Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

Rundfunk Berlin-Brandenburg, Masurenallee 8-14, 14057 Berlin

nachfolgend „**Verantwortlicher**“

ggf. als Vertreter der folgenden Rundfunkanstalten/Gemeinschaftseinrichtungen

ARD-Hauptstadtstudio

und

[Name/Firma], [Anschrift]

nachfolgend „**Auftragsverarbeiter**“

schließen folgenden Auftragsverarbeitungsvertrag (nachfolgend: AVV):

Hinweis:
§§ 1, 2, 5, 6, 15 (mit * markiert) sind zwingend vom Verantwortlichen (Auftraggeber) auszufüllen.

§ 1 Gegenstand, Zweck, Art und Dauer des Auftrags*

1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich

[Erneuerung Redaktionsarbeitsplätze]

gemäß Vertrag [ ] vom (nachfolgend: **Hauptvertrag**).

Teil der Durchführung des Hauptvertrages ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung („**DSGVO**").

Die vom Auftragsverarbeiter zu erbringenden Leistungen sowie Art und Zweck der Datenverarbeitung, ergeben sich aus dem Hauptvertrag.

2) Die Dauer der Verarbeitung

☒ entspricht der Laufzeit des Hauptvertrags.

☐ Ist befristet bis zum XX.XX.20XX .

3) Der Verantwortliche kann den AVV jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen die DSGVO oder weitere anwendbare datenschutzrechtliche Bestimmungen oder gegen Pflichten aus diesem AVV vorliegt, der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will oder der Auftragsverarbeiter den Zutritt des Verantwortlichen oder der zuständigen Aufsichts-behörde vertragswidrig verweigert.

§ 2 Konkretisierung des Auftragsinhalts*

1) Art der personenbezogenen Daten:

☒ Personalstammdaten

☒ Kommunikationsdaten (z. B. Telefon, E-Mail)

☐ Vertragsstammdaten

☒ Logdaten

☐ Zahlungs- und Finanzdaten

☐ Planungs- und Steuerungsdaten

☐ Besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO, und zwar:

☐ Sonstige:

2) Betroffene Personen:

☐ Nutzer (TV, Radio, Online)

☒ Beschäftigte

☒ Geschäftspartner

☐ Ansprechpartner, z.B. bei Dienstleistern, Geschäftspartner

☐ Besucher

☐ Sonstige:

* von Auftraggeber auszufüllen

§ 3 Unterauftragsverarbeiter

1) Der Auftragsverarbeiter darf Unterauftragsverarbeiter nur nach der vorherigen Zustimmung des Verantwortlichen beauftragen. Voraussetzung für die Unterbeauftragung ist der Abschluss einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO, die auch die zwischen Verantwortlichen und Auftragsverarbeiter getroffenen Regelungen hinreichend berücksichtigt. Insbesondere darf das vereinbarte Schutzniveau im Hinblick auf die vereinbarten technischen und organisatorischen Maßnahmen nicht unterschritten werden.

2) Sofern die Unterbeauftragung durch den Auftragsverarbeiter nach Abs. 1 zulässig ist, wird die Zustimmung bezüglich folgender Unterauftragsverarbeiter mit Abschluss dieser AVV erteilt:

Name und Anschrift des Unterauftragsverarbeiters	**Beschreibung der Aufgaben des Unterauftragsverarbeiters**

3) Vor einer möglichen Hinzuziehung weiterer oder Ersetzung der in Abs. 2 aufgeführten Unterauftragsverarbeiter informiert der Auftragsverarbeiter den Verantwortlichen eine angemessene Zeit vorab in Textform (z.B. E-Mail) unter Angabe der erforderlichen Daten gem. der Tabelle in Abs. 2. Hat der Verantwortliche gegen die Änderung innerhalb von 14 Tagen ab Information durch den Auftragsverarbeiter, in Textform keinen Einspruch erhoben, so gilt der Einsatz des Unteraufragnehmers als genehmigt.

4) Der Auftragsverarbeiter wird auf Verlangen dem Verantwortlichen Kopien der Unterauftragsverträge zur Verfügung stellen.

§ 4 Ort der Datenverarbeitung

☒ Die Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

☐ Die Datenverarbeitung durch den Auftragsverarbeiter selbst oder seine Unterauftragsverarbeiter gem. § 3 dieses AVV findet in einem oder mehreren Drittländern statt. Die Einhaltung der Vorgaben gem. Kapitel 5 der DSGVO wird sichergestellt durch einen Angemessenheits-beschluss sowie ggf. die Zertifizierung des (Unter-)Auftragsverarbeiters (Art. 45 Abs. 3 DSG-VO) oder sonstige geeignete Garantien gem. Art. 46 Abs. 2, Abs. 3 DSGVO (z.B. Standarddatenschutzklauseln, Binding Corporate Rules). Der Auftragnehmer hat sich im Rahmen eines durchgeführten Transfer Impact Assessment mit der Datenverarbeitung im Drittland auseinandergesetzt und die sich daraus abzuleitenden Maßnahmen ergriffen.

Ort der Datenverarbeitung durch Auftragsverarbeiter oder Unterauftragsverarbeiter	**Verarbeitungstätigkeit**	**Einhaltung der Vorgaben gem. Kapitel 5 der DSGVO wird sichergestellt durch:**
[ggf. Ort eintragen]	[ggf. Art der Datenverarbeitung eintragen]	[ggf. Maßnahmen zur Sicherstellung des Datenschutzniveaus eintragen]

§ 5 Weisungsbindung*

1) Der Auftragsverarbeiter darf die vertragsgegenständlichen personenbezogenen Daten ausschließlich im Rahmen dieses AVV oder unter Einhaltung der ggf. vom Verantwortlichen erteilten ergänzenden Weisungen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2) Eine Verarbeitung für andere Zwecke ist nicht zulässig.

3) Kopien der Daten werden nur mit Zustimmung des Verantwortlichen erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung notwendig, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

4) Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragsverarbeiter zu erteilen. Sie sind in Textform zu erteilen. Mündlich erteilte Weisungen sind durch den Verantwortlichen unverzüglich in Textform zu dokumentieren.

   Weisungsberechtigte Personen des Verantwortlichen sind:

   [Kasnitz Stephan, Organisationseinheit, E-Mail, Telefon]

   [Name, Organisationseinheit, E-Mail, Telefon]

   Der Verantwortliche kann weitere weisungsberechtigte Personen in Textform gegenüber dem Auftragsverarbeiter festlegen.

5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich, spätestens aber nach drei Tagen, zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen gesetzliche Regelungen.

§ 6 Technisch-organisatorische Maßnahmen*

1) Der Auftragsverarbeiter hat die Datensicherheit gem. Art. 25, 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO, herzustellen. Hierzu setzt der Auftragsverarbeiter die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen um. 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.

2) Zur Definition eines dem Risiko angemessenen Schutzniveaus hat der Verantwortliche den Schutzbedarf festgelegt, der durch den Auftragsverarbeiter bei der Umsetzung der technisch-organisatorischen Maßnahmen sichergestellt werden muss:

Vertraulichkeit	**Integrität**	**Verfügbarkeit**
☒ normal	☒ normal	☒ normal
☐ hoch	☐ hoch	☐ hoch
☐ sehr hoch	☐ sehr hoch	☐ sehr hoch

3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit wird der Auftragsverarbeiter die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig sowie anlassbezogen auf ihre Wirksamkeit kontrollieren. Dem Auftragsverarbeiter ist es gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen gemäß **Anlage 1** nicht unterschritten werden. Wesentliche Änderungen sind mit dem Verantwortlichen vor Durchführung der Änderungen abzustimmen und zu dokumentieren.

§ 7 Anfragen betroffener Personen

Wendet sich eine betroffene Person zur Geltendmachung eines datenschutzrechtlichen Anspruchs (z.B. Auskunft, Löschung oder Berichtigung) an den Auftragsverarbeiter, wird dieser die betroffene Person an den Verantwortlichen verweisen. Der Auftragsverarbeiter leitet den Antrag der betroffenen Person zudem unverzüglich, spätestens aber nach drei Tagen, an den Verantwortlichen weiter. Der Auftragsverarbeiter unterstützt den Verantwortlichen, auch bereits im Vorfeld, mit geeigneten technischen und organisatorischen Maßnahmen dabei, der Pflicht des Verantwortlichen zur Beantwortung von Betroffenenanfragen nachzukommen.

§ 8 Vertraulichkeit

1) Der Auftragsverarbeiter verpflichtet sich, die ihm vom Verantwortlichen zur Verfügung gestellten Unterlagen und Daten sowie die Arbeitsergebnisse vertraulich zu behandeln, insbesondere Unbefugten nicht zugänglich zu machen.

2) Der Auftragsverarbeiterstellt sicher, dass die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

3) Diese Verpflichtungen bestehen auch nach Beendigung des Vertrages fort.

§ 9 Unterstützungs- und Meldepflichten des Auftragsverarbeiters

1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Führung seines Verarbeitungsverzeichnisses nach Art. 30 Abs. 1 DSGVO, insbesondere bezüglich der Dokumentation der technischen und organisatorischen Maßnahmen.

2) Soweit der Verantwortliche 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 zu unterstützen.

3) Der Auftragsverarbeiter unterstützt den Verantwortlichen im Falle einer Verletzung des Schutzes personenbezogener Daten, die im Zusammenhang mit der Auftragsverarbeitung steht, bei der Erfüllung seiner diesbezüglichen Pflichten gegenüber der Aufsichtsbehörde sowie der Pflicht zur Dokumentation.

4) Bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht einer Datenschutzverletzung oder bei wesentlichen Unregelmäßigkeiten bei der Datenverarbeitung, die den Verantwortlichen betreffen könnten, informiert der Auftragsverarbeiter unverzüglich, spätestens aber nach 12 Stunden, den Verantwortlichen. Dasselbe gilt, wenn sich eine Aufsichtsbehörde oder Strafverfolgungsorgane bei dem Auftragsverarbeiter melden.

5) Sollen die Daten des Verantwortlichen 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 Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang involvierten Personen unverzüglich darüber informieren, dass die Hoheit der Daten beim Verantwortlichen liegt.

§ 10 Datenschutzbeauftragte*r/Ansprechperson des Auftragsverarbeiters

☐ Der Auftragsverarbeiter hat einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt, bestellt.

Als Datenschutzbeauftragte*r beim Auftragsverarbeiter ist

[Name]

[Organisationseinheit]

Telefon: [Nummer]

E-Mail: [E-Mail Adresse]

bestellt. Ein Wechsel des*der Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

☐ Der Auftragsverarbeiter ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechperson für Fragen zum Datenschutz und zur Informationssicherheit im Zusammenhang mit diesem Vertrag wird beim Auftragsverarbeiter

[Name]

[Organisationseinheit]

Telefon: [Nummer]

E-Mail: [E-Mail Adresse]

benannt. Ein Wechsel der Ansprechperson ist dem Verantwortlichen unverzüglich mitzuteilen.

☐ Sofern der Auftragsverarbeiter seinen Sitz außerhalb der Union hat, benennt er gem. Art. 27 Abs. 1 DSGVO folgenden Vertreter in der Union:

[Name]

Telefon: [Nummer]

E-Mail: [E-Mail Adresse]

§ 11 Kontrollrechte des Verantwortlichen

1) Der Verantwortliche hat das Recht, Überprüfungen, durchzuführen oder durch beauftragte Dritte durchführen zu lassen, um sich von der Umsetzung und Einhaltung dieser AVV, insbesondere bezüglich der technischen und organisatorischen Maßnahmen, durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen, insbesondere zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten, zur Verfügung. Die Überprüfung kann in begründeten Fällen auch durch eine Vor-Ort-Inspektion stattfinden, z.B. im Zusammenhang mit möglichen Datenschutzvorfällen. Der Verantwortliche teilt dem Auftragsverarbeiter in diesen Fällen rechtzeitig (in der Regel vier Wochen vorher) den Termin der Überprüfung mit. Außerordentliche oder behördlich verfügte Überprüfungen sind hiervon ausgenommen.

2) Der Nachweis von Maßnahmen gemäß Abs.1, kann in der Regel 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).

3) Eine gesonderte Vergütung des Auftragsverarbeiters für die Ermöglichung der Kontrollen gem. Abs. 1 fällt nicht an.

§ 12 Haftung

Der Auftragsverarbeiter haftet für die ordnungsgemäße Ausführung des Auftrags nach den gesetzlichen Bestimmungen. Machen betroffene Personen Ansprüche gegenüber dem Verantwortlichen wegen unzulässiger oder unrichtiger Datenverarbeitung geltend, so hat der Auftragsverarbeiter den Verantwortlichen zu unterstützen und im Innenverhältnis zu beweisen, dass die fehlerhafte Datenverarbeitung nicht in seinem eigenen Verantwortungsbereich liegt.

§ 13 Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts an Daten und Unterlagen des Verantwortlichen ist ausgeschlossen.

§ 14 Rückgabe und Löschung

1) Nach Abschluss der vertraglich vereinbarten Datenverarbeitung oder jederzeit nach Aufforderung durch den Verantwortlichen, spätestens aber mit Beendigung des Hauptvertrages, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

2) Im Falle einer Löschung durch physische Vernichtung muss diese regelkonform und dem Stand der Technik entsprechend gewährleistet sein, ein Transport in verschlossenen Behältern vorgenommen werden und die erfolgreiche Vernichtung unter Angabe der Schutzklasse und Sicherheitsstufe protokolliert und dokumentiert sein.

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

§ 15 Schlussbestimmungen*

1) Der ausschließliche Gerichtsstand ist [Berlin], Deutschland.

2) Die in diesem Vertrag in Bezug genommenen Anlagen sind Bestandteil des AVV. Sollte eine der Bestimmungen dieses AVV unwirksam sein oder werden, so wird die Gültigkeit der übrigen Bestimmungen hierdurch nicht berührt. Im Falle eines Widerspruchs zwischen dem Vertragstext und dem Inhalt der Anlagen ist der Vertragstext maßgebend.

[Ort], den [Datum]	[Ort], den [Datum]
Unterschrift Verantwortlicher (Informationsverantwortlicher bzw. Informationstreuhänder)	Unterschrift Auftragsverarbeiter

Anlage 1: Vereinbarte technisch und organisatorische Maßnahmen

Anlage zur Vereinbarung zur Verarbeitung vom

Gemäß Artikel 32 DSGVO 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.

☐ Die auf Basis des definierten Schutzbedarfs vertraglich zugesicherte technische und organisatorische Maßnahmen werden in gesonderter Anlage aufgeführt.

☐ Nachfolgende technische und organisatorische Maßnahmen werden auf der Basis des definierten Schutzbedarfs vertraglich zugesichert. *Handelt es sich bei der Auftragsverarbeitung um Fernwartung sind nur die mit * gekennzeichneten Anforderungen mindestens zu erfüllen.*

Maßnahmen, die die Vertraulichkeit im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (Art. 32 Abs. 1 lit. B DSGVO)

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: durch Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen	
Umsetzung eines wirksamen Zutrittsschutzes (EXT.2.1)	Räumlichkeiten in denen Daten des Auftraggebers verarbeitet und gespeichert oder abgelegt werden, MÜSSEN gegen den Zutritt unbefugter Personen durch geeignete Maßnahmen abgesichert werden.
Festlegung zutrittsberechtigter Personen (EXT.2.2)	Der Kreis der zutrittsberechtigten Personen MUSS festgelegt werden und die Zutrittsberechtigungen zu Räumlichkeiten in denen Daten des Auftraggebers verarbeitet und gespeichert oder abgelegt werden, MÜSSEN auf das notwendige Minimum beschränkt werden.
Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen (EXT.2.3)	Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. Entzug von Zutrittsrechten MÜSSEN personengebunden dokumentiert werden. Dies gilt auch für Besucher, Fremdpersonal, Reinigungs- und Wartungspersonal.

Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: durch (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern	
Implementation von Sicherheitsgateways * (EXT.6.1)	Zur Abwehr netzbasierter Angriffe MÜSSEN wirksame Sicherheitsmaßnahmen (d.h. Firewalls, Netzwerksegmentierung, unterschiedliche Sicherheitszonen) nach dem aktuellen Stand der Technik etabliert sein.
Authentifizierung nach dem Stand der Technik * (EXT.13.1)	Der Zugang zu Informationen und Systemen MUSS durch eine sichere Authentisierung nach dem aktuellen Stand der Technik geschützt werden. Dies gilt auch für alle Fernzugänge und Schnittstellen.
Zugang aus ungeschützten Netzen * (EXT.13.2)	Grundsätzlich MUSS immer eine Multi-Faktor-Authentisierung verwendet werden. Kann eine Multi-Faktor-Authentisierung nicht umgesetzt werden, darf der Zugang auf den Dienst ausschließlich auf vom Auftraggeber benannten IP-Adressbereichen (z.B. Datennetz der Rundfunkanstalt) erfolgen.
Starke Authentisierung bei privilegierten Zugängen * (EXT.13.3)	Für privilegierte Zugänge (administrative Zugänge) MUSS eine Multi-Faktor-Authentisierung verwendet werden. Dies gilt auch für alle Fernzugänge und Schnittstellen.
Einfache Authentifizierung (per Benutzername/Passwort) bei normalem Schutzbedarf * (EXT.13.4)	Bei Verwendung von Passwörtern: Es MUSS technisch sichergestellt werden, dass ausschließlich komplexe Passwörter verwendet werden (3 aus den folgenden 4 Merkmalen: Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen; Einhaltung einer definierten Mindestlänge von 10 Zeichen).
Umsetzung von Vorgaben einer Passwortrichtlinie (EXT.13.5)	Die Vorgaben einer Passwortrichtlinie MÜSSEN umgesetzt werden können (Definition von Passworthistorie, Passwortalter, Passwortlänge).
Gesicherte Übertragung von Authentisierungsinformationen im Netzwerk (EXT.13.6)	Übertragung der Authentisierungsinformationen (z.B. Passwörter, Pin, biometrische Merkmale): Die Übertragung der Authentisierungsgeheimnissen MUSS mit einem sicheren Verschlüsselungsverfahren nach aktuellem Stand der Technik (beispielsweise siehe BSI TR-02102) abgesichert werden.
Änderung voreingestellter Authentisierungsinformationen (EXT.13.8)	Voreingestellte Authentisierungsinformationen (z.B. Initialkennungen und Passwörter) MÜSSEN geändert werden können.

Protokollierung sicherheitsrelevanter Ereignisse (EXT.14.1)	Sicherheitsrelevante Ereignisse (z.B. erfolgreiche Zugriffe auf Ressourcen, fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Fehlern, allgemeine Fehlermeldungen, Löschen) MÜSSEN in der Art protokolliert werden, dass sie im Nachgang ausgewertet werden können.

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen	
Dokumentierte Verwaltung von Identitäten und Berechtigungen (EXT.12.1)	Es MUSS eine dokumentierte und stets aktuelle Identitäts- und Berechtigungsverwaltung existieren, die mindestens eine Trennung zwischen Benutzer und administrativen Konten (schließt auch Konten des Dienstleisters ein) ermöglicht.
Umsetzung des Need-to-known-Prinzips * (EXT.12.2)	Es MUSS gewährleistet werden, dass alle Benutzer und Administratoren nur diejenigen Berechtigungen besitzen, die zur Erfüllung der jeweiligen Aufgaben erforderlich sind (Prinzip der minimalen Rechte bzw. least privilege) und bei personellen Veränderungen (z.B. Funktionswechsel, Ausscheiden) Berechtigungen entzogen werden.

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. durch Mandantenfähigkeit, Virtualisierung, Trennung von Produktiv-, Test- und Entwicklungsumgebungen	
Prozess für Test und Freigabe (EXT.8.1)	Es MUSS ein geeigneter Prozess für Tests und Freigabe für alle Komponenten der Dienstleistung etabliert sein.
Trennung von Produktiv-, Test und Entwicklungsumgebungen* (EXT.8.3)	Entwicklungs-, Test- und Produktivumgebung SOLLTEN getrennt sein.
Trennung von Mandanten (EXT.9.1)	Es MUSS eine wirksame Mandantentrennung gewährleistet sein. Die Daten des Auftraggebers MÜSSEN dabei logisch von denen anderer Kunden getrennt sein.
getrennte Verarbeitung * (EXT.18.3)	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 nicht möglich ist (z.B. physikalische bzw. logische Trennung von Systemen, Datenbanken und Datenträgern, Steuerung über Berechtigungskonzepte).

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Umsetzung von Anonymisierung (EXT.18.1)	Sofern vom Auftraggeber gefordert MÜSSEN Maßnahmen zur Anonymisierung, die eine Zuordnung bzw. Verbindung zu einer Person unmöglich machen (z.B. durch Informationsreduktion, datenveränderte Verfahren, Mikroaggregationsverfahren) umgesetzt werden.
Umsetzung von Pseudonymisierung (EXT.18.2)	Sofern vom Auftraggeber gefordert MÜSSEN Maßnahmen zur Pseudonymisierung (z.B. Transformationsverfahren) nach Stand der Technik (z.B. aktuelle BSI Richtlinien zu Kryptoverfahren) umgesetzt werden.

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	
Härtung der Front- und Backendsysteme * (EXT.3.1)	Die für die Erbringung der Dienstleistung genutzten Systeme MÜSSEN gehärtet sein. Hierzu zählen u.a. die Deinstallation nicht notwendiger Software-Pakete; Deaktivierung/Abschaltung von nicht benötigten Programmen, Diensten, Konten, Services und Ports; die Anpassung von Konfigurationen; das Erzwingen von Firewall-Regeln; Änderung von Standardpasswörtern.
Verschlüsselung nach Stand der Technik * (EXT.7.1)	Der Dienstleister MUSS sich bei Verwendung von Verschlüsselungsverfahren nach dem aktuellen Stand der Technik (beispielsweise siehe BSI TR-02102) richten.
Verschlüsselte Datenübertragung zu externen Systemen * (EXT.7.2)	Transport: Jegliche Datenkommunikation MUSS auf dem Transportweg verschlüsselt werden.
Verschlüsselung ruhender Daten * (EXT.7.3)	Der Dienstleister MUSS die ruhenden Daten auf Datenträgern verschlüsselt speichern. Dabei MUSS ein Verfahren genutzt werden, dass dem aktuellen Stand der Technik entspricht.
Löschung und Entsorgung nach dem Stand der Technik * (EXT.11.1)	Nicht mehr benötigte Daten und Informationen MÜSSEN nach dem aktuellen Stand der Technik vernichtet bzw. gelöscht werden. Nach Beendigung der Beauftragung MÜSSEN alle Daten und Informationen des Auftraggebers unwiederbringlich gelöscht werden. Dem Auftraggeber darf kein Schaden durch nicht vernichtete bzw. gelöschte Daten und Informationen entstehen.

Bei erhöhtem Schutzbedarf für Vertraulichkeit: **Nachweis der Datenlöschung** (EXT.11.2)	Als Nachweis SOLLTE dem Auftraggeber ein Löschprotokoll bzw. ein Löschbericht vorgelegt werden, der diesen Datenlöschprozess belegen kann.
Speicherung von Authentisierungsinformationen* (EXT.13.7)	Authentifizierungsinformationen MÜSSEN nach dem aktuellen Stand der Technik geschützt werden (z.B. TPM, sichere Hash-Verfahren wie Argon2).

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert, kopiert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement	
Sicherung der Protokolldaten vor Verlust und Veränderung (EXT.14.2)	Protokollierungsdaten MÜSSEN vor unberechtigtem Zugriff und Manipulation geschützt werden.
Kontrolle der Protokolldaten (EXT.14.3)	Der Dienstleister MUSS die Protokolle regelmäßig auswerten. Unregelmäßigkeiten MÜSSEN dokumentiert und dem Auftraggeber unverzüglich gemeldet werden.
Protokollierung bei Lese-, Eingabe-, Änderungs- und Löschtransaktionen (EXT.18.4)	Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen von personenbezogenen Daten MÜSSEN protokolliert werden.

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

Verfügbarkeitskontrolle

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	
Test neuer Hard und Software * (EXT.8.2)	Es MUSS sichergestellt werden, dass der produktive Einsatz von Komponenten erst nach erfolgreichem Test und Freigabe erfolgt.
Durchführung von Datensicherungen (EXT.10.1)	Der Dienstleister SOLLTE Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.
Umsetzung eines Datensicherungskonzeptes (EXT.10.2)	Die Vorgaben des Auftraggebers zu Aufbewahrungszeiten und Wiederherstellungszeiten MÜSSEN umgesetzt werden können.
Bei erhöhtem Schutzbedarf für die Verfügbarkeit: **Durchführung von Datensicherung bei hohem Schutzbedarf** (EXT.10.3)	Bei hohem Schutzbedarf der Verfügbarkeit MUSS der Dienstleister Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.
Portabilität bei Vertragsende (EXT.15.1)	Bei Vertragsende MÜSSEN die Daten des Auftraggebers in elektronischen Standardformaten, wie z. B. CSV, XML, ZIP-Archiv portierbar und exportierbar sein.
Bei erhöhtem Schutzbedarf für die Verfügbarkeit: **Portabilität bei hohem Schutzbedarf** (EXT.15.2)	Eine Übertragung bzw. Rückführung der Daten MUSS möglich sein. Dazu MÜSSEN durch den Dienstleister entsprechende Schnittstellen, wie z.B. API, Protokolle bereitgestellt werden.
Notfallvorsorge (EXT.16.2)	Zur Schadensminimierung und weiterer Schadensabwehr MUSS der Dienstleister geeignete Verfahren zur Notfallvorsorge z.B. BCM etabliert haben.

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)	
Betrieb eines Schwachstellen- und Patchmanagements (EXT.4.1)	Der Dienstleister MUSS ein Verfahren für seine Verarbeitungsanlagen betreiben, das Schwachstellen erkennt, bewertet, priorisiert und zeitnah behebt. z.B. Patchmanagement, regelmäßige Penetrationstests
Erkennung und Abwehr von Cyberangriffen * (EXT.5.1)	Es MUSS ein geeigneter und aktueller Schutz vor Cyberangriffen nach dem aktuellen Stand der Technik eingerichtet sein. z.B. End-Point-Protection, Einbruchserkennungssysteme (IDS/IPS), zentrale Logauswertung (SIEM), Security Operation Center (SOC), Computer Emergency Response Team (CERT).
Incident-Response-Management (EXT.16.1)	Der Auftraggeber MUSS über alle ihn betreffende Sicherheitsvorfälle und deren mögliche Auswirkungen unverzüglich und in geeigneter Weise informiert werden. Dafür MÜSSEN Ansprechpartner beim Auftraggeber und beim Dienstleister benannt werden.

Angriffserkennung und -abwehr (EXT.16.3)	Es MÜSSEN Methoden und Technologien verwendet werden, um Cyberangriffe auf die Dienstleistung (z.B. DDoS, Brute-Force) zu erkennen und abzuwehren.

Unterweisung

Unterweisung in Datenschutz und Informationssicherheit (EXT.21.1)	Alle an der Erbringung der Dienstleistung beteiligten Personen MÜSSEN regelmäßig hinsichtlich der Datenschutz- und Informationssicherheitsvorschriften unterwiesen werden.

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

Überprüfung, Bewertung und Evaluierung

Zertifizierung von Rechenzentren (EXT.1.1)	Alle beteiligten Rechenzentren, MÜSSEN im Rahmen eines Information Security Management System (ISMS) betrieben werden, welches nach ISO/IEC 27001, BSI IT-Grundschutz oder einem vergleichbaren, anerkannten Standard zertifiziert ist. Eine gültige Zertifizierung für das ISMS MUSS vor Beauftragung nachgewiesen werden.
Fortführung der Zertifizierung gewährleisten und nachweisen (EXT.1.2)	Bei Ablauf der Zertifizierung während der Beauftragung MUSS der Dienstleister die Fortführung der entsprechenden Zertifizierung gewährleisten und nachweisen.
Bei erhöhtem Schutzbedarf für Vertraulichkeit, Integrität oder Verfügbarkeit: **Zertifizierung der Dienstleister bei hohem Schutzbedarf** (EXT.1.3)	Alle an der beauftragten Dienstleistung beteiligten Dienstleister MÜSSEN ein Information Security Management System (ISMS) nach ISO/IEC 27001, BSI IT-Grundschutz oder einem vergleichbaren, anerkannten Standard betreiben. Die Information Security Management Systeme SOLLTEN zertifiziert sein und eine gültige Zertifizierung vor Beauftragung nachgewiesen werden.

Weitere Maßnahmen bei erhöhtem Schutzbedarf

Bei erhöhtem Schutzbedarf für Vertraulichkeit, Integrität oder Verfügbarkeit: **Zusätzliche Anforderungen bei erhöhtem Schutzbedarf** * (EXT.22.1)	[Bei Bedarf durch Verantwortlichen (Auftraggeber) zu ergänzen]