Anlage [2] zum Vertrag [75-2026-001]

Vereinbarung zum Datenschutz gemäß Art. 28 DSGVO

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,

.....

- Verantwortlicher -

und dem/der

[gleiche Angaben, wie im Hauptvertrag zu Auftragnehmer]

.....

- Auftragsverarbeiter -

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragsverarbeiter verarbeitet dabei personenbezogene Daten für den Verantwortlichen im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieser Vereinbarung.

(2) Der Auftrag umfasst die sich aus dem Vertrag 75-2050-005, dem dieser Anhang zugeordnet ist (nachfolgend „Vertrag“), ergebenden Leistungen.

(3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen

(1) Zweck der Verarbeitung sind
Rahmenvereinbarung zur Betriebsunterstützung, Anpassungs- und Weiterentwicklung für gewässer- und abwasserbezogene IT-Fachverfahren in der Wasserwirtschaftsverwaltung RLP

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

☒ Personenstammdaten
☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☐ Vertragsabrechnungs- und Zahlungsdaten
☐ Planungs- und Steuerungsdaten
☒ Fachdaten
☐ _____

(3) Dabei werden die unter (2) genannten Daten in folgenden Kategorien betroffener Personen verarbeitet:

☐ Bürgerinnen und Bürger
☒ Beschäftige
☐ Interessenten
☒ Beschäftigte (eingeschlossen Inhaber) bei aufzusuchenden Unternehmen

☐ Lieferanten

☒ Ansprechpartner

☐ _____

§ 3 Pflichten und Rechte des Verantwortlichen

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der Betroffenen nach den Art. 12 bis 22 DSGVO ist allein der Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Der Verantwortliche erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.

(3) Der Verantwortliche hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind schriftlich zu bestätigen. Die weisungsberechtigten Personen des Verantwortlichen und die Weisungsempfänger beim Auftragsverarbeiter werden in der Anhang 1 mit Name, Organisationseinheit und Kontaktdaten benannt.

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen und insoweit die Anhang 1 entsprechend zu aktualisieren.

Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse, die personenbezogene Daten betreffen, feststellt.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, es sei denn, es liegt ein Anwendungsfall von Art. 28 Abs. 3 lit. a DSGVO vor.

Er verwendet die zur Datenverarbeitung überlassenen personenbezogenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

Er beachtet die Bestimmungen der DSGVO und des Landesdatenschutzgesetzes Rheinland-Pfalz (LDSG) und unterwirft sich hinsichtlich der in dem Vertrag vereinbarten Leistungen der Kontrolle des Landesbeauftragten für den Datenschutz.

Ein Auftragsverarbeiter, der unter Verstoß gegen die DSGVO die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

(2) Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen sowie die strikte Trennung der Daten des Verantwortlichen von sonstigen Datenbeständen des Auftragsverarbeiters zu.

Die Datenträger, die vom Verantwortlichen stammen bzw. für den Verantwortlichen genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

(3) Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in das Verzeichnis von Verarbeitungstätigkeiten, die

gespeicherten Daten und die Datenverarbeitungs-programme einschließlich einer Inspektion beim Auftragsverarbeiter.

(4) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgenabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

(5) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine vom Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Behördenleitung beim Verantwortlichen nach Überprüfung bestätigt oder geändert wird.

(6) Der Auftragsverarbeiter hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen.

(7) Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung des Verantwortlichen im Einzelfall gestattet. Die Maßnahmen nach Art. 32 DSGVO sind sicherzustellen und der Zutritt zur Wohnung des Beschäftigten zu Kontrollzwecken vertraglich zu vereinbaren.

(8) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Verantwortlichen datenschutzgerecht vernichtet werden.

(9) Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen.

Seitens des Verantwortlichen elektronisch zur Verfügung gestellte Informationen sowie etwaige Testdaten sind nach erklärter Abnahme der Leistung zu löschen. Die Löschung erfolgt derart, dass eine Reproduktion nach dem Stand der Technik nicht möglich ist. Die Löschung bzw. Vernichtung ist dem Verantwortlichen schriftlich zu bestätigen.

(10) Die Beauftragung von weiteren Auftragsverarbeitern ist ausgeschlossen.

(11) Der Verantwortliche ist über wesentliche Veränderungen, die die Art der Datenverarbeitung betreffen, rechtzeitig zu unterrichten.

Für den Datenschutz oder die Informationssicherheit erhebliche Entscheidungen zur Organisation und Durchführung der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

§ 5 Datengeheimnis

(1) Der Auftragsverarbeiter verpflichtet sich zusätzlich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten für den Verantwortlichen das Datengeheimnis gemäß § 8 LDSG (neu) zu wahren. Er verpflichtet sich weiter, über Informationen, die ihm im Rahmen des Auftrags zur Kenntnis gelangen, gegenüber Dritten Verschwiegenheit zu wahren. Die Verschwiegenheitspflicht besteht auch nach Erfüllung des Auftrags weiter fort.

(2) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgeblichen Bestimmungen des

Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Wiese zur Verschwiegenheit verpflichtet (Art. 28 Absatz 3 Satz 2 lit. b, Art. 29 DSGVO). Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

§ 6 Kontrollrechte des Landesbeauftragten für den Datenschutz

(1) Der Auftragsverarbeiter verpflichtet sich, dem Landesbeauftragten für den Datenschutz und den von ihm eingesetzten Bediensteten Zugang zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe der DSGVO bzw. des LDSG in seiner jeweiligen Fassung.

(2) Soweit Daten in einer Privatwohnung verarbeitet werden, ist der Zugang des Landesbeauftragten für den Datenschutz und der von ihm eingesetzten Bediensteten vorher mit dem Auftragsverarbeiter abzustimmen.

§ 7 Datensicherungsmaßnahmen

(1) Der Auftragsverarbeiter verpflichtet sich, die nach Art. 32 DSGVO erforderlichen technisch-organisatorischen Maßnahmen zu treffen und in einem Sicherheitskonzept zu dokumentieren. Das Sicherheitskonzept ist auf Anforderung dem Verantwortlichen zur Verfügung zu stellen. Ist eine Zurverfügungstellung des Sicherheitskonzeptes, insbesondere aus Gründen der Informationssicherheit oder der Geheimhaltung ganz oder teilweise nicht möglich, so stellt der Auftragsverarbeiter dem Verantwortlichen die relevanten Auszüge aus dem Sicherheitskonzept zur Einsichtnahme beim Auftragsverarbeiter zur Verfügung.

Das in Anhang 2 beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

Das ebenfalls in Anhang 2 beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt.

(2) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses im Hinblick auf ihre Wirksamkeit regelmäßig, mindestens aber jährlich, zu überprüfen, zu bewerten und zu evaluieren (Art. 32 Abs. 1 lit. d DSGVO).

Änderungen dürfen die vereinbarten Sicherheitsstandards nicht unterschreiten.

Wesentliche Änderungen sind schriftlich zu vereinbaren. Solche Abstimmungen sind für die Dauer dieser Vereinbarung aufzubewahren.

(4) Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen nach Art. 33 und Art. 34 DS-GVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung durchführen.

§ 8 Vereinbarungsdauer

(1) Diese Vereinbarung

beginnt am [XX.XX.XXXX] und endet am [XX.XX.XXXX]

(2) Der Verantwortliche kann die Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen die Bestimmungen der DSGVO und anderer Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer möglichen Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO meldet der Auftragsverarbeiter dies unverzüglich, damit der Verantwortliche in die Lage versetzt wird, die Meldefrist von 72 Stunden gegenüber der zuständigen Aufsichtsbehörde einzuhalten.

§ 10 Haftung

(1) Der Auftragsverarbeiter haftet dem Verantwortlichen für Schäden, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die eine betroffene Person wegen einer nach der DSGVO oder dem LDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Verantwortliche oder der Auftragsverarbeiter gegenüber der betroffenen Person verantwortlich.
Der Auftragsverarbeiter haftet nur dann, wenn er den ihm auferlegten Pflichten nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

§ 11 Vertragsstrafe

Bei einem Verstoß des Auftragsverarbeiters gegen die Pflichten aus dieser Vereinbarung, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von 5.000 € vereinbart.

§ 12 Sonstiges

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.

(3) Änderungen oder Ergänzungen zu dieser Vereinbarung sind nur wirksam, wenn sie schriftlich vereinbart werden. Dies gilt auch für eine Änderung dieser Schriftformklausel. Satz 1 gilt nicht für Anpassungen bezüglich der weisungsberechtigten Personen sowie Weisungsempfänger (Anhang 1).

(4) Nebenabreden wurden nicht vereinbart.

(5) Sollte die EU-Kommission oder die zuständige Aufsichtsbehörde gemäß Art. 28 Abs. 7 und 8 DSGVO Standardvertragsklauseln für Verträge zur Auftragsverarbeitung entwickeln, werden sich die Parteien auf eine mögliche Anpassung oder Ersetzung der Vereinbarung verständigen.

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

§ 13 Wirksamkeit der Vereinbarung

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

Für den Verantwortlichen:

_____, _____

.....

(Unterschrift und Dienstsiegel)

Für den Auftragsverarbeiter:

_____, _____

.....

(Unterschrift)

Anhänge:

1. Weisungsberechtigte Person und Weisungsempfänger sowie ggf. Subunternehmer
2. Übersicht der technisch-organisatorischen Maßnahmen

ANHANG 1

zu Anlage [2] zum Vertrag [75-2026-001]

Übersicht von Verarbeitungstätigkeiten **Auftragsverarbeiter gem. Artikel 30 Abs. 2 DSGVO**
Angaben zum Auftragsverarbeiter Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc. Firmengruppe ☐ ja ☐ nein Name Straße Postleitzahl Ort Telefon E-Mail-Adresse Internet-Adresse
Angaben zu ggf. einem weiteren gemeinsamen Auftragsverarbeiter Name Straße Postleitzahl Ort Telefon E-Mail-Adresse

Angaben zum Vertreter des Auftragsverarbeiters

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten* des Auftragsverarbeiters
(extern mit Anschrift) * sofern gem. Artikel 37 DSGVO benannt

Anrede Titel
Name, Vorname
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse

Angaben zum jeweiligen Auftraggeber	**lfd. Nr.:** _____
Unternehmen (Auftraggeber) (Art. 30 Abs. 2 lit. a)	Name Landesamt für Umwelt Rheinland-Pfalz Straße Kaiser-Friedrich-Straße 7 Postleitzahl 55116 Ort Mainz Telefon 06131 6033-0 E-Mail poststelle@lfu.rlp.de
Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden (Art. 30 Abs. 2 lit. b) (mit Erläuterung der jeweiligen Verarbeitung)	☐ Datensicherung/Archivierung ☐ Cloud-Services ☒ (Weiter-)Entwicklung von Fachanwendungen ☐ Hosting von Fachanwendungen ☒ Betriebsunterstützung von Fachanwendungen ☐ Beratung/(Weiter-)Entwicklung einer IT-Infrastruktur ☐ Hosting einer IT-Infrastruktur ☐ Betriebsunterstützung von IT-Infrastruktur ☐ 2te Level Support ☐ Lohn- und Gehaltsabrechnung ☐ Personalverwaltung ☐ Zeiterfassung ☐ Reisekosten ☐ Aktenvernichtung ☐Sonstige

ggfs. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 2 lit. c)	☒ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name):
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DSGVO genannte Datenübermittlung handelt.	☐ Dokumentation geeigneter Garantien:
Subunternehmer	☐ Name:

Für den Auftragsverarbeiter:

_____, _____

.....

(Unterschrift)

ANHANG 2

zu Anlage [2] zum Vertrag [75-2026-001]

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO

Diese Anlage stellt die Auswahl der technischen und organisatorischen Maßnahmen dar, die passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer gefordert sind.

Abweichungen, Änderungen und Ergänzungen nach Abschluss dieser Vereinbarung werden dem Verantwortlichen noch vor Aufnahme der veränderten Umgebung der Verarbeitung von personen-bezogenen Daten vom Auftragsverarbeiter kommuniziert und auf erste Anforderung dem Verantwortlichen detailliert zur Verfügung gestellt.

Der Auftragverarbeiter bestätigt, dass er Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen hat bzw. vor Auftragsverarbeitung ergreifen wird (Art. 32 DSGVO und § 64 BDSG (neu)).

1. Gewährleistung der Vertraulichkeit

a) Zutrittskontrolle

(kein unbefugter Zutritt zu Datenverarbeitungsanlagen)

- ☐ Magnet- und Chipkarten
- ☐ Automatisches Zugangskontrollsystem
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Empfang / Protokollierung der Benutzer
- ☒ Alarmanlagen / Videoüberwachung der Zugänge
- ☐ Sonstige:

b) Zugangskontrolle

(keine unbefugte Systembenutzung)

- ☒ Authentifikation der Nutzer durch (sichere) Kennwörter aufgrund einer Passwortrichtlinie
- ☒ Einsatz von Sperrmechanismen
- ☐ Zwei-Faktor-Authentifizierung
- ☒ Verschlüsselung von Datenträgern
- ☒ Einsatz von Anti-Viren-Software und Firewalls
- ☐ Sonstige:

c) Zugriffskontrolle

(kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems bzw. der Anwendung)

- ☐ Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
- ☒ Festlegungen von Datenbankrechten
- ☒ Protokollierung von Zugriffen
- ☒ Verwaltung von Benutzerberechtigungen (durch Systemadministratoren)
- ☒ Begrenzung der Anzahl der Administratoren auf das Notwendigste
- ☒ Protokollierung der Vernichtung von Daten
- ☐ Einsatz von zertifizierten Dienstleistern zur Aktenvernichtung
- ☒ Vernichtung von Datenträgern (DIN 32757)
- ☐ Sonstige:

d) Trennungskontrolle

(getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)

- ☐ Mandantenfähigkeit
- ☒ Festlegung von Datenbankrechten
- ☒ Sandboxing
- ☒ Trennung von Produktiv- und Testsystem
- ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Sonstige:

e) Pseudonymisierung personenbezogener Daten

(Schutz vor einfacher Zuordnung personenbezogener Daten nach Löschung)

- ☒ Trennung von Kundenstammdaten und Kundenumsatzdaten
- ☐ Schwärzung von Dokumenten (Anonymisieren)
- ☐ Codierung der Namen (bei Löschung)
- ☐ Verwendung von Personal-, Kunden-, Lieferanten-Kennziffern statt Namen
- ☐ Sonstige:

f) Konkretisierung/Ergänzung

2. Gewährleistung von Integrität

a) Wiedergabekontrolle

(kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

☐ Verschlüsselung von E-Mails

☐ Symmetrische Verschlüsselung der Daten

☒ Asymmetrische Verschlüsselung der Daten

☐ Hashing

☒ Virtual Private Networks (VPN)

☐ Elektronische Signatur

☐ Weitergabe von Daten in anonymisierter Form

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der planten Überlassung bzw. vereinbarten Löschfristen

☐ Sonstige:

b) Eingabekontrolle

(Festlegung, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind)

☐ Vergabe von Rechten zur Eingabe

☐ Änderung und Lösung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Protokollierung/ Nachvollziehbarkeit von Eingabe

☐ Dokumentenmanagement

☒ Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

☐ Sonstige:

c) Konkretisierung/Ergänzung

3. Gewährleistung der Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

(Schutz vor zufälliger Zerstörung oder Verlust)

☒ Backup-Strategie (online/offline; on-site/off-site)
☒ Unterbrechungsfreie Stromversorgung
☒ Virenschutz
☒ Firewall
☐ Meldewege und Notfallpläne
☐ Feuerlöschgeräte sowie Klimaanlage im Serverraum
☐ Redundante unterbrechungsfreie Stromversorgung (NEA, USV, Diesel)
☐ Sonstige:

b) Auftragskontrolle

(Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers)

☒ Eindeutige Vertragsgestaltung
☐ Formalisiertes Auftragsmanagement
☐ Strenge Auswahl des Dienstleisters (Subunternehmens)
☐ Vorabüberzeugungspflicht
☐ Nachkontrollen
☐ Sonstige:

c) Belastbarkeit der Systeme und Dienste / rasche Wiederherstellbarkeit nach einem physischen oder technischen Zwischenfall

☐ Ausstattung (z. B. Speicher-, Zugriffs-, Leitungskapazitäten etc.) ausgelegt auch an punktuelle hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen
☐ Erstellen eines Notfallplanes
☒ Erstellen eines Backup- & Recoverykonzepts (dokumentiert im Betriebshandbuch)
☐ Redundante Datenspeicherung
☐ Doppelte IT-Infrastruktur
☐ Schatten-Rechenzentrum
☒ Datensicherung in Form von Tages-, Wochen- und Monatssicherungen
☐ Einbindung in eine zentrale Backupumgebung
☒ Automatische und standardisierte Werkzeuge für Datensicherung und Wiederherstellung
☐ Sonstige:

d) Konkretisierung/Ergänzung

4. Gewährleistung der Wirksamkeit der gewählten Maßnahmen

(Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung)

- ☐ Datenschutz-Management
- ☐ Prüfung des DSB, der IT-Revision
- ☐ Externe Prüfungen, Audits, Zeritifzierungen
- ☐ Incident-Response-Management
- ☒ Verfahren zur Meldung von Störungen und Verstößen
- ☐ Datenschutzfreundliche Voreinstellungen
- ☐ Zugang zum einem Computer Emergency Response Team (CERT)
- ☐ Richtlinien für standardisierte Voreinstellungen
- ☐ Auftragskontrolle
- ☐ Sonstige:

d) Konkretisierung/Ergänzung

5. Es liegen folgende Dokumentationen zu sonstigen Maßnahmen vor

a) Datenschutzschulungen, Zertifikate etc.

b) Allgemeine Konkretisierung/Ergänzung

6. Durch folgende Maßnahmen wird eine Bewertung und Evaluierung der Wirksamkeit der o.g. Maßnahmen sichergestellt

Für den Auftragsverarbeiter:

_____, _____

.....

(Unterschrift)