tsaaro

Data Processing Agreement Template

Contact Us:

THIS DATA PROCESSING AGREEMENT (hereinafter “Agreement”) dated _____by and between

_____
_____
_____

(hereinafter “Controller”)

AND

_____
_____
_____

(hereinafter “Processor”)

WHEREAS the Controller is engaged in the business of _____

AND WHEREAS the Processor is independently engaged in the service of Processing Personal Data on behalf of other entities.

AND WHEREAS the Controller desires to hire the Processor for services of Processing of Personal Data and to perform services described herein this Agreement and as such, the Processor wishes to render such services to the Controller.

THEREFORE, in consideration of mutual promises and covenants set forth herein, the parties hereby acknowledge and agree as follows:

1. Definitions

For purposes of this Agreement, the terms shall have the following meanings:

“Consent” of the Data Subject means any freely given, specific, informed, direct and unambiguous indication of the Data Subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

“Controller” has the meaning given to it in the GDPR and shall be interpreted in the light of rights and obligations thereof.

“Data Protection Law” shall include the GDPR and any other applicable law, regulation and rules for the time being in force.

“Data Subject” has the same meaning and effect given to in the GDPR and shall include an identifiable or identifiable natural person and shall be interpreted in the light of circumstances.

"GDPR" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" has the meaning given to it in GDPR and shall include any information relating to an identified or identifiable natural person.

"Processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"Processor" has the meaning given to it in the GDPR and shall be interpreted in the light of rights and obligations thereof.

"Security Incident" means a breach of Processor's systems leading to accidental or unlawful destruction, alteration, unauthorized access or any damage caused to Personal Data provided by controller for Processing.

Terms otherwise not defined under this Agreement shall be interpreted in light of the meanings assigned to them under the GDPR.

2. Purpose and Scope

2.1. The Processor shall process Personal Data for the limited purpose of performing the obligations set out under the Agreement or within the scope of written lawful documented instructions provided from time to time by the Controller.

2.2. The term of this Agreement shall continue until the later of the following:
   A. The termination of the Agreement;
   B. The date at which the Data Processor ceases to process Personal Data for the Data Controller.

2.3. The Personal Data to be processed by the Processor for purposes of the Processing set out in Clause 3 in this Agreement.

3. Processing Operations

3.1. The Personal Data shall be processed in accordance with this Agreement and may be subject to the following Processing activities.
   A. Storage and Processing of data necessary to provide and maintain services subscribed by the Controller.
   B. Disclosures permissible by GDPR and in accordance with this Agreement or as authorised by Controller in writing.

3.2. The Parties shall comply with all laws, regulations and rules applicable to its performance under this Agreement.

4. Confidentiality of Data

4.1. The Processor shall not access or disclose data provided by the Controller to any third party in the European Economic Area ("EEA") which will provide for hosting of the services, except to the extent necessary for provision of services or maintenance under this Agreement or as necessary to comply with the law in force. The obligations of such third party are envisaged in a separate data processing agreement which is within the framework of this Agreement. All data in the service shall be stored on servers located in Europe.

4.2. The Processor shall implement policies and impose contractual obligations on its personnel regarding data protection, data security and confidentiality. Failure to comply with the same will lead to termination of this Agreement with immediate effect.

5. Obligations of the Data Processor

5.1. The Processor agrees and warrants to:

5.2. To process Personal Data only on behalf of the Controller while complying with the terms of the Agreement and the Data Protection Law;

5.3. Process any Personal Data transferred to or collected by the Data Processor only as a 'processor', as such terms are defined in the Data Protection Law on behalf of the Data Controller;

5.4. Implement appropriate technical and organizational measures and follow established routines in such a manner that Processing will meet the requirements of the applicable Data Protection Law and ensure the protection of the rights of the Data Subjects;

5.5. To deal promptly and properly with requests and inquiries of the Data Controller;

5.6. Assist the Data Controller in ensuring compliance with the requirements for security of Personal Data;

5.7. On a regular basis or on the demand of the Controller, to carry out third party security audits for systems and similar relevant for the Processing of Personal Data and the reports documenting such security audits shall be available to the Controller;

5.8. Take into account the nature of the Processing, assist the Data Controller by appropriate technical and organizational measures, in so far as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights according to the Data Protection Law;

5.9. Make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and to allow for, co-operate and contribute to audits, including inspections to facilities under the control of the Data Processor, conducted by the Controller or an auditor mandated by the Controller and provide access to data systems;

5.10. Promptly notify:
   A. Any binding request for disclosure of Personal Data made by law enforcement authorities under the law in force unless otherwise explicitly prohibited under criminal law to preserve the confidentiality of an investigation;
   B. Any breach, accidental, lawful or unauthorised access; and
   C. Any request received directly from the Data Subjects unless it has been authorised;

5.11. To send promptly a copy of any sub-processor agreement it concludes to the Controller;

5.12. Ensure that its Sub-processors involved in the Processing of Personal Data at all times comply with the obligations and subject to the limitations set forth herein above;

5.13. To ensure confidentiality and non-disclosure of Personal Data at all times;

5.14. To implement and maintain appropriate technical and organisational measures to protect Personal Data from Security Incidents and not to update or modify the security measures provided that such modification or update does not result in a material degradation in the protection offered to Personal Data.

6. Obligation of Data Controller

6.1. The Controller agrees and warrants to:

6.2. The Data Controller will be separately responsible for complying with the Data Protection Law as applicable to them

6.3. Ensure that the Processing of Personal Data which the Data Processor is instructed to perform has a legal basis and has been obtained as per the Data Protection Law

6.4. Instruct the Processor to process the Personal Data transferred only on the Controller's behalf and in accordance with the applicable Data Protection Law

6.5. Ensure compliance with security measures

6.6. Inform the Controller of the transmission of special categories of data prior to data transfer for Processing

6.7. The Data Controller shall inform the Data Processor in writing without undue delay following the Data Controller's discovery of failure to comply with Data Protection Law and/or Agreement with respect to Processing of Personal Data.

6.8. Shall be responsible for providing accurate and relevant information to the Processor after entering into the Agreement and thereafter to assist in Data Processor's notification obligations.

7. Assistance to controller

7.1. The Processor undertakes to provide timely assistance to the Controller in respect of:
   A. Any request from a data subject to exercise any of its rights under data protection law;
   B. Inquiries and complaints of Data Subjects in connection with Processing of Personal Data;
   C. Request from data protection authorities relating to Processing of Personal Data.

7.2. The Processor shall co-operate and provide reasonable assistance to the Controller for conduction of any data protection impact assessments and prior consultation with supervisory authorities or other competent data privacy authorities.

8. Security of Data Processing

8.1. The Processor shall undertake:
   A. Implementation and maintenance of technical and organizational security measures during the subsistence of this Agreement to protect Personal Data against any unauthorized disclosure and appropriation and against unlawful destruction, loss, damage;
   B. Reasonable steps including third party background checks to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited on a need to know / access basis strictly for the for the purposes of this Agreement, and to comply with applicable laws, company guidelines and ethical standards and ensure that such individuals are subject to confidentiality undertakings and/or statutory obligations of confidentiality;
   C. Regular testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented for protection of Personal Data.

8.2. The Controller may elect to implement technical and organisational measures in relation to:
   A. Pseudonymisation and encryption to ensure an appropriate level of security;
   B. Measures to ensure the ongoing confidentiality, integrity, availability and resilience of the Processing systems and services that are being operated by the Controller;
   C. Measures to allow Customer to backup and archive appropriately in order to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
   D. Measures to prevent network traffic using unauthorized protocols from reaching the product infrastructure;
   E. Processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational security measures implemented by Controller.

9. Personal Data Breach

9.1. In an event of Security Incident the Processor shall:
   A. Notify Controller of the Security Incident without undue delay after becoming aware of the Security Incident within 24 hours; and
   B. Take reasonable steps to mitigate the effects to minimise any damage resulting from the Security Incident.

9.2. The notification referred to in Clause 8.1 shall include:
   A. Description of the nature of the Personal Data breach including qualitative and quantitative characteristics of the data breached;
   B. Communicate the name and contact details of the person with the Data Processor where more information can be obtained regarding the Security Incident;
   C. Describe the likely consequences of the Personal Data breach;
   D. Describe the measures taken or proposed to be taken by the Data Processor to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3. In an event of security breach, the Processor shall assist the Controller to make notifications in compliance with the Data Protection Law.

10. Sub-Processors

10.1. The Processor may use sub-processors to fulfil its contractual obligations under this Agreement and to provide certain services on its behalf to the Controller.

10.2. The Processor shall ensure that sub-processors undertake process Personal Data under in accordance with this Agreement and Data Protection Law.

10.3. The Processor shall ensure that its sub-processors shall implement and maintain the security of Personal Data Processing in accordance with Clause 5.1 of the Agreement.

10.4. Any transfer of Personal Data to third countries or international organizations by the Data Processor for the process of sub-Processing shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.

11. Obligations of Sub-Processors

11.1. The Processor shall enter into written agreements with sub-processors and to the extent that the sub-processor is performing the same data Processing services that are being provided by the Processor under this Agreement, the Processor shall/will impose on the sub-processor the same contractual obligations and restrictions that the Processor is bound by under this Agreement.

11.2. The sub-processor shall access data in accordance with the permissions provided by the Processor to the extent of fulfilling its obligations under the sub-Processing agreements.

11.3. The Processor shall be liable for acts or omissions of the sub-processors breaching the obligations of the processor under this Agreement.

12. Liability to Data Subjects

Each party's liability towards Data Subjects shall be to the extent of their acts and omissions contributing to the violation of Data Subject rights under the Data Protection Law.

13. Liability for Breach of Contract

The party committing the breach of contract shall be liable to pay damages to the affected party and/or perform its obligations under this contract to make good any actual and direct losses.

14. Data Transfer

14.1. The Controller must be informed of data transfers prior to such transfer. The Controller must provide written Consent authorizing such transfer by the Processor or sub-processor as applicable. Should the Controller approve such transfer of Personal Data the Processor is obligated to cooperate with the Controller in order to ensure compliant transfers.

14.2. The transmission of data shall be done in accordance with the relevant data protection law applicable to the importing and exporting jurisdictions.

14.3. Any transfer of Personal Data to third countries or international organizations by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.

14.4. If the transfer involves sensitive categories of data then the Consent of the Data Subject shall be obtained by either party for the transmission of the data to a third country not providing adequate protection within the meaning of the GDPR.

15. Deletion or Return of Personal Data

The Processor shall provide the Controller the recourse of deletion and retrieval of Personal Data which had been provided for fulfilling the purposes of this Agreement.

16. Audit Rights

The Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Controller or a third party auditor mandated in relation to the Processing of the Personal Data.

17. Enforcement of Agreement

This Agreement shall remain in full force and effect unless amended, terminated or deemed unenforceable under the law in force. In an event of conflict with the law in force, the Agreement shall be deemed to be unenforceable to the extent it is in conflict with the law.