Commissioned data processing agreement according to Art. 28 GDPR

Status: 30.10.2023

Between

.....

- Person responsible - hereinafter referred to as the Client -

and

Formtastic GmbH
Amalienstr. 77
80799 Munich
Germany

.....

- Processor - hereinafter referred to as Contractor -

This agreement is written in German and English. In case of discrepancies between the German and the English version of this document, the German version shall prevail. The English text is only a non-binding convenience translation.

1. Subject matter and duration of the contract

(1) The subject of the data handling contract is the performance of the following tasks by the Contractor: Provision of the software-as-a-service system (SaaS) "Formtastic".

(2) The contract is concluded electronically during registration and is valid without signature. It is concluded for an indefinite period and can be terminated by either party with 4 weeks' notice to the end of the month. The possibility of termination without notice remains unaffected.

(3) The contract shall apply, without prejudice to the preceding paragraph, for as long as the Contractor processes personal data of the Client (including backups).

(4) Insofar as other agreements between the Client and the Contractor result in other arrangements for the protection of personal data, this contract for commissioned processing shall take precedence, unless the parties expressly agree otherwise.

2. Specification of the content of the contract

(1) Type and purpose of the intended processing of data

Detailed description of the subject matter of the contract with regard to the type and purpose of the Contractor's tasks:

- The Contractor provides the Client with the SaaS system Formtastic

- The Contractor can map personalised processes with the system and process his own data in this context. It is up to the Client to decide which data it processes.

(2) Type of data

The following types/categories of data are the subject of the processing of personal data (list/description of data categories)

- Form input data
- Personal master data
- Communication data (e-mail)
- Contract master data (contractual relationship)
- Customer history
- Contract billing and payment data
- Planning and control data
- Information (from third parties, e.g. credit agencies or public directories)

(2) Categories of persons concerned

The categories of data subjects affected by the processing include:

- Customers

3. Technical and organisational measures

(1) The Contractor shall take all necessary technical and organisational measures in its area of responsibility in accordance with Art. 32 GDPR to protect personal data and shall provide the Client with the documentation for review [Annex 2 TOM]. If accepted by the Client, the documented measures shall become the basis of the contract.

(2) Insofar as the review/audit of the Client reveals a need for adjustment, this shall be implemented by mutual agreement.

(3) The agreed technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor shall be permitted to implement alternative adequate measures in the future. In doing so, the security level of the specified measures may not be undercut. The Client shall be informed immediately of any significant changes which are to be documented by the Contractor.

4. Rights of persons concerned

(1) The Contractor shall support the principal within his area of responsibility and as far as possible by means of suitable technical and organisational measures in responding to and implementing requests from data subjects regarding their data protection rights. The Contractor may not inform, port, correct, delete or restrict the processing of data processed on behalf of the Client on its own authority, but

only in accordance with the Client's documented instructions. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

(2) Insofar as included in the scope of services, the rights to information, correction, restriction of processing, deletion and data portability shall be ensured directly by the Contractor in accordance with documented instructions from the Client.

5. Quality assurance and other obligations of the Contractor

(1) In addition to compliance with the provisions of this Agreement, the Contractor shall have its own statutory obligations pursuant to the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

a) Maintaining confidentiality in accordance with Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. When carrying out the work, the Contractor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarised with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who legitimately has access to personal data may process this data exclusively in accordance with the Client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.

b) The contracting authority and the Contractor shall cooperate with the supervisory authority in the performance of its duties upon request.

c) The immediate information of the Client about control actions and measures of the supervisory authority, insofar as they relate to this contract. This shall also apply insofar as a competent authority investigates in the context of administrative offence or criminal proceedings with regard to the processing of personal data during commissioned processing at the Contractor.

d) Insofar as the Client, for its part, is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party, another claim or a request for information in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.

e) The Contractor shall regularly monitor the internal processes as well as the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

f) Verifiability of the technical and organisational measures taken vis-à-vis the Client within the scope of its control powers pursuant to Clause 8 of this Agreement.

g) The Contractor shall immediately report breaches of the protection of personal data to the Client in such a way that the Client can fulfil its legal obligations, in particular pursuant to Art. 33, 34 of the GDPR. The Contractor shall prepare documentation of the entire process and make it available to the Client for further measures.

h) The Contractor shall support the Client in its area of responsibility and as far as possible within the scope of existing information obligations vis-à-vis supervisory authorities and data subjects and shall provide it with all relevant information in this context without delay.

i) Insofar as the Client is obliged to carry out a data protection impact assessment, the Contractor shall support the Client taking into account the type of processing and the information available to it. The same applies to any existing obligation to consult the competent data protection supervisory authority.

(2) This contract does not release the Contractor from compliance with other requirements of the GDPR.

(3) The Contractor is not obliged to appoint a data protection officer. Enquiries on the subject of data protection can be sent to datenschutz@formtastic.de.

6. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this regulation shall be understood to be those services which directly relate to the provision of the main service. This does not include ancillary services used by the Contractor, e.g. telecommunications services, postal/transport services, cleaning services or guarding services. Maintenance and testing services shall constitute a subcontracting relationship if they are provided for IT systems which are provided in connection with a service of the Contractor under this contract. However, the Contractor shall be obliged to enter into appropriate and legally compliant contractual agreements and to take control measures to ensure data protection and data security of the Client's data also in the case of outsourced ancillary services.

(2) The Client consents to the commissioning of the subcontractors specified in Annex 1 subject to the condition of a contractual agreement with the subcontractor in accordance with Article 28 (2-4) of the GDPR.

The Contractor may only commission further processors with the prior express written or documented consent of the Client.

The contractual agreement shall be presented to the Client at the Client's request, with the exception of business clauses not related to data protection law.

The outsourcing to subcontractors or the change of subcontractors existing in accordance with Annex 1 are permissible insofar as:

- the Contractor gives the Client prior written or textual notice of such outsourcing to subcontractors within a reasonable time, which shall not be less than 14 days; and
- the Client does not object to the planned outsourcing in writing or in text form to the Contractor by the time the data is handed over, and
- a contractual agreement in accordance with Article 28 (2-4) of the GDPR is used as a basis.

(3) The transfer of the Client's personal data to the subcontractor and the subcontractor's initial activity shall only be permitted once all requirements for subcontracting have been met. Compliance with and implementation of the technical and organisational measures at the subcontractor shall be checked by the Contractor in advance of the processing of personal data, taking into account the risk at the subcontractor, and then regularly. The Contractor shall make the control results available to the Client upon request. The Contractor shall also ensure that the Client can exercise its rights under this Agreement (in particular its control rights) directly against the subcontractors.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of paragraph 1 sentence 2 are to be used.

(5) Further outsourcing by the subcontractor requires the express consent of the main Contractor (at least in text form).

All contractual provisions in the contractual chain shall also be imposed on the further subcontractor.

7. International data transfers

(1) Any transfer of personal data to a third country or to an international organisation shall require documented instructions from the principal and shall be subject to compliance with the requirements for the transfer of personal data to third countries under Chapter V of the GDPR.

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area.

(2) Insofar as the Client instructs a data transfer to third parties in a third country, the Client shall be responsible for compliance with Chapter V of the GDPR.

8. Control rights of the principal

(1) The Client shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations during normal business hours by means of spot checks, which must generally be notified in good time.

(2) The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations under Article 28 of the GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

(3) Evidence of the technical-organisational measures for compliance with the specific requirements of data protection in general as well as those relating to the contract may be provided by compliance with approved codes of conduct pursuant to Art. 40 of the GDPR.

9. Authority of the principal to issue instructions

(1) The Contractor shall process personal data only on the basis of documented instructions from the Client, unless he is obliged to process them under the law of the Member State or under Union law. The Client shall confirm verbal instructions without delay (at least in text form). The Client's initial instructions shall be determined by this contract.

(2) The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Client.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be made without the knowledge of the Client. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data required with regard to compliance with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Client - but at the latest upon termination of the service agreement - the Contractor shall hand over to the Client or, after prior consent, destroy in accordance with data protection law all documents, processing and utilisation results produced and data files connected with the contractual relationship that have come into its possession. The same shall apply to test and reject material. The protocol of the deletion shall be submitted upon request.

Annex 1 - Approved subcontracting relationships

Company SubContractor	Address/Country	Service
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Germany T: +49 98315050 info@hetzner.com	Data center (server) in Germany
Payment processing and invoicing in the paid tariffs		
Billwerk+ Germany GmbH	Mainzer Landstraße 51 60329 Frankfurt am Main Germany T: +49 69348779920 contact@billwerk.plus	Payment processing and invoicing
Billwerk+ Denmark A/S	Pilestræde 28A 1112 København Denmark T: +45 89878581 ree-support@billwerk.com	Payment processing and invoicing
PPRO Financial Ltd	48 Chancery Lane WC2A 1JF London United Kingdom T: +44 2030029170 info@ppro.com	Payment processing with SEPA direct debit
PPRO Payment Services S.A.	48 Rue de Bragance 1255 Luxembourg Luxembourg info@ppro.com	Payment processing with SEPA direct debit
Rapyd Europe hf	Dalshraun 3 220 Hafnarfjordur Iceland hallo@rapyd.net	Payment processing with credit card
Newsletter service (can be cancelled at any time)		
Rocket Science Group, LLC (Mailchimp)	Rocket Science Group, LLC, 675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308 USA personaldatarequests@mailchimp.com	Newsletter service

Annex 2 - Technical and organisational measures (TOM)

1. Confidentiality (Art. 32(1)(b) GDPR)

Access

Measures implemented to prevent unauthorised persons from entering the Contractor's business premises where personal data is used.
Electronic access control
Instruction and documentation for issuing access authorisations
Accompaniment of visitors' accesses by own employees

Access control

Measures that prevent data processing systems from being used by unauthorised persons.
Password protection of computer workstations
Functional assignment of user authorisations
Use of individual passwords
Automatic blocking of user accounts after multiple incorrect password entries
Automatic password-secured locking of the screen after inactivity (screen saver)
Password policy with minimum requirements for password complexity: at least 8 digits / upper and lower case, special characters, number (of which at least 3 criteria)
Process for assigning rights when new employees join the company
Process for disenfranchisement in the event of employee resignation
Obligation of confidentiality

Access control

Measures to ensure that those authorised to use a data processing system can only access the information subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.
Use of user-related and individualised credentials
Authorisation concept at application level with differentiated authorisation levels (roles)
Logging of file accesses and file deletions

Separation control

Measures to ensure that personal data collected for different purposes are processed separately

User profiles / separation of user accounts
Separation of development, test and productive system
Separation of functions via roles

Pseudonymisation

(Art. 32 (1)(a) GDPR; Art. 25(1) GDPR) **Measures to process personal data in such a way that the data can no longer be attributed to a specific data subject without obtaining additional information.**
No data is pseudonymised.

2. Integrity (Art. 32(1)(b) GDPR)

Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or during their transport or storage on data media, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.
Data exchange via https connection (SSL)

Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into, modified or removed from data processing systems.
Definition of user authorisations, differentiated user authorisations
Logging of entries/deletions, access logs of the servers and systems
Commitment to data secrecy

3. Availability and resilience (Art. 32(1)(b) GDPR)

Availability control

Measures to ensure that personal data is protected against accidental destruction or loss. These measures shall be designed to ensure continued availability.
Daily execution of automated data backups and backups
Monitoring of system availability

Resilience and fail-safe control

Measures to ensure that systems can cope with risk-related changes and have a tolerance and compensatory capacity for disruptions.
Backup concept
Recovery tests
Limitation of authorisations to necessity (need-to-know)

4. procedures for periodic review, assessment and evaluation (Art. 32(1)(d) of the GDPR; Art. 25(1) of the GDPR)

Control procedures

Measures for documented arrangements so that the state of information security is regularly reviewed and updated
Internal procedure directories are updated at least annually.
Notification of new/changed data processing procedures to the IT Security Officer
Safety measures taken are subject to regular internal control
In the event of a negative outcome of the aforementioned review, the security measures are adapted, renewed and implemented on a risk-related basis

Order control

Measures to ensure that personal data are only processed in accordance with the instructions of the controller.
Contract design according to legal requirements (Art. 28 DSGVO)
Central registration of existing service providers (uniform contract management)
Review of the data security concept at the Contractor's premises
Review of existing IT security certificates of the Contractors