# Data Processing Agreement

## 1. INTRODUCTION

This Data Processing Agreement (”**Agreement”**) governs the framework by which **ClicData** (Data Processor) will process data on your behalf, the Customer (Data Controller).

It is complementary and in addition to our Terms of Service Agreement, our Data Privacy Agreement and Acceptable Use Policy and it includes Standard Contractual Clauses (SCC) between controllers and processors under Article 28 (7) of Regulation (EU0 2016/679 of the European Parliament and of the Council an Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Annex to the Commission Implementing Decision, of the European Commission of 4 June 2021 (C 2021)3701.

Although it is intended to ensure compliance with Article 28 of the EU General Data Protection Regulation (GDPR) it is also aligned with other applicable privacy laws (such as Canada’s PIPEDA, Australia’s Privacy Act 1988, Brazil’s LGPD, California’s CCPA, etc.) where applicable. In case of any conflict, the terms of this DPA shall prevail over the Agreement on matters of data protection.

If the agreement is not acceptable to you then please contact us prior to using our Platform (”Service”) with Personal Data.

## 1.1. Purpose and scope

1. The purpose of this Agreement is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 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.

2. The controller(s) and processor(s) listed in **Annex I** have agreed to this Agreement in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

3. This Agreement applies to the processing of personal data as specified in **Annex II**.

4. **Annexes I to IV** are an integral part of this Agreement.

5. This agreement is without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

6. This Agreement does not by itself ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

## 1.2. Invariability of the Clauses

1. The Parties undertake not to modify this Agreement, except for adding information to the Annexes or updating information in them.

2. This does not prevent the Parties from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the existing clauses in this Agreement or detract from the fundamental rights or freedoms of data subjects.

## 1.3. Interpretation

1. Where this Agreement uses the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

2. This Agreement shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

3. This Agreement shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

## 1.4. Hierarchy

In the event of a contradiction between the provisions in this Agreement and the provisions of related agreements between the Parties existing at the time when this Agreement was agreed or entered into thereafter, this Agreement shall prevail.

## 1.5. Docking clause

1. Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to the Agreement at any time as a controller or a processor by completing the Annexes and signing **Annex I**.

2. Once the Annexes are completed and signed, the acceding entity shall be treated as a Party to this Agreement and have the rights and obligations of a controller or a processor, in accordance with its designation in **Annex I**.

3. The acceding entity shall have no rights or obligations resulting from this Agreement from the period prior to becoming a Party.

# 2. DESCRIPTION OF PROCESSING(S)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in **Annex II**.

## 3. OBLIGATIONS OF THE PARTIES

### 3.1. Instructions

1. The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

2. The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

### 3.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in **Annex II**, unless it receives further instructions from the controller.

### 3.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in **Annex II**.

### 3.4. Security of processing

1. The processor shall at least implement the technical and organisational measures specified in **Annex III** to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

2. The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 3.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

## 3.6. Documentation and compliance

1. The Parties shall be able to demonstrate compliance with this Agreement.

2. The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with this Agreement.

3. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in this Agreement and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals and cost to the Processor or only if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

4. The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

5. The Parties shall make the information referred to in this Agreement, including the results of any audits, available to the competent supervisory authorityies on request.

## 3.7. Use of sub-processors

1. The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least one month in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

2. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with this Agreement. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to this Agreement and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

3. At the controller's request, the processor shall provide a copy of such a subprocessor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

4. The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor

shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

5. The processor shall agree to a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the subprocessor contract and to instruct the sub-processor to erase or return the personal data.

## 3.8. International transfers

1. Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject **and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

2. The controller agrees that where the processor engages a sub-processor in accordance with paragraph 3.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the subprocessor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

# 4. ASSISTANCE TO THE CONTROLLER

1. The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

2. The processor shall assist the 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 its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

3. In addition to the processor's obligation to assist the controller pursuant to paragraph 4 (b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

    1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

    2. the obligation to consult the competent supervisory authorities prior to processing where a data protection impact assessment indicates that the processing would

result in a high risk in the absence of measures taken by the controller to mitigate the risk;

3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

4. the obligations in Article 32 Regulation (EU) 2016/679.

4. The Parties shall set out in **Annex III** the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Agreement as well as the scope and the extent of the assistance required.

## 5. NOTIFICATION OF PERSONAL DATA BREACH

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

### 5.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- in notifying the personal data breach to the competent supervisory authorities, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

- in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

    - the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    - the likely consequences of the personal data breach;

    - the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the

personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

### 5.2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

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

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

## 6. NON-COMPLIANCE WITH THE AND TERMINATION

1. Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with this Agreement or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with the Agreement, for whatever reason.
2. The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with this Agreement if:
    1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with the Agreement is not restored within a reasonable time and in any event within one month following suspension;
    2. the processor is in substantial or persistent breach of this Agreement or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
    3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

3. The processor shall be entitled to terminate the contract as it concerns processing of personal data under this Agreement where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with paragraph3.1 (b), the controller insists on non-compliance with the instructions or if in breach of the Terms of Service Agreement, the Data Privacy Agreement or the Acceptable Use Policy.

4. Following termination of the contract, the processor shall delete all personal data processed on behalf of the controller and certify to the controller that it has done so. Until the data is deleted or returned, the processor shall continue to ensure compliance with this Agreement.

## ANNEX I. LIST OF PARTIES

**MUTUALLY AGREED** AND SIGNED BY THE DATA CONTROLLER AND CLICDATA (PROCESSOR) ON THE DATES AS INDICATED BELOW:

| **PROCESSOR** | **CONTROLLER** |
|---|---|
| ClicData SAS | |
| Signature | Signature |
| Name | Name |
| Date | Date |

## ANNEX II. DESCRIPTION OF PROCESSING

**Categories of data subjects whose personal data is processed**

Please check those that apply or fill out additional entries

☐ Employees

☐ Employee relatives

☐ Candidates

☐ Clients/Consumers

☐ Business Partners (including their staff)

☐ Website visitors

☐ Suppliers (including their staff)

☐ Visitors

☐ Shareholders

☐ Other stakeholders

☐ Patients

☐ Advisers, consultants and other professional experts

☐ _____

☐ _____

☐ _____

**Categories of personal data processed**

Please check those that apply or fill out additional entries

☐ Personal details, including any information that identifies the data subject and their personal characteristics

☐ Employment details

☐ Education and training details, including certificates and diplomas

☐ CV, working history/experience, education

☐ Pre and intra employment screening data (e.g. reference checks, reports, certificate of good conduct)

☐ Employee participation plan administration data

☐ Financial details

☐ Personal details issued as an identifier by a public authority

☐ Family, lifestyle and social circumstances

☐ Past purchases (consumers)

☐ Goods or services provided and related information

☐ Creditworthiness, credit rating

☐ Profile information (either group profile or individual profile information)

☐ Social media account and social media history of the individual

☐ _____

☐ _____

☐ _____

**Type Sensitive data processed**

If applicable, please check those that apply or fill out additional entries

☐ **None (no special categories of data are being processed)**

☐ Health

☐ Racial or ethnic origin

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Genetic data

☐ Biometric data (if used to identify a natural person)

☐ Sex life or sexual orientation

☐ Criminal convictions and offences

☐ Social security number or national ID

☐ _____

☐ _____

☐ _____

**Nature of the processing and purpose of Processing**

Please check those that apply or fill out additional entries

☐ **HR support services and staff administration**

☐ Training and education services

☐ Recruitment, matching and selection services

☐ Benefits, welfare, grants and loans administration

☐ Pensions administration

☐ Health administration and services and Patient Care

☐ Private investigation

☐ Advertising, marketing targeting and public relations

☐ Consulting and advisory services

☐ Data analytics, including profiling

☐ Property management

☐ Financial services and advice

☐ Accounting and auditing services

☐ Procurement

☐ Legal services

☐ _____

☐ _____

☐ _____

**Duration of the processing**

Describe duration and retention criteria.

---

## ANNEX III. TECHNICAL AND ORGANIZATION MEASURES

Description of the technical and organisational security measures implemented by the processor(s):

**1. Measures of pseudonymisation and encryption of personal data**

ClicData uses encryption to protect personal data both at rest and in transit:

- All personal data stored in the platform is encrypted using **AES-256** encryption.
- All data in transit between users and the platform is encrypted using **TLS 1.2 or higher**.
- Where applicable, tokenization and pseudonymisation are applied for logs and analytics involving personal data.

**2. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services**

- Role-based access control (RBAC) and least privilege principles are enforced.
- Systems are hosted on Microsoft Azure with built-in high availability, resilience, and security features.
- Intrusion detection and prevention systems (IDS/IPS) are in place.
- Regular vulnerability scans and third-party penetration tests are conducted.

**3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner**

- Daily encrypted backups are performed and stored in geographically redundant storage.
- Disaster recovery and business continuity plans are in place and tested regularly.
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) policies ensure timely restoration of services.

**4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures**

- Security audits and assessments are conducted at least annually.
- Penetration testing by external cybersecurity firms is conducted at least once a year.
- Internal compliance reviews are performed regularly to ensure adherence to policies.

**5. Measures for user identification and authorisation**

- Strong password policies and optional **Multi-Factor Authentication (MFA)** for platform access.
- Single Sign-On (SSO) integration with enterprise identity providers (IdPs) is supported.

- User activity logs and session controls are enforced.

**6. Measures for the protection of data during transmission**

- All data transmitted over public networks is protected using **HTTPS with TLS 1.2+**.

**7. Measures for the protection of data during storage**

- Azure storage is encrypted at rest with AES-256.
- Logical data separation ensures tenant isolation in the multi-tenant architecture.
- Dedicated databases are available for customers requiring strict isolation.

**8. Measures for ensuring physical security of locations at which personal data are processed**

- Physical security is ensured by Microsoft Azure data centers, which are ISO 27001 and SOC 2 certified.
- Data centers are protected with biometric access controls, surveillance, and redundant power and cooling.

**9. Measures for ensuring events logging**

- All administrative and access events are logged and monitored.
- Logs are stored securely and retained according to policy.
- Anomalies and suspicious behavior trigger alerts via the monitoring system.

**10. Measures for ensuring system configuration, including default configuration**

- Baseline system configurations are maintained and regularly reviewed.
- Hardening guidelines are applied based on industry standards (e.g., CIS Benchmarks).
- Secure-by-default configurations are applied during service provisioning.

**11. Measures for internal IT and IT security governance and management**

- A formal information security policy is in place, reviewed annually.
- Access control, change management, and incident response procedures are defined and enforced.
- Staff undergo regular security awareness and data protection training.

**12. Measures for certification/assurance of processes and products**

- ClicData operates within Azure environments that are certified for **ISO 27001, ISO 27018, SOC 1/2/3**, and **GDPR-compliant**.
- Internal processes align with **ISO 27001** best practices.

**13. Measures for ensuring data minimisation**

- Only the minimum required personal data is collected and retained.
- Customers can configure data retention policies and anonymize or pseudonymize datasets.

---

**14. Measures for ensuring data quality**

- Customers are responsible for data quality of their content.
- ClicData provides data validation tools and transformations to assist with maintaining quality.

---

**15. Measures for ensuring limited data retention**

- Data retention policies are configurable by customers.
- Deleted data is removed from production systems within a fixed period, and backups are purged according to policy.

---

**16. Measures for ensuring accountability**

- A Data Protection Officer (DPO) is appointed.
- Data processing records are maintained.
- Data breach response procedures comply with GDPR Article 33 & 34.

---

**17. Measures for allowing data portability and ensuring erasure**

- Customers may export personal data in structured formats (e.g., CSV, Excel, JSON).
- Secure deletion tools are available within the platform to ensure erasure upon request.

---

**18. Measures by sub-processors**

- Sub-processors (e.g., Microsoft Azure, email service providers) are required to meet equivalent technical and organisational security standards.
- Data processing agreements are in place with all sub-processors, ensuring GDPR compliance.
- Sub-processors are regularly reviewed for compliance and data handling practices.