Fernwartung für KWIS

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 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 durchzuführenden Fernwartungsarbeiten:

1. Software-Wartung (für folgendes Softwareprodukt):
    - Kommunales Wirtschaft-Informations-System KWIS

Dauer des Auftrags

Die Dauer des Auftrags (Laufzeit) ergibt sich aus der Zusatzvereinbarung zum Wartungs- und Betreuungsvertrag. 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 nutzt im Regelfall einen Fernzugang mittels der Software „Teamviewer“ zur Wartung des beim Verantwortlichen installierten Softwareproduktes. Der Zugang wird zu diesem Zweck zuerst vom Verantwortlichen aktiviert und anschließend vom Auftragsverarbeiter genutzt. Sollte der Verantwortliche eine andere Software für den Fernzugang zwingend vorschreiben, stellt der Verantwortliche sicher, dass der Auftragsverarbeiter diese Software kostenfrei nutzen kann. Die Wartungsarbeiten wird der Auftragsverarbeiter so weit möglich immer in der Weise vornehmen, dass ihm während des Arbeitens keinerlei personenbezogene Daten zugänglich und / oder sichtbar werden. Sollte sich dies nicht vermeiden lassen, so kann der Auftragsverarbeiter die Wartung jedoch auch mit und an personenbezogenen Daten vornehmen.

Eine Verarbeitung und Nutzung der Daten findet innerhalb dieser Fernwartung nicht statt.

Art der Daten

Grundsätzlich findet keine Erhebung, Verarbeitung und / oder Nutzung im Sinne des DS-GVO statt. Es kann jedoch zu einer Zur-Kenntnisnahme aller bei dem Verantwortlichen vorliegenden personenbezogenen Daten kommen. 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 kann es auch zu einer Zur-Kenntnisnahme von Personenangaben (Vor- und Nachname, E-Mail, u.U. Telefon-Nr.) von sonstigen Personen kommen (siehe nachfolgend Kategorien betroffener Personen).

Kategorien betroffener Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- In KWIS erfasste Daten der dort hinterlegten Unternehmen und anderer Institutionen
- Einschließlich der jeweiligen Kommunikationspartner (Beschäftigte)

Im Sonderfall der Beauftragung des Zusatzmoduls KWIS.job kann der Kreis der Betroffenen auch Schüler, Auszubildende und Personen betreffen, die Angebote der erfassten Unternehmen im Rahmen der Fachkräftesicherung nutzen.

3. Technisch-organisatorische Maßnahmen

(1) 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 die Anpassungen einvernehmlich umzusetzen.

(2) Die Fernwartung erfolgt grundsätzlich auf Anforderung durch den Verantwortlichen. Dieser startet das Fernwartungstool, worauf er dem durch Namen und Rufnummernübermittlung authentifizierten Mitarbeiter des Auftragsverarbeiters die Zugangsdaten telefonisch übermittelt.

(3) Die Fernwartung wird von den hierfür beauftragten Mitarbeitern des Auftragsverarbeiters durchgeführt (siehe aktuelle Liste der Mitarbeiter mit den Kommunikationsdaten unter https://www.gefak.de/datenschutz/technischer-support-sowie-anwender-hotline-und-betreuung). Die hierfür notwendige Übertragung von Steuerungsdaten (Tastatur und Maus) sowie Ausgabedaten (Bildschirm) erfolgt verschlüsselt. Eine Aufzeichnung der Sitzung erfolgt spätestens auf Wunsch des Verantwortlichen, wenn der Fernwartungsumfang die reine Hilfestellung übersteigt und Eingriffe am System notwendig macht.

(4) 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.

4. Berichtigung, Sperrung und Löschung von Daten

Im Rahmen der Fernwartung werden keinerlei personenbezogene Daten gespeichert, daher entfällt dieser Punkt.

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 EUDSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- ⇨ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 28 und 29 EU-DSGVO ausübt. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Verantwortlichen unverzüglich mitgeteilt.
- ⇨ Der Auftragsverarbeiter teilt dem IT-Verantwortlichen des Verantwortlichen vor Beginn der Fernwartung schriftlich mit, welche Mitarbeiter (namentlich mit Durchwahl) er dafür einsetzen wird und wie diese Mitarbeiter sich identifizieren werden, nämlich durch Nennung ihres Namens und Anzeige ihrer Rufnummer.
- ⇨ 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 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“).
- ⇨ Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- ⇨ 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.
- ⇨ 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.

- ⇨ 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.
- ⇨ Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen 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 Auftragsverarbeiter 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 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 Verantwortliche stimmt dem nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

- ⇨ TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen

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 anzeigt und
- ⇨ der Verantwortliche diesem fristgemäß mindestens in Textform zugestimmt hat und
- ⇨ eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO 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 ein 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) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, 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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(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.