Sample

We provide the following content in English for better accessibility. Please note that only the German text is binding.

Contract of Order Processing acc. to Art. 28 of the EU GDPR

Agreement

Between

D010XXXX
Sample Company

– Responsible party – hereinafter "Customer" –

and

PIN AG, Alt-Moabit 91, 10559 Berlin, Germany
– Order processor – hereinafter "Service Provider" –

1. Scope and duration of order

(1) Scope
The Customer is required to submit datasets electronically to the Service Provider via the PIN eBrief portal for the creation of letters.

(2) Duration
The duration of this order (*Laufzeit*) refers to the timeframe in which the service is to be completed.

2. Specification of the order content

(1) Type and purpose of the designated processing of data
The data item provided by the Customer is prepared for printing and then sent to the printing service provider. It is subsequently printed by the printing service provider. The completed letters are then placed in envelopes and physically delivered by the Service Provider.

The purpose is the physical delivery of the electronically provided data item.

The provision of the contractually agreed data processing takes place exclusively in a Member State of the European Union or in another state party to the Agreement on the European Economic Area (EEA).

Sample

(2) Type of data

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

- Standard personal data (address, access data)
- Communication data (email)
- Contractual invoicing and payment data
- Planning and steering data
- Content of the data provided (documents)

(3) Categories of data subjects

The categories of the data subjects affected by processing encompass:

- Customer data of the Customer

3. Technical and organisational measures

(1) The Service Provider shall establish their internal organisational system in accordance with the order, ensuring compliance with the applicable data privacy requirements.

(2) It is the responsibility of the Customer is to establish security in accordance with Art. 28, para. 3c and Art. 32 of the GDPR, in particular in conjunction with Art. 5, para. 1 and 2 of the GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The technology`s currentness, the implementation costs, and the nature, scope and purposes of the processing must also be considered, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, as defined in Art. 32, para. 1 of the GDPR, as outlined in **Annex 1**, must be given due consideration.

(3) The technical and organisational measures are subject to technical progress and further development. In this regard, the Service Provider is authorized to implement alternative adequate measures. However, it is important to note that the security level of the specified measures cannot be compromised. Significant changes must be properly documented.

4. Correction, restriction and deletion of data

(1) The Service Provider is obliged to comply with the instructions set out by the Customer in relation to the processing of the data provided to them. In the event that a data subject contacts the Service Provider directly regarding this matter, the Service Provider shall promptly forward this request to the Customer.

(2) If included in the scope of services, the erasure concept, right to be forgotten, rectification, data portability and information are to be ensured directly by the Service Provider in accordance with the documented instructions of the Customer.

5. Quality assurance and other obligations of the Service Provider

Sample

In addition to complying with the provisions of this Agreement, the Service Provider is bound by statutory obligations under Art. 28 to 33 of the GDPR; in this respect, the Service Provider is committed to complying with the following requirements in particular:

a) The appointment of a Data Protection Officer is formalised in writing, with the understanding that their duties are to be performed in accordance with Art. 38 and Art. 39 of the GDPR and whose contact details are communicated to the Customer for the purpose of direct contact. The Customer must be informed immediately of any change of Data Protection Officer.

b) Maintaining confidentiality in accordance with Art. 28, para. 3, sentence 2b; Art. 29; and Art. 32, para. 4 of the GDPR. When carrying out the work, the Service Provider is to only use employees who have obliged to maintain confidentiality and who have previously been familiarised with the relevant provisions of data privacy, including the special legal requirements of postal law. The Service Provider, along with any person under their command who has access to personal data, may process this data exclusively in accordance with the Customer`s instructions, including the authorisations granted in this Agreement, unless they are legally obliged to perform processing.

c) The implementation and maintenance of all technical and organisation measures required for this order, in accordance with Art. 28, para. 3, sentence 2C and Art. 31 of the GDPR (**Annex 1**).

d) The Customer and the Service Provider are to cooperate with the supervisory authority when requested to support them in performing their tasks.

e) Immediately informing the Customer about monitoring activities and measures of the supervisory authority, insofar as they relate to this order. This also applies if a competent authority investigates the processing of personal data by the Service Provider in the context of an administrative offence or criminal proceedings relating to the processing of personal data within the processing of the order.

f) In the event that the Customer is subject to monitoring by the supervisory authority, is exposed to misdemeanour or criminal proceedings, a liability claim by a data subject or a third party, or any other claim in connection with the order processing by the Service Provider, the Service Provider shall support the Customer to the best of their ability.

g) The Service Provider shall regularly monitor the internal processes and 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 are protected.

h) The Service Provider shall provide evidence of the affected technical and organisational measures towards the Customer within the scope of its monitoring powers as outlined in Section 7 of this Agreement.

6. Subcontracting relationships

(1) For the purposes of this provision, a subcontracting relationship is defined as a service that is directly related to the performance of the main service. This does not include ancillary services utilised by the Service Provider, such as telecommunications, postal/transport services,

Sample

maintenance, user services, or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Service Provider is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Customer's data, even in the case of outsourced ancillary services.

(2) The Service Provider may only engage the services of subcontractors (other order processors) with the prior express written or documented consent of the Customer.

a) The Customer shall agree to the commissioning of the following subcontractors, under the conditions of a contractual agreement according to Art. 28, para. 2–4 of the GDPR:

Company	Subcontractor address/country	Service
BC Directgroup GmbH	Rigistr. 9, 12277 Berlin, Germany	Printing service provider
Möller Druck & Verlag GmbH	Zeppelinstr. 9, 16356 Ahrensfelde, Germany	Printing service provider
ODS – Office Data Service GmbH	Ehrenbergstr. 16A, 10245 Berlin, Germany	Printing service provider

b) The outsourcing to subcontractors or the changing of existing subcontractors is permitted, provided that:

- the Service Provider must notify the Customer in writing or in text form of such outsourcing to subcontractors at a reasonable time in advance.
- the Customer may object to the planned outsourcing in writing or in text form to the Service Provider by the time the data is handed over.
- a contractual agreement in accordance with Art. 28, para. 2-4 of the GDPR serves as a basis.

(3) The transfer of the Customer's personal data to the subcontractor and the subcontractor's initial activities are only permitted once all requirements for subcontracting have been met.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Service Provider must ensure the service is permissible under data protection laws by taking appropriate measures. The same applies if service providers within the meaning of Para. 1, sentence 2 are to be used.

(5) Any further outsourcing by the subcontractor requires the express consent of the main Service Provider (at least in text form), and all contractual provisions in the contractual chain must also be imposed on the additional subcontractor.

7. Control rights of the Customer

(1) The Customer reserves the right to carry out inspections at the Service Provider's premises at any time and without hindrance or to have inspections carried out by inspectors to be commissioned in individual cases. The Customer shall have the right to seek confirmation of the

Sample

Service Provider's compliance with this Agreement in its business operations by means of spot checks, notification of which must be given in good time.

(2) The Service Provider must ensure that the Customer can seek confirmation of the Service Provider's compliance with their obligations under Art. 28 of the GDPR. The Service Provider is obliged to provide the Customer with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

(3) Evidence of such measures that do not only relate to the specific contract may be provided by

- compliance with approved codes of conduct in accordance with Art. 40 of the GDPR or
- certification of an approved certification process in accordance with Art. 42 of the GDPR.

(4) The Service Provider may not assert a claim to remuneration for enabling inspections by the Customer. The duties, actions, provisions and cooperation owed by the Service Provider under this Agreement are covered by the remuneration agreed in the respective order for the services owed by the Service Provider.

8. Reporting of security breaches by the Service Provider

(1) The Service Provider shall support the Customer in complying with the obligations set out in Art. 32–36 of the GDPR regarding the security of personal data, notification obligations in the event of data security breaches, data protection impact assessments and prior consultations. This includes, among other things,

a) ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential breach through security vulnerabilities and enable the immediate detection of relevant events of security breaches;

b) the obligation to report personal data security breaches immediately to the Customer;

c) the obligation to support the Customer within the scope of their duty to inform the data subject and to provide the data subject with all the relevant information in this context without delay;

d) supporting the Customer with the Customer's data protection impact assessments; and

e) supporting the Customer within the scope of prior consultations with the supervisory authority.

(2) The Customer may claim remuneration for support services that are not included in the service description or are not attributable to misconduct on part of the Customer.

9. Authorization of the Customer to issue instructions

(1) The Customer is required to provide immediate confirmation of any instructions given verbally (at least in text form).

Sample

(2) The Service Provider must inform the Client immediately if they are of the opinion that an instruction violates data protection regulations. The Service Provider is authorized to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Customer.

10. Deletion and return of personal data

(1) Copies or duplicates of data are not created without the Customer`s knowledge. Excluded from this are backup copies, insofar as they are required to ensure proper data processing, as well as data that is required in order to comply with statutory retention obligations.

(2) Upon completion of the contracted work or at the Customer`s request, at the latest 28 days after the service is rendered, the Service Provider is obligated to destroy all Customer data in accordance with data protection regulations.

(3) The Service Provider shall retain documentation that serves as evidence of proper data processing in accordance with the order beyond the end of the contract in accordance with the respective retention periods. The Service Provider may hand the documentation over to the Customer at the end of the contract.

11. Liability

(1) In the event that a data subject successfully asserts a claim against the controller or the Service Provider due to a breach of the provisions of the GDPR, Art. 82 of the GDPR applies.

(2) The Service Provider shall be liable in accordance with the statutory provisions for all other damages incurred by the controller due to non-compliance with an issued instruction.

12. Contractual changes, escape clause

(1) Amendments or additions to this Agreement must be made in writing or text form to be effective. This also applies to this clause itself.

(2) Should a provision of this Agreement be wholly or partially invalid or lose its legal validity at a later date, this shall not affect the validity of the remaining provisions. In the event of such an occurrence, the invalid provision shall be replaced by the statutory provision.

(3) This Agreement is be governed by the laws of the Federal Republic of Germany to the exclusion of its conflict of laws provisions.

Place, Berlin,

Customer
(valid legal signature)

Service Provider
(valid legal signature)