Fragen und Antworten zum Vergabeverfahren

Nr.	Bezug (Dokument, Kap., Seite,…)	Frage Bieter bzw. Bewerber	Antwort Beschaffungsamt des BMI
1	EVB IT Instandhaltungsvertrag Nr. 4.1 i.V.m. Leistungsbeschreibung, Kapitel 3.6.1	In Kapitel 4.1 des EVB-IT Instandhaltungsvertrags wird die langfristige Versorgungs- und Reparatursicherheit "von mindestens 6 Jahren ab dem Zeitpunkt der ersten Lieferung" gefordert. In der Leistungsbeschreibung hingegen wird diese "für einen Zeitraum von mindestens 6 Jahren ab dem Zeitpunkt der Lieferung" gefordert. Unserem Verständnis nach handelt es sich hierbei um einen Widerspruch und die Leistungsbeschreibung beschreibt ein nicht klar definierten längeren Zeitraum. Wir bitten um Klarstellung und darum, den gewünschten Zeitraum genau zu definieren, um objektive Vergleichbarkeit über alle Angebote zu gewährleisten	Die Versorgungs- und Reparatursicherheit beginnt gemäß der vorrangigen Leistungsbeschreibung für jedes Gerät individuell mit dessen tatsächlichem Lieferdatum. Die Erwähnung der „ersten Lieferung“ im Kaufvertrag markiert lediglich den generellen Start der Garantiepflichten im Projektverlauf.
2	Hinweis der Vergabestelle Aufgrund redaktioneller Fehler (Zahlendreher im Aktenzeichen), werden folgende Dokumente korrigiert bereitgestellt: • 01. Besondere Bewerbungsbedingungen V2 • 03. Aufforderungsschreiben V2 Zudem wurde im Dokument „19. Bewertungsmatrix Bodycams V2“ in Zeile 27 das fehlende Modul 7: Integration & Sicherheit (Kap. 7.3.7) aufgenommen, so dass nun alle Testmodule berücksichtigt werden. Beachten Sie bitte, dass Sie für die Angebotsabgabe nur noch dieses Dokument benutzen.		
3	Referenzen	Ist eine Eignungsleihe für die Teile der Referenzen zugelassen? Da kleine und mittelständische Unternehmen zugelassen sind, sollte dies möglich sein.	Ja, Ihre Annahme ist zutreffend.
4	EVB IT Instandhaltungsvertrag, Leistungsbeschreibung Kap. Nr. 3.6.4, Punkt 3	In der Leistungsbeschreibung, Kapitel 3.6.4, Punkt 3 (Kosten und Prozess) wird ein fester Reparaturpreis verlangt für Reparaturen außerhalb der 2-jähreigen Gewährleistung, der in das Preisblatt einzutragen ist. Dafür sieht das Preisblatt jedoch keine Eintragung vor. Wir bitten um Aufklärung und ggf. Korrektur des Preisblatts.	Sämtliche Leistungen im Zusammenhang mit dem RMA-Prozess gem. Kapitel 3.6.4 der Leistungsbeschreibung sind über die Pauschale der „Hardware-Wartung / Support je Bodycam-System“ des Preisblatts (Pos. 2) abgegolten. Beachten Sie hierzu auch die Klarstellung in Kapitel 3.6.4 der Leistungsbeschreibung.
5		Aus der Anlage 22. erlesen wir, dass es eingestuften Unterlagen gibt, die für das Vergabeverfahren wichtig sind und bitten um die Zusendung der dieser Unterlagen.	In diesem Verfahren sind sämtliche Vergabeunterlagen öffentlich zugänglich, eine Einschränkung von Inhalten aufgrund von VS-NfD Anforderungen ist von der Vergabestelle

			nicht vorgesehen. Auf Einzelabruf-Ebene kann dies jedoch zur Anwendung kommen. Bitte beachten Sie in diesem Zusammenhang § 14 Abs. 4 der Rahmenvereinbarung.
6	Vergabeunterlagen	Aufgrund der Komplexität und den benötigten Abstimmungen mit Herstellern und Lieferanten, inmitten der Urlaubszeit, bitten wir dringend um eine Angebots- und Bieterfragenfristverlängerung um mindestens 6 Wochen.	Ihrem Antrag auf eine sechs wöchige Verlängerung der Angebotsfrist kann nicht entsprochen werden. Gleichwohl wird die Angebotsfrist im Zusammenhang mit der Bereitstellung der nachstehend aufgeführten aktualisierten Vergabeunterlagen um eine Woche verlängert.
7	Hinweis der Vergabestelle Aufgrund redaktioneller Fehler (Zahlendreher im Aktenzeichen), werden folgende Dokumente korrigiert bereitgestellt: • 04. Angebotsformular V2 • 06. Vordruck Referenzen V2 • 07. Eigenerklärung Ausschlussgründe V2 • 08. Eigenerklärung Sanktionen Russland V2 • 09. Unternehmensdaten V2 • 12. Rahmenvereinbarung V2 • 14. Eigenerklärung Verpflichtungsgesetz V2 • 15. Verpflichtung Verpflichtungsgesetz mit Anlagen V2 • 19. Bewertungsmatrix - Bodycams V3 • 23. Anlage EVB-IT - Kaufvertrag (Langfassung) V2 • 24. Anlage EVB-IT - Kaufvertrag (Kurzfassung) V2 • 27. Anlage EVB-IT - Instandhaltungsvertrag V2 • 29. Anlage EVB-IT - Instandhaltung - Leistungsnachweis V2 • 31. Anlage EVB-IT - Cloudvertrag V2 • 33. Anlage EVB-IT - Cloud - Kriterienkatalog für Cloudleistungen V2 • 34. Bieterfragen-Antworten V4 • 35. Ansprechpartner zur Rahmenvereinbarung V2 • 36. Mustervereinbarung Auftragsverarbeitung V2 • 37. Bewerber Bietergemeinschaftserklärung V2 • 38. Verpflichtungserklärung Eignungsleihe Unteraufträge V2 • 39. Unteraufträge V2 • 40. Unternehmenszahlen V2		

	Beachten Sie bitte, dass die Angebotsfrist um 7 Kalendertage auf den 01.09.2026 verlängert wurde. Nutzen Sie für die Angebotsabgabe nur noch die aktualisierten Dokumente.		
8	Leistungsbeschreibung, M54	Die Ausschreibungsunterlagen setzen eine deutsche Sicherheitsüberprüfung der Stufe Ü1 voraus. Gemäß dem deutsch-britischen Sicherheitsabkommen wird die entsprechende britische Sicherheitsüberprüfung „Vertraulich“ für den Zugang zu VS-VERTRAULICH-Informationen gegenseitig anerkannt. Bitte bestätigen Sie, dass der Nachweis einer gültigen britischen Sicherheitsüberprüfung „Vertraulich“ für MSI-UK-Mitarbeiter als vollständige Erfüllung dieser Ausschreibungsanforderung akzeptiert wird. Bitte beachten Sie, dass die Bestimmungen des deutsch-britischen Sicherheitsabkommens zwingende Rechtskraft besitzen und deren Nichtbeachtung in einer Ausschreibung die Wettbewerbsfähigkeit des öffentlichen Vergabeverfahrens erheblich beeinträchtigt.	Ja, Ihre Anmerkung ist korrekt. Der Nachweis einer gültigen britischen Sicherheitsüberprüfung „Vertraulich“ für MSI-UK-Mitarbeiter wird als vollständige Erfüllung dieser Ausschreibungsanforderung akzeptiert.
9	Vergabeunterlagen	Wir bitten um Verlängerung der Angebotsfrist um mindestens zwei Wochen. Das Leistungsverzeichnis wurde gegenüber dem aufgehobenen Vorverfahren umfassend überarbeitet. Zur Prüfung der geänderten Anforderungen und Erstellung eines zuschlagsfähigen Angebots sind noch interne Abstimmungen, insbesondere mit Produktentwicklung, Technik, IT/SaaS, Informationssicherheit, Support und Kalkulation, erforderlich. Eine Fristverlängerung würde daher Wettbewerb stärken und die Einreichung wertbarer Angebote fördern.	Siehe Antwort auf Bieterfrage 6 sowie 7.
10	22. Verpflichtung VS-NfD und VS-NfD-Merkblatt; Leistungsbeschreibung; VSA §§ 49–50, 52, 55	Geltungsbereich VS-NfD und Schutzbedarfsfestlegung Aus den vorliegenden Unterlagen ist nach unserem Verständnis nicht eindeutig ableitbar, welche im Gesamtsystem erzeugten, übertragenen oder gespeicherten Informationen als VS-NfD eingestuft sind bzw. während der Vertragslaufzeit eingestuft werden können. Diese Festlegung ist für Architektur, Produktwahl, Betriebsmodell, Personal, Kommunikationswege und Kalkulation maßgeblich. Wir bitten daher um eine verbindliche Schutzbedarfs- bzw. Einstufungsmatrix für die wesentlichen Datenarten und Systembereiche. Bitte stellen Sie insbesondere klar, ob und in welchem Umfang die nachfolgenden Informationen bzw. Komponenten vom VS-NfD-Scope erfasst werden: • Video- und Audioaufzeichnungen einschließlich lokal auf der Bodycam gespeicherter Daten, • Metadaten, Zeit-, Standort-, Geräte-, Nutzer- und Zuordnungsinformationen, • Protokoll-, Audit-, Monitoring- und Security-Daten, • Konfigurationsdaten, Zertifikate, Schlüsselmaterial und Secrets,	Siehe hierzu bereits die Antwort auf Bieterfrage 5. Im vorliegenden Vergabeverfahren sind keine als VS-NfD eingestuften Vergabeunterlagen enthalten. Für die spätere Leistungserbringung gilt: Die Video- und Tondaten des polizeilichen Regeldienstes sind primär personenbezogene Daten und unterliegen dem Bundesdatenschutzgesetz (BDSG) sowie den IT-Sicherheitsanforderungen der Leistungsbeschreibung. Eine generelle Einstufung des gesamten Regelsystems oder aller Aufzeichnungen als VS-NfD erfolgt nicht.

		• Backups, Replikate, Snapshots, Exporte und temporäre Verarbeitungsdaten sowie • Management-, Administrations- und Supportsysteme, sofern von dort auf VS-relevante Systeme eingewirkt werden kann. Bitte stellen Sie außerdem klar, ab welchem Prozesspunkt die jeweilige Einstufung gilt und ob bzw. unter welchen Voraussetzungen eine Herabstufung gilt.	Die Verpflichtungserklärung VS-NfD (Anlage 22) sowie § 14 Abs. 4 der Rahmenvereinbarung sichern ab, dass der Auftragnehmer die materiellen und personellen Geheimschutzvorschriften einhält, sofern bei einzelnen operativen Einsätzen oder Abrufen im Einzelfall Verschlusssachen des Geheimhaltungsgrades VS-NfD anfallen.
11	Leistungsbeschreibung u. a. Ziff. 4.2.4; 33. Anlage EVB-IT – Cloud – Kriterienkatalog, M54; 22. Verpflichtung VS-NfD; VSA §§ 50, 52–55, 58	Kommunikation zwischen Bodycam, Dienststelle und Cloud sowie Auslegung „Zugriff“ in M54 Aus den Vergabeunterlagen geht nach unserem Verständnis nicht eindeutig hervor, wie die Kommunikations- und Übertragungswege zwischen den Bodycams und der Cloud-Infrastruktur sowie zwischen der IT-/Netzinfrastruktur der Bundespolizei und der Cloud-Infrastruktur technisch und organisatorisch ausgestaltet werden sollen. 1. Bitte beschreiben Sie die vorgesehene Zielarchitektur einschließlich Verantwortungs- und Übergabepunkten. Insbesondere bitten wir um Klarstellung, ob ein direkter mobiler Upload der Bodycam, eine Übertragung über Docking-/Dienststelleninfrastruktur oder beide Varianten vorgesehen sind und wer Mobilfunkanbindung, SIM/eSIM, APN/VPN bzw. andere gesicherte Übertragungswege bereitstellt und die laufenden Kosten trägt. 2. In diesem Zusammenhang bitten wir um Konkretisierung der Anforderung M54: Umfasst der dort verwendete Begriff „Zugriff“ bereits eine potenzielle technische Möglichkeit, auf Compute-, Plattform-, Speicher-, Netzwerk-, Sicherheits-, Administrations- oder Managementkomponenten einzuwirken, oder ausschließlich einen tatsächlichen Zugriff auf Daten, Aufzeichnungen, Metadaten oder Anwendungen der Bundespolizei? Bitte stellen Sie klar, welche Personengruppen und Zugriffsszenarien von M54 erfasst werden, insbesondere Administratoren und Betriebspersonal des Auftragnehmers, Unterauftragnehmer, Cloud-/RZ-Personal, Support- und Wartungspersonal, privilegierte Plattform-/Netzwerkadministratoren sowie Remote-Zugriffe. 3. Sofern VS-NfD betroffen ist, bitten wir um Klarstellung, ob neben den produktiven Systemen auch die Management- und Betriebsumgebungen in den Sicherheits-Scope fallen, von denen aus technisch oder administrativ auf die für die Bundespolizei bereitgestellte Infrastruktur eingewirkt werden kann. • IAM/PAM, Bastion-/Jump-Hosts und Administratorarbeitsplätze,	**Zu Frage 1: Kommunikationswege und Zielarchitektur:** Geschuldeter Mindeststandard ist gemäß Kapitel 3.4.3 (M32) der Leistungsbeschreibung der automatische, kabel- oder WLAN-gebundene Upload der Bodycams über die Dockingstationen an den Dienststellen der Bundespolizei in die Cloud. Die hierfür erforderliche behördliche Liegenschafts- und Netzinfrastruktur stellt die Auftraggeberin. Der Übergabepunkt in die Cloud-Infrastruktur richtet sich nach Ziffer 5.1 der EVB-IT Cloud-AGB. Die mobile Datenübertragung (LTE/5G) ist ein optionales Bewertungskriterium (B19/B20); hierfür erforderliche SIM-Karten/Mobilfunkverträge stellt im Bedarfsfall die Bundespolizei bereit. **Zu Frage 2: Auslegung des Begriffs „Zugriff“ in M54:** Gemäß Kapitel 4.2.4 (M54) der Leistungsbeschreibung sowie Ziffer 8.1 des EVB-IT Cloudvertrags erfasst die Anforderung Personal der Auftragnehmerin oder von Unterauftragnehmern, welches im Rahmen von Betrieb, Administration, 2nd/3rd-Level-Support oder Wartung administrativen bzw. logischen Zugriff auf die Cloud-Software, Mandantensysteme oder Produktivdaten der Bundespolizei besitzt oder erlangen kann.

		• Cloud-Control-Plane, Orchestrierung und Virtualisierungsmanagement, • KMS/HSM-, Backup-, Monitoring-, Logging- und Security-Management, • CI/CD-, Deployment- und Konfigurationsmanagement sowie • Support-/Wartungswerkzeuge, soweit diese Zugriff oder Konfigurationsänderungen ermöglichen. Bitte benennen Sie für diese Komponenten das jeweils geforderte Sicherheitsniveau und die Grenze zwischen VS-relevantem und nicht VS-relevantem Management-Scope.	Physisches Rechenzentrumspersonal ohne logische Zugriffsmöglichkeiten auf Kundendaten oder Applikationsebenen fällt nicht unter M54. **Zu Frage 3:VS-NfD Sicherheits-Scope:** Dies hat keine Relevanz, da in diesem Verfahren keine generelle VS-NfD-Einstufung besteht.
12	33. Anlage EVB-IT – Cloud – Kriterienkatalog, M54; 22. Verpflichtung VS-NfD; SÜG §§ 1, 8, 24 ff.	Personeller Geltungsbereich SÜ1 und Verhältnis zu M54 Für welche Personengruppen ist eine SÜ1 konkret erforderlich und an welches Zugriffskriterium knüpft die Anforderung an? Bitte stellen Sie insbesondere klar, ob die SÜ1 auch für Personal von Unterauftragnehmern, Cloud-/Rechenzentrumsbetreibern, Remote-Support, physischem Rechenzentrumsbetrieb sowie für Personen mit privilegiertem System- oder Managementzugriff gilt, obwohl technisch kein Zugriff auf Inhaltsdaten vorgesehen ist. Bitte erläutern Sie zudem das Verhältnis zwischen M54 und der SÜ1-Anforderung: Ist die tatsächliche Kenntnisnahme von Daten maßgeblich, die technische Möglichkeit zur Kenntnisnahme bzw. Einflussnahme oder bereits die Zugehörigkeit zu einer bestimmten Betriebsrolle? Sofern technische und organisatorische Maßnahmen – z. B. Trennung von Rollen, kundenseitige Schlüsselkontrolle oder technisch ausgeschlossener Klartextzugriff – den Anwendungsbereich reduzieren können, bitten wir um Beschreibung der hierfür anerkannten Voraussetzungen.	Eine SÜ1 (bzw. die gem. Antwort zu Bieterfrage 8 anerkannte gleichwertige Sicherheitsüberprüfung) ist für diejenigen Personen erforderlich, die mit der Administration der SaaS-Anwendung, dem privilegierten Support oder Systemeingriffen auf Bundespolizei-Instanzen betraut sind und hierbei potenziell Kenntnis von Daten oder Systemkonfigurationen erlangen können (vgl. Kap. 4.2.4 der Leistungsbeschreibung). Durch geeignete technische und organisatorische Maßnahmen (TOMs) – insbesondere strikte Mandantentrennung, Datenzugriffsverbote gem. Kap. 4.2.2 der Leistungsbeschreibung, verschlüsselte Datenspeicherung und rollenbasierte administrative Zugriffsbeschränkungen kann der Bieter den Kreis der berechtigten Personen auf das zwingend erforderliche Minimum begrenzen. Personal ohne Zugriffsmöglichkeit auf die Systeme oder Daten der Bundespolizei (z. B. operatives Facility-/Hardwarepersonal im Rechenzentrum) bedarf keiner SÜ1
13	§ 16 Rahmenvereinbarung; 33. Anlage EVB-IT – Cloud – Kriterienkatalog	§ 16 Rahmenvereinbarung – Drittstaatenjurisdiktion, Informationspflichten und zukünftige Souveränitätsanforderungen Wir verstehen § 16 der Rahmenvereinbarung dahingehend, dass die unabhängige Handlungsfähigkeit deutscher Sicherheitsbehörden geschützt und	**Zu § 16 der Rahmenvereinbarung:** Die Informationspflicht nach § 16 Abs. 2 der Rahmenvereinbarung greift, sobald für den Auftragnehmer eine konkrete Verpflichtung oder Notwendigkeit entsteht oder erkennbar

		ein möglicher Informationsabfluss an ausländische Sicherheitsbehörden transparent gemacht werden soll. Nicht eindeutig geregelt erscheint, welche Bedeutung der Eigentümer- und Kontrollstruktur sowie der Unterwerfung von Konzernunternehmen, Unterauftragnehmern oder eingesetzten Cloud-/Infrastrukturprovidern unter das Recht eines Drittstaates zukommt. Dies ist insbesondere vor dem Hintergrund extraterritorial wirkender Vorschriften relevant. So können z. B. nach dem US CLOUD Act erfasste Anbieter aufgrund eines wirksamen US-Rechtsakts zur Herausgabe von Daten verpflichtet sein, die sich außerhalb der USA befinden, soweit diese ihrer Verfügungs- bzw. Kontrollsphäre unterliegen. In bestimmten Fällen kann zugleich eine gesetzliche oder gerichtliche Beschränkung der Information des betroffenen Kunden bestehen. Bitte stellen Sie daher klar, ob bereits die abstrakte Unterworfenheit eines Bieters, beherrschenden Konzernunternehmens, Unterauftragnehmers oder Cloud-/Infrastrukturproviders unter eine Drittstaatenjurisdiktion für § 16 relevant ist oder ob § 16 erst bei Vorliegen einer konkreten gesetzlichen Herausgabe- bzw. Offenlegungspflicht greift. Wie ist die Informationspflicht zu erfüllen, wenn das einschlägige Drittstaatenrecht die Information über ein konkretes Herausgabeverlangen untersagt? Die Europäische Kommission hat am 3. Juni 2026 den Vorschlag für den Cloud and AI Development Act (CADA), COM(2026) 502 / 2026/0138(COD), vorgelegt; das Gesetzgebungsverfahren ist noch nicht abgeschlossen. Der Vorschlag adressiert unter anderem unterschiedliche Souveränitäts-/Assurance-Level und strukturelle Kriterien wie Drittstaatenabhängigkeiten sowie Eigentums- und Kontrollverhältnisse. Für dieses angestrebte Vertragsverhältnis werden die Regelungen der EU-Verordnung voraussichtlich während der Laufzeit verbindlich. Wie ist während der Vertragslaufzeit zu verfahren, wenn aufgrund zukünftiger verbindlicher europäischer oder nationaler Vorgaben ein höheres Souveränitätsniveau erforderlich wird, das der Auftragnehmer aufgrund seiner Konzern-, Eigentums-, Kontroll- oder Lieferkettenstruktur nicht erreichen kann? Bitte stellen Sie insbesondere Anpassungs-/Austauschpflichten, Beendigungsrechte und die Kostentragung einer regulatorisch erforderlichen Umstellung klar.	wird, die an der Einhaltung der Vertraulichkeit hindert oder einen Informationsabfluss begründen könnte. Eine rein abstrakte Unterwerfung verbundener Unternehmen unter ausländische Rechtsordnungen schließt eine Angebotsabgabe nicht aus, sofern durch vertragliche, technische und organisatorische Maßnahmen (u. a. Serverstandort EU gem. M53, Verschlüsselung gem. M50/M51, Vereinbarung zur Auftragsverarbeitung) die Hoheit über die Daten gewährleistet bleibt. **Zu künftigen regulatorischen Anforderungen:** Für während der Vertragslaufzeit in Kraft tretende gesetzliche oder behördliche Vorgaben gelten die Regelungen der EVB-IT Cloud-AGB (insb. Ziffern 1.2 und 2.1.3 zur Anpassung an geänderte Rechtsvorschriften) sowie § 14 der Rahmenvereinbarung.

14	Leistungsbeschreibung (SaaS / „über das Internet beziehbar“); 33. Anlage EVB-IT – Cloud – Kriterienkatalog für Cloudleistungen	Zulässiges Cloud-Betriebsmodell Welche Cloud-Betriebsmodelle sind für die Leistungserbringung zulässig? In den Vergabeunterlagen ist teilweise von SaaS und „über das Internet beziehbar“ die Rede. Bitte stellen Sie klar, ob ein SaaS auf einer marktüblichen Public-Cloud-Infrastruktur mit logisch dediziertem bzw. isoliertem Tenant zulässig ist oder ob darüber hinaus dedizierte physische Infrastruktur, eine Sovereign-Cloud-Ausprägung, eine Private Cloud oder ein anderes Betriebsmodell gefordert wird. Sofern mehrere Betriebsmodelle zulässig sind, bitten wir um Benennung der für alle Modelle einheitlich geltenden Mindestanforderungen, damit Sicherheitsniveau und Kalkulationsgrundlage der Angebote vergleichbar sind.	Gemäß Kapitel 4.2.1 der Leistungsbeschreibung und Ziffer 8.2 des EVB-IT Cloudvertrags ist ein SaaS-Modell auf Public- oder Multi-Tenant-Cloud-Infrastrukturen zulässig, sofern ein logisch isolierter Mandant (Tenant), eine strikte Mandantentrennung sowie die vollständige Einhaltung aller in Kapitel 4 definierten Mindestanforderungen gewährleistet sind. Hierzu zählen insbesondere: • Server- und Speicherstandort ausschließlich in der EU (M53), • Verschlüsselung AES-256 (At-Rest, M50) und TLS 1.3 oder höher (In-Transit, M51), • IT-Sicherheitskonzept nach BSI-Vorgaben/C5 (M49), • Einhaltung der SLAs und Verfügbarkeit von mind. 99,5 % (M83), • Vollständige Datenhoheit, REST-API und Export in Standardformaten (M46–M48, M82). Eine physisch dedizierte Private-Cloud-Infrastruktur wird nicht gefordert.
15	§ 16 Rahmenvereinbarung; 33. Anlage EVB-IT – Cloud – Kriterienkatalog; BSI-Mindeststandard zur Nutzung externer Cloud-Dienste	Daten-, Betriebs- und Supportstandorte sowie Unterauftragnehmerkette Aus den Unterlagen ist nach unserem Verständnis nicht abschließend ersichtlich, welche geografischen und juristischen Anforderungen für sämtliche Teile der Leistungskette gelten. Bitte stellen Sie verbindlich klar, in welchen Staaten die folgenden Leistungen erbracht bzw. Daten verarbeitet werden dürfen: • Produktivspeicherung und -verarbeitung, Replikation sowie Disaster-Recovery-Standorte, • Backups, Snapshots und Archive, • KMS/HSM und Schlüssel- bzw. Secret-Management, • Logging, Monitoring, Telemetrie und Security-Analytics sowie • Remote-Administration, Support und Incident-/Forensik-Leistungen.	**Speicher- und Betriebsstandorte:** Gemäß Kapitel 4.1.4 (M53) der Leistungsbeschreibung, Ziffer 8.2 des EVB-IT Cloudvertrags und Ziffer 4 der EVB-IT Cloud-AGB müssen alle Rechenzentren für Produktivspeicherung, Replikation, Backups, Archive und Schlüsselmanagement (KMS/HSM) ausnahmslos in der Europäischen Union (bevorzugt Deutschland) belegen sein. **Support und Administration:** Sämtliche Support- und Kommunikationsleistungen haben gemäß

		Bitte stellen Sie ferner klar, ob Zugriffe aus Drittstaaten – auch ohne dortige Datenspeicherung – zulässig sind und welche Anzeige-, Zustimmungs- oder Austauschpflichten bei Änderungen von Standorten, Unterauftragnehmern oder Cloud-/Rechenzentrumsprovidern während der Vertragslaufzeit gelten.	Kapitel 3.6.2 der Leistungsbeschreibung in deutscher Sprache zu erfolgen. **Zugriffe aus Drittstaaten und Unterauftragnehmer:** Zugriffe aus Drittstaaten auf personenbezogene Daten richten sich nach § 14 Abs. 2 der Rahmenvereinbarung i. V. m. Art. 44 ff. DSGVO. Der Einsatz und Wechsel von Unterauftragnehmern richtet sich nach Ziffer 15 der EVB-IT Cloud-AGB.
16	Vergabe-/Vertragsunterlagen Datenschutz; § 16 Rahmenvereinbarung; 33. Anlage EVB-IT – Cloud – Kriterienkatalog	Datenschutzrechtliche Rollen, Unterauftragnehmer und technische Nebenverarbeitung Bitte stellen Sie klar, welche datenschutzrechtliche Rollenverteilung für die Verarbeitung der durch die Bodycam-Lösung entstehenden personenbezogenen Daten nach den für die Bundespolizei einschlägigen Vorschriften vorgesehen ist und welche vertraglichen Datenschutzregelungen Bestandteil der Leistung werden. Insbesondere bitten wir um Klarstellung, ob und in welchem Umfang der Auftragnehmer bzw. seine Unterauftragnehmer Daten zu Support-, Telemetrie-, Sicherheits-, Abrechnungs- oder Produktverbesserungszwecken verarbeiten dürfen und ob eine Nutzung zu eigenen Zwecken ausgeschlossen ist. Bitte benennen Sie außerdem die Anforderungen an die Einbindung und Änderung von Unterauftragnehmern, internationale Zugriffe/Übermittlungen, Audit- und Kontrollrechte sowie die Trennung von Mandanten und Verarbeitungszwecken.	Die Bundespolizei ist verantwortlich für die Ausgestaltung der Regelungen. Die Auftragnehmerin erbringt die SaaS-Leistungen als Auftragsverarbeiter gemäß Art. 28 DSGVO (vgl. § 14 Abs. 2 der Rahmenvereinbarung, Ziffer 3.5.7 der Besonderen Bewerbungsbedingungen und Ziffer 6.1.3 der EVB-IT Cloud-AGB). Grundlage ist die Mustervereinbarung zur Auftragsverarbeitung (Anlage 36). Eine Verarbeitung von Bild-, Ton- oder Metadaten der Bundespolizei zu eigenen Zwecken des Auftragnehmers (z. B. Produktentwicklung, KI-Training, Profiling) ist strikt ausgeschlossen. Gemäß Kapitel 4.2.2 der Leistungsbeschreibung gilt ein umfassendes Datenzugriffsverbot für die Auftragnehmerin. Notwendige administrative Eingriffe sind auf Infrastrukturmaßnahmen zu beschränken und lückenlos zu protokollieren.
17	Leistungsbeschreibung Ziff. 4.5.3; 33. Anlage EVB-IT – Cloud – Kriterienkatalog; VSA §§ 50–52; BSI TR-02102-1	Verbindliches Schlüssel- und Verschlüsselungsmodell Den Vergabeunterlagen ist nach unserem Verständnis nicht eindeutig zu entnehmen, welches verbindliche Schlüssel- und Verschlüsselungsmodell für die Verarbeitung und Speicherung der Daten der Bundespolizei erwartet wird. Die möglichen Ausgestaltungen – beispielsweise Schlüssel in Hoheit der Auftraggeberin, BYOK/HYOK, Schlüsselmanagement durch Auftragnehmer bzw. Cloud-Provider oder ein Escrow-Modell – unterscheiden sich erheblich	Mindestanforderung gemäß Kapitel 4.1.2 (M50), Kapitel 4.5.3 der Leistungsbeschreibung und Ziffer 8.2 des EVB-IT Cloudvertrags ist eine dem Stand der Technik entsprechende AES-256-Verschlüsselung der ruhenden Daten (At-Rest) sowie TLS 1.3 oder höher für die Übertragung (M51).

		hinsichtlich Sicherheitsniveau, Zugriffsmöglichkeiten, digitaler Souveränität, Betriebsmodell und Kosten. Wird die Auswahl vollständig dem jeweiligen Bieter überlassen, könnten Angebote mit unterschiedlichen technischen Zugriffsmöglichkeiten und Sicherheitsniveaus miteinander verglichen werden. Wir bitten daher um verbindliche Festlegung bzw. Mindestanforderungen. • Muss die Schlüsselhoheit ausschließlich bei der Auftraggeberin liegen oder darf eine Verwaltung durch Auftragnehmer bzw. Cloud-/Infrastrukturprovider erfolgen? • Welche Modelle (AG-Key, BYOK, HYOK, AN-/Provider-Key, Escrow) sind zulässig? • Wo müssen KMS/HSM-Komponenten betrieben werden und wer darf technisch auf Schlüsselmaterial bzw. Schlüsseloperationen zugreifen? • Welche Anforderungen gelten für Rotation, Sperrung, Widerruf, Löschung, Backup und Recovery des Schlüsselmaterials? • Ist für kritische Schlüsseloperationen Dual Control/Vier-Augen-Prinzip erforderlich? • Wie sind Backups, Replikate, Snapshots, Protokoll- und Metadaten kryptografisch zu behandeln? Gehen wir recht in der Annahme, dass hierfür ein einheitliches Mindest-Sicherheitsniveau vorgegeben wird? Sofern mehrere Modelle zulässig sind, bitten wir um Klarstellung, wie unterschiedliche Sicherheits- und Souveränitätsniveaus in der Angebotswertung berücksichtigt werden.	Die technische Ausgestaltung des Schlüsselmanagements (KMS durch Cloud-Provider, BYOK oder Escrow-Verfahren) obliegt dem Bieter im Rahmen seines nach Mindestkriterium M49 einzureichenden IT-Sicherheitskonzepts. Entscheidend ist, dass KMS-Komponenten in der EU betrieben werden und organisatorisch sowie technisch sichergestellt ist, dass Unbefugte oder der Auftragnehmer keinen unberechtigten Klartextzugriff auf Videoaufnahmen erhalten. Die Bewertung erfolgt rein binär über die Erfüllung der Mindestkriterien M49, M50 und M51. Eine gesonderte Bepunktung alternativer Schlüsselarchitekturen erfolgt nicht.
18	Leistungsbeschreibung (Betrieb/Wartung/Updates); 33. Anlage EVB-IT – Cloud – Kriterienkatalog; VSA § 50 Abs. 8–9; BSI C5	Patch-, Update-, Schwachstellen- und Sicherheitsprüfmanagement Bitte stellen Sie klar, welche verbindlichen Anforderungen für Schwachstellenmanagement, Sicherheitsupdates und Änderungen der Bodycam-, Backend- und Cloud-Komponenten gelten. Bitte spezifizieren Sie insbesondere Fristen für die Bewertung und Behebung kritischer/hoher Schwachstellen, Verfahren für Zero-Day-Schwachstellen und Notfallpatches, regelmäßige Penetrations-/Sicherheitstests, Umgang mit Firmware- und Software-Signierung, Support-/EOL-Zeiträume sowie die Bereitstellung von Schwachstellen- bzw. Komponenteninformationen. Sofern VS-NfD betroffen ist: Welche Änderungen gelten als geheimschutzrelevant und bedürfen vor Umsetzung einer Zustimmung bzw. erneuten Prüfung/Freigabe? Wie ist mit dringenden Security-Patches zu verfahren, wenn die reguläre Freigabe noch nicht abgeschlossen ist?	Die verbindlichen Anforderungen und Fristen ergeben sich aus Kapitel 5.2 der Leistungsbeschreibung (M84, M85, M86) sowie Ziffer 9.2 des EVB-IT Cloudvertrags: **Sicherheits-Patches:** Bei Bekanntwerden von Sicherheitslücken sind Patches unverzüglich zu installieren. Die Auftraggeberin ist über Art, Umfang und Maßnahmen fortlaufend zu informieren (M85). **Software-Updates:** Reguläre Feature-Updates sind der Bundespolizei mindestens zwei Wochen im Voraus anzukündigen (M84).

			Bug-Fix-Zyklen: Regelmäßige Releases erfolgen monatlich, bei kritischen Fehlern ad-hoc (M86). **Bodycam-Firmware:** Gemäß Kapitel 3.1.11 (M8) sind Firmware-Updates für mindestens 6 Jahre ab Lieferung sicherzustellen
19	Leistungsbeschreibung (Betrieb/Sicherheitsmanagement); 33. Anlage EVB-IT – Cloud – Kriterienkatalog; VSA § 52; BSI C5	Security Logging, SOC/SIEM, Incident Response und Forensik Bitte konkretisieren Sie die Anforderungen an Sicherheitsprotokollierung, Überwachung und Behandlung von Sicherheitsvorfällen über die gesamte Lösungskette. Bitte stellen Sie insbesondere klar, welche Logs der Auftraggeberin in welcher Granularität und Latenz bereitzustellen sind, ob eine Anbindung an ein SOC/SIEM der Bundespolizei vorgesehen ist, welche Aufbewahrungsfristen und Zeitquellen gelten und welche Anforderungen an Manipulationsschutz, Zugriff und Einstufung der Logdaten bestehen. Weiterhin bitten wir um Vorgaben zu Meldefristen und Eskalationswegen bei Sicherheitsvorfällen, zur Sicherung forensischer Artefakte, zur Unterstützung der Auftraggeberin bei Analyse/Beweissicherung sowie zu Zugriffsrechten auf relevante Telemetrie und Provider-Nachweise. Bitte benennen Sie die Verantwortungsabgrenzung zwischen Auftraggeberin, Auftragnehmer, Cloud-Provider und weiteren Unterauftragnehmern für Detection, Response, Forensik und Wiederherstellung.	Die Anforderungen an das Logging ergeben sich aus Kapitel 4.2.2, Kapitel 4.3.4 (M71), Kapitel 4.5.4 (M79) und Kapitel 4.6.1 (M82) der Leistungsbeschreibung: Die Cloud-Software muss eine automatische, revisionssichere und unveränderbare Protokollierung aller Zugriffe und Bearbeitungen je Datei sowie aller administrativen Aktionen gewährleisten (wer, wann, was, IP-Adresse). Audit-Logs müssen über die REST-API (M48, M82) durch die Bundespolizei exportierbar sein. Bei Sicherheitsvorfällen (z. B. unberechtigter Datenzugriff, Infrastrukturangriff) greifen die Notfall-SLAs der Priorität P1 gemäß Kapitel 5.1 (M83) der Leistungsbeschreibung und Ziffer 9.1 des EVB-IT Cloudvertrags (Reaktionszeit max. 1–2 Stunden 24/7, Wiederherstellungszeit max. 4 Stunden).
20	Leistungsbeschreibung (SLA/Verfügbarkeit/Backup); 33. Anlage EVB-IT – Cloud – Kriterienkatalog; VSA §§ 49–50, 52	Verfügbarkeit, Backup, Wiederanlauf und Disaster Recovery Bitte spezifizieren Sie die verbindlichen Anforderungen an Verfügbarkeit und Wiederanlauf der Gesamtlösung. Insbesondere bitten wir um Vorgabe von RTO/RPO, erforderlicher Standort-/Zonenredundanz, Backup-Intervallen und -Aufbewahrung, Wiederherstellungstests, Notfallbetriebsverfahren sowie dem Verhalten bei Ausfall von Internet-/Mobilfunkanbindung oder Cloud-Komponenten. Bitte stellen Sie klar, ob Bodycams im Offline-Fall weiter aufzeichnen und wie lange Daten lokal sicher vorgehalten werden müssen bzw. dürfen und wie die	**Verfügbarkeit und SLAs:** Mindestverfügbarkeit von 99,5 % im Jahresmittel gem. Kapitel 5.1 (M83) der Leistungsbeschreibung und Ziffer 9.1 des EVB-IT Cloudvertrags. Wiederherstellungszeiten richten sich nach den Störungsklassen P1 bis P4 (P1 max. 4 Stunden).

		spätere sichere Synchronisation erfolgt. Wir bitten um Klarstellung, welche Anforderungen auch für Backup-/DR-Umgebungen und deren Management, Schlüsselmaterial, Standorte und Personal gelten.	**Datensicherung und Redundanz:** Mindestens tägliche automatisierte Datensicherung mit einer Aufbewahrung von mindestens 4 Wochen (M77) sowie redundante Infrastruktur/Rechenzentren (M78) gemäß Kapitel 4.5.2 der Leistungsbeschreibung. **Offline-Fähigkeit der Bodycams:** Gemäß Kapitel 3.2.1 (M10) verfügen die Bodycams über mindestens 64 GB internen Speicher (ausreichend für ca. 20–24 Stunden kontinuierliche Videoaufzeichnung). Die Kameras zeichnen im Einsatzfall autark ohne bestehende Netzwerkverbindung auf. Der Upload und die Synchronisation erfolgen fehlertolerant beim Einstecken in die Dockingstation (M32, M33).
21	Leistungsbeschreibung (Speicherung/Aufbewahrung/Löschung); 33. Anlage EVB-IT – Cloud – Kriterienkatalog; VSA § 56	Aufbewahrung, Löschung, Vertragsende und Exit Bitte stellen Sie verbindlich klar, welche Aufbewahrungs- und Löschfristen für Aufzeichnungen, Metadaten, Logs, temporäre Daten, Backups und Replikate gelten und durch wen diese gesteuert werden. Bitte konkretisieren Sie außerdem die Anforderungen an die vollständige Löschung bzw. kryptografische Unzugänglichmachung einschließlich verbleibender Backup-Kopien sowie die hierfür geforderten Nachweise. Für das Vertragsende bzw. einen Anbieterwechsel bitten wir um Vorgaben zum Datenexport in dokumentierten/offenen Formaten, zur Übergabe von Metadaten und Audit-/Integritätsinformationen, zur Übergangsunterstützung und zur Abschaltung/Löschung von Mandanten, Schlüsseln, Konten und administrativen Zugängen. Bitte stellen Sie klar, welche Exit-Leistungen im Angebot einzupreisen sind und wie zusätzliche Aufwände behandelt werden, die durch eine regulatorisch oder sicherheitstechnisch erforderliche Migration während der Vertragslaufzeit entstehen.	**Steuerung von Aufbewahrung und Löschung:** Löschfristen werden ausschließlich durch berechtigte Administratoren der Bundespolizei über die SaaS-Software konfiguriert und gesteuert (M57, M69). **Vertragsende und Exit:** Gemäß Kapitel 4.5.6 (M81), Kapitel 4.6.2 der Leistungsbeschreibung und Ziffer 3.2 des EVB-IT Cloudvertrags schuldet die Auftragnehmerin bei Vertragsende: • vollständigen Datenexport aller Videos und Metadaten in offenen Standardformaten (MP4, JSON/XML), • eine 12-monatige Aufbewahrungs- und Übergangsphase nach Vertragsende mit Zugriffsmöglichkeit für die Bundespolizei, • vollständige logische und physische Löschung der Daten nach Freigabe und Ablauf der Frist

			nebst Ausstellung eines Löschzertifikats. Diese Exit-Leistungen sind in die allgemeinen SaaS-Lizenzpreise einzupreisen und werden nicht gesondert vergütet.
22	Leistungsbeschreibung – BSI-Vorgaben; 33. Anlage EVB-IT – Cloud – Kriterienkatalog, M49; 22. Verpflichtung VS-NfD; VSA §§ 49–50; BSI-Mindeststandard externe Cloud-Dienste V2.1	Verbindliches BSI-/C5-/VS-NfD-Nachweisniveau In der Leistungsbeschreibung wird die Einhaltung einschlägiger Vorgaben und Empfehlungen des BSI gefordert. Gleichzeitig werden als Nachweis ein C5-Testat bzw. eine gleichwertige Dokumentation genannt. Bitte konkretisieren Sie, welches Sicherheits- und Nachweisniveau tatsächlich verbindlich ist. Bitte stellen Sie insbesondere klar, ob der BSI-Mindeststandard zur Nutzung externer Cloud-Dienste in der Bundesverwaltung anzuwenden ist und wie sich dessen Anforderungen zu C5, IT-Grundschutz und – sofern VS-NfD verarbeitet wird – den Anforderungen an die Freigabe von VS-IT nach der VSA verhalten. Welches Testat-/Zertifizierungs-/Freigabeniveau muss bei Angebotsabgabe und welches spätestens zum Wirkbetrieb vorliegen? Ist ein aktueller C5-Typ-2-Bericht verpflichtend oder genügt die in M49 genannte gleichwertige Dokumentation? Was wird konkret als gleichwertig anerkannt und wie ist der Nachweis zu führen?	Gemäß Kapitel 4.1.2 (Mindestkriterium M49) der Leistungsbeschreibung ist mit dem Angebot ein dokumentiertes IT-Sicherheitskonzept einzureichen. Als Nachweis der Umsetzung werden akzeptiert: • ein aktuelles BSI-C5-Testat (Typ 1 oder Typ 2) **oder** • ein vergleichbarer unabhängiger Prüfbericht **oder** • eine gleichwertige, prüffähige Dokumentation (z. B. auf Basis eines nach ISO/IEC 27001 zertifizierten ISMS in Verbindung mit einer detaillierten Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen). Ein C5-Typ-2-Testat ist somit nicht zwingend alleiniger Nachweis, sofern die Gleichwertigkeit der dokumentierten Sicherheitsmaßnahmen zweifelsfrei dargelegt wird.
23	22. Verpflichtung VS-NfD und VS-NfD-Merkblatt im Anhang; Vergabeunterlagen/Angebotsfrist	Bereitstellung VS-NfD-eingestufter Vergabe- und Vertragsinformationen Welche als VS-NfD eingestuften Vergabe-/Vertragsinformationen werden erst nach Eingang der Verpflichtungserklärung bereitgestellt? Bitte stellen Sie klar, bis wann ein Bieter diese Informationen vor Ablauf der Angebotsfrist erhält und ob sich hieraus Anforderungen ergeben können, die Einfluss auf Architektur, Kalkulation, Eignung, Nachweise oder die Auswahl von Unterauftragnehmern haben. Sofern solche Informationen erst nach Abgabe der Verpflichtungserklärung bereitgestellt werden, bitten wir um Bestätigung, dass den Bietern eine angemessene Frist zur Prüfung und Berücksichtigung im Angebot verbleibt.	Siehe Antwort auf Bieterfrage 5. Sämtliche für das Vergabeverfahren und die Angebotserstellung relevanten Vergabeunterlagen sind öffentlich über die e-Vergabeplattform abrufbar. Es existieren keine gesonderten, als VS-NfD eingestuften Unterlagen, die den Bietern erst nach Einreichung der Verpflichtungserklärung zugänglich gemacht würden.

24	33. Anlage EVB-IT – Cloud – Kriterienkatalog für Cloudleistungen; Zelle A18 / Kriterien M1–M93	Prüflogik der Mindestkriterien / Bewertungsmatrix Bitte bestätigen Sie die korrekte Logik zur Prüfung der Mindestkriterien und stellen Sie eine korrigierte Bewertungsmatrix bereit. Die Formel in A18 prüft COUNTIF(F30:F121;"Ja")=95, obwohl dieser Bereich nach der vorliegenden Fassung nur die Kriterien M1–M92 umfasst und M93 in Zeile 122 steht. Bitte bestätigen Sie, welche Kriterien und welche Anzahl positiver Antworten für die Erfüllung der Mindestkriterien tatsächlich maßgeblich sind.	Maßgeblich für die Angebotswertung ist die vollständige und ausnahmslose Erfüllung aller 93 Mindestkriterien (M1 bis M93) gemäß Kapitel 8.1 der Leistungsbeschreibung. Die Formel in Zelle A18 diente lediglich als redaktioneller Prüfhinweis. Das Dokument „19. Bewertungsmatrix - Bodycams“ wurde in der Formel korrigiert und wird als V4 aktualisiert bereitgestellt.
25	Leistungsbeschreibung/EVB-IT Cloudvertrag/EVB-IT Clud Kriterienkatalog; SLA P1-P4	Einige der vorgeschlagenen Lösungszeiten einzuhalten, wird für uns eine Herausforderung darstellen, da bestimmte Zielvorgaben, insbesondere bei Problemen mit niedrigerer Priorität, nicht dem Branchenstandard entsprechen. Wir schlagen vor, diese anzupassen, damit wir einen zuverlässigen und robusten Service erbringen können. Wir bitten daher um Akzeptanz der Vorschläge wie folgt: ● **P1 - 4 Stunden** - Keine Änderung vorgeschlagen. ● **P2 - 72 Stunden** - Die Erwartung einer Behebungszeit von 12 Stunden für P2-Probleme geht von einfachen Konfigurationsänderungen aus; Fehlerbehebungen im Softwarecode erfordern jedoch Build-Pipelines, automatisierte Tests und sichere Deployment-Strategien. Ein Zeitfenster von 72 Stunden für die Lösung ermöglicht es unserem Team, die Fehlerursache zu untersuchen, einen Fix zu entwickeln, vollständige Regressions- und Sicherheitstests durchzuführen und einen Hotfix sicher bereitzustellen. Dies stellt sicher, dass der Fix funktioniert und keine anderen wesentlichen Funktionen beeinträchtigt. ● **P3 - 42 Tage** - Ein Zeitfenster von 42 Tagen entspricht den standardmäßigen, sicheren agilen Entwicklungszyklen (üblicherweise zwei Sprints). Dies ermöglicht es, Bugs mit geringen Auswirkungen in unseren regulären, strengen Release-Zyklus einzuplanen, um sicherzustellen, dass sie mit vollständiger Qualitätskontrolle behoben werden. ● **P4 - 90 Tage** - Bei kosmetischen Fehlern ohne Auswirkungen auf den Betriebsablauf entspricht ein 90-Tage-Fenster den üblichen vierteljährlichen Wartungs-Releases. Dies verhindert, dass unser Entwicklungsteam durch Tippfehler oder UI-Ausrichtungen abgelenkt wird, und hält den Fokus auf wichtigen Prioritäten wie Systemstabilität	Unter Berücksichtigung der operativen Einsatzanforderungen der Bundespolizei sowie branchenüblicher Release- und Testzyklen werden die Service-Level-Agreements (SLA) in Kapitel 5.1 der Leistungsbeschreibung sowie in Ziffer 9.1 des EVB-IT Cloudvertrags wie folgt angepasst: • **Klasse P1 (Kritisch):** Unverändert (Reaktionszeit max. 1–2 h 24/7, Wiederherstellungszeit max. 4 h) • **Klasse P2 (Hoch):** Unverändert (Reaktionszeit max. 4 h, Wiederherstellungszeit max. 12 h) • **Klasse P3 (Mittel):** Reaktionszeit max. 8 h, Wiederherstellungszeit **max. 48 h** (bisher 24 h) • **Klasse P4 (Niedrig):** Reaktionszeit max. 24 h, Wiederherstellungszeit **max. 120 h** (bisher 72 h) **Ergänzend wird klargestellt:** Bei Störungen der Klassen P3 und P4 kann im Einzelfall in Abstimmung und im Einvernehmen mit den zuständigen Systemadministratoren der Bundespolizei entschieden werden, die Fehlerbehebung in den regulären Software-Wartungs- bzw. Release-Zyklus zu überführen. Die Vergabeunterlagen (Leistungsbeschreibung Kap. 5.1 und EVB-IT Cloudvertrag Ziff. 9.1)

		und Sicherheit.	werden entsprechend angepasst. Beachten Sie bitte die neu bereitgestellten Dokumente: • 13. Leistungsbeschreibung V3 • 31. Anlage EVB-IT - Cloudvertrag V3
26	EVB-IT - Kaufvertrag (Langfassung)	Um das lukrativste kommerzielle Angebot zu ermitteln, bitten wir um die Verkürzung der Zahlungsziele von 90 auf 60 Tage.	Ihrem Antrag wird entsprochen und die Änderungen wurden im Dokument „23. Anlage EVB-IT - Kaufvertrag (Langfassung) V3“ unter Ziff. 7.1 aktualisiert.
27	**Hinweis der Vergabestelle** Aufgrund einer umfassenden Überarbeitung der Vergabeunterlagen und um allen Bietern eine verlässliche und kalkulationssichere Angebotserstellung auf Basis der aktualisierten Unterlagen zu ermöglichen, wird die Angebotsfrist um drei Wochen auf den 22.09.2026 verlängert. Die aktualisierten Dokumente werden Ihnen in Kürze über die e-Vergabe-Plattform bereitgestellt.		
28	Allgemein	Wir bereiten derzeit ein Angebot zu diesem Verfahren vor und möchten aufgrund des Umfangs der Leistungsbeschreibung (97 Seiten, 93 Mindest- und 46 Bewertungskriterien über Hardware, Cloud-Software, IT-Sicherheit und Service) sowie der für ein vollständiges Angebot erforderlichen Einbindung spezialisierter Partnerunternehmen anfragen, ob eine Verlängerung der Angebotsfrist um 10 Tage möglich ist. Eine etwas großzügigere Bearbeitungszeit würde aus unserer Sicht mehr belastbare, vollständig ausgearbeitete Angebote ermöglichen.	Siehe Antwort auf Bieterfrage 27.

Hinweis 1: Für den Inhalt der Fragen sind die Fragestellenden verantwortlich!
Hinweis 2: Neue Fragen und Antworten sind gelb unterlegt, Änderungen zur Vorversion sind grün unterlegt!!
Hinweis 3: Bitte prüfen Sie, ob alle Ihre Fragen vollständig und richtig in die Bieterinformationen übernommen wurden!
Fehlende und fehlerhafte Fragen sind der Vergabestelle unverzüglich zu melden.

Hinweis 4: Bitte beachten Sie, dass Bieterfragen zum Verfahren spätestens 8 Tage vor Ablauf der Angebotsfrist übermittelt werden sollen. Spätere Anfragen können unberücksichtigt bleiben.