

# Data Processing Agreement

Pursuant to Art. 28 GDPR · Template for SMEs · EN

Legally reviewed by a certified Data Protection Officer (CIPP/E) · Provided by ETHYX · Version 1.1 · July 2026

» **HOW TO USE** Use this Data Processing Agreement (DPA) whenever you engage another company to process personal data on your behalf – for example a CRM, email tool, hosting or payroll provider (Art. 28 GDPR requires it). Large providers (Google, Microsoft, AWS) usually supply their own DPA; accept theirs and skip this template. Use this template when YOU are the controller engaging a smaller processor that has none, or when you act AS a processor and need to offer one. Replace every [orange placeholder], complete the three Annexes, delete all guidance boxes, then have both parties sign. Have the final version checked by a qualified Data Protection Officer.

## Parties

This Data Processing Agreement (the “Agreement”) is concluded between:

**[CONTROLLER COMPANY NAME], [address] (the “Controller”)**

and

**[PROCESSOR COMPANY NAME], [address] (the “Processor”)**

(each a “Party”, together the “Parties”).

» **HOW TO USE** The Controller decides why and how data is processed; the Processor only acts on the Controller's instructions. If you are buying a service, you are usually the Controller.

## Preamble

The Parties have entered into a main agreement for the provision of **[describe the main service, e.g. CRM software / payroll services]** (the “Main Agreement”), under which the Processor processes personal data on behalf of the Controller. This Agreement sets out the data-protection obligations under Art. 28 GDPR. In case of conflict regarding data protection, this Agreement prevails over the Main Agreement.

## § 1 Subject matter, nature, purpose and duration

(1) The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are specified in Annex 1.

(2) This Agreement runs for the term of the Main Agreement and ends automatically when the Main Agreement ends, subject to the deletion and return obligations in § 9.

---

## § 2 Scope and instructions

- (1) The Processor shall process personal data only on documented instructions from the Controller, including this Agreement and the Main Agreement, unless required to do otherwise by Union or Member State law; in that case the Processor shall inform the Controller before processing, unless the law prohibits it (Art. 28(3)(a)).
- (2) Instructions may be issued in writing or in a documented electronic form. Verbal instructions shall be confirmed in documented form without delay.
- (3) The Processor shall inform the Controller without delay if it considers that an instruction infringes data-protection law. The Processor may suspend the affected processing until confirmed.

---

## § 3 Obligations of the Processor

The Processor shall, in particular:

- a) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b));
- b) implement and maintain the technical and organisational measures set out in Annex 2 (Art. 32, Art. 28(3)(c));
- c) respect the conditions for engaging sub-processors set out in § 4 (Art. 28(3)(d));
- d) assist the Controller, taking into account the nature of processing, in responding to requests from data subjects exercising their rights under Chapter III GDPR (Art. 28(3)(e), see § 5);
- e) assist the Controller in ensuring compliance with Art. 32–36 GDPR (security, breach notification, data protection impact assessment and prior consultation), taking into account the information available to it (Art. 28(3)(f));
- f) at the choice of the Controller, delete or return all personal data after the end of the provision of services, and delete existing copies unless storage is required by law (Art. 28(3)(g), see § 9);
- g) make available to the Controller all information necessary to demonstrate compliance with Art. 28 and allow for and contribute to audits and inspections (Art. 28(3)(h), see § 7);
- h) designate a contact for data-protection matters: **[name / email]**.
- i) (optional) maintain its own record of processing activities under Art. 30(2) GDPR for the processing carried out on behalf of the Controller, and provide the Controller with the relevant extract on request (mirrors the EU Commission's 2021/915 model clauses).

---

## § 4 Sub-processors

- (1) The Processor shall not engage another processor ("sub-processor") without the Controller's prior specific or general written authorisation. The sub-processors approved at the date of this Agreement are listed in Annex 3.
- (2) Where general authorisation is given, the Processor shall inform the Controller of any intended addition or replacement of sub-processors with at least **[14]** days' notice, giving the Controller the opportunity to object on reasonable data-protection grounds (Art. 28(2)).

(3) The Processor shall impose on each sub-processor the same data-protection obligations as set out in this Agreement by way of a contract, and remains fully liable to the Controller for the sub-processor's performance (Art. 28(4)).

---

## **§ 5 Assistance with data-subject rights**

(1) The Processor shall, by appropriate technical and organisational measures, assist the Controller in fulfilling its obligation to respond to requests to exercise the data subject's rights (access, rectification, erasure, restriction, portability, objection – Art. 15–22 GDPR).

(2) If a data subject contacts the Processor directly, the Processor shall forward the request to the Controller without undue delay and shall not respond itself unless instructed to do so.

---

## **§ 6 Personal data breaches**

(1) The Processor shall notify the Controller without undue delay, and in any event within **[24]** hours, after becoming aware of a personal data breach affecting the Controller's data, to enable the Controller to meet its 72-hour notification duty under Art. 33 GDPR.

(2) The notification shall describe, as far as possible, 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.

---

## **§ 7 Audits and inspections**

(1) The Processor shall make available to the Controller all information necessary to demonstrate compliance with Art. 28 GDPR.

(2) The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by it. Audits shall be announced with reasonable notice (at least **[14]** days), take place during business hours, and not unreasonably disrupt operations. Recognised certifications or audit reports (e.g. ISO 27001, SOC 2) may be submitted to reduce the scope of on-site audits.

---

## **§ 8 Transfers to third countries**

(1) The Processor shall transfer personal data to a third country (outside the EU/EEA) only on the Controller's documented instructions and only where an adequate safeguard under Chapter V GDPR is in place (e.g. an adequacy decision or the EU Standard Contractual Clauses).

(2) Existing third-country transfers and their safeguards are documented in Annex 3.

---

## **§ 9 Deletion and return**

(1) Upon termination of the Main Agreement, the Processor shall, at the choice of the Controller, return or delete all personal data processed on the Controller's behalf, and delete existing copies, unless Union or Member State law requires further storage.

(2) The Processor shall confirm deletion in documented form upon request.

---

## § 10 Liability and term

(1) Liability is governed by Art. 82 GDPR and the Main Agreement. Each Party is liable for damage caused by processing that infringes the GDPR in accordance with Art. 82.

(2) This Agreement may be terminated together with the Main Agreement. The deletion and return obligations under § 9 survive termination.

## § 11 Final provisions

(1) Amendments to this Agreement must be made in documented form. The same applies to any waiver of this requirement.

(2) Should any provision be invalid, the validity of the remaining provisions is unaffected.

(3) This Agreement is governed by the law of **[Germany]**, without prejudice to mandatory provisions of the GDPR. Place of jurisdiction is **[city]**, where legally permissible.

## Signatures

| For the Controller | For the Processor |
|--------------------|-------------------|
| Place, date        | Place, date       |
| Name, position     | Name, position    |
| Signature          | Signature         |

## Annex 1 – Description of the processing

» **HOW TO USE** Complete this annex precisely – it defines exactly what the Processor may do. Vague entries weaken the whole agreement. Keep it consistent with the corresponding entry in your ROPA.

| ITEM                           | DETAILS                                                                      |
|--------------------------------|------------------------------------------------------------------------------|
| Subject matter of processing   | <b>[e.g. provision of CRM software for customer relationship management]</b> |
| Nature and purpose             | <b>[e.g. storage, organisation and retrieval of customer contact data]</b>   |
| Duration                       | <b>[term of the Main Agreement]</b>                                          |
| Categories of data subjects    | <b>[e.g. the Controller's customers, prospects, employees]</b>               |
| Types of personal data         | <b>[e.g. name, business contact details, communication history]</b>          |
| Special-category data (Art. 9) | <b>[none / specify, e.g. health data – if any]</b>                           |
| Frequency of processing        | <b>[continuous / periodic]</b>                                               |

## Annex 2 – Technical and organisational measures (Art. 32)

The Processor implements and maintains the technical and organisational measures (TOMs) required by Art. 32 GDPR. The measures are documented in the Processor's TOM documentation, attached as part of this Annex, covering at least the following areas:

- Physical access control
- Logical access control
- Network and server security
- Encryption (in transit and at rest)
- Pseudonymisation
- Transmission/transfer security
- Input control and data minimisation
- Availability and resilience (backup, recovery)
- Separation control
- Sub-processor management
- Data-protection management and incident response
- Privacy by design and by default

» **HOW TO USE** Attach the completed ETHYX TOM Checklist (Art. 32) here, or reference the Processor's own security documentation (e.g. ISO 27001 certificate, SOC 2 report). The areas above match the sections of the TOM Checklist.

## Annex 3 – Approved sub-processors

| SUB-PROCESSOR              | SERVICE PROVIDED           | LOCATION          | THIRD-COUNTRY SAFEGUARD |
|----------------------------|----------------------------|-------------------|-------------------------|
| [e.g. Amazon Web Services] | [hosting / infrastructure] | [EU region / USA] | [N/A (EU) / SCCs]       |
| [e.g. SendGrid]            | [transactional email]      | [USA]             | [SCCs]                  |
| [ ]                        | [ ]                        | [ ]               | [ ]                     |
| [ ]                        | [ ]                        | [ ]               | [ ]                     |

» **HOW TO USE** List every sub-processor and the safeguard for any outside the EU/EEA. This must match your ROPA and your privacy notice's third-country-transfers section.