

DATA PROCESSING AGREEMENT

This Data Processing Agreement regulates the relationship between:

WAP – Web Access Platforms, a one-person-business, administrated by Hugo Gameiro and subject of Portuguese Law, in the condition of Processor according to the General Data Protection Regulation (GDPR)

and

By contracting with WAP, the Client assumes the role of Controller according to the General Data Protection Regulation (GDPR).

I. Contract Object and Services Provided by WAP

1. The Client subscribes WAP's services by choosing in between the following plans:
 - 1.1. Moon (includes Shared CPU/RAM; 2 GB of Database Disk Space; 20 GB of Media Disk Space; 100 GB of Bandwidth; Low Federation Capacity; Sidekiq 1 thread; Web 1 thread)
 - 1.2. Planet (includes Shared CPU/RAM; 5 GB of Database Disk Space; 50 GB of Media Disk Space; 125 GB of Bandwidth; Moderate Federation Capacity; Sidekiq 2 threads; Web 2 threads)
 - 1.3. Star (includes Shared CPU/RAM; 10 GB of Database Disk Space; 100 GB of Media Disk Space; 250 GB of Bandwidth; Medium Federation Capacity; Sidekiq 4 threads; Web 4 threads)
 - 1.4. Constellation (includes Shared CPU/RAM; 20 GB of Database Disk Space; 200 GB of Media Disk Space; 500 GB of Bandwidth; High Federation Capacity; Sidekiq 10 threads; Web 10 threads)
 - 1.5. Galaxy (includes Shared CPU/RAM; 40 GB of Database Disk Space; 400 GB of Media Disk Space; 1000 GB of Bandwidth; Very High Federation Capacity; Sidekiq 25 threads; Web 25 threads)
 - 1.6. Extra Resources (additional units added to the base plan – each unit includes an additional 4 GB of Database Disk Space; 40 GB of Media Disk Space; 100 GB of Bandwidth; Sidekiq 2 threads; Web 2 threads)
 - 1.7. Custom (only by direct contact with info@masto.host)
2. WAP will be responsible for hosting the Client's instance on Mastodon according to the conditions described above and depending on the plan the client chooses.
3. The above-mentioned plans are monthly and can be cancelled at any time.
4. The Client can upgrade and downgrade a plan, at any time.
5. Instances and the data associated with them are stored in OVH data centres. WAP assures its sub-processors are compliant with GDPR's principles and rules.
6. WAP is not responsible for the data introduced in the instances administered by the Client – the Client is responsible for informing its users of the processing of their data within Mastodon and for collecting consent where and when it is needed.
7. WAP provides this service in open Beta. Meaning the service is still being developed, optimised and tested. WAP cannot guarantee that the service will work as expected or at all and should only be used for testing purposes.
8. WAP can access to the Client's user's data in case of needed assistance and regular maintenance.
9. The Client accepts WAP's Privacy Policy.

II. Client and right of Instruction

1. As the controller according to Article 4 No. 7 GDPR, the Client is responsible for compliance with data protection regulations, in particular, the selection of WAP, as a processor, the Data transmitted to the processor and the instructions issued (Article 28 (3) a, 29 and 32 (4) GDPR).
2. WAP may process Data only within the framework configured by part I of this Agreement (I. Contract Object and Services Provided by WAP) and the instructions of the Client (including in particular the modification, erasure or restriction of the Data) and only to the extent that the processing is necessary for the agreed purpose, unless WAP is required to process Data for another purpose by Union or Member State law to which WAP is subject; in such a case, WAP shall inform the Client of that legal requirement before processing, unless that law prohibits such information on substantial grounds of public interest (Article 28 (3) paragraph 3 a) GDPR).
3. The Client has the right to issue additional instructions at any time with regard to the processing of the Data and the security measures.
4. If WAP believes an instruction of the Client violates applicable data protection law, then WAP is entitled to suspend the execution of the instruction until the Client confirms the instruction or to reject the instruction in the case of an obviously illegal instruction.
5. WAP may refuse instructions if they are not possible or unreasonable according to the service the Client has purchased (in particular because compliance with them would impose disproportionate effort or due to a lack of technical possibilities of WAP).
6. If additional instructions of the Client go beyond the contractual duty of WAP under the Data Processing Agreement and are not based on misconduct on the part of WAP, then the Client shall reimburse WAP separately for the additional time and effort arising therefrom.

III. Security of Processing and Related Obligations

1. WAP shall take technical and organisational measures for appropriate security, in particular, the confidentiality, integrity and availability of the Client's Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects and ensuring their safeguarding (Article 28 (3) and 32 - 39 in conjunction with Article 5 GDPR). Technical and organisational measures include physical access control, access to processing systems, control of access to Data and input of Data, Data transfer control, control of orders and assignments, availability and integrity control, guarantee of the principle of purpose/ segregation of data and securing the rights of the affected data subjects.
2. WAP ensures that only one person is authorised to process the personal data and that this person is committed to confidentiality (Article 28 (3) and 29, 32 (4) GDPR) and has been instructed in the data protection regulations of the GDPR.
3. The Data and data carriers and all copies made of them within the scope of the DPA shall remain the property of the Client, shall be carefully stored by WAP, protected from access by unauthorized third parties and may only be deleted with the consent of the Client, and then only in accordance with data protection law and this agreement. Copies of Data may only be made if they are necessary to fulfil the main and secondary contractual obligations of WAP towards the Client (e.g. backups).
4. WAP cannot be responsible by damages emerging from data loss by the Client.
5. When the service provided is cancelled (due to direct Cancellation request or automatic cancellation based on illegal conduct or failure of payment) the Client's instance is suspended or deleted within 24 hours.

IV. Information Duties and Duties to Cooperate

1. The rights of the data subjects are to be fulfilled by the Client, whereby WAP supports the Client according to Article 28 (3) e) GDPR, providing support when needed to fulfil the requests.
2. The Client must inform WAP immediately and entirely if he detects errors or irregularities regarding the processing of the Data or regarding compliance with the provisions of this DPA or relevant data protection regulations.
3. In the event that WAP ascertains facts which justify the assumption that the protection of the Data processed for the Client has been breached, WAP must immediately and entirely inform the Client, take the necessary protective measures without delay and assist in the fulfilment of the obligations' incumbent on the Client pursuant to Articles 33 and 34 GDPR (data breach).
4. Should the security of the Client's Data be endangered by third-party actions (e.g. creditors, authorities, courts with seizure, confiscation, insolvency proceedings, etc.) WAP will immediately inform the third parties that the sovereignty and ownership of the Data lie exclusively with the Client and, after consultation with the Client, will, if necessary, take appropriate protective measures (e.g. file objections, applications, etc.).
5. WAP shall inform the Client without delay if a supervisory authority takes action against it and its activities may affect the Data processed for the Client. WAP supports the Client in the performance of his duties (in particular the provision of information and toleration of inspections) towards supervisory authorities (Article 31 GDPR).
6. WAP shall provide the Client with the information necessary for the fulfilment of legal obligations (which may include, in particular, inquiries from data subjects or authorities and compliance with his accountability duties pursuant to Article 5 (2) GDPR, as well as the carrying out of a data protection impact assessment in accordance with Article 35 GDPR) and shall provide the necessary information regarding the processing of Data within the scope of this DPA if the Client cannot acquire this information himself. The information must be accessible to WAP and does not have to be obtained from third parties, whereby employees, agents and sub-processors of the Client are not considered as third parties.
7. If the provision of the necessary information and the cooperation go beyond the duties of WAP according to the Principal Agreement and is not based on misconduct on the part of WAP, the Client shall reimburse WAP separately for the additional work and expenses arising therefrom.

V. Engagement of Subprocessors

1. When WAP uses the services of a sub-processor in order to carry out specific processing activities on behalf of the Client, the same data protection obligations as set out in this DPA or other legal act between the Client and WAP shall be imposed on the sub-processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this DPA and the applicable data protection law (in particular with regard to compliance with instructions of the Client, compliance with technical and organisational measures, provision of information and the toleration of inspections). Furthermore, WAP must carefully select the sub-processor, check its reliability and monitor its compliance with the requirements of this DPA and the data protection law (Article 28 (2) and 4 GDPR).
2. The Client agrees that WAP may engage sub-processors for the processing of the Data.
3. WAP shall inform the Client of any changes to the sub-processors that are relevant to the processing of the Data. The Client shall exercise its right to object to the changes or new sub-processors only in compliance with the principles of good faith, fairness and equity.

4. Contractual relationships in which WAP uses the services of third parties as a purely ancillary service in order to carry out his business activities (e.g. cleaning, security or transport services) do not constitute sub-processing within the meaning of the above provisions of this DPA. Nevertheless, WAP must ensure, e.g. through contractual agreements or information and instructions, that the security of the Data is not endangered and that the requirements of this DPA and the data protection laws are complied with.

VI. Processing in Third Countries

1. The processing of Data as contractually specified is carried out only in a Member State of the European Union or in another state party to the Agreement on the European Economic Area (EEA).
2. The processing of Data in a third country, also by sub-processors, may only be carried out on documented instructions from the Client and if the particular requirements of Article 44 ff. GDPR are met, unless WAP is obliged to carry out processing in the third country by the law of the Union or the Member States to which WAP is subject, in which case WAP shall notify the Client of these legal requirements before processing, unless the law prohibits such an information on important grounds of public interest (Article 28 (3) a) GDPR).

VII. Duration of the Processing, Termination of Contract and Deletion of Data

1. This DPA becomes valid upon the payment of the service subscribed. It becomes void after cancellation.
2. The right to termination without notice for a compelling reason is available to the Contracting Parties, in particular in the event of a serious breach of the provisions of this DPA, applicable data protection law or if illegal content is found on data stored by the Client. The extraordinary termination must, in general, be preceded by a warning of the infringements with a reasonable period of notice, whereby the warning is not necessary if it is unlikely that the objected infringements will be remedied or if they are so severe that it is unreasonable to expect the terminating contracting party to adhere to this DPA.
3. After completion of the processing services under this DPA, WAP will either delete or return all personal data and copies thereof (as well as all documents obtained in connection with the contractual relationship, processing and processing results obtained and datasets), at the choice of the Client, unless an obligation to store the personal data exists under Union law or the law of the Member States (Article 28 (3) S. 2 g. GDPR). The right of retention is excluded regarding the processed Data and the associated data carriers. Regarding the cancellation or return of the Data, the Client's rights of information, documentation and inspection shall apply in accordance with this DPA.
4. In any case, the obligations arising from this DPA with regard to the Data processed in the assignment shall remain in force even after termination of the DPA.

VIII. Liability

1. In the internal relationship with WAP, the Client alone shall be responsible to the data subject for the compensation of damages suffered by the data subject due to Data processing or use within the scope of processing instructions which is inadmissible or incorrect in accordance with data protection laws.
2. In 24 hours, after the termination of this contract all of the Client's data will be deleted.
3. This contract is valid from the moment of payment.