Technical and organisational measures (TOMs) of the Contractor

Data Protection Officer of the Contractor

The Contractor's Data Protection Officer is:

Andreas Bethke
Papenbergallee 34
25548 Kellinghusen, Germany

Telephone: +49 48 22 36 63 000
Fax: +49 48 22 36 63 333
Mob.: + 49 17 93 21 97 88
http://www.b3-unternehmensgruppe.de

The Contractor takes the following technical and organisational measures for data security within the meaning of Art. 32 GDPR:

1 Entry control

The Contractor denies unauthorised persons entry to the office, server and archive rooms. The following measures prevent unauthorised persons from gaining physical access to the processing facilities/rooms of personal data or other personal documents, e.g. files or data carriers:

- Entry to the buildings is secured by door locks and additionally by a so-called badge system (electronic entrance chip).
  The access control system ensures access only for authorised employees by means of the so-called "badge" and in each case in compliance with the following principles:
  the entity issuing a mobile personal storage and processing device or using a procedure for automated processing of personal data which takes place wholly or partly on such a medium, and which places this on the medium, modifies it or holds for this purpose, must inform the data subject via their identity and address, in a generally comprehensible form, of the functioning of the medium, including the nature of the personal data to be processed, of how to exercise their rights and of the measures to be taken in the event of loss or destruction of the medium in so far as the person concerned has not already become aware of it.
- Withdrawal of access means (badge) takes place after expiry of the authorisation and is recorded in writing by an employee of the internal sales service.
- The entrances to the offices in Mainz, Bonn and Hamburg are equipped with electronic door openers and by means of a security lock. Access control to the offices is granted via a security key and/or transponder. The distribution of the transponders and keys is documented.
- Data carriers and paper files of sensitive data are stored in lockable cabinets.

- The visitors' admission control takes place at the reception by personal control. External visitors have to check in and are personally escorted to the rooms in question during the visits. If information relevant to data protection can be viewed on the premises, a personal escort of the visitor takes place. A visitor policy regulates the handling of external visitors.
- In the event of an alarm, all staff must leave the building immediately. The doors are self-closing both in the offices and in the data centres, so that even after leaving the rooms it is ensured that no unauthorised access by third parties can take place.
- dtms uses its own server capacities, which are protected on the basis of a separate IT security concept (§ 166 TKG) (Frankfurt, Hamburg, Berlin, and Mainz locations). The accesses to the server rooms are provided with additional security. Only staff with the appropriate rights may enter this area.
- Access to outsourced data centres (Frankfurt, Hamburg, Berlin) is only possible after prior registration. Identity card checks are carried out. External visitors are only admitted in the company of a qualified member of staff.
  Separate house rules apply in each case. Some of the areas are under video surveillance.
- Remote access to the data centres is only permitted for selected technical staff, who can access the data centres via a separately secured virtual VPN tunnel access.
- The external data centre in Frankfurt, where the data for processing within the framework of AI and ACD digicom is also processed, is ISO 27001 certified and is subject to quality management in accordance with ISO 9001.
  The monitoring equipment of the data centre has an alarm system and video surveillance (24/7) in compliance with Section 4 of the German Federal Data Protection Act (BDSG).

  Care is taken to ensure that data within the scope of AI, ACD applications digicom and dialog control are processed exclusively within the EU. Attention is paid to the existence of effective access control measures.

2 Access control

The Contractor prevents IT systems from being used by unauthorised persons. This is done as follows:

- A password procedure is used (including special characters, minimum length, and regular change of password) to ensure that passwords meet the minimum security requirements. These are issued for the IT area (PC, printers, other hardware environment for office IT) by the sister company in Berlin – nexnet GmbH, specifically by the head of the IT department there. For the telecommunications area, they are issued by the Head of Technology in Hamburg).
- The passwords are subject to precise security specifications. The details are regulated by the password policy of dtms GmbH (e.g. minimum length 8 characters, compliance with which is technically checked and enforced). Furthermore, it is ensured that only employees of dtms GmbH have access to the areas required for their work. This is ensured by assigning appropriate rights in the office IT and telecommunications areas.
- A password change is enforced every 3 months by asking the employee to change their password. If this is not done after repeated requests, access will be blocked.

- Likewise, external USB interfaces are blocked and only enabled for employees who need this medium due to their professional activities. The handling of mobile devices is regulated in detail in the mobile device guidelines of dtms GmbH. Personal data must not be stored on mobile data carriers.
- The IT systems in the area of office IT and in the area of telecommunications are protected against viruses and malware by means of a firewall. This enables unauthorised access to be detected and prevented accordingly. In the e-mail access area, incoming e-mails are checked for viruses and malware and, if necessary, filed in a quarantine area.
- In addition to the firewall and virus scanner described above, dtms GmbH also has a so-called interface protection.
- The user account is blocked after three failed login attempts.
- The PCs in the IT and TC area are secured by automatic, password-protected screen and computer locks.
- There is a clear assignment of user accounts to the users.
- Sensitive systems, especially server systems, can only be used as an administrator.
- Personal data is only transferred within the company’s network (SSH, VPN) and is therefore secured.
- Access to the in-house VPN is only possible via certificate-based authentication. The allocation of authentications is regulated in the IT policy of dtms GmbH.
- The destruction of data carriers that are no longer required is carried out by means of controlled destruction by a qualified disposal company.
- If an employee leaves, the person concerned must return all access authorisations immediately upon leaving. This is logged.

3 Data access control

The Contractor ensures that the persons authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, changed or removed without authorisation during processing or use and after storage. This is done in the following way:

- Office IT ensures that differentiated authorisations (e.g. in the form of profiles, roles, transactions, objects) are granted as specified by the management. Employees only have access to areas within IT that are necessary and required for their respective activities. These authorisations are checked cyclically. The exact specifications are regulated by the IT guidelines of dtms GmbH.
- The evaluation, access, modification and deletion of personal data are controlled and recorded.
- There is an automatic block on IT systems if incorrect authentication has been carried out several times.
- Avoiding the concentration of functions – functions from administrative tasks are attributed to different qualified persons.
- If a member of staff leaves the company, all access authorisations are blocked immediately on departure.

4 Transmission control

The Contractor ensures that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during transport or storage on data carriers, and that it is possible to check and establish to which bodies personal data are intended to be transmitted by data transmission equipment. This is done in the following way:

- Data transmission is encrypted by means of SSH or SSL or, depending on the application, by a tunnel connection (VPN = Virtual Private Network)
- The interfaces of PCs are protected against access and coupling by unauthorised hardware and other technical devices.
- During data exchange, the transmission is secured by means of transport protocols (SSL) as standard.
- In the case of working from home, the data transmission is encrypted in the aforementioned sense; a transmission of data is only possible through a tunnel connection.
- The disposal of paper and data media in accordance with data protection regulations is carried out by a company qualified to do so.

5 Input control

The Contractor ensures that it can be subsequently checked and determined whether and by whom personal data have been entered into data processing systems, changed or removed. This is done in the following way:

- The input of who enters data into the systems is done through logging and log evaluation systems. In sensitive areas, it is recognisable from which PC with which access authorisation the data was entered, changed or deleted. For the area of Office IT, the Head of Office IT, his/her deputy and the Managing Directors have access to the logs. For the area of IT used in telecommunication, the Head of Technology and his/her deputy as well as the Managing Directors have access to the respective logs.
- The authorisation concept of dtms GmbH applies both in the area of office IT and in the area of telecommunications (IT guidelines of dtms GmbH)
- The authorisation concept ensures that employees only have access to the required data within the scope of their respective function in the company and only to the extent that is necessary and required for their activity in the company.
- Allocation of authorisations to resources worthy of protection is only requested and granted by persons authorised to do so.

6 Order control

The Contractor ensures that personal data processed on behalf of the Client are only processed in accordance with the Client's instructions and to fulfil the contractually defined purpose. This is done in the following ways:

- Obligation of employees to data secrecy.
- Processing of data takes place in the European Union and the European Economic Area.

- Existence of a contract for commissioned data processing pursuant to § 32 GDPR.

The processing of data within the meaning of and on the basis of the German Telecommunications Act (TKG) is carried out exclusively in accordance with the security concept within the meaning of Section 166 of the TKG. The processing of this data does not constitute order processing within the meaning of Section 28 of the GDPR.

7 Availability control

The Contractor ensures that personal data is protected against accidental destruction or loss. This is done through:

- Backup procedures / regular backup copies
- Monitoring the computer system
- Use of uninterruptible power supply (UPS) and emergency power generators in the data centre. Presence of air-conditioning and fire alarm system as well as overvoltage filter
- Separate storage
- Constantly updated virus protection/firewall
- Emergency plan

8 Pseudonymisation, storage, and deletion

8.1. General processing principles

The system of dtms GmbH is designed to comply with the general principles of the GDPR. The following principles must be observed.

8.1.1. Reservation of permission and purpose limitation

Data may only be processed by dtms GmbH or the authorised party if

- this is **legally permitted for** the specific purpose
- or the end customer has **consented (reservation of permission**).

Data processing for a specific purpose is therefore only permissible

- if this is **provided for in these instructions for action** (which comply with the TKG)
- or the **end customer** has **effectively consented** to this specific data processing. In this case, it must be checked on a case-by-case basis whether the customer has provided sufficient written or electronic consent (Art. 6 ff. GDPR).

In this context, the **requirement of limitation of purpose** must be observed in particular. A legal permission to process data or the consent of the end customer only applies for the specific purpose that the legal permission or the consent of the end customer expressly provides for. For the processing of data for further purposes, a new authorisation is required (legal authorisation or the consent of the end customer). In the case of concrete processing of data, it is therefore still necessary to check whether the legal permission or consent covers the intended processing purpose.

8.1.2. Prohibition of using combined consents

The offers of dtms GmbH as well as the offers of the service providers observe the prohibition of using combined consents, according to § 7 para. 4 GDPR. The data subjects must effectively be free to consent to further data processing for the purpose of advertising (by Dtms or the service providers) or to refuse this consent.

8.1.3. Data avoidance and data economy

The offer of dtms GmbH is aligned with the objectives of data avoidance and data economy, as by default only the CLI and/or the IP address are collected as well as the data of the end customers required for billing and the data of the service customers required.

8.1.4. Information

The service customers are informed about the type, scope, location and purpose of the collection, processing and use of personal data in the General Terms and Conditions and in the other information available on the Internet, among other places.

The end customers are informed by the service providers as well as their local exchange carriers in particular. Asserted rights (e.g. with regard to itemised bills for billing) are to be exercised vis-à-vis the subscriber network operator and shall be observed by the latter, also insofar as the services of the service providers are billed (cf. § 62 TKG). Furthermore, the end customers may be additionally informed about the use of personal data by the service providers used in their general terms and conditions, taking into account Section 305a No. 2b) of the German Civil Code (BGB).

8.1.5. Data transmission

The transfer of data to third parties is aligned with legal requirements (e.g. billing, transfer to supervisory authorities) according to the following schedules. Any **disclosure of** personal data to **third parties** beyond the scope of the legal permissions is **not permitted** without the express consent of the customer.

8.1.6 Third-party involvement

Third parties may only be involved in the collection and processing of personal data with a legal basis within the meaning of data protection law (TKG) or on the basis of the consent of the person concerned (prohibition with reservation of consent (section 2.1 of the data protection concept)).

Accordingly, third parties may be involved if

- a **legal permissibility provision of the German Telecommunications Act [TKG], in particular Section 10 (1) of the German Telecommunications and Telemedia Data Protection Act [TTDSG] (collection of fees)**, applies to the activity of the third party, or
- an **agreement on commissioned data processing has been concluded with the third party in accordance with the GDPR (Section 28 GDPR)**.

The prerequisites must be checked before involving third parties in data processing.

8.1.6. Special processing facts

Specification of the processing sequences

The following **data protection concept** is based on the data processing procedures as they arise and are to be carried out during the realisation of the services.
The following rules and regulations are mandatory.

8.2. Collection of the service provider’s inventory data upon conclusion of the contract

Upon **conclusion of the contract**, the following **data of the** service customer are to be collected and stored:

1. Name, address and the number(s) allocated to the service customer or the numbers or services to be implemented and, if applicable, porting data. Either the numbers already allocated to the service customer by another provider are to be collected and/or numbers are to be allocated (hereinafter “DA numbers”).
2. Other inventory data required for setting up and maintaining the service and for billing, insofar as this is necessary for the future provision of services and billing (e.g. type of services, tariffs, IVR data, VAT ID, tax number, bank code, account number, account holder, IBAN, BIC/SWIFT, etc.).
3. Consideration of the itemised bill request of the end customer to his service provider by dtms GmbH: option no itemised bill / yes complete itemised bill; this may be in electronic form. An itemised bill will only be issued if a formal “co-user declaration” according to § 10 para. 3 TTDSG is available.
4. After **termination of the contract**, the inventory data shall be deleted at the end of the calendar year following the termination (following the expired Section 35 (3) of the German Federal Data Protection Act (BDSG) old version as well as Section 95 (3) of TKG old version). If necessary, it is to be **blocked** if further storage is required for a total of **6/10 years** in accordance with the German Tax Code (AO) and the German Commercial Code (HGB). For this purpose, the data shall be blocked for contract processing and can only be accessed/processed, both electronically and physically, only by the managing director or his representative for purposes according to the AO and the HGB. Processing for other purposes is not permitted.
5. Information on inventory data shall only be provided in accordance with Section 8.3.2. Section 7

8.3. Collection and storage of traffic data for the provision of telecommunications services

8.3.1. Collection of traffic data

The following **traffic data** may be collected, processed and used by dtms GmbH for the **duration of the connection**, insofar as or because this is necessary for the provision of the telecommunications services (Section 9 (1) TTDSG):

1. the **CLI of** the end customer (caller number/ANR) and the desired destination number (BNR) (or, in the case of NGNs, the IP address of the ANR and BNR or the CNR)
2. Start and end or start and duration of the respective connection according to date and time
3. if necessary for service provision, the type of telecommunications service used by the end customer (usually via the destination number/BNR)
4. other traffic data necessary for the establishment and maintenance as well as for the billing of charges, insofar as these are necessary for the processing of calls – this also includes

signalling of the end customer's telephone number (CLIP) or suppression (CLIR), depending on what the end customer wants on a case-by-case basis. Independently of this, the caller number is always signalled at network level.

8.3.2. Deletion and further use of traffic data after the end of the connection

According to Section 9 (1) TTDSG, the aforementioned traffic data may **only** be **further processed** or **used** beyond the **end of the connection** if it is **necessary for** the following purposes:

1. **Billing data**: Preparation of the billing to the end customer (offline billing) with first collection of receivables – on behalf of the service providers

2. **Billing data**: Processing of complaints against certain service providers)

3. **Billing data**: Commercial dunning in offline billing**.**

4. **Billing data**: Collection and judicial assertion of claims. **Billing data**: Rating and invoice processing, as well as billing for certain service providers.

5. **Traffic data**: Combating abuse and detecting and eliminating disruptions. **Requests for information according to the Code of Criminal Procedure (StPO) and other laws**

6. **"Surveillance" under the TKG**

7. **Needs-based design of services if permissible under the TKG.**

8. **Interception circuits,** if ordered in accordance with the TKG.

9. **Surveillance measures according to the Order on Monitoring Telecommunications (TKÜV)** (e.g. foreign head surveillance)

If none of these constellations exist, the data must be deleted immediately after the end of the connection (Section 9 (1) sentence 2 of TTDSG).

Required billing data (Section 10 (1-4) of the TKG)

In the case of connections to telecommunications-based services, the following data (CDR) must therefore generally be **stored for billing purposes (Section 9 (1) in conjunction with Section 10 (1) TTDSG)**:

- the CLI and/or IP address of the ANR
- BNR or the called CNR
- Start and end or start and duration of the respective connection according to date and time
- Identification of the service (usually via the B-NR).

Data not required for billing purposes must be deleted immediately, unless they are to be stored due to another regulation of the TKG or specialised laws (e.g. the Code of Criminal Procedure, StPO) (Section 9 (1) in conjunction with Section 10 (1-4) TTDSG).

Dtms GmbH collects these billing data in its switches and stores them in the central billing database. From this database, dtms GmbH exports the traffic data that have accrued for the respective service providers and transmits these data to them via a secure VPN connection.
Permission is granted under section 9 (1) in conjunction with section 10 (1-3) of the TTDSG.

In addition, dtms GmbH uses this data for the billing of its own services with the service providers according to the German Teleservices Act TDG (see clause 9) and for the other purposes permitted in this concept (e.g. fault clearance according to § 12 TTDSG).

9 Separation control

The Contractor ensures that data collected for different purposes can be processed separately. There is no need for physical separation; logical separation of the data carriers is sufficient. This is done in the following way:

- If data is processed for different purposes, it is ensured that the processing is only carried out on a client-related basis for the respective data subject. The systems for end customer processing have an internal multi-client capability and are based on the respective purpose of the processing of the personal data (purpose limitation)
- Separation of functions / production / test
- Logical separation of personal data from different clients
- Identification of recorded data (file number, CRM and billing number)

10 Organisational control

The Contractor has appointed an (external) company Data Protection Officer in writing to monitor, control and advise on the implementation of data protection requirements. The advisory and control tasks are carried out free of instructions and audit results are documented in writing.

Contact details of the Data Protection Officer:

Data protection officer of the Contractor (see above)

Furthermore, the following measures were implemented by the Contractor:

- The employees entrusted with the data processing were obliged to maintain data secrecy.
- The employees entrusted with data processing were made aware of their obligation to maintain confidentiality about company and business secrets.
- The employees entrusted with data processing were familiarised with the provisions of the Federal Data Protection Act and other regulations on data protection in data protection training courses.
- Extra pair of eyes principle

11 Procedures for regular review, assessment and evaluation

The management has issued guidelines for data protection and information security and published them on the intranet for employees.

Employees are regularly trained in data protection, at least once per calendar year.

Employees are obliged by their employment contract to handle personal data confidentially and to respect the secrecy of telecommunications.

Technical measures for the implementation of data protection through technology design and through data protection-friendly default settings (Art. 25 of the GDPR) are not necessary, as the TKG contains additional and more restrictive regulations in this regard with respect to the handling of inventory and traffic data.

There are guidelines for employees on how to handle personal data.

Our fraud management system ensures that data breaches are identified and reported immediately.

Requests from data subjects are forwarded to a designated staff member for this purpose, who processes these requests in a timely manner and coordinates with the Data Protection Officer.

Dtms GmbH has corresponding directories of processing activities within the meaning of Art. 30 (1) and (2) GDPR for its processes within the scope of which personal data are processed.

Dtms has implemented a data protection management system (DPMS)

12 Remote maintenance control

<u>Only applicable if the Contractor carries out activities via remote maintenance access:</u>

The Client shall ensure through technical and organisational measures that only the personal data absolutely necessary for maintenance can be accessed.
The persons entrusted by the Contractor with maintenance work have been obliged to maintain data secrecy in accordance with the GDPR, the TKG and – where relevant – the German Federal Data Protection Act (BDSG). In the case of maintenance work, it must be ensured that access to the Client’s systems and the transmission/transfer of data can only take place in encrypted, pseudonymised or anonymised form.

The following measures have been implemented by the Contractor:

- Remote maintenance access is realised via an encrypted connection
- Logging of remote maintenance (staff, duration, reason)
- Exclusion of external access as far as is technically possible

13 Location(s) of data processing

The data processing carried out by the Contractor takes place at the following locations:

Any change in the locations where the Client's data are processed and/or used shall require the written consent of the Client.

Location of the Contractor's business premises:

- Taunusstrasse 57, 55118 Mainz;
- Konrad-Zuse-Platz 5, 53227 Bonn;
- Haferweg 38, 22769 Hamburg

Location of the Contractor's data centres:

- Wendenstr. 408, 20537 Hamburg;
- Reuchlingstrasse 10/11, 10553 Berlin;
- Kleyerstrasse 88-90, Frankfurt

14 Declaration of commitment to implement the TOMs

The Contractor confirms that it has implemented the technical and organisational measures for the protection of the Client's personal data prior to the commencement of data processing. The Contractor undertakes to ensure compliance with these requirements for the duration of the cooperation, to monitor them regularly, to document them and to make them available upon request by the Client.

The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. In doing so, the safety level of the defined measures must be attained. Significant changes shall be documented and the Client shall be informed immediately.