VEREINBARUNG ÜBER DIE AUFTRAGSVERARBEITUNG NACH ART. 28 DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

zwischen

dem **Oldenburgisch-Ostfriesischer Wasserverband,**
vertreten durch den Geschäftsführer Karsten Specht, Georgstraße 4, 26919 Brake

- im Folgenden „**Auftraggeber“** genannt -

und

- im Folgenden „**Auftragnehmer“** genannt -

- im Folgenden (gemeinsam) auch „**Vertragspartner“** genannt -

Inhaltsverzeichnis

Präambel 3
§ 1 Gegenstand und Dauer der Vereinbarung 3
§ 2 Verantwortlichkeit und Weisungsbefugnis 4
§ 3 Pflichten des Auftragnehmers 4
§ 4 Pflichten des Auftraggebers 7
§ 5 Nachweis der Einhaltung dieser Vereinbarung 7
§ 6 Weitere Auftragsverarbeiter (Art. 28 Abs. 3 S. 2 lit. d) DS-GVO) 8
§ 7 Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO 9
§ 8 Verpflichtungen des Auftragnehmers nach Beendigung dieser Vereinbarung 10
§ 9 Vergütung 11
§ 10 Haftung und Schadenersatz 11
§ 11 Schlussbestimmungen 11
Anlage 1 13
Anlage 2 14
Anlage 3 15

Präambel

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DS-GVO).

Diese Vereinbarung konkretisiert die Pflichten der Vertragspartner zum Schutz personenbezogener Daten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Die Vereinbarung findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder sonstige durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

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 DS-GVO zugrunde gelegt.

Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DS-GVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer.

§ 1
Gegenstand und Dauer der Vereinbarung

(1) Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Leistungen:

Siehe Dokument 2026-04827_B01_Leistungsbeschreibung

(2) Dauer auf die Leistungsvereinbarung

Der Vertrag beginnt mit Unterzeichnung und wird auf unbestimmte Zeit geschlossen. Er ist mit einer Frist von drei Monaten zum Quartalsende kündbar. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers 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) Die Kategorien personenbezogener Daten und betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt.

(4) Die vertraglich vereinbarte Leistung des Auftragnehmers wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung insgesamt oder von Teilen in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln oder genehmigte Verhaltensregeln).

§ 2
Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Verarbeitung der personenbezogenen Daten i. S. d. Art. 4 Nr. 7 DS-GVO verantwortlich und weisungsbefugt.

(2) Weisungen werden zu Beginn der Auftragsverarbeitung vertraglich festgelegt und können vom Auftraggeber danach in Schrift- oder Textform an die vom Auftragnehmer bezeichneten Stellen durch einzelne Weisung geändert, ergänzt oder ersetzt werden.

(3) Weisungen, die in der Vereinbarung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich in Schrift- oder Textform zu bestätigen.

(4) Ist der Auftragnehmer der Meinung, dass eine Weisung des Auftraggebers gegen anwendbare Gesetze verstößt, so teilt er dies dem Auftraggeber unverzüglich mit. In einem solchen Fall ist der Auftragnehmer berechtigt, die Umsetzung der Weisung solange auszusetzen, bis diese vom Auftraggeber bestätigt oder abgeändert wurde.

§ 3
Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf die personenbezogenen Daten ausschließlich im Rahmen der in dieser Vereinbarung oder dem dieser Vereinbarung zugrunde liegenden Vertragsverhältnis getroffenen Regelungen und nach den Weisungen des Auftraggebers verarbeiten, es sei denn, es liegt ein Ausnahmefall i. S. d. Art. 28 Abs. 3 lit.

a) DS-GVO vor. In einem solchen Fall, teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer verarbeitet die personenbezogenen Daten für den Auftraggeber getrennt von sonstigen Datenbeständen und ausschließlich zur Erfüllung der ihm gegenüber dem Auftraggeber obliegenden Verpflichtungen. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Datenträger, die vom Auftraggeber stammen oder für den Auftraggeber benutzt werden, sind besonders zu kennzeichnen. Eingang und Ausgang sowie die laufende Verwendung dieser Datenträger werden durch den Auftragnehmer dokumentiert.

(3) Der Auftragnehmer überwacht die Einhaltung der anwendbaren Datenschutzgesetze sowie dieser Vereinbarung bei der Ausführung der Auftragsverarbeitung. Er macht die bei der Auftragsverarbeitung eingesetzten Personen vor der Aufnahme ihrer Tätigkeiten mit den für sie maßgebenden Bestimmungen der Datenschutzgesetze sowie dieser Vereinbarung vertraut und stellt sicher, dass die Daten ausschließlich gemäß den Weisungen des Auftraggebers verarbeitet werden (Art. 29 DS-GVO). Der Auftragnehmer wird zudem die mit der Auftragsverarbeitung befassten Personen zur Vertraulichkeit verpflichten bzw. sicherstellen, dass diese einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 S. 2 lit. b) DS-GVO). Die Vertraulichkeits- bzw. Verschwiegenheitspflicht muss auch nach Beendigung der Auftragsverarbeitung fortbestehen.

(4) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung seiner Pflichten gegenüber betroffenen Personen aus Kapitel III der DS-GVO sowie bei der Einhaltung der Pflichten aus Art. 32 bis 36 DS-GVO. Der Auftragnehmer hat insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DS-GVO nachkommen kann. Auskünfte über personenbezogene Daten aus dem Auftragsverarbeitungsverhältnis, betroffene Personen oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung des Auftraggebers erteilen.

(5) Der Auftragnehmer ist verpflichtet, den Auftraggeber unverzüglich zu unterrichten, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minimierung möglicher nachteiliger Folgen der betroffenen Person und berät sich hierzu unverzüglich mit dem Auftraggeber.

(6) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DS-GVO bestehen kann, die eine Meldung an die

Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(7) Der Auftragnehmer gewährleistet die Erfüllung seiner Pflichten aus Art. 32 Abs. 1 lit. d) DS-GVO durch ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(8) Der Auftragnehmer berichtigt oder löscht personenbezogene Daten aus dem Auftragsverarbeitungsverhältnis nach Weisung des Auftraggebers oder schränkt deren Verarbeitung ein. Sind eine Löschung oder eine Einschränkung der Verarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien, soweit er vom Auftraggeber eine Weisung hierzu erhält. Andernfalls gibt er die Datenträger an den Auftraggeber zurück.

(9) Der Auftragnehmer nennt dem Auftraggeber in Schrift- oder Textform einen Ansprechpartner für alle bei der Durchführung dieser Vereinbarung auftretenden Fragen. Ein Wechsel des Ansprechpartners ist dem Auftraggeber unverzüglich in Schrift- oder Textform mitzuteilen.

(10) Wird der Auftraggeber durch eine betroffene Person nach Art. 82 DS-GVO in Anspruch genommen, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen. Er wird den Auftraggeber zudem unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, 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 Auftraggeber ermittelt.

(11) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogene Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Schweigepflicht unterliegen (Art. 28 Abs. 3 lit. b DS-GVO).

(12) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DS-GVO benannt hat, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(13) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 12 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

§ 4
Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er bei der Durchführung dieser Vereinbarung von Fehlern oder Unregelmäßigkeiten in der Auftragsverarbeitung Kenntnis erlangt.

(2) Wird der Auftragnehmer durch eine betroffene Person nach Art. 82 DS-GVO in Anspruch genommen, verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.

(3) Der Auftraggeber nennt dem Auftragnehmer einen Ansprechpartner für alle bei der Durchführung dieser Vereinbarung auftretenden Fragen. Ein Wechsel des Ansprechpartners ist dem Auftragnehmer unverzüglich in Schrift- oder Textform mitzuteilen.

§ 5
Nachweis der Einhaltung dieser Vereinbarung

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der Pflichten aus dieser Vereinbarung mit geeigneten Mitteln nach.

(2) Der Auftraggeber ist berechtigt, sich vor Beginn der Auftragsverarbeitung sowie in regelmäßigen Abständen von der Einhaltung der beim Auftragnehmer betroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen. Soweit er hierzu die Durchführung von Inspektionen (selbst oder durch einen von ihm beauftragten Prüfer) beabsichtigt, teilt er dies dem Auftragnehmer mit angemessener Vorlaufzeit mit. Inspektionen haben grundsätzlich zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs zu erfolgen. Soweit erforderlich, ist der Auftraggeber oder ein von ihm beauftragter Prüfer verpflichtet, eine Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden des Auftragnehmers oder der eingerichteten technischen organisatorischen Maßnahmen abzugeben. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen beauftragten Prüfer ein Einspruchsrecht.

§ 6
Weitere Auftragsverarbeiter (Art. 28 Abs. 3 S. 2 lit. d) DS-GVO)

(1) Der Auftragnehmer nimmt keinen weiteren Auftragsverarbeiter bei der Erfüllung seiner vertraglichen Verpflichtungen gegenüber dem Auftraggeber ohne vorherige schriftliche Zustimmung des Auftraggebers in Anspruch. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 2 zu diesem Vertrag angeben.

(2) Nimmt der Auftragnehmer die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer vereinbart sind. Dabei müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Der Vertrag wird in Schriftform geschlossen. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(3) Der Auftragnehmer ist verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (§ 5 (2) 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.

(4) Der Auftragnehmer ist verpflichtet, vor der Beauftragung eines weiteren Auftragsverarbeiters die Eignung der von dem weiteren Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen i. S. v. Art. 32 DS-GVO zu prüfen. Die relevanten Prüfungsunterlagen sind dem Auftraggeber auf dessen Verlangen hin zur Verfügung zu stellen.

(5) Eine Beauftragung von weiteren Auftragsverarbeitern in Drittstaaten darf nur erfolgen, soweit die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind und der Auftraggeber über den Umstand informiert ist und dem zugestimmt hat. Der Auftragnehmer hat die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicherzustellen.

(6) Die Übermittlung von personenbezogenen Daten an den weiteren Auftragsverarbeiter ist erst zulässig, wenn der weitere Auftragsverarbeiter die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

(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 und 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 personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und eine Auftragsverarbeitung i. S. d. Art. 28 DS-GVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und sofern bei der Wartung personenbezogene Daten zur Kenntnis genommen werden können, die im Auftrag des Auftraggebers verarbeitet werden.

§ 7
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

(1) Der Auftragnehmer hat die Umsetzung der nach Art. 32 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren. Soweit der Auftraggeber den technischen und organisatorischen Maßnahmen zustimmt, werden diese Grundlage dieser Vereinbarung.

(2) Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den geltenden Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der zu verarbeitenden Daten des Auftraggebers treffen, die insbesondere den Anforderungen der Art. 28 Abs. 3 lit c, 32 DS-GVO i. V. m. Art. 5 Abs. 1, 2 DS-GVO genügen. Zu diesem Zweck trifft der Auftragnehmer technische und organisatorische Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die Einzelheiten hierzu ergeben sich aus Anlage 3 zu dieser Vereinbarung.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

(4) Der Auftraggeber kann jederzeit die aktuelle Dokumentation der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(5) Wesentliche Änderungen der vom Auftragnehmer getroffenen organisatorischen und technischen Maßnahmen sind dem Auftraggeber in Schrift- oder Textform mitzuteilen. Etwaige Korrespondenz zwischen Auftragnehmer und Auftraggeber über die Änderung der technischen und organisatorischen Maßnahme sind für die Dauer dieser Vereinbarung aufzubewahren.

§ 8
Verpflichtungen des Auftragnehmers nach Beendigung dieser Vereinbarung

(1) Sämtliche personenbezogenen Daten sowie Datenträger und sonstige Materialien sind nach Beendigung dieser Vereinbarung dem Auftraggeber herauszugeben oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Dies gilt auch für Dokumentationen, die dem Nachweis der Auftragsverarbeitung dienen.

(2) Der Auftragnehmer verpflichtet sich, auch über die Beendigung dieser Vereinbarung hinaus die Vertraulichkeit zu wahren.

(3) Für den Fall der Beendigung der Vereinbarung zur Auftragsverarbeitung, gleich aus welchen Rechtsgründen, hat der Auftragnehmer die erforderlichen

Übergangsdienstleistungen für den Auftraggeber zu erbringen. Der Auftragnehmer ist verpflichtet, bei der Übermittlung der personenbezogenen Daten an einen anderen Auftragnehmer redlich und schnellstmöglich Unterstützung zu leisten oder die Daten an den Auftraggeber zurückzugeben.

§ 9
Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart. Ein Anspruch auf eine darüber hinaus gehende Vergütung aus dieser Vereinbarung besteht nicht.

§ 10
Haftung und Schadenersatz

Die Vertragspartner haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

§ 11
Schlussbestimmungen

(1) Für den Fall, dass die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.

(2) Der Auftragnehmer verpflichtet sich, in diesem Zusammenhang alle Verantwortlichen unverzüglich darüber zu informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DS-GVO liegen.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform, wobei auch die elektronische Form zulässig ist. Mündliche Nebenabreden bestehen nicht.

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

Ort, Datum	Ort, Datum
OOWV (Unterschrift 1)	Auftragnehmer
OOWV (Unterschrift 2)	Auftragnehmer

Anlage 1

1. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z. B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (z. B. von Auskunfteien, oder aus öffentlichen Verzeichnissen)

2. Kategorien betroffener Person

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Beschäftigte
- ☒ Kunden
- ☒ Interessenten
- ☐ Lieferanten
- ☒ Marktplatzpartner

3. Weisungsberechtigte Personen des Auftraggebers

Jacek Zielinski, zielinski@oowv.de

Jens Wittkopf, wittkopf@niedersachen-wasser.de

4. Weisungsempfangsberechtigte Personen des Auftragnehmers

Hier ggf. Personen benennen oder Passage streichen.

Anlage 2

Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

[Hier sind alle Unternehmen mit Namen, Rechtsform, Kontaktdaten und ladungsfähiger Anschrift vom Auftragnehmer anzugeben. Ferner ist die Art der Leistung kurz zu beschreiben.]

Anlage 3

Technische und organisatorische Maßnahmen

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

A. Zutrittskontrolle

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

	Maßnahme	Beschreibung
☐	Absicherung von Gebäudeschächten	
☒	Alarmanlage/Einbruchmeldesystem	
☐	Automatisches Zugangskontrollsystem	
☒	Begleitung von Besuchern und Fremdpersonal	
☒	Besucherbuch/Protokollierung der Besucher	
☐	Biometrische Zugangskontrollen	
☐	Chipkarten-/Transponder-Schließsystem	
☐	Drehkreuz mit Chipkarte	
☐	Einfriedung des Geländes	
☒	Festlegung von Sicherheitsbereichen	
☒	Festlegung zutrittsberechtigter Personen	
☐	Lichtschranken/Bewegungsmelder	
☐	Manuelles Schließsystem	
☒	Personenkontrolle beim Pförtner/Empfang	
☒	Regelungen für firmenfremdes Wartungspersonal vor Ort	
☒	Regelungen für Reinigungskräfte (-firmen)	
☐	Schließsystem mit Codesperre	
☒	Schlüsselregelung/Schlüsselbuch	
☒	Sicherheitsschlösser	
☐	Sorgfältige Auswahl von Sicherheitspersonal	
☐	Tragepflicht von Mitarbeiter-/Gästeausweisen	
☐	Vereinzelungsanlage	
☐	Videoüberwachung der Zugänge	
☐		
☐		

B. Zugangskontrolle

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

	Maßnahme	Bemerkung
☒	Anweisung zur manuellen Zugangssperre bei vorübergehendem Verlassen des Arbeitsplatzes	
☒	Authentifikation mit Benutzername + Passwort	
☐	Authentifikation mit biometrischen Daten	
☐	Authentifikation mit Chipkarte/Zertifikaten und PIN	
☒	Automatische Abmeldevorgänge	
☐	Automatische Zugangssperre durch kennwortgeschützte Bildschirmschoner	
☒	Einsatz von Löschsoftware	
☐	Einsatz von Mobile Device Management	
☒	Einsatz von VPN-Technologie	
☐	Gehäuseverriegelungen	
☐	Gesicherte Übertragung von Authentisierungsgeheimnissen (z. B. Verschlüsselung der Übertragungsstrecke)	
☒	Kontensperrung nach mehrmaliger Falscheingabe des Passworts	
☒	Passwortvergabe/Passwortregeln (gemäß akt. Empfehlungen des BSI)	
☒	Protokollierung des Zugangs	
☒	Prozess zur Rücksetzung gesperrter Zugangskennungen	
☐	Regelungen beim Ausscheiden von Mitarbeitern	
☐	Single Sign-On	
☐	Sperren der Bootkonfiguration (BIOS, UEFI)	
☒	Sperrung bei Fehlversuchen/Inaktivität	
☒	Sperrung externer Schnittstellen (z. B. USB-Anschlüsse)	
☐	Verbot Speicherfunktion für Passwörter und/oder Formulareingaben	
☒	Verschlüsselung von Datenträgern	

	Maßnahme	Bemerkung
☐	Verschlüsselung von Smartphones	
☐	Verwendung von Benutzerprofilen	
☒	Vorliegen eines Firewallkonzeptes	
☒	Vorliegen eines Virenschutzkonzeptes	
☒	Zugangsberechtigungen verwalten (Prinzip der minimalen Berechtigung)	
☐		
☐		

C. Zugriffskontrolle

Gewährleistung, dass die zum Datenverarbeitungssystem Zugangsberechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

	Maßnahme	Bemerkung
☒	Anzahl der Administratoren auf das „Notwendigste“ reduzieren	
☒	Berechtigungen verknüpft mit Rollen	
☒	Berechtigungskonzept („Need-to-know-Prinzip“)	
☐	Einsatz von Aktenvernichtern	
☐	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (mit Zertifikat)	
☐	Fernlöschung von mobilen Endgeräten	
☐	Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)	
☐	Physische Löschung von Datenträgern vor deren Wiederverwendung	
☐	Protokollierung der Vernichtung von Daten	
☒	Protokollierung von Zugriffen auf Anwendungen	
☒	Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen	
☐	Sichere Aufbewahrung von Datenträgern	
☐	Sperrung der Nutzung von persönlichem Cloud-Speicher am Arbeitsplatz-PC	
☒	Verschlüsselung von Datenträgern	
☒	Verwaltung der Benutzerrechte durch Systemadministratoren	
☐		
☐		

D. Trennungskontrolle

Gewährleistung der getrennten Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

	Maßnahme	Bemerkung
☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	
☐	Festlegung von Datenbankrechten	
☐	Logische Mandantentrennung (softwareseitig)	
☐	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	
☒	Sparsamkeit der Datenerhebung	
☐	Trennung von Produktiv- und Testsystemen	
☐	Versehen der Datensätze mit Zweckattributen/Datenfeldern	
☐		
☐		

E. Pseudonymisierung

Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

	Maßnahme	Bemerkung
☒	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren	
☐	Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	
☐		
☐		

II. Integrität (Art. 32 Abs.1 lit. b) DS-GVO)

A. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten bei elektronischer Übertragung oder Transport.

	Maßnahme	Bemerkung
☐	Automatisierte Löschung temporärer Zwischenspeicher	
☒	Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste	
☒	Datenschutzgerechte Lösch- und Zerstörungsverfahren	
☒	Dedizierte Netze für Systeme mit sensiblen Daten	
☐	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	
☐	E-Mail-Verschlüsselung	
☐	Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen	
☐	Festlegung empfangs- und weitergabeberechtigter Instanzen/Personen	
☒	Führung von Löschprotokollen	
☐	Härtung der Backendsysteme	
☐	Implementation von Sicherheitsgateways an den Netzübergabepunkten	
☒	Prozess zur sicheren Sammlung und Entsorgung von Datenträgern (Entsorgungskonzept)	
☐	Prüfung der Rechtmäßigkeit der Übermittlung ins Drittland	
☐	Qualifizierte Datenträgerverwaltung	
☐	Risikominimierung durch Netzseparierung	
☒	Sichere Datenübertragung zwischen Server und Client	
☐	Sichere Transportbehälter/-verpackungen	
☐	Signieren elektronischer Dokumente	
☐	Sorgfältige Auswahl von Transportpersonal und -fahrzeugen	
☐	Sperren externer Schnittstellen wie USB	
☒	Überwachung von Fernwartungsaktivitäten	
☐	Verschlüsselte Dateisysteme	
☐	Verschlüsselte Datenbanken	
☐	Verschlüsselte Speicherung auf mobilen Datenträgern	
☐	Verschlüsselung in der Applikation	
☒	Verwendung von VPN-Tunneln	
☒	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form	
☐		
☐		

B. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

	Maßnahme	Bemerkung
☐	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind	
☒	Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können	
☒	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	
☒	Protokollierung der Eingabe, Änderung und Löschung von Daten	
☐		
☐		

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO); Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DS-GVO)

A. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung bzw. Verluste geschützt sind.

	Maßnahme	Bemerkung
☒	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	
☒	Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort	
☐	Automatisches Benachrichtigungssystem bei Erreichung der max. Auslastung	
☒	Backup- & Recoverykonzept	
☐	Feuer- und Rauchmeldeanlagen	
☐	Feuerlöschgeräte in Serverräumen	
☐	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	
☐	In Hochwassergebieten: Serverräume über der Wassergrenze	
☐	Klimaanlage in Serverräumen	
☐	Lastausgleich (load balancing) der Dienste	
☐	Lastausgleich (load balancing) der Netzwerkkomponenten	
☐	Lastausgleich (load balancing) der Server	
☒	Notfallplan	

☐	Schutzsteckdosenleisten in Serverräumen	
☐	Serverräume nicht unter sanitären Anlagen	
☐	Spiegelung von Festplatten (z. B. RAID-Verfahren)	
☐	Testen einer raschen Datenwiederherstellung	
☐	Überspannungsschutz	
☐	Unterbrechungsfreie Stromversorgung (USV)	
☐		
☐		

IV. Organisationskontrolle, Rechenschaftspflicht und Wirksamkeitsnachweis (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 DS-GVO)

A. Datenschutzmanagement

	Maßnahme	Bemerkung
☐	Beachtung von Datenschutz durch Technikgestaltung	
☒	Bestellung eines Datenschutzbeauftragten	
☒	Bestellung eines Informationssicherheitsbeauftragten (ISB)	
☐	Datenschutzleitlinie veröffentlicht	
☒	Die Organisation kommt den Informationspflichten nach Art. 13/14 DS-GVO nach	
☒	Dokumentation/Inventarisierung der eingesetzten IT-Systeme	
☒	Dokumentation über eingesetzte Programme und Anwendungen	
☒	Durchführung interner Datenschutzaudits	
☒	Formalisierter Prozess zur Bearbeitung von Betroffenenanfragen implementiert	
☒	Führung des Verzeichnisses für Auftragsverarbeiter nach Art. 30 Abs. 2 DS-GVO	
☐	Funktionstrennung zwischen operativen und kontrollierenden Funktionen	
☒	IT-Sicherheits-Zertifizierung (z. B. ISO 27001, ISIS12)	
☐	Mind. jährliche Prüfung der technischen Schutzmaßnahmen	
☒	Nachweisbare Durchführung von Datenschutzschulungen	
☒	Protokollierung aller Administratorenaktivitäten	
☐	Protokollierung der Datenträgervernichtung	
☐	Softwarelösung für Datenschutzmanagement	
☐	Strukturierte Auftragskontrolle	
☐	Umsetzung datenschutzfreundlicher Voreinstellungen	
☒	Verpflichtung der Beschäftigten auf die Vertraulichkeit	

☒	Zentrale Dokumentation aller Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Beschäftigte nach Bedarf/Berechtigung	
☐	Schutzstufenkonzept	

B. Incident-Response-Management

	Maßnahme	Bemerkung
☒	Dokumentierter Prozess zur Erkennung und Meldung von Datenschutzvorfällen	
☒	Einbindung von Datenschutzbeauftragtem und Informationssicherheitsbeauftragtem bei Sicherheits- und Datenschutzvorfällen	
☒	Formaler Prozess zur Nachbearbeitung von Sicherheits- und Datenschutzvorfällen	
☐	Intrusion Detection System (IDS)	
☐	Intrusion Prevention System (IPS)	
☐		
☐		