

INSTRUCTIONS FOR COMPLETING THE AGREEMENT

For the contractor:

1. Enter company data:

- Enter your company data in the contract header under "Processor". This includes the name of your company, the legal form, the address and the representative.

2. Information in the contract figures:

- Add the following items to the contract:
 - **1.1:** Indicate the subject of the order, i.e. what exactly you will be processing for the client.
 - **2.1:** Describe the nature and purpose of the data processing.
 - **2.2:** Indicate what type of personal data is processed (e.g. names, addresses, e-mail addresses).
 - **2.3:** List the categories of data subjects (e.g. customers, employees).
 - **5a):** Name your data protection officer or indicate if none is required.

3. Technical and organisational measures (TOM):

- Use the TOM proposed in **Appendix 1** as a template. You can also provide your own measures, provided they meet the requirements.

4. List of subcontractors:

- In **Appendix 2**, list all subcontractors that you will use to fulfil this order. This includes the name of the company, legal form, contact details, address and a brief description of the respective services.

5. Contact details for queries:

- Enter your contact details on the last page so that you can be contacted quickly if you have any queries.

6. Transmission of the completed contract:

- Send the completed contract to your contact person at DRK e.V. from whom you received this contract and also to the e-mail address datenschutz-gs@drk.de.

7. Feedback:

- You will receive feedback after the DRK e.V. has checked your application.

For the client (German Red Cross e.V.):

1. Responsibility for the conclusion of the contract:

- Ensure that a data processing agreement (DPA) is concluded for each order processing. Have the data protection officer check whether a contract is required.

2. Verification of the information provided by the contractor:

- Check that the information provided by the contractor in sections 1, 2 and 5 is correct and complete.

3. Final review by the data protection officer:

- Send the complete agreement including attachments to the data protection officer for final review via the e-mail address datenschutz-gs@drk.de.

4. Queries:

- If you have any questions, please contact the data protection officer of the DRK e.V. at the e-mail address datenschutz-gs@drk.de.

Thank you for your co-operation!

Data processing agreement

between

German Red Cross e.V.

Carstennstraße 58, 12205 Berlin,
represented by the Management Board,
represented by the Chairman (Secretary General) Christian Reuter

- **Controller** -

- hereinafter also referred to as the "**Client**" -

and

[Company Legal form
Address
represented by]

- **Processor** -

- hereinafter also referred to as "**Contractor**" -

1. Object and duration of the order

1.1. Object

☐ The subject matter of the order results from the agreement [name of the agreement, e.g. "Service Agreement"] dated DD.MM.YYYY. to which reference is made here (hereinafter: Service Agreement);

or

☐ On the basis of this contract, the data records provided by the controller are processed for the following purpose [description of the reason for processing, e.g. "to carry out marketing campaigns"].

1.2. Duration

The duration of this agreement corresponds to the term of the main contract. The Client may terminate this Agreement and the Main Agreement at any time without notice in the event of a serious breach by the Processor of data protection regulations or the provisions of this Agreement. A serious breach shall be deemed to exist in particular if the Processor

- uses the data of the controller for purposes other than those specified in this agreement;
- breaches an essential obligation arising from this agreement (e.g. in the event of data loss or the possibility of unauthorised access by third parties through fault).

Furthermore, the Controller shall be entitled to terminate this Agreement and the Main Agreement without notice even if the conditions set out in sentences 2 and 3 are not met if the Processor repeatedly breaches this Agreement. A repeated breach shall be deemed to have occurred if the Controller has notified the Processor of a breach at least twice in writing or in text form and the Processor has not remedied the breach within a reasonable period of time.

2. Concretisation of the order content

2.1. Nature and purpose of the intended processing of data

☐ The nature and purpose of the processing of personal data by the contractor for the client are specifically described in the service agreement dated DD.MM.YYYY .

or

☐ Detailed description of the subject matter of the contract with regard to the nature and purpose of the contractor's tasks: [insert detailed description].

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client in text form and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled. The appropriate level of protection

☐ is established by an adequacy decision of the Commission (Art. 45 (3) GDPR);

☐ is established by binding internal data protection regulations (Art. 46 para. 2 lit. b in conjunction with 47 GDPR);

☐ is established through standard data protection clauses (Art. 46 para. 2 lit. c and d GDPR);

☐ is established by approved rules of conduct (Art. 46 para. 2 lit. e in conjunction with 40 GDPR);

☐ is established by an authorised certification mechanism (Art. 46 para. 2 lit. f in conjunction with 42 GDPR);

☐ is produced by other measures [Description of the measures](Art. 46 para. 2 lit. a, para. 3 lit. a and b GDPR).

2.2. Type of data

☐ The type of personal data used is specifically described in the service agreement under [Description]

or

☐ The following data types/categories are subject to the processing of personal data:

- ☐ Personal master data
- ☐ Communication data (e.g. telephone, e-mail)
- ☐ Contract master data (contractual relationship, product or contract interest)
- ☐ Customer history
- ☐ Contract billing and payment data
- ☐ Planning and control data
- ☐ Information (from third parties, e.g. credit agencies)
- ☐ [Other additions]

2.3. Categories of affected persons

- ☐ The categories of data subjects affected by the processing are specifically described in the service agreement at

or

- ☐ The categories of data subjects affected by the processing include

- ☐ Customers
- ☐ Interested parties
- ☐ Subscribers
- ☐ Employees
- ☐ Suppliers
- ☐ Sales representative
- ☐ Contact person
- ☐ [Other additions]

3. Technical and organisational measures

3.1. Documentation and testing

The Contractor shall document the necessary technical and organisational measures before the start of processing and submit them to the Client for review (Annex 1). After acceptance by the client, the measures become the basis of the order. Any need for adjustments shall be implemented and documented by mutual agreement.

3.2. Regular verification of the measures

The Contractor shall provide written proof of compliance with the technical and organisational security measures at least every two years and at any time at the request of the Client. The proof shall include detailed descriptions of the measures, audit logs or certificates.

3.3. Security requirements in accordance with the GDPR

The contractor guarantees security in accordance with Art. 28 para. 3 lit. c and Art. 32 GDPR, in particular with regard to confidentiality, integrity, availability and resilience of the systems, taking

into account the state of the art, implementation costs, type, scope and purpose of the processing and the risk assessment in accordance with Art. 32 para. 1 GDPR.

3.4. Adjustments due to technical progress

Due to technical progress and expected developments in legislation, it may be necessary to adapt the technical and organisational measures taken. The Contractor is authorised to implement alternative adequate measures, provided that the security level of the specified measures is not undercut. Significant changes must be documented and communicated to the client immediately in writing. The Contractor undertakes to immediately implement any necessary adjustments to the technical and organisational measures in accordance with changed legal requirements.

4. Correction, restriction and deletion of data

- 4.1. The Contractor may only rectify, erase or restrict the processing of the data processed on behalf of the Client in accordance with documented instructions from the Client. If a data subject contacts the contractor directly, the contractor shall forward the request to the client without delay.
- 4.2. The Contractor shall ensure the rights of data subjects, in particular a deletion concept, the right to be forgotten, rectification, data portability and information in accordance with the documented instructions of the Client, insofar as this is technically possible and legally necessary.

5. Obligations of the contractor

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

a) Data Protection Officer

The Contractor shall appoint a data protection officer in accordance with Art. 38 and 39 GDPR. The Client shall be informed immediately of any change of data protection officer.

☐ Data Protection Officer [Name, organisational unit, telephone, e-mail]:

☐ The contractor is not obliged to appoint a data protection officer. Contact person: [Name, organisational unit, telephone, e-mail]

☐ The contractor based outside the Union appoints the following representative in accordance with Art. 27 para. 1 GDPR: [name, organisational unit, telephone, email]

b) Maintaining confidentiality

The Contractor shall only use employees who are bound to confidentiality and who have been familiarised with the relevant data protection regulations beforehand. Personal data shall only be processed in accordance with the client's instructions.

c) Cooperation with the supervisory authority

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

d) Information about control actions

The Contractor shall inform the Client immediately of any inspections and measures taken by an authority insofar as they relate to this order.

e) **Support for the client**

The Contractor shall support the Client to the best of its ability in the event of inspections by the supervisory authority, administrative offence or criminal proceedings, liability claims by data subjects or other claims in connection with the commissioned processing.

f) **Support with obligations pursuant to Art. 32 to 36 GDPR**

The processor supports the controller in the fulfilment of the obligations under Art. 32 to 36 GDPR.

6. Subcontracting relationships

6.1. Definition of subcontracting relationships

Subcontracting relationships within the meaning of this regulation are services that relate directly to the provision of the main service. This does not include ancillary services such as telecommunications services, postal/transport services, maintenance and user services or the disposal of data storage media. Even in the case of outsourced ancillary services, the contractor must make appropriate and legally compliant contractual agreements and take control measures to ensure the data protection and data security of the client's data.

6.2. Consent of the client

The commissioning of subcontractors by the Contractor requires the prior consent of the Client in text form. All existing subcontracting relationships shall be listed in **Annex 2** to this contract.

6.3. Selection and control

The Contractor shall carefully select subcontractors and check before commissioning and regularly during the term of the contract that they comply with the agreed data protection measures in accordance with Art. 32 GDPR. The result of the check must be documented and forwarded to the client on request.

6.4. Application of the contractual provisions

The Contractor shall ensure that the agreed regulations and instructions of the Client also apply to the subcontractor.

6.5. Data processing agreement with subcontractor

The contractor shall conclude an order processing contract with the subcontractor that fulfils the requirements of Art. 28 GDPR. The subcontractor shall have the same obligations to protect personal data as the contractor. A copy of the order processing contract will be sent to the client on request.

6.6. Control rights

The contractor shall ensure that the control rights of the client and the supervisory authorities also apply to the subcontractor and that corresponding contractual provisions are made.

6.7. Provision of the service outside the EU/EEA

If the subcontractor provides the service outside the EU/EEA, the contractor shall ensure that the service is permissible under data protection law by taking appropriate measures. The same applies to ancillary services in accordance with 6.1.

7. Control rights of the client

7.1. Audits by third parties

The client may have the audit carried out by a named third party (auditor). The performance of an audit must be announced in writing at least five (5) working days in advance. The Client shall not have access to data or information about other customers of the Contractor, cost information, quality audits, management reports or other confidential data that is not directly relevant to the agreed audit purposes. The Client undertakes to maintain strict confidentiality regarding the Contractor's business and trade secrets.

7.2. Obligation of the contractor to provide information

The Contractor shall ensure that the Client can verify compliance with the Contractor's obligations pursuant to Art. 28 GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and to provide evidence of the implementation of the technical and organisational measures.

7.3. Proof of suitable measures

Proof of the measures, which do not only concern the specific order, can be provided by suitable measures, including

- compliance with approved codes of conduct in accordance with 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).

7.4. Costs

No remuneration is payable for the exercise of control rights.

8. Authorisation of the client to issue instructions

8.1. Processing according to instructions

The contractor may only collect, use or otherwise process data within the scope of the main contract and in accordance with the client's instructions. This applies in particular to the transfer of personal data to a third country or to an international organisation.

8.2. Confirmation of verbal instructions

Verbal instructions must be confirmed by the client immediately in writing or in text form.

8.3. Information in the event of unlawful instructions

The Contractor shall inform the Client immediately if it is of the opinion that an instruction violates data protection regulations. The Contractor is authorised to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Client.

9. Deletion and return of personal data

9.1. Creation of copies

Copies or duplicates of the data will not be made without the client's knowledge, with the exception of backup copies for proper data processing and data for compliance with statutory retention obligations.

9.2. Return and deletion of data

After completion of the contractually agreed work or at the request of the client - at the latest upon termination of the service agreement - the contractor shall hand over to the client all documents, processing and utilisation results as well as data pertaining to the contractual relationship or destroy them with prior consent in accordance with data protection regulations. The same applies to test and scrap material. The deletion log must be submitted on request.

9.3. Storage of documentation

Documentation that serves as proof of proper data processing in accordance with the order shall be retained by the Contractor beyond the end of the contract in accordance with the statutory retention periods. The Contractor may hand over this documentation to the Client at the end of the contract in order to discharge the Client.

10. Remuneration

The Contractor's remuneration is based on the underlying main contract. The Contractor shall not be entitled to any additional remuneration for measures under this contract.

11. Liability, indemnity, contractual penalty

11.1. Liability of the processor

The processor shall be liable to the controller in accordance with the statutory provisions for all damages caused by culpable breaches of this agreement and of the statutory data protection provisions. This applies to breaches by the processor, its employees or persons commissioned by the processor in the provision of the contractual service. Any limitations of liability of the parties from the main contract shall not apply.

11.2. Compensation for damages and indemnification

The controller or processor shall be liable to the data subject for compensation for damages claimed by a data subject due to unauthorised or incorrect data processing within the scope of the contractual relationship in accordance with Art. 82 GDPR. The processor shall indemnify the controller internally against all claims for damages asserted against the controller due to a culpable breach of the obligations imposed on the processor or non-compliance with lawfully issued instructions from the controller. The processor bears the burden of proof that the damage is not due to its breach of duty and that it is not responsible for this.

11.3. Contractual penalty

If the processor violates the provisions of this agreement and/or the applicable data protection provisions, it undertakes to pay an appropriate contractual penalty. The amount of the contractual penalty shall be determined by the Controller at its reasonable discretion and shall be subject to review by the competent court in the event of a dispute. The assertion of further claims for damages remains unaffected by this.

12. Miscellaneous

- 12.1. In the event of contradictions between the provisions of this agreement and the provisions of the main contract, the provisions of this agreement shall take precedence.
- 12.2. Agreements on the technical and organisational measures as well as control and audit documents (also for subcontractors) must be kept by the contractor for their period of validity and subsequently for three full calendar years.
- 12.3. Amendments and supplements to this agreement must be made in writing and expressly state that they amend and/or supplement these provisions. This also applies to the waiver of the formal requirement.
- 12.4. Should the property and/or the personal data of the Client to be processed by the Contractor be jeopardised by third-party measures (e.g. seizure or confiscation), by insolvency or composition proceedings or by other events, the Contractor must inform the Client immediately.
- 12.5. The defence of the right of retention in accordance with § 273 BGB is excluded with regard to the data processed for the client and the associated data carriers.
- 12.6. Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

Place, date

Place, date

Client

Contractor

Appendix 1

Technical and organisational measures (TOM)

Organisations that collect, process or use personal data themselves or on their behalf must take the technical and organisational measures necessary to ensure compliance with the provisions of data protection legislation. Measures are only necessary if their cost is proportionate to the intended purpose of protection.

The above-mentioned organisation fulfils this requirement through the following measures:

1. Confidentiality

1.1. Access control

Measures that are suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data is processed or used. Access control measures that can be used to secure buildings and rooms include automatic access control systems, the use of chip cards and transponders, access control by doorman services and alarm systems. Servers, telecommunications systems, network technology and similar systems should be protected in lockable server cabinets. In addition, it makes sense to support access control with organisational measures (e.g. instructions to lock offices when absent).

Technical measures	Organisational measures
<input type="checkbox"/> Alarm system	<input type="checkbox"/> Key regulation / list
<input type="checkbox"/> Automatic access control system	<input type="checkbox"/> Reception / Reception / Porter
<input type="checkbox"/> Biometric access locks	<input type="checkbox"/> Visitors' book / Visitors' log
<input type="checkbox"/> Chip cards / transponder systems	<input type="checkbox"/> Employee / visitor badges
<input type="checkbox"/> Manual locking system	<input type="checkbox"/> Visitors accompanied by employees
<input type="checkbox"/> Security locks	<input type="checkbox"/> Careful selection of security personnel
<input type="checkbox"/> Locking system with code lock	<input type="checkbox"/> Careful selection of cleaning services
<input type="checkbox"/> Securing the building shafts	<input type="checkbox"/>
<input type="checkbox"/> Doors with knob outside	<input type="checkbox"/>
<input type="checkbox"/> Doorbell system with camera	<input type="checkbox"/>
<input type="checkbox"/> Video surveillance of the entrances	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.2. Access control

Measures that are suitable for preventing data processing systems (computers) from being used by unauthorised persons. Access control refers to the unauthorised prevention of the use of systems. Options include, for example, boot passwords, user IDs with passwords for operating systems and software products used, screensavers with passwords, the use of chip cards for logging in and the use of call-back procedures. In addition, organisational measures may also be necessary, for example to prevent unauthorised access (e.g. specifications for setting up screens, issuing guidance for users on choosing a "good" password).

Technical measures	Organisational measures
<input type="checkbox"/> Login with user name + password	<input type="checkbox"/> Manage user authorisations
<input type="checkbox"/> Login with biometric data	<input type="checkbox"/> Creating user profiles
<input type="checkbox"/> Anti-virus software server	<input type="checkbox"/> Centralised password assignment
<input type="checkbox"/> Anti-virus software clients	<input type="checkbox"/> Secure password" policy
<input type="checkbox"/> Anti-virus software for mobile devices	<input type="checkbox"/> Directive "Delete / Destroy"
<input type="checkbox"/> Firewall	<input type="checkbox"/> Clean desk" guideline
<input type="checkbox"/> Intrusion detection systems	<input type="checkbox"/> General data protection and / or security policy
<input type="checkbox"/> Mobile Device Management	<input type="checkbox"/> Mobile Device Policy
<input type="checkbox"/> Use of VPN for remote access	<input type="checkbox"/> Manual desktop lock" instructions
<input type="checkbox"/> Encryption of data carriers	<input type="checkbox"/>
<input type="checkbox"/> Encryption smartphones	<input type="checkbox"/>
<input type="checkbox"/> Enclosure lock	<input type="checkbox"/>
<input type="checkbox"/> BIOS protection (separate password)	<input type="checkbox"/>
<input type="checkbox"/> Locking external interfaces (USB)	<input type="checkbox"/>
<input type="checkbox"/> Automatic desktop lock	<input type="checkbox"/>
<input type="checkbox"/> Encryption of notebooks / tablet	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.3. Access control

Measures that ensure that those 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, modified or removed without authorisation during processing, use and after storage. Access control can be ensured, among other things, by suitable authorisation concepts that enable differentiated control of access to data. It is important to differentiate both the content of the data and the possible access functions to the data. Furthermore, suitable control mechanisms and responsibilities must be defined in order to document the granting and withdrawal of authorisations and to keep them up to date (e.g. when hiring, changing jobs, terminating employment). Particular attention must always be paid to the role and possibilities of administrators.

Technical measures	Organisational measures
<input type="checkbox"/> File shredder (min. level 3, cross cut)	<input type="checkbox"/> Use of authorisation concepts
<input type="checkbox"/> External document shredder (DIN 66399)	<input type="checkbox"/> Minimum number of administrators
<input type="checkbox"/> Physical deletion of data carriers	<input type="checkbox"/> Data protection vault
<input type="checkbox"/> Logging of access to applications, specifically when entering, changing and deleting data	<input type="checkbox"/> Management of user rights by administrators
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

1.4. Separation control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logically and physically separating the data.

Technical measures	Organisational measures
<input type="checkbox"/> Separation of production and test environment	<input type="checkbox"/> Control via authorisation concept
<input type="checkbox"/> Physical separation (systems / databases / data carriers)	<input type="checkbox"/> Definition of database rights
<input type="checkbox"/> Multi-client capability of relevant applications	<input type="checkbox"/> Data records are provided with purpose attributes
<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------

1.5. Pseudonymisation

The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures;

Technical measures	Organisational measures
<input type="checkbox"/> In the case of pseudonymisation: separation of the assignment data and storage in a separate and secure system (possibly encrypted)	<input type="checkbox"/> Internal instruction to anonymise / pseudonymise personal data as far as possible in the event of disclosure or even after expiry of the statutory deletion period
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

2. Integrity

2.1. Transfer control

Measures to ensure 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 verify and establish to which bodies personal data is intended to be transmitted by data transmission equipment. Encryption techniques and virtual private networks, for example, can be used to ensure the confidentiality of electronic data transmission. Measures for the transport and transfer of data carriers include transport containers with locking devices and regulations for the destruction of data carriers in accordance with data protection regulations.

Technical measures	Organisational measures
<input type="checkbox"/> E-mail encryption	<input type="checkbox"/> Documentation of the data recipients and the duration of the planned transfer or deletion periods
<input type="checkbox"/> Use of VPN	<input type="checkbox"/> Overview of regular call-off and transmission processes
<input type="checkbox"/> Logging of accesses and retrievals	<input type="checkbox"/> Disclosure in anonymised or pseudonymised form
<input type="checkbox"/> Secure transport containers	<input type="checkbox"/> Careful selection of transport personnel and vehicles

<input type="checkbox"/> Provision via encrypted connections such as sftp, https	<input type="checkbox"/> Personal handover with protocol
<input type="checkbox"/> Use of signature procedures	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

2.2. Input control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, changed or removed from data processing systems. Input control is achieved by logging, which can take place at various levels (e.g. operating system, network, firewall, database, application). It is also necessary to clarify which data is logged, who has access to logs, by whom and on what occasion/at what time these are checked, how long storage is required and when the logs are deleted.

Technical measures	Organisational measures
<input type="checkbox"/> Technical logging of the entry, modification and deletion of data	<input type="checkbox"/> Overview of which programmes can be used to enter, change or delete which data
<input type="checkbox"/> Manual or automated control of the logs	<input type="checkbox"/> Traceability of data entry, modification and deletion through individual user names (not user groups)
<input type="checkbox"/>	<input type="checkbox"/> Assignment of rights to enter, change and delete data on the basis of an authorisation concept
<input type="checkbox"/>	<input type="checkbox"/> Retention of forms from which data has been transferred to automated processing
<input type="checkbox"/>	<input type="checkbox"/> Clear responsibilities for cancellations

3. Availability and resilience

3.1. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss. This includes topics such as an uninterruptible power supply, air conditioning systems, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.

Technical measures	Organisational measures
<input type="checkbox"/> Fire and smoke detection systems	<input type="checkbox"/> Backup & recovery concept (formulated)

<input type="checkbox"/> Fire extinguisher server room	<input type="checkbox"/> Control of the backup process
<input type="checkbox"/> Server room monitoring Temperature and humidity	<input type="checkbox"/> Regular tests for data recovery and logging of results
<input type="checkbox"/> Air-conditioned server room	<input type="checkbox"/> Storage of backup media in a secure location outside the server room
<input type="checkbox"/> UPS	<input type="checkbox"/> No sanitary connections in or above the server room
<input type="checkbox"/> Protective socket strips server room	<input type="checkbox"/> Existence of an emergency plan (e.g. BSI IT-Grundschutz 100-4)
<input type="checkbox"/> Data protection safe (S60DIS, S120DIS, other suitable standards with swelling seal, etc.)	<input type="checkbox"/> Separate partitions for operating systems and data
<input type="checkbox"/> RAID system / hard disc mirroring	<input type="checkbox"/>
<input type="checkbox"/> Video surveillance server room	<input type="checkbox"/>
<input type="checkbox"/> Alarm message in the event of unauthorised access to the server room	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4. Procedures for regular review, assessment and evaluation

4.1. Data protection management

Technical measures	Organisational measures
<input type="checkbox"/> Software solutions for data protection management in use	<input type="checkbox"/> Internal / external data protection officer Name / Company / Contact details
<input type="checkbox"/> Central documentation of all procedures and regulations on data protection with access for employees as required / authorised (e.g. wiki, intranet ...)	<input type="checkbox"/> Employees trained and committed to confidentiality/data secrecy

<input type="checkbox"/> Security certification in accordance with ISO 27001, BSI IT-Grundschutz or ISIS12	<input type="checkbox"/> Regular sensitisation of employees: at least annually
<input type="checkbox"/> Other documented safety concept	<input type="checkbox"/> Internal / external information security officer Name / company Contact
<input type="checkbox"/> A review of the effectiveness of the technical protective measures is carried out at least once a year	<input type="checkbox"/> The data protection impact assessment (DPIA) is carried out as required
<input type="checkbox"/>	<input type="checkbox"/> The organisation fulfils its information obligations
<input type="checkbox"/>	<input type="checkbox"/> Formalised process for processing requests for information from data subjects is in place
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.2. Incident response management

Support in responding to security breaches

Technical measures	Organisational measures
<input type="checkbox"/> Use of firewall and regular updates	<input type="checkbox"/> Documented process for recognising and reporting security incidents / data protection breaches (also with regard to the obligation to report to the supervisory authority)
<input type="checkbox"/> Use of spam filters and regular updates	<input type="checkbox"/> Documented procedure for dealing with security incidents
<input type="checkbox"/> Use of virus scanners and regular updates	<input type="checkbox"/> Integration of <input type="checkbox"/> DPO and <input type="checkbox"/> ISB in security incidents and data breaches
<input type="checkbox"/> Intrusion Detection System (IDS)	<input type="checkbox"/> Documentation of security incidents and data protection violations, e.g. via ticket system
<input type="checkbox"/> Intrusion Prevention System (IPS)	<input type="checkbox"/> Formal process and responsibilities for the follow-up of security incidents and data breaches
<input type="checkbox"/>	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.3. Privacy-friendly default settings

Privacy by design / Privacy by default

Technical measures	Organisational measures
<input type="checkbox"/> No more personal data is collected than is necessary for the respective purpose	<input type="checkbox"/>
<input type="checkbox"/> Simple exercise of the data subject's right of cancellation through technical measures	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

4.4. Order control (outsourcing to third parties)

Measures that ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions. In addition to data processing on behalf of the client, this point also includes the performance of maintenance and system support work both on site and via remote maintenance. If the contractor uses service providers for the purposes of commissioned processing, the following points must always be agreed with them.

Technical measures	Organisational measures
<input type="checkbox"/>	<input type="checkbox"/> Prior review of the safety measures taken by the contractor and their documentation
<input type="checkbox"/>	<input type="checkbox"/> Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
<input type="checkbox"/>	<input type="checkbox"/> Conclusion of the necessary agreement on order processing or EU standard contractual clauses
<input type="checkbox"/>	<input type="checkbox"/> Written instructions to the contractor
<input type="checkbox"/>	<input type="checkbox"/> Obligation of the contractor's employees to maintain data secrecy

<input type="checkbox"/>	<input type="checkbox"/> Obligation to appoint a data protection officer by the contractor if there is an obligation to appoint one
<input type="checkbox"/>	<input type="checkbox"/> Agreement of effective control rights vis-à-vis the contractor
<input type="checkbox"/>	<input type="checkbox"/> Regulation on the use of additional subcontractors
<input type="checkbox"/>	<input type="checkbox"/> Ensuring the destruction of data after completion of the order
<input type="checkbox"/>	<input type="checkbox"/> In the case of long-term cooperation: Ongoing review of the contractor and its level of protection

Annex 2 - Subcontractors

For the processing of data on behalf of the client, the contractor utilises the services of third parties who process data on its behalf ("subcontractors"). These are the following companies:

Subcontractor 1

- **Company:** [name of the company]
- **Legal form:** [Legal form of the company]
- **Contact details:** [Telephone number, e-mail address]
- **Address for service:** [address]
- **Type of service:** [Brief description of the service]

Subcontractor 2

- **Company:** [name of the company]
- **Legal form:** [Legal form of the company]
- **Contact details:** [Telephone number, e-mail address]
- **Address for service:** [address]
- **Type of service:** [Brief description of the service]

Subcontractor 3

- **Company:** [name of the company]
- **Legal form:** [Legal form of the company]
- **Contact details:** [Telephone number, e-mail address]
- **Address for service:** [address]
- **Type of service:** [Brief description of the service]

Completed for the **APPLICANT** by:

Name

Function

Phone number

e-mail

Place, date

(Signature)

To be completed by the **CLIENT**:

Tested on by .

Result(s):

- ☐ There is still a need for clarification regarding
- ☐ There is no further need for clarification. The agreement can be concluded as it stands.

By signing this document, the employee of the GRC General Secretariat confirms that the data protection officer has carried out an audit with the aforementioned result.

Place, date

(Signature)