Vereinbarung zur Gemeinsamen Verantwortung über die Datenverarbeitung („Joint Control“)

zwischen

Freie Universität Berlin
vertreten durch den Präsidenten
Kaiserswerther Straße 16-18
14195 Berlin
ausführende Organisationseinheit
Universitätsbibliothek
Abteilung Forschungs- und Publikationsservices
Team Digitale Interview-Sammlungen
Garystr. 39
14195 Berlin
Ansprechpartner:
Dr. Cord Pagenstecher

und

Archivinhaber
vertreten durch
ausführende Organisationseinheit

Straße
PLZ, Ort
(im Folgenden: Archivinhaber)

Präambel

Die EU-Datenschutzgrundverordnung führt die „Gemeinsam für die Datenverarbeitung Verantwortlichen“ ein. Damit wird Situationen Rechnung getragen, in denen zwei oder mehrere Verantwortliche gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Hierin ist eine Unterscheidung zur klassischen „Auftragsverarbeitung“ zu sehen, im Rahmen derer die Entscheidungsgewalt weitgehend beim Verantwortlichen liegt und der Auftragsverarbeiter weisungsgebunden agiert. Ziel dieser Vereinbarung ist die Festlegung und Verteilung der bestehenden Rechte und Pflichten unter den oben genannten gemeinsam Verantwortlichen.

§ 1 Gegenstand der Datenverarbeitung

(1) Die Verantwortlichen führen die Erhebung, Verarbeitung und/oder Nutzung nachstehend bezeichneter personenbezogener Daten gemeinsam aus.
(2) Der Gegenstand der gemeinsamen Datenverarbeitung und damit der Zweck, die Art und der Umfang der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten ist die Durchführung der folgenden Aufgabe(n) durch die Vertragsparteien:

Aufgaben Freie Universität Berlin:

- Bereitstellung der technischen Infrastruktur für die Archivierung, Erschließung und Veröffentlichung der personenbezogenen Daten (Ton- und Videoaufzeichnungen, Transkripte, Begleitdokumente, Metadaten) im Portal Oral-History.Digital

- Übermittlung der personenbezogenen Daten der Interviewpartner*innen und anderer an der Aufzeichnung der Interviews Beteiligter (Ton- und Videoaufzeichnungen, Transkripte, Begleitdokumente, Metadaten zu Zwecken der Langzeitarchivierung
- Verwaltung und Organisation der personenbezogenen Daten von Archivinhabern und ihren Mitarbeiter*innen zu Zwecken der Registrierung (E-Mail-Adresse, Name, Kontaktdaten, Geschlecht, Titel, Beruf, Institution)
- Verwaltung und Organisation der personenbezogenen Daten von Nutzer*innen der Plattform zu Zwecken der Registrierung (E-Mail-Adresse, Name, Kontaktdaten, Geschlecht, Titel, Beruf, Institution)
- Verwaltung und Organisation von Nutzungsdaten auf der Plattform zu Zwecken der technischen Verbesserung und Anpassung (IP-Adresse, Cookies etc.)

Aufgaben Archivinhaber:

- Bereitstellung der Ton- und Videoaufzeichnungen (mit Transkripten, Begleitdokumenten und Metadaten), sofern erforderlich, nach Einwilligung der Interviewpartner*innen und anderer an der Aufzeichnung der Interviews Beteiligter
- Verwaltung der Registrierungsdaten der Nutzer*innen zwecks Berechtigungsvergabe für Zugriffe auf die Inhalte der Archive der Archivinhaber
- Bereitstellung der Registrierungsdaten der Archivinhaber und ihrer Mitarbeiter*innen zu Zwecken der Kompetenzvergabe

(3) Nachträgliche Änderungen der Aufgabenverteilung (Zweck, Art und Umfang der Datenverarbeitung) sind zu dokumentieren.

§ 2 Anlaufstelle für die betroffenen Personen

Anlaufstelle für die Plattformnutzer*innen ist die Freie Universität Berlin. Anlaufstelle für die Interviewpartner*innen und andere an den Interviews Beteiligte ist der Archivinhaber.

Die Parteien sind sich darüber bewusst, dass ungeachtet der bezüglich einer allgemeinen Anlaufstelle getroffenen Vereinbarung Betroffene ihre Rechte bei jedem einzelnen Verantwortlichen im Rahmen dieser Vereinbarung geltend machen können.

§ 3 Dauer der gemeinsam verantworteten Datenverarbeitung

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit der Kooperationsvereinbarung. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 4 Art der Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind die Daten aus folgenden Datenkategorien:

☐ Abrechnungsdaten	☒ Adressdaten	☐ Bankverbindungsdaten
☐ Biometrische Daten	☐ Bonitätsdaten	☐ Funktionsbezeichnung
☒ Geburtsdaten	☐ Gesundheitsdaten	☐ Interessen
☒ IT-Nutzungsdaten	☒ Kontaktdaten	☐ Lohn- und Gehaltsdaten
☒ Name	☐ Personalstammdaten	☐ Planungsdaten
☐ Qualifikationsdaten	☐ Sozialversicherungsdaten	☐ Telefonate
☐ Vertragsdaten	☐ Vertragsstammdaten	☒ Videoaufzeichnungen
☒ E-Mail-Adresse	☒ Geschlecht	☒ Tonaufzeichnungen
☒ Berufsspezifische Daten (Beruf, Titel, Institution)		☐ sonstige Daten:

Sofern sich der Umgang mit den angegebenen Datenkategorien einem jeweiligen Verantwortlichen zuordnen lässt, so kann die Aufteilung der verwendeten Datenarten wie folgt beschrieben werden:

Durch die Freie Universität Berlin verwendete Datenkategorien:

- Geburtsdaten
- IT-Nutzungsdaten
- Name
- E-Mail-Adresse
- Adressdaten/Kontaktdaten
- Geschlecht
- Berufsspezifische Daten
- Video- und Tonaufzeichnungen

Durch den Archivinhaber verwendete Datenkategorien:

- Geburtsdaten
- Name
- E-Mail-Adresse
- Adressdaten/Kontaktdaten
- Personalstammdaten
- Geschlecht
- Berufsspezifische Daten
- Video- und Tonaufzeichnungen

§ 5 Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst folgende Kategorien:

☒ Mitarbeiter*innen	☐ Lieferanten	☐ Veranstaltungsteilnehmer
☐ Bewerber	☐ Handelsvertreter	☐ Abonnenten
☐ Dienstleister	☐ Ansprechpartner	☐ Patienten
☐ Kunden/Mandanten	☐ Besucher/Gäste	☐ Passanten

☒ sonstige Betroffene: Interviewpartner*innen und andere an der Aufzeichnung der Interviews Beteiligte, Mitarbeiter*innen der Archivinhaber, Plattformnutzer*innen

Sofern die von der jeweiligen Verarbeitung Betroffenen sich dem/den entsprechend Verantwortlichen zuordnen lassen, so kann diese Zuordnung wie folgt beschrieben werden:

Von der Datenverarbeitung der Freien Universität Berlin Betroffene:

- Mitarbeiter*innen
- Interviewpartner*innen
- Andere an den Interviews Beteiligte
- Plattformnutzer*innen

Von der Datenverarbeitung des Archivinhabers Betroffene:

- Mitarbeiter*innen
- Interviewpartner*innen
- Andere an den Interviews Beteiligte
- Plattformnutzer*innen

§ 6 Wahrung der Betroffenenrechte

(1) Im Zuge der Datenverarbeitung kommen der/den betroffenen Person(en) umfassende Rechte zu („Betroffenenrechte"). Hiervon umfasst ist u.a. das Auskunftsrecht der betroffenen Person, das Recht auf Berichtigung und auf Löschung (bzw. „Recht auf Vergessenwerden"), das Recht auf Datenportabilität sowie das Recht auf allgemeinen Widerspruch oder gegenüber automatisierten Einzelentscheidungen. Es muss im Rahmen der gemeinsamen Verantwortung in transparenter Weise festgelegt sein, welcher Verantwortliche für die Wahrung welcher Betroffenenrechte zuständig ist.

(2) Es erfolgt eine funktionale Aufteilung der Zuständigkeiten hinsichtlich der normierten Betroffenenrechte, die sich wie folgt beschreiben lässt:

<u>Zuständigkeiten der Freien Universität Berlin:</u>
- Bearbeitung von Betroffenenanfragen der Plattformnutzer*innen
- Bearbeitung von Betroffenenanfragen von Mitarbeiter*innen

<u>Zuständigkeiten des Archivinhabers:</u>
- Bearbeitung von Betroffenenanfragen von Interviewpartner*innen
- Bearbeitung von Betroffenenanfragen von anderen an der Aufzeichnung und Archivierung der Interviews Beteiligten
- Bearbeitung von Betroffenenanfragen von Mitarbeiter*innen

§ 7 Pflicht zur Information über die Datenverarbeitung

(1) Sofern personenbezogene Daten bei der/den betroffenen Person(en) erhoben werden, so hat der im Rahmen dieser Vereinbarung zu bestimmende Verantwortliche der betroffenen Person im Sinne einer transparenten Verarbeitung die Mitteilungen gem. Art. 13 Abs. 1 und Abs. 2 DSGVO zu machen.

(2) Ähnliches gilt für die Situation, in der die Erhebung personenbezogener Daten nicht bei der betroffenen Person bzw. den betroffenen Personen erfolgt. Die Pflicht zur Information des/der Betroffenen richtet sich in diesem Fall nach Art. 14 Abs. 1 und Abs. 2 DSGVO.

(3) Die Freie Universität Berlin erfüllt im Rahmen dieser Vereinbarung die Informationspflichten gegenüber den Plattformnutzer*innen.
Der Archivinhaber erfüllt seine Informationspflichten gegenüber den Interviewpartner*innen und anderen Beteiligten an den eigenen Sammlungen bzw. eigens durchgeführten Interviewprojekten.

§ 8 Melde- und Benachrichtigungspflichten, Datenschutz-Folgenabschätzung und vorherige Konsultation

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten können die Verantwortlichen Pflichten zur Meldung bzw. Benachrichtigung treffen. Dies gilt für die unverzügliche Meldung des Verstoßes gegenüber der Datenschutz-Aufsichtsbehörde sowie für die Benachrichtigung des/der Betroffenen.

(2) Liegt für eine Form der Verarbeitung (z.B. aufgrund der verwendeten Technologien, der Art, des Umfangs, der Umstände) ein hohes Risiko für Rechte und Freiheiten der Betroffenen vor, so ist grundsätzlich eine Datenschutz-Folgenabschätzung durchzuführen. Sofern sich durch die Folgenabschätzung ein entsprechend hohes Risiko bestätigt, so haben die Verantwortlichen vor Beginn der Verarbeitung die Datenschutz-Aufsichtsbehörde zu konsultieren.

(3) Da die in den Absätzen 1 und 2 genannten Pflichten hinsichtlich ihrer Erfüllung in transparenter Form unter den jeweils Verantwortlichen festzulegen sind, ergibt sich hierfür folgende Aufteilung:

Zuständigkeiten der Freien Universität Berlin:
Melde- und Benachrichtigungspflichten, Datenschutz-Folgenabschätzung und vorherige Konsultation im Hinblick auf die Verarbeitung von Daten der Plattformnutzer*innen

Zuständigkeiten des Archivinhabers:
Melde- und Benachrichtigungspflichten, Datenschutz-Folgenabschätzung und vorherige Konsultation im Hinblick auf die Verarbeitung von Ton- und Videoaufzeichnungen und anderen Inhalten der Interviews

§ 9 Beiderseitige, nicht aufteilbare Verpflichtungen aus der DSGVO

(1) Alle für die (gemeinsame) Verarbeitung personenbezogener Daten Verantwortlichen haben unter Berücksichtigung der Umstände geeignete technische u. organisatorische Maßnahmen zu ergreifen, welche ein dem Risiko angemessenes Schutzniveau gewährleisten. Hiervon ist u.a. die Fähigkeit umfasst, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme auf Dauer sicherzustellen. Die Herstellung eines angemessenen Sicherheitsniveaus ist Aufgabe jedes einzelnen für die Datenverarbeitung Verantwortlichen. Die Vereinbarung konkreter technisch-organisatorischer Maßnahmen erfolgt in einer Anlage 1 zu diesem Vertrag und wird explizit in diesen einbezogen.
(2) Die Wahrung des Datengeheimnisses ist sicherzustellen. Alle für die Verantwortlichen handelnden Personen, die auf personenbezogene Daten der Betroffenen zugreifen können, müssen auf das Datengeheimnis und die Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Zweckbindung belehrt werden.
(3) Jeder Verantwortliche hat ein Verzeichnis über die Verarbeitungstätigkeiten zu führen, die seiner Zuständigkeit unterliegen.
(4) Die Vertragsparteien im Rahmen dieser Vereinbarung sind im Hinblick auf ihre Verpflichtungen aus den Regelungen der Datenschutzgrundverordnung und anderer Vorschriften über den Datenschutz selbst verantwortlich. Dies gilt hinsichtlich der in den Abs. 1-3 genannten Pflichten sowie weiterer formaler Datenschutzvorschriften (z.B. Bestellung eines betrieblichen Datenschutzbeauftragten).

§ 10 Auftragsverarbeitung

(1) Die Parteien sind berechtigt, für Verarbeitungen in ihrer jeweiligen Zuständigkeit Auftragsverarbeiter*innen im Sinne des Art. 28 DSGVO einzusetzen. Die Parteien führen jeweils eine Liste mit von ihnen für Verarbeitungsvorgänge nach dieser Vereinbarung beauftragten Auftragsverarbeiter*innen. Bei Vorliegen eines berechtigten Interesses (z. B. Kontrolle der Einhaltung der Pflichten nach diesem Vertrag, Anfrage einer Aufsichtsbehörde oder einer betroffenen Person) stellen sich die Parteien die Listen gegenseitig zur Verfügung, sofern die Anfrage nicht durch eine direkte Auskunft der jeweiligen Partei an die anfragende Person beantwortet werden kann.
(2) Die zum Zeitpunkt des Vertragsschlusses bereits mit Verarbeitungsvorgängen beauftragten Auftragsverarbeiter*innen, die von der jeweiligen Partei ebenfalls zur Erbringung der Verarbeitungsvorgänge nach dieser Vereinbarung eingesetzt werden, gelten als von den übrigen Parteien genehmigt.

(3) Die Parteien beauftragen nur solche Subunternehmer*innen, die die Anforderungen des Datenschutzrechts und die Festlegungen dieser Vereinbarung erfüllen. Nicht als Leistungen von Subunternehmer*innen im Sinne dieser Regelung gelten Dienstleistungen, die die Parteien bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nehmen, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Die Parteien sind jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der personenbezogenen Daten auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
(4) Die Parteien verpflichten sich, beim Einsatz von Auftragsverarbeiter*innen im Anwendungsbereich dieser Vereinbarung einen Vertrag nach Art. 28 DSGVO abzuschließen. Die beauftragende Partei muss ihren Auftragsverarbeiter*innen Verpflichtungen zu Datenschutz, Vertraulichkeit und Datensicherheit auferlegen, die den Anforderungen der Art. 28, 29 DSGVO genügen und zumindest so streng ausfallen, wie die in dieser Vereinbarung niedergelegten. Für den Fall der Ermöglichung zur Beauftragung von Unterauftragnehmer*innen haben die Parteien dafür Sorge zu tragen, dass die Auftragsverarbeiter*innen diese entsprechend verpflichten

§ 11 Prüfungsrechte

Die Verantwortlichen im Rahmen dieser Vereinbarung haben das Recht, die Kontrolle der Einhaltung der vertraglich vereinbarten Datenschutz- und Datensicherungsmaßnahmen bezüglich der im Rahmen dieser Vereinbarung überlassenen personenbezogenen Daten im Benehmen mit der/m Vertragspartner*in durchzuführen oder durch im Einzelfall zu benennende Prüfer*innen durchführen zu lassen. Jeder/m Verantwortlichen kommt das Recht zu, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung im Geschäftsbetrieb der/s Vertragspartners/in im Sinne dieser Vereinbarung zu überzeugen.

§ 12 Haftung u. uneingeschränkte Verantwortlichkeit gegenüber Betroffenen

(1) Ungeachtet der im Rahmen dieser Vereinbarung getroffenen Abmachungen hinsichtlich der Aufteilung von Verpflichtungen können betroffene Personen ihre Rechte bei und gegenüber jeder/m einzelnen der Verantwortlichen geltend machen. Der bloße Verweis/die Weiterleitung des/der Betroffenen an einen anderen Verantwortlichen im Rahmen dieser Vereinbarung ist unzulässig.
(2) Jede/r Verantwortliche haftet für den gesamten durch die Datenverarbeitung entstandenen Schaden zur Sicherstellung eines wirksamen Schadensersatzes für die betroffene(n) Person(en) (Art. 82 Abs. 4 DSGVO).
(3) Jede/r Verantwortliche, durch dessen unrichtige oder unzulässige Datenverarbeitung ein Schaden entstanden ist, haftet gegenüber seiner/m Vertragspartner*in im Sinne dieser Vereinbarung für ohne dessen eigenes Verschulden geleisteten Schadensersatz. Die Haftung im Innenverhältnis hat sich am jeweiligen Anteil an der Verantwortung für den etwaigen entstandenen Schaden zu orientieren (Art. 82 Abs. 5 DSGVO).

§ 13 Informationspflichten, Schriftformgebot

(1) Das Wesentliche dieser Vereinbarung ist den/dem Betroffenen auf Anfrage zur Verfügung zu stellen. Dies wird durch die Freie Universität Berlin sichergestellt.
(2) Sollten die Daten einer/s Verantwortlichen bei seiner/m Vertragspartner*in durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die/der jeweilige Verantwortliche ihre/seine(n) Vertragspartner*in unverzüglich darüber zu informieren.

(3) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen durch eine/n Verantwortliche/n oder Verantwortliche – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(4) Es gilt das unmittelbar und zwingend anzuwendende Recht der Europäischen Union sowie ggf. das national erlassene Recht der Bundesrepublik Deutschland.

§ 14 Salvatorische Klausel

(1) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.
(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der (datenschutz-)rechtlichen Zielsetzung am nächsten kommen, welche die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

_____	_____
Ort, Datum	Stempel/ Unterschrift Freie Universität Berlin
_____	_____
Ort, Datum	Stempel/ Unterschrift Archivinhaber

Checklisten zur vollständigen Aufgabenaufteilung bei „Joint Control"-Verträgen

Die Verantwortlichen legen gemäß Art. 26 Abs. 1 S. 2 DSGVO in einer Vereinbarung fest, „*wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt*". Das heißt, dass sich diese Regelung grundsätzlich auf alle Pflichten der EU-Datenschutzgrundverordnung erstreckt und über die gesondert (Wortlaut: „*insbesondere*") genannten Betroffenenrechte und Informationspflichten hinausgeht. Die folgenden beiden Checklisten dienen einem Überblick, welcher Verantwortliche welche Aufgabe übernimmt.

Pflichten aus der DSGVO gegenüber Interviewpartner*innen und an den Interviews Beteiligten	**Verantwortliche FU Berlin**	**Archivinhaber**
Festlegung des Zwecks und der Mittel der Datenverarbeitung sowie der Art der Daten und des Kreises der Betroffenen	☐	☒
Art. 13 Information bei Erhebung personenbezogener Daten	☐	☒
Art. 14 Information, wenn Daten nicht bei der betroffenen Person erhoben wurden	☐	☒
Art. 15 Bearbeitung von Auskunftsverlangen	☐	☒
Art. 16 Bearbeitung von Berichtigungsverlangen	☐	☒
Art. 17 Bearbeitung von Löschbegehren	☐	☒
Art. 18 Bearbeitung von Anfragen zur Beschränkung	☐	☒
Art. 19 Mitteilung bei Berichtigung oder Löschung	☐	☒
Art. 20 Bearbeitung von Herausgabeverlangen	☐	☒
Art. 21 Bearbeitung von Widersprüchen	☐	☒
Art. 22 Wahrung des Rechts auf nicht-automatisierte Einzelentscheidungen	☐	☒
Art. 24 Abs. 1 i.V.m. Art. 32 Umsetzung der technischen und organisatorischen Maßnahmen	☐	☒
Art. 28 Inanspruchnahme von Auftragsverarbeitern und ggf. Unterauftragsverarbeitern	☐	☒
Art. 30 Führung eines Verzeichnisses von Verarbeitungstätigkeiten	☐	☒
Artt. 33 und 34 Meldung an Aufsichtsbehörde und Benachrichtigung an den Betroffenen bei Datenpannen	☐	☒
Art. 35 Datenschutz-Folgeabschätzung	☐	☒
Art. 36 Konsultation einer Aufsichtsbehörde	☐	☒
Art. 37 Benennung eines Datenschutzbeauftragten	☐	☒

Pflichten aus der DSGVO gegenüber <u>Plattformnutzer*innen</u>	**Verantwortliche FU Berlin**	**Archivinhaber**
Festlegung des Zwecks und der Mittel der Datenverarbeitung sowie der Art der Daten und des Kreises der Betroffenen	☒	☐
Art. 13 Information bei Erhebung personenbezogener Daten	☒	☐
Art. 14 Information, wenn Daten nicht bei der betroffenen Person erhoben wurden	☒	☐
Art. 15 Bearbeitung von Auskunftsverlangen	☒	☐
Art. 16 Bearbeitung von Berichtigungsverlangen	☒	☐
Art. 17 Bearbeitung von Löschbegehren	☒	☐
Art. 18 Bearbeitung von Anfragen zur Beschränkung	☒	☐
Art. 19 Mitteilung bei Berichtigung oder Löschung	☒	☐
Art. 20 Bearbeitung von Herausgabeverlangen	☒	☐
Art. 21 Bearbeitung von Widersprüchen	☒	☐
Art. 22 Wahrung des Rechts auf nicht-automatisierte Einzelentscheidungen	☒	☐
Art. 24 Abs. 1 i.V.m. Art. 32 Umsetzung der technischen und organisatorischen Maßnahmen	☒	☐
Art. 28 Inanspruchnahme von Auftragsverarbeitern und ggf. Unterauftragsverarbeitern	☒	☐
Art. 30 Führung eines Verzeichnisses von Verarbeitungstätigkeiten	☒	☐
Artt. 33 und 34 Meldung an Aufsichtsbehörde und Benachrichtigung an den Betroffenen bei Datenpannen	☒	☐
Art. 35 Datenschutz-Folgeabschätzung	☒	☐
Art. 36 Konsultation einer Aufsichtsbehörde	☒	☐
Art. 37 Benennung eines Datenschutzbeauftragten	☒	☐

Anlage 1:

Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

a) Technisch-organisatorische Maßnahmen der FU Berlin

Dokumentation der nach 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen[1].

1.	**Pseudonymisierung** Wie wird die Pseudonymisierung der Daten gewährleistet? Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.	☐ Personenbezogene Daten werden durch Zufallscodes ersetzt ☐ Data Masking ☒ Sonstige: Software ermöglicht bei Bedarf Pseudonymisierung durch Archivinhaber
2.	**Verschlüsselung** Wie wird die Verschlüsselung gewährleistet? Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.	☐ Nutzung von kryptografischen Tools ☐ Data Hashing ☐ Verschlüsselung von Speichermedien ☒ Verschlüsselung der Kommunikation ☒ Sonstige: Verschlüsselung der Mediendateien beim HLS-Streaming
3.	**Fähigkeit der Vertraulichkeit** Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	☒ Elektronisches Zutrittskontrollsystem ☒ Sicherheitstüren und/oder -fenster ☐ Gitter vor Fenstern und Türen ☐ Werkschutz, Pförtner ☒ Alarmanlage ☐ Videoüberwachung ☒ Spezielle Schutzvorkehrungen für den Serverraum ☒ Individueller Log-In und Kennwortverfahren

[1] Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine **allgemeine** Beschreibung darstellen, die es ermöglicht, **vorläufig** zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem gemeinsam Verantwortlichen bei wesentlichen Änderungen und im Übrigen jährlich vorzulegen.

		☐ Zusätzlicher Log-In für bestimmte Anwendungen ☐ Automatische Sperrung der Clients (Zeitablauf) ☒ Verwaltung von Berechtigungen ☒ Dokumentation von Berechtigungen ☐ Verschlüsselung von Systemen ☐ Verschlüsselung der Kommunikation ☐ Verschlüsselung von Datenträgern ☐ VPN (Virtual Private Network) ☐ Gesichertes WLAN ☒ SSL-Verschlüsselung bei Web-Access ☐ Sonstige:
4.	**Fähigkeit der Integrität** Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet? Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.	☒ Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern ☒ Verwendung von Zugriffsrechten ☒ Systemseitige Protokollierungen ☐ Funktionelle Verantwortlichkeiten ☐ Sonstige:
5.	**Fähigkeit der Verfügbarkeit** Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet? Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	☒ Back-Up Verfahren ☒ Spiegeln von Festplatten ☒ Unterbrechungsfreie Stromversorgung (USV) ☒ Virenschutz /Firewall ☒ Notfallplan ☒ Klimaanlagen ☒ Brand- und Löschwasserschutz ☒ Alarmanlage ☐ Geeignete Archivierungsräumlichkeiten ☐ Sonstige:
6.	**Fähigkeit der Belastbarkeit** Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet? Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.	☐ Penetrationstests ☐ Sonstige:

7.	**Wiederherstellbarkeit der Verfügbarkeit und des Zugangs** Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?	☒ Back-Up Verfahren ☒ Unterbrechungsfreie Stromversorgung (USV) ☒ Notfallplan ☐ Vertretungsregelungen ☐ Sonstige:
8.	**Verfahren zur regelmäßigen Überprüfung** Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?	☒ Es existiert eine festgelegte Prüfroutine ☐ Prüfberichte werden evaluiert ☐ Implementierung von Verbesserungsvorschlägen ☐ Sonstige:
9.	**Unrechtmäßiger Zugang zu personenbezogenen Daten** Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?	☒ Individueller Log-In und Kennwortverfahren ☐ Zusätzlicher Log-In für bestimmte Anwendungen ☐ Automatische Sperrung der Clients (Zeitablauf) ☒ Verwaltung von Berechtigungen ☒ Dokumentation von Berechtigungen ☐ Verschlüsselung von Systemen ☐ Sonstige:
10.	**Verarbeitung personenbezogener Daten nur nach Anweisung** Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?	☒ Mitarbeiter sind zu Verhaltensregeln verpflichtet ☒ Implementierung unternehmensinterner Datenschutz-Richtlinien ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis ☐ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag ☐ Sonstige:

b) Technisch-organisatorische Maßnahmen des Archivinhabers

Dokumentation der nach 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen[2].

1.	**Pseudonymisierung** Wie wird die Pseudonymisierung der Daten gewährleistet? Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.	☐ Personenbezogene Daten werden durch Zufallscodes ersetzt ☐ Data Masking ☐ Sonstige:
2.	**Verschlüsselung** Wie wird die Verschlüsselung gewährleistet? Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.	☐ Nutzung von kryptografischen Tools ☐ Data Hashing ☐ Verschlüsselung von Speichermedien ☐ Verschlüsselung der Kommunikation ☐ Sonstige:
3.	**Fähigkeit der Vertraulichkeit** Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	☐ Elektronisches Zutrittskontrollsystem ☐ Sicherheitstüren und/oder -fenster ☐ Gitter vor Fenstern und Türen ☐ Werkschutz, Pförtner ☐ Alarmanlage ☐ Videoüberwachung ☐ Spezielle Schutzvorkehrungen für den Serverraum ☐ Individueller Log-In und Kennwortverfahren ☐ Zusätzlicher Log-In für bestimmte Anwendungen ☐ Automatische Sperrung der Clients (Zeitablauf) ☐ Verwaltung von Berechtigungen ☐ Dokumentation von Berechtigungen ☐ Verschlüsselung von Systemen ☐ Verschlüsselung der Kommunikation

[2] Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine **allgemeine** Beschreibung darstellen, die es ermöglicht, **vorläufig** zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem gemeinsam Verantwortlichen bei wesentlichen Änderungen und im Übrigen jährlich vorzulegen.

		☐ Verschlüsselung von Datenträgern ☐ VPN (Virtual Private Network) ☐ Gesichertes WLAN ☐ SSL-Verschlüsselung bei Web-Access
4.	**Fähigkeit der Integrität** Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet? Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.	☐ Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern ☐ Verwendung von Zugriffsrechten ☐ Systemseitige Protokollierungen ☐ Funktionelle Verantwortlichkeiten ☐ Sonstige:
5.	**Fähigkeit der Verfügbarkeit** Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet? Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	☐ Back-Up Verfahren ☐ Spiegeln von Festplatten ☐ Unterbrechungsfreie Stromversorgung (USV) ☐ Virenschutz /Firewall ☐ Notfallplan ☐ Klimaanlagen ☐ Brand- und Löschwasserschutz ☐ Alarmanlage ☐ Geeignete Archivierungsräumlichkeiten ☐ Sonstige:
6.	**Fähigkeit der Belastbarkeit** Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet? Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.	☐ Penetrationstests ☐ Sonstige:
7.	**Wiederherstellbarkeit der Verfügbarkeit und des Zugangs** Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?	☐ Back-Up Verfahren ☐ Unterbrechungsfreie Stromversorgung (USV) ☐ Notfallplan ☐ Vertretungsregelungen ☐ Sonstige:
8.	**Verfahren zur regelmäßigen Überprüfung** Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?	☐ Es existiert eine festgelegte Prüfroutine ☐ Prüfberichte werden evaluiert ☐ Implementierung von Verbesserungsvorschlägen
9.	**Unrechtmäßiger Zugang zu personenbezogenen Daten**	☐ Individueller Log-In und Kennwortverfahren

	Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?	☐ Zusätzlicher Log-In für bestimmte Anwendungen ☐ Automatische Sperrung der Clients (Zeitablauf) ☐ Verwaltung von Berechtigungen ☐ Dokumentation von Berechtigungen ☐ Verschlüsselung von Systemen ☐ Sonstige:
10.	**Verarbeitung personenbezogener Daten nur nach Anweisung** Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?	☐ Mitarbeiter sind zu Verhaltensregeln verpflichtet ☐ Implementierung unternehmensinterner Datenschutz-Richtlinien ☐ Verpflichtung der Mitarbeiter auf das Datengeheimnis ☐ Schulungen aller zugriffsberechtigten Mitarbeiter ☐ Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag