Anlage [3] zum Vertrag [75-2026-001]

Hinweis: Der Vertragsgegenstand des Hauptvertrages mit der bezüglichen Vertragsnummer ist unten in § 1 aufzunehmen.

Vereinbarung über Inanspruchnahme von technischen Einrichtungen zur Fernkommunikation von einem Standort außerhalb des Einsatzortes des Systems des Landesamtes für Umwelt (Remote-Zugriff - Vereinbarung)

zwischen dem

Land Rheinland-Pfalz, vertreten durch das Ministerium für Klimaschutz, Umwelt, Energie und Mobilität, vertreten durch das Landesamt für Umwelt, Kaiser-Friedrich-Straße 7, 55116 Mainz, dieses vertreten durch den Präsidenten

- Auftraggeber-

und dem/der

[gleiche Angaben, wie im Hauptvertrag zu Auftragnehmer]

- Auftragnehmer -

§ 1 Gegenstand der Vereinbarung

(1) Der Auftraggeber gestattet dem Auftragnehmer den Zugang zu den bei dem Auftraggeber vorhandenen informationstechnischen Systemen durch Aufbau externer Kommunikationsverbindungen („Remote-Zugriff“) im Zusammenhang mit der Erfüllung des Vertrags „*Rahmenvereinbarung zur Betriebsunterstützung, Anpassungs- und Weiterentwicklung für gewässer- und abwasserbezogene IT-Fachverfahren in der Wasserwirtschaftsverwaltung RLP“ 75-2026-001*, auf den Bezug genommen wird. Die Einzelheiten der Eröffnung dieses Zugangs richten sich nach den folgenden Vorschriften.

(2) Der Auftragnehmer führt ausschließlich die Tätigkeiten durch, die zur Erfüllung der beauftragten Leistungen erforderlich sind. Er führt sie ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Änderungen des Tätigkeitsfeldes und Verfahrensänderungen sind schriftlich zu vereinbaren. Der Auftragnehmer speichert oder verarbeitet personenbezogene Daten ausschließlich im Auftrag und auf Weisung des Auftraggebers.

(3) Der Auftraggeber orientiert sich beim Umgang mit informationsverarbeitenden Systemen und bei der Informationssicherheit an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI-Grundschutz). Der Auftraggeber nutzt das vom Land Rheinland-Pfalz bereitgestelltes, BSI-zertifiziertes RLP-Netz, dessen IT-Sicherheitsbestimmungen bei Betrieb von IT-Infrastrukturen und IT-Systemen vom Auftraggeber und Auftragnehmer einzuhalten sind.

(4) Die Parteien informieren sich unverzüglich gegenseitig, wenn sie Fehler oder Unregelmäßigkeiten beim Remote-Zugriff und bei Prüfung der Auftragsergebnisse oder der Verarbeitungsschritte feststellen. (aus den Pflichten AG hierzu vorgezogen!)

§ 2 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber wird dem Auftragnehmer nur die für die Durchführung der vereinbarten Tätigkeiten benötigten Zugriffsrechte bereitstellen, deren Aktualität regelmäßig überprüfen und gegebenenfalls Korrekturen vornehmen.

(2) Der Auftraggeber hat das Recht, den Zugriff des Auftragnehmers auf die informationstechnischen Systeme des Auftraggebers jederzeit zu unterbrechen. Dies gilt insbesondere, wenn der Verdacht besteht, dass unbefugt auf Informationen und Ressourcen zugegriffen wird.

(3) Der Auftraggeber ist berechtigt, sämtliche Aktionen des Auftragnehmers innerhalb seiner Infrastruktur zu protokollieren und auszuwerten; soweit technisch möglich ist der Auftraggeber berechtigt, den Zugriff von einem Kontrollbildschirm aus zu verfolgen.

(4) Notwendige Datenübertragungen zu Zwecken des Zugriffs müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen.

(5) Der Auftraggeber ist berechtigt, die ordnungsgemäße Einhaltung der Vorschriften aus dieser Vereinbarung in der Umgebung, aus der heraus die Tätigkeiten erfolgen zu kontrollieren oder kontrollieren zu lassen. Der Auftragnehmer gewährt dazu nach Absprache ungehinderten Zutritt, Zugang und Zugriff zu informationsverarbeitenden Systemen, Programmen, Dateien und Informationen, die mit der Durchführung der Tätigkeiten in Verbindung stehen. Dem Auftraggeber sind durch den Auftragnehmer alle Auskünfte zu erteilen, die zur Erfüllung der Kontrollfunktion benötigt werden.

§ 3 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Tätigkeiten unerlässlich notwendigen Umfang Gebrauch machen.

(2) Der Auftragnehmer ist verpflichtet, Unbefugten den Zutritt zu seinen Systemen, mit denen Daten des Auftraggebers verarbeitet und genutzt werden, zu verwehren und die eingesetzten Systeme zum Remote-Zugang vor Nutzung von Unbefugten zu schützen.

(3) Der Auftragnehmer trägt dafür Sorge, dass Daten des Auftraggebers bei Speicherung, Verarbeitung oder Nutzung in Systemen des Auftragnehmers nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,

(3) Informationen, Daten und Programme dürfen lediglich im Rahmen der Erfüllung der vereinbarten Tätigkeiten und nach der Genehmigung durch den Auftraggeber von oder aus der Infrastruktur des Auftraggebers übertragen bzw. installiert werden. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(4) Der Zugriff darf nur von Systemen aus erfolgen, deren Sicherheitsniveau den Vorgaben der Informationssicherheit beim Auftraggeber entspricht. Der Zugriff über mobile Endgeräte ist ebenso wenig gestattet wie der Zugriff von einer Infrastruktur außerhalb der Geschäftsräume des Auftragnehmers.

(5) Der Auftragnehmer sichert zu, dass

a. die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

b. seine Rechnerumgebung, aus dem der Remote-Zugriff erfolgt, dem aktuellen Stand der Technik entspricht und durch geeignete Mittel sichergestellt ist, dass diese frei von Schadsoftware (Viren, Würmer, Trojaner, …) sind. Dies gilt auch für alle ausgetauschten Daten.

c. Systeme, welche sich unter seinem Zugriff befinden, keine Verbindungsversuche zu sonstigen Systemen des Auftraggebers initiieren.

d. alle Tätigkeiten, welche nicht eng an die Erfüllung der vereinbarten Dienstleistung gebunden sind, unterlassen werden. Dazu gehört unter anderem das eigenmächtige Einrichten von Verbindungen zu Dritt-Netzwerken, wie z.B. dem Internet.

e. die einschlägigen europa-, bundes- und landesrechtlichen Bestimmungen zum Datenschutz eingehaltenwerden.

(6) Innerhalb von vierzehn (14) Tagen sind nach der schriftlichen Aufforderung durch den Auftraggeber von dem Auftragnehmer alle ihm vorliegenden vertraulichen Informationen und aufgrund dieser Informationen gefertigten weiteren Unterlagen, dem Auftraggeber zurückzusenden bzw. nachvollziehbar zu vernichten.

(7) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln, auch über das Vertragsende unbefristet hinaus.

(8) Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

(9) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

(10) Der Auftragnehmer stellt sicher, dass die Infrastruktur des Auftraggebers nicht durch seine Tätigkeiten negativ beeinflusst wird. Unter negativer Beeinflussung ist das unregelmäßige, abnormale Verhalten der Infrastruktur zu verstehen, das zu einem Versagen einzelner Komponenten oder des gesamten Systems führt und der Auftragnehmer verschuldet hat.

(11) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen.

(12) Der Auftragnehmer verpflichtet alle Personen, die von ihm mit der Erfüllung oder Bearbeitung von Leistungen oder in anderer Weise beauftragt sind, auf die Pflichten

aus dieser Vereinbarung vermittels einer gesonderten vertraglichen, haftungsbegründenden Vereinbarung.

(13) Die Einschaltung von Unterauftragnehmern ist ausgeschlossen. Soll im Einzelfall davon abgewichen werden, bedarf dies der gesonderten schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer stellt in diesem Falle vertraglich sicher, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen.

§ 4 Remote-Zugriff und Auftragsverarbeitung

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung von personenbezogenen Daten sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Eine Verarbeitung erfolgt nur, soweit es im zugrunde liegenden Leistungsvertrag vereinbart ist oder der Zugriff auf personenbezogene Daten im Rahmen eines Remote-Zugriffs technisch nicht ausgeschlossen werden können. Hierunter fallen ebenfalls Tätigkeiten, bei denen Daten von einem System in ein anderes migrieren.

(3) Die Parteien schließen in diesem Fall in Ergänzung zu diesem Vertrag eine schriftliche Vereinbarung zur Auftragsverarbeitung ab, die zumindest die gesetzlichen Mindestanforderungen beinhaltet und die beim Auftraggeber durch einen Remote-Zugriff oder eine Datenmigration betroffenen personenbezogenen Daten nach ihrem Umfang, der Art und dem Zweck der vorgesehenen Verarbeitung von Daten, der Art der Daten und dem Kreis der Betroffenen vom Auftraggeber vor der Auftragserteilung schriftlich fixiert.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei dieser Aufgabe.

(5) Der Auftragnehmer speichert oder verarbeitet personenbezogene Daten ausschließlich im Auftrag und auf Weisung des Auftraggebers.

(6) Der Auftragnehmer stellt im Zusammenhang mit datenschutzrelevanten Tätigkeiten die gem. Art. 28 Abs. 1 DS-GVO zu treffenden technischen und organisatorischen Maßnahmen sicher. Die technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung anzupassen.

(7) Die weiteren Rechte und Pflichten aus einer Auftragsverarbeitung, insbesondere Weisungsrechte des Auftraggebers gegenüber dem Auftragnehmer, unterliegen den Regelungen der bezüglichen Vereinbarung über die Auftragsverarbeitung.

§ 5 Remote-Zugriff im Zusammenhang mit Prüfungs-/Wartungsarbeiten

(1) Remote-Zugriffe zu Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagenwerden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.

(2) Vor Durchführung von Remote-Zugriffe zu Zwecken von Prüfungs- und/oder Wartungsarbeiten werden sich Auftraggeber und Auftragnehmer über etwaig notwendige Datensicherungsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch den Auftragnehmer feststellt.

(4) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfange – auch in zeitlicher Hinsicht - Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(5) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions- /Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.

(6) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchen des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.

§ 6 Zugang

(1) Die Durchführung von Arbeiten des Auftragnehmers im Remote-Zugriff erfolgt über ein vom Auftraggeber eingerichtetes Virtual Private Network (VPN), in dem authentifizierte Personen verschlüsselte Daten über standardmäßige Internetprotokolle austauschen. Durch die Verschlüsselung wird sichergestellt, dass Daten während der Übertragung nicht von Dritten verändert werden können (Integrität).

(2) Der Auftragnehmer erhält vom Auftraggeber eine VPN-Software (Endpoint Security), die auf dem Rechner des Auftragnehmers aufgespielt wird.

(3) Für den Auftragnehmer wird entsprechend der vertraglich vereinbarten Aufgaben für die Zugänge zu und Rechte auf Servern des Auftraggebers ein Zugriffsprofil erstellt.

(4) Mitarbeiter des Auftragnehmers erhalten auf Antrag des Auftragnehmers hin vom Auftraggeber eigene individualisierte Einwahl- und Zugriffsdaten. Mit diesen können die Mitarbeiter des Auftragnehmers auf die im Zugriffsprofil für sie hinterlegten Server zugreifen. Auf den Servern werden ebenso personalisierte Zugänge eingerichtet.

(5) Vor Freischaltung des VPN-Zugangs hat der betreffende Mitarbeiter des Auftragnehmers die Kenntnisnahme hinsichtlich der Regelungen in dieser Vereinbarung schriftlich gegenüber dem Auftraggeber zu bestätigen.

(6) Die Authentifizierungen und Zugriffe werden protokolliert. Die Arbeiten auf den Servern werden entsprechend den Mitteln des Betriebssystems protokolliert.

(7) Die Protokollierungen werden aus betrieblichen Gründen maximal drei Monate aufbewahrt.

(8) Anträge hinsichtlich des Zugangs von Mitarbeitern werden unter Bezugnahme auf den in § 1 Bezug genommen Vertrag gerichtet an: support@lfu.rlp.de.

§ 7 Weisungen des Auftraggebers

(1) Der Auftragnehmer darf den Zugriff nur im Rahmen der Weisungen des Auftraggebers durchführen. Der Auftragnehmer wird den Auftraggeber informieren, wenn eine vom Auftraggeber erteilte Weisung nach Auffassung des Auftragnehmers gegen gesetzliche Vorschriften verstößt.

(2) Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftraggeber kann durch Einzelweisungen die Berichtigung, Löschung und Sperrung von Daten verlangen, die der Auftragnehmer bei dem Zugriff erhalten hat.

§ 8 Ansprechpartner des Auftraggebers

Ansprechpartner des Auftraggebers im Zusammenhang mit dieser Vereinbarung über Remote-Zugriff, insbesondere für die Einrichtung und Überwachung der VPN-Zugänge ist das Referat für „Informations- und Kommunikationstechnik“ (IuK) mit folgender Kontaktadresse: support@lfu.rlp.de

§ 9 Haftung

(1) Der Auftragnehmer haftet ohne Beschränkung für alle Schäden, die dem Auftraggeber durch schuldhafte Verletzung von Verpflichtungen aus dieser Vereinbarung über den Remote-Zugriff entstehen.

(2) Eventuelle Regelungen in bestehenden Verträgen, die mit dieser Vereinbarung verbinden sind (Grundvertrag und Vereinbarung über Auftragsverarbeitung) bleiben von dieser Vertraulichkeitsverpflichtungserklärung unberührt.

§ 10 Wirksamkeit der Vereinbarung / Schriftform

(1) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(2) Ergänzungen und sonstige Änderungen dieser Vereinbarung bedürfen der Schriftform.

Für den Auftraggeber:

Mainz, _____

.....

(Unterschrift)

Für den Auftragnehmer:

_____, _____

.....

(Unterschrift)