Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO zur Verarbeitung personenbezogener Daten* im Auftrag

zwischen

Südwestrundfunk, Anstalt des öffentlichen Rechts, Stuttgart,
vertreten durch den Intendanten

– nachstehend **Auftraggeber** genannt –

und

[AUFTRAGNEHMER
Name, Anschrift]

– nachstehend **Auftragsverarbeiter** genannt –

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand:

☒ Der Gegenstand des Auftrags ergibt sich aus den Vertragsunterlagen (Leistungsblatt) vom **17.04.2024**, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

☒ Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter: **Digitalisierung von Dokumenten für die Abteilung „Lizenzen und Rechtemanagement (LuR)“ für die HA IDA**

(2) Dauer:

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

☐ Die Dauer dieses Auftrags ist unbefristet. Eine Kündigung ist mit einer Frist von drei Monaten zum Quartalsende möglich, sofern davon in der Leistungsvereinbarung nicht abgewichen wird. Die Kündigung bedarf der Schriftform.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragsverarbeiter eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragsverarbeiter den Zutritt des Auftraggebers oder der Aufsichtsbehörde vertragswidrig verweigert.

* alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, Art. 4 Ziff. 1 DSGVO

§ 2 Konkretisierung des Auftragsinhalts

(1) Art der Daten:

☐ Die Art der zu verarbeitenden personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

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

- ☒ Personaldaten/Stammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Log-Dateien
- ☐ personenbezogene Planungs- und Steuerungsdaten
- ☒ personenbezogene Vertragsdaten
- ☒ personenbezogene Abrechnungs- und Zahlungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☒ Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO, z. B. Gesundheitsdaten, Religion, Gewerkschaftszugehörigkeit)
- ☐ Altersversorgungsinformationen (Rente, Beihilfe, etc.)

(2) Betroffene Personen:

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Zuschauer/Zuhörer
- ☐ Nutzer Online-Angebote
- ☒ Beschäftigte
- ☒ Geschäftspartner
- ☐ Ansprechpartner
- ☐ Beitragszahler/potentielle Beitragszahler
- ☐ Besucher
- ☐ ...

(3) Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten:

☒ Der Zweck der Verarbeitung personenbezogener Daten durch den Auftrag für den Auftraggeber ist konkret beschrieben in der Leistungsvereinbarung (Leistungsblatt) vom **[17.04.2024].**

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf den Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter:

(4) Ort der Datenverarbeitung

☒ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Übermittlung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind.

☐ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet **nicht** oder nicht ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, sondern in einem Drittland statt. Der Auftraggeber erteilt hierzu seine Zustimmung.

Das angemessene Schutzniveau in …… (Drittland)

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO) einschließlich ggf. erforderlicher weiterer Garantien;

☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DSGVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO);

☐ wird hergestellt durch sonstige Maßnahmen: …… (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO)

§ 3 Verantwortlichkeit

(1) Die Auftragsverarbeitung richtet sich nach Artikel 28 DS-GVO. Der Auftraggeber ist als Verantwortlicher für die Einhaltung der anzuwendenden Datenschutzvorschriften im Hinblick auf die Verarbeitung seiner Daten verantwortlich. Er hat insbesondere zu prüfen, ob die Datenverarbeitung zulässig ist.

(2) Macht eine betroffene Person datenschutzrechtliche Ansprüche (z.B. auf Auskunft) geltend, so unterstützt der Auftragsverarbeiter den Auftraggeber bei der Erfüllung dieser Pflichten. Der Auftragsverarbeiter trifft für diese Unterstützung technische und organisatorische Maßnahmen nach dem Stand der Technik. Welche Tätigkeiten der Auftragsverarbeiter im Rahmen der Unterstützung auszuführen hat, bestimmt sich im jeweiligen Einzelfall.

(3) Der Auftraggeber hat als Verantwortlicher die Pflichten aus Art. 32 – 36 DSGVO zu erfüllen. Der Auftragsverarbeiter unterstützt ihn bei der Erfüllung dieser Pflichten und zwar

auch gegenüber den Aufsichtsbehörden. Der Auftragsverarbeiter trifft auch für diese Unterstützung die erforderlichen technischen und organisatorischen Maßnahmen nach dem Stand der Technik.

§ 4 Weisungsbefugnis

(1) Der Auftragsverarbeiter darf die Daten nur im Rahmen dieses Auftrags und nach den Weisungen des Auftraggebers verarbeiten. Eine Verarbeitung für andere Zwecke – worunter insbesondere eigene Zwecke des Auftragsverarbeiters fallen – ist nicht zulässig.

(2) Der Auftraggeber entscheidet allein und ausschließlich über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten.

(3) Weisungen können generell oder im Einzelfall erteilt werden. Sie sind schriftlich zu erteilen, was auch in elektronischer Form erfolgen kann. Für mündlich erteilte Weisungen ist unverzüglich die Schriftform nachzuholen.

Weisungen können von folgenden Personen erteilt werden:

- Florian Schad, Datenschutzbeauftragter
- Imke Schacht, Hauptabteilung Information, Dokumentation und Archive
- Tobias Fasora, Hauptabteilung Information, Dokumentation und Archive
- Katharina Stephan, Hauptabteilung Information, Dokumentation und Archive

(4) Der Auftragsverarbeiter hat den Auftraggeber zu unterrichten, wenn eine Weisung nicht unverzüglich durchgeführt werden kann. Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, so informiert er unverzüglich den Verantwortlichen.

(5) ☒ Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) **findet nicht statt**. Sollte sich dies während der Vertragslaufzeit ändern, bedarf es der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann

☐ Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) ist zulässig. Die Einhaltung der Schutzmaßnahmen wird durch angemessene technische und organisatorische Maßnahmen für die Verarbeitungssituation sichergestellt und nachgewiesen.

§ 5 Technisch-organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragsverarbeiter ist verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung zu überwachen. Er versichert, dass er die Regelungen der Art. 25 und Art. 32 DSGVO einhält, beachtet und dokumentiert. Wesentliche Änderungen sind dem Auftraggeber mitzuteilen. Die verwendeten Daten werden von sonstigen Datenbeständen getrennt.

(2) Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen und ein entsprechendes Sicherheitskonzept inklusive einer Auflistung der umgesetzten technisch-organisatorischen Maßnahmen vorzulegen (Beispiele von möglichen Maßnahmen siehe Anlage). Die zu treffenden Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten siehe Anlage).

☒ Der Auftragsverarbeiter hat sich hierzu wie folgt zertifizieren lassen (Nennung der Zertifikate mit Nennung und Gültigkeitsdauer):

☒ Die Datenverarbeitung durch den Auftragsverarbeiter findet zusätzlich oder ausschließlich auf dem Gelände und in den Räumen des Auftraggebers statt. Der Auftragsverarbeiter hat Zugang zu personenbezogenen Daten alleine durch den für die Auftragsdurchführung/Leistungserbringung notwendigen Zugriff auf Systeme auf dem Gelände und in den Räumen des Auftraggebers. In diesem Fall gewährleistet der Auftraggeber die Sicherheit im Hinblick auf seine IT-Systeme gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO.

☐ Für den Fall, dass der Auftragsverarbeiter mittels eines Fernzugriffs (z.B. Fern-wartung/Remotezugriff) auf die Systeme des Auftraggebers zugreift, gewährleistet er die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO für seinen Verantwortungsbereich, insbesondere die Datenverarbeitung und IT-Sicherheit am Ort des Fernzugriffs (Einzelheiten siehe Anlage).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind mit dem Auftraggeber abzustimmen und zu dokumentieren.

(4) Der Auftragsverarbeiter wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig sowie anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragsverarbeiter den Auftraggeber in Kenntnis setzen.

§ 6 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragsverarbeiter sicherzustellen.

(3) Wird festgestellt, dass Daten unrichtig sind, hat der Auftragsverarbeiter den Auftraggeber hierüber zu informieren und nach dessen Weisung unverzüglich zu berichtigen. Daten, für welche die Voraussetzungen des Art. 18 DS-GVO vorliegen, dürfen nur entsprechend eingeschränkt verarbeitet werden.

(4) Anfallendes Test- und Ausschussmaterial wird vom Auftragsverarbeiter unter Verschluss gehalten, bis es entweder vom Auftragsverarbeiter datenschutzgerecht gelöscht bzw. vernichtet oder dem Auftraggeber übergeben wird. Löschungen sind mit Protokollen zu dokumentieren und dem Auftraggeber auf Verlangen zur Verfügung zu stellen. Es muss eine rückinformationssichere Vernichtung gemäß DIN 66399 gewährleistet sein, ein Transport in verschlossenen Behältern vorgenommen werden und eine protokollierte und dokumentierte physische Vernichtung erfolgen (siehe auch unter § 14 dieses Vertrages).

§ 7 Vertraulichkeit

(1) Der Auftragsverarbeiter verpflichtet sich, die ihm vom Auftraggeber zur Verfügung gestellten Unterlagen und Daten sowie die Arbeitsergebnisse vertraulich zu behandeln, insbesondere Unbefugten nicht zugänglich zu machen und dem Auftraggeber hierzu jederzeit Auskunft zu geben.

(2) Der Auftragsverarbeiter gewährleistet die Einhaltung der Vertraulichkeit. Er sichert zu, alle für ihn im Rahmen der Ausführung dieses Auftrags tätigen Personen auf die Vertraulichkeit zu verpflichten. Soweit Personen einer gesetzlichen Verschwiegenheitspflicht in Bezug auf diese Tätigkeit unterliegen und deshalb eine Verpflichtung auf Vertraulichkeit nicht erfolgen soll, ist der Verzicht auf die Vereinbarung auf die Vertraulichkeit nur zulässig, wenn diese gesetzliche Verschwiegenheitspflicht einen angemessenen Schutz bietet.

(3) Bei einer Kontrolle durch Stellen, die einem Informationsfreiheitsgesetz unterliegen, ist dafür Sorge zu tragen, dass Betriebs- und Geschäftsgeheimnisse des Auftraggebers gewahrt und wirtschaftliche Informationen geschützt werden.

(4) Diese Verpflichtungen bestehen auch nach Beendigung des Vertrages fort.

§ 8 Sonstige Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragsverarbeiter

[Name, Telefonnummer, E-Mail-Adresse, bei externen DSB zusätzlich Firma, Anschrift]

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) ☐ Der Auftragsverarbeiter ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner für Fragen zu Datenschutz und Informationssicherheit im Zusammenhang mit diesem Vertrag wird beim Auftragsverarbeiter Herr/Frau [*Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail*] benannt.

c) ☐ Da der Auftragsverarbeiter seinen Sitz außerhalb der Union hat, benennt er folgenden, auch schon im Rubrum dieses Vertrages benannten Vertreter nach Art. 27 Abs. 1 DSGVO in der Union: [*Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail*].

(2) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, 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 Auftragsverarbeiter ermittelt.

(3) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

§ 9 Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen (Art. 28 Abs. 2 DSGVO).

☐ Eine Unterbeauftragung ist unzulässig.

☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

☒ Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird, welche auch die zwischen Auftraggeber und Auftragsverarbeiter getroffenen Regelungen hinreichend berücksichtigt

(2) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(3) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Auf § 2 Abs. 4 wird insoweit verwiesen.

(4) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(5) Der Auftragsverarbeiter wird auf Verlangen dem Auftraggeber Kopien der Unteraufträge zur Verfügung stellen und alle erforderlichen Auskünfte erteilen.

§ 10 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb ohne zusätzliche Vergütung zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiter nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Es wird Bezug genommen auf § 5 dieses Vertrages.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

Die Nachweise der ergriffenen Maßnahmen stellt der Auftragsverarbeiter dem Auftraggeber zur Verfügung.

(4) Der Auftragsverarbeiter unterwirft sich auch der Kontrolle durch die für den Auftraggeber zuständige Aufsichtsbehörde, soweit Daten des Auftraggebers betroffen sind.

§ 11 Haftung und gegebenenfalls Vertragsstrafe

(1) Der Auftragsverarbeiter haftet für die ordnungsgemäße Ausführung des Auftrags nach den gesetzlichen Bestimmungen, insbesondere nach Art. 82 Abs. 2 EU-DS-GVO. Machen betroffene Personen Ansprüche gegenüber dem Verantwortlichen wegen unzulässiger oder unrichtiger Datenverarbeitung geltend, so hat der Auftragsverarbeiter den Verantwortlichen zu unterstützen und zu beweisen, dass die fehlerhafte Datenverarbeitung nicht in seinem eigenen Verantwortungsbereich liegt.

(2) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

(3) Der Auftragsverarbeiter haftet für Verschulden eines weiteren Auftragsverarbeiters bzw. Subunternehmers wie für eigenes Verschulden.
Der Auftragnehmer unterhält zur Abdeckung etwaiger Schäden eine Betriebs- und Produkthaftpflichtversicherung. Die Haftung des Auftragnehmers aus und im Zusammenhang mit der einfachen fahrlässigen Verletzung von Haupt- und/oder Nebenpflichten dieses Vertrages und seiner Anlagen ist - mit Ausnahme bei Vorsatz und grober Fahrlässigkeit, bei zugesicherten Eigenschaften, bei arglistigem Verhalten, aus Garantien, nach dem Produkthaftungsgesetz sowie bei der Verletzung von Leib, Leben und Gesundheit - für die Dauer des Bestandes der vorbezeichneten Versicherung der Höhe nach auf 10 Mio. Euro für Personen- und Sachschäden, 6 Mio. Euro für Produktvermögensschäden und 1 Mio. Euro für sonstige Vermögensschäden beschränkt.
Die Haftung bei Verletzung einer vertragswesentlichen Pflicht (Kardinalpflicht) ist darüber hinaus - mit Ausnahme bei Vorsatz und grober Fahrlässigkeit, bei zugesicherten Eigenschaften, bei arglistigem Verhalten, aus Garantien, nach dem Produkthaftungsgesetz sowie bei der Verletzung von Leib, Leben und Gesundheit - beschränkt auf den vertragstypischen Schaden, mit dessen Entstehen der Auftragnehmer bei Vertragsschluss aufgrund der zu diesem Zeitpunkt bekannten Umstände rechnen musste. Ei-ne solche vertragswesentliche Pflicht liegt immer dann vor, wenn es sich um eine Pflicht handelt, auf deren ordnungsgemäße Erfüllung der Auftraggeber vertrauen konnte und auch redlicherweise vertrauen durfte.

(4) ☐ Kommt es bei Verletzungen von Datenschutzbestimmungen durch den Auftragsver-

arbeiter zu Nachteilen für den Auftraggeber, bspw. zu Veröffentlichungen in Medien über den Auftraggeber, so hat der Auftragsverarbeiter unabhängig von Schadenersatzleistungen eine Vertragsstrafe in Höhe von….€ (bis 10 % des Auftragswertes eintragen) zu leisten. Dasselbe gilt für die Fälle, wenn es der Auftragsverarbeiter versäumt hat den Auftraggeber entsprechend Art. 33 Abs. 2 EU-DS-GVO (Meldung von Datenschutzverletzungen) unverzüglich zu informieren.
Eine Vertragsstrafe fällt auch an, wenn ohne Zustimmung des Verantwortlichen eine Datenübermittlung an eine natürliche oder juristische Person erfolgt, die nicht unter die EU-DS-GVO fällt oder die Verarbeitung im außereuropäischen Ausland vorgenommen worden ist.

§ 12 Informationspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter wird den Auftraggeber darauf hinweisen, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Bis zur Bestätigung der Weisung durch den Auftraggeber ist der Auftragsverarbeiter nicht verpflichtet, die Weisung auszuführen. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragsverarbeiter geltend machen.

(2) Bei schwerwiegenden Störungen des Betriebsablaufs oder bei Verdacht auf Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) oder wesentlichen Unregelmäßigkeiten bei der Datenverarbeitung unterrichtet der Auftragsverarbeiter gemäß Art. 33 II DSGVO unverzüglich den Auftraggeber. Dasselbe gilt, wenn sich eine Aufsichtsbehörde oder Strafverfolgungsorgane bei dem Auftragsverarbeiter melden.

(3) Sollen die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden oder droht eine wesentliche Änderung der Eigentumsverhältnisse beim Auftragsverarbeiter, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang involvierten Personen unverzüglich darüber informieren, dass die Hoheit der Daten beim Auftraggeber liegt.

§ 13 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts an Daten und Unterlagen ist während der Vertragsdauer und danach (gleichgültig aus welchem Grund das Auftragsverhältnis endet) ausgeschlossen.

§ 14 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat

der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 15 Sonstiges

(1) Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile -einschließlich etwaiger Zusicherung des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrages handelt. Dies gilt auch für den Verzicht auf das Formerfordernis.

(2) Die Unwirksamkeit einer Bestimmung dieses Vertrages berührt nicht die Gültigkeit der übrigen Bestimmungen. Die Parteien werden unwirksame Bestimmungen durch wirtschaftlich ihnen nahekommende neue Bestimmungen ersetzen.

Stuttgart, den _____ _____

Ort, Datum

_____ _____

(Auftraggeber) (Auftragsverarbeiter)

Anlage zur Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DS-GVO (zur Leistungsvereinbarung/Leistungsblatt vom **[dd.mm.yyyy]**) – Vereinbarte technisch-organisatorische Maßnahmen

Gemäß Artikel 32 DS-GVO treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Hierzu wurde vorab durch den Verantwortlichen eine Schutzbedarfsermittlung durchgeführt, dokumentiert und dem Auftragsverarbeiter mitgeteilt.

Nachfolgende Sicherheitsmaßnahmen werden auf der Basis des definierten Schutzbedarfs vertraglich zugesichert:

1. Maßnahmen, die die Vertraulichkeit und Integrität im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: durch Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

Umsetzung eines wirksamen Zutrittsschutzes	Sicherheitsbereiche in denen personenbezogene Daten verarbeitet und gespeichert oder abgelegt werden, sind gegen den Zutritt unbefugter Personen durch geeignete technische oder organisatorische Maßnahmen abgesichert.
Festlegung zutrittsberechtigter Personen	Der Kreis der zutrittsberechtigten Personen ist festgelegt und die Zutrittsberechtigungen zu sicherheitsrelevanten Bereichen, sind auf das notwendige Minimum beschränkt.
Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen	Es besteht ein Prozess zur Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. zum Entzug von Zutrittsrechten.
Regelungen für Besucher, Fremdpersonal, Reinigungs- und Wartungspersonal	Es existieren schriftlich fixierte Regelungen für Besucher, Fremdpersonal, Reinigungs- und Wartungspersonal, dass die erlaubten Tätigkeiten regelt und die sicherstellen, dass keine unberechtigten Personen Zutritt erlangen können.

Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: durch sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Implementation von Sicherheitsgateways	IT-/Netztechnische-Systeme sind durch entsprechende Maßnahmen (i.d.R. Firewalls) nach aktuellem Stand der Technik vor unerwünschten Zugriffen oder Datenströmen geschützt.
Zugangsschutz (Authentifizierung)	Der Zugang zu DV-Anlagen ist erst durch entsprechende Sicherheitsmaßnahmen nach Stand der Technik möglich.
Einfache Authentifizierung (per Benutzername/Passwort) bei normalem Schutzbedarf	Passwörter entsprechen angemessenen Mindestregeln nach Stand der Technik wie z.B. Passwortlänge, Passwortkomplexität.
Starke Authentifizierung bei hohem und sehr hohem Schutzbedarf	Bei hohem und sehr hohem Schutzbedarf erfolgt eine starke Authentifizierung auf Basis von mindestens zwei Merkmalen. Dies sind beispielsweise: Chipkarte mit Zertifikaten und PIN, OneTime-Passwörter (OTP Generator, SMS TAN, ChipTAN) und Nutzerpasswort sowie der Einsatz von biometrischen Verfahren und Passwort.
Authentifizierung administrativer Tätigkeiten	Der Zugang zu administrativen Tätigkeiten insbesondere über das Internet erfolgt durch starke Authentifizierung (z.B. Mehrfaktor Authentifizierung, SSH Zertifikatsbasierend).
Protokollierung des Zugangs	Erfolgreiche und abgewiesene Zugangsversuche werden protokolliert, ausgewertet und mindestens für 90 Tage revisionssicher aufbewahrt.
Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk	Authentisierungs-Credentials werden nicht im Klartext übertragen. Es wird ein ausreichend geschütztes Verfahren angewendet.
Reaktion bei Fehlversuchen/Inaktivität	Es existiert ein Prozess zur Reaktion auf wiederholte fehlerhafte Authentisierung. Ein Prozess zur Rücksetzung bzw. Entsperrung von gesperrten Zugangskennungen ist eingerichtet, beschrieben und wird angewendet.
Festlegung, Verwaltung und Dokumentation befugter Personen	Es besteht ein Verfahren zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugangsberechtigungen und ggf. von Authentifizierungsmedien. Vergebene Berechtigungen werden dokumentiert.
Persönliche Zuordnung von Zugangskennungen	Zugangskennungen sind personengebunden und an ein persönliches Passwort und ggf. Authentifizierungsmedien geknüpft.

Verhaltensweise	Der Mitarbeiter oder Erfüllungsgehilfe des Auftragsverarbeiters/Dienstleisters ist verpflichtet, die Regelungen und Vorgaben der technischen und organisatorischen Zugangskontrolle zu befolgen und stellt zudem sicher, dass nicht durch falsches Verhalten Unberechtigten der Zugang zu DV-Anlagen des Auftraggebers ermöglicht wird.
Regelungen zum Arbeitsplatz	Es bestehen Regelungen zur Sperrung des Systems z.B. manuelle Bildschirmsperrung bei Verlassen des Arbeitsplatzes, automatische Bildschirmsperre nach einer bestimmten Inaktivitätszeit.
Mobiles Arbeiten /Fernzugriff	Sofern der Auftragsverarbeiter mobiles Arbeiten bzw. Fernzugriff erlaubt, sind geeignete Regelungen und Maßnahmen nach Stand der Technik vorhanden, die die Integrität, Vertraulichkeit und Belastbarkeit sicherstellen.

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Erstellung eines Berechtigungskonzepts	Ein Berechtigungskonzept für Benutzer und Administratoren stellt generell und anwendungsspezifisch sicher, dass der Zugriff auf Daten nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung gemäß interner Aufgabenverteilung und Funktionstrennung des Benutzers erforderlich ist. Die Umsetzung des „Need-to-know-Prinzip“ ist sichergestellt.
Bindung an die Aufgabe	Der Auftragsverarbeiter stellt sicher, dass ausschließlich die Personen auf die Daten Zugriff erlangen, die mit der Erfüllung der damit verbundenen Aufgabe beschäftigt sind.
Anpassung der Berechtigung bei personellen Veränderungen	Bei Abteilungs- /Funktionswechsel und/oder Ausscheiden eines Mitarbeiters werden die Zugriffsberechtigungen aktualisiert bzw. entzogen. Die Vergabe und Änderung von Zugriffsberechtigungen werden protokolliert.
	Für den Fall das der Auftragsverarbeiter Fernzugriffsberechtigungen erhält wird bei personellen Veränderungen der MDR durch den Auftragsverarbeiter informiert.
Inhouse-Wartung, Zugriff auf Geräte des Auftraggebers	Soweit der Auftragsverarbeiter Wartungen beim Auftraggeber durchführt oder den Zugriff auf die Hardware des Auftraggebers erhält, stellt er sicher, dass er bzw. seine beauftragten Mitarbeiter die internen Datenschutz- und IT-Sicherheitsregelungen und –weisungen des Auftraggebers befolgen.

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. durch Mandantenfähigkeit, Virtualisierung, Trennung von Produktiv-, Test- und Entwicklungsumgebungen.

Zweckbindung	Es werden nur solche personenbezogenen Daten verarbeitet, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses zwingend notwendig sind und unmittelbar dem eigentlichen Zweck dienen. Dieser Zweck darf sich in keinem nachgelagerten Schritt der Verarbeitung, auch nicht nach einer Übermittlung ändern.
Getrennte Verarbeitung	Der Auftragsverarbeiter stellt sicher, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten wird so gestaltet, dass eine Vermischung von Daten für unterschiedliche Verarbeitungszwecke oder anderer Vertragspartner/Auftraggeber nicht möglich ist (z.B. physikalische bzw. logische Trennung von Systemen, Datenbanken und Datenträgern, Steuerung über Berechtigungskonzepte).
Trennung von Produktiv-, Test und Entwicklungsumgebungen	Der Auftragsverarbeiter setzt Maßnahmen ein, die die Entwicklungsumgebung sowie die Testumgebung strikt von der Produktionsumgebung trennt.

Pseudonymisierung bzw. Anonymisierung

Anonymisierung	Der Auftragsverarbeiter verwendet Maßnahmen zur Anonymisierung die eine Zuordnung bzw. Verbindung zu einer Person unmöglich machen z.B. durch Informationsreduktion, datenveränderte Verfahren, Mikroaggregationsverfahren usw….
Pseudonymisierung, Transfomationsverfahren	Der Auftragsverarbeiter verwendet zur Pseudonymisierung von personenbezogenen Daten Transformationsverfahren nach Stand der Technik (z.B. aktuelle BSI-Richtlinien zu Kryptoverfahren) die bei langfristiger Verwendung von pseudonymisierten Daten durch jeweils aktuelle Verfahren ausgetauscht werden.
Pseudonymisierung, Umgang mit geheimen Parametern	Der Auftragsverarbeiter verwendet geeignete Maßnahmen, nach Stand der Technik, zur Erzeugung und Verwaltung (z.B. Verteilung. Speicherung und Löschung) geheimer Parameter (z.B. Schlüssel und Zuordnungstabellen).
Initiierung der Pseudonymisierung	Das Verfahren zur Pseudonymisierung wird so früh wie möglich im Verarbeitungsprozess angewendet.

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Speicherung, Übertragung oder Transport, z.B.: durch Prüfsummen, Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

Verschlüsselte Datenübertragung zu externen Systemen	Werden personenbezogene Daten zu externen Systemen übertragen oder zwischen Auftragsverarbeiter und Auftraggeber ausgetauscht, erfolgt zwingend eine Verschlüsselung nach Stand der Technik. Z. B. EMail-Verschlüsselung, VPN, Verschlüsselte Übertragungsprotokolle, Nutzung von Signaturverfahren, …
Härtung der Front-- und Backendsysteme	Die Systeme des Auftragsverarbeiters sind nach dem Stand der Technik gehärtet z.B. Einsatz von Virenscannern und oder Anomalieerkennungs-Systemen auf Client- und Server-Systemen, Beschränkung von Dienstkonten, Einsatz eines speziellen Administrationsnetzes, schließen nichtbenötigter Ports, löschen nichtbenötigter Benutzerkennungen, setzen restriktiver Rechte, ändern der Default-Passwörter, Nutzung von Verschlüsselungsmöglichkeiten, Bildschirmsperre, Verschlüsselung der gespeicherten Passwörter, ...
Verschlüsselte Ablage von Daten mit hohem oder sehr hohem Schutzbedarf	Zur sicheren Ablage personenbezogener Daten nach DSGVO Artikel 9 Abs. 1 und Artikel10 wird eine verschlüsselte Datenablage verwendet. Dies gilt auch für etwaige Backups.
Gesicherte Speicherung auf mobilen Datenträgern/Systemen	Die Speicherung auf mobilen Datenträgern bzw. mobilen Systemen ist aufgrund des hohen Verlustrisikos nicht zulässig. Sollte eine Speicherung dennoch unumgänglich sein, ist die Form der Verarbeitung zu regeln und die Verschlüsselung der Daten auf dem Medium nach Stand der Technik sicherzustellen.
Prozess zur Sammlung und Entsorgung	Ein Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern und Informationsträgern ist eingerichtet und in einer Organisationsrichtlinie /Verfahrensanweisung beschrieben. Die Mitarbeiter werden regelmäßig für dieses Thema sensibilisiert.
Weitergabe von Datenträgern	Es bestehen Regelungen zur Weitergabe von Datenträgern z.B. Verschlüsselung der zu übermittelten Daten, unverschlüsselte Datenträger werden vor der Weitergabe an externe Stellen stets datenschutzgerecht gelöscht.
Speicherung von Authentifizierungsgeheimnissen	Authentifizierungsgeheimnissen werden ausreichend geschützt gespeichert. Z.B. TPM, sichere Hash-Verfahren wie Argon2.

Mobile Endgeräte	Wenn Auftragsdaten auch auf mobilen Endgeräten verarbeitet werden, sind die Endgeräte durch ein MDM verwaltet und wie folgt geschützt: - durch Benutzerkennung mit Passwort, - durch die Verschlüsselung der Festplatten bzw. Verzeichnisse gemäß Stand der Technik, - durch eine VPN-Verbindung zum eigenen Firmennetz oder durch eine VPN-Verbindung zum Auftraggeber, - durch Client-Security-Software, - durch den Ausschluß administrativer Rechte für den Benutzer.
Private Geräte	Eine Verarbeitung von Auftragsdaten des Auftraggebers auf privaten Geräten der Mitarbeiter ist nicht gestattet.

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert, kopiert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement.

Zuständigkeiten und Verantwortlichkeiten	Der Auftragsverarbeiter hat klare Zuständigkeiten für die Eingabe, Änderung und Löschung von personenbezogenen Daten und realisiert die Umsetzung auf Basis eines definierten Rollen- und Berechtigungskonzeptes.
Protokollierung bei Lese-, Eingabe-, Änderungs- und Löschtransaktionen	Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen relevanten personenbezogenen Daten werden protokolliert.
Protokollierung administrativer Tätigkeiten	Der Zugriff und die Aktivitäten der Administratoren werden protokolliert und manipulationssicher gespeichert z.B. durch einen separaten Protokollierungsserver (der von den zu protokollierenden Systemen getrennt installiert ist).
Sicherung der Protokolldaten vor Verlust und Veränderung	Der Auftragsverarbeiter setzt Maßnahmen ein, die den Verlust bzw. eine Veränderung der Protokolldaten sicher verhindert z.B. restriktive Berechtigungsvergabe, Datensicherung, Verschlüsselung der Protokolldaten oder signaturbasierende Maßnahmen
Kontrolle der Protokolldaten	Der Auftragsverarbeiter stellt sicher, dass die Protokolle der Zugriffe auf die personenbezogenen Daten regelmäßig ausgewertet werden. Unregelmäßigkeiten werden dokumentiert und dem Auftraggeber unverzüglich schriftlich mitgeteilt.

2. Maßnahmen, die die Verfügbarkeit und Belastbarkeit im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle, Detektion und Reaktion

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Datensicherungskonzept (online/offline; on-site/off-site), Redundanz- und/oder Havarie-Konzepte, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Zeitnahe Erkennung und Reaktion von Versuchen der zufälligen oder mutwilligen Zerstörung, Verlust und Missbrauch, z.B. durch Einbruchserkennungssysteme (IDS/IPS), zentrale Logauswertung (SIEM), Security Operation Center (SOC), Computer Emergency Response Team (CERT).

Brandschutz	Der Auftragsverarbeiter setzt Maßnahmen ein, die der Entstehung und Ausbreitung eines Brandes vorbeugen, bzw. die die Einhaltung von Brandschutzvorschriften gewährleisten z.B. Brandfrüherkennung, geeignete Löschtechnik, unterschiedliche Brandabschnitte, feuerfeste bzw. feuerhemmende Zugangstüren.
Einsatz von technischen Infrastruktur-Maßnahmen	Der Auftragsverarbeiter setzt in der technischen Infrastruktur Maßnahmen ein, die den Verlust oder die Zerstörung von personenbezogenen Daten verhindern z.B. unterbrechungsfreie Stromversorgung, Überspannungsschutz, Klimaanlage in Serverräumen, geeignete Brandschutzmaßnahmen, Datentresor, redundante Systeme in unterschiedlichen Brandabschnitten, infrastrukturelle Meldeanlagen (z.B. Einbruch, Brand, Feuchtigkeit, Temperatur,), Sicherungssysteme (z.B. Tape Libraries, Backupsysteme etc.) in einem anderen Brandabschnitt.
Schwachstellenmanagement	Der Auftragsverarbeiter betreibt ein Verfahren für seine Verarbeitungsanlagen das Schwachstellen erkennt, bewertet, priorisiert und zeitnah behebt (z.B. Patchmanagement, regelmäßige Penetrationstests …).
Erkennung und abwehren von Cyberangriffen	Der Auftragsverarbeiter setzt abgestimmte Sicherheitslösungen ein, die Einfallstore für Angriffe bzw. Cyberangriffe erkennen und erfolgreich abwehren können z.B. Virenschutz, Einbruchserkennungssysteme (IDS/IPS), zentrale Logauswertung (SIEM), Security Operation Center (SOC), Computer Emergency Response Team (CERT).
Incident-Response-Management	Der Auftragsverarbeiter besitzt ein Verfahren zur Behandlung und Nachbereitung von Datenschutz- bzw. Sicherheitsvorfällen.
Redundanz bei hohem Schutzbedarf	Der Auftragsverarbeiter gewährleistet durch geeignete redundante Maßnahmen die Verfügbarkeit der DV-Anlage bei Ausfall von einzelnen Komponenten z.B. RAID, Cluster, Hot/Cold-Stand-By usw..
Test neuer Hard und Software	Der Auftragsverarbeiter gewährleistet mit einem Test- und Abnahmeverfahren bei neu eingesetzter Hard- und Software, die fehlerfreie Funktion der Verarbeitungsanlage.

IT-Servicemanagement	Mit einem effizienten IT-Servicemanagement gewährleistet der Auftragsverarbeiter eine fehlerfreie Funktion der Verarbeitungsanlagen und Zugriffssystemen.
Backup- und Recovery-Konzept	Zur Sicherstellung der Verfügbarkeit besteht ein Backupkonzept zur regelmäßigen Datensicherung. Zur schnellstmöglichen Datenwiederherstellung besteht ein Recovery-Konzept, das einen befugten Mitarbeiter in die Lage versetzt, die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung zu stellen.
Monitoring	Der Auftragsverarbeiter verwendet ein Verfahren zur Überwachung der Verarbeitungsanlage das gewährleistet, dass alle Funktionen zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.
Notfallplan	Zur Schadensminimierung und weiterer Schadensabwehr erstellt der Auftragsverarbeiter einen Notfallplan in dem die einzuleitenden Schritte im Notfall aufgeführt und festgelegt werden. Der Notfallplan orientiert sich an einem geeigneten Standard, wie z.B. BSI-Standard 200-4 Notfallmanagement, ISO 22301/2012 Business Continuity Management oder die Good Practice Guidelines (GPG). Bestandteil des Notfallplans ist die angebotene Dienstleistung.
Sensibilisierung	Alle Personen, die mit personenbezogenen Daten umgehen oder sonst an der Auftragsdurchführung beteiligt sind (z.B. Wartungsunternehmen, Datenvernichter, usw.), sind nachweislich regelmäßig bzw. bei Bedarf zu unterweisen.

3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Überprüfung, Bewertung und Evaluierung

Der Auftraggeber erhält auf folgende Art und Weise Einblick in die Auditierungsergebnisse beauftragter Dritter:

Interne Prüfungensverfahren zur Prüfung der eingesetzten TOMs	Der Auftragsverarbeiter nutzt interne Prüfungsverfahren auf Einhaltung der festgelegten Prozesse, interner Vorgaben und auf Wirksamkeit der eingesetzten TOMs z.B. durch DSB, ISB, Revision …
Externe Audits, Zertifizierungsverfahren	Der Auftragsverarbeiter nutzt Verfahren zur Überprüfung des Datenschutzniveaus bzw. auf Einhaltung der DSGVO z.B. externe Audits nach ISO27001 oder BSI-IT-Grundschutz, ISO27018, Testate, Datenschutzsiegel und/oder –Prüfzeichen, …
Einsichtnahme durch den Auftraggeber	Der Auftraggeber erhält im Rahmen des §10 dieses AVV Einsichtnahme in die Prüfungsergebnisse der zuvor genannten Überprüfungen.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Datenschutz-freundliche Vor-einstellung	Der Auftragsverarbeiter stellt Maßnahmen zur datenschutzfreundlichen Voreinstellung nach Stand der Technik bereit. Entsprechende Maßnahmen bestehen unter anderem darin, dass: • nur die Daten erhoben werden, die auch tatsächlich benötigt werden, • die Datenverarbeitung selbst soweit eingeschränkt ist, dass ausschließlich die minimal erforderlichen Funktionen für die Verarbeitung der personenbezogenen Daten verwendet werden können, • durch Voreinstellungen eine Verarbeitung ausschließlich dem Verarbeitungszweck entsprechend erfolgen kann, • wo möglich eine Pseudonymisierung zur Datenminimierung erfolgt, • wo möglich, personenbezogene Daten so schnell wie möglich, pseudonymisiert werden, • Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird.