Anlage 4 – Datenschutzvereinbarung nach Art. 28 DSGVO
(Zum Verbleib beim Bieter bestimmt! Nicht mit dem Angebot einreichen!)

Datenschutzvereinbarung zum Vertrag über die Einsammlung und des Transportes von Rest-, Biomüll und Altpapier im Main-Tauber-Kreis

zwischen dem

Abfallwirtschaftsbetrieb Main-Tauber-Kreis (AWMT)
vertreten durch …,
Gartenstraße 2, 97941 Tauberbischofsheim

- nachstehend "Auftraggeber" genannt -

und

die

[Hinweis: wird bei Vertragsschluss entsprechend ergänzt]

- nachstehend "Auftragnehmer" genannt -

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Rahmen der Abfallwirtschaft gemäß Vertrag vom *[Hinweis: wird bei Vertragsschluss entsprechend ergänzt]* (im Folgenden: "Hauptvertrag"). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutz-Grundverordnung (DSGVO).

Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Regelungen des Art. 28 der Datenschutz-Grundverordnung (DSGVO) zwischen den Parteien getroffen.

1. Allgemeines

(1) Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "Auftraggeberdaten") erhält und diese ausschließ-

lich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO verarbeitet.

(2) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

2. Dauer und Beendigung des Auftrags

(1) Diese Vereinbarung beginnt ab Unterzeichnung durch beide Parteien und gilt für die Dauer des Hauptvertrages. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

(2) Ein außerordentliches Kündigungsrecht aus wichtigem Grund jeder Partei bleibt unberührt. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmer gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag 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.

3. Gegenstand des Auftrags

(1) Zweck, Art und Umfang der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten im Rahmen des Auftrags ergeben sich aus dem Hauptvertrag, auf den insoweit Bezug genommen wird. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich in der in der durch den Hauptvertrag spezifizierten Art sowie in dem dort spezifizierten Umfang und Zweck. Dem Auftragnehmer ist eine abweichende oder über die Festlegungen im Hauptvertrag hinausgehende Verarbeitung von Auftraggeberdaten untersagt. Dies gilt auch für die Verwendung anonymisierter Daten.

(2) Der Auftrag kann die Verarbeitung folgender Arten von personenbezogenen Daten beinhalten:

- Namen
- Adressdaten

(3) Kreis der von der Datenverarbeitung betroffenen Personen:

- Grundstückeigentümer
- Haushalte

4. Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung durch den Auftragnehmer allein verantwortlich.

(2) Der Auftraggeber und der Auftragnehmer sind darüber hinaus bezüglich der zu verarbeitenden personenbezogenen Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

5. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang und Methode der Verarbeitungstätigkeiten zu erteilen. Dieser kann jederzeit ergänzende Weisungen über Art, Umfang und Verfahren gegenüber dem Auftragnehmer zu erteilen.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich oder in Textform (z.B. E-Mail) erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer schriftlich zu bestätigen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

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

6. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 28 DSGVO (Auftragsverarbeitung), dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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 Auftraggeberdaten durch den Auftragnehmer findet ausschließlich 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 ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 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 ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Zusammenhang mit dem Hauptvertrag im Auftrag verarbeitet, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(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 unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(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 sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 24 Stunden in Schriftform oder elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen enthalten jeweils zumindest die in Art. 33 Absatz 3 DSGVO genannten Angaben.

(7) Der Auftragnehmer wird seinen Pflichten aus Art. 30 Abs. 2 DSG-VO zum Führen eines Verarbeitungsverzeichnisses nachkommen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(8) 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.

(9) Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat.

(10) Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

7. Kontrollbefugnisse des Auftraggebers

(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. Absatzes 1 erforderlich ist.

(3) 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, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden könnten.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSG-VO i.V.m. § 40 BDSG, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

8. Unterauftragverhältnisse

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der im Anhang 2 genannten Unterauftragnehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Unterauftragnehmern („Unterauftragsverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich zugestimmt hat.

(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, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personen-

bezogener 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. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(4) Die Verpflichtung des Unterauftragnehmers muss den Anforderungen von Art. 28 Abs. 4 DSGVO entsprechen.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 7 dieses Vertrages) 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, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln).

(7) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

9. Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 DSGVO. Er wird dem Auftraggeber unverzüglich die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftragnehmer nicht selbst über die entsprechenden Informationen verfügt.

(2) Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DSGVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich zu berichtigen, löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

(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.

10. Vertraulichkeit und Geheimhaltung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber wird dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitteilen.

(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 zur Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet hat, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

11. Technische und Organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, insbesondere mindestens die im Anhang 1 aufgeführten Maßnahmen.

(2) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber unverzüglich schriftlich zu informieren, wenn er Grund zu der Annahme hat, dass die getroffenen Maßnahmen gemäß Anhang 1 nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

12. Fernzugriff

(1) Für die Durchführung von Fernzugriffen auf die IT-Systeme des Auftraggebers gelten ergänzend folgende Regelungen:

a) Fernzugriffe werden, sofern und soweit hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ausschließlich mit Einwilligung der zuständigen Mitarbeiter des Auftraggebers ausgeführt.

b) Der Auftragnehmer verwendet angemessene Identifizierungs- und Verschlüsselungsverfahren.

c) Der Auftragnehmer darf personenbezogene 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.

d) Software-Aktualisierungen dürfen in Abstimmung mit dem Auftraggeber nur nach vorheriger Genehmigung des Kunden eingespielt werden.

e) 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 Auf-

tragnehmers 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.

13. Rechte und Pflichten nach Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

(2) 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. Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Tauberbischofsheim, den TT.MM.JJ

....
(Auftraggeber) (Auftragnehmer)

Anhang 1 – Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

(Zum Verbleib beim Bieter bestimmt! Nicht mit dem Angebot einreichen!)

Der Auftragnehmer ist verpflichtet, nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO einzuhalten:

1. Vertraulichkeit

Zutrittskontrolle

Der Auftragnehmer trägt Sorge dafür, dass seine Büro- und Geschäftsräume grundsätzlich außerhalb der Büro- und Geschäftszeiten geschlossen sind.

Während der Büro- und Geschäftszeiten ist sichergestellt, dass Besucher oder sonstige Dritte sich nicht alleine in Räumen bewegen können, in denen sie Zugang zu personenbezogenen Daten erhalten könnten.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Beschäftigten über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von einem oder mehreren Administratoren vergeben.

Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden nach einem vorgegebenen Turnus von 90 Tagen gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen.

Alle Server und Client-Systeme, die bei der Erbringung von Leistungen für den Auftraggeber im Einsatz sind, sind durch Firewalls geschützt, die gewartet und mit aktuellen Updates und Patches versorgt werden.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter, die der Auftragnehmer vom Auftraggeber erhält oder für dessen IT-Systeme verwendet, werden grundsätzlich verschlüsselt gespeichert und sind nur den Beschäftigten zugänglich zu machen, die konkret mit der Erbringung von Leistungen für den Auftraggeber betraut sind.

Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.

Trennung

Soweit der Auftragnehmer personenbezogene Daten vom Auftraggeber im Zusammenhang mit der Auftragsverarbeitung erhält, wird er diese getrennt von Daten anderer Kunden verarbeiten.

Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf IT-Systeme des Auftraggebers erfolgt grundsätzlich über verschlüsselte Verbindungen, soweit dieser nicht innerhalb der Räumlichkeiten des Auftraggebers erfolgt.

2. Integrität

Eingabekontrolle

Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag des Auftraggebers durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt.

Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie und soweit dies mit dem Auftraggeber abgestimmt ist.

Die Nutzung von privaten Datenträgern ist dem Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung für den Auftraggeber untersagt.

3. Verfügbarkeit und Belastbarkeit

Soweit der Auftragnehmer personenbezogene Daten oder Zugangsdaten für den Auftraggeber speichert oder verwaltet, trägt er Sorge dafür, dass diese Daten mindestens täglich inkrementell und wöchentlich „voll“ gesichert werden. Es gibt ein Datensicherungskonzept, dass auch das erfolgreiche Testen der Wiederherstellung von Daten beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DSGVO entspricht.

Dies beinhaltet insbesondere eine regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

Auftragskontrolle

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Etwaige nach Art. 25 DSGVO erforderliche Maßnahmen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten durch den Auftraggeber sind vom Auftraggeber zu treffen bzw. durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer festzulegen.

Anhang 2 – Unterauftragsverhältnisse beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

(Zum Verbleib beim Bieter bestimmt! Nicht mit dem Angebot einreichen!)

[Hinweis: wird bei Vertragsschluss entsprechend ergänzt]

Name und Anschrift des Unterauftragnehmers	Beschreibung der (Teil-)Leistungen	Ort der Leistungserbringung