Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR and the Turkish Personal Data Protection Law numbered 6698 (hereinafter KVKK))

between

Welthungerhilfe e.V.

Friedrich-Ebert-Str. 1

53173 Bonn

Germany

(the "**Data Controller**" or "**Welthungerhilfe**")

and

Name

Address

Postcode and City

Country

(the „**Data Processor**" or „ XXX ")

each a "**Party**"; together the "**Parties**"

HAVE AGREED on the following Data Processing Agreement (the "**Agreement**") in order to meet the requirements of the GDPR and KVKK and to ensure the protection of the rights of the data subject.

Table of content

Instructions to fill in the Data Processing Agreement (DPA) template

This pdf is protected with fields restrictions. The open fields (in blue in the clauses) have to be completed as per the indications written in the fields. Those indications will disappear automatically.

Welthungerhilfe is the Data Controller, who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

Data Processor is the person who processes personal data on behalf of the data controller, based on the authority given by the Data Controller

The Welthungerhilfe's representative should fill in the open fields of the main body of the Data Processing Agreement (DPA) and the Annex A. The Data Processor's representative should check the content and add information where necessary.

The Data Processor's representative is invited to complete the Annexes B and C. Welthungerhilfe will then check the input from the Data Processor and assess the adequacy of its Technical and Organizational Measures.

Preamble

1. This Agreement sets out the rights and obligations of the Data Controller and the Data Processor, when processing personal data on behalf of the Data Controller.

2. This Agreement has been designed to ensure the Parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter "**GDPR**") and Turkish Data Protection Law Numbered .6698 (hereinafter KVKK)).

3. In the context of the provision of DESIGNATION AND DATE OF THE MAIN CONTRACT ,the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses. In this context, the Data Processor is instructed to SHORT DESCRIPTION OF THE SERVICE .

4. This Agreement shall, regarding the processing of data, take priority over any similar provisions contained in other agreements between the Parties.

5. Three appendices are attached to this Agreement and form an integral part of the Agreement.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the Data Controller's conditions for the Data Processor's use of sub-processors and a list of sub-processors authorised by the Data Controller.

8. Appendix C contains the Data Controller's instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the Data Processor and how audits of the Data Processor and any sub-processors are to be performed.

9. This Agreement shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the GDPR and KVKK or other legislation.

1. The rights and obligations of the Data Controller

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State's law or Turkish Data Protection Law (KVKK) or other applicable mandatory data protection provisions and the Agreement.

2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The Data Controller is responsible, among other, for ensuring that the instructed processing of personal data has a legal basis.

2. The Data Processor acts according to instructions

1. The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law or KVKK to which the Data Processor is subject. In particular, the Data Processor will strictly abide by the principle of data minimisation in the performance of the Assessment and the preparation and finalisation of the Assessment Report. Such instructions are further specified in appendices A and C. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be documented at least in writing, including electronically, and kept together with the Agreement.

2. The Data Processor is obliged to assess the instructed data processing activities. The Data Processor must immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State or KVKK or other applicable mandatory data protection provisions. The Data Processor may suspend the implementation of instructed unlawful processing activities until the Data Controller has verified and confirmed the

lawfulness of its instructions or has – to the extent necessary - adequately adjusted the instructed processing activities. The Data Processor is entitled to reject the implementation of any instructed data processing activity which is obviously unlawful or void.

3. Confidentiality

1. The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The Data Processor will document and maintain a list of persons to whom access has been granted. In particular, if access is no longer necessary, the Data Processor shall immediately withdraw access to the relevant personal data for the person concerned.

2. The Data Processor shall at the request of the Data Controller submit such list and demonstrate that the concerned persons under the Data Processor's authority are subject to the abovementioned confidentiality.

4. Security of processing

1. Article 32 GDPR and Art.12 of KVKK stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   1. Pseudonymisation and encryption of personal data;

   2. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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

   4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. The Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information requested by the Data Processor and being necessary to identify and evaluate such risks.

3. The Data Processor is obliged to take all the technical and administrative measures in a way to prevent unauthorized access to personal data both by its own personnel and by third persons and use of personal data out of the purpose of being transferred to itself. The Data Processor accepts and declares that any measures to be taken in this regard shall in any event be in compliance with the legislation in force (if any) or at least equivalent to the measures taken by a prudent merchant operating in similar fields for security of the personal data that it stores.

4. In case of transfers of "Special Categories of personal data" by the Data Controller under the Agreement, such data shall be protected by the Data Processor subject to additional security measures and authorizations appropriate for their nature and as specified in the relevant legislation.

5. Furthermore, the Data Processor shall assist the Data Controller in complying with the Data Controller's obligations, including by providing information on the technical and organisational measures that the Data Processor has already implemented in accordance with Art. 32 GDPR and Art.12 of KVKK; these measures are listed in Annex C. In addition, the Data Processor shall provide the Data Controller with all

further information necessary for the Data Controller to comply with its obligations under Article 32 GDPR.

If subsequently – in the assessment of the Data Controller – mitigation of the identified risks require further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to Article 32 GDPR, the Data Controller shall specify these additional measures to be implemented in Appendix C.

5. Use of sub-processors

1. The Data Processor shall not engage another processor (sub-processor) for the fulfilment of the Agreement without the prior general written authorisation of the Data Controller.

2. The list of sub-processors already authorised by the Data Controller can be found in Appendix B. The Data Processor shall inform the Data Controller in writing with the request for approval of all intended changes concerning the addition or replacement of sub-processors at least 1 month in advance. Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B.

3. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the Data Processor will enter into a respective sub-processing agreement and will impose on that sub-processor the same data protection obligations as set out in the Agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Agreement and the GDPR and KVKK.

   The Data Processor agrees and commits to define the authorizations and obligations of sub- processors' accessing and processing of personal data in accordance with the relevant legislation on personal data. The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the Agreement and the GDPR and KVKK

4. A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the Agreement are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Data Controller.

5. The Data Processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the Data Processor – the Data Controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the Data Processor, e.g. enabling the Data Controller to instruct the sub-processor to delete or return the personal data.

6. Both the Data Processor and sub-processors shall be severally liable for the implementation of this agreement.

7. If the sub-processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR and KVKK – in particular those foreseen in Articles 79 and 82 GDPR – against the Data Controller and the Data Processor, including the sub-processor.

6. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the Data Processor shall only occur upon obtaining the explicit consent of the data subject. On the basis of documented instructions from the Data Controller and shall always take place in compliance with the GDPR Chapter V and the law of EU State Law or KVKK. Personal data may be transferred abroad without obtaining the

explicit consent of the data subject if the conditions set forth in the law of EU Member State or KVKK are provided.

2. In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, is required under EU or Member State law or KVKK to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a Data Controller or a Data Processor in a third country or in an international organization

   b. transfer the processing of personal data to a sub-processor in a third country

   c. have the personal data processed in by the Data Processor in a third country

4. The Data Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR KVKK Art.9 on which they are based, shall be set out in Appendix C.5.

7. Assistance to the Data Controller

1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject

   b. the right to be informed when personal data have not been obtained from the data subject

   c. the right of access by the data subject

   d. the right to rectification

   e. the right to erasure ('the right to be forgotten')

   f. the right to restriction of processing

   g. notification obligation regarding rectification or erasure of personal data or restriction of processing

   h. the right to data portability

   i. the right to object

2. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 4.3., the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

   a. The Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the Data Controller's obligation to without undue delay communicate 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;

c. the Data Controller's 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);

d. the Data Controller's 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 the Data Controller to mitigate the risk.

8. Notification of personal data breach

1. In case of personal data are acquired by others through unlawful means or in case of any other personal data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach and the situation.

2. The Data Processor's notification to the Data Controller shall, if possible, take place within 24 HOURS after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the Data Controller's obligation to notify the personal data breach to the competent supervisory authority.

3. In accordance with Clause7 (2)(a), the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, shall be stated in the Data Controller's notification to the competent supervisory authority:

   a. 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;

   b. the likely consequences of the personal data breach;

   c. the measures taken or proposed to be taken by the controller, or the processor respectively, to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9. Erasure and return of data

1. On termination of the provision of personal data processing services, the Data Processor shall be under obligation to delete or destroy or make anonymised all personal data processed on behalf of the Data Controller and certify to the Data Controller that it has done so, or, at the request of the Data Controller, return to the Data Controller the Personal Data processed and confirm that the Data Processor has not retained any data, unless Union or Member State law or KVKK requires storage of the personal data.

10. Audit and Inspection

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with its obligations and allow for and contribute to audits conducted by the Data Controller or another auditor mandated by the Data Controller.

2. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

11. Liability

1. The Data Controller will indemnify and keep indemnified the Data Processor in respect of all and any claims, legal proceedings or actions brought against the Data Processor arising from any Security Breach as a result of any grossly negligent act or omission by the Data Controller in the exercise of its obligations under the Applicable Law provided that the Data Processor, without undue delay, notifies the Data

Controller of any actions, claims or demands brought or made against it concerning any alleged Security Breach.

2. The Data Processor will indemnify and keep indemnified the Data Controller in respect of all and any claims, legal proceedings or actions brought against the Data Controller arising from any Security Breach as a result of any grossly negligent act or omission by the Data Processor in the exercise of its obligations under the Applicable Law provided that the Data Controller, without undue delay, notifies the Data Processor of any actions, claims or demands brought or made against it concerning any alleged Security Breach.

12. Data Controller and Data Processor contacts

1. Communications under this Agreement shall be addressed to:

For Data Controller:

Name [**Name**]

Position [**Position**]

Telephone [**Telephone**]

E-mail [**E-mail**]

For Data Processor:

Name [Name]

Position [Position]

Telephone [Telephone]

E-mail [E-mail]

The Parties will continuously inform each other of changes to contacts/contact points.

13. Contract Term and termination

1. This Agreement will come into force on the date of the last signature of the Parties. It will end with the fulfillment of the main contract or the processing purpose. In addition, either party may terminate the Data Processing Agreement in accordance with clause 13.2. The Parties' respective archiving and confidentiality obligations and obligation to support each other in the case of requests by data subjects or competent supervisory authorities will remain effective even after the termination of the Agreement.

2. Each Party may terminate this Agreement without notice if one of the following events occurs or if other comparable circumstances arise that make it unreasonable for the Party in question to continue adhering to the Agreement:

   I. The other Party becomes unable to pay; or it files for insolvency; or an insolvency claim is filed against it; or insolvency proceedings are initiated; or it assigns its assets to creditors; or it enters into receivership or sequestration; or it liquidates its business operations;

   II. The other Party violates one of its material obligations under this Agreement and does not remedy this violation within six weeks of receiving a written warning substantiating the violation of the Agreement;

   III. The other Party culpably violates statutory regulations that are directly or indirectly relevant to the performance of this Agreement, endangers the image of the other Party, or offends common decency.

3. Termination must be submitted in writing by registered mail with return receipt requested.

4. Both Parties are entitled to require the Agreement renegotiated if changes to the law or inexpediency of the Agreement should give rise to such renegotiation.

14. General Provisions

1. This Agreement contains all agreements made by the Parties regarding the object of the Agreement; no side agreements exist. Alterations and amendments to this Agreement as well as waivers of any rights arising from this Agreement must be made in writing to be effective. This also applies to the amendment or cancellation of this Written Form clause.

2. Without the Data Controller's prior written consent which the Data Controller may grant or deny at its own discretion, the Data Processor is not entitled to assign this Agreement or parts of it, whether directly or indirectly, to a third party.

3. The relationship between the Parties is that of independent parties. They are forming neither a joint venture nor any other kind of cooperative enterprise or partnership. Neither Party is authorised to act as the proxy, agent, or representative of the other Party; or to give or accept declarations on behalf

4. Should individual provisions of this Agreement be or become ineffective, or should this Agreement contain an unintended gap, or should a point in time or period of time be undefined, this will not affect the validity of the remaining provisions. In place of the invalid provision, the undefined point in time, or the undefined period of time or in order to close the gap, that effective and practicable provision, point in time, or period of time that legally and economically approximates best what the Parties had originally intended or would have intended within the intention and purpose of this Agreement if they had considered this aspect when concluding the Agreement shall be understood to retroactively take effect.

5. This Agreement is governed by the material law of Turkey. Federal Republic of Germany.

6. To the extent permissible by law, the competent court for all disputes regarding this Agreement is Gaziantep

7. This Agreement was prepared in duplicate, with one copy for each Party.

8. This Agreement enters into force as of the date of signing, subject to the Data Processor 's fulfilment of other conditions stipulated in the Agreement

[Place] this [ ] of [,]

[name of Data Processor]

Name, Position

(name, position)

Name, Position

(name, position)

[WHH_Pl] this [ ] of [,]

Deutsche Welthungerhilfe e.V.

Name, Position

(name, position)

Name, Position

(name, position)

Appendix A Information about the processing

A.1. The purpose of the Data Processor's processing of Personal Data on behalf of the Data Controller is:

DESCRIBE THE PURPOSE OF THE PROCESSING

A.2. The instruction for the processing of Personal Data

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

DESCRIBE THE PROCESSING THAT THE DATA PROCESSOR HAS BEEN INSTRUCTED TO PERFORM

A.3. Processing includes the following categories of data subject:

DESCRIBE CATEGORY OF DATA SUBJECT

A.4. The processing includes the following types of personal data about data subjects: [SELECT]

Personal details: ⬓ name ☐ address ☐ contact details ☐ age ☐ date of birth ☐ sex ☐ written physical description ☐ picture ☐ video

Identifier issued by a public authority: ☐ passport details ☐ national insurance numbers ☐ identity card numbers ☐ driving licence details.

Family, lifestyle and social circumstances: ☐ current marriage and partnerships ☐ marital history ☐ details of family and other household members ☐ habits ☐ housing ☐ travel details ☐ leisure activities ☐ membership of charitable or voluntary organisations.

Education and training: ☐ information education and professional training ☐ academic records ☐ qualifications ☐ skills ☐ training records ☐ professional expertise ☐ student and pupil records.

Employment details: ☐ current employment ☐ career history ☐ recruitment and termination details ☐ attendance records ☐ health and safety records ☐ performance appraisals ☐ security records.

Financial details: ☐ income ☐ salary ☐ assets ☐ investments ☐ payments ☐ creditworthiness ☐ loans ☐ benefits ☐ insurance details ☐ pension information.

Goods or services provided and related information: ☐ goods or services supplied ☐ licences issued ☐ contracts.

Special categories of Personal Data: ☐ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data (if used to identify a natural person) ☐ health ☐ sex life or sexual orientation ☐ criminal convictions and offences

Other: [SPECIFY]

Specify

A.5. Duration of personal data processing and erasure

Personal Data is processed by the Data Processor for [State time Period]

Upon termination of the provision of personal data processing services, the Data Processor shall delete the personal data in accordance with Clause 9.1., unless the Data Controller – after the signature of the contract – has modified the its original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses

Other: [SPECIFY]

Specify

A.6. Processing location

Processing of the personal data under the Agreement cannot be performed at other locations than the following without the Data Controller's prior written authorisation:

STATE WHERE PROCESSING TAKES PLACE, STATE THE DATA PROCESSOR OR SUB-PROCESSOR USING THE ADDRESS

A.7. Instruction on the transfer of personal data to third countries

DESCRIBE AN INSTRUCTION ON THE TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY OR INTERNATIONAL ORGANISATION

If the Data Controller does not in the Areement or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled within the framework of the Agreement to perform such transfer.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the Data Controller authorises the engagement of the following sub-processors:

NAME	ADDRESS	DESCRIPTION OF PROCESSING
Name	Address	Description of Processing
Name	Address	Description of Processing
Name	Address	Description of Processing

The Data Controller shall on the commencement of the Agreement authorise the use of the abovementioned sub-processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

DESCRIBE THE TIME PERIODS OF PRIOR NOTICE FOR AUTHORISATION OF SUB-PROCESSORS

Appendix C Technical and Organizational Measures (TOM)

Taking into account the nature, scope, context and purpose of the processing activity as well as the risks for the rights and freedoms or natural persons, describe the Technical and Organizational Measures (TOM) in place for the data processing.

C.1 Devices security such as desktop, laptop, mobile phones and USB drive.

Desktops and laptops: ☐ antivirus software ☐ automatic session and screen lockout ☐ firewall ☐ unique identifier (login) for each user ☐ strong password ☐ password periodically changed ☐ Endpoint Configuration Manager

Mobile phones: ☐ automatic screen lockout ☐ PIN ☐ password ☐ fingerprint access ☐ antivirus ☐ remote device wipe ☐ Mobile Device Management (MDM)

External storage devices (USB drives): ☐ not used (preferred option) ☐ scanned by anti-virus

Other information: [SPECIFY]

Specify

C.2 Data storage and encryption: Describe where the Personal Data will be stored:

Personal Data must be encrypted whenever technically possible. Sensitive Personal Data must be stored encrypted without exception. Encryption can be done at the device or at the file level.

■ Desktops	Is the Personal Data encrypted?	☐ Yes ☒ No
■ Laptops	Is the Personal Data encrypted?	☐ Yes ☒ No
■ Mobile phones & tablets	Is the Personal Data encrypted?	☐ Yes ☒ No
■ External USB drives	Is the Personal Data encrypted?	☐ Yes ☒ No
■ File Server	Is the Personal Data encrypted?	☐ Yes ☒ No
■ Cloud storage	Is the Personal Data encrypted?	☐ Yes ☒ No

Other information: [SPECIFY]

Specify

C.3 Access to the Personal Data

The Data Processor must restrict the access to Personal Data to the authorised users.

☐ user accounts are centrally managed ☐ access to the files containing Personal Data is restricted to authorised users ☐ user accounts are periodically reviewed ☐ process in place for user on-boarding and off-boarding

Other information: [SPECIFY]

Specify

C.4 Data availability: Describe the measures to ensure the access to Personal Data in a timely manner in the event of an incident.

☐ data backup in place ☐ restoration of backup tested ☐ back up stored in a secure location ☐ back up stored off-site

Other information: [SPECIFY]

Specify

C.5 Data sharing: Describe how the Personal Data will be shared between the Data Controller and the Data Processor.

☐ Email The files are encrypted: ☐ Yes ☐ No

☐ External USB drives The devices are managed by the ☐ Data Controller ☐ Data Processor

☐ Cloud storage The platform is managed by the ☐ Data Controller ☐ Data Processor

Other information: [SPECIFY]

Specify

C.6 Applications used specifically for the processing activity.

LIST THE KEY APPLICATIONS THAT WILL BE USED FOR THE PROCESSING ACTIVITY

C.7 The Data Processor must handle **pseudonymised** and/or **anonymized** Personal Data whenever possible.

WHERE APPLICABLE, EXPLAIN THE MEASURES

C.8 Physical security of location at which personal data are processed.

☐ Access to the premises with locked doors ☐ Intrusion alarms ☐ Security guards

Other information: [SPECIFY]

Specify

C.9 Organisational measures

The Data Processor has assigned roles and responsibilities for ☐ Information Security ☐ Data Protection

The Data Processor has policies and procedures in place: ☐ Information Security Policy ☐ Data Protection Policy ☐ Work at home ☐ Incident Management

Other: [SPECIFY]

Specify

The Data Processor regularly test the effectiveness of technical and organisational measures for ensuring the security of the processing:

☐ Internal audit ☐ External audit ☐ Security certifications: [SPECIFY]

Specify