

Data Processing Agreement

Customer:

Service Provider:

netfiles GmbH
Marktler Straße 2b
84489 Burghausen
DEUTSCHLAND
- Processor -

1. Nature and duration of the contract

A contractual agreement covering the use of netfiles online services is in place between the Controller and the Processor. The nature and scope of the services provided as specified in the netfiles Service Level Agreement (SLA) <https://www.netfiles.de/downloads/SLA-netfiles.pdf> meet the requirements for data processing according to Art. 4 Par. 2 and Art. 28 GDPR.

The duration of this agreement shall correspond with the duration of the primary contract between Controller and Processor. The agreement shall terminate by default at the end of the primary contract. If the Controller enters multiple service contracts with the Processor, this agreement shall be valid for all of them. The Controller may terminate this agreement immediately and without notice if the Processor commits a significant breach against data protection regulations or the clauses of the agreement, without valid reason refuses to execute an order issued by the Controller, or denies the Controller a contractually agreed right. Failure to comply with the obligations arising from this contract and derived from Art. 28 GDPR constitutes a significant breach.

2. Nature, purpose and location of processing

Nature and purpose of the processing of personal data by the Processor are defined in the netfiles Service Description <https://www.netfiles.de/downloads/Service-Description-netfiles.pdf>

The nature of personal data processing according to Art. 4 Par. 2 GDPR includes in particular the storage, adaption, alteration, use, dissemination, disclosure, restriction and the display, querying and deletion of data.

The contractually agreed services are provided exclusively in the territory of the Federal Republic of Germany. Any transfer of services or parts thereof shall require the previous agreement of the Controller and is only permissible if the requirements of Art. 44ff. GDPR are fulfilled (e.g. adequacy decision of the European Commission, equivalent data protection and supervision measures).

3. Types of personal data and categories of data subjects

The Processor stores and processes the following types of personal data according to Art. 4 Par. 1,13,14, 15 GDPR:

- Master data such as name, surname, e-mail address, company, telephone number etc. recorded in the netfiles user administration.
- Any other type of personal data stored by the Controller in netfiles.

The data subjects concerned by the processing (Art. 4 Par. 1 GDPR) are:

- Individuals, whose personal data is transmitted by the Controller to the Processor in the context of contract administration and fulfilment.
- Individuals, whose personal data is stored by the Controller in netfiles.

4. Controller rights, obligations and authorities

The Controller is solely responsible for ensuring the lawfulness of processing according to Art. 6 Par. 1 GDPR and the exercise of the rights of data subjects according to Art. 12 to 22 GDPR. The Processor shall forward any associated enquiry by a data subject to the Controller without undue delay.

Changes to the scope of processing and process amendments shall be agreed jointly between Controller and Processor and documented in writing or an equivalent electronic format. The Controller shall issue all orders and directions in writing or an equivalent electronic format. Verbal directions shall be confirmed in writing or an equivalent electronic format without undue delay.

Prior to commencement of processing and at regular intervals thereafter, the Controller is entitled to verify the Processor's compliance with the obligations from this contract and the agreed Technical And Organisational Measures in line with the provisions of part 5 of this contract.

Unless the Controller provides the Processor with a list of individuals authorised to issue orders and directions, the Processor will accept orders and directions from the following functions:

- authorised signatories for the Controller
- the designated contact person for the data room contract
- the responsible data room administrator
- all other data room administrators

The Controller shall notify the Processor immediately of any errors or irregularities identified within the contract deliverables.

The Controller shall treat as confidential any information, in particular trade secrets and information security measures, disclosed by the Processor in the course of fulfilling the contract. This obligation shall remain in force also after termination of the contract.

5. Obligations of the Processor and individuals authorised to receive orders

The Processor shall process personal data only on the basis of documented instructions from the Controller, unless required otherwise by European Union or member state law (e.g. in the context of investigations by law enforcement or national security authorities). In such cases the Processor shall notify the Controller before processing, unless law prohibits such a notification on grounds of public interest (Art. 28 Par. 3 Pt. 2 GDPR).

The Processor shall not use personal data belonging to the Controller for other purposes. No data copies shall be maintained outside of the scope of contractual agreements and without knowledge of the Controller.

The Processor guarantees compliance with all contractually agreed measures related to the processing of personal data and the strict separation of data belonging to the Controller from other data.

Portable data storage devices belonging to or used for personal data owned by the Controller shall be uniquely labelled and their receipt, use and dispatch documented.

The Processor shall contribute to the extent required in the execution of data subject rights according to Art. 12 to 22 GDPR and in the compilation of processing registers and data protection impact assessments by the Controller (Art. 28 Par. 3 Pt. e, f). The Processor shall provide information requested by the Controller in this context without undue delay.

The Processor shall notify the Controller immediately if he believes that an order issued by the Controller contravenes legal requirements (Art. 28 Par. 3, Pt. 3 GDPR). The Processor may suspend the execution of such an order until it is validated and confirmed by the Controller.

The Processor shall correct, delete or restrict the processing of personal data associated with the contractual relationship if directed to do so by the Controllers, unless this contravenes legitimate interests of the Processor.

The Processor shall disclose or provide information about personal data to data subjects or third parties only if directed by or after having received explicit permission from the Controller.

The Controller is entitled to check by appointment and to the extent required the Processor's compliance with the agreed Technical and Organisational Measures and the obligations from this contract, or to instruct a third party to do so. This includes information about and access to stored data and data processing tools, as well as on-site inspections (Art. 28 Par. 3 Pt. 2 GDPR). The Processor shall contribute to these reviews as required and shall support the Controller in fulfilling the requirements of Art. 32 to 36 GDPR within the scope of the nature of processing conducted and information available to the processor.

The processing of personal data in private homes (remote or home office) shall be permitted only if approved by the Controller. Access for inspection to private homes used for data processing shall be contractually assured. The requirements of Art. 32 GDPR shall be fulfilled.

The Processor confirms that he is aware of all applicable requirements for the processing of personal data according to GDPR and commits to compliance with the following regulations concerning the protection of confidential information: Bank Secrecy (Bankgeheimnis), Telecommunications Secrecy (Fernmeldegeheimnis), Social Data Secrecy (Sozialgeheimnis) and Professional Secrecy (Berufsgeheimnis) according to Par. 203 StGB (Strafgesetzbuch / German Criminal Code).

Within the scope of the Controllers instructions, the Processor shall maintain strict confidentiality and medical secrecy when processing personal data. This obligation shall remain in force also after termination of the contract. The Processor shall instruct every employee processing personal data on all relevant data protection and medical secrecy requirements prior to commencement of the processing. Employees shall be bound by contract to maintain confidentiality and medical secrecy during and after termination of their employment (Art. 28 Par. 3 Pt. 2b and Art. 29 GDPR Par. 209 Art. 4 Pt. 1 StGB). The Processor shall monitor compliance with data protection regulations in the course of operations.

Orders and directions shall be issued in writing, either by mail addressed to the Processor's registered office or by e-mail to sales@netfiles.de. Orders and directions addressed to individual employees will not be accepted. Orders include, but are not restricted to, the termination of data room contracts and the compilation of data room archives by the Processor.

The Processor has appointed a Data Protection Officer, whose contact details are accessible for the Controller on the netfiles web site <https://www.netfiles.de/en/about-us/privacy-policy/>.

6. Disclosure obligations of the Processor

The Processor shall inform the Controller immediately about disruptions and breaches of data protection regulations or contractual requirements, as well as suspicion of data protection breaches or irregularities in the context of the processing. This particularly applies with regards to reporting and notification obligations according to Art. 33, 34 GDPR. The Processor shall support the Controller in meeting the obligations of these requirements (Art. 28 Par. 3 Pt. 2f GDPR) to the extent necessary. The Processor shall issue notifications according to Art. 33, 34 GDPR only following permission from the Controller according to section 4 of this contract.

7. Subcontractor relationships

The Processor shall be entitled to engage another processor (- Subcontractor -) for carrying out specific processing activities on behalf of the Processor. The Processor shall disclose to the Controller the name and business address of and the processing steps outsourced to the Subcontractor. Outsourcing is permitted exclusively to European Union member states, states party to the Agreement on the European Economic Area, and Switzerland. Before engaging a Subcontractor, the Processor shall verify that the Subcontractor has implemented appropriate Technical and Organisational Measures according to Art. 32 GDPR. Verification records shall be provided to the Controller on request.

The Processor shall ensure that the contractual agreement with the Subcontractor covers all contractual agreements between Controller and Processor concerning data processing. The contract between Processor and Subcontractor shall clearly identify which responsibilities are assigned to either party. This equally applies to subcontractors engaged by the Subcontractor.

All contractual agreements between Processor and Subcontractor shall be documented in writing or an equivalent electronic format (Art. 28 Par. 4, 9 GDPR). Transfer of personal data to the Subcontractor shall only commence if the Subcontractor has met the requirements of Art. 29 and Art. 32, Par. 4 GDPR. The Processor is liable towards the Controller for ensuring that the Subcontractor meets all contractually agreed data protection requirements.

At the time this contract becomes effective, the Processor engages the subcontractors listed under <https://www.netfiles.de/downloads/Subcontractor-Register-netfiles.pdf>. The Controller hereby approves the engagement of the listed entities.

The Processor shall notify the Controller if he engages new or substitutes existing subcontractors. The Controller has the right to object to these changes (Art. 28, Par. 2 Pt. 2 GDPR).

Agreements for ancillary services such as telecommunication services, maintenance, cleaning services, auditing or disposal of data carriers are not considered subcontracting agreements in the context of this contract. The Processor shall nevertheless ensure that all ancillary agreements include adequate and legally compliant data protection provisions and shall put into place control measures accordingly.

8. Technical and Organisational Measures

The Processor shall ensure a level of security that adequately reflects the risk for the rights and freedoms of data subjects by implementing appropriate Technical and Organisational Measures. These measures shall take into account the provisions of Art. 32 Par. 1 GDPR, in particular confidentiality, integrity and availability of data processing systems and services and their suitability with regards to the intended nature and purpose of the processing. The measures shall include long-term risk management procedures compliant with Art 32 Par. 2 GDPR.

The netfiles Technical and Organisational Measures <https://www.netfiles.de/downloads/Technical-and-organisational-measures-netfiles.pdf> provide a detailed description of the measures taken by the Processor, considering the technical state-of-the-art, data processing systems and procedures and the likelihood and severity of risks.

The Processor confirms as binding the procedures defined for the regular control and evaluation of the effectiveness of the measures with regards to compliant processing of data.

The Processor operates an Information Security Management System certified according to ISO27001:2013. The Processor shall maintain the certification in line with the requirements of the certification body. The maintenance audits shall include an evaluation of the Technical and Organisational Measures according to Art. 32 Par. 1d. Audit results and full audit reports shall be disclosed to the Controller upon request.

Security-relevant decisions with a major impact on data processing procedures and measures shall be aligned between the Processor and the Controller. The Controller shall immediately notify the Processor if any measures taken do not meet the Controller's requirements.

The Technical and Organisational Measures may be amended during the contract duration to reflect technical or organisational developments. Any amendments shall as a minimum maintain the standards defined in this agreement.

Significant changes to the Technical and Organisational Measures shall be aligned between Processor and Controller and documented in writing or an equivalent electronic format. Documentation of this nature shall be retained for the duration of the contract.

9. Obligations of the Processor after contract termination

Upon termination of the contract the Processor shall securely delete or destroy all data, documentation and output associated with the processing of personal data (Art. 28 Par. 3 Pt. 2g GDPR). The Processor shall confirm the date of deletion or destruction to the Controller in writing or an equivalent electronic format.

The Processor shall provide a copy of all data to the Controller on request and at the Controller's expense.

10. Concluding provisions

This agreement is subject to German Federal Legislation. Place of fulfilment and sole court of jurisdiction is Burghausen, Germany. If this contracts contains a regulatory gap, or if a clause of this contract is fully or partly ineffective, the remainder of the contract shall remain unaffected. To close the regulatory gap or replace the ineffective clause a regulation shall apply which is effective, proportional and resembles the purpose of the ineffective or missing regulation. Changes to this contract shall only be valid in written form.