Mautic Trials Data Processing Agreement

Between:

Company name:

Company address:

Company number:

Duly represented by:

Function:

Hereinafter referred to as the “Controller”;

The main GDPR contact person’s name:

Contact e-mail address:

Contact phone number:

And:

Open Source Collective on behalf of Mautic, 440 N Barranca Ave #3939 Covina, CA 91723 ;
Hereinafter referred to as the “Processor”;

The contact e-mail address of the processor for all related matters concerning privacy legislation and this processor agreement is info@mautic.org.

The parties to this agreement are hereinafter collectively referred to as the “Parties” and individually as a “Party”.;

Whereas:

1. This personal data processing agreement (the “Agreement”) is concluded pursuant to, and is an integral part of, the Mautic Trials Agreement between the Parties (the “Trials

Agreement")];

2. Within the scope of the Trials Agreement Personal Data will be transferred to and processed by the Processor;

3. In the Agreement, the Parties wish to set out the conditions under which Personal Data will be transferred and processed within the scope of the Trials Agreement; The provisions of this Agreement do not affect the rights and obligations between the Parties which do not relate to processing Personal Data;

4. The definitions used in the Agreement are those included in the Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "General Data Protection Regulation");

The parties agree as follows:

1. Objective of the agreement

1.1. The Controller processes Personal Data of the data subjects listed in Annex I (the "Data Subjects") as a result of the processing purposes listed in Annex I (the "Processing Purposes") that the Processor performs for and on behalf of the Controller. For these Processing Purposes the Controller shall provide the Processor with the Data Subjects' categories of Personal Data listed in Annex I (the "Personal Data").

1.2. The Personal Data will be processed by the Processor for the entire duration of the Trials Agreement.

2. Use

2.1. The Processor and every person under its responsibility or authority, shall process the Personal Data on behalf of the Controller and only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of such legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.2. The Processor processes the Personal Data in accordance with the Processing Purposes, unless it is subject to a legal obligation whereby it is required to perform another processing activity. In such a case, the Processor shall inform

the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3. Duties of the parties

3.1. The Parties will comply with the provisions of the General Data Protection Regulation, and any other legal requirement concerning data protection. In particular, the Parties undertake to:

3.1.1. Maintain a record of processing activities that take place under their authority. This register shall contain the information set forth in article 30 of the General Data Protection Regulation and shall be updated on a regular basis;

3.1.2. Provide the necessary cooperation to the competent data protection authority/authorities in the fulfillment of their duties;

3.1.3. To designate a data protection officer in the cases provided for in article 37 of the General Data Protection Regulation or if this is required by Union or Member State law. In cases other than those referred to above, the Controller and the Processor may choose to designate a data protection officer.

3.2. The Processor shall implement appropriate technical and organizational measures to ensure and demonstrate that the processing of the Personal Data is carried out in accordance with the General Data Protection Regulation. The Processor shall implement at least the following measures:

3.2.1. On a regular basis, the Processor shall inform each person (internally or externally) who intervenes in the processing of the Personal Data about their duties and responsibilities with respect to the processing and provide suitable training for these persons regarding the performance of their functions and their responsibilities in respect of information security;

3.2.2. The Processor shall draft a management plan for security incidents. This management plan must contain at least the notification duty provided for in article 3.8 of the Agreement.

The Processor shall inform the Controller of the measures taken.

3.3. Given the performance of the information security policy and the prevention of Personal Data Breaches, the Processor shall implement the appropriate technical and organizational measures to protect against accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed (the “Personal Data Breach(es)”).

These measures correspond to the latest state of the art regarding security and ensure a level of security that corresponds to the risks of the processing. The Processor shall implement at least the following measures:

3.3.1. The use of access codes, usernames and passwords by authorized persons in order to have access to (the carriers of the) Personal Data and to process them. The Processor shall change these codes and passwords repeatedly. The Processor ensures that the authorized persons respect the confidentiality of these codes and passwords;

3.3.2. Placing the carriers of the Personal Data and IT systems that process the Personal Data in identified and protected premises whereby access is limited to the persons authorized by the Processor and to the hours during which they perform their duties;

3.3.3. Installing and maintaining devices for the prevention, detection and handling of physical threats such as fires or floods in the premises where the carriers of the Personal Data and/or the IT systems that process the Personal Data are located;

3.3.4. The Processor ensures that the networks, with which the equipment or IT systems that process the Personal Data are connected, guarantee the confidentiality and integrity of the Personal Data;

3.3.5. The installation of logging and detection mechanisms that register the identity of every person that has access to the Personal Data or processes them.

The Processor shall inform the Controller of the measures taken.

3.4. The Processor shall not act nor allow anyone to act in breach of the provisions of the Agreement.

3.5. Without prejudice to article 2.1 and 5 of the Agreement, the Controller agrees with the transfers of Personal Data by the Processor to third parties who participate directly to the processing. Unless the transfer is anonymised and is performed with the written consent of the Controller or pursuant to an international or national law, the Processor shall not transfer the Personal Data to third parties that are not directly involved in the processing. In such a case, the Processor shall inform the Controller of that legal requirement and the transfer of Personal Data to third parties.

3.6. The Processor has the right to make a copy of the Personal Data if the Controller has given its prior consent and it is necessary for performing the Processing

Purposes in accordance with article 1.1 of the Agreement that has been assigned to him by the Controller. The Processor can also make back-ups if the Controller has given its prior consent. The Processor has to abide by the same rules for the use of these copies and back-ups as for the use of the original Personal Data.

3.7. The Processor shall inform the Controller if a Personal Data Breach has occurred. This notification must happen immediately after becoming aware of this Personal Data Breach, to the person appointed in Annex I.

3.8. The Processor shall assist the Controller in meeting its obligations under the General Data Protection Regulation regarding the timely notification of a Personal Data Breach to the supervisory authority, the communication thereof to Data Subjects, and the measures that are (to be) taken to address the Personal Data Breach.

3.9. If the Data Subject issues a request for exercising its rights laid down in Chapter 3 of the General Data Protection Regulation, the Processor shall inform the Controller immediately. At the Controller's request, the Processor shall assist the Controller by appropriate technical and organizational measures for the fulfillment of the Controller's obligation to respond to these requests in accordance with the General Data Protection Regulation.

3.10. The Processor shall assist the Controller with the Controller's obligation to implement appropriate technical and organizational measures in accordance with article 32 of the General Data Protection Regulation.

3.11. The Processor will make available to the Controller all information necessary to demonstrate compliance of the processing with the Agreement.

3.12. The Controller is entitled (to mandate an auditor) to conduct an audit of the Processor's processing of the Personal Data at any time during normal business hours. The audit shall be preceded by a minimum of four week's notice. The Processor shall make available all information necessary for the performance of the audit by the Controller or an auditor. The Controller shall bear all reasonable costs of the audit, including the reasonable costs made by the Processor to perform the audit.

3.13. The Processor shall immediately inform the Controller if an instruction infringes the General Data Protection Regulation or another law regarding data protection. The Processor is entitled to refuse to perform the instruction until it has been aligned with the General Data Protection Regulation.

3.14. At the explicit request of the Controller and if applicable, the Processor shall provide the Controller with a copy of the Personal Data being processed under

the Agreement.

4. Representations and warranties

4.1. The Parties ensure the integrity, confidentiality and accuracy of all the Personal Data being processed within the scope of the Agreement.

4.2. The Processor shall supervise that the Personal Data can only be accessed by the authorized persons and application programs. The authorized persons who process the Personal Data under its responsibility and authority, shall only have access to the Personal Data necessary to perform their task within the scope of the Agreement. The Processor shall inform these persons of the provisions of the General Data Protection Regulation.

4.3. The Processor ensures that no IT system, software or other appliance used for the processing of Personal Data infringes the intellectual property rights of any third parties.

5. Sub-processors

5.1. The Processor shall not engage another processor (the “Sub-processor”) to carry out a specific processing activity on behalf of the Controller without the prior specific written authorisation of the Controller.

5.2. The Processor shall by way of a contract impose on the Sub-processor the same obligations and guarantees as provided for in the Agreement, and ensures that the Sub-processor will implement the appropriate technical and organizational measures in such a manner to ensure and be able to demonstrate that the processing is performed in accordance with the General Data Protection Regulation.

5.3. The Processor shall remain fully liable to the Controller for the performance of the Sub-processor’s obligations. The Processor shall indemnify the Controller in accordance with article 9.1 of the Agreement against the acts or omissions of the Sub-processor in violation of the Agreement.

6. Confidentiality

6.1. The Processor and every person authorized to process the Personal Data shall respect the confidentiality and integrity of the Personal Data. The Processor

ensures that the persons having access to the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.2. The confidentiality obligation of article 6.1 of the Agreement shall remain in force after the termination of the Agreement.

7. Intellectual property

7.1. Unless otherwise agreed between the Parties, all intellectual property rights in connection with the (carriers of the) Personal Data shall belong to the Controller. The Processor is only granted an individual and non-transferable right of use for the authorized persons.

7.2. Without prejudice to article 7.1 of the Agreement, all intellectual property rights in connection with the software developed and delivered by the Processor, shall remain the sole property of the Processor.

8. Duration and termination of the Agreement

8.1. The Agreement enters into force on the same date as the Trials Agreement (“Commencement Date”) and remains in effect for the duration of the Trials Agreement.

8.2. After the end of the Trials Agreement, the Processor shall terminate the processing, unless the Parties decide otherwise. The Processor shall delete or return, at the choice of the Controller, all the Personal Data in its possession, as well as every existing copy or back-up made in accordance with article 3.6 of the Agreement, unless the storage of the Personal Data is legally required.

8.3. At the explicit request of the Controller, the Processor shall provide an actual copy of the database(s) containing the processed Personal Data, prior to the termination date of the Trial Services Agreement via an export of their instance.

8.4. The Processor ensures that any Sub-Processor shall terminate the processing of the Personal Data and delete all the Personal Data from its files upon termination of the Agreement.

8.5. The Processor shall inform every third party involved in the processing that it is no longer participating in the processing.

9. Liability

9.1. Notwithstanding any provision to the contrary in the Trials Agreement, the Processor is liable for the damage that directly stem from or relate to an infringement or caused by the non-performance of its duties under the Agreement. The Processor shall hold harmless and indemnify the Controller against all complaints or claims of the competent data protection authority, a Data Subject or a third party under the General Data Protection Regulation, to the extent that the complaint or claim is the result of an act or negligence on the part of the Processor in violation of the Agreement, limited to the amount claimable under professional liability insurance in the case in question . Neither Party shall be liable for any indirect or consequential damage, such as (but not limited to) loss of revenue, loss of profit, loss of opportunity or third party claims.

9.2. The Processor shall not be exempt from its warranty obligation referred to in article 9.1 of the Agreement by invoking breaches committed by third parties. The Processor shall neither be exempt from its warranty obligation by declaring that it acted in accordance with the instructions of the Controller which violate the General Data Protection Regulation or any other legal provision.

10. Severability

10.1. In the event any (part of a) provision of this Agreement is found to be invalid, illegal or unenforceable, then the offending provision shall not render any other provision of this Agreement invalid or unenforceable, and all other provisions shall remain in full force and effect and shall be enforceable. The Parties shall in good faith negotiate and replace such provision(s) with (a) provision(s) that is/are valid and enforceable and ensures the same or as approximate an effect as possible as the one aspired by the Parties with the invalid, illegal or unenforceable provision(s).

11. Applicable law and jurisdiction

11.1. The Agreement shall be exclusively governed by and construed in accordance with the laws of Belgium. The Courts of Ghent shall have sole jurisdiction over any claim or controversy arising hereunder, if the Parties cannot find a mutual agreement.

12. General provisions

12.1. The terms and conditions of the Agreement shall be interpreted in light of the General Data Protection Regulation. In case this regulation does not offer a clear and unambiguous interpretation, the terms and conditions shall be given the interpretation that ensures the same or as approximate an effect as possible as the one aspired by the Parties.

12.2. In the event of any conflicting provisions between the Trials Agreement and the Agreement, the terms of the Agreement shall take precedence over the terms of the Trials Agreement. None of the Parties shall be deemed to have waived any of the rights arising from the Agreement or any of the rights arising from an error or infringement committed by the other Party, unless the first Party has explicitly confirmed such waiver in writing.

Annexes:

- ANNEX 1: Overview of the personal data to be processed
- ANNEX 2: Technical and Organizational measures (TOM)

Signatures

IN WITNESS HEREOF, the Parties have signed the Agreement on date _____ :

The controller

Name

Function

Signature

The processor

Name Lauren Gardner

Function Executive Director, Open Source Collective

Signature 

Annex 1: Overview of the personal data to be processed

This Appendix 1 contains certain details regarding the processing of Personal Data as required by Article 28 (3) GDPR.

Subject of the processing of Personal Data

The Processing of Personal Data takes place in the context of the performance of Services that the Processor offers, as described in the Mautic Trials Agreement.

The Controller always has access via the Mautic instance to the Personal Data that visitors leave on the website. The Processor recommends that this data be deleted regularly after the Personal Data is no longer relevant to be processed (e.g. a dormant contact).

Nature and purpose of the processing of Personal Data

The personal data may only be processed by the Processor if and insofar as this is necessary for the performance of the Main Agreement, including but not limited to collection, storage, structures, consultation, transfer of Personal Data, on the instructions of the Controller (e.g. to other software)

Categories of processing Personal Data

(indicate what is applicable)

✓ Identification data, such as but not limited to name, surname, e-mail, data via contact forms on the website, e-mail addresses to subscribe to newsletters, IP-addresses.
❏ Financial data
❏ Invoice data
❏ Wages data
❏ Personal characteristics, such as but not limited to age, gender, birth date, civil status
❏ Lifestyle habits
❏ Composition of the family, such as but not limited to data marriage, name partner and children.
❏ Interests and sports
❏ Memberships, specifically asked via contact form, being
.....
❏ Education and curriculum, such as academic curriculum, professional qualifications and education
❏ Profession
❏ National Insurance Number

❏ Video recordings
❏ Audio recordings
❏ Other specific categories which the Controller are processed by the Data Processor:
.....

Attention, if special categories of personal data, such as specified in art 9 AVG are being processed :

❏ Genetical data with remark to the unique identification of a person
❏ Data about health
❏ Data about race or ethnic offenses
❏ Data about political views
❏ Data about religious or philosophical belief
❏ Data about union membership
❏ Data about sexual behavior of de sexual orientation
❏ Processing of Personal Data about criminal offenses, as stipulated in art 10 AVG.

Annex 2: Technical and Organizational Measures (TOM)

The technical and organizational measures are implemented by the Provider of the Trials Services in accordance with Art 32 GDPR. They are continuously improved by the Provider according to feasibility and brought to a higher level of security and protection.

1. Confidentiality

1.1. Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

Technical Measures

- Alarm system
- Automatic access control system
- Server room is locked and limited to IT staff
- Backup Server is located in an external location

Organizational Measures

- Reception / Receptionist at building entrance
- Visitors accompanied by employees
- Clean desk policy

1.2. System Authorisation

Measures suitable for preventing data processing systems from being used by unauthorized persons.

Technical Measures

- Login with username + password
- Anti-Virus Software
- Firewall
- Use of VPN for remote access
- Two-factor authentication in data center and for critical systems

Organizational Measures

- User permission management
- Password policy

1.3. Data Authorization

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Technical and organizational measures

- Logging of accesses to applications, specifically when entering, changing, and deleting data
- Use of authorization concepts
- Minimum number of administrators

1.4. Data Separation

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical and organizational measures

- Separation of productive and test environment
- Physical separation (systems / databases / data carriers)
- Multi-tenancy of relevant applications
- Client systems logically separated
- Staging of development, test and production environment
- Separated storage of customer data

2. Integrity

2.1. Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures

- Use of VPN when agreed upon with clients
- Logging of accesses and retrievals
- Provision via encrypted connections such as sftp, https and secure cloudstores
- Use of signature procedures (case¬dependent)

- When using external networks for transmission of personal data, encryption methods are available, such as TLS, SFTP

Organizational Measures

- Information Security Policy
- Data Protection Policy

2.2. Input Control

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical and organizational measures

- Unique user ID is in place
- Admin activities are recorded
- Technical logging of the entry, modification and deletion of data
- Survey of which programs can be used to enter, change or delete
- Manual or automated control of the logs
- Traceability of data entry, modification and deletion
- Retention of forms from which data has been transferred to automated processes
- Clear responsibilities for deletions

3. Availability and Resilience

3.1. Availability Control

Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).

Technical Measures

- Fire and smoke detection systems
- Fire extinguisher

Organizational Measures

- Backup concept
- Existence of an emergency plan
- Storage of backup media in a secure location

- Data recovery process and penetration tests can be performed on request to ensure the robustness of the data processing

3.2. Recoverability Control

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical Measures

- Backup monitoring and reporting
- Restorability from automation tools
- Backup concept according to criticality and customer specifications

Organizational Measures

- Recovery concept
- Control of the backup process
- Storage of backup media in a safe place outside the server room

4. Procedures for regular Review, Assessment and Evaluation

4.1. Data Protection Management

Measures especially designed to keep the measures for data security described here up to date.

- Central documentation of all data protection regulations with access for employees
- Internal Privacy Officer appointed
- Internal Information Security Officer appointed
- Staff trained and obliged to confidentiality/data secrecy
- Regular awareness trainings
- Formalized process for requests for information from data subjects is in place

4.2. Incident Response Management

Support for security breach response and data breach process.

- Formalized procedure for handling security incidents
- Involvement of privacy officer in security incidents and data breaches
- Documentation of security incidents and data breaches via ticket system
- A formal process for following up on security incidents and data breaches
- Providers are contracted to report incidents and to take appropriate actions

4.3. Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

Organizational Measures

- No more personal data is collected than is necessary for the respective purpose
- Use of data protection-friendly default settings in standard and individual software

4.4. Order Control (outsourcing, subcontractors and order processing)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

- Monitoring of remote access by external parties, e.g. in the context of remote support
- Work instruction supplier management and supplier evaluation
- Monitoring of subcontractors
- Selection of the contractor with regard to data protection and data security
- Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
- Written instructions to the contractor
- Agreement on effective control rights over the contractor
- Ensuring the destruction of data after termination of the contract

5. Organization and Data Protection at Dropsolid

Dropsolid has set itself the goal of providing its customers with the products and services to be delivered at the highest possible level of information security in compliance with the law.

A set of binding policies on implementing data protection and information security are established at Dropsolid by the management. These policies are fixed in writing, freely accessible, communicated to all employees and relevant external parties, and applied.

Employees are continuously informed and trained in the area of data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External parties who may come into contact with personal data in the course of their work for Dropsolid are obligated to maintain secrecy and confidentiality as well as to comply with data protection and data secrecy by means of a so-called NDA (Non-Disclosure Agreement) before they begin their work.

Any subcontractors entrusted with further processing (as “other processors”) are only used after approval as Controller and after conclusion of a Data Processing Agreement (DPA) in accordance with Art 28 GDPR, with which they are fully bound by all data protection obligations to which Dropsolid itself is subject.

All of these organizational measures are flanked by Dropsolid’s current, high technical security standards, and both dimensions are periodically reviewed and confirmed for adequacy and effectiveness in the course of ongoing internal audits.