



Data Processing Agreement

This Data Processing Agreement supplements the main contract or other agreements existing between the customer and proLogistik that govern the customer's use of proLogistik's products and the associated services (hereinafter: the "main contract").

The parties are the contractor named in the main contract (a company of the proLogistik Group, the data processor; hereinafter the "Contractor") and the customer named in the main contract (the controller; hereinafter the "Client"). Referred to individually or jointly as a "Party" or the "Parties."

1. Subject Matter and Duration of the Assignment

Subject matter

The Contractor processes personal data on behalf of the Client (commissioned processing). This encompasses all activities performed by the Contractor under the respective contractual agreements with the customer (provision of software products, contracts for individual services, and maintenance and support activities) that constitute commissioned processing.

Insofar as other agreements between the Client and the Contractor contain differing arrangements for the protection of personal data, this data processing agreement shall take precedence, unless the Parties expressly agree otherwise (including with regard to backups).

Duration

Unless otherwise agreed, this agreement enters into force upon signature of the main contract and applies for as long as the Contractor processes personal data for the Client.

2. Specification of the Assignment

Nature and purpose of the intended data processing

Personal data is processed exclusively to provide the services agreed in the main contract. In particular, for hosting, support, maintenance and troubleshooting services, access to personal data may be necessary in order to identify and resolve technical problems.

Categories of data subjects

The Contractor processes the following categories of data for the Client: contact data, IP addresses, metadata, analytical data, user settings and preferences (understood here exclusively as personal data).

The data processing concerns the following categories of data subjects: employees, customers and suppliers of the Client.

3. Technical and Organizational Measures

(1) Before processing begins, the Contractor shall document the technical and organizational measures set out and required in advance of the assignment – in particular with regard to the specific performance of the assignment – and provide them to the Client for review. Upon acceptance by the Client, the documented measures become the basis of the assignment. Insofar as the Client's review / audit reveals a need for adjustment, this shall be implemented by mutual agreement.

(2) The Contractor shall establish security in accordance with Art. 28(3)(c) and Art. 32 GDPR, in particular in conjunction with Art. 5(1) and (2) GDPR. Overall, the measures to be taken are measures of data security and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the implementation costs, and the nature, scope and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32(1) GDPR, shall be taken into account. The technical and organizational measures currently in force can be accessed at the following link:

www.proLogistik.com/trustcenter

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative, adequate measures, provided that the security level of the specified measures is not undercut. Material changes shall be documented.

4. Rights of Data Subjects

(1) Within its area of responsibility, and to the extent possible by means of appropriate technical and organizational measures, the Contractor supports the Client in responding to and implementing requests from data subjects regarding their data protection rights. The Contractor may not rectify, erase or restrict the processing of the data processed under the assignment on its own initiative, but only on the documented instruction of the Client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without undue delay.

(2) Insofar as covered by the scope of services, the rights to erasure, to be forgotten, to rectification, to data portability and to access shall be ensured directly by the Contractor on the documented instruction of the Client.

5. Quality Assurance and Other Duties of the Contractor

In addition to complying with the provisions of this assignment, the Contractor has statutory obligations under Art. 28 to 33 GDPR; in this respect it ensures, in particular, compliance with the following requirements:

Data protection officer

Insofar as the Contractor is obliged pursuant to Art. 37 GDPR or § 38 BDSG to appoint a data protection officer, it shall provide the Client with the officer's contact details for the purpose of direct contact. A change of data protection officer shall be communicated to the Client without undue delay.

Contact details of the Contractor's data protection officer: Data Protection Officer of the proLogistik Group, LL.M. Melanie Rumpke (CIPP/E, ISO/IEC 27701 LA), Fallgatter 1, 44369 Dortmund, email: dsb@prologistik.com.

Preservation of confidentiality (Art. 28(3) sent. 2(b), Art. 29, Art. 32(4) GDPR)

When carrying out the work, the Contractor employs only staff who are bound to confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The Contractor, and any person subordinate to the Contractor who has access to personal data, may process such data exclusively in accordance with the Client's instructions – including the powers granted in this agreement – unless they are legally obliged to process it.

Implementation of and compliance with the technical and organizational measures

The implementation of and compliance with all technical and organizational measures required for this assignment pursuant to Art. 28(3) sent. 2(c) and Art. 32 GDPR.

The Contractor is responsible for demonstrating the technical and organizational measures taken to the Client within the scope of its audit powers under Clause 7 of this agreement.

Oversight by the supervisory authority

Upon request, the Client and the Contractor cooperate with the supervisory authority in the performance of their tasks.

The Contractor shall inform the Client without undue delay of any inspection actions and measures by the supervisory authority insofar as they relate to this assignment. This also applies where a competent authority investigates the processing of personal data in connection with the commissioned processing at the Contractor in the context of administrative-offense or criminal proceedings.

Insofar as the Client is itself exposed to an inspection by the supervisory authority, to administrative-offense or criminal proceedings, to a liability claim of a data subject or a third party, or to any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support the Client to the best of its ability.

6. Subprocessing Relationships

(1) Subprocessing relationships within the meaning of this provision are services that relate directly to the provision of the main service. This does not include ancillary services that the Contractor uses – e.g. telecommunications services, postal / transport services, maintenance and user services, or the disposal of data media – as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

Maintenance and inspection services constitute a subprocessing relationship where they are provided for IT systems that are used in direct connection with a service of the Contractor under this agreement.

The Contractor is nevertheless obliged, in order to ensure data protection and data security of the Client's data, to take appropriate and legally compliant contractual arrangements as well as control measures even in the case of outsourced ancillary services.

(2) The Client grants the Contractor general authorization to engage further processors within the meaning of Art. 28 GDPR. The Client can retrieve the further processors currently engaged, on a product-specific basis, at the following link:

www.proLogistik.com/trustcenter

The Contractor informs the Client when a change is intended regarding the engagement or replacement of further processors. The Client may object to such changes, whereby this may not be done without an important data-protection-related reason. The objection to the intended change must be raised in text form within 21 days of the change information being made available, to: dsb@prologistik.com. In the event of an objection, the Contractor may, at its own choice, provide the service without the intended change or – if providing the service without the intended change is unreasonable for the Contractor – cease the service toward the Client within 4 weeks of receipt of the objection and terminate the service agreement without notice and with immediate effect.

(3) The transfer of the Client's personal data to the subprocessor and the subprocessor's first activity are permitted only once all requirements for subprocessing are met.

(4) If the subprocessor provides the agreed service outside the EU / EEA, the Contractor ensures data-protection compliance through appropriate measures. The same applies if service providers within the meaning of Clause 6(1) sentence 2 are to be engaged.

7. Audit Rights of the Client

(1) The Client has the right to carry out reviews in consultation with the Contractor, or to have them carried out by auditors to be designated on a case-by-case basis. It has the right to satisfy itself of the Contractor's compliance with this agreement in the Contractor's business operations by means of spot checks, which must be announced in good time, without disproportionately disrupting the Contractor's business operations.

(2) If the Client commissions a third party to carry out the audit, the Client shall obligate the third party in writing to the Contractor to secrecy and confidentiality, unless the third party is subject to a professional duty of confidentiality. At the Contractor's request, the Client shall present the confidentiality undertaking without undue delay. The Client may not commission a competitor of the Contractor to carry out the audit. The Client documents the audit result and communicates it to the Contractor. The Contractor may request reasonable remuneration for its effort in carrying out the audits.

(3) The Contractor ensures that the Client can satisfy itself of the Contractor's compliance with its obligations under Art. 28 GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to demonstrate the implementation of the technical and organizational measures.

(4) Evidence of such measures, where they do not relate only to the specific assignment, may be provided by:

- a)** compliance with approved codes of conduct pursuant to Art. 40 GDPR;
- b)** certification under an approved certification procedure pursuant to Art. 42 GDPR;
- c)** current attestations, reports or report excerpts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);
- d)** a suitable certification by IT security or data protection audit (e.g. under BSI IT-Grundschutz, ISO 27001, ISO 27701).

8. Notification of Violations by the Contractor

(1) The Contractor supports the Client in complying with the obligations set out in Art. 32 to 36 GDPR concerning the security of the processing of personal data, notification obligations for personal data breaches, data protection impact assessments and prior consultations. This includes, among other things:

- a) ensuring an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible legal infringement due to security vulnerabilities, and that enable the immediate detection of relevant breach events;
- b) the obligation to report personal data breaches to the Client without undue delay;
- c) the obligation to support the Client within the scope of its duty to inform the data subject and, in this context, to provide it with all relevant information without undue delay;
- d) supporting the Client with its data protection impact assessment;
- e) supporting the Client in the context of prior consultations with the supervisory authority.

9. Client's Authority to Issue Instructions

(1) The Contractor processes personal data only on the basis of the Client's documented instructions, unless it is required to process by the law of a Member State or by Union law. In that case, the Contractor informs the Client of these legal requirements, provided that the law in question does not prohibit such notification on grounds of an important public interest. The Client confirms oral instructions without undue delay (at least in text form).

(2) The Contractor shall inform the Client without undue delay if it is of the opinion that an instruction violates data protection provisions. The Contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

10. Deletion and Return of Personal Data

(1) Copies or duplicates of the Client's data are not created without the Client's knowledge. Excepted from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data required to comply with statutory retention obligations.

(2) Upon completion of the contractually agreed work, or earlier upon request by the Client – at the latest upon termination of the service agreement – the Contractor shall hand over to the Client all documents, processing and usage results produced, and data holdings that have come into its possession in connection with the contractual relationship, or destroy them in a data-protection-compliant manner subject to prior consent. The same applies to test and reject material. The deletion record shall be presented upon request.