GENERAL TERMS AND CONDITIONS FOR THE HOSTING OF PERSONAL DATA

IN THE CONTEXT OF THE GENERAL DATA PROTECTION REGULATION

Table of content

Article 1. Context and Purpose

The Client, acting as Data Controller, has subscribed to one or more services from IKOULA under IKOULA's General Terms and Conditions or through a specific agreement.

The Client hosts personal data on IKOULA's servers, which, in accordance with the CNIL's guidelines, qualifies IKOULA as a Sub-Processor.

The purpose of these clauses is to define the conditions under which the Sub-Processor agrees to perform the processing operations of personal data on behalf of the Data Controller as defined below.

Both parties agree to comply with the applicable personal data protection regulations, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, applicable as of 25 May 2018 ("the European Data Protection Regulation").

It is recalled that in the commercial relationship with the Data Controller, IKOULA merely provides hosting space and does not directly handle the Client's personal data. IKOULA does not process personal data beyond storage and, if subscribed to, backup.

As a hosting provider, IKOULA has no general obligation to monitor the content it hosts and is not aware of whether its Clients host personal data, unless a specific service states otherwise.

Article 2. Description of the Processing Subject to Subcontracting

The Sub-Processor is authorized to host and, subject to subscription to this service, to back up, on behalf of the Data Controller, the personal data that it has declared in the declaration form.

The nature of the operations carried out on the data is data hosting and, subject to subscription to this service, data backup.

The purpose(s) of the processing are unknown to the Sub-Processor, in accordance with Article 6-1-2 of Law No. 2004-575 of 21 June 2004. However, the Data Controller may, subject to the implementation of a separate service, disclose the personal data it hosts on IKOULA's servers.

The personal data processed shall be ignored by the Sub-Processor, in accordance with Article 6-1-2 of Law No. 2004-575 of 21 June 2004. However, the Data Controller may, subject to the establishment of a separate service, disclose the personal data it hosts on IKOULA's servers.

The categories of persons concerned are ignored by the Sub-Processor, in accordance with Article 6-1-2 of Law No. 2004-575 of 21 June 2004. However, the Data Controller may, subject to the establishment of a separate service, disclose the personal data it hosts on IKOULA's servers.

Article 3. Duration of the Contract

These General terms and conditions for the hosting of personal data shall enter into force with effect from 25 May 2018.

Article 4. Obligations of the Sub-Processor towards the Data Controller

The Sub-Processor undertakes to:

1. Process data solely for the purpose(s) for which it is being processed, namely to host the data, it being understood that the processor shall not perform any action on the personal data of the Data Controller other than hosting it on its servers, whether production servers and/or backup servers, provided that the Data Controller has subscribed to backup for the latter case.

2. Process data in accordance with the services subscribed to by the Client. If the Sub-Processor considers that an instruction constitutes a breach of the European Data Protection Regulation or any other provision of Union law or Member State law relating to data protection, it shall immediately inform the Data Controller.
   Furthermore, if the Sub-Processor is required to transfer data to a third country or to an international organization pursuant to Union law or the law of the Member State to which it is subject, it shall inform the Data Controller of this legal obligation prior to processing, unless the law in question prohibits such information on grounds of important public interest.

3. Guarantee the confidentiality of personal data processed under this contract (to the extent that the Data Controller does not make its hosting accessible to unauthorized third parties and ensures that security measures are taken to ensure confidentiality, since the Client has full access to the personal data hosted by IKOULA).

4. Ensure that all persons authorized to process personal data under this contract:
   - Are committed to maintaining confidentiality or are subject to an appropriate legal obligation of confidentiality,
   - Receive the necessary training in personal data protection.

5. Take into account, with regard to its tools, products, applications or services, the principles of data protection by design and data protection by default.

Article 5. Subcontracting

The Sub-Processor may engage another Sub-Processor (hereinafter, **the subsequent Sub-Processor**') to carry out specific processing activities. In this case, it shall inform the Data Controller in advance and in writing of any changes planned regarding the addition or replacement of other Sub-Processors.

This information must clearly indicate the processing activities subcontracted, the identity and contact details of the Sub-Processor and the dates of the subcontracting agreement.

The Data Controller shall have a maximum period of 15 days from the date of receipt of this information to raise any objections.

Such subcontracting may only be carried out if the Data Controller has not raised any objections within the agreed time limit.

The subsequent Sub-Processor is required to comply with the obligations of this contract on behalf of and in accordance with the instructions of the Data Controller. It is the responsibility of the initial Sub-Processor to ensure that the subsequent Sub-Processor provides the same sufficient guarantees regarding the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the European Data Protection Regulation.

If the subsequent Sub-Processor fails to fulfil its data protection obligations, the initial Sub-Processor shall remain fully liable to the Data Controller for the performance by the other Sub-Processor of its obligations.

Article 6. Right to Information of Data Subjects

It is the responsibility of the Data Controller to provide information to individuals concerned by processing operations at the time of data collection.

Article 7. Exercise of Personal Rights

Where possible, the Sub-Processor shall assist the Data Controller in fulfilling its obligation to respond to requests from data subjects exercising their rights: right of access, rectification, erasure and objection, right to restriction of processing, right to data portability, right not to be subject to automated individual decision-making (including profiling).

When data subjects exercise their rights with the Sub-Processor, the Sub-Processor must forward these requests as soon as they are received by email to the address provided by the Client when subscribing to the services.

Article 8. Notification of Personal Data Breaches

The Sub-Processor shall notify the Data Controller of any personal data breach as soon as possible after becoming aware of it and by email to the address provided by the Client when subscribing to the services.

This notification shall be accompanied by any useful documentation to enable the Data Controller, if necessary, to report the breach to the competent data protection authority.

The notification shall contain at least:

- a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned by the breach and the categories and approximate number of personal data records;
- the name and contact details of the Data Protection Officer or other contact point from which further information can be requested;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

If, and to the extent that it is not possible to provide all this information at the same time, the information may be provided in stages without undue delay.

The Data Controller is responsible for communicating personal data breaches to the data subjects. It is noted that the Sub-Processor has no knowledge of the personal data it hosts and is therefore not in a position to determine whether a personal data breach is likely to result in a high risk to the rights and freedoms of a natural person.

Article 9. Assistance from the Sub-Processor in connection with the Data Controller's Compliance with its Obligations

The Sub-Processor shall provide the Data Controller with the relevant documentation for the performance of data protection impact assessments by the latter, solely in relation to the aspects for which the Sub-Processor is responsible, i.e., for the Sub-Processor, data hosting.

The Sub-Processor shall assist the Data Controller, to the extent possible and reasonable, in carrying out prior consultation with the data protection authority by providing the necessary documentation.

Article 10. Safety Measures

The Sub-Processor undertakes to implement the following security measures:

- Classification and control of information assets

Designation of information owners, classification of each piece of information, security rules associated with each class of information, and inventory.

- Staff security

IKOULA has developed a security awareness plan for all employees, tailored to each individual's role. In addition, the IKOULA security team raises awareness among all staff so that everyone is aware of their responsibility in the security improvement process.

- IKOULA's logical security policy is based on a set of fundamental principles applied within our infrastructure. These principles are:

    - Anything that is not explicitly authorized is prohibited.
    - There is never a direct connection between the protected and internal network(s) (firewall),
    - Equipment connected to the internal network is 'invisible' to the internet,
    - Private communications between different sites via an external network (i.e. not managed by IKOULA) are protected (e.g. via a VPN),

- Access to services is operational at all times:

All equipment (air conditioners, electrical panels, etc.) used by IKOULA (excluding routers, whose availability is ensured by a redundancy + spare policy) is covered by a 24/7 maintenance contract with repair within 4 hours by the manufacturer or its authorized representative. In addition, to ensure the best possible availability of critical shared services (network, DNS, etc.), IKOULA has set up a fully redundant infrastructure for these services. Some services even benefit from load balancing to limit bottlenecks and network congestion.

IKOULA is currently implementing the security measures provided for in the CISPE Code of Conduct.

It is hereby reiterated that, within the framework of the hosting service, the Data Controller is solely responsible for deciding on the security policy to which it subscribes, which may be more or less extensive depending on the options chosen (including subscription to a firewall, etc.). IKOULA's measures do not replace the security measures that the Data Controller must take for the processing of personal data in order to ensure that its processing complies with the GDPR.

Article 11. What happens to Data after the Commercial Relationship ends

The fate of the data at the end of the contractual relationship between IKOULA and the Client is specified in the IKOULA General Terms and Conditions.

Article 12. Data Protection Officer

The DPO's contact details are available on the website www.ikoula.com and the Client can contact them at rgpd@ikoula.com.

Article 13. Documentation

The Sub-Processor shall provide the Data Controller with the documentation necessary to demonstrate compliance with all of its obligations, within the limits of the Sub-Processor's role, namely the hosting of the Data Controller's data.

Article 14. Obligations of the Data Controller towards the Sub-Processor

The Data Controller undertakes to:

1. Document in writing all instructions concerning the processing of data by the Sub-Processor;
2. Ensure, in advance and throughout the duration of the processing, that the Sub-Processor complies with the obligations laid down in the European Data Protection Regulation;
3. Supervise the processing by the Sub-Processor in accordance with the Contract.

Article 15. Scope of the General Terms and Conditions for Data Exchange

These General Terms and Conditions for the hosting of personal data within the framework of the General Data Protection Regulation coming into force on 25 May 2018 and the IKOULA General Terms and Conditions or the specific contract concluded with the Client form a single contractual document.

All provisions of the IKOULA General Terms and Conditions or of the specific contract that are not derogated from or contradicted by the terms of the General Terms and Conditions for the hosting of personal data shall remain fully applicable between the parties. In the event of any discrepancy between IKOULA's General Terms and Conditions and these General Terms and Conditions for the Hosting of Personal Data, these General Terms and Conditions for the Hosting of Personal Data shall prevail from the date of their entry into force.

If any provision of the General Terms and Conditions for the Hosting of Personal Data is found to be invalid under any applicable law or by a final court decision, such provision shall be deemed null and void, without affecting the validity of the remaining provisions of the General Terms and Conditions for the Hosting of Personal Data.