# Data protection agreement

## 1. Introduction

The Data Protection Agreement (hereinafter referred to as the “Agreement”) is intended to govern the use of Personal Data belonging to customers (hereinafter referred to as the “Customer”) of Praiz SAS (hereinafter referred to as the ‘Processor’ or “Praiz SAS”) when they use the Praiz service (hereinafter referred to as the “Service”).

## 2. Definitions

The terms "adequacy decision", "technical and organisational measures", "data subjects", "privacy by design", "privacy by default", "register", "joint controller(s)", "controller of processing activities", "processor", "processing", "personal data breach" present in the Agreement have the meanings described in Articles 4 et seq. of the GDPR.

Other terms are defined below:

* "Agreement" means the appendix to the Contract governing the use of the Customer's Personal Data in accordance with the provisions of Article 28 of the GDPR also entitled "Data Processing Addendum" ("DPA").
* "PIA": means an privacy impact assessment to verify the proportionality of the processing of Personal Data and to prevent the risks associated with the processing of Personal Data.
* "Anonymisation": refers to a process designed to make it irreversibly impossible to identify the persons concerned by the processing carried out in the context of the Service.
* "Supervisory Authority": means the supervisory authority for GDPR matters competent for the Service provided by the Processor.
* "Customer": means the entity that has subscribed to the Service provided by the Processor
* "Contract": means the contract entered into between the Processor and the Customer for the use of the Service to which this Agreement is attached
* "Right request(s)": refers to the fundamental right(s) created by the GDPR in Articles 15 et seq. (e.g. right of access, right of erasure, etc.).
* "Customer Personal Data": means any data relating to an identified or identifiable natural person transmitted to the Processor and processed by the latter on behalf of the Customer as part of the Service, a detailed list of which is given in the Appendix.
* "Party(ies)": refers jointly to the Customer and the Processor
* "GDPR": means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data also known as the "General Data Protection Regulation".
* "Applicable regulations on the protection of personal data": together means French Law no. 78-17 of 6 January 1978 on data processing, data files and individual liberties and the GDPR.
* "Reversibility": means the operation aimed at enabling the transfer and integration, in a usable and recognised format, of the Customer's Personal Data from the Processor’s Service to an equivalent service offered by another service provider.
* "SaaS Service": refers to software hosted by the Processor that can be used simultaneously by an infinite number of customers.
* "Sub-processor": refers to the processors recruited by the Processor to process the Customer's Personal Data exclusively in the context of the Service
* "End Users": means the persons whose Personal Data are processed by the Processor on behalf of the Customer.

## 3. Contractual relations and duration

The Agreement is an indivisible appendix to the Contract signed between the Customer and the Processor for the use of the Service.

In the event of any contradiction between the Contract concluded for the use of the Service and the Agreement, the obligations set out in the Agreement shall prevail over the Contract with regard to the GDPR as a whole.

The Agreement is applicable for the duration of the Contract entered into in connection with the use of the Service and may continue beyond that period as long as all the obligations set out herein remain applicable.

## 4. Role of the Parties and scope of application

Under the Agreement, the Customer acts as the data controller and Praiz SAS acts as the data processor within the meaning of Article 28 of the GDPR.

Under no circumstances may the Parties be considered to be jointly liable in connection with the Service. However, the Parties agree that in the event of an error or change in their qualification, the Parties shall meet, as soon as possible, to amend the Agreement and take all measures relating to such a situation in order to comply with the requirements of the applicable Regulations regarding the protection of personal data.

The Agreement exclusively governs the processing of the Customer's Personal Data carried out within the framework of the Service as a Processor within the meaning of article 28 of the GDPR to the exclusion of the processing carried out by Praiz SAS as data controller which is governed by the Contract.

## 5. Instructions and commitments

The Processor undertakes to use the Customer's Personal Data in connection with the use of the Service only in accordance with the instructions documented in the appendix to the Agreement. The Processor shall immediately inform the Customer if it considers that an instruction given by the Customer is illegal with regard to the Regulations applicable to the protection of personal data. The Processor may not be held liable in the event that, despite the Processor’s notification concerning the illegality of the instruction, the Customer maintains and applies this instruction via the Service.

The Processor undertakes to comply with the provisions of the GDPR and, in particular, to keep a register of processing activities specific to the Service and to develop its Service in compliance with the rules of "Privacy by Design" and "Privacy by Default".

The Processor undertakes never to transfer the Customer's Personal Data for any reason other than the provision of the Service and undertakes never to use the Customer's Personal Data for its own purposes as data controller.

The Processor declares that all internal or external personnel required to process the Customer's Personal Data are bound by one or more binding legal documents and regularly undergo training and awareness-raising.

The Processor undertakes to guarantee the security of the Customer's Personal Data and to implement all the technical and organisational measures necessary for its Service, details of which are set out in the appendix to the Agreement.

On the other hand, the Processor is never liable for the Customer's failure to comply with the Regulations applicable to the protection of personal data when using the Service as the data controller.

## 6. Assistance with PIA

PIAs must be carried out by the Customer, in accordance with the provisions of the GDPR. Nevertheless, the Processor undertakes to provide, at the Customer's written request, all the information necessary and required for the Customer to ensure that a PIA is carried out.

However, the Processor is not obliged to carry out the PIAs for and on behalf of the Customer. Any additional request for information may be refused.

## 7. Assistance with Entitlement Requests

Entitlement Requests sent by End Users are transferred to the Customer as soon as possible. The Processor is not required to maintain an inventory of Entitlement Requests on behalf of the Customer and is not liable for any failure by the Customer to manage Entitlement Requests.

At the Customer's written request, the Processor shall carry out the technical actions to be undertaken so that the Customer can fulfil its obligation to follow up the requests of the persons concerned.

The Customer accepts and understands that the Processor is not obliged to manage Requests for personal rights made as part of the Service in place of and on behalf of the Customer. Any additional request for such management will be refused.

Requests for rights sent to the Processor as data controller are processed exclusively by the Processor and are not transferred to the Customer.

## 8. Assistance with safety measures

The Processor undertakes to provide all necessary and required information on the technical and organisational security measures to be implemented to guarantee the security of the Customer's Personal Data in the context of the provision of the Service.

## 9. Violations of Personal Data

The Processor undertakes to notify the Customer, as soon as possible and, at the latest, within 48 working hours of becoming aware of any personal data breach in connection with the Service likely to affect the Customer's Personal Data, together with all the necessary and required information in its possession to reduce the effects of the personal data breach. The Customer accepts and acknowledges that the 72-hour period applicable to him only starts from the time he becomes aware of the personal data breach and that, in this respect, the 48-hour period complies with the GDPR.

The Processor is not authorised to handle notifications of personal data breaches to the Supervisory Authority and to inform End Users on behalf of the Customer. Any such request from the Customer will be refused.

## 10. Sub-processors

The Customer grants the Processor general authorisation to recruit Sub-processors on condition that it is informed of any changes to these Sub-processors as soon as possible in order to allow the Customer to raise objections. The Customer accepts and acknowledges that a specific authorisation, for a SaaS tool, is not applicable and could lead to the Service being blocked.

In the absence of any objections raised by the Customer within eight (8) days of notification, the new Sub-processor shall be definitively recruited without the Customer being able to object, claim damages or request termination of the Contract. If the objection made within the time limit is deemed admissible by the Processor, the latter may offer the Customer one of the following solutions: i) the withdrawal of the Sub-processor, ii) the implementation of additional measures to guarantee the security of the Customer's Personal Data, iii) the termination of the Service without the Customer being able to claim damages.

In order to be considered admissible by the Processor, objections must be objective and serious and must be duly demonstrated. The Parties accept that the following situations will, by default, be considered admissible: i) the proposed Sub-processor is a direct competitor of the Customer, ii) the Sub-processor is involved in a dispute with the Customer, iii) the Sub-processor has been convicted by a Supervisory Authority in the 12 months prior to its recruitment and iv) the Sub-processor does not comply, if applicable, with the applicable rules relating to transfers outside the European Union.

The Processor undertakes to only recruit Sub-processor who, after verification, present the necessary and sufficient guarantees to ensure the security and confidentiality of the Customer's Personal Data. The relationship between the Processor and the Sub-processor must be set out in an agreement containing obligations similar to this Agreement.

The Processor remains responsible, within the limits of liability set out in the Contract, for any breaches of the GDPR that its Sub-processor may carry out in the context of the Service.

## 11. Hosting and transfers outside the European Union

## a) Data hosting

The Processor undertakes to take all necessary steps to host the Customer's Personal Data exclusively within a Member State of the European Union. The Customer authorises the Processor to choose the Member State of the European Union of its choice. In the event that the Personal Data is hosted in a country outside the European Union, the Processor undertakes to obtain the Customer's prior authorisation and to implement all the mechanisms required to govern this transfer, such as concluding Standard Contractual Clauses and, where applicable, implementing additional technical measures designed to strengthen the security of the Customer's Personal Data.

## b) Data transfers

The Customer grants the Processor a general authorisation for transfers outside the European Union if, cumulatively, (i) the transfers are made exclusively to Sub-processor that comply with the GDPR and (ii) the transfers are made exclusively to a country benefiting from an adequacy decision or are governed by appropriate guarantees such as, in particular, Standard Contractual Clauses. If these conditions are not met, transfers outside the European Union are only authorised with the Customer's prior consent. Additional technical security measures designed to strengthen the security of the Customer's Personal Data must be implemented if the Personal Data is transferred to a non-democratic country.

## 12. Retention periods and fate of Customer Personal Data

The Processor undertakes to retain the Customer's Personal Data only for the duration of the use of the Service, in accordance with the instructions detailed in the appendix, and to delete it at the end of the Contract. The Processor shall certify, upon written request, that the Personal Data and all existing copies thereof have been deleted.

The Customer is informed that they must retrieve their personal data before the end of the Agreement. If it fails to do so, the Customer may no longer recover its Personal Data, the deletion of the Personal Data being irreversible and definitive. The Processor shall not be held responsible for any loss of Personal Data following its deletion, as the Customer assumes full responsibility. The Customer agrees that the total and irreversible and definitive anonymisation of the Customer's Personal Data may be used as a means of deletion and that the Processor shall retain the anonymised data for the improvement of the Service, as is accepted for the Supervisory Authorities.

The Processor informs the Customer that the return of Personal Data provided for in the GDPR does not constitute Reversibility of the data to a new processor and that any request to this effect will always be refused by the Processor.

## 13. Audits

The Customer has the right to carry out an audit in the form of a written questionnaire once a year to verify compliance with this Agreement. The questionnaire shall have the force of a sworn undertaking binding on the Processor. The questionnaire may be sent in any form to the Processor, who undertakes to reply as soon as possible after receiving it.

The Customer also has the right to carry out, once a year and at its own expense, an on-site audit at the Processor’s premises in the event of a data breach due to a proven and demonstrated breach by the Processor which has resulted in duly justified prejudice to the Customer. An audit at the Processor’s premises may be carried out either by the Customer or by an independent third party appointed by the Customer and must be notified to the Processor in writing at least thirty (30) days before the audit is carried out. The Processor has the right to refuse the choice of the independent third party if the latter is i) a direct or indirect competitor of the Processor, ii) in a situation of conflict of interest with the Processor (e.g. counsel to a competitor of the Processor) or ii) in pre-litigation or litigation with the Processor. In this case, the Customer undertakes to select a new independent third party to carry out the audit. The Processor may refuse access to certain areas for reasons of confidentiality or security. In this case, the Processor carries out the audit in these areas and communicates the results to the Customer.

In the event of a discrepancy being identified during the audit, the Processor undertakes to implement, without delay and at its own expense, the necessary measures to comply with this Agreement. Deviations may only concern the Regulations applicable to the Customer's Personal Data and may not concern internal procedures or measures implemented by the Customer on a specific basis. Deviations must be duly demonstrated, justified and documented.

In the event that the Processor disputes the discrepancies identified, the Processor may, at the customer's option and subject to prior written acceptance, propose to i) meet in order to find an amicable solution and a compromise, ii) refer the matter to the Control Authority in order to obtain arbitration of the dispute, and iii) refer the matter to an independent expert to arbitrate the dispute.

## 14. Cooperation with the authorities

The Processor undertakes to cooperate with the CNIL, the competent supervisory authority, in the event of an inspection concerning the processing carried out as part of the Service and undertakes to notify the Customer as soon as possible in the event of requests concerning his Personal Data being made by the supervisory authority or by an administrative, judicial or police authority.

## 15. Contact

The Customer and the Processor shall each appoint a contact person to be responsible for this Agreement, who shall be the addressee of the various notifications and communications to be made under the Agreement.

The Processor informs the Customer that it has appointed Dipeeo SAS as its Data Protection Officer, who can be contacted at the following address:

* Email address: dpo@praiz.io
* Postal address: Dipeeo SAS, 95 avenue du Président Wilson, 93100 Montreuil, France
* Phone number: +33 (0)1 59 06 81 85

## 16. Revisions

The Processor reserves the right to amend this Agreement in the event of changes to the rules applicable to the protection of Personal Data or in the event of changes to the Service which would have the effect of amending any of its provisions.

*Certified by Dipeeo ®*