Appendix:

Data Processing Agreement pursuant to Art. 28 GDPR

§ 1 Scope and Definitions

1) This Data Processing Agreement ("**Agreement**") applies exclusively to the business relationship between GO TO KI GmbH and its business customers ("**Client**") and supplements the respective Project Agreement concluded and the General Terms and Conditions of GO TO KI GmbH.

2) In the event of any conflict between this Agreement and the Project Agreement or the General Terms and Conditions, this Agreement shall take precedence.

3) Terms and variations thereof used in this Agreement correspond to those used in the General Terms and Conditions of GO TO KI GmbH, unless otherwise or additionally provided below. The following terms apply in deviation from or in addition thereto:

- **"Client"**: Means the business customer, i.e. a natural or legal person wishing to use the services of GO TO KI GmbH.
- **"Contractor"**: Means GO TO KI GmbH, Schumannstraße 17, 10117 Berlin.
- **"Project Agreement"**: Means the agreement concluded between the Client and the Contractor on the use of the services of GO TO KI GmbH. The content of the Project Agreement is derived from the framework agreement and the individual orders agreed thereunder, supplemented by the General Terms and Conditions.
- **"Parties"**: Collective term for the Client and the Contractor.
- **"Agreement"**: Means this Data Processing Agreement pursuant to Art. 28 GDPR, including its annexes.

§ 2 Subject Matter and Duration of the Engagement

1) This Agreement specifies the data protection obligations of the Parties arising from the processing on behalf to be carried out by the Contractor for the Client for the purpose of providing the services under the Project Agreement. The subject matter of the engagement is therefore derived from the Project Agreement, to which reference is hereby made.

2) In addition, this Agreement applies to all activities that are related to the activities under the Project Agreement and in the course of which employees of the Contractor or third parties engaged by the Contractor may come into contact with personal data of the Client.

3) This Agreement shall enter into force upon conclusion of the Project Agreement. The term of this Agreement corresponds to the term of the Project Agreement. However, the obligations under this Agreement shall continue to apply after termination of the Project Agreement for as long as the Contractor has not returned, erased or otherwise destroyed all personal data of the Client in accordance with this Agreement.

§ 3 Specification of the Content of the Engagement

1) The nature and purpose of the processing of personal data by the Contractor on behalf of the Client are specifically described in the Project Agreement. Changes to the subject matter of processing and changes to procedures shall be agreed jointly between the Parties and laid down in writing or in a documented electronic format.

2) Within its area of responsibility, the Contractor shall ensure compliance with all statutory data protection provisions.

3) The contractually agreed data processing shall be performed primarily in a Member State of the European Union or in another State party to the Agreement on the European Economic Area. Insofar as the Contractor uses subcontractors based in a third country that process the Client's data processed on its behalf (also) in a third country, the Contractor shall ensure, by means of the measures required for this purpose within the meaning of Art. 44 et seq. GDPR, that an adequate level of data protection is guaranteed in the third country.

4) The Client hereby consents to the relocation of individual processing operations to the third countries listed in **Annex 1** (Subcontractors). For an overview of how an adequate level of data protection is ensured in the respective third country, reference is made to **Annex 1** (Subcontractors).

5) The following types of personal data are the subject of this data processing:

- Personal master data (e.g. name, date of birth, address, nationality)
- Communication data (e.g. telephone number, email)
- Audio inputs from users, text transcriptions generated therefrom and AI-generated responses; these may include, among other things:
  - Contract master data (e.g. contractual relationship, product or contract interest)
  - Customer history
  - Employee history
  - Appointment requests/appointment arrangements
  - Contract billing and payment data
  - Internal notes (e.g. notes relating to callers)
  - Health data (e.g. severe disability), marital status and/or ethnic origin, insofar as this information emerges from the communication
- Metadata (e.g. timestamps, technical logs)

- Professional information (e.g. title, specialty, employer or practice, professional registration number), including from publicly accessible sources and registers, with source reference
- Responses to surveys (e.g. by email, form or telephone)
- Segment assignments (e.g. segment, confidence, underlying evidence)
- Marketing consents and objections (e.g. blocking notes)
- User accounts (e.g. role, tenant assignment, login credentials)
- Content that users upload to or create in Campaign OS (e.g. knowledge base, briefings, campaign drafts)

6) The categories of data subjects affected by the processing include:

- End customers of the Client
- Prospective customers
- Suppliers and other business partners of the Client
- Employees and other contact persons of the Client
- Persons researched or surveyed on behalf of the Client (e.g. healthcare professionals), as well as third parties reached in the process (e.g. practice staff)

§ 4 Technical and Organisational Measures

1) Within its area of responsibility, the Contractor shall organise its internal operations in such a way that they meet data protection requirements. For this purpose, it shall ensure the security of data processing pursuant to Art. 28(3)(c) and Art. 32 GDPR, in particular in conjunction with Art. 5(1) and (2) GDPR. Overall, the measures to be taken are measures of data security and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the costs of implementation and the nature, scope and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32(1) GDPR, shall be taken into account. The specific measures taken by the Contractor are set out in **Annex 2** (Technical and Organisational Measures).

2) To demonstrate the measures taken, the Contractor may also present current attestations, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security or data protection audit [e.g. in accordance with BSI IT-Grundschutz]). Insofar as an audit by the Client reveals a need for adjustment, this shall be implemented by mutual agreement.

3) 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 security level of the specified measures must not be undercut. Material changes shall be documented.

§ 5 Client's Authority to Issue Instructions

1) The Client is responsible for compliance with the statutory provisions of data protection law, in particular for the lawfulness of the processing and for safeguarding the rights of data subjects. Statutory or contractual liability provisions as well as the responsibility of the Contractor as processor remain unaffected.

2) The Contractor processes personal data on behalf of the Client in accordance with the provisions of the Project Agreement. The Contractor and any person acting under the authority of the Contractor who has access to personal data may collect, process and use the data processed on behalf of the Client only on the basis of documented instructions from the Client, including the powers granted in this Agreement, unless they are required to process the data by law (Art. 29 GDPR). In such a case, the Contractor shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest

3) The Contractor shall not use the data for any other purposes and, in particular, is not entitled to disclose it to third parties. Copies and duplicates of data shall not be made without the knowledge of the Client. This excludes backup copies insofar as they are necessary to ensure proper data processing, as well as copies of data required to comply with statutory retention obligations.

4) The Client shall issue instructions in writing or in a documented electronic format (e.g. text form). In principle, instructions may also be given orally. However, oral instructions must be confirmed by the Client without undue delay in a documented manner (at least in text form).

5) The Contractor shall inform the Client without undue delay if it considers that an instruction infringes data protection provisions. The Contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client. If the Client confirms the instruction and directs the Contractor to carry out this instruction despite the Contractor's concerns regarding its possible unlawfulness, the Client shall indemnify the Contractor against all damages and costs incurred by the Contractor as a result of carrying out this instruction, should the instruction in fact prove to be unlawful and claims be asserted or a fine be imposed against the Contractor for this reason.

§ 6 Obligations of the Contractor

In addition to complying with the provisions of this engagement, the Contractor has statutory obligations pursuant to Art. 28 to 33 GDPR; in this respect, it shall in particular ensure compliance with the following requirements:

1) Where legally required to do so, the Contractor has appointed in writing a data protection officer who performs their duties in accordance with Art. 38 and 39 GDPR. Their contact details shall be communicated to the Client for the purpose of direct contact. Any change of data protection officer shall be communicated to the Client without undue delay.

2) The Contractor shall maintain confidentiality pursuant to Art. 28(3) sentence 2 (b) and Art. 32(4) GDPR. For this purpose, when performing the services under the Project Agreement, the Contractor shall only use employees who have been bound to confidentiality and who have previously been familiarised with the data protection provisions relevant to them. The confidentiality obligation shall continue to apply after termination of the activity.

3) Upon request of the competent supervisory authority, the Client and the Contractor shall cooperate in responding to such request.

4) The Contractor shall inform the Client without undue delay of inspections and measures by the supervisory authority insofar as they relate to this engagement. This also applies insofar as a competent authority is investigating the Contractor in the context of administrative offence or criminal proceedings with regard to the processing of personal data in the course of the processing on behalf.

5) Insofar as the Client, for its part, is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, a liability claim by a data subject or a third party, or any other claim in connection with the processing on behalf carried out by the Contractor, the Contractor shall support the Client appropriately to the best of its ability.

§ 7 Rectification, Restriction and Erasure of Data, Data Subject Rights

1) The Contractor may not rectify or erase the data processed on behalf of the Client, or restrict its processing, on its own authority, but only on the basis of documented instructions from the Client.

2) If a data subject contacts the Contractor directly regarding the rights referred to in para. 1 or in order to exercise their other data subject rights, the Contractor shall forward this request to the Client without undue delay and support the Client in responding to the request within the scope of its possibilities.

§ 8 Subcontracting

1) Subcontracting relationships within the meaning of this provision are understood to be those services that relate directly to the provision of the main service under this Agreement. This does not include ancillary services that the Contractor itself uses, e.g. telecommunications services, postal/transport services, maintenance and user support or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Contractor is obliged to put in place appropriate and legally

compliant contractual arrangements and control measures to ensure data protection and data security of the Client's data, even in the case of outsourced ancillary services.

2) The Client hereby grants its general authorisation for the use of subcontractors by the Contractor, provided that the following conditions are met, in particular that a contractual agreement in accordance with Art. 28(2)–(4) GDPR is in place in each case.

3) In particular, the Client consents to the engagement of the subcontractors used at the time of conclusion of the Agreement and listed in Annex 1 (Subcontractors).

4) The transfer of personal data of the Client to a subcontractor and the subcontractor's initial commencement of activities are only permitted once all requirements for subcontracting have been met, in particular a contractual agreement in accordance with Art. 28(4) GDPR.

5) The use or change of existing subcontractors is permissible insofar as:

   a) the Contractor notifies the Client of the engagement of a new subcontractor or a change (exchange or replacement) of subcontractors a reasonable time in advance in writing or in text form (email is sufficient), stating the planned date of the engagement or change, and

   b) the Client does not object to the planned engagement or change vis-à-vis the Contractor in writing or in text form by the end of the period specified by the Contractor in this notification (at least fourteen days from the date of receipt of the information referred to in lit. a), and

   c) a contractual agreement in accordance with Art. 28(4) GDPR is used as the basis.

6) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure admissibility under data protection law by means of appropriate measures. The same applies if service providers within the meaning of para. 1 sentence 2 are to be used.

7) The Contractor shall be liable to the Client for the data processing carried out by the subcontractors engaged by it as for its own services under this Agreement.

§ 9 Audit Rights of the Client

1) The Client has the right, in consultation with the Contractor, to carry out inspections or to have them carried out by auditors to be designated in individual cases, provided that these auditors are not competitors of the Contractor. It has the right to satisfy itself of the Contractor's compliance with this Agreement at the Contractor's business premises during normal business and operating hours, without disrupting operations, by means of spot checks, which as a rule are to be announced in good time, but which in the case of incident-related inspections may also be carried out at any time without prior notice.

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, upon request, with the information required to carry out an inspection and, in particular, to demonstrate the implementation of the technical and organisational measures.

3) Evidence of such measures, which do not relate solely to the specific engagement, may be provided by

- compliance with approved codes of conduct pursuant to Art. 40 GDPR;
- certification under an approved certification mechanism pursuant to Art. 42 GDPR;
- current attestations, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);
- appropriate certification by an IT security or data protection audit (e.g. in accordance with BSI IT-Grundschutz).

4) Should an on-site inspection at the Contractor's premises by the Client or an auditor commissioned by the Client be necessary, the Contractor may make the inspection conditional upon the prior signing of a non-disclosure agreement with regard to the data of third parties and the other business and trade secrets of the Contractor. The signing of a non-disclosure agreement is not required if the inspection is carried out by a data protection supervisory authority or another governmental supervisory authority. The Client is obliged to treat as confidential all knowledge of the Contractor's business secrets and data security measures obtained within the scope of the contractual relationship. This obligation shall survive the termination of this Agreement.

§ 10 Support Obligations of the Contractor

1) The Contractor shall support the Client in complying with the Client's obligations regarding the security of processing of personal data, notification obligations in the event of personal data breaches, data protection impact assessments and prior consultations (Art. 32 to 36 GDPR). The Contractor's support services include in particular

   a) ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible infringement due to security vulnerabilities and that enable relevant breach events to be detected immediately (cf. § 4 of this Agreement);

b) the obligation to report personal data breaches to the Client without undue delay. The Client shall therefore inform the Contractor without undue delay and in full if it detects errors or irregularities relevant under data protection law when reviewing the results of the engagement. In addition, the Contractor shall inform the Client without undue delay in the event of serious disruptions to operations, suspected data protection breaches or other irregularities affecting the Client's data in the processing of the Client's data. The Contractor shall take all necessary and reasonable measures to secure the affected data and to mitigate possible adverse effects for the Client;

c) the obligation to support the Client in fulfilling its duty to provide information to the supervisory authority and, where applicable, to the data subject, and to provide the Client with all relevant information in this context without undue delay;

d) supporting the Client in the context of any data protection impact assessment;

e) supporting the Client in the context of prior consultations with the supervisory authority.

2) For support services that are not included in the Project Agreement or are not attributable to misconduct on the part of the Contractor, the Contractor may claim reasonable remuneration.

§ 11 Erasure and Return of Personal Data or Destruction

1) Upon completion of the contractually agreed services, or earlier upon request by the Client – but at the latest upon termination of the services under the Project Agreement – the Contractor shall hand over to the Client all documents that have come into its possession, processing and usage results created, and data sets that are related to the contractual relationship, or, subject to prior consent, destroy them in a manner compliant with data protection law or erase the data, unless legitimate grounds within the meaning of Art. 17(3) GDPR preclude erasure. The same applies to test and scrap material. The Contractor is obliged to keep a record of the return or erasure of personal data or destruction of data carriers and to present it to the Client upon request.

2) Documentation serving as proof of data processing in accordance with the engagement and in a proper manner shall be retained by the Contractor beyond the end of the Agreement in accordance with the respective retention periods. The Contractor may hand it over to the Client at the end of the Agreement to discharge itself.

§ 12 Liability of the Parties

1) The Contractor shall be liable for the fulfilment of its obligations under this Agreement in accordance with the provisions of the Project Agreement. The liability arrangement agreed therein also extends to liability for breach of obligations under this Agreement.

2) In relation to the data subject, the liability provisions of Art. 82 GDPR apply. The Parties shall each indemnify one another against liability towards the data subject if one Party proves that it is not responsible for the circumstance that caused the damage to the data subject.

§ 13 Miscellaneous

1) The Contractor shall have no right of retention pursuant to § 273 of the German Civil Code (BGB) in respect of the data processed within the scope of the engagement.

2) Should the Client's data held by the Contractor be endangered by attachment or seizure, by insolvency or composition proceedings, or by other events or measures of third parties, the Contractor shall inform the Client thereof without undue delay. The Contractor shall inform all persons responsible in this context without undue delay that sovereignty over and ownership of the data lie exclusively with the Client as controller within the meaning of the GDPR.

3) The exclusive place of jurisdiction for all disputes in connection with this Agreement is Berlin, unless an exclusive statutory place of jurisdiction exists.

4) Should individual parts of this Agreement be invalid, this shall not affect the validity of the remainder of the Agreement.

5) The following annexes form an integral part of this Agreement:

- **Annex 1** – Subcontractors
- **Annex 2** – Technical and Organisational Measures

Annex 1 – Subcontractors

Subcontractor company name	Service	Country / location of data processing	Ensuring an adequate level of data protection
ElevenLabs	Speech recognition (Speech-to-Text) Generation of voice responses from text (Text-to-Speech)	USA	Certification under the EU-U.S. Data Privacy Framework
Deepgram	Speech recognition (Speech-to-Text)	USA	Conclusion of EU Standard Contractual Clauses
Microsoft Ireland Operations Limited, Dublin, Ireland (service: Azure OpenAI in Microsoft Foundry)	Processing of text inputs, generation of responses and creation of text embeddings using the following Azure OpenAI models: gpt-6.1-sol, gpt-6-sol, gpt-6-luna, gpt-5.6-sol, gpt-5.6-terra, gpt-5.6-luna, gpt-5.5, gpt-5.4, gpt-5.4-mini, gpt-5.4-nano, gpt-4o; Embeddings: text-embedding-3-large, text-embedding-3-small, text-embedding-ada-002. Successor versions of these model families are also covered, insofar as they are used in the same deployment types (column 3).	EU/EEA and Switzerland: processing exclusively in the Azure deployment types “Data Zone” (EU) or “Standard” or “Regional Provisioned” in an Azure region in the EU; the Data Zone EU follows the Microsoft EU Data Boundary. Deployment types with global processing (“Global”) are not used. Storage at rest in the region of the Azure resource (Germany West Central, Germany; Sweden Central, Sweden.)	Processing within the EU/EEA; insofar as processing takes place in Switzerland: adequacy decision of the EU Commission (Art. 45 GDPR, Decision 2000/518/EC). Contractual basis: Microsoft Products and Services Data Protection Addendum.
Pipecat Cloud (Daily, Co.)	Orchestration and execution of the voice agent pipeline	USA, but server locations within Germany/EU	n/a, otherwise: Certification under the EU-U.S. Data Privacy Framework
Amazon Web Services (AWS)	Hosting of the platform	Germany/EU	n/a

Subcontractor company name	Service	Country / location of data processing	Ensuring an adequate level of data protection
Amazon Web Services EMEA SARL, Luxembourg (service: Amazon Bedrock)	Processing of text inputs and generation of responses using the language models Claude Opus 5.5 and Claude Sonnet 5.5 (provider of the models: Anthropic; operated exclusively by AWS, without Anthropic having access to inputs and responses). Successor versions of these model families are also covered, insofar as they are used via the same EU inference profile.	EU/EEA, Switzerland and United Kingdom: processing exclusively via the EU inference profiles of Amazon Bedrock (identifier “eu.”); global inference profiles (“global.”) are not used.	Processing within the EU/EEA; insofar as processing takes place in Switzerland or the United Kingdom: adequacy decisions of the EU Commission (Art. 45 GDPR). Contractual basis: AWS Data Processing Addendum.
Google Firebase	Authentication and user management	USA	Certification under the EU-U.S. Data Privacy Framework
Google Cloud	Hosting of Campaign OS	EU	n/a
Vercel	Hosting of the Campaign OS web interface	USA, but server locations within Germany/EU	Conclusion of EU Standard Contractual Clauses
Twilio	Telephony (phone numbers, call connection, call recording)	USA	Certification under the EU-U.S. Data Privacy Framework

Annex 2 – Technical and Organisational Measures

1. Confidentiality

(a) Physical access control:

- **Technical measures:** Manual locking system, locking system with code lock, security locks, external doors with security fittings, doors with fixed knobs on the outside, video surveillance of the building/entrance.
- **Organisational measures:** Alarm chain process, key/transponder rules, visitors accompanied by employees, careful selection of cleaning services, policies on locking office rooms.

(b) System access control:

- **Technical measures:** Login with username + password, login with biometric data, two-factor authentication, anti-virus software on servers, anti-virus software on clients, anti-virus software on mobile devices, hardware firewall, intrusion detection systems, remote access via encrypted VPN, encrypted data carriers, encrypted notebook/tablet, automatic desktop lock, blocking of interfaces (USB, FireWire, etc.).
- **Organisational measures:** Use of a password policy, graduated permissions according to tasks, assignability of user profiles to individuals, restriction of access rights to the data that is necessary, automatic screen lock, user lockout after multiple incorrect password entries, minimum number of administrators, issuance of a policy on the use of teleworking workstations to ensure the same level of security as in the Contractor's business premises, central password allocation, "Delete/Destroy" policy, "Clean Desk" policy, Mobile Device Policy.

(c) Data access control:

- **Technical measures:** Logging of access to data, logging of access to applications, physical erasure of data carriers.
- **Organisational measures:** Use of authorisation concepts, management and review of user rights by administrators, process for revoking permissions after an employee leaves, process for adjusting permissions after an internal change of position, minimum number of administrators, issuance of a policy on the use of teleworking workstations to ensure the same level of security as in the Contractor's business premises.

(d) Data separation:

- **Technical measures:** Separation of test environment and production system, physical system separation (file servers, databases, applications), multi-tenant-capable applications.
- **Organisational measures:** Use of authorisation concepts, use of database permissions, purpose attributes for data records.

(e) Pseudonymisation and encryption of data:

- **Technical measures:** Pseudonymisation of data possible by separating attributable characteristics from the personal data in separate systems.
- **Organisational measures:** Internal policies on the application of pseudonymisation.

2. Integrity

(a) Input control:

- **Technical measures:** Logging of the entry, modification and deletion of data, manual or automated review of logs.
- **Organisational measures:** Process for reviewing logging, process for retaining log files, access rules for logs, list of applications used to enter, modify or delete data, assignability of usernames to the entry, modification and deletion of data, assignment of permissions to enter, modify and delete data.

(b) Transfer control:

- **Technical measures**: Email transport encryption (TLS 1.2 or 1.3), transport-encrypted data lines (such as sftp, https), VPN tunnelling of data lines (home office, remote sites), encryption of mobile data carriers, signature procedures, logging of data access, retrieval and transport, secure transport containers for mobile data carriers.
- **Organisational measures**: Review of access logs, data transfer in anonymised form, documentation of the recipients of data and of the duration of the planned provision or the deletion periods, policy on the use of mobile data carriers, process for reviewing logging, logging of the personal handover of data, care in the selection of transport personnel and vehicles.

3. Availability and resilience

- **Technical measures:** Fire and smoke detection system, server room monitoring of temperature and humidity, fire extinguishers in the server room, air-conditioned server room, flood protection, use of UPS, server power supply separate from the rest of the power supply, use of protective contact sockets, RAID system/hard disk mirroring, data protection safe (S60/S120 DIS), separate alarm system in the server room, redundant data storage/backup in separate fire protection zones, separate partitions for operating system and peripheral data, video surveillance of the server room.
- **Organisational measures:** Use of a data backup and recovery plan (3-2-1 principle), encryption of data backups, backup and recovery concept (fully documented), policy on the documentation and review of data backups, storage of a data backup in a secure location outside the building, regular tests of the recoverability of backups, no sanitary connections in or above the server room, separate partitions for operating systems and data.

4. Regular review, assessment and evaluation

- **Technical measures:** Software solutions for data protection management in use, central documentation of all data protection procedures and rules accessible to

employees as needed/authorised (e.g. wiki, intranet …), other documented security concept, A review of the effectiveness of the technical protective measures is carried out at least annually.

- **Organisational measures:** Internal data protection officer, employees trained and bound to confidentiality/data secrecy, regular awareness training for employees, at least annually, internal information security officer, The data protection impact assessment (DPIA) is carried out as required, The organisation complies with the information obligations under Art. 13 and 14 GDPR, a formalised process for handling access requests from data subjects is in place, data protection and information security guideline issued by management, policies for employees on the handling of personal data, process for reporting data protection breaches, maintenance of the record of processing activities pursuant to Art. 30 GDPR.

(a) Incident response plan:

- **Technical measures:** Use of intrusion detection solutions, use of intrusion prevention solutions, firewall with attack detection and blocking mechanisms, use of anti-virus solutions updated at least daily, use of anti-spam solutions for email, use of anomaly detection systems with distributed sensors, separation of network components, separability of network segments, backup internet connection, Separate alarm system in the server room, Redundant data storage/backup in separate fire protection zones, Separate partitions for operating system and peripheral data.
- **Organisational measures:** Process for detecting, reporting and documenting data protection and security incidents, process for involving IT service providers in security incidents, establishment of reporting chains for incidents, process for assigning responsibilities and deputies, crisis communication process, process for domain delisting with spam list providers in the event of blocking, involvement of the DPO and ISO in security incidents and data breaches.

(b) Data protection by default:

- **Technical measures**: Compliance with data minimisation, enabling the exercise of the right of withdrawal through technical measures.
- **Organisational measures:** Policies on compliance with data-protection-friendly default settings, process for establishing data-protection-friendly default settings.

(c) Order control:

- **Organisational measures:** Careful selection of the (sub)contractor with regard to data protection and data security, prior review of the technical and organisational measures taken by the (sub)contractor and their documentation, conclusion of necessary data processing agreements (DPA), inclusion of necessary safeguards for data transfers to third countries (EU Standard Contractual Clauses), where required, written instructions to the (sub)contractor, obligation of the (sub)contractor's employees to maintain data secrecy and confidentiality pursuant to § 203 of the German Criminal Code (StGB), where necessary, appointment of a data protection officer by the (sub)contractor where there is an obligation to appoint one, agreement of effective audit rights, rules on the engagement of further subcontractors, ensuring the destruction of personal data after termination of the engagement, In the case of longer-term cooperation: ongoing

monitoring of the (sub)contractor and its level of protection, rules on the cooperation of the (sub)contractor in the exercise of data subject rights, data protection breaches and inspections by the supervisory authority.