# Data Processing Agreement

This document serves as an indivisible addendum to the Agreement executed between the TrustCloud companies and the Customer, forming an integral component thereof. It does not constitute an amendment to the Agreement, which shall remain in effect and fully enforceable.

## Controller and Processor

- The Customer will act as the Data Controller.
- The Provider will act as the Data Processor.

## Categories of Personal Data (mark or delete as appropriately)

- Identifying Data (name and surname, ID number, passport, SS number, address, phone, signature, fingerprint, image/voice, physical marks, electronic signature, email, phone number, electronic identification data).
- Biometric data, when required for the provision of the service (e.g. face match).
- Electronic location data, IP address.
- Any information contained in a signed document, electronic certificate, power of attorney or stored documents.
- Personal Characteristic Data (marital status, family data, date of birth, place of birth, age, gender, nationality, mother tongue, physical or anthropometric characteristics).
- Data on social circumstances (housing characteristics, property or possessions, hobbies and lifestyle, membership of clubs or associations, licenses, permits, or authorizations).
- Academic and Professional Data (education/qualifications, student history, professional experience, membership of professional colleges or associations).
- Employment Details Data (profession, job position, non-economic payroll data, worker's employment history).
- Commercial information Data (activities or businesses, commercial licenses, subscriptions to publications or media, literary, artistic, scientific or technical creations).
- Economic, Financial, and Insurance Data (income and earnings, investments and assets, credits, loans, and guarantees, banking information, pension and retirement plans, economic payroll data, tax deductions and taxes, insurance, mortgages, subsidies and benefits, credit history, credit card).
- Data on Goods and Services Transactions (goods and services provided by the Data Subject, goods and services received by the Data Subject, financial transactions, compensations, and indemnities).
- Health or Disability Data.
- Union membership, religion, beliefs, or data related to sexual life data.
- Data related to criminal offenses.
- Any special category of data that may be included in signed documents, electronic certificates, powers of attorney or stored documents.
- Others necessary for the provision of services.

## Categories of Data Subjects Whose Data Will Be Processed (mark or delete as appropriately)

- Customers.
- Users or End-user of Customer's Customer.
- Potential Customers.
- Providers.
- Contact person.
- Employees.
- HR candidates.
- Any person whose images are captured through videoidentification.
- Other as needed by the controller.
- Any user of the services.
- Any person the controller allows to use the services.

## Activities of Treatment

The relevant activities consist of providing electronic trust services such as videoidentification (based on assisted, unassisted procedures or the use of the platform), electronic signature, qualified or non-qualified preservation, archiving, or any other as contracted in each moment. The Personal Data transferred will be subject to the following basic processing activities: Collection, Recording, Structuring, Modification, Preservation, Storage, Extraction, Consultation, Dissemination, Measurement, Interconnection, Review, Suppression, Deletion, Limitation, Destruction, Communication, Anonymisation, Comparation, Any other derived from the provision of the services.

# CLAUSES

## OBJECT.

1.1 This DPA aims to define the conditions under which the Data Processor will carry out the processing of Personal Data necessary for the proper provision of the Services provided to the Data Controller.
1.2 The Customer will act as the Data Controller.
1.3 The Provider will act as the Data Processor.
The provision of the contracted Services implies the execution by the Data Processor of the following processing activities: collection, recording, consultation, dissemination, modification, communication by transmission, interconnection, storage, and erasure of Personal Data, as well as any others directly resulting from the provision of the contracted Services.

## DURATION.

2.1 This DPA will be in effect for the entire duration of the Services provided by the Data Processor. Notwithstanding the foregoing, both Parties agree that the provisions of this DPA, whether expressly or implicitly intended to remain in force after its termination or expiration, shall remain in effect and continue to bind both Parties as stipulated.

## PURPOSE OF PROCESSING.

3.1 The Data Processor commits to ensure that the data processing performed remains strictly necessary for the provision of the Services.
3.2 The Data Processor agrees to process the data following the instructions provided in writing by the Data Controller at any given time.
3.3 If the Data Controller deems it necessary to issue different instructions from those mentioned, they shall expressly communicate these instructions to the Data Processor. In the event that the Data Processor believes that an instruction from the Data Controller may contravene applicable data protection regulations, the Data Processor shall inform the Data Controller of this.
3.4 If the Data Processor deems it necessary to carry out data processing beyond these limits or to use the data for a purpose other than the provision of the Service referred to in this Agreement or compliance with legal obligations, it must first request written authorization from the Data Controller. In the absence of this authorization, the Data Processor may not carry out such processing.
3.5 The Data Processor will exercise the utmost diligence in the provision of the Services concerning the processing of Personal Data conducted within the framework of the Agreement.

## DATA RETENTION.

4.1 Personal Data shall be retained by the parties during the term of the Agreement and, upon its termination, for the duration of the statute of limitations for any potential legal liabilities of any kind. Once the legal statute of limitations has expired, the Personal Data shall be destroyed.

## TYPES OF PROCESSED DATA AND CATEGORIES OF DATA SUBJECTS.

5.1 The categories of data subjects, as well as the identification of the types of Personal Data that will be processed by the Data Processor, are detailed in the table located at the top of this Annex.

## PROHIBITION OF PERSONAL DATA DISCLOSURE.

6.1 Personal Data shall not be transferred to third parties, except when required by law. However, they may be accessible to providers that offer services to the parties and other companies within the group of which TrustCloud belongs, in order to fulfill the purposes of the processing.
6.2 The Data Processor commits to keep Personal Data provided by the Data Controller under its control and custody, which may be accessed during the provision of services. The Data Processor shall not disclose, transfer, or otherwise communicate them to any third party unrelated to the provision of the service under this Agreement, not even for the purpose of retention.
6.3 The Data Processor shall not be held liable when, following an explicit written instruction from the Data Controller, it discloses the data to a third party designated by the Data Controller, to whom it has assigned the provision of a service in accordance with the prevailing data protection regulations.
6.4 Access by the Data Processor to personal data for the proper provision of the services under this Agreement shall not be considered data disclosure or transfer.

## SUBCONTRACTING OF SERVICES.

7.1 The services provided by TrustCloud require the subcontracting of essential service providers, which are listed in Appendix I to this DPA. These providers will be considered Subprocessors in relation to the personal data of the Data Controller processed under the Service or Services contracted. In this regard, the Data Controller may request more detailed information about the Service contracted with the Data Processor during the provision of the Service.
7.2 Appendix I to this DPA will be reviewed and, if necessary, updated during renewals of the contracted Service or Services.
7.3 Notwithstanding the above, the Data Processor shall inform the Data Controller of any relevant changes in Appendix I to this DPA that affect the contracted Service or Services within a maximum of 15 days. If, within 15 days from the date of notification, the Data Controller does not object to the change, it will be considered authorized.
7.4 The Data Controller authorizes the data to be subject to international transfer outside the European Economic Area by the Data Processor and/or the Sub-processor when necessary for the proper provision of the contracted Services.
7.5 The Data Processor will implement the necessary legal safeguards to ensure an equivalent level of security in the processing of Personal Data through appropriate additional safeguards, as well as compliance with the legal requirements as required by current regulations.
7.6 The transfer of data from the Data Processor to the Sub-processor will be solely for the purpose of subcontracting all or some of the Services contracted by the Data Controller to the Data Processor, limited to the Personal Data necessary for the provision of the subcontracted Services. The transfer will not reduce the obligations and responsibilities assumed by the Data Processor under this Agreement.
7.7 The Data Processor may provide more detailed information upon request by the Data Controller via the following email: dpo@trustcloud.tech.

## PERSONAL DATA SECURITY.

8.1 The Data Processor commits to ensuring the application of appropriate technical and organizational measures so that the processing complies with legal requirements, specifically ensuring an adequate level of security in accordance with the risk and the protection of the rights of data subjects. This consideration shall take into account the latest techniques, the costs of implementation, the nature, scope, context, and purposes of the processing, as well as the varying risks to the rights and freedoms of individuals, including:
a) Pseudonymization and encryption of Personal Data;
b) The ability to ensure permanent confidentiality, integrity, availability, and resilience of processing systems and services;
c) The capability to promptly restore availability and access to Personal Data in the event of a physical or technical incident;
d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure processing security.
8.2 When assessing the appropriate level of security, the Data Processor commits to specifically consider the risks presented by the processing, especially those arising from accidental or unlawful destruction, loss, alteration, and unauthorized disclosure or access to Personal Data that is transmitted, stored, or subject to any other form of processing.

## SECURITY BREACH NOTIFICATION AND COLLABORATION.

9.1 In the event of a security breach occurring in the systems of the Data Processor that may affect data for which the Data Controller is responsible, the Data Processor, within a maximum of 48 hours after becoming aware of the Personal Data breach, is obliged to notify the Data Controller through the Project Manager, along with all relevant information for documenting and reporting the incident.
9.2 Notification will not be required when it is unlikely that such a security breach constitutes a risk to the rights and freedoms of individuals.
9.3 If the Data Processor has it, they shall provide the Data Controller with, at a minimum, the following information:
a) A description of the nature of the Personal Data breach, including, if possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of records of Personal Data involved.
b) The name and contact information of the data protection officer or another contact point where information can be obtained.
c) A description of the likely consequences of the Personal Data breach.
d) A description of the measures taken or proposed to address the Personal Data breach, including, if applicable, measures taken to mitigate potential negative effects. If it is not possible to provide the information simultaneously, and to the extent that it is not possible, the information will be provided gradually without undue delay.
9.4 In the event and to the extent that it is not possible to provide all the information at once, it may be provided in phases without undue delay.

## RIGHTS OF ACCESS, RECTIFICATION, ERASURE, RESTRICTION, OBJECTION, AND DATA PORTABILITY.

10.1 The Data Processor commits to assist the Data Controller in responding to requests regarding the exercise of rights of access, rectification, erasure, objection, restriction of processing, data portability, and to not be subject to automated individualized decisions (including profiling).
10.2 In the event that those affected exercise their rights before the Data Processor and/or authorized Sub-processor, they should immediately transfer the request to the Data Controller and in no case later than the business day following the receipt of the data, together, where appropriate, with other information that may be relevant to resolve the request, so that the Data Controllers can properly resolve said request.
10.3 The Data Processor and/or Sub-processor shall take the necessary measures to ensure the timely transfer to the Data Controller, as described, along with the requested information, in order to effectively address the exercised rights.
10.4 In any case, the Data Processor and/or Sub-processor shall be held responsible for any negligence that may lead to the failure to address the exercised rights, as well as for any damages that may be caused to the Data Controller.

## RESPONSIBILITIES OF THE DATA CONTROLLER.

For the execution of the Service, the Data Controller commits to:

11.1 Make available to the Data Processor the Personal Data and/or information necessary for the proper processing of such data for the provision of the Services.
11.2 Issue the corresponding instructions regarding the processing of Personal Data and monitor their compliance by the Data Processor.
11.3 Conduct a risk analysis that may arise from the processing activity to be entrusted and, based on such analysis, specify to the Data Processor the technical and organizational measures to be implemented for the provision of the entrusted processing Service.
11.4 Conduct, if necessary, an impact assessment on the protection of Personal Data for the processing operations to be carried out by the Data Processor.
11.5 The development of the contracted Services may involve the Data Processor capturing various Personal Data and subsequently processing them, with the aim of allowing the Data Controller to demonstrate the authenticity of electronic communications that have been intermediated by the Data Processor, as a trusted service provider. In this regard, it is the responsibility of the Data Controller to assess whether the data processed during the provision of the contracted Services are necessary, proportionate, and appropriate, and their processing is lawful in accordance with the applicable data protection regulations.

## CONFIDENTIALITY

12.1 The duty of secrecy and confidentiality arising from this Agreement obliges the Data Processor during the term of the relationship with the Data Controller and it will extend, depending on the type of information, for the maximum periods provided for in the applicable legislation. In particular, with regard to the processing of personal data, the duty of confidentiality shall have an indefinite duration, even after the termination of the relationship between the Parties.
12.2 The Data Processor ensures that the persons under its supervision, authorized to process the Personal Data for which the Data Controller is responsible, commit to confidentiality and will be subject to appropriate legal confidentiality obligations, even after the termination of the Agreement. The Data Processor will make available to the Data Controller the documentation proving that the corresponding confidentiality commitments have been signed.
12.3 The Data Processor commits to allowing access to such data only to those employees who need to know them for the proper performance of their duties under the Agreement.

## DATA RETURN OBLIGATION.

13.1 Once the provision of the Services under the Agreement has been completed, the Parties shall execute the Transfer Plan detailed in the Service Provision Agreement.

## GUARANTEE OF COMPLIANCE.

14.1 The Data Processor guarantees the compliance with the obligations that apply to it as the Data Processor under the data protection regulations.
14.2 The Data Controller reserves the right to verify the Data Processor's compliance with the obligations specified in this Agreement, periodically and always with prior notice of the audit, while minimizing any inconvenience.
14.3 In this regard, the Data Processor commits to provide the Data Controller with certificates and documents confirming these terms if requested.
14.4 Likewise, in the event of an inspection or request by the Spanish Data Protection Agency or other competent authorities, the Data Processor will provide any necessary information related to the purpose and development of the Services covered by this Agreement to demonstrate compliance with current regulations

## COOPERATION AND RESPONSIBILITIES IN THE CASE OF CLAIMS.

15.1 If the Data Processor becomes involved in any investigation or administrative sanction procedure initiated by the Spanish Data Protection Agency or another Regulatory Authority, or in a claim by a third party, it shall immediately inform the Data Controller, describing the facts attributed to it and the actions taken. Once the procedure is concluded, it must provide a copy of the issued Resolution.
15.2 In the event that the Spanish Data Protection Agency or another Regulatory Authority sanctions the Data Controller or any of its customers directly or indirectly as a result of the Data Processor's failure to comply with the provisions of this Agreement, the Data Processor shall indemnify the Data Controller or, as the case may be, the customer for an amount equal to the fine, plus legal interest, as well as the defense and procedural costs incurred, in addition to quantifying any other damages and losses that may arise.
15.3 Notwithstanding the above, both parties mutually agree to be liable for all damages and losses incurred by the other in all cases of negligent or wrongful conduct in the performance of contractual and regulatory obligations as agreed in this Agreement.

## RESPONSIBILITIES.

16.1 The Data Processor commits to fulfilling the obligations established in this Data Processing Annex in accordance with the provisions of the main Agreement between the parties and current regulations.
16.2 In the event that the Data Processor uses the data for another purpose, communicates them, or uses them in violation of the provisions of this Agreement, it shall also be considered a Data Controller, and shall be liable for any violations incurred personally.
16.3 The Data Processor shall indemnify the Data Controller for any damages caused by the Data Processor's failure to comply with any of the obligations contained in this Agreement or the applicable regulations.

## DATA PROTECTION OFFICER.

17.1 As of the date of signing this Annex, the name and contact details of the Provider's Data Protection Officer are as follows:
Name: PricewaterhouseCoopers Tax & Legal, S.L
Contact details: dpo@trustcloud.tech

## DATA OF THE PARTIES.

18.1 Personal Data included in the Service Provision Agreement and any other data exchanged between the Parties to facilitate the provision of the Services will be processed by the other Party for the purpose of enabling the development, fulfillment, and monitoring of the contracted service relationship. The legal basis for this processing is the fulfillment of the contractual relationship, and the data will be retained for the duration of the relationship and even thereafter until any potential liabilities stemming from it become statute-barred. The Parties undertake to inform the data subjects of the data provided about this information, and to indicate that they can submit written requests to the respective addresses provided to exercise their rights of access, rectification, objection, and deletion.

## LEGISLATION AND APPLICABLE JURISDICTION.

19.1 This Agreement shall be governed by the Spanish and European regulations on the protection of personal data, as well as the resolutions and guidelines of the Spanish Data Protection Agency and the other competent authorities in the field.
19.2 To resolve any disputes regarding the interpretation and/or execution of the provisions of this Agreement, both Parties agree to seek an amicable resolution.
19.3 However, in the event an amicable resolution is not reached, the Parties submit to the jurisdiction of the Courts and Tribunals of Madrid, expressly waiving any other laws or jurisdictions that may apply to them.

## ENTRY INTO FORCE.

20.1 This Annex shall come into effect on the date of its signing and shall remain in force until the termination of the service provision relationship by the Data Processor in favor of the Data Controller, and until all the obligations outlined in this Agreement have been duly fulfilled, irrespective of any other legal obligations applicable to the Parties following the termination of the said relationship.