# Data Processing Agreement (DPA) Template

**This Data Processing Agreement ("DPA")** is entered into as of [Insert Date], by and between:

* **Data Controller**: [Insert Name], having its principal place of business at [Insert Address], ("Controller");
* **Data Processor**: [Insert Name], having its principal place of business at [Insert Address], ("Processor").

## 1. Definitions

* **GDPR**: [Regulation (EU) 2016/679](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679) of the European Parliament and the Council on the protection of natural persons concerning the processing of personal data and on the free movement of such data.
* **Personal Data**: Any information relating to an identified or identifiable natural person as defined in [Article 4(1) of the GDPR](https://gdpr-info.eu/art-4-gdpr/).
* **Processing**: Any operation or set of operations performed on Personal Data as defined in [Article 4(2) of the GDPR](https://gdpr-info.eu/art-4-gdpr/).
* **Data Breach**: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
* **Sub-processor**: Any third party the Processor engages to assist in Processing Personal Data.

## 2. Subject Matter and Duration

This DPA governs the Processor’s handling of Personal Data on behalf of the Controller as described in [**Appendix 1: Details of Processing Activities**.](#_fqramykewnr6) The DPA remains effective for the services provided under [Insert Main Agreement Name].

## 3. Roles and Responsibilities

### 3.1 Controller Responsibilities:

* Ensure Personal Data is processed in compliance with GDPR.
* Provide lawful instructions to the Processor.
* Inform the Processor of any changes affecting the processing of Personal Data.

### 3.2 Processor Responsibilities:

* Process Personal Data only on documented instructions from the Controller.
* Implement appropriate technical and organizational measures to protect Personal Data.
* Ensure confidentiality agreements are in place with employees and agents.

## 4. Processing Details

### 4.1 Purpose:

Personal Data will be processed solely for the purposes outlined in [**Appendix 1**](#_fqramykewnr6).

### 4.2 Types of Data and Data Subjects:

Detailed in [**Appendix 1**](#_fqramykewnr6).

### 4.3 Special Categories of Data:

The Processor shall not process sensitive data (e.g., health data) unless explicitly instructed by the Controller.

## 5. Sub-processors

* The Processor shall not engage sub-processors without the Controller’s prior written consent.
* Sub-processors must implement security measures equivalent to those in this DPA.
* The Processor shall maintain a list of sub-processors and notify the Controller of changes at least 30 days in advance.

## 6. Data Subject Rights

The Processor shall assist the Controller in responding to Data Subject requests regarding:

* Access, rectification, and erasure of Personal Data.
* Restriction or objection to processing.
* Data portability.

The Processor shall notify the Controller of requests within [Insert Timeframe].

## 7. Security Measures

The Processor shall implement the following measures to protect Personal Data:

* Encryption during transmission and at rest.
* Role-based access controls.
* Regular penetration testing and vulnerability assessments.
* Incident response plans and regular security audits.
* Staff training on data protection.

Details are provided in [**Appendix 2: Security Measures**](#_y2vaqsmzje3r).

## 8. Data Breach Notification

* The Processor shall notify the Controller of a Data Breach within 72 hours of discovery.
* The notification shall include:
  + Description of the breach.
  + Likely consequences.
  + Measures taken to address the breach.

## 9. Audit Rights

* The Processor shall make available all necessary documentation to demonstrate GDPR compliance.
* The Controller may conduct audits once per year or as required by law, focusing solely on compliance.
* Audits must be conducted during business hours with reasonable notice.

## 10. Return or Deletion of Data

Upon termination of the agreement, the Processor shall:

* Return all Personal Data to the Controller, or
* Delete all Personal Data and certify the deletion unless retention is legally required.

## 11. International Data Transfers

If Personal Data is transferred outside the European Economic Area (EEA):

* Transfers must comply with [GDPR Chapter V](https://gdpr-info.eu/chapter-5/).
* The Processor shall utilize standard contractual clauses or equivalent mechanisms.

## 12. Liability and Indemnification

* Each party shall be liable for breaches of this DPA in accordance with GDPR.
* The Processor’s liability shall be capped at [Insert Amount or Formula], except in cases of gross negligence or willful misconduct.
* The Processor shall indemnify the Controller for damages caused by non-compliance.

## 13. Governing Law

This DPA shall be governed by the laws of [Insert Applicable Jurisdiction], and disputes shall be resolved under [Insert Dispute Resolution Mechanism, e.g., arbitration].

## 14. Miscellaneous

* This DPA forms part of the [Insert Agreement Name] between the parties.
* Amendments must be in writing and signed by both parties.
* If any provision is deemed invalid, the remainder shall remain enforceable.

## 15. Signatures

**Data Controller:**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Data Processor:**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Appendix 1: Details of Processing Activities

| **Activity** | **Data Subjects** | **Data Types** | **Purpose** | **Retention Period** |
| --- | --- | --- | --- | --- |
| [Insert Activity] | [Insert Subjects] | [Insert Data Types] | [Purpose] | [Retention Period] |

## Appendix 2: Security Measures

* **Encryption:** Data encrypted in transit and at rest.
* **Access Control:** Role-based access, multifactor authentication.
* **Incident Management:** Defined response procedures and regular testing.
* **Training:** Annual GDPR training for all staff.
* **Monitoring:** Continuous monitoring for anomalies and threats.