

Annex on Outsourcing of data processing in accordance with Art. 28 GDPR to contract number: [REDACTED]

Contractor (name, address, country):

Content

- Clauses 1 to 11
- [Appendix I - Description of the processing](#)
- [Appendix II – List of Subcontractor](#)
- [Appendix III – Technical and organisational measures \(TOM\)](#)

Clause 1 - Purpose and scope

- a) The purpose of this Annex on Outsourcing of data processing (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**General Data Protection Regulation**).
- b) GIZ as controller and the contractor as processor (the Parties) have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.
- c) These Clauses apply to the processing of personal data as specified in Appendix I.
- d) Appendices I to III are an integral part of the Clauses.
- e) These Clauses are without prejudice to obligations to which GIZ is subject by virtue of Regulation (EU) 2016/679.
- f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679. If a transfer of personal data by GIZ to the contractor in a third country takes place, a legal basis is required for this transfer of data. Where a transfer could not be based on an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 or appropriate safeguards pursuant to Article 46 of Regulation (EU) 2016/679 and none of the derogations for specific situations pursuant to Article 49 of Regulation (EU) 2016/679 is applicable, a legally binding agreement shall be concluded between GIZ and the contractor, to establish a legal basis. The agreement shall be established by entering into standard data protection clauses in accordance with Article 46(1) and point (c) of Article 46(2) of Regulation (EU) 2016/679.

Clause 2 - Invariability of the Clauses

The Parties undertake not to modify the Clauses, except for adding information to the Appendices or updating information in them. Amendments and supplements to the information embodied in the Appendices do not call for a written contract supplement and can be agreed in text form.

Clause 3 - Interpretation

- a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 respectively, those terms shall have the same meaning as in that Regulation.
- b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679
- c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Description of processing

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of GIZ, are specified in Appendix I.

Clause 6 - Obligations of the Parties

6.1 Instructions

- a) The contractor shall process personal data only on documented instructions from GIZ, unless required to do so by Union or Member State law to which the processor is subject. In this case, the contractor shall inform GIZ of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by GIZ throughout the duration of the processing of personal data. An instruction is the written, electronic or oral order of GIZ aimed at a specific handling of data by the contractor. The arrangements shall be documented. The instructions are first defined by the terms of reference and can then be changed, supplemented or replaced by GIZ in documented form by an individual instruction.
- b) The contractor shall immediately inform GIZ if, in the contractor's opinion, instructions given by GIZ infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.
- c) GIZ may request the surrender, correction, adaptation, deletion and restriction of the data processing at any time.
- d) The contractor may only provide information to third parties or the data subject with the prior express consent of GIZ. The consent must be documented by the contractor.

6.2 Purpose limitation

The contractor shall process the personal data only for the specific purposes of the processing, as set out in Appendix I, unless it receives further instructions from GIZ.

6.3 Duration of the processing of personal data

Processing by the contractor shall only take place for the duration specified in Appendix I.

6.4 Security of processing

- a) The contractor shall at least implement the technical and organisational measures specified in Appendix III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- b) Due to technical progress, the contractor is permitted to implement alternative adequate measures. This shall not fall below the safety level of the measures laid down in Appendix III. Significant changes must be documented.
- c) The contractor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The contractor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the contractor shall apply specific restrictions and/or additional safeguards. This may include, for example, restricting the personnel who have access to the personal data or ensuring the ability, confidentiality, integrity, availability and resilience of the systems and services.

6.6 Documentation and compliance

- a) The contractor shall deal promptly and adequately with inquiries from GIZ about the processing of data in accordance with these Clauses.
- b) At GIZ's request, the contractor shall provide GIZ with information that GIZ needs to maintain the record of processing activities within the meaning of Article 30(1) of Regulation (EU) 2016/679.
- c) The contractor shall inform GIZ immediately of any inspections and measures taken by the supervisory authorities or if a supervisory authority requests, investigates or obtains other enquiries from the contractor within the scope of its responsibility.

- d) The contractor shall make available to GIZ all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At GIZ's request, the contractor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, GIZ may take into account relevant certifications held by the contractor.
- e) GIZ may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the contractor and shall, where appropriate, be carried out with reasonable notice.
- f) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority on request.

Clause 7 - Use of subcontractor

- a) The contractor shall not subcontract any of its processing operations performed on behalf of GIZ in accordance with these Clauses to a subcontractor (other processor), without GIZ's prior specific documented written authorisation. The contractor shall submit the request for specific authorisation at least 20 calendar days prior to the intended engagement of the subcontractor in question, together with the information necessary to enable GIZ to decide on the authorisation. The information includes at least the full name including address and country of the subcontractor as well as a description of the processing by the subcontractor (including subject matter, nature and duration). GIZ agrees to the commissioning of the subcontractors specified in Appendix II. The Parties shall keep Appendix II up to date.
- b) If the engagement of subcontractors (other processors) is excluded, this is specified by GIZ in Appendix II.
- c) Where the contractor engages a subcontractor for carrying out specific processing activities (on behalf of GIZ), it shall do so by way of a contract which imposes on the subcontractor at least the same data protection obligations as the ones imposed on the contractor in accordance with these Clauses. The contractor shall ensure that the subcontractor complies with the obligations to which the contractor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.
- d) At GIZ's request, the contractor shall provide a copy of such a subcontracting agreement and any subsequent amendments to GIZ. To the extent necessary to protect business secret or other confidential information, including personal data, the contractor may redact the text of the agreement prior to sharing the copy.
- e) The contractor shall remain fully responsible to GIZ for the performance of the subcontractor's obligations in accordance with its contract with the contractor. The contractor shall notify GIZ of any failure by the subcontractor to fulfil its contractual obligations. In this case, at GIZ's request, the contractor shall terminate the subcontractor's employment in whole or in part or terminate the contractual relationship with the subcontractor if and insofar as this is not disproportionate.

- f) Subcontracting within the meaning of this Clauses does not include services which the contractor makes use of from third parties as ancillary services to support the execution of the order, such as telecommunications services. However, the contractor is obliged to make appropriate and legally binding contractual agreements and take appropriate inspection measures to ensure the data protection and data security of GIZ's data, even in the case of outsourced ancillary services.
- g) The contractor shall agree a third party beneficiary clause with the subcontractor whereby – in the event the contractor has factually disappeared, ceased to exist in law or has become insolvent – GIZ shall have the right to terminate the subcontract and to instruct the subcontractor to erase or return the personal data.

Clause 8 - International transfers

- a) The undertaking of the contractually agreed processing of data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA).
- b) Any transfer of data to a third country or an international organisation by the contractor shall be done only on the basis of documented instructions from GIZ or in order to fulfil a specific requirement under Union or Member State law to which the contractor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.
- c) GIZ agrees that where the contractor engages a subcontractor in accordance with Clause 7 for carrying out specific processing activities (on behalf of GIZ) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the contractor and the subcontractor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 9 - Assistance to GIZ

- a) The contractor shall promptly notify GIZ of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by GIZ.
- b) The contractor shall assist GIZ in fulfilling her obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the contractor shall comply with GIZ's instructions
- c) In addition to the contractor's obligation to assist GIZ pursuant to Clause 9(b), the contractor shall furthermore assist GIZ in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the contractor:
 - 1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2. the obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by GIZ to mitigate the risk;
 3. the obligation to ensure that personal data is accurate and up to date, by informing GIZ without delay if the contractor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 4. the obligations in Article 32 Regulation (EU) 2016/679.
- d) The Parties shall set out in Appendix III the appropriate technical and organisational measures by which the contractor is required to assist GIZ in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 10 - Notification of personal data breach

In the event of a personal data breach, the contractor shall cooperate with and assist GIZ for GIZ to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the contractor.

10.1 Data breach concerning data processed by GIZ

In the event of a personal data breach concerning data processed by GIZ, the contractor shall assist GIZ:

- a) in notifying the personal data breach to the competent supervisory authority, without undue delay after GIZ has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in GIZ's notification, and must at least include:
 - 1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - 2) the likely consequences of the personal data breach;
 - 3) the measures taken or proposed to be taken by GIZ to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

10.2 Data breach concerning data processed by the contractor

In the event of a personal data breach concerning data processed by the contractor, the contractor shall notify GIZ without undue delay after the contractor having become aware of the breach. Such notification shall contain, at least:

- a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- b) the details of a contact point where more information concerning the personal data breach can be obtained;
- c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Appendix III all other elements to be provided by the contractor when assisting GIZ in the compliance with GIZ's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Clause 11 - Non-compliance with the Clauses and termination

- a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the contractor is in breach of its obligations under these Clauses, GIZ may instruct the contractor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The contractor shall promptly inform GIZ in case it is unable to comply with these Clauses, for whatever reason.
- b) GIZ shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - 1) the processing of personal data by the contractor has been suspended by GIZ pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - 2) the contractor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;
 - 3) the contractor fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

If GIZ terminates the contract for one of the aforementioned reasons, then such termination shall be deemed to be the responsibility of the contractor, in accordance with section 5.3.2 of the Terms and Conditions.

- c) The contractor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed GIZ that her instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), GIZ insists on compliance with the instructions.
- d) Following termination of the contract, the contractor shall return all personal data processed on behalf of GIZ to GIZ and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.
- e) Data carriers and data records provided to the contractor remain the property of GIZ.

Appendix I - Description of the processing

The following selection was made by GIZ. Should the contractor notice gaps, errors or ambiguities in the context of the award procedure or the execution of the order, a notice must be sent to GIZ.

Nature, purpose and duration of the processing

☐ Subject matter and duration of the outsourcing of data processing as well as scope, nature and purpose of the processing of personal data are determined by the Terms of Reference and by the offer submitted by the contractor.

☒ Detailed description of the scope, nature and purpose of the processing:

The processing of personal data is required for the implementation of activities under a GIZ-supported coaching and training programme for private sector development in the country at hand. The objective of the programme is to strengthen the capacities and competitiveness of selected enterprises through targeted support.

Personal data is processed for the following purposes:

- Application and selection process for participation (beneficiaries), as well as (if applicable) control group
- Data in relation to certification and accreditation of (new) coaches or trainers
- Carrying out training and coaching sessions
- Monitoring and evaluation of training and coaching progress, as well as impacts on key performance indicators (e.g., monthly business figures, employment numbers)
- Travel management including booking of transportation, accommodation etc.
- Contact and communication purposes
- Public relations work and internal showcasing

The service provider will select business trainers and coaches for certification, as well as private enterprises to participate in the programme. In order to plan, implement and follow-up on training of trainers / coaches, as well as coaching and training sessions tailored to the needs of enterprises, the service provider will collect and process personal data.

Categories of data subjects whose personal data is processed

- ☐ Employees of GIZ including applicants
- ☐ Subscribers of e.g. magazines and newsletters
- ☒ External participants in events
- ☒ Participants in surveys
- ☐ Visitors to the premises of GIZ
- ☐ Visitors to websites
- ☒ Service Provider / Supplier
- ☒ Contact persons of partner institutions
- ☐ Representatives of official bodies and government representatives
- ☐ Students/Scholarship holders
- ☐ Other:

Categories of personal data processed

- ☒ Personal Master Data (Name, date of birth)
- ☒ Address data
- ☒ Contact- and communication data (e.g. telephone, e-mail etc.)
- ☒ Qualification data (e.g. career history, CV, qualification etc.)

- ☒ Employee data (wages and salaries, bank account, tax information etc.)
- ☒ Billing and payment data
- ☒ User data (browsing data, IP addresses, cookies, login data etc.)
- ☒ Photo and sound recordings
- ☒ Travel and location data
- ☐ Special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 (e.g. data concerning health, biometric data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning a natural person's sex life or sexual orientation).
- ☐ Other:

Appendix II – List of Subcontractor

- ☐ The contractor may not subcontract any of its processing operations performed on behalf of GIZ in accordance with these Clauses to a subcontractor.

GIZ agrees to the commissioning of the following subcontractors:

Name	Address incl. Country	Description of the processing (incl. subject matter, nature and duration)	When transferring data to a third country or an international organisation: How is compliance with Chapter V of Regulation (EU) 2016/679 ensured?

Appendix III – Technical and organisational measures (TOM) including technical and organisational measures to ensure the security of the data

Description of the technical and organisational security measures implemented by the contractor (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

The following checklist, which contains a large number of possible technical and organisational measures, can be used for presentation. The checklist is not exhaustive and must be supplemented by the contractor for each individual case, if necessary. In order to ensure the concrete description, explanations must be inserted in each case.

The presentation and description of the technical and organisational measures implemented by the contractor can alternatively also be made in a separate document.


1. Measures of pseudonymisation and encryption of personal data


- ☐ Pseudonymisation of personal data no longer required in clear text
- ☐ Pseudonymisation Policy
- ☐ Encryption of data carriers
- ☐ Pseudonymisation of test system data
- ☐ Encryption of websites (SSL)
- ☐ Encryption of database
- ☐ Email encryption (TLS 1.2 or 1.3)
- ☐ Encryption of passwords and keys
- ☐ Encryption of mobile devices
- ☐

Explanation:


2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services


- ☐ Non-disclosure agreement with employees
- ☐ Employees' data protection obligations
- ☐ Non-disclosure agreement with third parties
- ☐ External storage / backup server
- ☐ Support contracts with third parties
- ☐ Data outsourcing agreements
- ☐ Utilization of certified cloud provider
- ☐ Firewall
- ☐ Anti-virus software
- ☐ Regular data backups
- ☐ Redundant systems
- ☐ Monitoring of systems and services
- ☐ RAID systems

- ☐ Network Attached Storage (NAS)
- ☐ Maintenance agreement
- ☐ Regular IT incident tests
- ☐ Internal storage of copies / backups
- ☐ Uninterruptible Power Supply (UPS),
- ☐ Fire and smoke alarm systems
- ☐ Devices for monitoring temperatures
- ☐ Firefighting equipment
- ☐ Alarm warning in case of unauthorized access
- ☐ Load balancing
- ☐ 


Explanation: 


3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- ☐ Regular backups of the entire system
- ☐ Storage on multiple systems
- ☐ Data backup concept
- ☐ Regular test backup/recovery
- ☐ Hardware support and maintenance agreement
- ☐ Concept for emergency preparedness
- ☐ Outsourced data backup
- ☐ Regular training of IT staff
- ☐ 


Explanation: 


4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- ☐ Internal controls
- ☐ Order or contract control (careful selection of contractors, clear contract design, etc.)
- ☐ Regular review of IT processes
- ☐ Regular audits (e.g. by data protection officer)
- ☐ Regular review of procedures
- ☐ Audit of technical and organisational measures by data protection officer
- ☐ Regular checks of employees
- ☐ Conducting data protection impact assessments
- ☐ Check of privacy by design and by default
- ☐ Data protection management system / data protection manual
- ☐ 


Explanation: 


5. Measures for user identification and authorisation

- ☐ Two-factor authentication
- ☐ Authentication with username / password
- ☐ Separation of roles between test and production system
- ☐ Regular assessment of authorizations
- ☐ BIOS passwords
- ☐ Permission management
- ☐ Mobile Device Management Policy
- ☐ User profiles
- ☐ Password policy
- ☐ Limitation the number of admins
- ☐ Identification of new employees
- ☐ Separation of user roles
- ☐ Automatic locking mechanisms
- ☐ Identification of external person with ID cards
- ☐ Management of rights by an admin
- ☐ Differentiation between permissions
- ☐ 


Explanation: 


6. Measures for the protection of data during transmission

- ☐ Utilisation of encryption technologies
- ☐ Virtual Private Network (VPN)
- ☐ Logging of activities and events
- ☐ Transport via private cloud
- ☐ Documentation of data recipients
- ☐ Email encryption (TLS 1.2 or 1.3)
- ☐ Verification of the identity of the recipients
- ☐ Utilisation of non-public drives
- ☐ Physical transport: secure transport containers
- ☐ Careful selection of transport personnel
- ☐ 

Explanation: 


7. Measures for the protection of data during storage


- ☐ Encryption of data carriers
- ☐ Data classification
- ☐ Permission management
- ☐ Limitation of access
- ☐ Logging of actions and events
- ☐ Security doors
- ☐ Limitation the number of admins
- ☐ Magnetic or chip cards
- ☐ Anonymization of data
- ☐ Pseudonymization of data
- ☐ Secure storage of data carriers
- ☐ Firewall
- ☐ 

Explanation: 


8. Measures for ensuring physical security of locations at which personal data are processed


- ☐ Alarm system
- ☐ Facility security services and/or entrance security staff
- ☐ Protection of building shafts
- ☐ Logging of visitors
- ☐ Automatic access control
- ☐ Careful selection of cleaning staff
- ☐ Careful selection of security staff
- ☐ Magnetic or chip cards

- ☐ Locking system with code lock
- ☐ Obligation to wear authorization cards
- ☐ Manual locking system
- ☐ Concept of access
- ☐ Biometric entrance barrier
- ☐ Lockable server cabinets
- ☐ Video surveillance of the entrances
- ☐ Doors with a knob on the outside
- ☐ Light barriers / motion detectors
- ☐ Visitors: Only accompanied by employees
- ☐ Safety locks
- ☐ Bell system with camera
- ☐ Key issuance procedure
- ☐ 

Explanation: 

9. Measures for ensuring events logging

- ☐ Use of automatic logging
- ☐ Creation of incident reports
- ☐ Notification with real-time alarm
- ☐ Application-level logging
- ☐ Automatic review of logs
- ☐ Synchronization of system clocks
- ☐ Regular manual review of logs
- ☐ Automatic consolidation of incidents
- ☐ Logs are stored in the application and automatically sent to another location
- ☐ 

Explanation: 

10. Measures for ensuring system configuration, including default configuration

- ☐ Configuration management policy exists
- ☐ Process for changes to configurations
- ☐ Privacy by Default
- ☐ Check of the default configurations
- ☐ Definition of default configurations
- ☐ Configuration by system administrator
- ☐ Logging of changes to configurations
- ☐ Regular training of IT staff
- ☐ [REDACTED]


Explanation: [REDACTED]


11. Measures for internal IT and IT security governance and management

- ☐ IT security guideline
- ☐ IT administration guideline
- ☐ Regular compliance audits / reviews
- ☐ Register of IT systems
- ☐ Training of employees on data security
- ☐ Regular system review/evaluation
- ☐ IT team with assigned roles/responsibilities
- ☐ Incident-management guidelines
- ☐ Risk assessment and risk management measures at all stages and levels
- ☐ [REDACTED]


Explanation: [REDACTED]


12. Measures for certification/assurance of processes and products

- ☐ Implementation of ISO 9001 - *Quality Management*
- ☐ Implementation of ISO 27001 - *Information technology management system*
- ☐ Implementation of ISO 27701 - *Privacy Information Management System*
- ☐ GDPR-Certification – Data Protection Management
- ☐ Overview of the regulations applicable to products/services/processes
- ☐ Identification of industry-specific standards
- ☐ Regular internal and/or external audits
- ☐ Assignment of audit responsibilities to certified experts
- ☐ Regular check for new requirements and renewal of certificates
- ☐ 


Explanation: 


13. Measures for ensuring data minimisation

- ☐ Identification of the purpose of the processing
- ☐ Assessment of the connection between processing and purpose
- ☐ Assessment of the scope and quality of the data processed in relation to the purpose
- ☐ Identification of the applicable retention periods
- ☐ Secure deletion of data after expiry of the retention period
- ☐ 


Explanation: 


14. Measures for ensuring data quality

- ☐ Data profiling and classification
- ☐ Control of incoming or new data
- ☐ Logging of the input/change of data
- ☐ Assignment of rights for data entry
- ☐ Log retention
- ☐ Traceability of users when entering, change of data (no user groups)
- ☐ Avoidance of duplicate data
- ☐ Identification of data requirements
- ☐ Application of data quality measures
- ☐ 


Explanation: 


15. Measures for ensuring limited data retention

- ☐ Retention policy with roles
- ☐ Separation of data according to retention periods
- ☐ Regular training
- ☐ Regular review and evaluation of stored data
- ☐ 


Explanation: 

16. Measures for ensuring accountability

- ☐ Training / Awareness Raising
- ☐ Regular checks and audits
- ☐ Data protection team exist
- ☐ Guidance and support for employees
- ☐ Appropriate privacy policies
- ☐ Conclusion of Standard Contractual Clauses (SCC)
- ☐ Joint Controllership Agreements
- ☐ Responding to requests from data subjects
- ☐ Transparency documents (Article 13 / 14 GDPR)
- ☐ Secure deletion of data
- ☐ Documented privacy statement
- ☐ Audit reports and measures are documented
- ☐ Proper involvement of the Data Protection Officer
- ☐ Specific consent procedure / keeping of consent logs
- ☐ 

Explanation: 

17. Measures for allowing data portability and ensuring erasure

- ☐ Storage in a structured format
- ☐ Monitoring of statutory periods
- ☐ Transfer via end-to-end encryption
- ☐ Compliance with retention periods
- ☐ Enabling data portability
- ☐ Dealing with the rights of data subjects pursuant to Chapter 3 of Regulation (EU) 2016/679
- ☐ Secure data deletion ensured
- ☐ Secure destruction of data carriers ensured
- ☐ 

Explanation: 