Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 Abs. 3 DSGVO im Rahmen der Nutzung des Videokonferenztools des KITA HUB

Zwischen

- Verantwortlicher (nachfolgend **Auftraggeber** genannt) -

und

Staatsinstitut für Frühpädagogik und Medienkompetenz (IFP)
Mildred-Scheel-Str. 4, 92224 Amberg
- Auftragsverarbeiter (nachfolgend **Auftragnehmer** genannt) -

Präambel

Diese Vereinbarung regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer nach Art. 28 Abs. 3 DSGVO zum Schutz der personenbezogenen Daten betroffener Personen. Die Vereinbarung ergänzt insoweit die zugrunde liegenden Allgemeinen Geschäftsbedingungen des Auftragnehmers.

1. Gegenstand, Dauer, Spezifizierung und Ort der Auftragsverarbeitung

1.1 Der Auftragnehmer ermöglicht dem Auftraggeber die Nutzung des auf Systemen des Auftragnehmers und dessen Unterauftragnehmer betriebenen Videokonferenzsystems BigBlueButton (Dienst) gemäß der vereinbarten Nutzungsbedingungen. Die Verarbeitung umfasst die Bereitstellung, Administration und Wartung des Dienstes.

1.2 Die Verarbeitung erfolgt solange, bis der Auftraggeber die in den Nutzungsbedingungen festgelegten Voraussetzungen nicht mehr erfüllt oder bis der Auftraggeber das Ende der Verarbeitung anweist.

1.3 Es werden folgende Arten personenbezogener Daten verarbeitet:

- Daten aus Nutzerprofilen: Vorname, Nachname, Einrichtung, E-Mail, Passwort

    - Meeting-Inhaltsdaten: Audio-, Video- und ggf. Textdaten, Chatinhalte, geteilte Notizen
    - Meeting-Metadaten: Thema, Namen des Konferenzraums, Beschreibung
- Bei Aufzeichnung: MP4-Datei aller Video- und Audioaufnahmen und Präsentationen, M4A-Datei aller Audioaufnahmen, Textdatei des Chatverlaufs, Audio-Protokolldatei
- Cachefiles, die beim Schließen eines Konferenzraums automatisch gelöscht werden
- Logdaten (Name des Konferenzraums, selbst gewählter Name der Teilnehmenden Personen, IP-Adressen der Teilnehmenden, Dateinamen von ausgetauschten Dateien, Informationen über den Zugang und das Verlassen eines Raums)

Im Rahmen der Nutzung des Dienstes dürfen keine besonderen Kategorien personenbezogener Daten i. S. d. Art. 9 Abs. 1 DSGVO verarbeitet werden.

1.4 Von der Verarbeitung betroffen sind folgende Personen:

- Beschäftigte des Auftraggebers
- Sonstige Personen, die an Videokonferenzen des Auftraggebers teilnehmen

1.5 Die vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. Rechte und Pflichten des Auftragnehmers

2.1 Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers sowie entsprechend den datenschutzrechtlichen Regelungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. a DSGVO). Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke und insbesondere nicht für eigene Zwecke. Kopien der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.
Sofern Weisungen des Auftraggebers zunächst mündlich erfolgen, sind sie unverzüglich schriftlich oder elektronisch zu bestätigen.

2.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Unterabs. 2 DSGVO). Ist die Rechtmäßigkeit einer Weisung zweifelhaft, ist der Auftragnehmer berechtigt, die Durchführung der Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Stehen schwere Persönlichkeitsrechtsverletzungen im Raum oder nimmt der Auftragnehmer bei weisungsgemäßem Handeln das Risiko einer strafbaren Handlung auf sich, darf er die Umsetzung der Weisung darüber hinaus aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

2.3 Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft insbesondere geeignete technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten des Auftraggebers zu gewährleisten (Art. 32 Abs. 1 DSGVO). Sofern personenbezogene Daten in Telearbeit und Heimarbeit verarbeitet werden, ist er verpflichtet, dies dem Auftraggeber mitzuteilen. Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 1. Änderungen der getroffenen Maßnahmen durch den Auftragnehmer sind nur zulässig, wenn sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen und mit diesem abzustimmen.

2.4 Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (Art. 28 Abs. 3 Unterabs. 1 Buchst. e DSGVO) nachzukommen und unterstützt den Auftraggeber unter Berücksichtigung der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

2.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. b DSGVO). Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

2.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

2.7 Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen Aufbewahrungspflichten.

2.8 Nach Auftragsende sind Daten (einschließlich vorhandener Kopien), Datenträger sowie sonstige Materialien auf Verlangen und nach Wahl des Auftraggebers entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. g DSGVO).

2.9 Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3. Rechte und Pflichten des Auftraggebers

3.1 Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, die Datenweitergabe an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

3.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich, falls er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.3 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3.4 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen. Die Befugnisse der Aufsichtsbehörden – insbesondere nach Art. 58 Abs. 1 DSGVO – bleiben hiervon unberührt.

4. Anfragen betroffener Personen

Macht eine betroffene Person ihre Rechte gemäß Art. 15 ff. DSGVO gegenüber dem Auftragnehmer geltend, wird dieser die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Nr. 2.4 dieser Vereinbarung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte.

5. Kontrollrechte des Auftraggebers

5.1 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 Unterabs. 1 Satz 2 Buchst. h DSGVO*).*

5.2 Der Auftraggeber ist berechtigt, sich vor Beginn und während der Verarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen. Dies und Maßnahmen nach Nr. 5.4 werden nicht durch die Vorlage von Nachweisen nach Nr. 5.1 ausgeschlossen.

5.4 Inspektionen durch den Auftraggeber oder durch einen von diesem beauftragten Prüfer werden grundsätzlich nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlauffrist zu den üblichen Geschäftszeiten durchgeführt. Der Auftragnehmer hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen, wenn die Möglichkeit besteht, dass der Auftraggeber oder ein von diesem beauftragte(r) Prüfer / Prüferin im Rahmen seiner / ihrer Inspektion auch Kenntnis von Daten erlangt, die der Auftragnehmer im Auftrag eines anderen Verantwortlichen verarbeitet. Der Auftraggeber stellt sicher, dass ein von ihm beauftragter Prüfer / Prüferin in keinem Wettbewerbsverhältnis zu dem Auftragnehmer steht.

6. Unterauftragsverarbeiter (weitere Auftragsverarbeiter)

6.1 Ein Unterauftragsverarbeitungsverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragsverarbeiter mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer trägt bei der Auswahl eines Unterauftragsverarbeiters insbesondere Sorge dafür, dass dieser hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der Datenschutz-Grundverordnung erfolgt. Nicht als Unterauftragsverarbeitungsverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn ein Zugriff auf personenbezogene Daten des Auftraggebers ausgeschlossen ist), Reinigungskräfte und Prüfer. Der Auftragnehmer trifft mit diesen Dritten im erforderlichen Umfang schriftliche Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten und behält sich Kontrollmaßnahmen vor, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

6.2 Der Auftragnehmer nimmt keinen Unterauftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung in Anspruch. Der Auftragnehmer teilt dem Auftraggeber die bereits bei Abschluss dieses Vertrags bestehenden Unterauftragsverarbeitungsverhältnisse vorab mit. Die bei Vertragsbeginn bestehenden Unterauftragsverarbeitungsverhältnisse sind in Anlage 2 zu diesem Vertrag aufgeführt. Diese gelten als von Beginn des Auftrages an genehmigt.

6.3 Gemäß den vorgenannten Regelungen erteilt der Auftraggeber dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 Abs. 2 DSGVO in Anspruch zu nehmen (Art. 28 Abs. 2 Satz 1 Alt. 2, Satz 2 DSGVO). Der Auftragnehmer informiert den Auftraggeber frühzeitig, wenn er Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Der Einspruch ist innerhalb von einem Monat nach Zugang der Information über die Änderungen schriftlich gegenüber dem Auftragnehmer einzulegen. Kann keine einvernehmliche Lösung erzielt werden, erfolgt eine Einschränkung oder Beendigung der Auftragsverarbeitung.

6.4 Der Vertrag mit dem Unterauftragsverarbeiter muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). In dem Vertrag mit dem Unterauftragsverarbeiter sind dieselben datenschutzrechtlichen Pflichten aus der vorliegenden Vereinbarung diesem wirksam aufzuerlegen. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragsverarbeitern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

6.5 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragsverarbeiter den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Abschnitt vertraglich auferlegt wurden (Art. 28 Abs. 4 Satz 2 DSGVO).

6.6 Eine Beauftragung von Unterauftragsverarbeitern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftraggeber vorab zustimmt.

7. Haftung und Schadensersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

8. Schlussbestimmungen

8.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn die Daten des Auftraggebers durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter beim Auftragnehmer gefährdet werden. Der Auftragnehmer informiert in diesem Fall alle Beteiligten unverzüglich darüber, dass das Eigentum an den Daten ausschließlich beim Auftraggeber liegt.

8.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen oder in einem elektronischen Format abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt.

8.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

Amberg, Dezember 2023

Anlage 1 – Technische und Organisatorische Maßnahmen

Nr.	Ergriffene technische und organisatorische Maßnahmen
1.	**Zutrittskontrolle**
1.1	Zutrittsregelungen zu Diensträumen
1.2	Schlüsselmanagement mit spezifischen Identitätskennungen
1.3	Sicherheitsschlösser
1.4	Sichere Aufbewahrung durch abschließbare Schränke
1.5	Besuch nur in Begleitung von Mitarbeitenden
1.6	Sorgfalt bei der Auswahl von Reinigungsdiensten
1.7	Videoüberwachung der Eingänge
2.	**Zugangskontrolle**
2.1	Mitarbeitenden ist ein eigener Benutzerstammsatz zugeordnet.
2.2	Zugriffsrechte auf verschiedene Netzsegmente sind eingeschränkt auf Tätigkeitsbereiche (z.B. Kurstätigkeiten vs. Verwaltungsaufgaben).
2.3	Zugang zu informationstechnischen Systemen ist mindestens durch Benutzername und Passwort geschützt (Ausnahme: Telefon).
2.4	Passwortrichtlinie
2.5	IT-Systeme werden durch Firewall ihrer Funktionen entsprechend voneinander separiert und vor unerlaubten Zugriffen geschützt.
2.6	Nicht mehr benötigte Zugangsberechtigungen werden entzogen.
3.	**Zugriffskontrolle**
3.1	Rollenbasiertes Zugriffssystem gewährt den Zugriff zu IT-Systemen und Daten nur gemäß den zugeordneten Tätigkeitsbereichen.
3.2	Berechtigungskonzepte und Zugriffsrechte sind den spezifischen Gegebenheiten der IT-Systeme und den Anforderungen der Mitarbeitertätigkeit angepasst.
3.3	Strikte und teilweise physikalische Trennung von Datennetzen entsprechend ihrer Risikobewertung.
4.	**Weitergabekontrolle**
4.1	IT-Systeme, auf die über das Internet zugriffen werden kann, sind grundsätzlich nur über dem aktuellen Stand der Technik entsprechend verschlüsselte Transportwege erreichbar.
4.2	Auf IT-Geräten, die außerhalb der Betriebsräume genutzt werden (z.B. Laptop, Tablet) dürfen sensible Daten nur in verschlüsselter Form gespeichert werden.
4.3	Sensible Daten dürfen nur in verschlüsselter Form oder auf verschlüsselten Datenträgern aus den Unternehmensräumlichkeiten mitgenommen werden.
4.4	Eine Übertragung von Daten zwischen IFP und Auftragsverarbeitern ist nur über dem aktuellen Stand der Technik entsprechend verschlüsselte Transportwege möglich.
4.5	Im Rahmen der Audits werden Abruf- und Übermittlungsvorgänge Regelmäßige Audits zur Prüfung von Abruf- und Übermittlungsvorgängen und Kontrolle von Datenempfängern.
5.	**Eingabekontrolle**
5.1	Eingaben und Änderungen auf dem zentralen Fileserver werden durch eine interne Protokollierung erfasst.
5.2	Zugang zu Systemen und Diensten zur Verarbeitung personenbezogener Daten wird durch rollenbasierte Zugriffssysteme nur den entsprechend autorisierten Personen ermöglicht.
6.	**Auftragskontrolle**
6.1	Sicherstellung der weisungsgemäßen Durchführung der Auftragsverarbeitung und Gestaltung der internen Organisation derart, dass Weisungen des Auftraggebers

	berücksichtigt werden und sich die Datenverarbeitung innerhalb der Grenzen des abgeschlossenen Vertrags bewegt.
6.2	Auftragsverarbeitung beruht auf einem eindeutig ausgestalteten Vertrag, der die Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer abgrenzt, die durchzuführenden Kontrollmaßnahmen festlegt und die eindeutige Erteilung von Weisungen in schriftlicher Form festschreibt.
6.3	Information über die getroffenen technischen und organisatorischen Sicherheitsmaßnahmen und über die Regelung des Einsatzes von Unterauftragnehmern.
6.4	Trennung personenbezogener Daten einzelner Auftraggeber und Daten aus eigener Erhebung.
7.	**Verfügbarkeitskontrolle**
7.1	Zentrale IT-Systeme können aus Redundanzbeständen der Hardware kurzfristig neu aufgesetzt werden.
7.2	Serversysteme und Windows-Arbeitsplätze werden automatisch mit den neuesten Patches versehen.
7.3	Periodische Backups der im Sicherungsprozess definierten Daten und Systeme werden über einen Cloudspeicher außerhalb des Betriebsgeländes gespeichert.
7.4	Unterbrechungsfreie Stromversorgung für den zentralen Fileserver kann kurze Ausfälle überbrücken und ein definiertes Abschalten des Systems bei längerem Ausfall ermöglichen.
8.	**Trennungskontrolle**
8.1	Logische Trennung der Daten für verschiedene Auftraggeber.
8.2	Klare Trennung der für verschiedene Zwecke gespeicherten Daten.
8.3	Auf die jeweiligen Datensätze angepasste Datenbankrechte und Berechtigungskonzepte.
8.4	Benachrichtigungen an einzelne Betroffene eines Auftraggebers oder eines Projektes werden ohne gegenseitige Kenntnisnahme einzelner Betroffener ausgeführt.
8.5	Unterscheidung zwischen Produktiv- und Testsystemen.
9.	**Löschkontrolle**
9.1	Daten werden gemäß den im Verfahrensverzeichnis angegebenen Fristen gelöscht.
9.2	Löschung wird im Rahmen der Audits stichprobenartig kontrolliert.
9.3	Datenträger werden so gelöscht und entsorgt oder vernichtet, dass keine Daten in unberechtigte Hände gelangen.
9.4	Papierdokumente werden mit geeigneten Aktenvernichtern gemäß DIN-Norm 66399 Schutzklasse 2, Sicherheitsstufe P-3 oder P-4 vernichtet.
10.	**Pseudonymisierung und Verschlüsselung**
10.2	Einsatz verschlüsselter Übertragungswege nach aktuellem Stand der Technik (z.B. IPSec, TLS).
10.3	Personenbezogene Daten, die im Rahmen der internen Entwicklung von Kursen oder Seminaren (z.B. Online-Schulungen) zu Trainings- und Testzwecken genutzt werden, stehen nur in anonymisierter Form zur Verfügung.
11.	**Überprüfung, Bewertung und Evaluierung der Wirksamkeit**
11.1	Bei IT-Systemen werden datenschutzfreundliche Betriebsparameter nachgepflegt, soweit sie nicht ohnehin Voreinstellungen sind und zu keinen Einschränkungen führen (z.B. die Nutzung von Videokonferenzen).
11.2	Externe Dienstleister zur Auftragsverarbeitung werden ihrer DSGVO-Konformität entsprechend ausgewählt. Auftragsverarbeiter werden zur Erfassung der Änderungen ihrer Datenverarbeitung im zweijährigen Turnus kontaktiert.

11.3	Auditierungen der Maßnahmen werden in regelmäßigen Abständen durchgeführt.
12.	**Weitere organisatorische Maßnahmen**
12.1	Verpflichtung der Mitarbeitenden auf das Datengeheimnis und zur Verschwiegenheit
12.2	Regelmäßige Schulungen zum Datenschutz und Informationssicherheit.
12.3	Arbeitsanweisung zu den Sicherheitsmaßnahmen am IFP.
12.4	Anweisung zu Sicherheitsmaßnahmen bei mobiler Arbeit und Telearbeit.
13.	**Weitere technische Maßnahmen**
13.1	Alle Windows-Systeme haben einen Virenscanner installiert.
13.2	Alle Windows-Systeme sind mit aktivierter Firewall konfiguriert.
13.3	Die Anmeldung an den PC-Systemen der Mitarbeiter erfolgt über lokale Benutzer.
13.4	Bewegliche Datenträger (USB-Sticks usw.) werden in abgeschlossenen Schränken aufbewahrt, wenn sie nicht benutzt werden.

Anlage 2 – Liste der Unterauftragsverarbeitungsverhältnisse

Auftragnehmer	**Funktion**
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen Burckhardtweg 4, 37077 Göttingen	Serverbetrieb, Support, Monitoring, Fehlerbehebung