

DATA PROCESSING AGREEMENT

(hereinafter the "**DPA**")

Status: 13/03/2024

1. Scope

- 1.1. Swat.io GmbH, with its registered office in Vienna, registered in the commercial register of the Commercial Court of Vienna under FN 348798p (hereinafter referred to as the "**Processor**"), shall provide all processing of personal data on behalf of its Controller (hereinafter each the "**Controller**" and each Controller together with the Processor the "**Parties**") on the basis of this DPA, in each case in the version valid at the time of conclusion of the contract.
- 1.2. The provisions of this DPA may be amended by the Processor at any time without stating reasons, whereby such amendments shall be announced on the Processor's website at least 30 days before they come into force and by sending the text of the contract to the email address last notified by the Controller. If the Controller does not object to the changes within 30 days of receipt of the aforementioned announcement in writing by email to privacy@swat.io, the changes shall be deemed accepted. In the event of a timely objection by a Controller, the contractual relationship between this Controller and the Processor shall continue in accordance with the DPA in the version prior to the announced amendment, whereby the Processor shall be entitled to terminate the DPA without stating reasons by giving 14 days' notice to the last day of the month.
- 1.3. The Processor shall carry out the processing of personal data described in Annex ./1 on behalf of the Controller (hereinafter the "**Data Processing**") under the Main Agreement concluded between the Parties for the use of the social media management software operated by Swat.io (hereinafter the "**Main Agreement**").

2. Place of processing

- 2.1. The Data Processing shall take place in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area, unless otherwise agreed between the Parties. The Data Processing by the sub-processors named in Annex ./1 shall be deemed approved at the locations named in Annex ./1.
- 2.2. Any transfer of Data Processing to a third country requires the prior consent of the Controller and may only take place if the requirements of Art 44 et seq GDPR are met.

3. Obligations of the Processor

- 3.1. The Processor undertakes to carry out Data Processing exclusively on the basis of documented instructions from the Controller. If the Processor considers an instruction of the Controller to be unlawful, the Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller.
- 3.2. The Processor shall be obliged to treat confidentially any personal data of which it becomes aware in connection with the Data Processing. The Processor shall impose a confidentiality obligation

on all persons authorized by it to process the data, unless they are already subject to a statutory duty of confidentiality. The obligation of confidentiality and non-disclosure shall continue to apply after termination of this DPA.

- 3.3 The Processor shall take all necessary technical and organizational measures within the meaning of Art. 32 of the GDPR. These technical and organizational measures are data security measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. They shall take into account the state of the art, the costs of implementation and the nature, scope and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons. The technical and organizational measures taken by the Processor are available at <https://swat.io/en/legal> in the current version.
- 3.4 The Processor shall, where possible, support the Controller with appropriate technical and organizational measures to enable the Controller to comply with the data subject rights under Chapter III of the GDPR within the legal time limits and shall provide the Controller with the necessary information to do so upon the Controller's request, provided that the Processor has such information. If a subject submits a request to the Processor to exercise the data subject rights, the Processor shall be obliged to forward the request to the Controller if the request relates to Data Processing by the Controller.
- 3.5 The Processor shall support the Controller in the performance of the obligations incumbent upon the Controller pursuant to Art. 32 to 36 of the GDPR, which shall include, but not be limited to, the implementation of security measures, the notification of data protection breaches and, where applicable, the preparation of a data protection impact assessment.
- 3.6 The Processor shall delete the personal data of the Data Processing after the expiry of the retention periods provided for in the Main Agreement and/or without delay at the request of the Controller. If the Controller expressly requests this, the personal data shall be returned to the Party. Statutory retention periods remain unaffected by this.
- 3.7 The Processor is obliged to provide the Controller with information at the latter's request in order to demonstrate compliance with the obligations pursuant to Art. 28 of the GDPR. The Processor shall support the Controller in verifying the Data Processing and shall grant the Controller access to the documents and technical systems necessary for verifying the Data Processing in accordance with Section 5 of this DPA.
- 3.8 To the extent permitted by law, the Processor shall inform the Controller about control actions and measures taken by the supervisory authorities insofar as they relate to the Controller's Data Processing operations.

4. Sub-processor

- 4.1 The Controller expressly authorizes the use of the services of sub-processors by the Processor in the performance of the Data Processing operations. The sub-processors listed in Annex ./1 shall be deemed to have been approved at the time of conclusion of the contract.
- 4.2 The Processor shall inform the Controller of any intended change regarding the use or replacement of a sub-processor. The Controller may object to the intended change in writing by

email to privacy@swat.io within 30 working days from the date of notification. In case of timely objection, the processor shall not be entitled to use the services of the rejected sub-processor in the Data Processing operations. If no objection is raised by the Controller within the aforementioned period, the intended change shall be deemed approved by the Controller.

- 4.3 If the Processor uses a sub-processor, it shall be obliged to conclude an agreement with the sub-processor within the meaning of Art. 28(4) of the GDPR. In this agreement, it must be ensured that the sub-processor enters into the same obligations that apply to the contractor on the basis of this DPA.

5. Rights of control and inspection

- 5.1 The Controller has the right, in agreement with the Processor, to carry out audits on Data Processing or to have them carried out by auditors to be named in individual cases. Unless otherwise indicated for urgent reasons to be documented by the Controller, inspections shall take place after reasonable advance notice and during the Processor's business hours, and not more frequently than every twelve months. Insofar as the Processor provides evidence of the correct implementation of the agreed data protection obligations of this DPA, checks shall be limited to random samples.
- 5.2 The internal costs incurred by the Processor for a yearly audit and inspection to a reasonable extent shall be borne by the Processor. If the internal costs incurred by the Processor for the yearly audit and inspection exceed a reasonable extent or if additional audits and inspections are requested to the yearly audit and inspection per calendar year, the Processor shall inform the Controller accordingly and provide a cost estimate for these services. These services exceeding the reasonable extent of the appropriate scope will be provided by the Processor on the basis of the cost estimate after being commissioned by the Controller. The reasonable extent of the scope of the annual review and inspection is determined by the Processor. In addition, the Controller shall bear his own costs and all costs in connection with the commissioning of external auditors.

6. Remuneration

The Processor assists in complying with the Controller's obligations under data protection law to a reasonable extent without additional costs. If the requested assistance in complying with the Controller's data protection obligations exceeds the reasonable extent, the Processor shall inform the Controller accordingly and provide a cost estimate for these services. These services exceeding the reasonable extent of the appropriate scope will be provided by the Processor on the basis of the cost estimate after being commissioned by the Controller. The reasonable extent of the scope of the annual review and inspection is determined by the Processor.

7. Term

The term of this DPA corresponds to the term of the Main Agreement plus the retention period provided for therein.

8. Final provisions

8.1 The law of the Main Agreement is applicable to this DPA.

8.2 Should individual provisions of this DPA be or become invalid, this shall not affect the remaining content of the DPA. The invalid provision shall be replaced by a valid provision that is legally valid and comes as close as possible to the economic intent of the Parties. The same shall apply in the event of a loophole in the contract.

Description of Data Processing

1. Subject of the Data Processing

Operation of a social media management tool that allows the client to centrally manage various social media channels, communicate with users of the social media channels, and schedule and publish content.

2. Duration of Data Processing

During the term of the Main Agreement and the retention periods provided for therein.

3. Nature and purpose of the Data Processing

The data from the social media networks is automatically imported into the social media management tool operated by the Processor via interfaces provided by the social media networks and subsequently displayed and managed in this tool.

The purpose of the processing is the management of the client's social media channels and the planning and publication of content on the social media channels by the client. Moreover, the purpose lies in the centralization of all social media communication of the Controller.

4. Categories of personal data

First and last name, user IDs of various social media platforms, profile URLs, profile pictures, website URLs, phone number (when using WhatsApp or other phone channels), as well as various content stored and published on social media platforms (timestamps, posting IDs, posted texts, pictures, videos, links, comments, ratings, private messages, other attachments and metadata of social media content).

With the optional use of email channels within the tool, email addresses of senders & recipients as well as contents of email messages are also processed.

5. Categories of data subjects

Data subjects are the users of the social media platforms used, or in the case of the optional use of email channels, the users who communicate via these email channels.

6. Authorized sub-processors

Hosting and sending and receiving email notifications to the client:

- Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg (data center in Frankfurt, Germany)
- tecRacer GmbH & Co KG, Vahrenwalder Str. 156, 30165 Hanover, Germany

Hosting & API Services

- Microsoft Ireland Operations, Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland (data center in the European Union)

Sending and receiving emails to the client in regard to the functionality “Ticket forwarding per e-mail” and “E-Mail Channels”. The use of both functions is optional and is the responsibility of the Controller:

- Active Campaign LLC (formerly Wildbit LLC) - Postmark, North Dearbon Str, 5th Floor, Chicago, IL 60602, USA, data processing in the USA (data processing in the USA; the USA is considered a third country as defined in Chapter V of the GDPR)