Data Processing Agreement

This DPA has 2 parts: (1) the Key Terms on this Cover Page and (2) the Common Paper DPA Standard Terms Version 1 posted at commonpaper.com/standards/data-processing-agreement/1.0/ ("**DPA Standard Terms**"). A copy of the DPA Standard Terms is attached for convenience only. Any modifications to the Standard Terms should be made on the Cover Page. If there is any inconsistency between the parts of the DPA, the part listed earlier will control over the part listed later for that inconsistency. Capitalized words have the meanings or descriptions given in this Cover Page, the DPA Standard Terms, or the **Agreement**. However, if the Cover Page omits or does not define a highlighted word, the default meaning will be "none" or "not applicable". All other capitalized words have the meanings given in the Standard Terms.

Key Terms

The key legal terms of the DPA are as follows:

Approved Subprocessors	None. The Provider's server is hosted in Finland in a certified infrastructure (https://www.hetzner.com/unternehmen/zertifizierung)
Provider Security Contact	fabio.annovazzi@gmail.com
Security Policy	Provider will use commercially reasonable efforts to secure the Service from unauthorized access, alteration, or use and other unlawful tampering.
DPA Covered Claim	Without limiting the indemnity obligations in the **Agreement**, if any, **Provider** will indemnify, defend, and hold harmless **Customer** from and against any action, proceeding, or claim made by someone other than **Customer**, **Customer's** Affiliates, or Users, and all out-of-pocket damages, awards, settlements, costs, and expenses, including reasonable attorneys' fees and other legal expenses, that arise from **Provider's** gross negligence or willful misconduct, in each case, that results in a Security Incident.
DPA Liability Cap	However**, Provider's** total cumulative liability arising out of or related to **DPA Covered Claims** will not be more than the greater than 10 times the fees paid or payable by **Customer** to **Provider** in the 12-month period immediately before the claim.
Governing Law and Chosen Courts	Notwithstanding the governing law or similar clauses of the **Agreement**, all interpretations and disputes about this DPA will be governed by the laws of the **Governing State** without regard to its conflict of laws provisions. In addition, and notwithstanding the forum selection, jurisdiction, or similar clauses of the Agreement, the parties agree to bring any legal suit, action, or proceeding about this DPA in, and each party irrevocably submits to the exclusive jurisdiction of, the courts of the **Governing State**. **Governing State** means: Switzerland, Canton of Geneva
Restricted Transfers	
Governing Member State	EEA Transfers: Netherlands
Annex I(A) List of Parties	

Data Exporter	Name: Customer Address: Customer address Contact Person: TBD Position: TBD Address: TBD Activities relevant to transfer: See Annex 1(B)
Data Importer	Name: Fabio Annovazzi – 'Mparanza Address: 290 Route de Hermance, Anieres (CH) Activities relevant to transfer: See Annex 1(B) Role: Processor

Annex I(B) Description of Transfer and Processing Activities

Service	'Mparanza is a web-based business intelligence app that, based on an uploaded flat sales csv or excel dataset, allows the user to generate a large number of charts.
Categories of Data Subjects	Customer's users of the app
Categories of Personal Data	No personal data is processed by the Service. Data is never saved on disk. and discarded from RAM one session is closed. It is the customer's responsibility not to upload personal data or to anonymize it adequately.
Special Category Data **Is special category data Processed?**	No
Frequency of Transfer	Based on customer data uploads. Data is never saved on disk.
Nature and Purpose of Processing	Provider will never process Customer Personal Data. It is the responsibility of the customer not to upload personal data or to anonymize it appropriately. The nature of processing includes: • Receiving data in encrypted form. Data is never saved on disk. • Using data, including analysis. Sharing data or results of analysis is never allowed unless explicitly demanded and authorized in written form by the data exporter • Returning processed data (in the form of charts or of a csv file) to the data exporter • Erasing data from RAM. |Data is discarded from RAM one session is closed
Duration of Processing	Tied to duration of user session. All data is deleted from RAM at the end of each session. Recording data on disk is never allowed

Annex I(C)

Competent Supervisory Authority	The supervisory authority will be the supervisory authority of the data exporter, as determined in accordance with Clause 13 of the EEA SCCs or the relevant provision of the UK Addendum.

Annex II

Technical and Organizational Security Measures	**Pseudonymization and encryption of personal data:** No personal data is ever processed. It is the responsibility of the customer not to upload personal data, or to anonymize it adequately. **Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services:** Server is hosted in certified infrastructure. System is hardened based on best practices. **Ability to restore the availability of and access to Customer Personal Data in a timely manner following a physical or technical incident:** No personal data is ever processed or saved to disk.

Regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures used to secure Processing:
Penetration testing is performed regularly to check for vulnerabilities.

User identification and authorization process and protection:
There is not user identification mechanism. User sessions are never not logged in any way. The system does not use any cookies or other tracking mechanisms.

Protecting Customer Personal Data during transmission (in transit):
All data transmission is encrypted with SSL certificate. No personal data is ever processed. It is the customer's responsibility not to upload personal data or to anonymize it adequately.

Protecting Customer Personal Data during storage (at rest):
No data is ever stored on disk.

Physical security where Customer Personal Data is processed:
Code is regularly analyzed for issues that could lead to laps in security

Systems configuration, including default configuration:
Access to system is protected according to best practices

Provider and Customer have not changed the DPA Standard Terms except for the details on the Cover Page above. By signing this Cover Page, each party agrees to enter into this DPA as of the last date of signature below.

	PROVIDER:	CUSTOMER:
Signature		
Print Name	Fabio Annovazzi	
Title	Mr	
Date	March 2, 2023	

1. Processor and Subprocessor Relationships

1.1 Provider as Processor. In situations where **Customer** is a Controller of the Customer Personal Data, **Provider** will be deemed a Processor that is Processing Personal Data on behalf of **Customer**.

1.2 Provider as Subprocessor. In situations where **Customer** is a Processor of the Customer Personal Data, **Provider** will be deemed a Subprocessor of the Customer Personal Data.

2. Processing

2.1 Processing Details. Annex I(B) on the Cover Page describes the subject matter, nature, purpose, and duration of this Processing, as well as the **Categories of Personal Data** collected and **Categories of Data Subjects**.

2.2 Processing Instructions. **Customer** instructs **Provider** to Process Customer Personal Data: (a) to provide and maintain the Service; (b) as may be further specified through **Customer's** use of the Service; (c) as documented in the **Agreement**; and (d) as documented in any other written instructions given by **Customer** and acknowledged by **Provider** about Processing Customer Personal Data under this DPA. **Provider** will abide by these instructions unless prohibited from doing so by Applicable Laws. **Provider** will immediately inform **Customer** if it is unable to follow the Processing instructions. **Customer** has given and will only give instructions that comply with Applicable Laws.

2.3 Processing by Provider. **Provider** will only Process Customer Personal Data in accordance with this DPA, including the details in the Cover Page. If **Provider** updates the Service to update existing or include new products, features, or functionality, **Provider** may change the **Categories of Data Subjects**, **Categories of Personal Data**, **Special Category Data**, **Special Category Data Restrictions or Safeguards**, **Frequency of Transfer**, **Nature and Purpose of Processing**, and **Duration of Processing** as needed to reflect the updates by notifying **Customer** of the updates and changes.

2.4 Customer Processing. Where **Customer** is a Processor and **Provider** is a Subprocessor, **Customer** will comply with all Applicable Laws that apply to **Customer's** Processing of Customer Personal Data. **Customer's** agreement with its Controller will similarly require **Customer** to comply with all Applicable Laws that apply to **Customer** as a Processor. In addition, **Customer** will comply with the Subprocessor requirements in **Customer's** agreement with its Controller.

2.5 Consent to Processing. **Customer** has complied with and will continue to comply with all Applicable Data Protection Laws concerning its provision of Customer Personal Data to **Provider** and/or the Service, including making all disclosures, obtaining all consents, providing adequate choice, and implementing relevant safeguards required under Applicable Data Protection Laws.

2.6 Subprocessors.

(a) **Provider** will not provide, transfer, or hand over any Customer Personal Data to a Subprocessor unless **Customer** has approved the Subprocessor. The current list of **Approved Subprocessors** includes the identities of the Subprocessors, their country of location, and their anticipated Processing tasks. **Provider** will inform **Customer** at least 10 business days in advance and in writing of any intended changes to the **Approved Subprocessors** whether by addition or replacement of a Subprocessor, which allows **Customer** to have enough time to object to the changes before the **Provider** begins using the new Subprocessor(s). **Provider** will give **Customer** the information necessary to allow **Customer** to exercise its right to object to the change to **Approved Subprocessors**. **Customer** has 30 days after notice of a change to the **Approved Subprocessors** to object, otherwise **Customer** will be deemed to accept the changes. If **Customer** objects to the change within 30 days of notice, **Customer** and **Provider** will cooperate in good faith to resolve **Customer's** objection or concern.

(b) When engaging a Subprocessor, **Provider** will have a written agreement with the Subprocessor that ensures the Subprocessor only accesses and uses Customer Personal Data (i) to the extent required to perform the obligations subcontracted to it, and (ii) consistent with the terms of **Agreement**.

(c) If the GDPR applies to the Processing of Customer Personal Data, (i) the data protection obligations described in this DPA (as referred to in Article 28(3) of the GDPR, if applicable) are also imposed on the Subprocessor, and (ii) **Provider's** agreement with the Subprocessor will incorporate these obligations, including details about how **Provider** and its Subprocessor will coordinate to respond to inquiries or requests about the Processing of Customer Personal Data. In addition, **Provider** will share, at **Customer's** request, a copy of its agreements (including any amendments) with its Subprocessors. To the extent necessary to protect business secrets or other confidential information, including personal data, **Provider** may redact the text of its agreement with its Subprocessor prior to sharing a copy.

(d) **Provider** remains fully liable for all obligations subcontracted to its Subprocessors, including the acts and omissions of its Subprocessors in Processing Customer Personal Data. **Provider** will notify **Customer** of any failure by its Subprocessors to fulfill a material obligation about Customer Personal Data under the agreement between **Provider** and the Subprocessor.

3. Restricted Transfers

3.1 Authorization. **Customer** agrees that **Provider** may transfer Customer Personal Data outside the EEA, the United Kingdom, or other relevant geographic territory as necessary to provide the Service. If **Provider** transfers Customer Personal Data to a territory for which the European Commission or other relevant supervisory authority has not issued an adequacy decision, **Provider** will implement appropriate safeguards for the transfer of Customer Personal Data to that territory consistent with Applicable Data Protection Laws.

3.2 Ex-EEA Transfers. **Customer** and **Provider** agree that if the GDPR protects the transfer of Customer Personal Data, the transfer is from **Customer** from within the EEA to **Provider** outside of the EEA, and the transfer is not governed by an adequacy decision made by the European Commission, then by entering into this DPA, **Customer** and **Provider** are deemed to have signed the EEA SCCs and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the EEA SCCs, which are completed as follows:

(a) Module Two (Controller to Processor) of the EEA SCCs apply when **Customer** is a Controller and **Provider** is Processing Customer Personal Data for **Customer** as a Processor.

(b) Module Three (Processor to Sub-Processor) of the EEA SCCs apply when **Customer** is a Processor and **Provider** is Processing Customer Personal Data on behalf of **Customer** as a Subprocessor.

(c) For each module, the following applies (when applicable):

(i) The optional docking clause in Clause 7 does not apply;

(ii) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes is 10 business days;

(iii) In Clause 11, the optional language does not apply;

(iv) All square brackets in Clause 13 are removed;

(v) In Clause 17 (Option 1), the EEA SCCs will be governed by the laws of **Governing Member State**;

(vi) In Clause 18(b), disputes will be resolved in the courts of the **Governing Member State**; and

(vii) The Cover Page to this DPA contains the information required in Annex I, Annex II, and Annex III of the EEA SCCs.

3.3 Ex-UK Transfers. **Customer** and **Provider** agree that if the UK GDPR protects the transfer of Customer Personal Data, the transfer is from **Customer** from within the United Kingdom to **Provider** outside of the United Kingdom, and the transfer is not governed by an adequacy decision made by the United Kingdom Secretary of State, then by entering into this DPA, **Customer** and **Provider** are deemed to have signed the UK Addendum and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the UK Addendum, which is completed as follows:

(a) Section 3.2 of this DPA contains the information required in Table 2 of the UK Addendum.

(b) Table 4 of the UK Addendum is modified as follows: Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum; to the extent ICO issues a revised Approved Addendum under Section 18 of the UK Addendum, the parties will work in good faith to revise this DPA accordingly.

(c) The Cover Page contains the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum.

3.4 Other International Transfers. For Personal Data transfers where Swiss law (and not the law in any EEA member state or the United Kingdom) applies to the international nature of the transfer, references to the GDPR in Clause 4 of the EEA SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority will include the Swiss Federal Data Protection and Information Commissioner.

4. Security Incident Response

Upon becoming aware of any Security Incident, **Provider** will: (a) notify **Customer** without undue delay when feasible, but no later than 72 hours after becoming aware of the Security Incident; (b) provide timely information about the Security Incident as it becomes known or as is reasonably requested by **Customer**; and (c) promptly take reasonable steps to contain and investigate the Security Incident. **Provider's** notification of or response to a Security Incident as required by this DPA will not be construed as an acknowledgment by **Provider** of any fault or liability for the Security Incident.

5. Audit & Reports

5.1 Audit Rights. **Provider** will give **Customer** all information reasonably necessary to demonstrate its compliance with this DPA and **Provider** will allow for and contribute to audits, including inspections by **Customer**, to assess **Provider's** compliance with this DPA. However, **Provider** may restrict access to data or information if **Customer's** access to the information would negatively impact **Provider's** intellectual property rights, confidentiality obligations, or other obligations under Applicable Laws. **Customer** acknowledges and agrees that it will only exercise its audit rights under this DPA and any audit rights granted by Applicable Data Protection Laws by instructing **Provider** to comply with the reporting and due diligence requirements below. **Provider** will maintain records of its compliance with this DPA for 3 years after the DPA ends.

5.2 Security Reports. **Customer** acknowledges that **Provider** is regularly audited against the standards defined in the **Security Policy** by independent third-party auditors. Upon written request, **Provider** will give **Customer**, on a confidential basis, a summary copy of its then-current Report so that **Customer** can verify **Provider's** compliance with the standards defined in the **Security Policy**.

5.3 Security Due Diligence. In addition to the Report, **Provider** will respond to reasonable requests for information made by **Customer** to confirm **Provider's** compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, or by giving additional information about its information security program. All such requests must be in writing and made to the **Provider Security Contact** and may only be made once a year.

6. Coordination & Cooperation

6.1 Response to Inquiries. If **Provider** receives any inquiry or request from anyone else about the Processing of Customer Personal Data, **Provider** will notify **Customer** about the request and **Provider** will not respond to the request without **Customer's** prior consent. Examples of these kinds of inquiries and requests include a judicial or administrative or regulatory agency order about Customer Personal Data where notifying **Customer** is not prohibited by Applicable Law, or a request from a data subject. If allowed by Applicable Law, **Provider** will follow **Customer's** reasonable instructions about these requests, including providing status updates and other information reasonably requested by **Customer**. If a data subject makes a valid request under Applicable Data Protection Laws to delete or opt out of **Customer's** giving of Customer Personal Data to **Provider**, **Provider** will assist **Customer** in fulfilling the request according to the Applicable Data Protection Law. **Provider** will cooperate with and provide reasonable assistance to **Customer**, at **Customer's** expense, in any legal response or other procedural action taken by **Customer** in response to a third-party request about **Provider's** Processing of Customer Personal Data under this DPA.

6.2 DPIAs and DTIAs. If required by Applicable Data Protection Laws, **Provider** will reasonably assist **Customer** in conducting any mandated data protection impact assessments or data transfer impact assessments and consultations with relevant data protection authorities, taking into consideration the nature of the Processing and Customer Personal Data.

7. Deletion of Customer Personal Data

7.1 Deletion by Customer. **Provider** will enable **Customer** to delete Customer Personal Data in a manner consistent with the functionality of the Services. **Provider** will comply with this instruction as soon as reasonably practicable except where further storage of Customer Personal Data is required by Applicable Law.

7.2 Deletion at DPA Expiration.

(a) After the DPA expires, **Provider** will return or delete Customer Personal Data at **Customer's** instruction unless further storage of Customer Personal Data is required or authorized by Applicable Law. If return or destruction is impracticable or prohibited by Applicable Laws, **Provider** will make reasonable efforts to prevent additional Processing of Customer Personal Data and will continue to protect the Customer Personal Data remaining in its possession, custody, or control. For example, Applicable Laws may require **Provider** to continue hosting or Processing Customer Personal Data.

(b) If **Customer** and **Provider** have entered the EEA SCCs or the UK Addendum as part of this DPA, **Provider** will only give **Customer** the certification of deletion of Personal Data described in Clause 8.1(d) and Clause 8.5 of the EEA SCCs if **Customer** asks for one.

8. Limitation of Liability

8.1 Liability Caps and Damages Waiver. **To the maximum extent permitted under Applicable Data Protection Laws, each party's total cumulative liability to the other party arising out of or related to this DPA will be subject to the waivers, exclusions, and limitations of liability stated in the Agreement.**

8.2 Related-Party Claims. **Any claims made against Provider or its Affiliates arising out of or related to this DPA may only be brought by the Customer entity that is a party to the Agreement.**

8.3 Exceptions. This DPA does not limit any liability to an individual about the individual's data protection rights under Applicable Data Protection Laws. In addition, this DPA does not limit any liability between the parties for violations of the EEA SCCs or UK Addendum.

9. Conflicts Between Documents

This DPA forms part of and supplements the **Agreement**. If there is any inconsistency between this DPA, the **Agreement**, or any of their parts, the part listed earlier will control over the part listed later for that inconsistency: (1) the EEA SCCs or the UK Addendum, (2) this DPA, and then (3) the **Agreement**.

10. Term of Agreement

This DPA will start when **Provider** and **Customer** agree to a Cover Page for the DPA and sign or electronically accept the **Agreement** and will continue until the **Agreement** expires or is terminated. However, **Provider** and **Customer** will each remain subject to the obligations in this DPA and Applicable Data Protection Laws until **Customer** stops transferring Customer Personal Data to **Provider** and **Provider** stops Processing Customer Personal Data.

11. Definitions.

11.1 "**Applicable Laws**" means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern a party.

11.2 "**Applicable Data Protection Laws**" means the Applicable Laws that govern how the Service may process or use an individual's personal information, personal data, personally identifiable information, or other similar term.

11.3 "**Controller**" will have the meaning(s) given in the Applicable Data Protection Laws for the company that determines the purpose and extent of Processing Personal Data.

11.4 "**Cover Page**" means a document that is signed or electronically accepted by the parties that incorporates these DPA Standard Terms and identifies **Provider**, **Customer**, and the subject matter and details of the data processing.

11.5 "**Customer Personal Data**" means Personal Data that **Customer** uploads or provides to **Provider** as part of the Service and that is governed by this DPA.

11.6 "**DPA**" means these DPA Standard Terms, the Cover Page between **Provider** and **Customer**, and the policies and documents referenced in or attached to the Cover Page.

11.7 "**EEA SCCs**" means the standard 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 European Council.

11.8 "**European Economic Area**" or "**EEA**" means the member states of the European Union, Norway, Iceland, and Liechtenstein.

11.9 "**GDPR**" means European Union Regulation 2016/679 as implemented by local law in the relevant EEA member nation.

11.10 "**Personal Data**" will have the meaning(s) given in the Applicable Data Protection Laws for personal information, personal data, or other similar term.

11.11 "**Processing**" or "**Process**" will have the meaning(s) given in the Applicable Data Protection Laws for any use of, or performance of a computer operation on, Personal Data, including by automatic methods.

11.12 "**Processor**" will have the meaning(s) given in the Applicable Data Protection Laws for the company that Processes Personal Data on behalf of the Controller.

11.13 "**Report**" means audit reports prepared by another company according to the standards defined in the Security Policy on behalf of **Provider**.

11.14 "**Restricted Transfer**" means (a) where the 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 (b) where the UK GDPR applies, a transfer of personal

data from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

11.15 "**Security Incident**" means a Personal Data Breach as defined in Article 4 of the GDPR.

11.16 "**Service**" means the product and/or services described in the **Agreement**.

11.17 "**Special Category Data**" will have the meaning given in Article 9 of the GDPR.

11.18 "**Subprocessor**" will have the meaning(s) given in the Applicable Data Protection Laws for a company that, with the approval and acceptance of Controller, assists the Processor in Processing Personal Data on behalf of the Controller.

11.19 "**UK GDPR**" means European Union Regulation 2016/679 as implemented by section 3 of the United Kingdom's European Union (Withdrawal) Act of 2018 in the United Kingdom.

11.20 "**UK Addendum**" means the international data transfer addendum to the EEA SCCs issued by the Information Commissioner for Parties making Restricted Transfers under S119A(1) Data Protection Act 2018.