ICARUS
INTERNATIONALES ZENTRUM
FÜR ARCHIVFORSCHUNG

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 Datenschutz-Grundverordung | DSGVO

zwischen

im Folgenden **Auftraggeber** genannt

und

ICARUS – Internationales Zentrum für Archivforschung
Gertrude-Fröhlich-Sandner-Straße 2-4, Tower C, Floor 7
A-1100 Wien

E-mail: info@icar-us.eu
Vereinssitz: Wien, Österreich
Rechtsform: gemeinnützige Organisation
ZVR 250156583
im Folgenden **Auftragnehmer** genannt

1. Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Vertragsverhältnis („Topothek – Allgemeine Kooperationsbedingungen") gemachten Angaben.
Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber i.S.v.Art.4 Nr.2 und Art.28 DS-GVO auf Grundlage dieses Auftrags.

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die **Art der Daten** und der **Kreis der Betroffenen** sind:

Art der Daten

Datenkategorie	Datenfeld
1. Kooperationspartner (Gde. + Kontaktperson)	Vorname Nachname Kontaktdaten (Tel.) Kontaktdaten (Email)
2. Einpflegende von Daten	Vorname Nachname Kontaktdaten (Tel.) Kontaktdaten (Email)
3. Zurverfügungsteller von Primärdaten	Vorname Nachname Adresse Kontaktdaten (Tel.) Kontaktdaten (Email) Primärdatei Erstellungsdatum Zustimmungserklärung
4. Urheber der Primärdaten	Vorname Nachname Primärdatei Erstellungsdatum Zustimmungserklärung
5. Rechtehalter der Primärdaten	Vorname Nachname Kontaktdaten (Email)
6. Abgebildete oder Genannte auf Primärdaten	Vorname Nachname in Primärdatei sichtbar Erstellungsdatum Metadaten Zustimmungserklärung
7. Beantworter von a.d. Topothek gestellten Fragen	Vorname Nachname Kontaktdaten (Email) Zustimmungserklärung (Checkbox)
8. Mitarbeiter und **Lieferanten** des Auftraggebers	Vorname Nachname Kontaktdaten (Tel.) Kontaktdaten (Email)

Kreis der Betroffenen

Der Kreis der durch diese Zusatzvereinbarung Betroffenen umfasst:
1. Kooperationspartner (Gemeinden) und deren Ansprechpartner
2. Im Namen der Kooperationspartner ehrenamtlich Tätige (TopothekarInnen)
3. Zurverfügungsteller der Primärdaten, die in der Topohtek gezeigt werden
4. Urheber der Primärdaten, die in der Topothek gezeigt werden
5. Rechtehalter der Primärdaten, die in der Topothek gezeigt werden.
6. Abgebildete, die auf Bildern oder Schriftstücken in der Topothek gezeigt werden
7. Beantworter von auf der Topothek gestellten Fragen (Antwortformular)
8. Mitarbeiter und Lieferanten des Auftraggebers

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Technisch-organisatorische Maßnahmen

nach Art. 32 DS-GVO

1.
Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben (siehe **ANHANG 1**).
Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

2.
Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 Satz 2 lit.c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

3.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Löschung, Berichtigung, Sperrung von Daten

1.
Das Recht auf Löschung (Recht auf Vergessenwerden), Recht auf Berichtigung, Recht auf Einschränkung der Verarbeitung, Datenportabilität und Auskunft (das sind die in Kapitel III der DSGVO genannte Rechte) sind unmittelbar durch den Verantwortlichen sicherzustellen. Der Auftragnehmer hat den Auftraggeber allerdings bei der Wahrung dieser Rechte zu unter-

stützen und trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der Auftraggeber Anträge auf Wahrnehmung dieser in Kapitel III genannten Rechte jederzeit gegenüber einem Betroffenen innerhalb der gesetzlichen Fristen nachkommen kann, und überlässt dem Auftraggeber alle dafür notwendigen Informationen unverzüglich nach Anfrage durch den Verantwortlichen spätestens jedoch innerhalb von 10 Werktagen.

2.
Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

3.
Soweit ein Betroffener das Recht auf Datenübertragbarkeit geltend macht, ist der Auftragnehmer je nach Weisung des Auftraggebers verpflichtet, die Daten in einem strukturierten gängigen und maschinenlesbaren Format – welches vom Auftraggeber bestimmt wird – entweder direkt an den Betroffenen oder an den Verantwortlichen bereitzustellen, oder die Daten an einen namhaft gemachten Verantwortlichen zu übermitteln.
Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Als Datenschutzzuständiger ist beim Auftragnehmer
  Mag. Alexander Schatek, +43 (0)2622 28 150, as@topothek.at bestellt.
  Ein Wechsel des Datenschutzzuständigen ist dem Auftraggeber unverzüglich mitzuteilen.
  Dessen jeweils aktuelle Kontaktdaten sind auf der Website
  https://www.topothek.at/de/datenschutz/ hinterlegt.

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO.
  Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO

und **ANHANG 1**.

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

- Dokumentation der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber gemäß **ANHANG 1**

6. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Providerleistungen, Renderservice f. Video- und pdf-Vorbereitung, Support, Wartung sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
Eine Liste der eingesetzten Subunternehmer finden Sie unter
https://www.topothek.at/de/datenschutz/

7. Kontrollrechte des Auftraggebers

1.
Der Auftraggeber hat das Recht, im Einvernehmen mit dem Auftragnehmer Überprüfungen

durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die ein Monat vor der Kontrollhandlung anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

2.
Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

3.
Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO erfolgen.

4.
Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

1.
Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören:

a. **die Sicherstellung eines angemessenen Schutzniveaus** durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige,Feststellung von relevanten Verletzungsereignissen ermöglichen

b. **die Verpflichtung**, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c. **die Verpflichtung**, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d. **die Unterstützung** des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e. **die Unterstützung** des Auftraggebers im Rahmen vorheriger Konsultationen mit der

Aufsichtsbehörde

2.
Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

1.
Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

2.
Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

1.
Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2.
Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

3.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstige Vereinbarungen

Gerichtsstand
Die Parteien vereinbaren als Gerichtsstand Wiener Neustadt.

Ort: ....., am .....

.....	.....
Auftraggeber	Auftragnehmer ICARUS Dr. Thomas Aigner

ANHANG 1
Technisch-organisatorische Maßnahmen

nach Art. 32 DS-GVO (Art.28 Abs.3 Satz 2 lit.c DS-GVO)

1.
Vertraulichkeit

a. **Zutrittskontrolle**
- zur Datenverabeitungsanlage: nicht möglich, da es sich um eine Server Farm (Hetzner, DE) handelt.
- zu Büros: Schlüssel, nur für Betriebsangehörige, Besucher nur mit Anmeldung, nie alleine in Büroräumlichkeiten. Für Termine gibt es Besprechungsräume außerhalb der Arbeitsräume.

b. **Zugriffskontrolle**
- Zugriff nur für Mitarbeiter durch Passwort + Login (sowohl Rechner als auch System).
- Zugriffskontrolle: Zugriff nur für Mitarbeiter durch Passwort + Login (sowohl Rechner als auch System).
- Server-Passwörter, welche nur dem Auftragnehmer bekannt sind
- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.

c. **Weitergabekontrolle**
- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

d. **Eingabekontrolle** bei internen Verwaltungssystemen des Auftragnehmers:
Eingabe von Topothekaren durch berechtigte Topothekare (Super-User - User).
- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

2.
Verfügbarkeit und Belastbarkeit

a. **Verfügbarkeitskontrolle**
- bei internen Verwaltungssystemen des Auftragnehmers
- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz

b. **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DS-GVO);

- Es ist definiert, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

3.

Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung

- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).
- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung.
- ICARUS hat einen Datenschutzzuständigen ernannt.