Anlage Technische und organisatorische Maßnahmen (TOM)

Datenschutz und Geheimhaltung

hier: Verarbeitung personenbezogener Daten im Auftrag bzw. Verarbeitung von Sozialdaten im Auftrag

1. Gegenstand des Auftrags (Art. 28 Abs. 3 S.1 DSGVO)

Der Gegenstand des Auftrags ist die Durchführung der unter Ziffer 2 der Leistungsbeschreibung zum Rahmenvertrag ALLEGRO 2026 beschriebenen Aufgaben durch den Auftragnehmer.

Bei der Verarbeitung personenbezogener Daten handeln der Auftraggeber als Verantwortlicher im Sinne von Art. 4 Nr. 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung, im Folgenden: DSGVO) und der Auftragnehmer als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO.

Bei diesem Auftrag ist nicht ausgeschlossen, dass der Auftragnehmer Kenntnis von personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DSGVO, Sozialdaten im Sinne von § 67 Abs. 2 SGB X, Betriebs- und Geschäftsgeheimnissen i.S.d. § 35 Abs. 4 Erstes Buch Sozialgesetzbuch (SGB I) sowie besonderen Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO erlangt.

2. Kontrollrechte des Auftraggebers

Aufgrund der Kontrollverpflichtung des Auftraggebers vor Zuschlagserteilung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber vor Ort, das heißt an der Stelle, an der die Daten verarbeitet werden, die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO nach. Dazu hat der Auftragnehmer dem Auftraggeber nach vorheriger Terminvereinbarung Zutritt in seine Geschäftsräume und zu seiner IT zu gewähren, alle erforderlichen Auskünfte zu erteilen und Einsichtnahme in die gespeicherten Daten oder Dokumente zu ermöglichen.

Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach Wahl des Auftraggebers dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) erbracht werden.

Da zum derzeitigen Stand (09/2025) keine aktualisierten Zertifizierungen möglich sind, wird die Umsetzung der Datenschutzmaßnahmen vor Zuschlagserteilung vor Ort geprüft.

3. Technische und organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren technische und organisatorische Maßnahmen gemäß Art. 32 Abs. 1 lit. a) bis d) DSGVO. Für die im Auftrag zu verarbeitenden Daten sind dabei die Grundwerte der Informationssicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) mit „sehr hoch“ festgelegt.

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrages.
Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c), 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur 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.

Die Umsetzung der technischen und organisatorischen Maßnahmen dient zugleich der effektiven Sicherstellung der Rechte der von der Verarbeitung personenbezogener Daten Betroffenen, namentlich das Recht auf Information aus Art. 13 und 14 DSGVO, das Recht auf Auskunft aus Art. 15 DSGVO, das Recht auf Berichtigung aus Art. 16 DSGVO und das Recht auf Löschung („Recht auf Vergessenwerden“) aus Art. 17 DSGVO.

Als Nachweis für die Erfüllung der Anforderungen aus Art. 32 Abs. 1 DSGVO werden die folgenden Maßnahmen bestimmt:

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)		
lfd. Nr.	**Maßnahme**	**Umsetzung der Maßnahme**
1	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungs-anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Verschlossene Türen und Fenster • Fenstersicherung durch Fenstergitter und/ oder verschließbare Fenstergriffe (Erdgeschoss) • Teilautomatisiertes Zutrittskontrollsystem mit Personenschleuse und Ausweislesegeräten nebst Protokollierung der Zu- und Abgänge im Gebäude allgemein • Gesonderte Protokollierung der Zu- und Abgänge in den Rechnerräumen im Besucherbuch • Alarmanlage mit Anzeige im Meldeboard des Gebäudeleitsystems • Besucherregelung • Zutrittsregelung für betriebsfremde Personen • Pförtnerdienst • Erstellung und Pflege der betroffenen IT-Sicherheitskonzepte • Festlegung und Einrichtung von Sicherheitsbereichen gem. Infrastruktur- und Bauplänen
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		
2	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungs-systeme von Unbefugten genutzt werden können.	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • In Ausnahmefällen sind separate Zugänge möglich, die jedoch im Einzelfall von einem bevollmächtigten Mitarbeiter des Auftraggebers aktiviert werden müssen. Der Auftraggeber stellt hierfür einen zentral verwalteten Remote-Zugang als generellen Zugangspunkt zur Verfügung. • Anmeldung besteht aus einer Identifizierung (Benutzerkennung) und einer Authentifizierung (Passwort) der berechtigten Mitarbeiter (keine Systemverwalterprivilegien) • Die dem Auftragnehmer für die Durchführung des Fernzugriffs (Remote-Zugang) ggf. offenbarten Passwörter muss der Auftraggeber nach Beendigung der Fehlerbeseitigung unverzüglich ändern. • Protokollierung der Zugriffe auf IT-Systeme des Auftraggebers • Einsatz von Gateway- und Firewall-Rechnern sowie Einsatz mobiler IT-Systeme gem. Firewall-Policy

		• Durchführung einer Benutzerverwaltung einschließlich dezidierter Rechtezuweisung gem. Rollen- und Rechtekonzept des Auftraggebers. • Identifizierung und Authentifizierung der Mitarbeiter des Auftragnehmers gegenüber der Dienststelle der BA durch einen Lichtbildausweis/Dienstausweis. • Mitarbeiter/-innen des Auftragnehmers (=externer Dienstleister) tragen im Dienstgebäude der BA ein Namensschild mit Firmennamen.
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		
3	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Verarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Protokollierung der Systemnutzung (Datenzugriffe, nicht nur Logfiles), mindestens bis 90 Tage • Im Falle eines Fernzugriffs (Remote-Zugang) ist insbesondere der Zugriff auf personenbezogene Daten mit Datum, Uhrzeit und Benutzerkennung zu protokollieren und für ein Jahr zu Kontrollzwecken zu speichern. • Beim Fernzugriff auf Mitarbeiterdaten des Auftraggebers betreffend besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO wird der Auftragnehmer nur festangestellten Mitarbeitern Zugriffsberechtigungen erteilen. Der Auftragnehmer wird dem Auftraggeber zu Kontrollzwecken auf Verlangen die erteilten Zugriffsberechtigungen offenlegen. • Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Fehler beim Fernzugriff feststellt, die einen Zugriff durch Unbefugte möglich machen. Entsprechendes gilt für den Verdacht bei Datenschutzverletzungen. • gesicherte Aufbewahrung von Sicherungsbeständen • verfahrensspezifisches Rollen- und Berechtigungskonzept (Zugriffsberechtigungen sind nur zweckgebunden zulässig) • verfahrensspezifisches Zugriffskonzept • Anwendung des verfahrensspezifischen Datensicherungskonzeptes • Auswertung von Protokollen (anlassbezogen, Stichprobenkontrolle), Speicherung der Protokolldaten mindestens bis 90 Tage • Anwendung von Zugriffs-Regelungen gem. Rollen- und Berechtigungskonzept • Verwendung eines dem Stand der Technik entsprechenden Verschlüsselungsverfahrens.
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		
4	**Trennungsgebot** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Physische Trennung der Rechnersysteme (Entwicklungs-, Test-, Produktionssystem) • Trennung der Daten des Auftraggebers von den Daten des Auftragnehmers und anderer Mandanten mit entsprechender Verschlüsselung – mindestens logische Trennung • Das Speichern personenbezogener Daten des Auftraggebers in den IT-Systemen des Auftragnehmers ist nur mit ausdrücklicher Genehmigung des Auftraggebers für maximal 48 Stunden zum Zwecke der Fehlerbehebung zulässig. Die nachfolgende datenschutzkonforme Löschung der Daten ist dem Auftraggeber auf Wunsch nachzuweisen. Eine Vermischung mit anderen Daten des Auftragnehmers ist durch logische Trennung zu verhindern.
5	**Pseudonymisierung**	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Identifikationsmerkmale werden durch ein Kennzeichen ersetzt, dieses wird gesondert von den weiteren Daten aufbewahrt und es ist eine Funktion verfügbar, aus der sich die Zuordnung des Kennzeichens zu einer bestimmten Person ergibt.

	Die Verarbeitung 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, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 32 Abs. 1 lit. a) DSGVO, Art. 25 Abs. 1 DSGVO)	• Bildung der Kennzeichen durch Erzeugung von Zufallswerten und deren Zuordnung zum Betroffenen über eine Zuordnungsliste (Referenzliste) • Errechnung von Hashwerten von den identifizierenden Daten (keine Speicherung einer Zuordnungsliste) Die Verschlüsselung muss bewirken, dass die personenbezogenen Daten für alle Personen, die nicht zum Zugang befugt sind, unzugänglich gemacht werden (vgl. Art. 34 Abs. 3 lit. a) DSGVO)
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		

II. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)		
lfd. Nr.	**Maßnahme**	**Umsetzung der Maßnahme**
1	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Verschlüsselter Datentransfer – es sind ausschließlich die Protokolle SSH, VNC und X Windows einzusetzen. Das VNC- und das X-Windows-Protokoll müssen über SSH oder eine VPN-Verbindung geführt werden. Direkte VNC- oder X-Windows-Verbindungen sind nicht zugelassen. • Passwortabfrage gem. Passwortrichtlinie des Auftragnehmers • Datenschutzkonformes Löschen • Einsatz von Gateway-und Firewall-Rechnern gem. Firewall-Policy • Verwendung aktueller Antiviren-Software • Protokollierung von Datenverbindungen
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		
2	**Eingabekontrolle**	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Identifizierung und Authentifizierung der Berechtigten

	Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind.	• Protokollierung der Aktionen (Änderungen) • Durchführung der Netzverwaltung gem. Firewall-Policy • regelmäßige Auswertung Protokolle (anlassbezogen, Stichprobenkontrolle)
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)		
	Maßnahme	**Umsetzung der Maßnahme**
	Verfügbarkeitskontrolle Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Unterbrechungsfreie Stromversorgung (USV) • Brandmelder • Notfallkonzept und Notfallpläne • Benennung von Krisenmanagern • Festlegen von Katastrophenabwehrmaßnahmen gegen Feuer, Wasser, Einbruch, Bombendrohung, allgemeine Unruhen
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO, Art. 25 Abs. 1 DSGVO)		
lfd. Nr.	**Maßnahme**	**Umsetzung der Maßnahme**
1	**Kontrollverfahren** systematische und umfassende Kontrolle, Prüfung der technischen und organisatorischen Maßnahmen, Bewertung bezogen auf prognostiziertes Risiko, Wirksamkeit der technischen und Organisatorischen Maßnahmen testen	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: Kontrollmaßnahmen des Auftragnehmers, die unbefugten Zugriff verhindern. Die Maßnahme-Beschreibung erfolgt durch den Auftragnehmer. • bis auf Weiteres: alle 2 Jahre Kontrolle durch den Auftraggeber, das Ergebnis ist zu protokollieren, festgestellte Mängel hat der Auftragnehmer umgehend zu beseitigen • Auftragskontrolle siehe unten (Punkt 2)
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		
2	**Auftragskontrolle**	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Identifizierung und Authentifizierung der Berechtigten • Protokollierung der Aktionen, mindestens bis 90 Tage • Überprüfung anhand von Audits

	Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	• Regelmäßige Auswertung der Protokolle (anlassbezogen, Stichprobenkontrolle), Speicherung der Protokolldaten mindestens bis 90 Tage • Der Auftragnehmer stellt der zuständigen Dienststelle der BA von Vertragsbeginn an unaufgefordert eine namentliche Aufstellung der eingesetzten Mitarbeiter zur Verfügung. Jeder Veränderung dieser Aufstellung hat er schriftlich mitzuteilen.
Erläuterungen des Auftragnehmers, wenn Maßnahme(n) anderweitig umgesetzt werden:		

V.	**Standort der IT-Systeme**	Der Auftragnehmer sichert zu, dass die Verarbeitung der Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfindet. Der Datentransfer in einen Drittstaat ist unzulässig. Dies gilt auch bei der Beauftragung von weiteren Auftragnehmern oder der Inanspruchnahme von Cloud-Diensten.
VI.	**Sonstiges**	Nachfolgende Anforderungen zur Umsetzung werden erfüllt: • Durchführung einer Sabotageschutzprüfung entsprechend dem Sicherheitsüberprüfungsgesetz. • Es gelten die Regelungen der Hausordnung für externe Mitarbeiter des Auftraggebers (=externer Dienstleister) (siehe Anlage 1 zur Leistungsbeschreibung „Hausordnung für externe Dienstleister der Bundesagentur für Arbeit zur Einhaltung des Datenschutzes“).
VII.	**Telearbeit**	• Eine Verarbeitung von personenbezogenen Daten und/oder Sozialdaten in Privatwohnungen der Mitarbeiter des Auftragnehmers einschließlich der in häuslicher Gemeinschaft lebenden Personen (Telearbeitsplätze, Heimarbeitsplätze) ist nur mit vorheriger Zustimmung des Auftraggebers zulässig. • Die Telearbeitsplätze sind vom Datenschutzbeauftragten des Auftragnehmers regelmäßig auf Datenschutzkonformität zu prüfen/zu kontrollieren (d. h. mindestens vor Beginn der Telearbeit und laufend alle zwei Jahre). • Die Telearbeitsplätze sind so zu gestalten, dass unbefugte Dritte keine Kenntnis von personenbezogenen Daten nehmen können. • Der Transport dienstlicher Unterlagen muss in einem verschlossenen Behältnis (z. B. verschließbarer „Pilotenkoffer“) erfolgen. Außerhalb der Aufgabenerledigung sind dienstliche Unterlagen in der Arbeitsstätte verschlossen und gegen den Zugriff Dritter, dies gilt auch für Familienangehörige und Haushaltsangehörige, gesichert aufzubewahren. • Fehlausdrucke dürfen nicht im Hausmüll entsorgt werden, sondern sind in der Arbeitsstätte des Auftragnehmers einer datenschutzkonformen Vernichtung durch Einwurf in die entsprechenden Behälter zuzuführen.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer mit Ausnahme von Abs. 1 lfd. Nrn. I. 4, V., VI. und VII. gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei dürfen die festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Die im Vertrag vereinbarten Regelungen zum Datenschutz bleiben unberührt.

(3) Verfügt der Auftragnehmer bezüglich der allgemeinen, nicht auftragsspezifischen, technischen und organisatorischen Maßnahmen über ein umfassendes und aktuelles Datenschutz- und IT-Sicherheitskonzept, kann dies bei Vorlage und nach Prüfung durch den Auftraggeber die vorstehend festgelegten technischen und organisatorischen Maßnahmen ersetzen, solange das Niveau der oben

genannten Maßnahmen nicht unterschritten wird. Das Datenschutz- und IT-Sicherheitskonzept wird Grundlage des Auftrags und von dem Auftragnehmer in der jeweils aktuellen Fassung bei Anforderung des Auftraggebers diesem vorgelegt.

(4) Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen.