

Anhang 1

Zur Vereinbarung zur Auftragsverarbeitung von Vergabeverfahren OeA-007-2026

zwischen der

Deutsches Institut für Urbanistik gGmbH Zimmerstraße 13–15
10969 Berlin

– nachfolgend „Auftraggeberin (AG)“ –

und

– nachfolgend „Auftragnehmer/in (AN)“ –

Hier sind zu ausgewählten Punkten der „Vereinbarung zur Auftragsverarbeitung“ nachfolgende Informationen durch die Auftragnehmerin/den Auftragnehmer anzugeben:

**1. Zu § 2 Abs. 1 der „Vereinbarung zur Auftragsverarbeitung“
Umfang und Art der Auftragsverarbeitung**

Hier bitte die konkrete Art und Weise bzw. die Auswahl der Mittel (z. B. verwendete Software, Standort der Server/Rechner, gemietete Speicherkapazitäten oder eigene Server etc.) der Auftragsverarbeitung auflühren.

2. Zu § 2 Abs. 2 der „Vereinbarung zur Auftragsverarbeitung“ Datenkategorien

Hier bitte die konkreten Datenkategorien (z. B. Personalstammdaten usw.) ankreuzen, deren Verarbeitung notwendig/erforderlich ist, um die Leistung gemäß Leistungsvereinbarung zu erbringen und ggfs. weitere benennen. Begründen Sie dieses bitte, wenn dieses nicht offensichtlich aus der Leistungsvereinbarung hervorgeht.

Erforderlich? Bitte ankreuzen.	Datenkategorien inkl. Beispiele	Ggf. Begründung zur Notwendigkeit der Erhebung/ Verarbeitung
☐	Personen(stamm)daten (z.B. Vorname, Nachname, Anrede, Geburtsdatum, Geschlecht)	
☐	Adress- und Kontaktdaten (z.B. Institution, Tätigkeit, Position in der Institution, Adresse, (Mobil-)Telefonnummern, Telefax, E-Mail)	
☐	Korrespondenzdaten (z.B. Inhalte von E-Mails, Briefen, Kontaktgeschichte)	
☐	Empirie-Daten (z.B. Umfrage- und Interviewantworten)	
☐	Audio- und Bilddaten (z.B. Foto und Video von Menschen in Nahaufnahme, Sprachaufzeichnungen)	
☐	Vertrags-, Abrechnungs- und Zahlungsdaten (z.B. Bankverbindung, bestellte Waren, Rechnungsdaten, Steuer-ID)	
☐	Log- und Nutzungsdaten (z.B. Benutzerkennung und Passwortdaten, Log-Infos, Aktivierungsinformationen, Gerätekennungen, Telekommunikationsdaten , Verbindungsdaten/Metadaten)	
☐	Authentifikations- und Legitimationsdaten (z.B. digitale Zertifikate, elektronische Signaturen, Unterschriftenprobe, Ausweispapiere)	
☐	Sonstige personenbezogene Daten (z.B. Themen- bzw. Interessenschwerpunkte)	
☐	Werden weitere Kategorien von Daten verarbeitet? Diese bitte nachfolgend angeben:	

3. Zu § 2 Abs. 3 der „Vereinbarung zur Auftragsverarbeitung“ Betroffene Personen

Hier bitte den Kreis der durch den Umgang mit ihren Daten Betroffenen ankreuzen und ggfs. weitere benennen.

Betroffen? Bitte ankreuzen.	Kategorien betroffener Personen und Beispiele
☐	Beteiligte in Difu-Projekten (z.B. Personen, die in irgendeiner Weise in Projekten mitwirken, z.B. Experten, Interviewpartner, Umfrageteilnehmer, Städtevertreter)
☐	Vertragspartner des Difu (z.B. Vertragspartner in Projektzusammenhängen wie Auftraggeber, Unterauftragnehmer; Sonstige Vertragspartner wie Referenten, Einmaldienstleistungen etc).
☐	Difu-Beschäftigte: Personen, die einen Arbeitsvertrag mit dem Difu haben.
☐	Difu-Bewerber: Personen, die im Difu tätig werden wollen, auch Studenten, Praktikanten.
☐	Gibt es weitere betroffene Personen? Diese bitte nachfolgend angeben:

4. Zu § 4 Abs. 3 der „Vereinbarung zur Auftragsverarbeitung“ Kontaktdaten Datenschutzbeauftragte(r) der/des AN

Hier bitte die Person(en) der Auftragnehmerin/des Auftragnehmers inkl. Kontaktdaten angeben, die als Datenschutzbeauftragte(r) benannt sind/wurden.

Name, Vorname	Kontaktdaten

☐ Nein, wir sind gesetzlich nicht dazu verpflichtet, eine(n) Datenschutzbeauftragte(n) zu bestellen.

5. Zu § 5 Abs. 1 der „Vereinbarung zur Auftragsverarbeitung“ Technisch-organisatorische Maßnahmen und deren Kontrolle

Hier bitte die **konkreten** technisch-organisatorischen Maßnahmen angeben, die getroffen werden/wurden, um den Anforderungen des Datenschutzes, insb. der Vorgaben des Art. 32 DSGVO, gerecht zu werden.

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	Zutrittskontrolle	
	Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. (z. B. Zutrittskontrollsystem, Ausweisser, Magnetkarte, Chipkarte, Schlüssel, Schlüsselvergabe, Werkschutz, Pfortner, Überwachungseinrichtung, Alarmanlage, Türsicherung)	Tech. Maßnahmen Org. Maßnahmen
2.	Zugangskontrolle	
	Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. (z.B. Technische [Kennwort-/Passwortschutz] und organisatorische [Benutzerstammsatz] Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren [Beispiele: Kennwortverfahren, automatisches Sperren, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern])	Tech. Maßnahmen Org. Maßnahmen
3.	Zugriffskontrolle	
	Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. (z. B. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren [Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc., Auswertungen, Kennnismahme, Veränderung, Löschung])	Tech. Maßnahmen Org. Maßnahmen

4.	Weitergabekontrolle	
	Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. (z. B. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger [manuell oder elektronisch] so- wie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur)	Tech. Maßnahmen Org. Maßnahmen
5.	Eingabekontrolle	
	Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. (z. B. Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Auswertungssysteme)	Tech. Maßnahmen Org. Maßnahmen
6.	Auftragskontrolle	
	Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der AG verarbeitet werden können. (Abgrenzen der Kompetenz zwischen der AG und der/des AN [Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl der/des AN, Kontrolle der Vertragsausführung])	Tech. Maßnahmen Org. Maßnahmen

7.	Verfügbarkeitskontrolle	
	Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. (z. B. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung [Beispiel: Backup- Verfahren, Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung, Firewall, Notfallplan])	Tech. Maßnahmen Org. Maßnahmen
8.	Trennungskontrolle	
	Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Tech. Maßnahmen Org. Maßnahmen
9.	Datensicherheit bei der Verarbeitung von personenbezogenen Daten außerhalb der Betriebsräume der/des AN	
	Es ist zu gewährleisten, dass Daten, die außerhalb der Betriebsräume der/des AN (z. B. im Home-Office, mobiles Arbeiten etc.) verarbeitet werden, vor Kenntnisnahme Dritter und Diebstahl geschützt sind.	Tech. Maßnahmen Org. Maßnahmen

6. Zu § 5 Abs. 8 der „Vereinbarung zur Auftragsverarbeitung“ Information zur Datenschutz-Folgeabschätzung

Hier bitte die Fragen in der nachfolgenden Tabelle beantworten, um festzustellen, ob eine Datenschutz-Folgeabschätzung gemäß Art. 35 DSGVO erforderlich ist.

Als Hintergrund: Die Datenschutz-Folgeabschätzung ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von hohen Risiken für die Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten. Solche Risiken können durch einen besonders riskanten Verarbeitungsvorgang, insbesondere bei Verwendung neuer Technologien, oder bei der Verarbeitung besonders sensibler „Risikodaten“ entstehen. Ein Schaden kann zum Beispiel dann entstehen, wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufbeschädigung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen von Betroffenen führen kann.

Nr.	Frage	Antwort (bitte begründen)
1. Neue Technologien		
1.1.	Werden bei der Verarbeitung der personenbezogenen Daten neue Technologien verwendet, die ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringen? Neue Technologien sind z. B. Hard- und Software, Prozesse und Methoden der IT- Technik, neue Entwicklungen, wie Smart Car, Smart Health, Big Data- und Trackingverfahren sowie neue Sicherheits- und Überwachungstechnik.	
1.2.	Wurde für diese neue Technologie bereits eine Datenschutz-Folgeabschätzung durchgeführt?	
1.3.	Ermöglicht die neue Technologie die Verarbeitung großer Mengen von personenbezogenen Daten auf regionaler, nationaler oder übernationaler Ebene?	
1.4.	Ermöglicht die neue Technologie die Verarbeitung von Daten einer großen Anzahl von Personen?	
2. Erschwerte Rechtsausübung		
	Werden Verarbeitungsverfahren eingesetzt, die den betroffenen Personen die Ausübung ihrer Rechte erschweren? Das ist z. B. anzunehmen bei komplexen und intransparenten Verfahren, einer Vielzahl von für die Verarbeitung verantwortlichen Personen, bei geheimen und anlasslosen Verarbeitungen insbesondere im Rahmen von Überwachungs- und Sicherheitsmaßnahmen.	
3. Profiling		
3.1.	Werden Daten zu persönlichen Aspekten automatisiert verarbeitet? (z.B. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel)	
3.2.	Werden diese Daten systematisch und umfassend bewertet, um daraus persönliche Profile zu erstellen?	
3.3.	Werden diese persönlichen Profile herangezogen, um Entscheidungen zu treffen, die Rechtswirkung gegenüber Personen entfalten?	
4. Besonders sensible Daten		

4.1.	Werden personenbezogene Daten verarbeitet, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen?	
4.2.	Werden genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung erhoben?	
4.3.	Werden personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängenden Sicherungsmaßnahmen verarbeitet?	
5. Videoüberwachung		
	Erfolgt eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels Videokameras?	
6. Sonstiges		
	Erfolgt ein Datentransfer außerhalb der EU?	
	Erfolgt ein Vergleich oder eine Kombination von Datensätzen?	

7. Zu § 8 Abs. 1 der „Vereinbarung zur Auftragsverarbeitung“ Unterauftragnehmer

Hier bitte Ihre Unterauftragnehmer auflisten, die Sie zur Erfüllung des Auftrags hinzuziehen werden.

Firma, Anschrift	Beschreibung der Verarbeitung und dessen Zweck	Zu verarbeitenden Datenkategorien	Kategorien betroffener Personen

, den

Ort, Datum

Unterschrift, Firmenstempel