

NOTES ON COMPLETING THE AGREEMENT

Contractor:

1. As a contractor, please complete the details of your company in the contract header on processors as well as the details under points 1.1, 2.1., 2.2., 2.3 and 5a) as well as Annex 2.
2. The technical and organisational measures (TOM), Annex 1, are an aid. You can also provide the DRK e.V. with your own TOM.
3. Please also include your contact details on the last page for any enquiries.
4. Send the completed contract to your contact person at the DRK e.V. and also to the e-mail address datenschutz-gs@drk.de.
5. You will receive feedback from the DRK e.V. after the review has been completed.

Client (German Red Cross e.V.)

1. It is the responsibility of the person in charge at DRK e.V. to ensure that a contract for the processing of orders (AVV) is concluded. You can have the data protection officer check in advance whether a contract is required.
2. The information provided by the Contractor in relation to Clauses 1, 2 and 5 must be checked by you for accuracy of content.
3. The complete agreement, including the annex, is to be given to the Data Protection Officer via datenschutz-gs@drk.de for final review.

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

Thank you very much!

Agreement on job processing

between

German Red Cross e.V.

Carstennstraße 58, 12205 Berlin,

represented by the Board of Directors,

represented by the Chairman (General Secretary) Christian Reuter

- **Responsible** -

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

and

[Add: Name, company form

Address

represented by].

- **Processor** -

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

1. Subject and duration of the contract

1.1. Subject

- ☐ The subject of the contract results from the service agreement/SLA/...
..... dated DD.MM.YYYY., to which reference is made here
(hereinafter: Performance Agreement);

or

- ☐ The subject of the data handling contract is the performance of the following tasks by the
contractor: (definition of tasks).

1.2. Duration

The term of this Agreement shall correspond to the term of the Principal Contract. The Principal may terminate this Agreement as well as the Principal Contract at any time without notice if there is a serious breach of data protection provisions or the provisions of this Agreement by the Processor, if the Processor does not or only partially carries out an instruction of the Principal or if the Processor refuses control rights of the Controller in breach

of the Agreement. A serious breach shall be deemed to have occurred if the Processor uses the Controller's data for purposes other than those specified in this Agreement or breaches a material obligation under this Agreement (e.g. in the event of a loss of data or in the event of a culpable possibility of unauthorised access by third parties).

Furthermore, even if the requirements pursuant to sentences 2 and 3 are not met, the Controller is entitled to terminate this Agreement and the main contract without notice if the Processor repeatedly breaches this Agreement. The prerequisite for this is that the controller has previously notified the processor of the breach in writing or in text form (fax/e-mail).

2. Specification of the order content

2.1. Nature and purpose of the intended processing of data

- ☐ The type and purpose of the processing of personal data by the contractor for the client are specifically described in the service agreement of..... .

or

- ☐ More detailed description of the subject matter of the contract with regard to the nature and purpose of the contractor's tasks:

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. DS-GVO are fulfilled. The adequate 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 DS-GVO);
- ☐ is established by standard data protection clauses (Art. 46 para. 2 litt. c and d DS-GVO);
- ☐ is established by approved rules of conduct (Art. 46 (2) (e) in conjunction with 40 GDPR);
- ☐ is established through an approved certification mechanism (Art. 46 (2) (f) in conjunction with 42 GDPR);
- ☐ is produced by other measures: (Art. 46 para. 2 lit. a, para. 3 litt. a and b DS-GVO).

2.2. Type of data

- ☐ The type of personal data used is specifically described in the service agreement at:

or

☐ The following data types/categories (enumeration/description of the data categories) are the subject of the processing of personal data:

☐ Personal master data

☐ Communication data (e.g. telephone, e-mail)

☐ Contract master data (contractual relationship, product or contractual interest)

☐ Customer history

☐ Contract billing and payment data

☐ Planning and control data

☐ Information (from third parties, e.g. credit agencies, or from public directories)
directories)

☐ [Other additions]

2.3. Categories of persons concerned

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

or

☐ The categories of data subjects concerned by the processing include:

☐ Customers

☐ Interested parties

☐ Subscribers

☐ Employees

☐ Suppliers

☐ Sales representative

☐ Contact

☐ [Other additions]

3. Technical-organisational measures

- 3.1. The contractor shall document the implementation of the required technical and organisational measures before the start of the processing, in particular with regard to the specific execution of the order, and shall hand them over to the client for inspection (Annex 1). If the client accepts the documented measures, they shall become the basis of the contract. If the examination or an audit reveals a need for adaptation, this shall be implemented by mutual agreement.
- 3.2. The Contractor shall provide written evidence at least every two years and at any time at the Client's request that it complies with the technical and organisational security measures in accordance with the contract and the statutory provisions. The Contractor shall be obliged to provide the written evidence in such a way that the Client can comply with the inspection obligations incumbent upon it.
- 3.3. The contractor shall establish security pursuant to Art. 28 (3) lit. c, 32 DS-GVO, in particular in connection with Art. 5 (1), (2) DS-GVO. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs 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 Article 32(1) of the GDPR must be taken into account.
- 3.4. Due to technical progress and expected developments in legislation, it may be necessary to adapt the technical and organisational measures taken. 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. Significant changes shall be documented and communicated to the Client without delay. The Contractor shall implement the necessary adaptations of the technical and organisational measures to the changed legal requirements without delay.

4. Correction, restriction and deletion of data

- 4.1. The contractor may not correct, delete or restrict the processing of data processed under the contract on its own authority, but only in accordance with documented instructions from the client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.
- 4.2. The rights of the data subjects, in particular a deletion concept, the right to be forgotten, correction, data portability and information in accordance with documented instructions from the client, must be ensured directly by the contractor; insofar as this is technically possible and legally necessary.

5. Quality assurance and other obligations of the contractor

In addition to compliance with the provisions of this Order, the Contractor shall have statutory obligations pursuant to Articles 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

- a) Written appointment of a data protection officer who performs his or her activities in accordance with Art. 38 and 39 DS-GVO. The Client shall be informed immediately of any change of data protection officer.

☐ The data protection officer at the contractor is *[Enter: Mr./Mrs. first name, surname, organisational unit, telephone, e-mail]*. has been appointed. The Client shall be informed immediately of any change of data protection officer. The current contact details of the data protection officer are easily accessible on the Contractor's homepage.

or

☐ The Contractor is not obliged to appoint a data protection officer. The contact person at the contractor shall be *[Enter: Mr/Mrs First name Surname, Organisational unit, Telephone, E-mail]* shall be appointed.

or

☐ As the Contractor has its registered office outside the Union, it shall appoint the following representative in accordance with Article 27(1) of the GDPR in the Union:*[enter: first name, last name, organisational unit, telephone, e-mail]*.

- b) The maintenance of confidentiality pursuant to Art. 28 (3) sentence 2 lit. b, 29, 32 (4) DS-GVO. When carrying out the work, the contractor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarised with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may process this data exclusively in accordance with the Client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.
- c) The implementation of and compliance with all technical and organisational measures required for this order in accordance with Art. 28 (3) sentence 2 lit. c, 32 DS-GVO (Annex 1).
- d) The contracting authority and the contractor shall cooperate with the supervisory authority in the performance of its duties upon request.
- e) The immediate information of the client about control actions and measures of the supervisory authority, insofar as they relate to this order. 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 during the commissioned processing.
- f) Insofar as the Client, for its part, is exposed to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.
- g) Verifiability of the technical and organisational measures taken vis-à-vis the Client within the scope of its supervisory powers pursuant to Clause 7 of this Agreement.

6. Subcontracting relationships

- 6.1. Subcontracting relationships within the meaning of this provision shall be understood to be those services which relate directly to the provision of the main service. This does not include ancillary services which the contractor uses, for example, as telecommunications services, postal/transport services, maintenance and user service 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 take appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the client's data also in the case of outsourced ancillary services.

- 6.2. The commissioning of subcontractors by the Contractor is only permissible with the consent of the Client in text form. The Contractor shall specify all subcontracting relationships already existing at the time of conclusion of the contract in Annex 2 to this contract.
- 6.3. The Contractor shall carefully select the subcontractor and check before commissioning that the subcontractor can comply with the agreements made between the Client and the Contractor. In particular, the contractor shall check in advance and regularly during the term of the contract that the subcontractor has taken the technical and organisational measures required under Art. 32 GDPR to protect personal data. The result of the control shall be documented by the contractor and communicated to the client upon request.
- 6.4. The Contractor shall be obliged to obtain confirmation from the subcontractor that the latter has appointed a company data protection officer in accordance with Article 37 of the Data Protection Act. In the event that no data protection officer has been appointed at the subcontractor, the Contractor shall point this out to the Client and provide information to the effect that the subcontractor is not legally obliged to appoint a data protection officer. Sentences 1 and 2 shall apply mutatis mutandis to a representative pursuant to Article 27 of the GDPR.
- 6.5. The Contractor shall ensure that the regulations agreed in this contract and, if applicable, supplementary instructions of the Client also apply to the subcontractor.
- 6.6. The contractor shall conclude a contract processing agreement with the subcontractor that complies with the requirements of Art. 28 GDPR. In addition, the contractor shall impose the same personal data protection obligations on the subcontractor as are laid down between the client and the contractor. A copy of the commissioned data processing contract shall be provided to the Client upon request.
- 6.7. The Contractor is in particular obliged to ensure by contractual provisions that the control powers (Clause 7 of this Contract) of the Client and of supervisory authorities also apply to the subcontractor and that corresponding control rights of the Client and supervisory authorities are agreed.
- 6.8. If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.

7. Control rights of the principal

- 7.1. The Client shall have the right, in consultation with the Contractor, to carry out inspections of this Agreement or to have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time.
- 7.2. The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations pursuant to Art. 28 of the GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.
- 7.3. Evidence of such measures, which do not only concern the specific order, can be provided by appropriate measures. These include in particular:

- compliance with approved rules of conduct in accordance with Art. 40 DS-GVO;
- certification in accordance with an approved certification procedure pursuant to Art. 42 DS-GVO;
- current attestations, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors);
- suitable certification by IT security or data protection audit (e.g. according to BSI-Grundschutz).

7.4. The contractor may claim remuneration for enabling inspections by the client.

8. Notification of infringements by the contractor

8.1. The Contractor shall assist the Client in complying with the personal data security obligations, data breach notification obligations, data protection impact assessments and prior consultations referred to in Articles 32 to 36 of the GDPR. This includes, among others

- a) ensuring an adequate 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 potential security breach and allow for the immediate detection of relevant breach events,
- b) the obligation to report personal data breaches to the principal without delay,
- c) the obligation to assist the principal within the scope of his duty to inform the data subject and, in this context, to provide him with all relevant information without delay,
- d) the support of the client for its data protection impact assessment; and
- e) the support of the principal in the context of prior consultations with the supervisory authority.

8.2. The Contractor may claim remuneration for support services that are not included in the service description or are due to misconduct on the part of the Client.

9. Authority of the principal to issue instructions

9.1. The client shall confirm verbal instructions without delay (at least in text form).

9.2. The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client.

10. Deletion and return of personal data

10.1. Copies or duplicates of the data shall not be made without the knowledge of the client. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data required with regard to compliance with statutory retention obligations.

10.2. After completion of the contractually agreed work or earlier upon request by the Client - at the latest upon termination of the service agreement - the Contractor shall hand over to the Client or, after prior consent, destroy in accordance with data protection law all documents, processing and utilisation results produced and data files which have come into its possession and which are

connected with the contractual relationship. The same shall apply to test and reject material. The protocol of the deletion shall be submitted upon request.

- 10.3. Documentation which serves as proof of the orderly and proper data processing shall be kept by the contractor beyond the end of the contract in accordance with the respective retention periods. He may hand them over to the Client at the end of the contract to relieve him of the burden.

11. Remuneration

The remuneration of the Processor results from the underlying main contract. The Contractor shall not be entitled to any remuneration for the implementation of measures specified in Article 28 of the GDPR and in this contract, in particular in accordance with sections 4, 7 and 9.

12. Liability, indemnification, contractual penalty

- 12.1. The Processor shall be liable to the Controller in accordance with the statutory provisions for all damage caused by culpable breaches of this Agreement as well as of the statutory data protection provisions applicable to it, which the Processor, its employees or those commissioned by it to perform the contract cause during the provision of the contractual service. Any limitations of liability of the parties (e.g. from the main contract) shall not apply in this respect.
- 12.2. The data controller or the processor shall be responsible to the data subject for compensation for damages claimed by a data subject due to inadmissible or incorrect data processing under the BDSG or the GDPR or other data protection regulations within the scope of the contractual relationship pursuant to Article 82 of the 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 by data protection regulations or due to the Processor's failure to comply with instructions lawfully issued by the Controller. The Processor shall bear the burden of proof for compliance with the obligations imposed on the Processor by data protection regulations and the observance of lawfully issued instructions of the Controller. The processor shall also bear the burden of proof for the fact that the damage is not based on its breach of duty and that it is not responsible for it.
- 12.3. In the event that the Processor breaches the provisions of this Agreement and/or the applicable data protection provisions, the Processor undertakes to pay an appropriate contractual penalty. The amount 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 shall remain unaffected.

13. Other

- 13.1. In the event of any inconsistency between the provisions in this Agreement and the provisions of the Main Contract, the provisions of this Agreement shall prevail.
- 13.2. Agreements on technical and organisational measures as well as control and audit documents (also on subcontractors) shall be kept by the contractor for their period of validity and subsequently for three full calendar years.

- 13.3. Amendments and supplements to this agreement must be made in writing and must expressly state that they amend and/or supplement these provisions. This also applies to the waiver of this formal requirement.
- 13.4. Should the property and/or the personal data of the Client to be processed at the Contractor be endangered by measures of third parties (for example by attachment or seizure), by insolvency or composition proceedings or by other events, the Contractor shall notify the Client without delay.
- 13.5. The defence of the right of retention within the meaning of § 273 of the German Civil Code (BGB) shall be excluded with regard to the data processed for the Client and the associated data carriers.
- 13.6. Should individual parts of this agreement be invalid, this shall not affect the validity of the rest of the agreement.

Place, date

Place, date

Client

Contractor

Enclosure 1

Technical and organisational measures (TOM)

Organisations that collect, process or use personal data themselves or on behalf of others shall take the technical and organisational measures necessary to ensure the implementation of the provisions of the data protection laws. Measures are only necessary if their effort is in a reasonable relation to the intended protective purpose.

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

1. Confidentiality

1.1. Access control

Measures suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data are 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 gatekeepers and alarm systems. Servers, telecommunications systems, network technology and similar equipment should be protected in lockable server cabinets. In addition, it makes sense to support access control through organisational measures (e.g. service instructions that provide for the locking of service rooms during absences).

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 / Gatekeeper
<input type="checkbox"/> Biometric access barriers	<input type="checkbox"/> Visitors' book / Visitors' log
<input type="checkbox"/> Chip cards / transponder systems	<input type="checkbox"/> Employee / visitor passes
<input type="checkbox"/> Manual locking system	<input type="checkbox"/> Visitors accompanied by staff
<input type="checkbox"/> Security locks	<input type="checkbox"/> Care in the selection of security guards
<input type="checkbox"/> Locking system with code lock	<input type="checkbox"/> Care in the 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"/> Bell 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 suitable for preventing data processing systems (computers) from being used by unauthorised persons.

Access control refers to the unauthorised prevention of the use of equipment. Possibilities are, for example, boot password, user ID with password for operating systems and software products used, screen saver with password, the use of chip cards for logging in as well as the use of call-back procedures. In addition, organisational measures may also be necessary, for example, to prevent unauthorised access (e.g. guidelines for setting up screens, issuing guidance to users on how to choose a "good" password).

Technical measures	Organisational measures
<input type="checkbox"/> Login with username + password	<input type="checkbox"/> Manage user permissions
<input type="checkbox"/> Login with biometric data	<input type="checkbox"/> Create user profiles
<input type="checkbox"/> Anti-Virus Software Server	<input type="checkbox"/> Central password assignment
<input type="checkbox"/> Anti-Virus Software Clients	<input type="checkbox"/> Secure Password Policy
<input type="checkbox"/> Anti-virus software mobile devices	<input type="checkbox"/> Delete / Destroy Policy
<input type="checkbox"/> Firewall	<input type="checkbox"/> Clean desk policy
<input type="checkbox"/> Intrusion detection systems	<input type="checkbox"/> General Policy Data Protection and / or Security
<input type="checkbox"/> Mobile Device Management	<input type="checkbox"/> Mobile Device Policy
<input type="checkbox"/> Use 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"/> Housing 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. In doing so, 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. in case of hiring, change of job, termination of employment). Special attention must always be paid to the role and possibilities of the administrators.

Technical measures	Organisational measures
<input type="checkbox"/> 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 safe
<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 logical and physical separation of the data.

Technical measures	Organisational measures
<input type="checkbox"/> Separation of productive and test environment	<input type="checkbox"/> Control via authorisation concept
<input type="checkbox"/> Physical separation (systems / databases / data carriers)	<input type="checkbox"/> Setting database rights

<input type="checkbox"/> Multi-client capability of relevant applications	<input type="checkbox"/> Data sets 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 way 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 by unauthorised persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment. Encryption techniques and virtual private networks, for example, can be used to ensure confidentiality in electronic data transmission. Measures for the transport or transfer of data media include transport containers with locking devices and regulations for the destruction of data media in accordance with data protection.

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 retrieval and transmission operations
<input type="checkbox"/> Logging of accesses and retrievals	<input type="checkbox"/> Disclosure in anonymised or pseudonymised form
<input type="checkbox"/> Safe transport containers	<input type="checkbox"/> Care in the 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 can be subsequently checked and determined whether and by whom personal data have been entered into, changed or removed from data processing systems. Input control is achieved by logging, which can take place at different levels (e.g. operating system, network, firewall, database, application). It must also be clarified 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 deletion of the logs takes place.

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 entry, modification and deletion of data through individual user names (not user groups)
<input type="checkbox"/>	<input type="checkbox"/> Allocation 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 have been transferred to automated processing operations
<input type="checkbox"/>	<input type="checkbox"/> Clear responsibilities for deletions

3. Availability and resilience

3.1. Availability control

Measures that ensure that personal data is protected against accidental destruction or loss. This includes topics such as an uninterruptible power supply, air conditioning, 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 the backup media in a safe place 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 swell seal etc.)	<input type="checkbox"/> Separate partitions for operating systems and data
<input type="checkbox"/> RAID system / hard disk mirroring	<input type="checkbox"/>
<input type="checkbox"/> Video surveillance server room	<input type="checkbox"/>
<input type="checkbox"/> Alarm message in case of unauthorised access to 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 according to need / authorisation (e.g. wiki, intranet ...)	<input type="checkbox"/> Staff trained and committed to confidentiality/data secrecy
<input type="checkbox"/> Security certification according to ISO 27001, BSI IT-Grundschutz or ISIS12	<input type="checkbox"/> Regular awareness-raising 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 annually.	<input type="checkbox"/> The data protection impact assessment (DPIA) is carried out as required
<input type="checkbox"/>	<input type="checkbox"/> The organisation complies with the information requirements
<input type="checkbox"/>	<input type="checkbox"/> Formalised process for handling 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 updating	<input type="checkbox"/> Documented process for the detection and notification of security incidents / data protection breaches (also with regard to the obligation to notify the supervisory authority)
<input type="checkbox"/> Use of spam filters and regular updating	<input type="checkbox"/> Documented procedure for dealing with security incidents
<input type="checkbox"/> Use of virus scanner and regular updating	<input type="checkbox"/> Involvement of <input type="checkbox"/> DPO and <input type="checkbox"/> IPM 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 follow-up on 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 withdrawal 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 in the sense of commissioned processing, the following points must always be regulated with them.

Technical measures	Organisational measures
<input type="checkbox"/>	<input type="checkbox"/> Prior review of the security 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 commissioned 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 on effective control rights vis-à-vis the contractor
<input type="checkbox"/>	<input type="checkbox"/> Regulation on the use of further subcontractors
<input type="checkbox"/>	<input type="checkbox"/> Ensuring the destruction of data after completion of the order
<input type="checkbox"/>	<input type="checkbox"/> In case of longer cooperation: Ongoing review of the contractor and its level of protection

Annex 2 - Subcontractor

For the processing of data on behalf of the Client, the *Contractor shall use the* services of third parties who process data on its behalf ("subcontractors").

This involves the following company or companies:

Here, all companies with company name, legal form, contact details and summonable address are to be stated by the contractor. Furthermore, the type of service must be briefly described.

1. *Subcontractor 1*
2. *Subcontractor 2*
3. *Subcontractor 3*

Completed for the CONTRACTOR by:

Name

Function

Phone number

E-mail

Place, date

(signature)

To be completed by the CONTRACTOR:

Tested on by (Data Protection Officer).

Result(s):

☐ There is still a need for clarification on

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

By signing, the employee of the DRC General Secretariat confirms that an audit with the aforementioned result was carried out by the data protection officer.

Place, date

(signature)