

DATA PROCESSING AGREEMENT

This is a customizable starting template, not a finished legal document. This document type carries significant legal and/or financial consequences and varies substantially by jurisdiction. Having a licensed attorney review it before use is strongly recommended. Replace every [BRACKETED] field with your specifics, delete or adapt any clause that does not fit your arrangement, and have a licensed attorney in the governing jurisdiction review it before you or anyone else signs. CyberSygn is not a law firm and this template is not legal advice.

This Data Processing Agreement (this "DPA") is entered into as of [EFFECTIVE DATE] (the "Effective Date") by and between:

[CONTROLLER LEGAL NAME], a [STATE/COUNTRY] [ENTITY TYPE] with its principal place of business at [CONTROLLER ADDRESS] (the "Controller"); and

[PROCESSOR LEGAL NAME], a [STATE/COUNTRY] [ENTITY TYPE] with its principal place of business at [PROCESSOR ADDRESS] (the "Processor").

Controller and Processor are each a "Party" and together the "Parties."

Recitals. The Parties have entered into, or will enter into, an underlying agreement under which the Processor provides services to the Controller (the "Principal Agreement"). In performing those services, the Processor processes Personal Data on behalf of the Controller. This DPA sets out the data-protection terms that govern that processing and forms part of the Principal Agreement. Where this DPA conflicts with the Principal Agreement on data-protection matters, this DPA controls. In consideration of the mutual promises below, the Parties agree as follows.

1. Definitions and Scope

1.1 Defined terms. "Personal Data," "Processing," "Data Subject," "Controller," "Processor," and "Supervisory Authority" have the meanings given under **Applicable Data Protection Law**. "Applicable Data Protection Law" means the privacy and data-protection laws and regulations that apply to the Processing of Personal Data under this DPA, as identified in **Schedule 1**.

1.2 Roles. With respect to Personal Data processed under this DPA, the Controller is the controller and the Processor is the processor (or, where applicable, the service provider). The Processor processes Personal Data only on behalf of the Controller.

1.3 Subject matter. The subject matter, duration, nature, and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are described in **Schedule 1** (Details of Processing).

1.4 Term. This DPA takes effect on the Effective Date and continues for as long as the Processor processes Personal Data on behalf of the Controller under the Principal Agreement.

2. Processor Obligations

2.1 Documented instructions. The Processor will process Personal Data only on the Controller's documented instructions, including the instructions set out in this DPA and the Principal Agreement, unless required to do otherwise by applicable law, in which case the Processor will inform the Controller before processing (unless that law prohibits such notice).

2.2 Unlawful instructions. The Processor will promptly inform the Controller if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law.

2.3 Purpose limitation. The Processor will not process Personal Data for its own purposes, will not sell Personal Data, and will not retain, use, or disclose Personal Data outside the direct business relationship or as otherwise prohibited by Applicable Data Protection Law.

2.4 Confidentiality. The Processor will ensure that persons authorized to process Personal Data are bound by confidentiality obligations and process Personal Data only as instructed.

3. Security Measures

3.1 Technical and organizational measures. The Processor will implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing. The measures are described in **Schedule 2** (Security Measures).

3.2 Risk-appropriate controls. The measures will include, as appropriate, pseudonymization and encryption, measures to ensure ongoing confidentiality, integrity, availability, and resilience of systems, the ability to restore availability after an incident, and a process for regularly testing and evaluating effectiveness.

3.3 Updates. The Processor may update its security measures from time to time, provided the updated measures do not materially reduce the overall level of protection.

4. Sub-Processing

4.1 Authorization. The Controller **[SELECT ONE: provides general written authorization for the Processor to engage sub-processors, subject to this Section / must give prior written authorization before the Processor engages any sub-processor]**.

4.2 List and notice. The Processor will maintain a current list of sub-processors and will give the Controller prior notice of any intended addition or replacement, allowing the Controller a reasonable period to object on reasonable data-protection grounds.

4.3 Flow-down. The Processor will impose on each sub-processor, by written contract, data-protection obligations no less protective than those in this DPA, and remains liable to the Controller for the acts and omissions of its sub-processors.

5. Data Subject Rights and Assistance

5.1 Assistance with requests. Taking into account the nature of the Processing, the Processor will assist the Controller, by appropriate technical and organizational measures, in responding to requests from Data Subjects to exercise their rights under Applicable Data Protection Law.

5.2 Forwarding requests. If the Processor receives a request from a Data Subject relating to Personal Data processed under this DPA, it will promptly forward the request to the Controller and will not respond directly except on the Controller's instruction or as required by law.

5.3 Compliance assistance. The Processor will provide reasonable assistance to the Controller with data-protection impact assessments and prior consultations with Supervisory Authorities, where required.

6. Personal Data Breach

6.1 Notification. The Processor will notify the Controller without undue delay, and in any event within **[NUMBER, e.g. 48 / 72]** hours, after becoming aware of a Personal Data breach affecting Personal Data processed under this DPA.

6.2 Information. The notification will describe, to the extent known, the nature of the breach, the categories and approximate number of Data Subjects and records affected, the likely consequences, and the measures taken or proposed to address it.

6.3 Cooperation. The Processor will cooperate with the Controller and take reasonable steps to mitigate the effects of the breach and to assist the Controller in meeting any notification obligations.

7. International Transfers

7.1 Transfer restrictions. The Processor will not transfer Personal Data to a country or organization outside the jurisdiction identified in **Schedule 1** unless it has taken the measures necessary to make the transfer lawful under Applicable Data Protection Law.

7.2 Transfer mechanisms. Where required, the Parties will enter into standard contractual clauses or rely on another lawful transfer mechanism, which will form part of this DPA. **[ATTACH OR REFERENCE APPLICABLE CLAUSES.]**

8. Audits and Records

8.1 Records. The Processor will maintain records of its Processing activities sufficient to demonstrate compliance with this DPA and Applicable Data Protection Law.

8.2 Audit rights. The Processor will make available to the Controller information reasonably necessary to demonstrate compliance and will allow for and contribute to audits, including inspections, conducted by the Controller or an auditor it mandates, subject to reasonable notice, confidentiality, and frequency limits set out in this DPA or the Principal Agreement.

8.3 Cost allocation. The Parties will bear the costs of audits as set out in the Principal Agreement or, absent agreement, as required by Applicable Data Protection Law.

9. Return and Deletion

9.1 End of services. On termination or expiry of the Principal Agreement, or on the Controller's earlier written request, the Processor will, at the Controller's choice, return all Personal Data to the Controller and delete existing copies, or delete the Personal Data, unless retention is required by applicable law.

9.2 Certification. On request, the Processor will certify in writing that it has complied with its return and deletion obligations.

10. Liability and General Provisions

10.1 Liability. Each Party's liability under this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement, except where Applicable Data Protection Law provides otherwise.

10.2 Order of precedence. This DPA forms part of and is subject to the Principal Agreement. On data-protection matters, this DPA prevails over any conflicting term of the Principal Agreement.

10.3 Governing law. This DPA is governed by the law specified in the Principal Agreement, except where Applicable Data Protection Law requires the application of a different law.

10.4 **Severability and counterparts.** If any provision is unenforceable, the rest remains in effect. This DPA may be signed in counterparts and by electronic signature, each of which is an original and all of which together form one agreement.

IN WITNESS WHEREOF, the Parties have executed this DPA as of the Effective Date.

CONTROLLER	PROCESSOR
Signature: _____	Signature: _____
Printed name: [NAME]	Printed name: [NAME]
Title: [TITLE]	Title: [TITLE]
Date: _____	Date: _____

Schedule 1 — Details of Processing

- Subject matter and duration: **[DESCRIBE]** - Nature and purpose of Processing: **[DESCRIBE]** - Types of Personal Data: **[e.g. names, contact details, account data]** - Categories of Data Subjects: **[e.g. customers, employees, end users]** - Applicable Data Protection Law: **[IDENTIFY]** - Permitted transfer locations: **[IDENTIFY]**

Schedule 2 — Security Measures

- **[DESCRIBE TECHNICAL AND ORGANIZATIONAL MEASURES — access controls, encryption, logging, backup, personnel training, vendor management, incident response, etc.]**

Template provided by CyberSygn. Not legal advice. CyberSygn is not a law firm. Consult a licensed attorney in your jurisdiction before relying on this document.