



Die treibende Kraft der
Data Driven Economy

DDV Rules for Commissioned Processing (DDV Declaration of Commitment)

Company (referred to as Service Provider or Contractor)	
Representative (Forename + Surname)	
Street Address incl. House Number	
Postcode, Town	
E-Mail Address	
Telephone	
Website	

These DDV Rules on Data Processing set out the minimum requirements for data processing and obligations regarding the handling of data. They are intended for service providers who process personal data on behalf of data owners in accordance with the General Data Protection Regulation (hereinafter referred to as the GDPR). The data owner or the authorised company is required to enter into a data processing agreement with the service provider within the scope of each data processing assignment. This agreement is established, when, firstly, the service provider signs these DDV Rules on Data Processing, submits them to the DDV, and references them, and secondly, when the data controller expressly or implicitly agrees to their applicability, in particular by transmitting the personal data. By signing and submitting these "DDV Rules for Commissioned Processing" to the DDV, the service provider thereby declares its binding commitment to comply with the

following rules and, consequently, the statutory contractual obligations of commissioned processing for each order. Together with the address order or the delivery note/service contract, which must expressly incorporate these "DDV Rules for Commissioned Processing," the service provider fulfils the legal requirements for commissioned processing. The address order or delivery note/service contract, in combination with the incorporated "DDV Rules for Commissioned Processing," enables data protection-compliant commissioned processing.

For companies that only cover specific aspects of statutory commissioned processing (for example, list brokers who do not conduct their own data processing but receive and forward data or manage data processing orders, or lettershops that solely process pre-addressed materials), the "DDV Rules for Commissioned Processing" apply only to the extent that the respective companies provide the agreed services and process address data in the course of doing so.

Preamble

These DDV Rules for Commissioned Processing (DDV DECLARATION OF COMMITMENT) apply to services in which the service provider processes the data of natural persons (data subjects pursuant to Article 4 No. 1 of the **GDPR**, in particular customers, prospective customers, and contact persons of legal entities) by way of commissioned processing, irrespective of whether the data processing and thus the service provider's access to the data of the data subjects constitutes the core task of the contractor or is otherwise classified as commissioned processing pursuant to Article 28 of the GDPR. In the latter case, the DDV Rules for Commissioned Processing apply accordingly.

The service described herein is typically a service of dialogue marketing (*although other services involving personal data can also be regulated in compliance with data protection laws under the terms of this DDV DECLARATION OF COMMITMENT*).

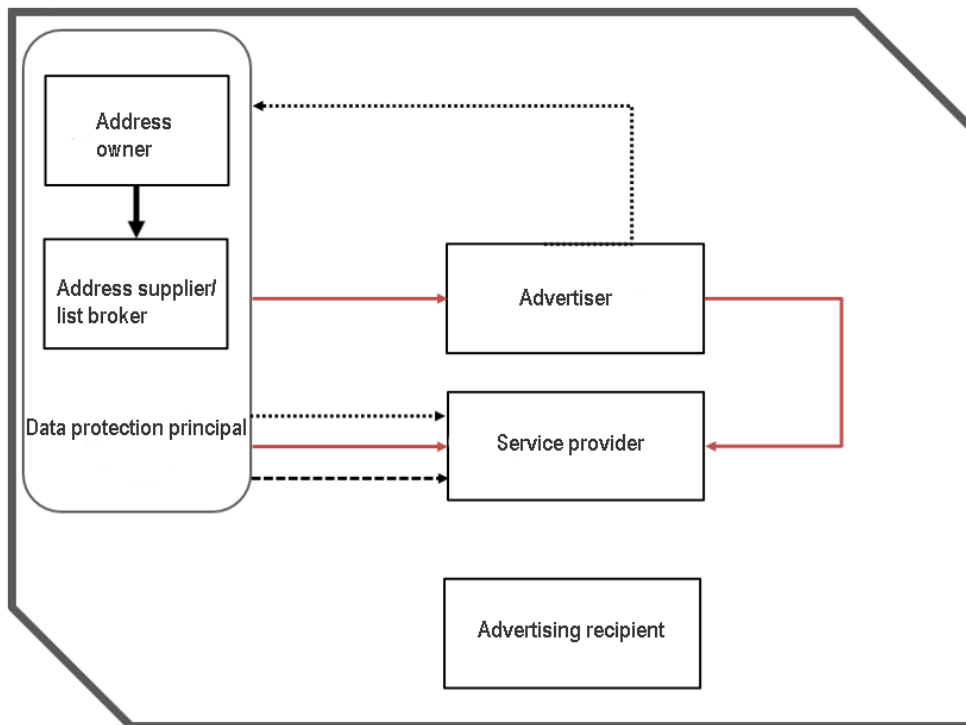
In dialogue marketing services, there are typically five parties involved from a data protection perspective: the **advertiser**, the **address owner**, the **address supplier/list broker**, the **service provider**, and the **recipient** of the advertisement (referred to as the "data subject" within the meaning of this DDV DECLARATION OF COMMITMENT). The advertiser economically initiates the commissioned processing by pursuing its objective of addressing the recipients (data subjects) for advertising purposes.

The advertising approach constitutes the processing of the address owner's personal data files (name, address, and possibly other data, such as address data) since this data must be processed for the delivery of direct advertising. The advertiser obtains usage rights to the personal data from the address owner and pays the service provider, who processes this data for dialogue marketing purposes based on a separate agreement.

To ensure data protection-compliant processing, the advertiser's access to the address data is excluded within the framework of the agreed commissioned processing, i.e., the data protection agreement. Access to the address data is controlled solely by the address owner/address supplier/list broker (data controller), who is responsible for the lawful processing of the personal data or acts as the responsible party (also referred to as the **data protection principal**). [This does not apply if the data is sold and the advertiser becomes legally responsible for data protection.] Therefore, data protection-compliant **commissioned processing** must, in principle, be agreed upon between the address

owner/address supplier/list broker on the one hand and the service provider, or between the intermediary service provider and the service provider, on the other hand.

The following diagram illustrates the parties involved and their legal relationships:



If the **address owner is also the advertiser**, the data protection responsibility as the principal and the commercial ownership of the usage rights are combined within a single company.

Note: The content of this DDV DECLARATION OF COMMITMENT specifically takes into account the requirements of Article 28 of the GDPR and is agreed upon with the principal through specific order-related instructions (**address order or delivery note/service contract**). The address order or delivery note/service contract must specify the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, as well as any recipients or categories of recipients and deletion periods, if applicable.

1. Definitions

Address owner: Owner of the data inventory (including data used for inserts); commissioning company and legally responsible entity for data protection.

Address data (records): Personal data, the processing of which is subject to data protection requirements and which may only be processed by the service provider within the scope of this DDV DECLARATION OF COMMITMENT after an order has been issued in accordance with Article 28 of the GDPR. This may include names, postal addresses, contact details, and other personal data.

Data protection principal: Controller pursuant to Article 4 No. 7 of the GDPR, namely the address owner/address supplier/list broker who issues the data processing order to the service provider in accordance with Article 28 of the GDPR. This entity does not have to be identical to the advertiser on whose economic behalf the data processing order is issued.

Address supplier: The company that holds address data based on its own contracts, has the right to use the address data, and agrees to the rules of this DDV DECLARATION OF COMMITMENT through express or implied acceptance, notably by transmitting the personal data.

DDV: Deutscher Dialogmarketing Verband e.V., Hahnstraße 70, 60528 Frankfurt, Germany, www.ddv.de.

Service provider: ([Sub-]Processor pursuant to Article 4 No. 8 of the GDPR, who processes address data for dialogue marketing purposes or other personal data (e.g., for document destruction, data centre services, or call centre services) on behalf of the address owner/address supplier/list broker and is a signatory party to this DDV DECLARATION OF COMMITMENT, including the respective separate address orders/service contracts.

GDPR: European Union General Data Protection Regulation.

Address Order and Delivery

Note/Service Contract: The DDV DECLARATION OF COMMITMENT, together with the address order or delivery note/service contract, constitutes the data protection agreement. This agreement forms the actual contractual relationship between the address owner/address supplier/list broker and the service provider, specifying concrete requirements regarding the subject matter and duration of processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, as well as any categories of recipients or individual recipients and data deletion obligations, if applicable. The combination of the DDV DECLARATION OF COMMITMENT (or the bilateral **Individual Agreement for Commissioned Processing**) with the address order or delivery note/service contract enables data protection-compliant order processing. An express declaration of acceptance for the offer made with the delivery note/service contract—i.e., the offer of data protection-compliant order processing—is not required; implied acceptance, notably through the transmission of personal data, is sufficient.

List broker: The company that obtains the usage rights to the address data (but not the address data itself) from the address owner and grants these rights, either directly or

indirectly through another list broker, to an advertiser for the purpose of carrying out an advertising campaign.

Advertising campaign: The marketing activity carried out using the address data (for example, a mailed letter, a paper catalogue, an email newsletter, a promotional phone call, or data processing/forwarding).

Advertiser: The advertiser, who, as the economic principal, may use the address data for its purposes only with the consent of the address owner and in accordance with this procedure, without processing the data itself.

2. General Obligations of the Service Provider

(1) The address owner/address supplier/list broker (the principal) grants the advertiser usage rights to address data. The advertiser acquires these usage rights for the execution of a specifically defined advertising campaign, either directly or through a list broker. The service provider engaged by the advertiser acts as a data processor on behalf of the address owner/address supplier/list broker to provide services within the scope of the advertising campaign that involve access to the address data specified in the address order or delivery note/service contract, to which the advertiser does not have access.

The service provider shall process the address data exclusively in accordance with this DDV DECLARATION OF COMMITMENT, the address order or delivery note/service contract, and any other instructions from the principal for the required order-related services, such as IT services (e.g., analysis, postal correction, deduplication, postage optimisation, and proofs), printing, lettershop, or call centre operations. Any processing beyond this scope (for example, storing data in anonymized form, order capture, history files, or optimisation analyses) shall only be carried out if legally permissible and if the necessary instructions from the principal or a mandatory legal obligation applicable to the service provider exist.

Instructions must generally be issued in text form; in exceptional cases where oral instructions are required, the principal must confirm them in text form without delay.

(2) The subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, as well as any categories of recipients or individual recipients and data deletion obligations, are—unless specified in this DDV DECLARATION OF COMMITMENT—set forth in the respective address order or delivery note/service contract.

(3) The service provider shall process the address data separately from data inventories that are not related to this DDV DECLARATION OF COMMITMENT and the address order or delivery note/service contract. This is to prevent unauthorized processing for other, non-permitted purposes.

(4) If the service provider receives the address data on portable storage media, it shall copy this data for the proper execution of this DDV DECLARATION OF COMMITMENT. The original storage media provided must only be deleted with the principal's consent and in the meantime must not be processed further (restriction of processing).

5) Upon completion of the work, the service provider must, at the principal's instruction, return the address data obtained within the scope of this DDV DECLARATION OF COMMITMENT, the address order, or the delivery note/service contract, as well as any other instructions, either to the principal or to another entity designated in writing, or delete the data in compliance with GDPR data protection requirements. This also applies to processing results generated within the scope of the DDV DECLARATION OF COMMITMENT, the address order, or the delivery note/service contract, as well as to test data and rejected material. Wastage containing personal data must be destroyed in accordance with security level 3 of DIN 66399-2, either using in-house shredders or specialized data processors.

The service provider must ensure that datasets containing personal address data do not remain as email attachments, on communication servers, clients, production computers, or in data backups beyond the deletion date. Unless the principal issues different instructions, for example, regarding database inventory held longer-term, the deletion of such data must be demonstrably completed no later than the seventh month following mailing date. The calendar week (ISO 8601) of the last mailing date must be communicated to the service provider if it is not specified in the address order or the delivery note/service contract.

Upon request, the service provider shall confirm the deletion in text form within five business days. Additionally, upon request, the service provider must provide the principal with a machine-generated deletion log that documents the physical deletion. The log must verify the deletion, including the date and time, the deletion method, and the responsible person, and must be retained for five years.

The obligation to return or delete data does not apply if the service provider is legally required to retain or otherwise store the specific data. Any further disclosure of the data is only permitted in accordance with the address order, the delivery note/service contract, or the principal's instructions.

(6) The engagement of subcontractors (particularly service providers with contractually agreed data access) to fulfil the address order or delivery note/service contract requires the prior written consent of the principal. The service provider may engage subcontractors without written consent, provided it adheres to its duty of order control and the contractual agreements in accordance with Article 28 of the GDPR, if the subcontracted services do not constitute the contractual main service or partial services of address processing performed by the service provider, but rather serve as ancillary services supporting the fulfilment of the main service. Examples include advanced telecommunications services or cleaning services that include the disposal of data carriers.

However, consent is required if the aforementioned service constitutes, in whole or at least in substantial parts, the service agreed upon with the principal. In all cases, the contents of this DDV DECLARATION OF COMMITMENT, the address order or delivery note/service contract, and any other instructions must be appropriately stipulated in the aforementioned (sub-)contracts. Upon request, the principal may receive a list of all subcontractors at any time, including those whose engagement has been expressly approved by the principal.

These provisions also apply to the engagement of independent contractors/freelancers who work for the service provider without being integrated into its company as employees and who provide essential services within the actual scope of this DDV DECLARATION OF COMMITMENT, the address order or delivery note/service contract, and any other instructions.

(7) The service provider shall implement appropriate technical and organisational measures within its area of responsibility to adequately protect the address owner’s data, particularly against accidental and unauthorised processing (appropriate technical and organisational data security measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR). The service provider shall also assist the principal, where necessary, with any required data protection impact assessment, limited to its area of responsibility and taking into account the information provided by the principal.

Upon the principal’s request, the service provider shall promptly support the principal, considering the nature of the processing and the resources and information available to the service provider, in fulfilling the principal’s obligations to inform data subjects and to provide information, as well as to rectify, delete, or restrict the processing of data and to uphold other data subject rights under applicable data protection laws.

In accordance with Article 30(2) of the GDPR, the service provider shall maintain a record of the processing activities carried out by it. This record must be provided to the principal upon request in the form of a copy, insofar as its content is related to the processing activities covered by this DDV DECLARATION OF COMMITMENT, the address order or delivery note/service contract, and any other instructions.

(8) The service provider shall cooperate in defending against claims for damages asserted by data subjects, provided such cooperation is possible without significant additional effort. If a data subject directly contacts the service provider to exercise their data subject rights, the service provider shall, without providing a substantive response, formally refer the data subject to the principal and forward the request to the principal. The service provider shall only respond on behalf of the principal if explicitly instructed to do so within the scope of this DDV DECLARATION OF COMMITMENT, the address order or delivery note/service contract, and any other instructions.

(9) The address owner is obliged to immediately report any unintended or unlawful data processing, including disclosures to third parties or other data breaches that may pose a risk to the rights and freedoms of natural persons, to the competent data protection supervisory authority. In the event of a high risk to the rights and freedoms of the affected person, the data subject must also be informed without delay. If the service provider becomes aware of such breaches within its area of responsibility, it shall immediately notify the principal. In such cases, the service provider shall, as an interim measure and at its reasonable discretion, take appropriate measures within its area of responsibility to protect the address data and mitigate any potential adverse effects (appropriate technical and organisational data security measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR). The service provider shall promptly inform the principal of the measures taken.

(10) The service provider shall promptly inform the principal if, in its opinion—which does not require comprehensive legal examination—an instruction issued by the principal may lead to a violation of legal regulations. The service provider is not required to follow the instruction if it is not modified or expressly confirmed by the principal.

(11) The service provider shall designate a single point of contact to liaise with the principal, through whom the principal can address any questions related to this DDV DECLARATION OF COMMITMENT, the address order or delivery note/service contract, and any other instructions. The service provider shall promptly notify the principal in text form of any change of the designated contact person.

3. Security Obligations of the Service Provider

(1) The service provider shall ensure, within its area of responsibility, that it processes the address data with a level of security appropriate to the state of the art, considering the implementation costs, the nature, scope, circumstances, and purposes of the processing related to this DDV DECLARATION OF COMMITMENT, as well as the likelihood and severity of risks to the rights and freedoms of natural persons, in accordance with Article 32 of the GDPR (data security measures).

At the principal's request, the service provider shall provide its current data security concept even after the order has been placed, thereby allowing, among other things, the principal's data protection officer or an auditor designated by the principal who is bound by professional confidentiality to review and inspect the data security concept. The data security concept must include sufficient explanations regarding the following aspects: building access control, system access control, application access control, transmission control, input control, order control, availability control, and separate processing.

If the principal requests modifications, the service provider shall implement them following prior written notice and at the principal's expense, provided that such modifications exceed the aforementioned requirements.

(2) Address data that is to be transmitted electronically may only be transmitted by the service provider in a secure manner that complies with the state of the art, particularly in encrypted form, and in accordance with the principal's instructions.

(3) The service provider is not authorised to use the principal's real data for software development or other testing purposes beyond what is legally permissible. Instead, anonymised original data or fictitious test data must be used.

(4) The service provider shall store and process address data separately by order and shall allow access by employees only to the extent necessary to fulfil the order. Furthermore, access to the data shall only be granted to employees who have been specifically and expressly obligated to maintain confidentiality and who receive regular training on data protection and data security regulations and procedures relevant to address processing. These measures must be documented.

4. Obligations of the Service Provider to Allow Controls

(1) The controller is legally obligated to verify the effectiveness of the data security measures implemented by the service provider. Therefore, the service provider shall permit the principal to inspect and audit, once per year, the processing of the data provided by the principal, including the data processing systems related to the services covered by this DDV DECLARATION OF COMMITMENT, the address order or delivery note/service contract, and any other instructions. This inspection may include stored data and its processing, data processing programs, the data protection organisation, and its documentation, including work instructions.

The service provider shall keep the documents related to this DDV DECLARATION OF COMMITMENT available for the principal's inspection and respond to inquiries within a reasonable timeframe. The inspection may be conducted by the principal's data protection officer or a person appointed by the officer who is bound by confidentiality.

(2) The principal may, at its discretion and without conducting on-site inspections, verify that the data security measures implemented by the service provider meet the aforementioned requirements by reviewing relevant evidence provided by the service provider. Such evidence may include audit reports on information security or certifications, such as the DDV quality award from the Competence Center DirectMail Services or Target Group Marketing.

5. Deduplication Protocol/Control Addresses

(1) If deduplication processes are performed using third-party data as part of the order, the service provider must create a complete and comprehensible protocol containing the following specified information for each third-party list.

<i>DDV Standard "Usage Report"</i>	
Issue date	
Name of the marketing campaign	
List name	
Delivered quantity of address data	
.-	Volume of deletions (e.g. after postal validation or incorrect records)
=	Gross quantity (input) for deduplication
-	Volume of data eliminated in deduplication
=	Net quantity (output) after deduplication
-	Records deleted to reach required volume
=	Mailed quantity

(2) To monitor and prevent unauthorised use, control addresses may be inserted into the respective datasets. If the principal presents evidence of unsolicited advertising sent to a control address, which can be clearly attributed to the dataset provided to the service provider for processing within the specific advertising campaign, it shall be presumed that unauthorized use has occurred. The service provider is obligated to promptly notify the principal of any unauthorized use of data that it becomes aware of. Such notification must be made at least in text form.

6. Miscellaneous

(1) When disclosing third-party data (either electronically or in printed form), the recipient must be informed that the address data originates from one or, where applicable, multiple controllers and may only be processed for the purpose for which it was provided.

(2) If deduplications are conducted using third-party data in the consumer sector (Business to Consumer), the service provider responsible for the third-party data deduplication shall use the current DDV Robinson List unless the principal has expressly waived its use in writing.

(3) This DDV DECLARATION OF COMMITMENT shall apply indefinitely to all address orders or delivery note/service contracts until it is effectively revoked.

(4) This DDV DECLARATION OF COMMITMENT, as well as the address orders or delivery note/service contracts and written instructions, are subject to German law. The place of jurisdiction shall be the local court of the principal's location, insofar as this is legally permissible.

_____, _____

Date

Place

Company stamp

Signatory (forename + surname)

Signature

2nd Signatory (if applicable)

Signature