Joint Controller Agreement

between

Freie Universität Berlin
represented by the President
Kaiserswerther Straße 16-18
14195 Berlin
Executing organisational unit
University Library
Research and Publication Services Department
Team Digital Interview Collections
Garystr. 39
14195 Berlin
Contact person:
Dr Cord Pagenstecher

and

Archive owner
represented by
Executing organisational unit

Street
Postcode, city
(hereinafter: archive owner)

Preamble

The EU General Data Protection Regulation introduces "joint controllers". This takes account of situations in which two or more controllers jointly decide on the purposes and means of data processing. This is in contrast to traditional "order processing", in which the decision-making power lies largely with the controller and the processor is bound by instructions. The aim of this agreement is to define and distribute the existing rights and obligations among the above-mentioned joint controllers.

§ 1 Object of data processing

(1) The controllers jointly carry out the collection, processing and/or use of the personal data specified below.

(2) The object of the joint data processing and thus the purpose, type and scope of the collection, processing and/or use of personal data is the performance of the following task(s) by the contracting parties:

Tasks Freie Universität Berlin:

- Provision of the technical infrastructure for the archiving, indexing and publication of personal data (audio and video recordings, transcripts, accompanying documents, metadata) in the Oral-History.Digital portal
- Transfer of the personal data of the interviewees and others involved in the recording of the interviews (audio and video recordings, transcripts, accompanying documents, metadata for the purposes of long-term archiving

- Management and organisation of the personal data of archive owners and their employees for registration purposes (email address, name, contact details, gender, title, profession, institution)
- Management and organisation of the personal data of platform users for the purposes of registration (email address, name, contact details, gender, title, profession, institution)
- Management and organisation of usage data on the platform for the purposes of technical improvement and adaptation (IP address, cookies, etc.)

Archive owner tasks:

- Provision of the audio and video recordings (with transcripts, accompanying documents and metadata), if necessary, following the consent of the interviewees and other parties involved in the recording of the interviews
- Management of user registration data for the purpose of assigning authorisations to access the contents of the archive owners' archives
- Provision of the registration data of archive holders and their employees for the purpose of allocating competences

(3) Subsequent changes to the allocation of tasks (purpose, type and scope of data processing) must be documented.

§ 2 Contact point for the persons concerned

The point of contact for platform users is Freie Universität Berlin. The contact point for the interviewees and others involved in the interviews is the archive owner.

The parties are aware that, notwithstanding the agreement reached regarding a general point of contact, data subjects may assert their rights with any individual controller under this agreement.

§ 3 Duration of jointly responsible data processing

The term of this agreement corresponds to the term of the cooperation agreement. The possibility of cancellation without notice remains unaffected by this.

§ 4 Type of data

The subject of the collection, processing and/or use of personal data is the data from the following data categories:

☐ Billing data	☒ Address data	☐ Bank details
☐ Biometric data	☐ Creditworthiness data	☐ Function name
☒ Dates of birth	☐ Health data	☐ interests
☒ IT usage data	☒ Contact data	☐ Wage and salary data
☒ Your name	☐ Personnel master data	☐ Planning data
☐ Qualification data	☐ Social security data	☐ Telephone calls
☐ Contract data	☐ Contract master data	☒ Video recordings
☒ e-mail address	☒ Gender	☒ Sound recordings
☒ Profession-specific data (profession, title, institution)		☐ other data:

If the handling of the specified data categories can be assigned to a respective controller, the breakdown of the data types used can be described as follows:

Data categories used by Freie Universität Berlin:

- Dates of birth

- IT usage data
- Name
- E-mail address
- Address data/contact data
- Gender
- Occupation-specific data
- Video and sound recordings

Data categories used by the archive owner:

- Dates of birth
- Name
- E-mail address
- Address data/contact data
- Personnel master data
- Gender
- Occupation-specific data
- Video and sound recordings

§ 5 Group of affected parties

The group of data subjects affected by the handling of their personal data within the scope of this contract includes the following categories:

☒ Employees	☐ Suppliers	☐ Event participants
☐ Applicants	☐ Commercial agents	☐ Subscribers
☐ Service provider	☐ Contact person	☐ Patients
☐ Customers/clients	☐ Visitors/guests	☐ Passers-by

☒ Other affected parties: interviewees and others involved in the recording of the interviews, employees of the archive owners, platform users

If the data subjects affected by the respective processing can be assigned to the corresponding controller(s), this assignment can be described as follows:

Data subjects affected by data processing at Freie Universität Berlin:

- Employees
- Interview partners
- Others involved in the interviews
- Platform users

Data subjects affected by the data processing of the archive holder:

- Employees
- Interview partners
- Others involved in the interviews
- Platform users

§ 6 Safeguarding the rights of data subjects

(1) In the course of data processing, the data subject(s) have comprehensive rights ("data subject rights"). This includes the data subject's right of access, the right to rectification and erasure (or "right to be forgotten"), the right to data portability and the right to object in general or to

automated individual decisions. Within the framework of joint responsibility, it must be determined in a transparent manner which controller is responsible for safeguarding which data subject rights.

(2) There is a functional division of responsibilities with regard to the standardised rights of data subjects, which can be described as follows:

Responsibilities of Freie Universität Berlin:
- Processing of enquiries from affected platform users
- Processing enquiries from affected employees

Responsibilities of the archive holder:
- Processing of enquiries from interview partners who are affected
- Processing requests from other parties involved in the recording and archiving of interviews
- Processing enquiries from affected employees

§ 7 Obligation to provide information about data processing

(1) If personal data is collected from the data subject(s), the controller to be determined within the framework of this agreement must provide the data subject with the notifications pursuant to Art. 13 (1) and (2) GDPR in the interests of transparent processing.

(2) The same applies to the situation in which personal data is not collected from the data subject(s). In this case, the obligation to inform the data subject(s) is governed by Art. 14 (1) and (2) GDPR.

(3) Within the scope of this agreement, Freie Universität Berlin fulfils the information obligations towards the platform users.
The archive owner fulfils its duty to provide information to the interview partners and other participants in its own collections or specially conducted interview projects.

§ Section 8 Reporting and notification obligations, data protection impact assessment and prior consultation

(1) In the event of a breach of the protection of personal data, those responsible may be subject to reporting or notification obligations. This applies to the immediate notification of the breach to the data protection supervisory authority and to the notification of the data subject(s).

(2) If there is a high risk to the rights and freedoms of data subjects for a form of processing (e.g. due to the technologies used, the type, scope or circumstances), a data protection impact assessment must always be carried out. If the impact assessment confirms a correspondingly high risk, the controller must consult the data protection supervisory authority before commencing processing.

(3) As the obligations set out in paragraphs 1 and 2 are to be defined in a transparent manner among the respective responsible parties with regard to their fulfilment, the following breakdown applies:

Responsibilities of Freie Universität Berlin:
Reporting and notification obligations, data protection impact assessment and prior consultation with regard to the processing of platform users' data

Responsibilities of the archive holder:
Reporting and notification obligations, data protection impact assessment and prior consultation with regard to the processing of audio and video recordings and other interview content

§ 9 Mutual, non-divisible obligations arising from the GDPR

(1) All controllers responsible for the (joint) processing of personal data must take appropriate technical and organisational measures to ensure a level of protection appropriate to the risk, taking into account the circumstances. This includes, among other things, the ability to ensure the confidentiality, integrity, availability and resilience of the systems in the long term. Establishing an appropriate level of security is the responsibility of each individual data controller. Specific technical and organisational measures are agreed in Annex 1 to this contract and are explicitly included in it.
(2) Compliance with data secrecy must be ensured. All persons acting on behalf of the controller who have access to the personal data of the data subjects must be obliged to maintain data secrecy and confidentiality and must be instructed about the special data protection obligations arising from this mandate and the existing purpose limitation.
(3) Each controller must keep a record of the processing activities for which it is responsible.
(4) The contracting parties under this agreement are responsible for their own obligations under the provisions of the General Data Protection Regulation and other data protection regulations. This applies with regard to the obligations specified in paragraphs 1-3 as well as other formal data protection regulations (e.g. appointment of a company data protection officer).

§ 10 Order processing

(1) The parties are authorised to use processors within the meaning of Art. 28 GDPR for processing operations under their respective responsibility. The parties shall each maintain a list of processors commissioned by them for processing operations under this agreement. In the event of a legitimate interest (e.g. monitoring compliance with the obligations under this agreement, enquiry by a supervisory authority or a data subject), the parties shall make the lists available to each other, unless the enquiry can be answered by direct information from the respective party to the person making the enquiry.
(2) The processors already commissioned with processing operations at the time of conclusion of the contract, who are also used by the respective party to carry out the processing operations in accordance with this agreement, shall be deemed to be authorised by the other parties.
(3) The parties shall only commission subcontractors who fulfil the requirements of data protection law and the provisions of this agreement. Services provided by subcontractors within the meaning of this provision do not include services that the parties utilise from third parties as ancillary services to support the execution of the order, such as telecommunications services and maintenance. However, the parties are obliged to enter into appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of personal data, even in the case of externally contracted ancillary services.
(4) The parties undertake to conclude a contract in accordance with Art. 28 GDPR when using processors within the scope of this agreement. The commissioning party must impose obligations on its processors regarding data protection, confidentiality and data security that meet the requirements of Art. 28, 29 GDPR and are at least as strict as those laid down in this agreement. In the event that subcontractors are authorised, the parties shall ensure that the processors impose corresponding obligations on them

§ 11 Audit rights

Those responsible under this agreement have the right to monitor compliance with the contractually agreed data protection and data security measures with regard to the personal data provided under this agreement in consultation with the contractual partner or to have such monitoring carried out by auditors to be appointed in individual cases. Each controller shall have the right to verify compliance

with this agreement in the business operations of the contractual partner within the meaning of this agreement by means of random checks, which must generally be notified in good time.

§ 12 Liability and unlimited responsibility towards data subjects

(1) Notwithstanding the arrangements made under this agreement regarding the allocation of obligations, data subjects may assert their rights with and against each of the controllers. The mere referral/forwarding of the data subject to another controller under this agreement is not permitted.
(2) Each controller is liable for the entire damage caused by the data processing to ensure effective compensation for the data subject(s) (Art. 82 para. 4 GDPR).
(3) Any controller whose incorrect or unauthorised data processing has caused damage shall be liable to its contractual partner within the meaning of this agreement for damages incurred through no fault of its own. Liability in the internal relationship shall be based on the respective share of responsibility for any damage incurred (Art. 82 para. 5 GDPR).

§ Section 13 Duty to provide information, written form requirement

(1) The essence of this agreement must be made available to the person concerned upon request. This will be ensured by Freie Universität Berlin.
(2) Should the data of a data controller be jeopardised by seizure or confiscation, by insolvency or composition proceedings or by other events or measures by third parties, the respective data controller must inform their contractual partner(s) immediately.
(3) Amendments and additions to this agreement and all its components - including any assurances by a responsible person or persons - require a written agreement and an express reference to the fact that it is an amendment or addition to these terms and conditions. This also applies to the waiver of this formal requirement.
(4) The directly and mandatorily applicable law of the European Union and, where applicable, the national law of the Federal Republic of Germany shall apply.

§ 14 Severability clause

(1) Should individual provisions of this agreement be invalid or unenforceable or become invalid or unenforceable after conclusion of the contract, this shall not affect the validity of the remainder of this agreement.
(2) The invalid or unenforceable provision shall be replaced by a valid and enforceable provision whose effects come closest to the (data protection) legal objective pursued by the contracting parties with the invalid or unenforceable provision. The above provisions shall apply accordingly in the event that the contract proves to be incomplete.

_____	_____
Place, date	Stamp/ Signature Freie Universität Berlin
_____	_____
Place, date	Stamp/signature of archive holder

Checklists for the complete division of tasks in joint control agreements

Pursuant to Art. 26 para. 1 sentence 2 GDPR, the controllers shall specify in an agreement "*which of them fulfils which obligation under this Regulation*". This means that this regulation basically covers all obligations of the EU General Data Protection Regulation and goes beyond the rights of data subjects and information obligations mentioned separately (wording: "*in particular*"). The following two checklists provide an overview of which controller fulfils which obligation.

Obligations arising from the GDPR towards interviewees and those involved in the interviews	**Responsible persons FU Berlin**	**Archive owner**
Determination of the purpose and means of data processing as well as the type of data and the group of data subjects	☐	☒
Art. 13 Information on the collection of personal data	☐	☒
Art. 14 Information if data was not collected from the data subject	☐	☒
Art. 15 Processing of requests for information	☐	☒
Art. 16 Processing of requests for rectification	☐	☒
Art. 17 Processing of cancellation requests	☐	☒
Art. 18 Processing of requests for restriction	☐	☒
Art. 19 Notification of rectification or erasure	☐	☒
Art. 20 Processing of requests for surrender	☐	☒
Art. 21 Processing of objections	☐	☒
Art. 22 Safeguarding the right to non-automated individual decisions	☐	☒
Art. 24 para. 1 in conjunction with. Art. 32 Implementation of technical and organisational measures	☐	☒
Art. 28 Utilisation of processors and, where applicable, sub-processors	☐	☒
Art. 30 Maintenance of a record of processing activities	☐	☒
Art. 33 and 34 Notification to the supervisory authority and notification to the data subject in the event of data breaches	☐	☒
Art. 35 Data protection impact assessment	☐	☒
Art. 36 Consultation with a supervisory authority	☐	☒
Art. 37 Appointment of a data protection officer	☐	☒

Obligations arising from the GDPR towards <u>Platform users</u>	**Responsible persons FU Berlin**	**Archive owner**
Determination of the purpose and means of data processing as well as the type of data and the group of data subjects	☒	☐
Art. 13 Information on the collection of personal data	☒	☐
Art. 14 Information if data was not collected from the data subject	☒	☐
Art. 15 Processing of requests for information	☒	☐
Art. 16 Processing of requests for rectification	☒	☐
Art. 17 Processing of cancellation requests	☒	☐
Art. 18 Processing of requests for restriction	☒	☐
Art. 19 Notification of rectification or erasure	☒	☐
Art. 20 Processing of requests for surrender	☒	☐
Art. 21 Processing of objections	☒	☐
Art. 22 Safeguarding the right to non-automated individual decisions	☒	☐
Art. 24 para. 1 in conjunction with. Art. 32 Implementation of technical and organisational measures	☒	☐
Art. 28 Utilisation of processors and, where applicable, sub-processors	☒	☐
Art. 30 Maintenance of a record of processing activities	☒	☐
Art. 33 and 34 Notification to the supervisory authority and notification to the data subject in the event of data breaches	☒	☐
Art. 35 Data protection impact assessment	☒	☐
Art. 36 Consultation with a supervisory authority	☒	☐
Art. 37 Appointment of a data protection officer	☒	☐

Appendix 1:

Technical and organisational measures in accordance with Art. 32 GDPR

a) Technical and organisational measures of the FU Berlin

Documentation of the technical and organisational measures to be taken in accordance with 32 GDPR[1] .

1.	**Pseudonymisation** How is the pseudonymisation of the data guaranteed? Pseudonymisation is the processing of personal data in such a manner that the personal 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 technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person.	☐ Personal data is processed by Random codes replaced ☐ Data Masking ☒ Other: Software enables pseudonymisation by archive owner if required
2.	**Encryption** How is encryption guaranteed? Encryption transforms plain text into an associated ciphertext (ciphertext) depending on additional information called a "key", which should be indecipherable for those who do not know the key.	☐ Use of cryptographic tools ☐ Data hashing ☐ Encryption of storage media ☒ Encryption of communication ☒ Other: Encryption of media files during HLS streaming
3.	**Ability to maintain confidentiality** How is data confidentiality guaranteed in the long term? Confidentiality means that personal related data is protected against unauthorised disclosure.	☒ Electronic access control system ☒ Security doors and/or windows ☐ Grilles in front of windows and doors ☐ Plant security, gatekeeper ☒ Alarm system ☐ Video surveillance ☒ Special protective measures for the server room ☒ Customised log-in and password procedure ☐ Additional log-in for certain applications ☐ Automatic blocking of clients (timeout) ☒ Management of authorisations

[1] This document serves to fulfil legal requirements and is intended to provide a **general** description that enables a **preliminary assessment to be made of** whether the data security measures taken are appropriate for the aspects addressed below. During the term of the contractual relationship, this data security concept must be continuously adapted and updated to reflect the current circumstances of order fulfilment. All adjustments and changes to the procedures for the fulfilment of the contract must be documented in writing. The document is part of the contract and must be submitted to the jointly responsible party in the event of significant changes and otherwise annually.

		☒ Documentation of authorisations ☐ Encryption of systems ☐ Encryption of communication ☐ Encryption of data carriers ☐ VPN (Virtual Private Network) ☐ Secure WLAN ☒ SSL encryption for web access ☐ Other:
4.	**Ability of integrity** How is the ability to ensure the integrity of the data permanently guaranteed? Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is applied to "data", it means that the data is complete and unchanged.	☒ Measures should be taken to prevent damage/alteration of the protected data during processing or transmission ☒ Use of access rights ☒ System logging ☐ Functional responsibilities ☐ Other:
5.	**Availability capability** How is the ability to make data available permanently guaranteed? The availability of services, functions of an IT system, IT applications or IT networks or even information is ensured if these can always be used by users as intended.	☒ Back-up procedure ☒ Mirroring hard drives ☒ Uninterruptible power supply (UPS) ☒ Virus protection /Firewall ☒ Emergency plan ☒ Air conditioning systems ☒ Fire and extinguishing water protection ☒ Alarm system ☐ Suitable archiving facilities ☐ Other:
6.	**Ability to work under pressure** How is the resilience of the data guaranteed in the long term? Systems are resilient if they are so robust that they can function even under heavy access or heavy utilisation.	☐ Penetration tests ☐ Other:
7.	**Recoverability of availability and access** How is it ensured that personal data is quickly available and accessible again after security incidents?	☒ Back-up procedure ☒ Uninterruptible power supply (UPS) ☒ Emergency plan ☐ Substitution rules ☐ Other:
8.	**Procedure for regular review*** How is it ensured that the aforementioned data backup measures are regularly reviewed?	☒ There is a defined test routine ☐ Test reports are evaluated ☐ Implementation of suggestions for improvement

		☐ Other:
9.	**Unlawful access to personal data** How can data processing systems be prevented from being used by unauthorised persons?	☒ Customised log-in and password procedure ☐ Additional log-in for certain applications ☐ Automatic blocking of clients (timeout) ☒ Management of authorisations ☒ Documentation of authorisations ☐ Encryption of systems ☐ Other:
10.	**Processing of personal data only according to instructions** How is it ensured that personal data is only processed in accordance with the controller's instructions?	☒ Employees are obliged to observe rules of conduct ☒ Implementation of internal company data protection guidelines ☒ Obligation of employees to maintain data confidentiality ☐ Training for all authorised employees ☒ Determination of contact persons and responsible project managers for the specific order ☐ Other:

b) Technical and organisational measures of the archive holder

Documentation of the technical and organisational measures to be taken in accordance with 32 GDPR[2] .

1.	**Pseudonymisation** How is the pseudonymisation of the data guaranteed? Pseudonymisation is the processing of personal data in such a manner that the personal 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 technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person.	☐ Personal data is processed by Random codes replaced ☐ Data Masking ☐ Other:
2.	**Encryption** How is encryption guaranteed? Encryption transforms plain text into an associated ciphertext (ciphertext) depending on additional information called a "key", which should be indecipherable for those who do not know the key.	☐ Use of cryptographic tools ☐ Data hashing ☐ Encryption of storage media ☐ Encryption of communication ☐ Other:
3.	**Ability to maintain confidentiality** How is data confidentiality guaranteed in the long term? Confidentiality means that personal data is protected against unauthorised disclosure.	☐ Electronic access control system ☐ Security doors and/or windows ☐ Grilles in front of windows and doors ☐ Plant security, gatekeeper ☐ Alarm system ☐ Video surveillance ☐ Special protective measures for the server room ☐ Customised log-in and password procedure ☐ Additional log-in for certain applications ☐ Automatic blocking of clients (timeout) ☐ Management of authorisations ☐ Documentation of authorisations ☐ Encryption of systems ☐ Encryption of communication ☐ Encryption of data carriers ☐ VPN (Virtual Private Network) ☐ Secure WLAN ☐ SSL encryption for web access

[2] This document serves to fulfil legal requirements and is intended to provide a **general** description that enables a **preliminary assessment to be made of** whether the data security measures taken are appropriate for the aspects addressed below. During the term of the contractual relationship, this data security concept must be continuously adapted and updated to reflect the current circumstances of order fulfilment. All adjustments and changes to the procedures for the fulfilment of the contract must be documented in writing. The document is part of the contract and must be submitted to the jointly responsible party in the event of significant changes and otherwise annually.

4.	**Ability of integrity** How is the ability to ensure the integrity of the data permanently guaranteed? Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is applied to "data", it means that the data is complete and unchanged.	☐ Measures should be taken to prevent damage/alteration of the protected data during processing or transmission ☐ Use of access rights ☐ System logging ☐ Functional responsibilities ☐ Other:
5.	**Availability capability** How is the ability to make data available permanently guaranteed? The availability of services, functions of an IT system, IT applications or IT networks or even information is ensured if these can always be used by users as intended.	☐ Back-up procedure ☐ Mirroring hard disks ☐ Uninterruptible power supply (UPS) ☐ Virus protection /Firewall ☐ Emergency plan ☐ Air conditioning systems ☐ Fire and extinguishing water protection ☐ Alarm system ☐ Suitable archiving facilities ☐ Other:
6.	**Ability to work under pressure** How is the resilience of the data guaranteed in the long term? Systems are resilient if they are so robust that they can function even under heavy access or heavy utilisation.	☐ Penetration tests ☐ Other:
7.	**Recoverability of availability and access** How is it ensured that personal data is quickly available and accessible again after security incidents?	☐ Back-up procedure ☐ Uninterruptible power supply (UPS) ☐ Emergency plan ☐ Substitution rules ☐ Other:
8.	**Procedure for regular review*** How is it ensured that the aforementioned data backup measures are regularly reviewed?	☐ There is a defined test routine ☐ Test reports are evaluated ☐ Implementation of suggestions for improvement
9.	**Unlawful access to personal data** How can data processing systems be prevented from being used by unauthorised persons?	☐ Customised log-in and password procedure ☐ Additional log-in for certain applications ☐ Automatic blocking of clients (timeout) ☐ Management of authorisations ☐ Documentation of authorisations ☐ Encryption of systems ☐ Other:

10.	**Processing of personal data only according to instructions** How is it ensured that personal data is only processed in accordance with the controller's instructions?	☐ Employees are obliged to observe rules of conduct ☐ Implementation of internal company data protection guidelines ☐ Obligation of employees to maintain data secrecy ☐ Training for all authorised employees ☐ Determination of contact persons and responsible project managers for the specific order