Bereitstellung einer KWIS-Datenbank

für die Wirtschaftsförderung

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 EU-DSGVO

zwischen dem

Verantwortlichen gemäß Zusatzvereinbarung zum Wartungs- bzw. Pflegevertrag

und der

Gesellschaft für angewandte Kommunalforschung mbH
Ockershäuser Allee 40 b, 35037 Marburg

im Folgenden „Auftragsverarbeiter“

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags

Diese Vereinbarung umfasst folgende, vom Auftragsverarbeiter durchzuführende Arbeiten **für KWIS und für ggf. zusätzlich beauftragte Schnittstellen und Zusatzmodule**:

a. Erstellen kundenspezifischer Datenbanken für KWIS und seine Zusatzmodule

b. Zur-Verfügung-Stellung der Datenbank auf dem IT-System des Verantwortlichen incl. Installationsbegleitung

c. Fehlerbehebung innerhalb der Datenbank bei der GEFAK

d. Befüllen der Datenbank mit den Daten der regionalen Wirtschaftsunternehmen und anderer Institutionen (Ergänzung und Berichtigung der Datenbank bei Weisung des Verantwortlichen durch die gesonderte Beauftragung von Datenimporten, Datenübernahmen oder Zusatzmodulen)

e. Durchführung von Befragungen zwecks Erhebung der Daten für die Datenbank (Ergänzung und Berichtigung der Datenbank bei Weisung des Verantwortlichen durch die gesonderte Beauftragung einer Befragung)

Der Zweck der Datenverarbeitung ist der ordnungsgemäße Betrieb eines CRM-Systems zur Erfüllung der dem Verantwortlichen obliegenden Aufgaben, insbesondere der Wirtschaftsförderung.

Dauer des Auftrags

Die Dauer des Auftrags (Laufzeit) ergibt sich aus der Zusatzvereinbarung zum Wartungs- bzw. Pflegevertrag. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

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

Der Auftragsverarbeiter hat ein Softwareprodukt namens KWIS (kommunales Wirtschaft-Informations-System) entwickelt. Dieses beschickt er mit den Daten von Wirtschaftsunternehmen und anderen Institutionen aus dem kommunalen Aufgabenbereich des Verantwortlichen. Diese können entweder vom Verantwortlichen selbst stammen oder aber aus einer vom Auftragsverarbeiter durchgeführten Befragung der entsprechenden Unternehmen hervorgegangen sein. Auf schriftlichen Wunsch können im Namen des Verantwortliches Listendaten bei BEDIRECT oder der CREDITREFORM eingekauft werden.

Diese Daten werden vom Auftragsverarbeiter insofern verarbeitet, als er sie in die dem Verantwortlichen zur Verfügung gestellten Datenbank einpflegt. **Eine Version dieser Datenbank verbleibt zu**

Supportzwecken beim Auftragsverarbeiter. Eine weitere Nutzung von personenbezogenen Daten durch den Auftragsverarbeiter erfolgt nicht.

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 Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind.

Art der Daten

In der KWIS Datenbank werden vor allem Daten zu den Wirtschaftsunternehmen im Raum des Verantwortlichen erfasst. Diese können unter anderem aus folgenden Kategorien stammen:

Personenstammdaten, Kommunikationsdaten (z.B. Telefon, E-Mail), Firmendaten; Wirtschaftskennzahlen, Geburtsdaten, Funktion der entsprechenden Personen in dem jeweiligen Unternehmen.

Im Sonderfall der Beauftragung des Zusatzmoduls KWIS.job werden auch Angaben von beispielsweise Schülern (Vor- und Nachname, E-Mail, u.U. Telefon-Nr.) erfasst (siehe nachfolgend Kategorien betroffener Personen).

Kategorien betroffener Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst die in KWIS erfassten Kontaktdaten von einzelnen Beschäftigten der dort hinterlegten Unternehmen oder sonstigen Institutionen.

Im Sonderfall der Beauftragung des Zusatzmoduls KWIS.job gehören zu den betroffenen Personen auch Schüler, Auszubildende und sonstige Personen, die Angebote der erfassten Unternehmen im Rahmen der Fachkräftesicherung nutzen.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter 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 die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen (vgl. Anlage „Datensicherheitskonzept der GEFAK“).

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate

Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten bisherigen Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter 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 Verantwortlichen zur Prüfung zu übergeben (vgl. Anlage „Datensicherheitskonzept der GEFAK“). Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, sind diese Anpassungen einvernehmlich umzusetzen.

4. Berichtigung, Sperrung und Löschung von Daten

(1) Der Wartungsvertrag mit dem Auftragsverarbeiter umfasst unter anderem den Support an der Datenbank. Um diesen unverzüglich und ohne das Entstehen zusätzlicher Kosten durchführen zu können, bleibt die Datenbank des Verantwortlichen auch nach der Übergabe an diesen auf dem System des Auftragsverarbeiters gespeichert. Die in der Datenbank gehaltenen Daten werden für jegliche Nutzung abseits des technischen Supports an der Datenbank selbst durch Zugriffsberechtigungen gesperrt. Eine Freigabe erfolgt nur im Supportfalle zu eben diesem Zweck. In Abwägung der Art der Daten gegen die Umstände, die sich bei Nicht-Speicherung durch die Notwendigkeit einer Neuübermittlung im Supportfalle ergäben, erscheint es sinnvoll und verhältnismäßig, eine Kopie beim Auftragsverarbeiter vorzuhalten.

(2) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortliches berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(3) Soweit vom Auftragsumfang umfasst (siehe 1.d und 1.e), sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter 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. 28 und 29 EU-DSGVO ausübt. Dessen Name und Kontaktdaten sind im Datensicherheitskonzept des Auftragsverarbeiters gelistet, um eine direkte Kontaktaufnahme zu ermöglichen. Ein Wechsel des Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt.

b. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DSGVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO (Anlage „Datensicherheitskonzept der GEFAK“).

d. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage durch die Aufsichtsbehörde mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e. Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

f. Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

g. Der Auftragsverarbeiter 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 Personen gewährleistet wird.

h. Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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

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 Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartungs- 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragsverarbeiter darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Verantwortlichen beauftragen.

Der Verantwortliche stimmt im Falle einer gesondert beauftragten Befragung der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO:

- Lahn-Werkstätten-Marburg; Industriestr. 14; 35041 Marburg: Versand von Unternehmensfragebögen
- NOCEANZ GmbH; Friedrich-Bergius-Ring 15; 97076 Würzburg: scannerbasierte Erfassung von Unternehmensfragebögen

Der Wechsel des bestehenden Unterauftragsverarbeiters ist zulässig, soweit:

- ⇨ der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragsverarbeiter dem Verantwortlichen eine angemessene Zeit vorab schriftlich oder in Textform mit Fristsetzung zur Rückäußerung anzeigt und
- ⇨ der Verantwortliche diesem fristgemäß mindestens in Textform zugestimmt hat und
- ⇨ eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Unterauftragsverarbeiter erbringen ihre Leistungen innerhalb der EU bzw. des EWR. Ansonsten wird der Auftragsverarbeiter hierauf ausdrücklich hinweisen und das schriftliche Einverständnis des Verantwortlichen erst einholen, soweit er sich vergewissert hat, dass die Art. 44-50 DS-GVO eingehalten werden.

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

7. Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter 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 Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 EU-DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

8. Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen 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.

- ⇨ 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
- ⇨ die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
- ⇨ die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- ⇨ die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung
- ⇨ die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder die nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen. **Jegliche diesbezügliche Vergütungsansprüche sind im Vorfeld mit dem Verantwortlichen einvernehmlich abzustimmen**.

9. Weisungsbefugnis des Verantwortlichen

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

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

10. Löschung von Daten und Rückgabe von Datenträgern

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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) Mit Beendigung der Vereinbarung zur Auftragsverarbeitung oder früher nach Aufforderung durch den Verantwortlichen hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten personenbezogenen Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten (Richtlinie zur Datenvernichtung im Anhang). Gleiches gilt für Test- und Ausschussmaterial.

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

11. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

(2) 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.