Data protection and order processing

The standard contractual clauses of the European Union pursuant to Art. 28 (7) GDPR, available here shall be deemed to have been concluded between the parties.

For the purposes of these Standard Contractual Clauses:

1. The customer is the "controller" and e-dialog is the "processor";
2. In the case of the use of sub-processors in point 7.7 of the standard contractual clauses, option B "GENERAL WRITTEN AUTHORISATION" shall be deemed to have been agreed between the parties. The companies affiliated with e-dialog are in any case considered authorised sub-processors.
3. All references to the "Annexes" in the Standard Contractual Clauses refer instead to the Annexes to the contract between the parties.

In any case, this does not affect the fact that the customer as the responsible party ("controller") is obliged to obtain and document any prescribed consents.

Annexes to the standard contractual clauses pursuant to Art. 28 (7) GDPR

Annex I - Description of the processing of categories of data subjects
Annex II - Technical and organisational measures
Annex III - List of sub-processors

Annexes to the standard contractual clauses pursuant to Art. 28 (7) GDPR

ANNEX I

Description of the processing of categories of data subjects

Description of the processing of categories of data subjects whose personal data is processed

Categories of personal data that is processed:
In principle, e-dialog does not work with personal data; even if campaigns are personalised, e-dialog does not have access to the data required for personalisation, but only has access via user interfaces to display and control elements of summaries of the data to be used in systems whose controller (responsible party) is the customer.

In exceptional cases - on written instruction from the customer - the following categories of data are processed:

- Data of data subjects of the customer: In the majority of cases, the personal data (user IDs) of the data subjects is anonymised.
- Names and contact details of employees and vicarious agents of the customer
- In the case of e-mail or newsletter marketing, these categories may include name, e-mail address and date of birth - the scope is defined in the individual order or according to the briefing.
- In the case of custom audience lists, these categories can include e-mail addresses and phone numbers, usually encrypted.

Please note that the customer is responsible for obtaining and documenting any consent in accordance with Art. 6 (1) a GDPR. The contractor is not obliged to check the customer.

In principle, we work with data from the customer's data subjects on systems that are subject to the customer's control or have been licensed by the customer. Systems include digital analytics tools and ad booking and management platforms.

In cases where data is processed on systems licensed by e-dialog, the following applies:
e-dialog works in the Google-licensed G-Suite (Google Workspace), as well as in the Google Cloud Platform with Google Ireland Ltd., for which the following Data Processing Agreements apply:

https://cloud.google.com/terms/data-processing-terms

Contact and project data is processed in "Zoho One" within the EU. In the course of invoicing to contact persons defined in advance by the customer, contact data is processed in "BMD Business Software" within the EU. Customer contact details are managed in "Active Campaign" for the purpose of invitations, event management, information and newsletters - the corresponding data processing agreements and standard contractual clauses have been concluded.

Type of processing: Collecting, recording, storing, modifying and retrieving data.

Purpose(s) for which personal data is processed on behalf of the controller: Within the scope of the purposes defined in the respective offer.

Duration of processing: for the duration of the provision of services in accordance with the controller's order

In the case of processing by (sub-)processors, the object, type and duration of the processing must also be stated.

ANNEX II

Technical and organisational measures

Technical and organisational measures, including to ensure the security of the data

*Measures to ensure the ongoing **confidentiality, integrity, availability and resilience** of the systems and services in connection with processing:*

Confidentiality:

Access control: Protection against unauthorised system use (passwords, including corresponding policy), two-factor authentication (Google Authenticator)
Access control: Reading, copying, modifying or removing within the system only after approval; standard process for assigning and withdrawing authorisations; logging of changes (creating, modifying and deleting files); administrative user accounts limited to the absolute minimum.

Integrity

Transfer control: No unauthorised reading, copying, modification or removal during electronic transmission or transport if handled entirely within the Google Cloud.

Input control: Personal data of the customer/client is only transferred to the systems (e.g. Google Analytics) by the customer/client (event log, logging).

Measures to ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident:

Availability and resilience

Availability control: Protection against accidental or wilful destruction or loss (Google Cloud solution), virus protection; backup concept within Google Cloud Services; standard processes when employees change/leave; rapid recoverability.

Procedures for regularly reviewing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing:

Data protection policy, including regular **employee training**.

Order control: No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the customer, through clear contract design, formalised order management, strict selection of the processor (ISO and other certifications), ongoing and ad hoc checks.

Measures to ensure the physical security of places where personal data is processed:

Access control: Protection against unauthorised access to data processing systems (multi-level locking system with key), electric door openers, video system, filing cabinets with lock

Measures to enable data portability and to ensure erasure

Deletion periods:

- Employees' access data and authorisations are revoked in a standardised procedure after they leave the company.
- Personal data of the customer's data subjects will be deleted after a written request or 12 months after termination of any contractual relationship between the customer and e-dialog, provided that there are no statutory retention obligations to the contrary.
- The customer's contact details are subject to a statutory retention period (invoicing, documentation, etc.) and are deleted after this period has expired.

The approved sub-processors (e-dialog GmbH and e-dialog AG) take exactly the same technical and organisational measures as part of the e-dialog Group

ANNEX III

List of sub-processors

In any case, the companies affiliated with e-dialog, such as e-dialog AG Switzerland, Weissbadstrasse 14, 9050 Appenzell and e-dialog GmbH Germany, Kurfürstendamm 15, 10718 Berlin, are agreed and approved as sub-processors.

As part of the provision of services in accordance with the basic contract, the above-mentioned group companies of the processor may be used (but this is not mandatory). In this case, the processor has concluded the corresponding contracts with the sub-processors to ensure compliance with data protection regulations.

The controller has authorised the use of the following sub-processors:

Name: e-dialog AG Switzerland

Address: Weissbadstrasse 14, 9050 Appenzell

Name: e-dialog GmbH, Germany

Address: Kurfürstendamm 15, 10718 Berlin