

Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO

zum

EVB-IT Systemvertrag

zwischen dem

Landkreis Schmalkalden-Meiningen
Eigenbetrieb „Kommunaler IT-Service (KITS)“

vertreten durch [●]

– nachfolgend „Auftraggeber“ genannt –

und

[●],

[●],

vertreten durch [●]

[Hinweis: Angaben zum Auftragnehmer werden bei Vertragsschluss entsprechend ergänzt]

– nachfolgend „Auftragnehmer“ genannt –

Auftraggeber und Auftragnehmer jeweils auch als „Partei“ und zusammen als „Parteien“ bezeichnet.

§ 1 Allgemeines

- (1) Im Rahmen der Leistungserbringung nach dem EVB-IT Systemvertrag vom [Hinweis: Datum wird bei Vertragsschluss entsprechend ergänzt] (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Diese Auftragsverarbeitungsvereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gemäß Art. 28 Datenschutzgrundverordnung (DSGVO) im Zusammenhang mit dem Umgang des Auftragnehmers oder von ihm unterbeauftragte Dritte mit Auftraggeber-Daten zur Durchführung des Hauptvertrages.
- (2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

§ 2 Gegenstand der Beauftragung

- (1) Der Auftrag des Auftraggebers an den Auftragnehmer nach dem Hauptvertrag umfasst die Erstellung eines Gebührenveranlagungssystems für die Abwicklung der abfallwirtschaftlichen Leistungen im Landkreis sowie die Erbringung von Systemserviceleistungen für das für den Auftraggeber errichtete System. Um die vom Auftragnehmer angebotenen Leistungen wie im Hauptvertrag definiert erbringen zu können, muss der Auftragnehmer die Auftraggeber-Daten in dem für die Erbringung der Leistungen erforderlichen Maß verarbeiten. Zweck der Verarbeitung ist folglich ausschließlich die Erbringung der Leistungen nach dem Hauptvertrag.
- (2) Die folgenden Datenarten sind regelmäßig Gegenstand der Verarbeitung:
 - Identifikationsdaten (z.B. Vor- und Nachname / Titel / Geburtsdatum / Geburtsort)
 - Kontaktdaten (z.B. Straße / Hausnummer / Wohnort / Postleitzahl / Land / Telefon / Handy / Fax / E-Mail-Adresse / Ausweisnummer (Personalausweis, Reisepass))
 - Finanzdaten
 - [•]

[Dieser Abschnitt wird vor Vertragsunterzeichnung noch ggf. ergänzt/angepasst auf Basis der Konzepte/Angaben des Auftragnehmers zur Leistungserbringung und auf Basis gegenseitiger Vereinbarungen zur Organisation der Zusammenarbeit.]

- (3) Folgende Kategorien von betroffenen Personen sind hiervon betroffen:
 - Grundstückseigentümer
 - Behältergemeinschaften
 - sonstige Bescheideempfänger
 - [•]

[Dieser Abschnitt wird vor Vertragsunterzeichnung noch ggf. ergänzt/angepasst auf Basis der Konzepte/Angaben des Auftragnehmers zur Leistungserbringung und auf Basis gegenseitiger Vereinbarungen zur Organisation der Zusammenarbeit.]

§ 3 Rechte und Pflichten des Auftraggebers

- (1) Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. Dem Auftragnehmer steht nach § 4 Abs. 3 dieser Vereinbarung das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässigen Datenverarbeitungen hinzuweisen.
- (2) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können schriftlich, per E-Mail und per Telefon erfolgen. Der Auftraggeber soll mündliche Weisungen, sofern diese in dieser Vereinbarung zulässig sind, unverzüglich in Textform (z. B. per E-Mail) gegenüber dem Auftragnehmer bestätigen.
- (3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
- (4) Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind:

Anrede, Vorname, Nachname	Kontaktdaten

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

- (5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer feststellt.

§ 4 Rechte und Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach dieser Vereinbarung und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat. Wird der Auftragnehmer durch

das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

- (2) Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer findet vornehmlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in Ländern, die weder Mitgliedstaat der Europäischen Union noch Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) sind („Drittländer“ genannt) bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.
- (4) Der Auftragnehmer soll dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Weisungsempfangsberechtigte Personen des Auftragnehmers sind:

Anrede, Vorname, Nachname	Kontaktdaten

- (5) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Auftraggeber-Daten durch ihn, die bei ihm mit der Verarbeitung beschäftigten Personen oder von ihm beauftragte Dritte erfolgt ist, unverzüglich mitzuteilen. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.
- (6) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO im Falle einer Datenschutzverletzung bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheits-relevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch unterbeauftragte Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 24 Stunden nach bekannt werden der Tatsachen in Schriftform

oder Textform informieren. Die Meldungen enthalten jeweils zumindest die in Art. 33 Absatz 3 DSGVO genannten Angaben.

- (7) *[Alternative 1:]* Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen betrieblichen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Die Kontaktdaten des Datenschutzbeauftragten sind wie folgt:

[vom Auftragnehmer zu ergänzen]

Einen Wechsel in der Person des Datenschutzbeauftragten hat der Auftragnehmer dem Auftraggeber unverzüglich schriftlich mitzuteilen.

[Alternative 2:] Der Auftragnehmer ist nicht verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Der Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen ist *[vom Auftragnehmer zu ergänzen]*.

- (8) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die personenbezogenen Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.
- (9) Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu Folge, so hat der Auftraggeber eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.
- (10) Der Auftragnehmer wird seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verzeichnisses nachkommen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen. An der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 5 Kontrollbefugnisse

- (1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.
- (2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i. S. d. § 5 Absatzes 1 dieser Vereinbarung erforderlich ist.

- (3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungs-systeme und -programme verlangen.
- (4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.
- (5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i. S. d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

§ 6 Unterauftragsverhältnisse

- (1) Die vertraglich vereinbarten Leistungen bzw. die beschriebenen Teilleistungen werden mit Hilfe der in Anhang 1 aufgeführten Unterauftragnehmer durchgeführt, mit deren Beauftragung sich der Auftraggeber einverstanden erklärt.

Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von neuen oder weiteren Unterauftragsverhältnissen mit Unterauftrag-nehmern befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt. Die Information des Auftraggebers umfasst mindestens die in Anhang 2 aufgeführten Angaben. Der Auftragnehmer hat den Auftraggeber mindestens 7 Tage vor Beauftragung des Subunternehmers schriftlich in Kenntnis zu setzen.
- (2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, ob der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten benannt hat, sofern dies nach Art. 37 DSGVO i.V.m. § 38 BDSG erforderlich ist.
- (3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzenden Weisungen des Auftraggebers auch gegenüber den Unterauftragnehmern gelten.
- (4) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungs-vertrag zu schließen, der den Voraussetzungen des Art.

28 DSGVO entspricht. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

- (5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (§ 5 dieser Vereinbarung) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.
- (6) Sofern eine Einbeziehung von Unterauftragnehmern in einem Drittland erfolgen soll, bedarf dies der gesonderten Zustimmung des Auftraggebers und der Auftragnehmer hat sicherzustellen, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau gewährleistet ist und die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).
- (7) Nicht als Unterauftragsverhältnisse i. S. d. Absätze 1 bis 5 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personen-bezogener Daten zu gewährleisten. Wartungs- und Prüfungsleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden. Die Parteien sind sich darüber einig, dass vorgenannte Wartungs- und Prüfleistungen eine „Auftragsverarbeitung“ i. S. d. Art. 28 DSGVO darstellen.

§ 7 Vertraulichkeitsverpflichtung

- (1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.
- (2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf die Wahrung der Vertraulichkeit verpflichtet. Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten

Beschäftigten schriftlich auf das Fernmeldegeheimnis i. S. d. § 88 TKG zu verpflichten.

- (3) Der Auftragnehmer wird alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Auftraggebers erbringen, in schriftlicher Form verpflichten, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten, vertraulich zu behandeln. Dazu gehört, falls nötig, auch die Verpflichtung der Mitarbeiter zur Geheimhaltung u.a. bei der Verarbeitung von Daten, die einem Berufsgeheimnis unterfallen (z.B. aus Krankenhäusern oder von niedergelassenen Ärzten) oder solcher Daten, die dem Fernmeldegeheimnis unterfallen, wenn und soweit im Hauptvertrag entsprechende Leistungen vereinbart sind. Soweit berufs- und standesrechtlich erforderlich, wird der Auftraggeber alle erforderlichen Maßnahmen vornehmen und den Auftragnehmer entsprechend informieren und instruieren. Diese Verpflichtung der Beschäftigten ist auf Anfrage dem Auftraggeber nachzuweisen.

§ 8 Wahrung der Betroffenenrechte

- (1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.
- (2) Soweit die Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.
- (3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

§ 9 Technische und organisatorische Maßnahmen

- (1) Der Auftragnehmer verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zu ergreifen und während der Dauer der Verarbeitung von Auftraggeber-Daten aufrecht zu erhalten, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.
- (2) Der Auftragnehmer garantiert, vor dem Beginn der Verarbeitung insbesondere die in Anhang 2 zu diesem Vertrag spezifizierten technischen und organisatorischen Maßnahmen zu ergreifen und sicherzustellen, dass die Verarbeitung der Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.

- (3) Der Auftragnehmer implementiert ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Geeignetheit der von ihm getroffenen technischen und organisatorischen Maßnahmen im Hinblick auf den Stand der Technik, etwaige Gesetzesänderungen und das Schutzniveau der verarbeiteten personenbezogenen Daten. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.
- (4) Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden.
- (5) Sämtliche Anpassungen sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber regelmäßig (mindestens jährlich) schriftlich oder in Textform mitzuteilen. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

§ 10 Fernzugriff

- (1) Für die Durchführung von Fernzugriffen auf die IT-Systeme des Auftraggebers gelten ergänzend folgende Regelungen:
- (2) Fernzugriffe werden, sofern und soweit hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ausschließlich mit Einwilligung der zuständigen Mitarbeiter des Auftraggebers ausgeführt.
- (3) Der Auftragnehmer verwendet angemessene Identifizierungs- und Verschlüsselungsverfahren.
- (4) Fernzugriffe werden vom Auftragnehmer dokumentiert und protokolliert. Der Auftraggeber ist berechtigt Fernzugriffe bei und nach Durchführung zu kontrollieren. Dabei hat er die in § 5 dieser Vereinbarung aufgeführten Bestimmungen zu beachten. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich und im Hinblick auf die Art der erbrachten Leistungen realisierbar - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abubrechen.
- (5) Fernzugriffe zu den relevanten Systemen des Auftraggebers erfolgen nur nach dem Need-to-know-Prinzip.
- (6) Der Auftragnehmer darf Auftraggeber-Daten im Wege eines Filetransfers oder Downloads für Zwecke der Leistungserbringung nur dann von den Datenverarbeitungssystemen des Auftraggebers abziehen und auf sein eigenes kopieren, wenn er dafür jeweils zuvor und für den Einzelfall die Einwilligung des Auftraggebers eingeholt hat. Auftraggeber-Daten dürfen nur zum Zweck der Leistungserbringung nach dem Hauptvertrag verwendet werden und dürfen

zudem nicht ohne angemessene Verschlüsselung auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.

- (7) Software-Aktualisierungen dürfen in Abstimmung mit dem Auftraggeber nur nach vorheriger Zustimmung eingespielt werden. Es ist sicherzustellen, dass eine hinreichende Datensicherung der Auftraggeber-Daten gewährleistet ist.
- (8) Personenbezogene Daten, die der Auftragnehmer beim Fernzugriff erhalten hat, wird der Auftragnehmer dem Auftraggeber unverzüglich zurückgeben, wenn diese Daten für die Durchführung der Leistungen des Auftragnehmers nach dem Hauptvertrag nicht mehr erforderlich sind, oder mit Einwilligung des Auftraggebers löschen. Etwaige dem Auftragnehmer übergebene Papierausdrucke mit personenbezogenen Daten muss der Auftragnehmer nach Abschluss des Hauptvertrages unverzüglich zurückgeben oder mit Zustimmung des Auftraggebers datenschutzgerecht vernichten.

§ 11 Dauer des Auftrags

- (1) Diese Vereinbarung beginnt ab Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.
- (2) Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieser Vereinbarung und eine Kündigung dieser Vereinbarung als Kündigung des Hauptvertrages.
- (3) Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

§ 12 Haftung

- (1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.
- (2) Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Auftraggeber in dieser AV-Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.
- (3) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DSGVO.
- (4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 13 Berichtigung, Einschränkung, Löschung und Rückgabe von personenbezogenen Daten

- (1) Der Auftragnehmer darf die Auftraggeber-Daten, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken
- (2) Der Auftragnehmer hat bei Beendigung der Auftragsverarbeitung, nach Wahl des Auftraggebers, sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Auftragsverarbeitung stehen, dem Auftraggeber zu übergeben oder datenschutzgerecht zu vernichten, soweit nicht EU oder nationales Recht die Aufbewahrung der Daten erfordert. Gleiches gilt für Test- und Ausschussmaterial. Nach Übergabe der personenbezogenen Daten an den Auftraggeber sind die im vorhergehenden Satz genannten Daten sowie etwaige Kopien der Daten beim Auftragnehmer von diesem unverzüglich datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist dem Auftraggeber auf Anforderung vorzulegen.
- (3) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

§ 14 Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

§ 15 Schlussbestimmungen

- (1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
- (2) Sofern nicht durch geltendes Recht oder ein behördliches Ersuchen untersagt, hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ersuchen von staatlichen Stellen, Datenschutzbehörden oder Strafverfolgungsbehörden um Zugang zu oder Beschlagnahme der Auftraggeber-Daten zu unterrichten.
- (3) Ergänzungen oder Änderungen dieser Vereinbarung einschließlich dieser Klausel bedürfen zu ihrer Wirksamkeit der Schriftform.
- (4) Erfüllungsort für die Leistungen aus dieser Vereinbarung ist der Sitz des Auftraggebers.
- (5) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Folgende Dokumente sind untrennbarer Bestandteil dieser Vereinbarung:

Anhang 1: Unterauftragsverhältnisse beim Auftragnehmer

Anhang 2: Technische und organisatorische Maßnahmen des Auftragnehmers zum
Datenschutz gemäß Art. 32 DSGVO

Auftraggeber

Auftragnehmer

(Ort/Datum)

(Ort/Datum)

(Unterschrift)

(Unterschrift)

Anhang 1:
Unterauftragsverhältnisse beim Auftragnehmer

Unterauftragnehmer (Firmenname mit Rechtsform)	Beschreibung der (Teil-)Leistungen	Anschrift/ Ort der Leistungserbringung
[Hinweis: Vom Auftragnehmer zu ergänzen]	[Hinweis: Vom Auftragnehmer zu ergänzen]	[Hinweis: Vom Auftragnehmer zu ergänzen]

Anhang 2:
Technische und organisatorische
Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

[Diese Angaben sind vom Auftragnehmer zu ergänzen]

ENTWURF