

Data Processing Agreement

Status 01 August 2023

fino data services GmbH
Universitätsplatz 12, 34127 Kassel

Contracting parties are fino data services GmbH (hereinafter referred to as processor or fino) Universitätsplatz 12, 34127 Kassel and the customer (hereinafter referred to as controller or customer).

– jointly referred to as “Parties” -.

1. Processing Contract

1. fino processes personal data on behalf of the customer (commissioned processing). This includes all activities performed by fino in accordance with the service descriptions and the respective contractual agreements with the customer (terms and conditions of fino, orders for standard products and contracts for individual services) and which constitute commissioned processing. This shall also apply if the service descriptions and the respective contractual agreements do not explicitly refer to this data processing agreement.
2. In all other respects, the provisions of the terms and conditions of the processor shall apply subordinately, which can be viewed on the Internet via the following link: <https://www.getmyinvoices.com/en/terms/>

2. Nature and purpose of the processing

1. The type of processing includes all types of processing within the meaning of the GDPR.
2. The purposes of the processing are all necessary for the provision of the contractually agreed service.

3. Type of personal data and categories of data subjects

1. Type of Personal Data means all types of Personal Data that the Processor processes on behalf of the Controller.
2. As a rule, the following types/categories of data are used:
 1. Company master data
 2. Account turnover data: optional at the customer's request
 3. Communication data (telephone, e-mail, ...)
 4. Contract master data (contractual relationship)
 5. Billing data (IBAN, credit card)
3. Categories of data subjects are in particular
 1. customers

2. Employees of the controller (if created as users by the controller)
3. Contractual partners of the controller

4. Controller's Obligations and Rights

1. The following obligations particularly reside with the Controller:
 1. evaluate the admissibility of the data processing and safeguard the rights of the affected persons;
 2. immediately inform the Processor in case the Controller notices errors or irregularities during the examination of the order results;
 3. treat all knowledge gained about the Processor's business secrets and data protection measures in the course of the contract relationship confidentially.
 4. The Controller shall inform the Processor in a timely manner of any claims by Data Subjects, such as rectification or erasure of the Personal Data or restriction of the Processing, related to the contracted performance, unless this proves impossible or involves a disproportionate effort.
2. The Controller is entitled to the following rights:
 1. Supervision rights:
 1. The Controller has the right to carry out inspections after consultation with the Processor, or to individually appoint an inspector to do so. The Controller is entitled to reassure himself of the Processor's adherence to this agreement by way of spot checks in the Processor's place of business, which as a rule have to be announced in a timely manner.
 2. The Processor ascertains that the Controller is able to reassure himself of the Processor's compliance with his obligations according to Art. 28 GDPR. The Processor is obligated to provide the Controller with any information required in relation to the observance of his order control obligation when requested, and to make the corresponding verifications available.
 3. If requested by the Controller, the Processor supplies verification relating to the implementation of technological and organisational measures in accordance with Art. 32 GDPR. In this case, verification of the implementation of such measures, which do not exclusively concern the specific order, may be presented in the form of a current attestation, reports or report excerpts from independent entities (e.g., accountant, auditor, data protection officer, IT security department, data protection auditor, quality auditor), or a suitable certificate from an IT security- or data protection auditor (e.g., certificate in accordance with the BSI Standards).
 4. Insofar external costs arise from enabling inspections beyond the outlined, the Processor may transfer those costs to the Controller. Before any such costs arise, both parties will communicate in order to keep those as low as possible, and adapt audit activities, if required.

5. Should the need arise on the part of the Controller to implement further inspections of the Processor, exceeding the degree to be met under the set regulations, the Controller will carry all costs and expenses arising to the Processor in relation to the execution of the Controller's rights to disclosure, insight, access, entry, instruction and inspection, insofar those costs exceed one man-day per year.
3. Right to instruction
The data shall be handled exclusively within the framework of the agreements made and in accordance with the instructions of the controller. Within the scope of the order description agreed in this agreement, the controller reserves a comprehensive right to issue instructions on the type, scope and procedure of data processing, which it may specify by means of individual instructions. Changes to the object of processing and procedural changes must be jointly agreed and documented. The Processor may only provide information to third parties or the Data Subject with the prior written consent of the Controller. The Controller shall immediately confirm verbal instructions in writing or by e-mail (in text form).

5. Processor's Obligations

1. Technological and organisational measures
 1. Regarding the handling of personal data, both the Controller and the Processor must take suitable technological and organisational measures (hereinafter: TOM) to meet the requirements according to Art. 28 Para. 3 lit. c, 32 GDPR, particularly in relation to Art. 5 Para. 1, Para. 2 GDPR.
 2. Any measures not specific to this order are described at <https://getmyinvoices.com/en/tom> and are an integral part of this data processing agreement.
 3. The Processor must document the implementation of the technological and organisational measures, which have been described before commencement of the processing, especially in regard to the specific order execution, and must submit it to the Controller for inspection. Insofar the inspection / an audit through the Controller results in a need for adaption, this has to be implemented consensually.
 4. Insofar any order-specific measures in consideration of the Controller's specific requirements have to be agreed upon, these will be set down in a separate appendix to the respective contract.
 5. The technological and organisational measures are subject to technological progress and further development. In this respect, the Processor is permitted to implement alternative, adequate measures. Those must not fall short of the level of security of the determined measures. Significant modifications must be documented.
2. Infringements to be communicated
 1. The Processor shall support the Controller in the event of personal data breaches pursuant to Art. 33 and 34 GDPR. This includes, among other things.

1. the guarantee of an appropriate level of protection through technological and organisational measures under consideration of the circumstances and purpose of the processing, as well as the severity of a possible infringement of rights caused by security gaps; and the enabling of immediate determination of relevant infringement incidents
 2. the obligation to report the violation of personal data to the Controller without delay
 3. taking all necessary measures to mitigate a Personal Data Breach and notifying the Controller thereof
 4. assisting the Controller in taking action in the event of a Personal Data Breach.
2. The Processor may claim compensation for support services that are not contained in the service description, or that are not due to any misconduct on the side of the Processor.
 3. The Processor will notify the Controller immediately if, in the Processor's view, an issued instruction is in breach of any legal provisions. The Processor is entitled to suspend the execution of the respective instruction until such a time when it has been confirmed or altered by the Controller.
3. Correction, blocking and deletion of data
 1. The Processor must only correct, delete or block any data processed in the course of the order following instruction by the Controller. Should an affected person approach the Processor directly for the purpose of correcting or deleting his data, the Processor will forward this request to the Controller without delay.
 2. Following completion of the contracted work, or earlier if requested by the Controller – latest on termination of the service agreement –, the Processor must deliver all documents that have come into his possession, all processing- and usage results created, as well as all data pools in connection with the contractual basis, or destroy the above, with prior agreement and in compliance with data protection regulations. The same applies to test- and scrap material. The deletion protocol must be presented if so requested.
 3. Documentation serving as evidence for lawful data processing as ordered must be preserved by the Processor beyond the contract termination in compliance with the relevant retention periods. For his relief, he may deliver those at the time of contract termination to the Controller.
 4. Processing, labelling, separation and copying of data
 1. The Processor exclusively processes personal data within the framework of the agreement and on the Controller's instructions. He will not use the data provided for data processing for any other purposes. No copies or duplicates will be created without the Controller's knowledge.
 2. The Processor ensures the contractual execution of all agreed measures throughout the processing of personal data as ordered. He ensures that any data to be processed will be strictly separated from other data pools.

5. Data secrecy

1. The Processor is obligated to maintain data secrecy throughout the contractual processing of the Controller's personal data, as well as that of his customers. He is obligated to observe the same secrecy protection regulations that the Controller is subject to. These obligations will continue beyond the contract termination.
2. The Processor confirms that the pertinent data protection regulations are known to him. The Processor ascertains that all members of staff employed for the execution of the order are familiarized with the significant data protection regulations. The Processor supervises the observance of all data protection regulations.
3. The Processor may provide information to third parties or affected persons only after previous written consent by the Controller. The transfer of data to third parties on the instructions of the controller is only permitted insofar as it is covered by the consent of the data subject and the controller has ensured compliance with the obligations under Article 32 GDPR by the third party and has demonstrated this to the processor or there is a legal obligation for the processor to hand over the data processed on behalf of the controller (e.g. in the context of a seizure by state authorities).

6. Other obligations of the Processor

1. The Processor must inform the Controller without delay about any monitoring activities and measures taken by the supervisory authority, insofar those regard the contract. This also applies if a relevant authority investigates the Processor.
2. The Processor must regularly execute order controls by way of inspection with regard to the contract execution or fulfilment, especially with a view to the observance of regulations and, if required, adjustments of regulations and measures taken to execute the order.
3. Insofar the Controller himself is subject to an inspection by the supervisory authority, to a non-compliance- or criminal procedure, to the liability claim of an affected person or third party, or to a different claim in connection with the order processing executed by the Processor, the Processor must support him to the best of his ability.
4. The Processor shall have a duty to notify the Controller in relation to the transfer of Personal Data to a third country or an international organization.
5. The Processor shall assist the Controller in complying with the personal data security obligations, data breach notification obligations, data protection impact assessments and prior consultations referred to in Articles 32 to 36 of the GDPR.
6. The Processor shall have the obligation to provide the Controller with all relevant information without undue delay in order to adequately assist the Controller, in particular in the context of
 1. the data protection impact assessment of the controller

2. prior consultations with the supervisory authority by the controller
7. The Processor shall support the Controller in its obligation to respond to requests for the exercise of the data subject's rights referred to in Chapter III of the GDPR with appropriate technical and organizational measures, where possible. The Processor may request reasonable remuneration from the Customer for this service.
8. The Processor shall keep a register pursuant to Article 30 (2) to (5) of the GDPR of all processing operations transferred by the Controller.

6. Subcontract Relations

1. Main- and supplementary services:
 1. Subcontract relations in accordance with this regulation are understood to be any such services directly referring to the delivery of the main service.
 2. Not part of the main service are supplementary services used by the Processor as, e.g., telecommunication services, other infrastructure service providers, postal or courier services, transport services, security and cleaning services, as well as other measures taken to ensure the data processing system's confidentiality, availability, integrity and capacity of the hard- and software. This also applies to purely technical maintenance that does not qualify as Processor or an application of Art. 28 GDPR.
 3. If the contractual object of the (remote) maintenance is the handling of not anonymized or pseudonymized, that is, directly recognizable personal data, especially IBAN, BIC, first and last name, and/or structured data bases with personal data, this is considered order processing in accordance with Art. 28 GDPR.
 4. To ensure the data protection and data security of the Controller, even in the case of outsourced supplementary services, the Processor is obligated to make appropriate and legally compliant contractual agreements as well as implement control activities.
2. The Processor may use third parties (subprocessors) to provide the contractual services. The Controller grants the Processor general authorization to use further Processors within the meaning of Art. 28 GDPR.
3. The subprocessors currently in use can be found at <https://getmyinvoices.com/en/subprocessors/>.
4. The Processor shall inform the Controller if it intends to make a change regarding the involvement or replacement of additional Processors. The Controller may object to such changes.
5. The objection to the intended change shall be raised with the Processor within 4 weeks after receipt of the information about the change. In the event of an objection, the Processor may, at its own discretion, provide the service without the intended change or – if the provision of the service without the intended change is not reasonable for the Processor – terminate the service affected by the change towards the Controller within 4 weeks after receipt of the objection.

6. If the Processor places orders with further Processors, it shall transfer its data protection obligations under this Agreement to the further Processor.

7. Contract Duration

1. The order duration (term) as well as the conditions for its termination shall be determined by the respective superordinate contract.
2. The Controller can terminate the contract at any time, without adhering to a notice period, if a serious infringement of the regulations set out in this contract occurs on the side of the Processor, if the Processor is unable or unwilling to execute an instruction made by the Controller, or if the Processor denies access to the Controller contrary to contractual agreements.

8. Liability

1. The Controller and the Processor are liable to affected persons in accordance with the regulations set out in Art. 82 GDPR.
2. If an affected person claims damages against a party because of infringements of data protection regulations, the respective party must inform the other party about the matter without delay.
3. If the claims of affected persons, whose data are being processed, are asserted against the Controller because of unlawful or incorrect data processing, the Processor must support the Controller during the investigation and the defence against the claims.
4. Should the Controller acknowledge any possible claims without the Processor's permission, he will be excluded from recourse to the Processor.

9. Miscellaneous

1. Choice of law, place of performance and place of jurisdiction shall be governed by the GTC for the use of GetMyInvoices.
2. If individual provisions of this agreement prove to be invalid, this shall not affect the validity of the remaining provisions. The invalid provision shall be replaced by such a provision that the parties would have made if they had thought about the invalidity of the respective point when concluding the agreement. Insofar as this agreement contains an unintentional loophole, this shall be replaced by such a provision as the parties would have made had they thought of the need for regulation of the respective point when concluding the agreement.