dtms

Order processing agreement of dtms GmbH according to GDPR

1. General

(1) The following terms and conditions govern the contractual relationship established between dtms GmbH, Taunusstraße 57, 55118 Mainz (hereinafter referred to as the "Contractor") and the contractual partner (hereinafter referred to as the "Client") with regard to the processing of personal data by dtms on behalf of the Partner as the Client within the meaning of Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). Both together are hereinafter referred to as "Parties".

(2) The Contractor processes personal data on behalf of the Client within the meaning of Art. 4 No. 8 and Art. 28 GDPR. This contract governs the rights and obligations of the parties in connection with the processing of personal data.

(3) Insofar as the term "data processing" or "processing" (of data) is used in this contract, the definition of "processing" within the meaning of Art. 4 No. 2 GDPR shall apply.

(4) Insofar as the Contractor is subject to special obligations laid down in Directive 2002/58/EC or the ePrivacy Directive with regard to the processing of personal data within the meaning of Art. 95 GDPR, the GDPR does not impose any additional obligations on the Contractor, so that an order processing agreement is not required; therefore, the provisions of this agreement shall not apply in these cases.

2. Object and duration of the order

2.1 Object

(1) The subject matter, nature and purpose of the processing, the type of personal data and the categories of data subjects are set out in Section 13 of this Agreement. The subject matter of the processing is also set out in the main contract concluded between the parties, to which reference is made here (hereinafter referred to as the Service Agreement).

(2) The data is collected when using the services and/or products of the Contractor specified in Section 13, insofar as the Client has entered into a contractual relationship with the Contractor for one of the services and/or products specified therein.

2.2 Duration

(1) The duration of the contract shall extend over the term of the service agreement within the meaning of Section 2.1 (1) of this contract. The possibility of termination without notice remains unaffected by this. In particular, the Client may terminate the contract at any time without notice if the Contractor commits a serious breach of the applicable data protection regulations or of obligations under this contract, if the Contractor is unable or unwilling to carry out an instruction of the Client or if the Contractor refuses access to the Client or the competent supervisory authority in breach of the contract.

(2) Notwithstanding the preceding paragraph, the contract shall apply for as long as the Contractor processes the Client's personal data (including backups).

(3) Insofar as other agreements on the protection of personal data arise from other agreements between the Client and the Contractor, this contract for commissioned processing shall take precedence, unless the parties expressly agree otherwise.

3. Technical and organizational measures

(1) The Contractor shall take all necessary technical and organizational 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 on the Contractor's website at https://www.dtms.de/agb/. If the Client accepts the offer, the documented measures shall form the basis of the contract.

(2) If the inspection/audit of the client reveals a need for adjustment, this shall be implemented by mutual agreement.

(3) The agreed technical and organizational 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. Changes can be viewed in the documentation on the Contractor's website at https://www.dtms.de/agb/. About significant changes the client will also be informed.

4. Rights of data subjects

(1) The Contractor shall support the Client in its area of responsibility and as far as possible by means of suitable technical and organizational measures in responding to and implementing requests from data subjects with regard to their data protection rights. The Contractor may not, without authorization, provide information on, port, correct, delete or restrict the processing of data processed on behalf of the Client, but only in accordance with documented instructions from the Client. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

(2) If covered by the scope of services, the rights to information, rectification, restriction of processing, erasure and data portability shall be ensured directly by the Contractor in accordance with the Client's documented instructions.

5. Quality assurance and other obligations of the contractor

(1) In addition to compliance with the provisions of this contract, the Contractor has its own legal obligations under the GDPR; in this respect, it guarantees compliance with the following requirements in particular:

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

b) The Client and the Contractor shall cooperate with the supervisory authority in the performance of their tasks upon request.

c) Immediately informing the Client of any inspections and measures taken by the supervisory authority insofar as they relate to this contract. This also applies if a competent authority investigates the processing of personal data in the context of an administrative offense or criminal proceedings relating to the processing of personal data by the contractor.

d) If the Client is subject to an inspection by the supervisory authority, administrative offense or criminal proceedings, a liability claim by 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 the Client to the best of its ability.

e) The Contractor shall regularly monitor the internal processes and the technical and organizational 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 organizational measures taken vis-à-vis the client within the scope of its

control powers pursuant to Section 8 of this contract.

g) The Contractor shall report any breaches of personal data protection to the Client without delay in such a way that the Client can comply with its legal obligations, in particular in accordance with Art. 33, 34 GDPR. The Contractor shall prepare documentation on the entire process, which it shall make 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 towards 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 it, 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 provisions of the GDPR.

6. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision shall be understood as those services that relate directly 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 security services. Maintenance and testing services shall constitute a subcontracting relationship if they are provided for IT systems that are provided in connection with a service of the Contractor under this contract. However, the Contractor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the data protection and data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Contractor may only commission subcontractors (other processors) with the prior express written or documented consent of the Client, unless such a subcontracting relationship already existed when the service agreement pursuant to Section 2.1 of this contract was concluded. The Contractor shall inform the Client of all subcontracting relationships already existing at the time of conclusion of the service agreement pursuant to Section 2.1 of this contract upon request (text form is sufficient).

The client consents to the commissioning of subcontractors on the condition of a contractual agreement with the subcontractor in accordance with Art. 28 (2-4) GDPR. The contractual agreement shall be presented to the client upon request, with the exception of business clauses not related to data protection law.

A change of existing subcontractors is permitted, provided that the client does not explicitly object to the planned outsourcing in writing or in text form, a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is used as a basis and the change of the existing subcontractor does not fall below the existing security level. Changes to subcontracting relationships that already existed when the service agreement was concluded in accordance with section 2.1 of this contract will be communicated to the client on request (text form is sufficient). The client shall also be informed of any significant changes.

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

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

(5) Any further outsourcing by the subcontractor shall require the express consent of the main client (at least in text form). All contractual provisions in the contractual chain shall also be imposed on the additional subcontractor.

7. International data transfer

(1) Any transfer of personal data to a third country or to an international organization requires documented instructions from the client and requires compliance with the requirements for the transfer of personal data to third countries in accordance with Chapter V of the GDPR.

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.

If the client has exceptionally permitted a transfer of data to a third country to a subcontractor, the measures approved by the client to ensure an adequate level of protection under Art. 44 et seq. GDPR are specified as part of the subcontracting.

(2) If the client instructs the transfer of data 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 client

(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 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 Art. 28 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 organizational measures.

(3) Proof of the technical and organizational measures for compliance with the special requirements of data protection in general and those relating to the order can be provided by

- compliance with approved codes of conduct pursuant to Art. 40 GDPR;

- certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;

- Current certificates, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);

- suitable certification through an IT security or data protection audit (e.g. in accordance with BSI basic protection).

9. Authority to issue instructions and responsibility of the client

(1) The Contractor shall process personal data only on the basis of documented instructions from the Client, unless it is obliged to do so 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 are set out in this contract.

Order processing agreement of dtms GmbH according to GDPR

(2) The Contractor shall inform the Client immediately if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client.

(3) The client shall be solely responsible for assessing the permissibility of the data processing and for safeguarding the rights of the data subjects. The client shall ensure in its area of responsibility that the legally required preconditions (e.g. by obtaining declarations of consent for the processing of the data) are created so that the contractor can provide the agreed services without violating the law.

10. Remuneration

The Contractor's remuneration shall be based conclusively on the contractual relationship entered into under Section 2.1 regarding the Contractor's services and/or products in the context of which the data processing is carried out.

11. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be created without the client's knowledge. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data required to comply with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier at the request of the Client - but at the latest upon termination of the service agreement - the Contractor shall hand over to the Client all documents, processing and usage results and data pertaining to the contractual relationship that have come into its possession or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material. The deletion log must be submitted on request. Any statutory retention obligations or other obligations to store the data shall remain unaffected.

(3) The Client shall have the right to check that the data has been returned to the Contractor in full and in accordance with the contract and that it has been deleted. This can also be done by inspecting the data processing systems at the Contractor's premises. The on-site inspection shall be announced by the client with reasonable notice.

12. final provisions

(1) The parties agree that the defense of the right of retention by the Contractor within the meaning of § 273 BGB (German Civil Code) is excluded with regard to the data to be processed and the associated data carriers.

(2) Amendments and supplements to this agreement must be made in writing or in a documented electronic format. This also applies to the waiver of this formal requirement. The precedence of individual contractual agreements remains unaffected by this.

(3) Should individual provisions of this agreement be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions.

(4) This agreement is subject to German law. The exclusive place of jurisdiction is Mainz.

13. Object and purpose of the processing

(1) When commissioning the services and/or products of the Contractor listed below, the Contractor shall process data on behalf of the Client. The object and purpose of this processing, the type of personal data and the categories of data subjects are set out below. In addition, the subject matter of the processing results from the service agreement concluded between the parties in accordance with section 2.1 of this contract, its supplementary agreements and the respective current service description of the commissioned service/product.

a) dtms routing portal

The dtms routing portal is used to process calls via a routing and extended voice application with call routing and monitoring functions for calls to the customer's telephone numbers. The dtms routing portal includes routing options (e.g. origin, percentage, time of day/business hours), call recording and various types of statistics (CDR, quantities, quality, origin, multiple calls and personalized statistics). dtms provides the dtms routing portal in a German software environment (server location). Online access provides the option of viewing information on past calls as well as important key figures, including quantities, quality and origin, provided this function has been activated for the customer. The statistics type "CDR", which can be called up, stores the incoming and outgoing calls of the respective subscriber, including their A call number. Call recording only takes place in purely technical terms via the call management system (recording and generation of voice files).

b) digicom

The digicom call management system includes routing options (e.g. origin, percentage, daily/business hours) and queue functions (e.g. dynamic or fixed, prioritization, limitation), their monitoring, optional call recording and various types of statistics (group, agent, pilot, event or campaign-specific). The dashboard makes it possible to view all information about active calls as well as important key figures for waiting loops, groups, agents and service numbers at a glance at any time. Within the call management system, the respective caller data (including their A-call number and their incoming and outgoing calls) is stored in various statistics types and processed for the purposes specified by the client. This data can also be used for outbound calls. It is also possible to integrate e-mail, social media, chat services and machine-triggered events into the digicom call management system and route them specifically. Optional call recording takes place purely technically via the call management system (recording and generation of voice files). The data is transferred to the customer's SFTP server and stored there. Hosting and display of call recording data does not take place via the call management system, but always from the respective storage location.

c) Dialog Control and other IVR platforms

The DialogControl call management system and other IVR platforms include the functions of call routing and monitoring of calls to the client's / customer's telephone numbers. This includes call recording, HTTP requests (incl. Zendesk, Freshdesk integrations, transcription and summarization). Within the call management system, the respective caller data and the caller history are stored and used for various statistics types and routing options. Voice files can be created in the call management system if the end customer has given their consent. The voice files are then transferred from the call management system to an internal cloud storage solution (Cloud Analytics) or to the customer's SFTP server. Voice files are therefore not stored in the call management system but in the dtms cloud storage solution (Cloud Analytics) and at the customer's premises. During transcription and summarization (if activated), voice files are transmitted to third-party providers (e.g. open.AI or MS Azure). After transcription, the generated text file is stored in the call management system.

d) Multichannel ACD

The Multichannel ACD service regularly includes call routing functions, waiting loop functions, IVR menus, mailbox and call recording options. The individually configurable online monitor enables the client to have an

up-to-date overview of service hotlines, queues and agent groups at all times. Statistics can be called up online or sent automatically by e-mail. Graduated rights management enables any number of logins with individually assigned configuration, statistics and monitoring options. The multichannel ACD supports various channels such as email, webchat and various messenger services such as whatsapp, instagram and telegram.

e) Competition

In the case of the competition service, the object and purpose of the order is the organization of a competition or prize draw for the client on a telecommunications platform of the contractor. Participation takes place by telephone or SMS. The Contractor shall provide the Client with the participant data to determine the winners. This expressly does not include the measures of determining the winner, notifying the winner, sending the prizes or processing a cash prize. With regard to call recording for competitions, see section 1. g).

f) Cloud analytics

If the Contractor provides the Cloud Analytics service for the Client, data, in particular voice files, which may originate from various applications of the Contractor (e.g. DialogControl), shall be stored. These voice files are stored on a file server (NAS) of the Contractor. A technical audio analysis is also carried out in which the following is determined and graphically displayed on the basis of the recorded signals: Agent call share, caller call share, simultaneous speech, pauses and on-hold times. A-call numbers are always displayed anonymously both within the interface and in the file names. The client accesses the data in Cloud Analytics or logs in via an https-encrypted WebFronted by entering user-specific access data. If the storage capacity in Cloud Analytics commissioned by the client is no longer sufficient, the oldest data will be deleted. The data is also automatically deleted 180 days after the date of the call recording.

g) Call recording

The following applies if a call recording is made for the Client in connection with a service or application of the Contractor. In addition to call recording via the call management system in Cloud Analytics or in an SFTP server of the Customer, call recording may also take place in the case of competitions (e.g. when using online prize draws) or when using WebControl Media. WebControl Media is an online tool for configuring, controlling or evaluating the service numbers and IVR applications used by the customer. Online prize draw is an online tool used to determine the winners of

a competition. The storage of voice files when using WebControl Media or Online Winner Drawing takes place on a file server (NAS) of the Contractor. The customer logs in via an https-encrypted WebFronted by entering user-specific access data. After logging in, the customer can listen to and/or download the data, whereby random playback takes place when the winner is drawn. In the case of IVR applications, which can be set up by the Contractor on a customer-specific basis, the voice files generated in the application are made available by storing them on an SFTP server of the Customer, via a telephone monitoring service by random playback of voice files (e.g. prize draw) or as a so-called transcription service (sequential playback). It can also be accessed via the online tools described above. In the context of call recording, it is possible to transcribe the respective recordings (e.g. address data from competitions). The employees of a service provider transcribe the recordings and send the transcripts to the client. Within an IVR application, A call numbers are always displayed anonymously.

h) Call center service

If the Contractor provides the Client with the use of a call center, e.g. as part of the information 118xy service or in the entertainment sector, the call center service is not provided by the Contractor itself. The Contractor is not the operator of the call center and does not have a shareholding in the call center used. The client only uses this call center, which is operated by a third party, to provide entertainment services (e.g. eroticism, astrology) and/or to provide information to a caller who calls the respective information number. When providing information, the caller is primarily given the telephone number, person and/or company requested by the caller and, if requested by the caller, the call is forwarded to services on special destinations of the client. The provision of entertainment services in the erotic sector includes a moderated adult entertainment service in which the call center operators receive the preferences expressed by callers and, after identifying a suitable call partner, forward the call to them. It is also possible for callers to listen to the profile responses of potential call partners and be automatically transferred to them at the touch of a button. In the case of astrology services, callers can listen to the profile responses of advisors and can be automatically transferred to them at the touch of a button in order to receive life advice over the phone. Callers also have the option of being trans-

ferred directly to a counselor by entering a PIN. This PIN has been communicated in advance, for example via a website or by the counselor in a previous conversation, so that a direct connection can be established.

i) Transcription services

dtms uses a subcontractor for the transcription of call recordings. This service can be booked optionally by the client and must be agreed individually on a project-specific basis. The voice files generated in the application are made available on an SFTP server of the customer or on a dtms server in a German software environment. In the context of transcription services, A call numbers are always displayed anonymously.

j) Peak Control

Peak Control is an IVR application with an associated online tool. The IVR application is controlled as an overflow destination of an ACD application if no registered contact center agents are available. The caller is offered a callback by the contact center via Peak Control. They are asked to enter their full A-number. If the full A-number has already been transmitted, the caller is asked to give their consent to use the callback. In both cases, the A-number is stored on the IVR system. The client accesses or logs in to the "Peak Control" online tool via an https-encrypted web front-end by entering user-specific access data. After logging in, the client can view all callbacks carried out for him by the Peak Control system via the "Callback Monitor" menu item. Among other things, the complete A-number is displayed (for the purpose of making contact in the event of failed connection attempts, for example).

k) Customer Feedback

Customer Feedback is an IVR application with an associated online tool. The IVR application is used to request customer ratings by telephone for questions defined by the client. In certain question/answer constellations, an announced, voluntary response can be made by the caller (leave a free opinion). The customer rating and the audio (if one was recorded) are made available to the client via the "Customer Feedback" online tool. If the caller ID is suppressed, the A-number is provided to the customer in anonymized form. The client accesses or logs in to the "Customer Feedback" online tool via an https-encrypted web fronted by entering user-specific access data.

l) WebControl Media

WebControl Media is an IVR application with an associated online tool. The client can use the online tool to configure and activate telephone

competitions (for their service numbers) on an IVR basis. In this context, caller response audios can be generated for prize notifications. These audios can be listened to and downloaded by the customer via the online tool "WebControl Media". The full A-number will only be transmitted and stored if it has been transmitted by the A-participant. Access or login to the "WebControl Media" online tool is carried out by the client via an https-encrypted web fronted by entering user-specific access data.

m) Click2Call

Click2Call is an IVR application that allows callers to request a callback via a web widget (website plug-in) on the client's website. The complete A-number (for the purpose of a callback) must be entered. After entering the callback number and callback request, the IVR application initiates a call setup between the customer's contact center and the caller.

n) Junk call protection

Junk Call Protection is an IN application that allows customers to maintain a so-called blacklist for their service numbers. By entering certain digits on the customer's telephone keypad (e.g. the customer's contact center), the caller's transmitted A number is blocked for a certain period of time (max. 7 days) in the dtms intelligent network (IN). This applies to avoid unwanted calls (junk calls), e.g. for freephone numbers.

o) Sending SMS and faxes

The Client shall provide the Contractor with lists of telephone numbers to which SMS or fax messages are to be sent, together with further dispatch information (bulk/mass mailing). If advertising is to be sent, the Client shall be responsible for obtaining and documenting the legally required consent of the subscriber/recipient. The client only undertakes the technical dispatch and the corresponding evaluation.

p) Classification - Voicebot

The voicebot is a software application that can use artificial intelligence to understand human speech and respond to spoken input or requests. The bot can be used for various applications and can exchange data with third-party systems via interfaces if required. Among other things, the software offers a bot builder to design processes; the possibility to train "intentions" and define "entities" to enable the A.I. to recognize certain inputs. The software also makes it possible to forward calls to a desired destination (e.g. telephone number) and to make collected data ("call history, extracted data such as date of birth, etc.) available to other applications such as digicom and Dialog Control.

The software is provided to the client on an IT platform and can be administered by the client. The Contractor shall provide operation, care and maintenance of the software. If the Client provides the Contractor with the internally stored customer correspondence for AI training purposes, this must be done in anonymized form (by agreement).

q) Chatbot

The chatbot is a software application that can use artificial intelligence to understand and respond to user input. The bot can be used for various applications and can exchange data with third-party systems via interfaces if required. Among other things, the software offers a bot builder to design processes; the possibility to train "intentions" and define "entities" to enable the A.I. to recognize certain inputs. The software also makes it possible to forward conversations to a desired destination (e.g. digicom) and to make collected data ("conversation history, extracted data such as date of birth, etc.) available to other applications such as digicom. The chatbot offers various input channels, including web, WhatsApp, Facebook Messenger, etc. and can also play media files to the user in addition to text. The WebGUI has a function called "Inbox", which allows agents (i.e. users with access rights) to view past and current conversations and intervene in ongoing conversations, i.e. take them over from the bot. The software is provided to the client on an IT platform and can be administered by the client. The Contractor shall provide operation, care and maintenance of the software. If the Client provides the Contractor with the internally stored customer correspondence for AI training purposes, this must be done in anonymized form (by agreement).

r) Consulting & Development

The consulting and development service is an individual service of the Contractor, which results from the service description of the respective contract concluded. If this service involves the processing of personal data and section 1.3 does not apply, the provisions of this contract shall also apply.

s) Webbilling

The web billing payment method enables a payment process to be initiated via a website on the Internet. The payment process itself is triggered via the buyer's mobile device. The buyer is asked to enter their mobile phone number on the payment page on the Internet. After entering the mobile phone number, the buyer is directed to the contractor's payment platform. A TAN is generated

there and this is sent back to the end user's mobile device via SMS. The end user is then asked to enter the TAN on the payment website. If the end user enters the TAN on the website via which he has previously sent his mobile phone number, the payment process is triggered via the payment platform to the mobile network operator and the amount is billed to the end user by his mobile network operator via his mobile phone bill. The end user also receives access to the chargeable area or is provided with the purchased digital goods.

(2) The following types of data are regularly subject to processing:

- TKG data (inventory, traffic, location and usage data, individual connection data within the meaning of the Telecommunications Act (TKG))
- Communication data (e.g. CDR data, telephone data)
- Planning and control data related to telecommunications routing
- Data from customer feedback including associated voice data (e.g. voice files)
- Information
- Conversation history
- Billing data
- Performance, address and customer data

(3) The following group of persons affected by data processing regularly exists:

- Employees
- Interested parties
- Contact persons
- Shareholders
- Customers
- End users within the meaning of the TKG
- Suppliers