Data protection

By means of the following contractual clauses and in compliance with Republic Act No 10173, otherwise known as the Data Privacy Act, a law that seeks to protect all forms of information, be it private, personal, or sensitive, and covers both natural and juridical persons involved in the processing of personal information by which ODILO.

Likewise, in accordance with article 28 of the RGPD Regulation (EU) 2016/679 of April 27, 2016 and 33 of the LOPDGDD and Organic Law 3/2018, of December 5, the limits established for data processing will be established. personal that ODILO TID S.L. (Spain).

The limits established for the processing of personal data that ODILO TID S.L. in charge of the treatment (hereinafter PROCESSOR), will treat on behalf of the CLIENT, responsible for the treatment (hereinafter CONTROLLER), to provide the library loan management service.

Both parties reciprocally recognize in the other the legal capacity necessary to endorse the present contract of provision of service with access to personal data and establish the following:

Instructions for data handling

1) Subject

Data processing will consist of:

The management of library loans of digital content to users authorized by the person or persons responsible via:

- Access control for user profiles defined by the person responsible
- Follow-up and management of use conditions which the person responsible establishes in order to manage users via platform use statistics.
    - Some of these statistics are necessary for full compliance with the loan conditions set by the person responsible
    - The other set of statistics allow the person responsible to manage more efficiently which digital content is chosen for their platform

The authorized treatment operations will be those strictly necessary to achieve the purpose of the assignment and are specified in the collection and capture of data, its organization and structuring, storage, use or treatment, limitation and deletion or destruction.

2) Types of personal data and categories of interested parties

The personal data which the PROCESSOR will be able to access corresponds to the following categories of actors: Users

Concretely the following data or categories of data:

Identification: identifier and password.

Usage data: user profile based on platform activity in relation to the digital contents accessed by said user. Usage statistics.

In the files and handling history of the person responsible this data will be included and be at their disposal in order to develop the contracted services, informing them that they must apply the appropriate security measures in accordance with article 32 of the RGPD.

3) Obligations of the Data Controller

The data CONTROLLER guarantees that the data provided to the Data PROCESSOR has been collected in accordance with the GDPR art. 5,6 and 8 or their equivalents in the member state of application, and in accordance with all applicable Data Protection Law.

The data CONTROLLER will be responsible for facilitating compliance with the right to information on the data processing described in this commission contract, and to facilitate this task may create "spaces" enabled for this purpose on the platform where he may include the necessary information pursuant to art. 13 and 14 of the RGPD. In case of not meeting this obligation, the responsible person must make it known to the person in charge so that it can be rectified as soon as possible.

The data CONTROLLER will make available to the data PROCESSOR as much information as is necessary to execute the services necessary for the object of this contract, specifically the user data and passwords necessary to verify authorized access.

The data CONTROLLER must carry out, when necessary, the mandatory evaluation of the impact of the protection of personal data on those processing operations, to be carried out by the person in charge and, as necessary, after prior consultations with the Control Authority.

The data CONTROLLER must ensure, prior to and throughout the handling, compliance with the RGPD by the person in charge of supervising the handling, including carrying out inspections and audits if deemed necessary.

The data CONTROLLER advises the data PROCESSOR that, if it determines on its own account the purposes and means of the treatment, it will be considered responsible for the treatment and will be subject to complying with the provisions of the current regulations applicable as such.

4) Rights and obligations of data PROCESSOR

The PROCESSOR must respect all obligations that may be incumbent upon it as processor of data in compliance with the terms set in the current rules and in any other rule or regulation that might be equally applicable.

The data PROCESSOR will not reissue, apply, or use the data for any objective other than the ones set forth in the present contract, or in ways which occasion a breach of this contract.

The data PROCESSOR will make available to the CONTROLLER the necessary information to demonstrate fulfilment of the contract, permitting inspections and audits necessary to evaluate processing and handling.

If the data PROCESSOR considers any instructions to infringe upon the RGPD or any other regulation regarding data protection of the Union or Member States, the PROCESSOR will immediately inform the responsible party.

The data PROCESSOR will keep in writing a register of all categories of processing activity carried out by the responsible party, all in compliance with article 30.2 of the RGPD.

5) Authorized personnel for data handling

The data PROCESSOR guarantees that the personnel authorized for data handling has agreed expressly and in writing to respect the confidentiality of the data, or is subject to a legal confidentiality agreement.

The data PROCESSOR will take measures to guarantee that all personnel acting under its authority and with access to personal data will only be able to process said data following the instructions of the data CONTROLLER or obligated to do so by virtue of the current legislation.

The data PROCESSOR guarantees that the personnel authorized to handle the data has received the necessary training to ensure there is no risk to personal data protection.

The data PROCESSOR will make available to the CONTROLLER the documentation accrediting compliance with the obligations established in this section.

6) Security measures

The CONTROLLER declares to be up-to-date with regard to the obligations derived from the data protection regulations, especially with regard to the implementation of security measures for the different categories of data and treatment established in article 32 of the RGPD.

The PROCESSOR guarantees the adequate implementation of said security measures and will cooperate with the CONTROLLER to ensure they are followed.

The CONTROLLER will carry out an analysis of the potential risks of data handling to determine the appropriate security measures for guaranteeing security of handled information and maintaining the rights of all parties, and if risks are identified, will pass on a report to the PROCESSOR with an impact evaluation in order to implement adequate measures to avoid or mitigate said risks.

The PROCESSOR must analyze possible risks on its end as well as other circumstances that could affect the security for which it is responsible and must inform the CONTROLLER of any such risks in order to evaluate their impact.

In any given case, the PROCESSOR guarantees that the following data protection measures will be implemented, bearing in mind the status of the technique, the costs of implementation, and the nature, scope, context, and ends of the processing:

- Control of individualized user access via password and email.
- Periodical renewal of password policy and required password complexity.
- Client-server communication via secure and encrypted protocols (HTTPS).
- Use of protective libraries against malicious code.
- Use of firewalls in servers which Odilo solutions deploy in SaaS
- User action and processes audits.
- Application access audits.
- Real time 24/7 monitoring of service and application function.
- Alerts service regarding availability of the applications.
- Continuous updating of base software used to offer the best security guarantees.
- Daily security copies of information in geo-redundant format.
- SaaS service managed with a world reference in secure provision of cloud services: Amazon Web Services.
- Simulation of business continuity scenarios (restoration in response to contingencies).
- Security incident management panel.
- Creation of spaces to comply with information obligations: legal notices, privacy policies, usage rules.

The processing subject to the client's order additionally is certified with the following certifications:

- ISO 27001 – Information Security Management
- ISO 27017 Security Controls for Cloud Services
- ISO 27018 Protection of Personally Identifiable Information in the Cloud
- ENS (National Security Outline) in high category
- ISO 22301 Business Continuity Management
- ISO 9001 Quality Management System
- ISO 27701 Privacy Information Management

The subprocessor chosen for cloud storage also has certifications on their own part https://aws.amazon.com/es/compliance/

In this way the following are guaranteed by an independent certifying agency:

- Confidentiality, integrity, availability, and permanent resilience of the systems and processing services.

- Rapid availability and access to data in case of a physical or technical incident.

- Regular verification, evaluation, and assessment procedures of the efficacy of technical and organizational measures to guarantee the security of data handling.

- If necessary, a pseudonym and data cipher can also be applied for personal data.

7) Security breaches

Security violations of which the PROCESSOR is aware must be reported, without undue delay and in a maximum of 24-48 hours, to the CONTROLLER for its awareness and application of measures to mitigate any possible effects. The report will not be necessary if it is improbable that there is any risk to the rights and liberties of physical persons.

The notification of a security breach, in compliance with art. 33 of the RGPD must contain at minimum the following information:

If it is not possible to facilitate all the information simultaneously, and to the extent that it is not possible, the information will be facilitated in a gradual manner without undue delay.

8) Communication of information to third parties

The PROCESSOR may not communicate information to other entities, unless it has obtained a prior authorization in writing from the CONTROLLER; in which case the authorization will be annexed to the present contract.

The transmission of information to public authorities in the exercise of their public function is not considered a communication of information, for which reason it will not require the authorization of CONTROLLER if the transmissions are necessary in order to carry out the contracted work.

9) International data transfer

The PROCESSOR may not carry out information transfers to third party countries or international organizations not established in the EU, unless it has obtained a prior authorization in writing from the CONTROLLER; in which case the authorization will be annexed to the present contract.

10) Data subprocessing

The responsible party is authorized to establish a subprocess corresponding to cloud storage in SaaS format (software as a service) with the company Amazon Web Services Inc.

Cloud storage in SaaS format (Software as a service)

Amazon Web Services Inc.

410 Terry Avenue North Seattle Washington 98109-5210

By means of a contract signed on the date: 24 of March 2011.

Odilo will deploy the solution (servers and data) in different locations based upon the client's situation, in particular:

- All European clients will have storage in AWS servers of the Republic of Ireland, within the European Union.

  AWS incorporates in a complementary way a data processing addendum "AWS GDPR" in its terms of privacy service that includes the European Commission's execution decision 914/2021 between managers and therefore, we understand that we offer sufficient guarantees in terms of when TID is carried out in those cases in which a European client needs to host data outside the EU. See this link:

- https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf

- All North American clients will have storage in AWS servers in North Virginia (USA).
- All Australian clients will have storage in AWS servers in Sydney.
- For clients located in other regions separate from the above mentioned, they will be offered the opportunity to choose between storage services in Ireland or the USA, depending on the restrictions for personal data processing and requirements of the application's performance.

The PROCESSOR is authorized to establish the sub-processing corresponding to the Chatbot of the Customer Service Technical Services (SAT) with the company Zendesk Inc. With registered office at 1019 Market Street, San Francisco, CA 94.103 address in Spain Paseo de la Castellana 43,28046 Madrid . That it provides as a guarantee for International Data Transfers standard contractual clauses of the Commission version 2021/914 and BCR of October 2020 formalized through the control authority of Ireland and Holland (Netherlands), which in our opinion guarantees a level of data protection equivalent to the European. Privacy policy Zendesk

The subprocessor, who will also be considered as a processor, is equally obligated to comply with the established requirements of this document for the data PROCESSOR and the instructions dictated by the CONTROLLER. The initial processor is responsible for regulating the relationship to the end that the new processor is subject to the same conditions (instructions, obligations, security measures) with the same formal requirements as the initial processor, in everything related to the adequate processing of personal data and the rights of all affected parties. In the case of noncompliance by the subprocessor, the initial processor will still be fully responsible to the controller in everything related to compliance with the established obligations.

11) Rights of interested parties

The PROCESSOR will create, assuming it is possible to do so and keeping in mind the nature of the processing, the technical and organizational conditions necessary to assist the CONTROLLER in its obligation to respond to requests about the rights of interested parties.

If the PROCESSOR receives a request regarding the exercise of said rights, it must communicate as much to the CONTROLLER immediately, and never later than the next working day following receipt of the request, along with other information relevant to the resolution of the request.

12) Data protection delegate

The PROCESSOR has a designated data protection delicate, Jose Manuel Mulero, who can be reached if necessary at the following email address: dpo@odilo.us

13) Responsibility

In compliance with article 82 of the RGPD, the PROCESSOR is responsible to the CONTROLLER for harms and losses caused to interested or third parties including administrative sanctions, which result from judicial or extrajudicial complaints or from penalizing processes from a control authority, which are the consequence of any violation of the instructions written in the present contract.

14) Duration

The present agreement has a duration linked to the duration of the provision of service contract established between the two parties, or in some cases the duration established in bid for the rendering of services.

15) End of provision of service

At the end of the provision of service which is the subject of this contract, the PROCESSOR and the CONTROLLER will proceed in the following manner:

- Disconnecting the controller's database, so that the system can no longer validate access to the platform by any user.

- Returning any personal registration dat, in cases in which the service included an auto registration for new users; to this end the controller must download this information before disconnecting. If these data are not exportable from the administration portal, the MANAGER will perform a manual export in Excel/CSV format from the database.

- Returning any monitoring data and/or usage statistics associated with users during the provision of service, to which end the controller must download this information before disconnecting.

- Once the return has been verified by both parties, the processor will definitively delete all associated data.

- In the event that the CONTROLLER does not have the own digital resources that he imported as administrator in the solution, said own digital resources may be returned on demand.

- On the agreed date for the termination of the service, disable the URL where the service is hosted in SaaS (DNS) and disconnect all integrations with external services (for example, authentication system of the CONTROLLER, discovery platforms ...).

• The data will not be eliminated when its conservation is required by a legal obligation, in which case the PROCESSOR will proceed in the custody of the same blocking the data and limiting its handling in anything related to the responsibilities of its relationship with the CONTROLLER.

The PROCESSOR will maintain the duty of secrecy and confidentiality of the data including after the finalization of the relationship detailed in this contract. For the record and as a demonstration of compliance from both sides they endorse the present contract, in duplicate, in the place and at the time indicated in the header

Fdo. CONTROLLER	23038433T RODRIGO RODRIGUEZ (R: B30856439) Firmado digitalmente por 23038433T RODRIGO RODRIGUEZ (R: B30856439) Fecha: 2022.12.22 16:11:47 +01'00' Fdo. PROCESSOR ODILO TID S.L. B30856439