Data Processing Agreement for Clients

Last Modification Date: [October/2023]

INTRODUCTION

The present contract governs the Data Processing Agreement (hereinafter referred to as the "**Processing Agreement**" and/or the "**Agreement**") which forms part of the Terms and Conditions of Contracting (hereinafter referred to as "**T&C**") between TRAMITAPP SL ("**TRAMITAPP**") and the CLIENT for the subscription to any Plan, as well as the free trial period that TRAMITAPP offers to the CLIENT.

In accordance with the T&C, TRAMITAPP provides cloud-based human resources services to its clients, whereby, in terms of data protection, TRAMITAPP shall assume the role of DATA PROCESSOR as described in this Agreement, and the CLIENT will assume the role of DATA CONTROLLER of the data of the data subjects.

This Data Processing Agreement shall prevail with respect to data protection regulations over any clause that may be included in the T&C and/or any subsequent agreements between the parties.

Important Note: *If you need or would like a signed copy of this Data Processing Agreement, please contact us via our email: gdpr@tramitapp.com to process your request.*

SECTION I

OVERVIEW

1. Scope and Purpose

In order to regulate the processing of personal data subject to this Data Processing Agreement, and replacing any prior clause related to this matter, both Parties agree to grant this Annex, which shall be governed by the GDPR of the European Parliament and of the Council, dated April 27, 2016 (hereinafter "**GDPR**"), Organic Law 3/2018, of December 5, on Data Protection and Guarantee of Digital Rights (hereinafter "**LOPDGDD**"), its implementing regulations, and, in particular, by the following:

2. Definitions

The definitions found throughout this Agreement shall have the meaning in accordance with the provisions of Article 4 of the GDPR.

The respective functions, duties, and obligations of the Data Controller as well as the Data Processor are defined in this Annex.

In Appendix I, the Parties are identified according to the roles assumed in terms of data protection.

SECTION II

OBLIGATIONS OF THE PARTIES

3. Description of Data Processing

The details of the processing of personal data, particularly the categories of personal data and the purposes of the processing for which the personal data is processed on behalf of the Data Processor, are specified in Appendix II.

4. Obligations of the Parties

4.1. Instructions

4.1.1. The Data Processor shall only process personal data following the documented instructions of the Data Controller, unless required to do so by Union or Member State law to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of this legal requirement before processing, unless such disclosure is prohibited by law for important reasons of public interest. The Data Controller may also issue further instructions during the processing of personal data. These instructions must always be documented.

4.1.2. The Data Processor shall immediately inform the Data Controller if, in its opinion, the instructions given by the Data Controller infringe the GDPR or the applicable data protection provisions of the Union or Member States.

4.2. Purpose Limitation

The Data Processor shall only process personal data for the specific purpose or purposes outlined in this Annex, unless it receives other documented instructions from the Data Controller during the course of the contractual relationship.

The documented instructions from the Data Controller cannot deviate from the scope of the service provided by the Data Processor, in accordance with the T&C.

4.3. Duration of Personal Data Processing

The processing by the Data Processor shall only take place for the duration specified in Appendix II.

4.4. Security of Processing

The Data Processor shall implement, at a minimum, the technical and organizational measures specified in **Appendix III** to ensure the security of personal data. This includes protecting the data against a security breach that results in its accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access (personal data breach). When assessing the appropriate level of security, the Parties shall duly consider the state of the art, implementation costs, the nature, scope, context, and purposes of the processing, as well as the risks to the data subjects.

The Data Processor shall grant access to the personal data being processed to its personnel only to the extent strictly necessary for the execution, management, and monitoring of the contract. The Data Processor shall ensure that persons authorized to process the personal data have committed to confidentiality or are under an appropriate legal obligation of confidentiality

4.5. Sensitive Data

The services provided by the Data Processor involve the processing of sensitive data. It is the responsibility of the Data Controller to oversee the communication of sensitive data, and the Data Controller must notify the Data Processor as early as possible so that the necessary technical measures can be applied.

4.6. Documentation and Compliance

The Parties must be able to demonstrate compliance with these Clauses.

The Data Processor shall promptly and appropriately address the Data Controller's inquiries regarding the processing of data in accordance with these clauses.

The Data Processor shall make available to the Data Controller all the necessary information to demonstrate compliance with the obligations established in these clauses and directly derived from the GDPR. Upon the Controller's request, the Data Processor shall also allow for and contribute to audits of the processing activities covered by these clauses, at reasonable intervals or if there are indications of non-compliance. When deciding on a review or an audit, the Data Controller may take into account any relevant certifications held by the Data Processor.

The Data Controller shall have the right to conduct audits of the Data Processor, in accordance with Article 28 of the GDPR, bearing any potential costs. The audit should be conducted remotely or through a compatible technological solution and must be carried out with reasonable notice, provided that 15 business days' notice is given and conducted within the Data Processor’s business hours. The audits must be supervised by a TRAMITAPP employee and must respect confidential data that is unrelated to the audit being conducted. Additionally, a confidentiality agreement must be signed.

The Parties shall make the information mentioned in this clause, including the results of any audit, available to the competent supervisory authority(ies) upon request.

4.7. Use of Sub-processors

GENERAL WRITTEN AUTHORIZATION: The Data Processor has the general written authorization from the Data Controller to engage sub-processors, who are listed in Appendix III.

The Data Processor shall specifically inform the Data Controller in writing of any proposed changes to that list, including the addition or replacement of sub-processors, with 30 days' notice, thus giving the Data Controller sufficient time to object to such changes before the engagement of the sub-processor(s) in question. The Data Processor shall provide the Data Controller with the necessary information to enable them to exercise their right to object.

At the Data Controller's request, the Data Processor shall provide the Data Controller with a copy of the Data Processing Agreement with the sub-processor and any subsequent modifications. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Data Processor may redact or remove such confidential information from the contract before sharing the copy.

The Data Processor shall remain fully responsible to the Data Controller for ensuring that the sub-processor complies with its obligations under its data processing agreement. The Data Processor shall notify the Data Controller of any breach of the sub-processor's contractual obligations.

The Data Processor shall agree with the sub-processor on a third-party beneficiary clause whereby—in the event that the Data Processor has effectively disappeared, ceased to exist legally, or has been declared insolvent—the Data Controller shall have the right to terminate the sub-processing agreement and instruct the sub-processor to delete or return the personal data that is under the responsibility of the Data Controller.

4.8. International Transfers

Any transfer of data to a third country or an international organization by the Data Processor shall only be carried out based on the services provided to the Data Controller (as accepted through the T&C) or to fulfill a specific requirement under the Union or Member State law to which the Data Processor is subject and shall take place in accordance with Chapter V of the GDPR.

The Data Controller agrees that, when the Data Processor engages a sub-processor in accordance with clause 4.7 to carry out specific processing activities (on behalf of the Data Controller) and such processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, the Data Processor and the sub-processor may ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of the GDPR, provided that the conditions for the use of such standard contractual clauses are met.

5. Assistance to the Data Controller

The Data Processor shall promptly notify the Data Controller of any request it has received from the data subject. However, the Data Processor is not obliged to respond to the request itself; this responsibility lies with the Data Controller.

The Data Processor shall assist the Data Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling these obligations, the Data Processor shall follow the Data Controller's instructions.

In addition to the Data Processor's obligation to assist the Data Controller, the Data Processor must also assist the Data Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Data Processor:

The obligation to carry out an assessment of the impact of the proposed processing operations on the protection of personal data (a "**Data Protection Impact Assessment**") when a type of processing may pose a high risk to the rights and freedoms of natural persons;

The obligation to consult the competent supervisory authority(ies) before processing when a Data Protection Impact Assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate it;

The obligation to ensure that personal data are accurate and up to date, promptly informing the Data Controller if the Data Processor becomes aware that the personal data being processed is inaccurate or has become outdated;

The obligations under Article 32 of the GDPR.

The Parties shall set out in **Appendix III** the appropriate technical and organizational measures by which the Data Processor shall assist the Data Controller in implementing this clause, as well as the scope and extent of the required assistance.

6. Notification of Personal Data Breach

In the event of a personal data breach, the Data Processor shall cooperate with the Data Controller and provide assistance to ensure compliance with the obligations under Articles 33 and 34 of the GDPR, as appropriate, taking into account the nature of the processing and the information available to the Data Processor.

6.1. Data Breach Related to Data Processed by the Data Processor

In the event that the Data Processor becomes aware of and verifies any accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure, or access to the Data Controller’s Personal Data ("**Security Breach**"), the Data Processor shall notify the Data Controller of the circumstances without undue delay and, in any case, within a period not exceeding 48 hours from the moment of becoming aware of it.

Such notification must contain, at a minimum:

- A description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records affected);
- The contact details of a point of contact where more information about the personal data breach can be obtained;
- Its likely consequences and the measures taken or proposed to address the breach, including those to mitigate its possible adverse effects.

When, and to the extent that it is not possible to provide all this information at the same time, the initial notification shall include the information available at that moment, and additional information shall be provided as it becomes available, without undue delay.

The Parties shall set out in Appendix III all other elements that the Data Processor must provide when assisting the Data Controller in fulfilling its obligations under Articles 33 and 34 of the GDPR.

7. Return, Retention, and Deletion of Personal Data

TRAMITAPP provides the CLIENT with 30 days, following their formal notification of termination or subscription cancellation, to download all the information stored and managed on the Platform.

After the 30-day notice period for the Client to download all information, TRAMITAPP shall proceed to block the data for security reasons and to comply with the applicable legal obligations. Upon the conclusion of the blocking period, TRAMITAPP shall automatically delete the data.

SECTION III

FINAL PROVISIONS

8. Termination and Conclusion of Service

Notwithstanding the provisions of the GDPR, if the Data Processor fails to fulfill its obligations under these Clauses, the Data Controller may order the Data Processor to suspend the processing of personal data until it complies with these Clauses or the contract is terminated. The Data Processor shall promptly inform the Data Controller if it is unable to comply with these Clauses, for any reason..

The Data Controller shall have the right to terminate the contract with respect to the processing of personal data under these Clauses if: (a) the Data Processor substantially or persistently breaches these Clauses or its obligations under the GDPR, and (b) the Data Processor fails to comply with a binding decision from a competent court or the competent supervisory authority(ies) concerning its obligations under these Clauses or the GDPR.

The Data Processor shall have the right to terminate the contract with respect to the processing of personal data under these Clauses when, after having informed the Data Controller that its instructions violate applicable legal requirements in accordance with Clause 4.1.1.2, the Data Controller insists on the implementation of those instructions.

Upon termination of the contract, the Data Processor provides the Data Controller with the option to access the platform and download all information related to the service provided, as well as any personal data. After the period specified in Clause 7 of this Agreement, the Data Processor will block the data for a period not exceeding one year for legal reasons and/or potential judicial matters. After this period, all personal data processed on behalf of the Data Controller will be deleted, unless Union or Member State law requires the retention of personal data. Until the data is deleted or returned, the Data Processor will continue to ensure compliance with these clauses.

APPENDIX I

List of Parties

Data Controller(s):

Name: CLIENT who has accepted the T&C.

Address: Address of the CLIENT.

Name of the CLIENT's contact person, position, and contact details:

Data Processor(s):

Name: TRAMITAPP SL

Address: Calle Diego de León 5, 6º derecha - 28006 Madrid

Contact: Blanca Cabanas (Administradora solidaria) - gdpr@tramitapp.com

APPENDIX II

1. Description of the Processing

- Creation and registration of clients on the Platform
- Management and storage of personal data necessary to provide cloud-based human resources services. Services include the following:
  - Management of schedules and Time Tracking (via web with IP registration, through mobile phone with geolocation, or through a kiosk with ID and PIN or Facial Recognition).
  - Management of leave and absences
  - Communications and document signing
  - Management of incidents and payroll distribution
  - Expenses, per diems, and mileage
  - Whistleblowing channel
  - Scheduler
  - Processes related to the HR department of companies
- Sending communications related to the use of the Platform
- Quality services and Platform improvement.
- Technical support

2. Categories

Categories of data subjects whose personal data is processed:

End Users of the Clients (Employees and Administrators)

Categories of personal data processed: *As indicated in point 3.*

TRAMITAPP has appointed a Data Protection Officer within its organization. If you wish to make an inquiry regarding the processing of your personal data, you can contact us via the following email: gdpr@tramitapp.com

3. Collection of Personal Data and Its Processing

Below are the personal data that we may process on our platform, as well as the legal basis that justifies such data processing.

Category of Data Subjects	**Personal Data and/or Category of Personal Data**
End Users	**Identifying and Personal Data:** Name and surname, ID number, address, email, phone number, social security number, nationality, marital status, date of birth, etc. **Employment Characteristics:** Position/job title, category or professional group, department, etc. **Academic and Professional:** Degree, training, experience, performance, etc. **Attendance Control:** Entry and exit date/time, absences (leave, vacations, sick leave…), etc. **Economic and Financial Data:** Bank account, payroll, expenses, etc. **Special Categories:** Biometric data (facial recognition), geolocation (at the time of clocking in from the app).

4. Nature of the Processing: Collection, gathering, recording, storage, consultation, use, retrieval, restriction, and deletion.

5. Purpose(s) for which the personal data is processed on behalf of the Data Controller: Provision of services agreed upon in the T&C.

6. Duration of Processing: The duration of this Agreement is tied to the duration established by the parties in the T&C.

APPENDIX II

Technical and Organizational Measures Applied to Ensure Data Security

1. Confidentiality (Art. 32(1)(b) GDPR)

A) Access Control

The following measures are intended to prevent unauthorized persons from accessing our data processing systems.

☐ Personal and individual user login when accessing the system
☐ Authorization process for access rights (onboarding/offboarding)
☐ Limitation of authorized users by access levels
☐ Password policy
☐ Password procedure (specification of password parameters regarding complexity and update intervals)
☐ Electronic documentation of passwords and protection of this documentation against unauthorized access
☐ Client access logging on the Platform
☐ Additional login to the system for specific applications

B) Access Control

We have implemented the following measures to ensure that unauthorized persons do not have access to the personal data processed by us.

☐ Administration and documentation of different authorizations
☐ Entering into data processing agreements with secure external providers for the control and management of user data storage on the Platform
☐ Evaluation/recording of data processing
☐ Management of the exercise of rights for Platform users
☐ Internal user profiles/roles
☐ Encryption of CD/DVD ROMs, external hard drives, and/or laptops
☐ Measures to prevent unauthorized data transfer to external data storage devices (e.g., copy protection, USB port blocking, Data Loss Prevention (DLP) system)
☐ Dual control principle
☐ Separation of duties
☐ Expert destruction of files and data storage media according to DIN 66399 standard
☐ Specific privacy policies for the website as well as for the Product contracting process

d) Separation Control

The following measures ensure that personal data collected for different purposes is processed separately.

☐ Storage of data sets in separate cloud databases
☐ Data processing in separate systems
☐ Access rights according to functional responsibility
☐ Data processing separately through differentiated access rules
☐ Separation of development and production environment

2. Integrity (Art. 32(1)(b) GDPR)

(a) Transfer Control

It is ensured that personal data cannot be read, copied, modified, or deleted without authorization during transmission or storage on data carriers, and that it is possible to verify which individuals or entities have received personal data. The following measures have been implemented to ensure this:

☐ Encryption of storage media on laptops
☐ Secure file transfer
☐ Secure data transport (e.g., SSL, FTPS)
☐ Secure Wi-Fi
☐ "Mobile Device Management (MDM) system"
☐ Device Management and Control Procedure or Policy
☐ Cloud backup logging
☐ Comment field on the Platform (SSL encryption)
☐ Encrypted cloud solutions for data transmission

b) Entry Control

The following measures ensure the ability to verify who processed personal data in the data processing systems and at what time

☐ Access rights
☐ Functional responsibilities, organizational responsibilities
☐ Principle of multiple user control

3. Availability and Resilience (Art. 32(1)(b) GDPR)

Availability Control and Resilience Control

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client.

☐ Security concept for software and IT applications
☐ Backup procedure
☐ Cloud backup storage process
☐ Ensure data storage in a secure network
☐ Proper installation of security updates

4. Procedure for periodic review, assessment, and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

a) Data protection management

The following measures are intended to ensure an organization that meets the basic data protection requirements:

☐ Data protection concept
☐ Appointment of a Data Protection Officer (“DPO”)
☐ Employee commitment to data confidentiality, especially with regard to sensitive data
☐ Sufficient employee training in data protection matters
☐ Maintain an overview of processing activities (Art. 30 GDPR)
☐ Conduct data protection impact assessments when necessary (Art. 35 GDPR)
☐ Extensive internal review of information security
☐ Definition of the processing of sensitive personal data through pseudonymization processes

b) Incident response management

The following measures are designed to ensure the activation of notification processes in the event of data protection breaches:

☐ Process for notifying data protection breaches to supervisory authorities in accordance with Art. 4(12) GDPR (Art. 33 GDPR)

☐ Process for notifying data protection breaches to affected individuals in accordance with Art. 4(12) GDPR (Art. 34 GDPR)

c) Service monitoring

The following measures ensure that personal data can only be processed in accordance with instructions.

☐ Data processing agreement regulating the rights and obligations of the TRAMITAPP Provider

☐ Instruction tracking process

☐ Assignment of contact persons and/or responsible employees

☐ Training/instruction for all employees with access rights to the Platform, especially concerning sensitive customer data

☐ Employee commitment to data confidentiality and signing of Non-Disclosure Agreements (NDAs)

☐ Agreement on contractual penalties for non-compliance with instructions

☐ Monitoring and oversight of service provider selection

☐ Standardized contract management for the prior assessment and ongoing monitoring of service providers

APPENDIX III

List of sub-processors

Due to confidentiality and trade secret agreements with our suppliers, the list of sub-processors is not publicly available. If you require more information about the sub-processors or wish to obtain a copy of this list as a party to the current Contract, you may contact us via our email at gdpr@tramitapp.com.