Bedingungen zur Auftragsverarbeitung

Die ekom21 als Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO führt im Sinne von § 7 Abs. 2 Nr. 18 der Satzung der ekom21 – KGRZ Hessen Aufträge zur Verarbeitung personenbezogener Daten nach Maßgabe von § 15 der ekom21-Benutzungsordnung und unter Einhaltung der nachstehenden Bedingungen zur Auftragsverarbeitung nach Art. 28 DSGVO aus.

§ 1 GEGENSTAND UND DAUER DES AUFTRAGS

(1) Zwischen Benutzer und ekom21 besteht ein öffentlich-rechtliches Benutzungsverhältnis (in seiner jeweils gültigen Fassung), unter welchem von ekom21 Dienste für den Benutzer erbracht werden. Diese Auftragsverarbeitungsbedingungen (im Folgenden „Vereinbarung“) ergänzen insoweit das Benutzungsverhältnis in Bezug auf die Verarbeitung personenbezogener Daten im Auftrag des Benutzers.

(2) Von dem Gegenstand des Auftrages kann auch die Verarbeitung von personenbezogenen Daten von Mitarbeitern des Benutzers umfasst sein, sofern diese für die Durchführung des Auftrags erforderlich sind und der ekom21 vom Benutzer oder dem Mitarbeiter des Benutzers selbst mitgeteilt werden (z. B. Anlegen eines Benutzerkontos für den Benutzer oder seine Mitarbeiter; Pflege der Daten von Benutzern (Aktualisierung, Änderung, Löschung) etc.).

(3) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Benutzungsverhältnisses.

(4) Der Benutzer und die ekom21 können diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß durch die ekom21 oder durch den Benutzer gegen deren Bestimmungen vorliegt. Insbesondere die Nichteinhaltung der in dieser Vereinbarung niedergelegten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt für beide Parteien unberührt.

§ 2 KONKRETISIERUNG DES AUFTRAGSGEGENSTANDES

(1) Die ekom21 verarbeitet personenbezogene Daten im Auftrag des Benutzers gemäß Art. 28 DSGVO auf Grundlage dieser Vereinbarung. Der Gegenstand des Auftrags, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen gemäß Art. 28 Abs. 3 Satz 1 DSGVO sind in den ergänzenden Informationen zur Auftragsverarbeitung, die zwischen Benutzer und ekom21 abgestimmt sind, festgelegt. Über ein elektronisches Datenschutz-Dokumentationsportal der ekom21, das jedem Benutzer zugänglich ist, sind die ergänzenden Informationen zur Auftragsverarbeitung individualisiert abrufbar.

(2) Datenverarbeitungen in einem Drittland bedürfen der vorherigen Zustimmung des Benutzers und dürfen nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 RECHTMÄßIGKEIT DER VERARBEITUNG UND ÄNDERUNG DES AUFTRAGSGEGENSTANDES

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Benutzer als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO verantwortlich.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen dem Benutzer und der ekom21 abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

§ 4 WEISUNGSBEFUGNIS DES BENUTZERS

(1) Die ekom21 und jede der ekom21 unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen die vom Auftrag umfassten Daten ausschließlich entsprechend der Weisung des Benutzers verarbeiten einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, sofern die ekom21 nicht durch das Recht der Union oder der Mitgliedstaaten hierzu verpflichtet ist; in einem solchen Fall teilt die ekom21 dem Benutzer diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Benutzer erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(3) Die ekom21 hat den Benutzer unverzüglich zu informieren, wenn die ekom21 der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Die ekom21 ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Benutzer bestätigt oder geändert wird.

§ 5 KONTROLLRECHTE DES BENUTZERS

(1) Der Benutzer hat das Recht, im Benehmen mit der ekom21, Überprüfungen bei ekom21 durchzuführen oder durch einen im Einzelfall zu benennenden Prüfer durchführen zu lassen. Der Benutzer hat das Recht, sich durch Stichprobenkontrollen zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch die ekom21 in dessen Geschäftsbetrieb zu überzeugen.

(2) Die ekom21 stellt sicher, dass sich der Benutzer von der Einhaltung der Pflichten der ekom21 nach Art. 28 DSGVO überzeugen kann. Die ekom21 verpflichtet sich, dem Benutzer auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen (TOM) nachzuweisen.

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

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

§ 6 UMSETZUNG DER DOKUMENTATION DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN DURCH DIE EKOM21

(1) Die ekom21 hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen (TOM) vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Benutzer auf Verlangen zur Prüfung zu übergeben. Der Benutzer akzeptiert die in Anlage „TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM)“ dokumentierten allgemeinen Maßnahmen. Soweit die Prüfung/ein Audit des Benutzers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Die ekom21 hat die Sicherheit der Verarbeitung gem. Art. 28 Abs. 3 Satz 2 lit. c), Art. 32 DSGVO herzustellen und die Sicherheit der personenbezogenen Daten gemäß Art. 5 Abs. 1 lit. f) DSGVO nachzuweisen. 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. Sofern neben den allgemeinen technischen und organisatorischen Maßnahmen der ekom21 (siehe ANLAGE „Technische und organisatorische Maßnahmen der ekom21 (TOM)“) für den jeweiligen Auftrag erforderlich sind, sind diese den ergänzenden Informationen zur Auftragsverarbeitung zu entnehmen.

(3) Die technischen und organisatorischen Maßnahmen (TOM) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der ekom21 gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen muss die ekom21 mit dem Benutzer in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieser Vereinbarung aufzubewahren.

(4) Die Verarbeitung personenbezogener Daten in Privatwohnungen (mobile Tele- oder Heimarbeit) ist unter Beachtung der technischen und organisatorischen Maßnahmen (TOM) und den Voraussetzungen gestattet, dass die Maßnahmen nach Art. 32 DSGVO auch in diesem Fall und der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers sichergestellt sind.

(5) Personenbezogene Daten, die einen sehr hohen Sicherheits- und Datenschutzbedarf aufweisen, dürfen im Rahmen der mobilen Tele- und Heimarbeit nicht verarbeitet werden. Dieses Verbot gilt für folgende Fälle:
- Verarbeitung von besonders sensiblen Gesundheits- und Sozialdaten,
- Verarbeitung personenbezogener Daten im Zusammenhang mit Disziplinarverfahren,
- Verarbeitung personenbezogener Daten im Zusammenhang mit strafbaren Handlungen,
- Verarbeitung von personenbezogenen Daten von Vertrauens- oder Verbindungsleuten,
- Verarbeitung von personenbezogenen Daten im Zusammenhang mit Tarnkennzeichen,
- Verarbeitung von personenbezogenen Daten von Personen, die einem Zeugenschutzprogramm unterliegen,
- Verarbeitung von personenbezogenen Daten im Zusammenhang mit Verschlusssachen nach § 2 Abs. 2 Nr. 1 und 2 des Hessischen Sicherheitsüberprüfungsgesetzes (HSÜG).

§ 7 BERICHTIGUNG, EINSCHRÄNKUNG UND LÖSCHUNG VON DATEN DURCH DIE EKOM21

Die ekom21 darf personenbezogene Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Benutzers berichtigen, deren Verarbeitung einschränken oder löschen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die ekom21 wendet, wird die ekom21 dieses Ersuchen unverzüglich an den Benutzer weiterleiten.

§ 8 QUALITÄTSSICHERUNG UND SONSTIGE PFLICHTEN DER EKOM21

Die ekom21 hat zusätzlich und unabhängig zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 39 DSGVO zu erfüllen. Insofern gewährleistet die ekom21 insbesondere die Einhaltung folgender Vorgaben:

- Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt, dessen jeweils aktuelle Kontaktdaten auf der Homepage der ekom21 leicht zugänglich hinterlegt sind.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), Art. 29, Art. 32 Abs. 4 DSGVO. Die ekom21 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.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c), Art. 32 DSGVO. Die Einzelheiten ergeben sich aus den technischen und organisatorischen Maßnahmen (TOM) sowie aus den ergänzenden Informationen zur Auftragsverarbeitung.
- Die ekom21 arbeitet auf Anfrage mit der für den Benutzer zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Benutzers 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 bei ekom21 ermittelt.
- Soweit der Benutzer 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 bei ekom21 ausgesetzt ist, hat ihn die ekom21 nach besten Kräften zu unterstützen.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen (TOM) gegenüber dem Benutzer im Rahmen seiner Kontrollbefugnisse nach § 5 dieser Vereinbarung.
- Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt die ekom21 den Benutzer bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

§ 9 UNTERAUFTRAGSVERHÄLTNISSE

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich auf den Gegenstand der Vereinbarung beziehen und durch weitere Auftragsverarbeiter gemäß Art. 28 Abs. 2 DSGVO (Unterauftragnehmer) durchgeführt werden.

(2) Die ekom21 ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Benutzers auch bei Unterauftragsverhältnissen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Der Benutzer stimmt der Beauftragung der Unterauftragnehmer (weiterer Auftragsverarbeiter gemäß Art. 28 Abs. 2 DSGVO) zu, die in den ergänzenden Informationen zur Auftragsdatenverarbeitung genannt sind, unter der Bedingung einer vertraglichen Vereinbarung zwischen der ekom21 und jedem Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

(4) Die Auslagerung auf Unterauftragnehmer und der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

a) die ekom21 eine solche Auslagerung auf Unterauftragnehmer dem Benutzer eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

b) der Benutzer nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber der ekom21 schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

c) eine vertragliche Vereinbarung zwischen dem Benutzer und dem Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

Erhebt der Benutzer gegen den Wechsel des bestehenden Unterauftragnehmers Einspruch, gilt § 6 Abs. 5 der ekom21-Benutzungsordnung entsprechend.

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

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt die ekom21 die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 eingesetzt werden sollen.

(7) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung der ekom21 (mind. Textform).

(8) Unteraufragnehmer werden im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dieser Vereinbarung zwischen dem Benutzer und der ekom21 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Die ekom21 haftet gegenüber dem Benutzer dafür, dass der Unterauftragnehmer den Datenschutzpflichten nachkommt, die ihm durch die ekom21 im Einklang mit der vorliegenden Vereinbarung auferlegt wurden.

§ 10 UNTERSTÜTZUNGSPFLICHT DER EKOM21

(1) Angesichts der Art der Verarbeitung unterstützt die ekom21 den Benutzer nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Bearbeitung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.

(2) Die ekom21 unterstützt den Benutzer bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten: Sicherheit der Verarbeitung personenbezogener Daten, Meldung von Verletzungen des Schutzes personenbezogener Daten und Benachrichtigung betroffener Personen bei Datenpannen, Datenschutz-Folgeabschätzung und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Art, den Umfang, die Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Benutzer zu melden;

c) die Verpflichtung, den Benutzer im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Benutzers bei der Erstellung seiner Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO;

e) die Unterstützung des Benutzers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde gem. Art. 36 DSGVO.

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Benutzers zurückzuführen sind und sofern die Unterstützungsleistungen über die der DSGVO hinausgehen, kann die ekom21 eine Vergütung beanspruchen.

§ 11 LÖSCHUNG UND RÜCKGABE VON PERSONENBEZOGENEN DATEN

(1) Kopien oder Duplikate personenbezogener Daten werden ohne Wissen des Benutzers 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 vereinbarten Arbeiten oder früher nach Aufforderung durch den Benutzer–spätestens mit Beendigung der Leistungsvereinbarung – hat die ekom21 sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Benutzer auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. 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 die ekom21 entsprechend der jeweiligen Aufbewahrungsfristen über das Ende der Vereinbarung hinaus aufzubewahren. Die ekom21 kann sie zu ihrer Entlastung bei Ende der Vereinbarung dem Benutzer übergeben.

§ 12 HAFTUNG

(1) Für die Haftung der Parteien gelten die Vorgaben des Art. 82 DSGVO sowie im Übrigen die Regelungen der ekom21-Benutzungsordnung.

(2) Die Parteien vereinbaren und gestatten der jeweils anderen Partei, Informationen aus diesem Vertag zum Zweck der Abwehr von Ansprüchen Dritter und zum Zweck des Nachweises, dass die jeweilige Partei in keinerlei Hinsicht für den Umstand, durch den ein Schaden eingetreten ist, verantwortlich ist, zu nutzen.

§ 13 GESCHÄFTSGEHEIMNISSE, VERTRAULICHKEIT

(1) Die ekom21 behandelt Unterlagen und Informationen, die sie im Rahmen der Vereinbarung erhält, vertraulich.

(2) Der Benutzer ist verpflichtet, alle im Rahmen der getroffenen Vereinbarung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der ekom21 vertraulich zu behandeln.

(3) Diese Verpflichtungen bleiben auch nach Beendigung dieser Vereinbarung bestehen.

§ 14 ANLAGE

Es gilt die nachfolgende Anlage:

- Technische und organisatorische Maßnahmen der ekom21 (TOM)