



Die treibende Kraft der
Data Driven Economy

**Rules
for Commissioned Processing
(DDV Declaration of Conformity)**

Service provider

(in the following **Service Provider**)

Representative

Street name and number

Postal code, place

E-mail address

Website

The following DDV rules for commissioned processing (in the following **DDV Rules**) state the minimum requirements for commissioned data processing and the obligations related to the treatment of the data. They apply for the Service Providers (in the following also **Processor**) processing personal data as processor on behalf of address owners (in the following also **Controller**) pursuant to the regulations of the General Data Protection Regulation (in the following **GDPR**). In the context of each data processing order, the address owner shall agree a verifiable agreement on commissioned processing with the Service Provider.

By signing and depositing the DDV Rules the Service Provider explicitly commits to comply with the following obligations (and thus with the statutory contractual duties for commissioned processing) for each order of commissioned processing. In conjunction with the separate address order, which shall expressly refer to the DDV Rules, this guarantees the service provider’s compliance with the legal obligations for commissioned processing. The separate address order in conjunction with the DDV Rules facilitates data processing in compliance with data protection laws.

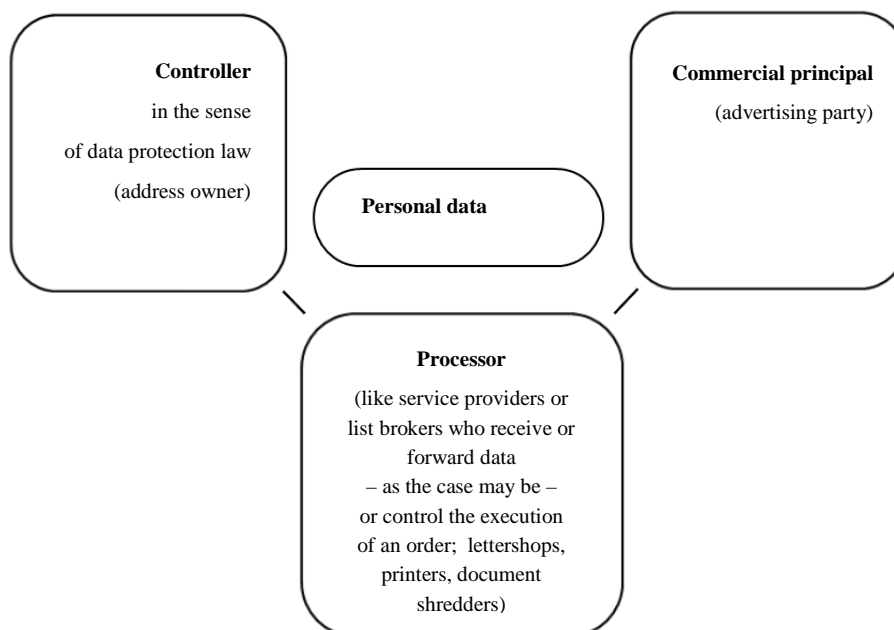
For companies which only cover parts of the commissioned processing (e.g., either list brokers who do not perform any data processing of their own, but receive and transmit data or control data processing, or lettershops which only process already addressed material), the DDV Rules only apply to the extent to which the companies in question render the agreed services and process address data doing so.

Preamble

The DDV Rules apply for services for which the Service Provider processes data of natural persons (data subjects pursuant to Art. 4 (1) of the European General Data Protection Regulation, **GDPR**; *in particular: customers, interested persons, contact persons of legal entities, other personal data*) on behalf of a list owner, independent of whether or not the data processing and thus the Service Provider’s accessing of the data subject’s data must be classified as a core activity of the processor or as commissioned processing pursuant to Art. 28 GDPR.

The service shown here is a typical dialogue marketing service (*however, the DDV Rules may also be used to regulate other types of services involving personal data in compliance with data protection laws*).

The data protection aspects of dialogue marketing services usually concern three or four parties: An **advertiser**, **address owner**, **service provider** and **potential customer**, receiving marketing material. The advertiser initiates the commissioned processing in order to contact a customer or a potential customer (the “data subject” in the sense of these DDV Rules) for marketing purposes. Such promotional activity constitutes a processing of personal data (name, address and, possibly, further data) held by the address owner. The address owner confers the right to use the personal data to the advertiser who, in turn, remunerates the Service Provider who processes such data for dialogue marketing purposes pursuant to a separate agreement. The commissioned processing under the DDV Rules does not allow the advertiser any access to the personal data of the data subject. Access to the data is managed by the address owner in his capacity as Controller of the data; this means that the address owner is also responsible for the processing of the data in compliance with data privacy laws (**controller in the sense of data protection law**). [*The situation is different, if the data are sold and the advertiser becomes the controller in the sense of data protection law.*] **From a data protection perspective, the contractual relationship (or commissioned processing) exists between the address owner and the Service Provider.** The following diagram illustrates the legal relationships between the parties.



If the **address owner** is **identical with** the advertiser, the Controller’s responsibility for compliance with data protection law and the commercial ownership of the rights of use are combined in one entity. In this case, only the rights and obligations of this agreement apply which are defined for the legal relationship between address owner and Service Provider.

Please note: These DDV Rules comply with the requirements of Art. 28 GDPR and are supplemented with specific instructions of the address owner relevant for each individual contract (**separate address order**). In the separate address order, the object and the duration as well as the type and purpose of the processing, the type of the personal data and the categories of the data subjects plus any possible recipients or categories of recipients need to be specified.

1. Definitions

Address owner (= list owner): The company which either collected the personal data itself or acquired them otherwise; any data processing by the Service Provider is subject to the instructions of the company.

Address data (records): Personal data which must only be processed in compliance with data privacy requirements; Service Providers may process such data on the basis of an AGREEMENT following an order pursuant to Art. 28 GDPR. Address data comprise names, postal addresses, communication data and further personal data.

Controller in the sense of data protection law: The controller pursuant to Art. 4 (7) GDPR and owner of the data instructing the data processing by the data processor pursuant to Art. 28 GDPR. He does not need to be identical with the advertiser in whose commercial interest the order is issued. Where companies advertise their own products and/or services, the controller and the advertiser are identical.

<i>DDV:</i>	Deutscher Dialogmarketing Verband e.V., Hahnstraße 70, 60528 Frankfurt, www.ddv.de .
<i>Service provider:</i>	Processor pursuant to Art. 4 (8) GDPR who processes the address data for dialogue marketing purposes or who processes other personal data (e.g. file destruction, data center services, list broking or call center services) on behalf of the address owner and who is a signatory to the separate address order (including the DDV Rules for commissioned processing).
<i>GDPR:</i>	European General Data Protection Regulation.
<i>Separate address order:</i>	Agreement between the address owner and the Service Provider containing instructions regarding the object and the duration of the processing, the type and purpose of the processing, the type of personal data as well as the category of the data subjects plus the categories of recipients or the recipient, where applicable. The combination of the separate address order in conjunction with the DDV Rules for commissioned processing guarantee a data processing which is compliant with data protection law.
<i>List broker:</i>	The company which receives the right of use of the contacts (not the address data themselves) from the address owner and grants it directly or indirectly via a list broker to an advertiser for advertising purposes.
<i>Marketing measure:</i>	The marketing measure which is carried out on the basis of the address data (e.g. the mailing of electronic adverts or of catalogues; an email newsletter, a promotional telephone call or a permanent data preparation or processing).
<i>Advertiser:</i>	The commercial service recipient who may only use the address data for his own purposes through Service Provider subject to prior approval by the address owner.

2. General obligations of the Service Provider

- (1) The owner of the addresses grants the rights of use for the address data in a *separate address order*. The advertiser acquires such rights of use in order to carry out a specified marketing measure either directly or with the help of a list broker. The Service Provider, who is paid by the advertiser, serves as a processor for the address owner and provides his services by using the data held by the address owner and specified in the separate address order. The Service Provider will process the address data exclusively pursuant to the specifications of the separate address orders or any other orders issued by the address owner for the required services like IT (e.g. analysis, correction of postal addresses, matching, postage optimization and printing), print, letter shop or call center services. The Service Provider will carry out any further processing (like storing of anonymized data, for order registration purposes, history files or optimization analyses) only, if this is allowed from a data protection perspective and if the address owner has issued the necessary orders or if there exists a binding legal obligation for the Service Provider. As a rule, the order shall always be issued in writing; as an exception, they may be issued orally, where necessary, but will then have to be confirmed in writing immediately by the address owner.
- (2) The object and the duration of the processing, the type and purpose of the processing, the type of personal data as well as the category of the data subjects plus the categories of recipients or the recipient, where applicable, shall be specified in the individual address order, to the extent to which they are not already specified in these DDV Rules.
- (3) The Service Provider shall process the address data separately from the data files which are not part of the separate address order. Thus, any unauthorized processing for other, illegal purposes shall be prevented.
- (4) To the extent to which the Service Provider receives the data on portable storage media, he shall copy the data for the proper handling of the separate address order. The data on the received storage media shall only be deleted after the address owner has given his consent; up to this point of time, they shall no longer be processed (restriction of processing). The Service Provider's expenses arising from such handling shall be remunerated by the address owner.

- (5) Once the contractually agreed services have been provided, the Service Provider shall return the address data which he received in the context of the separate address order either to the address owner himself or to a third party specified by the address owner in writing or destroy them in compliance with the GDPR, as specified by the address owner. This also applies for the processing results which are produced in the context of the separate address order as well as for any testing or reject material. Any waste containing persona data shall be destroyed in compliance with security level 3 of the DIN 66399-2, either by internal file destroyers or by specialized subcontractors. The Service Provider shall take care that data files containing personal data do not survive in the form of email attachments, on communication servers, clients, production computers or in data back-ups any longer than up to the specified destruction date. To the extent to which the address owner has not issued a deviating order, e.g. for trust inventories, the data shall have been verifiably deleted in the course of the seventh month following postal delivery. The calendar week (ISO 8601) of the latest postal delivery shall be communicated to the Service Provider, if it does not result from the separate address order. The Service Provider shall confirm the destruction of the data carried out by himself or by an external subcontractor to the address owner and his representative in writing within a period of five business days. Upon request, the Service Provider shall provide a deletion or destruction report to the address owner or his representative. The required report shall confirm the effected deletion and contain the date and time as well as the type of the deletion plus the responsible person; the document shall be valid for a period of five years. The Service Provider’s expenses associated with the obligations for the return and deletion specified above shall be remunerated by the address owner in compliance with the address order. The obligation to return or delete the data does not apply, if the Service Provider is legally or otherwise bound to retain or store the specific data. Any other disclosure of the data shall only be legal in compliance with the specific address order or a specific order issued by the address owner.
- (6) The engagement of subcontractors in order to fulfill the separate address order (Service Provider with an individually specified access to the data) shall only be possible subject to the prior consent declared by the address owner in writing. Where services related to contractual data processing are concerned, which third parties render to the Service Provider as ancillary services, the Service Provider may engage such subcontractor in order to fulfill the agreement without an explicit

written declaration of consent, as long as the subcontractor complies with the obligation to comply with instructions and verifiably agrees a contract in compliance with Art. 28 GDPR. This applies, e.g., for extended telecommunications services or for cleaning staff who are also responsible for the disposal of data media. A declaration of consent is required, however, if the said service represents the service agreed with the Service Provider in whole or in essential parts. In any case, the engagement of subcontractors shall always be subject to the provisions in these DDV Rules. Upon request, the address owner and a separate advertiser shall be provided with a list of all subcontractors, including those whose engagement was approved by the Controller. The DDV Rules also apply for the engagement of freelancers who work for the Service Provider without being integrated into the Service Provider’s company and render substantial services in relation to the separate address order.

- (7) In his area of responsibility, the Service Provider shall take technical and organizational measures for an adequate protection of the address owner’s address data, in particular against unintentional or unauthorized data leakage (suitable technical and organizational data protection measures in order to grant a level of protection appropriate with a view to the risk involved; pursuant to Art. 32 GDPR) and support the Controller with the privacy impact assessment, where necessary, by providing information related to his sphere of action and taking into account the data provided to him by the Controller. The Service Provider has the right to request appropriate remuneration for his support and the reimbursement of any related expenses. With regard to the address owner’s obligation to provide information to data subjects and to correct or delete data or to restrict the processing of data or to comply with any other rights of the data subjects pursuant to current data protection law, the Service Provider, depending on the type of processing performed by him and the means and information available to him, supports the address owner immediately. The Service Provider’s associated expenses shall be remunerated by the address owner in compliance with the address order. Pursuant to Art. 30 (2) GDPR, the Service Provider keeps a journal of the processing procedures carried out by him. Upon request of the address owner and his representative, a copy of such journal shall be made available, to the extent to which the content of the journal is related to the separate address order.

- (8) The Service Provider grants support for the defense against claims raised by data subjects, to the extent to which this is possible for him without major effort. If the data subject contacts the Service Provider directly in order to claim his/her rights, the Service Provider shall refer the data subject formally to the address owner, without giving any advance information, and forward the request to the address owner. The Service Provider shall only answer any requests, if the address owner has commissioned him to do so in the context of the commissioned processing and subject to reimbursement of expenses.
- (9) The address owner is obliged to report immediately any unintentional or unauthorized data protection law relevant leakage to third parties or any other infringements against data protection law which might lead to a risk for the rights and freedoms of natural persons to the responsible data protection supervisory authority and – where a high risk for the rights and freedoms of the data subject is involved – to the data subject directly. To the extent to which such infringements within his sphere of action come to the knowledge of the Service Provider, he shall immediately inform the address owner accordingly. In such case, the Service Provider shall, at his own dutiful discretion, take temporary measures appropriate in his sphere of action in order to protect the address owner’s address data and to mitigate its possible negative effects (appropriate technical and organizational measures to ensure a level of security appropriate to the risk; pursuant to Art. 32 GDPR). The Service Provider shall inform the address owner about any measures taken by him at his earliest convenience.
- (10) The Service Provider informs the Controller immediately, if an order issued by the address owner, in his view – which does not presuppose any comprehensive legal analysis -, might lead to an infringement against legal provisions. The order does not need to be followed, if it is neither amended nor explicitly confirmed by the address owner.
- (11) The Service Provider shall appoint a contact person with whom the address owner or his representative may clarify any issues in relation to the separate address order. The Service Provider has appointed a data protection officer pursuant to the relevant legal requirements. The Service Provider shall immediately inform the address owner about any change of the contact person in writing.

3. Safety obligation of the Service Provider

- (1) In his area of responsibility, the Service Provider guarantees that he, pursuant to Art. 32 GDPR, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk in order for the processing of address data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons (data protection measures). Upon the address owner’s request, the Service Provider makes his current data security concept available to the address owner and his representative, also once the order has already been placed, and facilitates either the address owner’s data privacy officer or an external auditor, who is committed to professional secrecy and appointed by the address owner, to access and review of the data security concept. The data security concept includes sufficient explanations regarding access control to the premises, the system and the applications, as well as transfer, input, order and availability control and, finally, regarding separate processing. To the extent to which the address owner requests changes, the Service Provider shall implement them following the prior written request of the address owner; all expenses shall be reimbursed by the address owner, if such changes go beyond the legally required state of the art.
- (2) Address data which must be transferred electronically, shall only be transferred in a safe (taking into account the state of the art) and encrypted form by the Service Provider, to the extent to which the address owner does not request another mode of transmission.
- (3) Beyond the legally permissible, the Service Provider does not have the right to use any real data of the address owner in order to develop software or for any other tests. Instead, he shall work with anonymized original data or with fictitious test data.
- (4) The Service Provider stores and processes the address data separately for each order and grants his employees access to the data only to the extent to which this is necessary for the fulfillment of the separate address order. In addition, he only grants access to such employees who have been explicitly committed to secrecy and have been trained regularly with regard to the data protection and data security rules and processes relevant for the data processing.

4. Obligations of the Service Provider to tolerate controls

- (1) The address owner is legally required to audit the effectiveness of the data protection measures taken by the Service Provider. The Service Provider shall, therefore, allow that the address owner controls the processing of the data provided by him by accessing and checking the data processing facilities, the stored data and the data processing programs used in the context of this agreement in an on-site audit as well as the documentation of the data protection organization, including work orders, usually once a year. The Service Provider shall make the documents related to the separate address order available and answer any upcoming questions without undue delay. Access shall be granted to the address owner’s data privacy officer or an external auditor, who is committed to professional secrecy and appointed by the address owner.
- (2) The address owner may also verify the data protection measures as to being up to the state to the art by receiving from the Service Provider proof like auditing reports regarding information security or the information regarding the receipt of the DDV quality label issued by the Competence Centers DirectMail Services and Target Group Marketing.

5. Matching report/control addresses

- (1) Where data, according to the order, are matched with the help of third party data, the Service Provider shall compile a complete and comprehensible protocol, containing the following information.

<i>DDV Standard “Accounting Protocol”</i>	
	Creation date
	Designation of the marketing measure
	Designation of lists per data file
	Number of delivered address data
./.	Address data resulting from postal validation (e.g. corrections)
=	Gross quantity for matching (Matching Input)

./.	Address data eliminated after the matching of duplicates
=	Net quantity after matching (Matching Output)
./.	Reduction pursuant to customer order
=	Application quantity

- (2) For verification purposes and for protection against use in violation of contract, verification addresses may be inserted into the individual data files. If the address owner is able to present marketing material which was not agreed with him and which was sent to a verification address, and if such verification address clearly belongs to the data file which was provided to the Service Provider for a specific marketing measure only, it must be assumed that the addresses were used without proper authorization. If the Service Provider notices such unauthorized use of data himself, he is obliged to communicate it to the address owner and his representative immediately. Such communication shall at least be effected in writing.

6. Miscellaneous

- (1) If third party address data are transmitted (electronically or in print), the recipient shall be informed that the address data stem from one specific or, as the case may be, several external Controllers and shall only be processed for the purpose for which they were delivered.
- (2) Where third party data are matched using third party data in the Business to Consumer sector, the Service Provider responsible for the matching process shall use the current DDV Robinson list (updated monthly), unless the Controller(s) has/have dispensed with its use in writing.
- (3) The fact that a company has committed itself to the DDV Rules by signature shall be published on the DDV website. The signed DDV Rules shall be deposited with DDV. Upon request, the Service Provider shall make copies of these DDV Rules available to the Controller, the list broker or other Service Providers involved. The Service Provider shall immediately inform DDV in writing of any changes or updates to the information provided in the DDV Rules. The publication of the

information that the relevant member has signed the DDV Rules will then be taken off the DDV website again.

- (4) The DDV Rules shall be valid for the signing member until revoked by the member; the revocation shall be sent to DDV by registered mail and shall become valid six (6) weeks after receipt with effect for the future. The DDV Rules shall remain valid for any separate address orders that already existed prior to the aforementioned six (6) week period.
- (5) With the signature, the Service Provider also affirms the concordance of the above text with the version of the DDV Rules provided by DDV (version: 10/2017).
- (6) The requirements for written form in the sense of the DDV Rules (apart from the requirement for written form regarding the placing of the order) can be met by using the text form (in particular, e-mail).
- (7) All agreements based on these DDV Rules are subject to German law. The place of jurisdiction is the place of each order’s local court, to the extent to which this is legally permitted.

_____, _____
Date Place

Firm stamp or firm name

(_____)
Signatory (printed name)

(_____)
2nd signatory (printed name) /
where applicable