Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO

zwischen
Westdeutscher Rundfunk Köln
.....
Rundfunkanstalt/Gemeinschaftseinrichtung - nachstehend **Auftraggeber** genannt -
(oder auch Verantwortlicher genannt)

und der
.....
nachstehend **Auftragsverarbeiter**
(oder auch Auftragnehmer**)** genannt -

.....
gemäß Art. 27 DS-GVO zu bestellender Vertreter, wenn der Auftragsverarbeiter keinen Sitz in der EU hat

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

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand:

☒ Der Gegenstand des Auftrags ergibt sich aus den Vergabeunterlagen im Verfahren ZE-2022-250-02**.**

☐ Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter: ……
(Definition der Aufgaben)

(2) Dauer:

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der gesamten Laufzeit des Leistungsverhätnis.

☐ 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. Die Kündigung bedarf der Schriftform.

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

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.

§ 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
  - ☒ 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)
  - ☒ IP-Adressen, Emailadressen und Telefonnummern (UGC-Einsendungen, freiwillig)
  - ☒ Videomaterial, das z.B. Abbildungen von Personen enthalten kann

(2) Betroffene Personen:

- ☐ 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
  - ☐ Alle Nutzer:innen der MOsys
  - ☒ Personen, die auf Videomaterial des WDR zu sehen sind

(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 vom …….

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

Planung/Konfiguration/Wartung/Fehlerbehebung von medientechnischen Systemen.

(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 Verlagerung 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** 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);

☐ 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 organi-

satorische 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.

Einzelne Weisungen können zu folgenden Gegenständen ……. von folgenden Personen erteilt werden: ……(*Namen*).

(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 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 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. Fernwartung/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 _____ 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 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).

a) ☒ Eine Unterbeauftragung ist unzulässig.

b) ☐ 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

c) ☐ 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;
oder
☐ 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

(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.

§ 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.

(4) 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.

(Ort), den…….	(Ort), den ……
……	……
(Auftraggeber)	(Auftragsverarbeiter)

Anlage zur Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DS-GVO (zur Leistungsvereinbarung***/zum Leistungsverzeichnis***/zum SLA***/zur Bestellung *** vom …….) **– 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 <u>Vertraulichkeit</u> im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (Art. 32 Abs. 1 lit. b DS-GVO)**
   Zum Beispiel:

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

  Nicht relevant

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

  Sichere Kennwörter sind gegeben.

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

  vorhanden

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

- Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung besonderer, personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

  Nicht relevant

- Weitere Maßnahmen, die zur Wahrung der Vertraulichkeit im konkreten Fall erforderlich sind:

2. **Maßnahmen, die die <u>Integrität</u> im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (Art. 32 Abs. 1 lit. b DS-GVO)**
   Zum Beispiel:

- 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;

Nicht relevant

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

Nicht relevant

- Weitere Maßnahmen, die zur Wahrung der Integrität im konkreten Fall erforderlich sind:

3. **Maßnahmen, die die <u>Verfügbarkeit und Belastbarkeit</u> im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (Art. 32 Abs. 1 lit. b DS-GVO)**
   Zum Beispiel:

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Datensicherungs-

konzept (online/offline; on-site/off-site), Redundanz- und/oder Havarie-Konzepte, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Vorhanden

- Detektion und Reaktion
  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);

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Rückholbarkeit sämtlicher Daten des Auftraggebers.

- Weitere Maßnahmen, die zur Wahrung der Verfügbarkeit und Belastbarkeit im konkreten Fall erforderlich sind:

Redundanzen

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

Zum Beispiel:

- Regelmäßige, unabhängige Auditierungen der vereinbarten TOM durch/von:
  - _____
  - _____
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Häufigkeit der Auftragskontrolle durch Auftraggeber:
  - _____

Der Auftraggeber erhält auf folgende Art und Weise Einblick in die Auditierungsergebnisse beauftragter Dritter (siehe oben):

Nicht relevant

5. Ggfs. weitere Maßnahmen, die für die konkrete Auftragsverarbeitung zur Wahrung eines angemessenen Schutzniveaus auf der Grundlage der Risikoanalyse erforderlich sind:

Nicht relevant

6. Vereinbarungen zur Fernwartung

- Der Auftragnehmer führt folgende Fernzugriffe auf DV-Anlagen durch:

- Folgende Bereiche wurden informiert und bestätigen dies (z. B. Informationssicherheitsbeauftragter, Leiter IT, Informationstreuhänder, Informationsverantwortlicher, Anbindungsverantwortlicher für den Fernzugriff)

_____

Rolle, Datum, Name, Unterschrift

_____

Rolle, Datum, Name, Unterschrift

_____

Rolle, Datum, Name, Unterschrift

_____

Rolle, Datum, Name, Unterschrift

_____

Rolle, Datum, Name, Unterschrift