is made directly to Cintoo, Cintoo will promptly inform Customer and will advise Data Subjects to submit their request to the Customer. Customer shall be solely responsible for responding to any Data Subjects' requests. Customer shall reimburse Cintoo for the costs arising from this assistance.

12 International Data Transfers

Processing locations: Cintoo stores Customer Personal Data inside the European Union within Microsoft Azure West Europe (Netherlands) and North Europe (Ireland) by default and within AWS (Germany). Customer Personal Data are processed inside the European Union. There is no Data Transfer outside the European Union.

13 Sub-processors

13.1 **Authorized Sub-processors**. Customer agrees that Cintoo may engage Sub-processors to process Customer Personal Data on Customer's behalf. The sub-processors currently engaged by Cintoo and hereby authorized by Customer are attached as Exhibit C

13.2 **Sub-processor obligations**. Cintoo shall: (i) enter into a written agreement with the sub-processor imposing data protection terms that require the sub-processor to protect the Customer Personal Data to the standard required by Data Protection Laws; (ii) and remain responsible for its compliance with the obligations of this DPA and for any act or omissions of the sub-processor that cause Cintoo to breach any of its obligations under this DPA.

13.3 **Changes to sub-processors**. Cintoo shall provide Customer reasonable advance notice (email shall suffice) if it adds or removes sub-processors.

13.4 **Right to object**. Customer may object in writing to Cintoo's appointment of a new sub-processor on reasonable grounds relating to data protection by notifying Cintoo promptly in writing within five (5) calendar days of receipt of Cintoo's notice in accordance with sub-section 13.3. Such notice shall explain the reasonable grounds for the objection. In such event, the Parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If this is not possible, either Party may terminate the applicable Services which cannot be provided by Cintoo without the use of the objected-to-new sub-processor.

14 Limitation of Liability :

Each party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the "limitation of liability" section of the Agreement. For the avoidance of doubt, Cintoo's total liability for all claims from Customer or any

third party arising out of or related to the Agreement and this DPA shall apply in the aggregate for all claims under both the Agreement and this DPA.

15 Term and Termination

The duration of the Processing shall be the term of the Agreement.

Both parties are entitled to terminate this DPA on the same terms as those which apply to the Agreement.

Upon either Customer's or Cintoo's (the "**non-breaching party**") reasonable knowledge of a material breach by the other party (the "**breaching party**") of its obligations under this DPA, such party shall: (i) provide reasonable written prior notice to the breaching party of the alleged breach under the DPA, (ii) provide an opportunity for the breaching party to cure the breach or otherwise terminate the Agreement and this DPA without penalty, (iii) in the event such breaching party does not cure the alleged breach within a reasonable amount of time, or terminate this DPA and the Agreement, and the non-breaching party's determination of the existence of a material breach was reasonable, terminate this DPA and the Agreement without penalty, or (iv) immediately terminate, without penalty, this DPA and the Agreement if the breaching party has breached a material term of this DPA and cure is not possible; or (v) if neither termination nor cure are feasible, report the violation to the Supervisory Authority.

Upon termination of the Agreement, for whatever reason, Processor shall cease processing any Personal Data on behalf of the Controller and, at the Controller's option, shall either (i) return to the Controller all of the Personal Data and any copies thereof which it is processing, has processed or have had processed on behalf of the Controller, in a format agreed upon with Controller or (ii) destroy the Personal Data within 15 calendar days of being requested to do so by the Controller and provide evidence of such destruction.

16 Miscellaneous.

16.1 **Order of Preference**. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

16.2 **Governing Law; Jurisdiction**. Unless required otherwise by applicable Data Protection Laws, this DPA shall be governed by and construed in accordance with the GDPR.In the event of any question, disputes or difference arising between the parties relating to the interpretation and application of this DPA, the parties require them to seek an out-of-court settlement before initiating legal proceedings. On failure to do so shall the dispute relating to this DPA be brought before a Court of competent jurisdiction in France.

16.3 **Update**s. Cintoo may update this DPA by providing no less than thirty (30) days' prior notice of any change to this DPA, unless prior notice is not practicable due to a conflict in applicable law or other changes outside of Cintoo's reasonable control.

16.4 **Severance**. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

EXHIBIT A
SUBJECT MATTER AND DETAILS OF PROCESSING

Subject Matter: Cintoo's provision of the Services and related technical support to Customer.

Duration: the term of this DPA and the Agreement plus the period from expiry of such term until deletion of all Customer Personal Data by Cintoo in accordance with Section 5.2 of this DPA.

Nature and Purpose of Processing: Cintoo shall process Customer Personal Data in order to provide to Customer and its End-Users the Services and related technical support to Customer in accordance with the Agreement and this DPA. More specifically, Customer instructs Cintoo to process Customer Personal Data for the following purposes:

(i) To perform, maintain and improve the Services for Customer and End-Users in accordance with this DPA, the Agreement, and Order Forms under the Agreement.
(ii) To provide technical support to Customer in accordance with the Agreement.
(iii) To comply with other reasonable documented instructions provided by Customer (e.g., email communications, chat platforms) where such instructions are consistent with the terms of the Agreement.
(iv) As otherwise required to Cintoo by applicable laws.

Categories of Data Subjects: Customer Personal Data processed concern the following categories of data subjects:

- Customer's employees, contractors, collaborators, business partners,
- Customer' customers, the personal of Customer's customers, suppliers and subcontractors,
- Any other individual invited by Customer or an End-User to use the Services,
- Any other individual whose Personal Data is transmitted to Cintoo in connection the Services by and at the discretion of the Customer.

Categories of Customer Personal Data:
Personal Data for Users:

(i) First and last name,
(ii) Email address,
(iii) Job position,
(iv) Company name,
(v) IP address,
(vi) Device and Browser information,

Personal Data for the Account Owner

(i) First and last name,
(ii) Email address,
(iii) Phone number,
(iv) Job position,
(v) Company name,
(vi) Company business address,
(vii) IP address,
(viii) Device and Browser information.

Cintoo shall not use any other Customer Personal Data, entered by Customer or End- User, except for categories of data, described in this Exhibit A. It is not Cintoo's obligation to monitor Customer Personal Data, entered or uploaded by Customer or End-User, to categorize or process it in any other way. It is the

Customer's responsibility to provide and guarantee that the processing Personal Data activities, performed by Customer and End-Users with the Services shall be compliant with the requirements of the GDPR.

EXHIBIT B
SECURITY MEASURES

Protecting Personal Information of our Customers and their End- is extremely important to Cintoo. We know you have questions about how we're protecting that Personal Information, so what follows are details about Cintoo's essential security measures.

Data Centers: Cintoo maintains data centers in Europe. Cintoo stores all production data in physically secure data centers with high availability and redundancy features.

Measures for pseudonymization/anonymization of Customer Personal Data: As of today, Cintoo does not take any measures for pseudonymization or anonymization of Customer Personal Data.

Measures for encryption of Customer Personal Data: All the web requested are encrypted with HTTPS. Connections to the Azure MySQL database are encrypted in SSL (AES256-SHA) and the database itself is encrypted at rest with Azure Storage using AES256.

Measure for ensuring ongoing confidentiality: Cintoo only allows access to Customer Personal Data to a restricted set of employees using such Customer Personal Data for administration or marketing purposes.

Access Control: Internal applications giving access to Customer Personal Data are only accessible with a personal password, and from the office network (including access via a VPN).

Measures for ensuring ongoing data integrity: Customer Personal Data can only be modified by the account owner (access protected by login / password).

Measures for ensuring availabilities of processing systems and services: Access to our Services has a high availability guaranteed by Microsoft Azure thanks to the usage of multiple virtual machines deployed in different availability sets. The database is backed up automatically by Microsoft Azure with a retention of 7 days, which allows to restore the data at any point in time in the previous week. There are also manual encrypted daily backups in another region.

Measures to ensure ongoing resilience of processing systems and services: Disaster recovery is ensured with Azure MySQL geo-redundant backups and the manual daily backups.

Measures to restore availability and access to personal data in the event of a technical of physical incident: Disaster recovery is ensured with Azure MySQL geo-redundant backups and the manual daily backups.

Procedures for periodical review, assessment, and evaluation: Disaster recovery plan is rehearsed and re-evaluated twice a year.

Microsoft Azure

- Personal Data storage and processing:
  - Microsoft Azure West / North Europe (Netherlands / Ireland)
- Project Data (3D data) storage and processing:
  - Any chosen region for project hosting, with several options in Europe
- Microsoft Azure DPA: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

AWS

- Project Data (3D data) storage and processing:
  - Any chosen region for project hosting, with several options in Europe
  - Default project data hosting is AWS Europe Central (Germany)
- Transactional emails sending:
  - AWS Germany
- AWS DPA: https://aws.amazon.com/fr/blogs/security/aws-gdpr-data-processing-addendum/

Freshdesk

- Technical support emails processing, sending and receiving
- Freshdesk DPA: https://www.freshworks.com/data-processing-addendum/

Stripe

- Invoicing and payment
- Stripe DPA: https://stripe.com/en-fr/legal/dpa

Datadog

- Monitoring
- Datadog DPA: Data Processing Addendum | Datadog (datadoghq.com)