

## **Vertrag zur Auftragsdatenverarbeitung Gemäß Art. 28 EU-Datenschutzgrundverordnung (EU-DSGVO)**

### **Vereinbarung**

zwischen der

Stadt [Name der Stadt]  
[Adresse]

Verantwortlicher – nachstehend Auftraggeber genannt -

und dem  
Kreis Recklinghausen,  
Fachdienst 62  
Kurt-Schumacher-Allee 1, 45657 Recklinghausen

Auftragsverarbeiter – nachstehend Auftragnehmer genannt -  
(ggf.: Vertreter gemäß Art. 27 EU-DSGVO)

## 1. Gegenstand und Dauer des Auftrags

### (1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Verarbeitung eines anonymisierten Auszugs aus dem Melderegister zu einer Bevölkerungsstatistik

### (2) Dauer

Der Auftrag wird zur einmaligen Ausführung erteilt.

## 2. Konkretisierung des Auftragsinhalts

### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen des Projekts „smartdemography“ zur einmaligen Verfahrensentwicklung und –einrichtung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat 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 des Art. 44 ff. EU-DSGVO erfüllt sind.

### (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

Vollständiger Auszug aus dem Melderegister der Stadt [Name der Stadt] mit folgenden Merkmalen:

Merkmal	Zweck der Verarbeitung
derzeitige und frühere Anschriften, Haupt- und Nebenwohnung*	Georeferenzierung (Zuordnung zu Gebietseinheit wie Baublock oder Rasterzelle), Ermittlung von Wanderungs-Statistiken (Straße, Hausnummer und Hausnummer-Zusatz als Hilfsmerkmale sind im Anschluss an die Georeferenzierung zu löschen)
Einzugsdatum, Auszugsdatum (nur Jahr), sowie Jahr des letzten Zuzugs aus dem Ausland (jeweils Jahr und Monat)	Ermittlung von Wanderungs-Statistiken zum Stichtag

Geburtsdatum und Geburtsort* sowie bei Geburt im Ausland auch den Staat (jeweils Jahr und Monat)	Zuordnung zu Altersgruppe, auch zu einem Stichtag im Jahresverlauf, z.B. für die Schulpflicht (30.09.) oder Kita-U3-Einstufung (31.10.)
Geschlecht	Differenzierung der Statistik nach Geschlecht
derzeitige Staatsangehörigkeiten	Differenzierung der Statistik nach Staatsangehörigkeit
Sterbedatum (Jahr und Monat)	Ermittlung der natürlichen Bevölkerungsentwicklung je Gebiet, Bestimmung des durchschnittlichen Sterbealters  Der Monat wird für eine Mortalitätsstatistik im Jahresverlauf benötigt, um z.B. Gebiete mit Handlungsbedarf zu identifizieren, die von Hitzewellen besonders betroffen sind.

### (3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Alle Einwohnerinnen und Einwohner der Stadt [Name der Stadt].

### 3. Technisch-organisatorische Maßnahmen

(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. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO 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 Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen (Einzelheiten in Anlage 1).

(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. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, 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.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## **5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt.

Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-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 diese gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für den Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO (Einzelheiten in Anlage 1).

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

e) 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.

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

g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## **6. Unterauftragsverhältnisse**

(1) 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 Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern 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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 – 4 EU-DSGVO:

Hochschule Bochum, Fachbereich Geodäsie, Lennershofstraße 140, 44801 Bochum

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

## **7. Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig 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 EU-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.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

**(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auf-tragnehmer 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 EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

- 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 Ver letzungsereignissen ermöglichen,
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- c) die Verpflichtung, dem 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 Datenschutzfolgenabschätzung,
- 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.

Weisungsberechtigte Personen des Auftraggebers sind:

---

Weisungsempfänger beim Auftragnehmer sind:  
der/die Leiter/in der Statistikstelle des Kreises Recklinghausen

## **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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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. Außerordentliche Kündigung**

Unabhängig von den Regelungen über die oben getroffenen Laufzeiten bzw. die Dauer der Vereinbarung steht dem Auftraggeber ein Recht auf fristlose Kündigung bei schwerwiegenden Vertragsverletzungen des Auftragnehmers zu. Dies kommt insbesondere in Betracht bei Verstoß gegen datenschutzrechtliche Vorschriften, Datenschutz- und Datensicherheitsvereinbarungen, wenn der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer eine Kontrolle des Auftraggebers oder der nordrhein-westfälischen Datenschutzbeauftragten vertragswidrig verweigert.

## **12. Haftung**

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder seine Subunternehmen bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der EU-DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

(3) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

## **13. Sonstiges**

(1) Es besteht bei den Vertragsparteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftragnehmers auf diese Vereinbarung keine Anwendung finden.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

#### **14. Wirksamkeit der Vereinbarung**

Diese Vereinbarung bleibt auch bei rechtlicher Unwirksamkeit einzelner Punkte in seinen übrigen Teilen verbindlich. Unwirksame Bestimmungen sind von den Parteien durch wirksame zu ersetzen, die dem gewollten Zweck möglichst nahe kommen. Entsprechendes gilt im Falle einer Vertragslücke.

Recklinghausen, den \_\_\_\_\_

\_\_\_\_\_  
Auftraggeber

\_\_\_\_\_  
Auftragnehmer (Kreis Recklinghausen)

Anlage 1  
Technisch-organisatorische Maßnahmen



## **Anlage 1**

### **Technisch-organisatorische Maßnahmen**

#### **1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)**

- Zutrittskontrolle  
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen
- Zugangskontrolle  
Keine unbefugte Systembenutzung, z. B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- Zugriffskontrolle  
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Trennungskontrolle  
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit
- Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)  
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen

#### **2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)**

- Weitergabekontrolle  
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur
- Eingabekontrolle  
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement

#### **3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)**

- Verfügbarkeitskontrolle  
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c EU-DSGVO)

#### **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)**

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)
- Auftragskontrolle  
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 EU-DSGVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungs-pflicht, Nachkontrollen