



Leistungsbeschreibung zu dem Vergabeverfahren

Rahmenvereinbarung über Bodycams inkl. Software-as-a-Service

Az. ZIB 15.03 - 0618/26/VV : 1

Offenes Verfahren

Inhalt

1.	Allgemeines.....	7
1.1	Anlass.....	7
1.2	Ausschreibungsart und Leistungsumfang.....	7
1.3	Mengengerüst und Abrufsicherheit	7
2.	Leistungsumfang	8
2.1	Klassifizierung der Anforderungen	8
2.1.1	Mindestanforderungen (gekennzeichnet mit M).....	8
2.1.2	Bewertungskriterien (gekennzeichnet mit B)	9
2.2	Überblick über die Mindestanforderungen	9
3.	Anforderungen an die Bodycam-Hardware	11
3.1	Grundlegende Eigenschaften und Einsatzumgebung.....	11
3.1.1	Gewicht und Tragbarkeit.....	11
3.1.2	Befestigung und Kompatibilität mit Uniformteilen und Ausrüstungsgegenständen	12
3.1.3	Intuitive Bedienbarkeit und Nutzerführung	12
3.1.4	Bedienbarkeit mit und ohne Handschuhe.....	13
3.1.5	Schutzklasse und Widerstandsfähigkeit	13
3.1.6	Falltests und mechanische Robustheit.....	14
3.1.7	Temperaturbereich	14
3.1.8	Display und visuelle Deeskalation	15
3.1.9	Schnellregistration von Einsatzkraft und Bodycam (RFID)	15
3.1.10	Automatisierte Auslösung beim Ziehen von weiteren Führungs- und Einsatzmitteln (FEM, Distanz-Elektroimpulsgerät sowie dienstlicher Schusswaffe) aus dem Holster	16
3.1.11	Firmware-Pflege und Update-Management	16
3.2	Speicher und Datenverwaltung	17
3.2.1	Interner Speicher und Backup.....	17
3.2.2	GNSS/GPS und Geo-Tagging.....	18
3.2.3	Manipulationssicherer Zeitstempel	19
3.2.4	Schutz gegen unbefugten Zugriff und Datenlöschung	19

3.2.5	Pre-Event-Recording (Vorlaufaufnahme)	20
3.3	Videoqualität und Aufnahmeformat	20
3.3.1	Auflösungsoptionen und Bildwiederholfrequenz	20
3.3.2	Video-Codec und Kompression	20
3.3.3	Bildstabilisierung	21
3.3.4	Sichtfeld und Kamera-Schwenkbereich.....	21
3.3.5	Mikrofonanforderungen und Audioqualität	22
3.3.6	Akustisches Startsignal	22
3.3.7	Optische und andere Benachrichtigungen.....	23
3.4	Schnittstellen und Konnektivität	23
3.4.1	USB-C Anschluss	23
3.4.2	WiFi-Konnektivität.....	24
3.4.3	Automatischer Cloud-Upload.....	24
3.4.4	Mobile Netzwerk-Unterstützung und Live-Streaming	24
3.4.5	Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten	25
3.5	Akku und Ladeinfrastruktur	27
3.5.1	Akku-Anforderungen	27
3.5.2	Externe Akku-Ladeinfrastruktur (Stand-Alone).....	28
3.5.3	Multi-Dockingstationen und Kombi-Ladefunktion.....	28
3.5.4	Firmware-Updates über Dockingstation	29
3.6	Reparatur und Wartung.....	30
3.6.1	Langfristige Versorgungs- und Reparatursicherheit.....	30
3.6.2	Kommunikation in deutscher Sprache	30
3.6.3	Hotline-Support und Reaktionszeiten	30
3.6.4	Instandsetzung und Austausch-Service (RMA-Prozess)	31
4.	Cloud-Software und SaaS-Modell	32
4.1	Grundlegende Prinzipien und Anforderungen	33
4.1.1	Digitale Souveränität und Vendor-Lock-In-Vermeidung	33
4.1.2	IT-Sicherheit und Verschlüsselung	33
4.1.3	Barrierefreiheit nach BITV 2.0	34
4.1.4	Server-/Speicherort in der Europäischen Union	35

4.2	SaaS-Betriebsmodell und Verantwortlichkeiten.....	35
4.2.1	Definition des SaaS-Modells.....	35
4.2.2	Verantwortlichkeiten der Auftragnehmerin	36
4.2.3	Verantwortlichkeiten der Bundespolizei.....	37
4.2.4	Personelle Sicherheit und Geheimschutz.....	37
4.3	Funktionale Anforderungen an die Cloud-Software.....	38
4.3.1	Grundlegende Funktionen	38
4.3.2	Erweiterte Such- und Filterfunktionen.....	39
4.3.3	Videobearbeitung und Verarbeitung	39
4.3.4	Verwaltungsfunktionen	40
4.3.5	Spezielle Funktionen als Bewertungskriterien	41
4.4	Rollen- und Berechtigungskonzept.....	42
4.4.1	Die neun Rollenprofile.....	42
4.4.2	Beispielszenarien	45
4.4.3	Sonderfunktionen zur Zugriffsberechtigung.....	45
4.5	Cloud-Infrastruktur und Speicherung	46
4.5.1	Speicherplatz und Skalierbarkeit.....	46
4.5.2	Datensicherung und Redundanz	46
4.5.3	Verschlüsselung nach BSI-Standards.....	47
4.5.4	Protokollierung nach BDSG	47
4.5.5	Warnmeldungen und Speicherverwaltung	47
4.5.6	Datenlöschung nach Vertragsende	48
4.6	Interoperabilität und Vendor-Lock-In-Vermeidung.....	48
4.6.1	REST-API	48
4.6.2	Datenexport in standardisierten Formaten	49
4.6.3	Container-Technologie und Cloud-Portabilität	49
5.	Service und Support.....	49
5.1	Service-Level-Agreements (SLAs).....	49
5.2	Cloud-Software-Update und Sicherheitsupdates	50
6.	Schulung und Dokumentation	51
6.1	Schulungsanforderungen.....	51

6.1.1	Multiplikator-Schulungen.....	51
6.1.2	Timing und Koordination.....	52
6.1.3	Schulungsmaterial	52
6.1.4	Reisekosten	52
6.2	Dokumentation und Bedienungsanleitungen.....	52
6.2.1	Bodycam-Bedienungsanleitung.....	52
6.2.2	Cloud-Software-Bedienungsanleitung	53
6.2.3	Technische Dokumentation.....	53
7.	Teststellung und funktionaler Labortest.....	53
7.1	Gegenstand der Teststellung.....	54
7.2	Organisatorische Rahmenbedingungen	54
7.2.1	Zeitpunkt und Dauer der Teststellung.....	54
7.2.2	Testort und Infrastruktur.....	55
7.2.3	Bereitzustellende Geräte und Zubehör	55
7.2.4	Anwesenheit und Mitwirkung der Bieter	56
7.2.5	Testkommission und Bewertungsgremium.....	57
7.2.6	Dokumentation und Protokollierung	57
7.3	Testszenarien und Prüfkriterien	58
7.3.1	Testmodul 1: Hardware – Ergonomie & Robustheit	58
7.3.2	Testmodul 2: Video & Audio	59
7.3.3	Testmodul 3: Konnektivität & Akku.....	61
7.3.4	Testmodul 4: Cloud-Grundfunktionen	63
7.3.5	Testmodul 5: Speicher & Warnung	65
7.3.6	Testmodul 6: Spezielle Features & Interoperabilität	66
7.3.7	Testmodul 7: Integration & Sicherheit	67
7.4	Bewertung und Punktevergabe	69
7.4.1	Grundsätze	69
7.4.2	Zusammenführung mit der schriftlichen Bewertung	69
7.4.3	Umgang mit Testausfällen und technischen Problemen	69
8.	Liste aller in der Leistungsbeschreibung vorkommenden Kriterien	70
8.1	Mindestkriterien	70

8.2	Bewertungskriterien	94
-----	---------------------------	----

1. Allgemeines

Dieses Kapitel beschreibt den Anlass und den Rahmen der Beschaffung. Es legt die Ausschreibungsart, den Leistungsumfang und das Mengengerüst fest und schafft damit die verbindliche Grundlage für alle nachfolgenden Anforderungen und Bewertungsvorgaben. Alle in diesem Verfahren eingereichten Angebote müssen auf den hier beschriebenen Rahmenbedingungen basieren.

1.1 Anlass

Die Bundespolizei befindet sich in einem kontinuierlichen Prozess der Modernisierung ihrer Ausrüstung und der Stärkung ihrer Einsatzfähigkeit im Dienste der öffentlichen Sicherheit. Im Rahmen dieses Modernisierungsprozesses hat die Bundespolizei einen Bedarf an moderner, feldgestützter Videodokumentation identifiziert. Dieser Bedarf resultiert aus der Notwendigkeit, Einsatzsituationen bereits frühzeitig, aufgrund der Möglichkeit diese in Bild- und Ton festzuhalten, zu deeskalieren und somit Gefahren von Einsatzkräften und Dritten abzuwehren. Zudem ermöglicht die körpernah getragene Videotechnik Polizeieinsätze nachvollziehbar und transparent zu dokumentieren, Beweise für gerichtliche Verfahren zu sichern und die Einsatztaktik durch objektive Dokumentation zu unterstützen.

Zu diesem Zweck veranlasst das Beschaffungsamt des Bundesministeriums des Innern die Beschaffung von Bodycams in Verbindung mit einer cloudbasierten Software-Infrastruktur (SaaS-Dienst) zur Verwaltung, Speicherung, Archivierung und Verarbeitung der erfassten Aufnahmen. Diese Leistungsbeschreibung regelt die geforderten Leistungen und legt hierbei die technischen, funktionalen, organisatorischen und wirtschaftlichen Anforderungen fest.

1.2 Ausschreibungsart und Leistungsumfang

Diese Beschaffung erfolgt in einem offenen Verfahren als Rahmenvereinbarung in Form einer Ein-Los-Ausschreibung. Dies bedeutet, dass alle erforderlichen Leistungen bestehend aus Hardware (Bodycams und Zubehör), Software (cloudbasierte Verwaltungs- und Speicherlösung als SaaS-Dienst), Service (technischer Support und Wartung), Schulung und Dokumentation von einer einzigen Auftragnehmerin aus einer Hand erbracht werden müssen. Dieses Vorgehen ermöglicht eine nahtlose Integration, durchgehende Verantwortlichkeit und vereinfachte Kommunikation über alle Leistungskomponenten hinweg.

Die Rahmenvereinbarung wird für eine Laufzeit von maximal vier Jahren (initial zwei Jahre + optionale Verlängerung von bis zu zweimal für jeweils ein weiteres Jahr) geschlossen.

1.3 Mengengerüst und Abrufbarkeit

Folgendes Mengengerüst wurde für diese Beschaffung festgestellt:

Eine Mindestabnahmemenge von 2.500 Bodycam-Systemen stellt die garantierte Abnahmemenge dar, auf die sich die Auftragnehmerin einstellen muss. Diese Mindestmenge ist Bestandteil der

Rahmenvereinbarung und wird als verlässliche Nachfrage von der Bundespolizei zugesichert. Die Bundespolizei wird diese Menge über die oben genannte Vertragslaufzeit hinweg kontinuierlich in Einsatz nehmen und in ihren operativen Diensten verwenden.

Zusätzlich zur Mindestabnahmemenge besteht die Möglichkeit, bis zu 2.250 weitere Bodycam-Systeme über die Rahmenvereinbarung abzurufen. Diese Abrufmenge ist nicht mit einer Abnahmeverpflichtung verbunden. Die Bundespolizei kann jedoch während der Vertragslaufzeit beschließen, diese zusätzlichen Geräte in Anspruch zu nehmen, falls dies operativ notwendig ist.

Die maximale Gesamtabnahmemenge beträgt somit 4.750 Bodycam-Systeme. Sollte die operative Anforderung die Mindestmenge übersteigen, können weitere Abrufe bis zu diesem Maximum erfolgen, ohne dass ein neues Ausschreibungsverfahren erforderlich wäre. Dies gewährleistet Planungssicherheit für beide Seiten und ermöglicht eine flexible Skalierung in Abhängigkeit von der tatsächlichen Einsatzentwicklung und Ressourcenallokation.

2. Leistungsumfang

Dieses Kapitel definiert das Klassifizierungssystem für alle Anforderungen dieser Leistungsbeschreibung. Es erläutert, nach welcher Systematik Anforderungen als Mindestanforderungen oder als Bewertungskriterien eingestuft werden, und gibt einen strukturierten Überblick über die sechs Kernleistungen, die von der Auftragnehmerin zwingend zu erbringen sind. Das Verständnis dieser Klassifizierung ist Voraussetzung für die korrekte Interpretation aller nachfolgenden Kapitel.

2.1 Klassifizierung der Anforderungen

Die nachfolgenden Anforderungen sind in drei Kategorien eingeteilt, die unterschiedliche Grade der Verbindlichkeit und Flexibilität widerspiegeln. Dieses Klassifizierungssystem ermöglicht es dem Beschaffungsamt des BMI, klare Minimalstandards zu definieren, gleichzeitig aber auch Raum für Innovation und Optimierung in Bereichen zu schaffen, die nicht ausschließlich dem Minimalschutz dienen.

2.1.1 Mindestanforderungen (gekennzeichnet mit M)

Die als Mindestanforderungen gekennzeichneten Anforderungen sind nicht verhandelbar und **müssen** ohne Ausnahme und ohne Einschränkung vollständig **erfüllt werden**. Bieter, die diese Anforderungen nicht in vollem Umfang erfüllen, werden vom Vergabeverfahren ausgeschlossen. Mindestanforderungen stellen sicher, dass die beschaffte Lösung grundsätzlich die Anforderungen der Bundespolizei erfüllt und interoperabel mit bestehenden oder geplanten Systemen ist.

Diese Anforderungen konzentrieren sich auf Aspekte der Sicherheit, der Funktionalität, der rechtlichen Konformität und der operativen Grundlagen. Ein Beispiel für eine Mindestanforderung ist die Forderung nach integrierten Bodycams mit eingebauter Kamera, Mikrofon, lokalem Speicher und Konnektivität, nicht etwa separate Komponenten, die erst noch montiert werden müssen.

2.1.2 Bewertungskriterien (gekennzeichnet mit B)

Anforderungen, die mit dem Kürzel B gekennzeichnet sind, sind Bewertungskriterien im Sinne eines offenen Vergabeverfahrens. Sie stellen keine Ausschlusskriterien dar, das heißt, ihre Nichterfüllung führt nicht zum Ausschluss eines Bieters, sondern dienen der Differenzierung und Rangfolgenbildung bei der Angebotsbewertung. Diese Kriterien ermöglichen es dem Beschaffungsamt des BMI, zwischen mehreren Angeboten, die alle Mindestanforderungen erfüllen, eine objektive Rangfolge zu bilden und diejenige Lösung auszuwählen, die das beste Preis-Leistungs-Verhältnis bietet.

Jedes Bewertungskriterium hat einen klar definierten, zugeordneten Punktwert. Bieter, die über die Mindestanforderungen hinausgehen oder zusätzliche Funktionalitäten anbieten, erhalten die entsprechenden Punkte. Dies schafft einen vergaberechtlich zulässigen Anreiz für qualitativ hochwertige, innovative Lösungen und ermöglicht es dem Beschaffungsamt des BMI, das wirtschaftlichste Angebot im Sinne des besten Preis-Leistungs-Verhältnisses zu identifizieren.

Die Bewertungskriterien sind objektiv, transparent und diskriminierungsfrei gestaltet. Sie ermöglichen eine nachprüfbare Bewertung und Punktevergabe, sodass alle Bieter gleiche Chancen haben und die Auswahlentscheidung rechtssicher nachvollziehbar ist. Nähere Details entnehmen Sie bitte dem Kapitel 4.5.2 des Dokuments „01. Hinweise f. dieses Verfahren und besondere Bewerbungsbedingungen“.

Ein Beispiel für ein Bewertungskriterium ist ein Falltest aus 1,5 Metern Höhe ohne Funktionsbeeinträchtigung. Während ein erfolgreicher Falltest aus 1 Meter Höhe eine Mindestanforderung ist, erhalten Bieter zusätzliche 10 Punkte, wenn ihre Bodycams einen Fall aus 1,5 Metern unbeschädigt überstehen.

Die Bewertung der mit „B“ gekennzeichneten Kriterien erfolgt grundsätzlich zweistufig:

1. Zunächst werden alle Angebote auf Basis der mit dem Angebot einzureichenden Unterlagen (z. B. Eigenerklärungen, Datenblätter, Zertifikate, Prüfberichte) schriftlich bewertet. Hieraus ergibt sich eine vorläufige Rangfolge.
2. Anschließend werden die nach der schriftlichen Bewertung **zwei bestplatzierten Bieter** zu einer praktischen Teststellung (funktionaler Labortest) eingeladen. Im Rahmen dieser Teststellung werden ausschließlich solche Bewertungskriterien praktisch geprüft, die sich nicht hinreichend zuverlässig über Unterlagen nachweisen lassen (insbesondere Bedienbarkeit, Ergonomie, Video-/Audio-Qualität, Konnektivität und Cloud-Software-Handhabung). Die detaillierte Ausgestaltung der Teststellung und die Zusammenführung von schriftlicher Bewertung und Teststellung zur endgültigen Gesamtwertung ergeben sich aus Kapitel 7 - Teststellung und funktionaler Labortest.

2.2 Überblick über die Mindestanforderungen

Die Auftragnehmerin verpflichtet sich, die folgenden Kernleistungen vollständig zu erbringen:

Die erste Kernleistung besteht in der Lieferung von **integrierten Bodycam-Systemen**. Diese müssen als vollständig in sich geschlossene Geräte ausgeführt sein, die eine integrierte Kamera, ein Mikrofon, einen internen Speicher und Konnektivitätsmodule, insbesondere WiFi und optional Mobilfunk, enthalten. **Keinesfalls akzeptabel sind modulare Systeme**, bei denen einzelne Komponenten noch vom Nutzer oder von Wartungspersonal montiert oder verbunden werden müssen oder die offenliegende Kabel beinhalten und damit eine Gefahr im Sinne der Eigensicherung/Angriffspunkte darstellen.

Die zweite Kernleistung besteht in der **Bereitstellung einer cloudbasierten Software-Infrastruktur als SaaS-Modell** (Software as a Service). Das bedeutet, dass die Auftragnehmerin die volle Verantwortung für die Infrastruktur, das Hosting, die Sicherheit, die Verfügbarkeit und die regelmäßige Wartung trägt. Die Bundespolizei nutzt diese Software als Anwenderin und ist nicht für den technischen Betrieb zuständig. Das SaaS-Modell ist obligatorisch, ein Lizenzkauf, bei dem die Bundespolizei eigenverantwortlich ein Produkt in ihren eigenen Rechenzentren betreibt, ist nicht akzeptabel.

Die dritte Kernleistung besteht in der **Gewährleistung von Digitaler Souveränität**. Dies bedeutet, dass die Bundespolizei nicht in einen Vendor-Lock-In-Zustand geraten darf, in dem ein Wechsel zu einem anderen Anbieter praktisch unmöglich oder unwirtschaftlich ist. Dies wird durch mehrere Maßnahmen erreicht:

- Verwendung offener Standards,
- Bereitstellung einer dokumentierten REST-API für Datenzugriff,
- Möglichkeit zum vollständigen Datenexport in nicht-proprietären Formaten (MP4-Video, JSON/XML-Metadaten) und
- transparente Dokumentation aller Schnittstellen.

Die vierte Kernleistung besteht in der **sicheren und rechtskonformen Speicherung und Verarbeitung von Videodaten**. Alle Daten müssen ausschließlich auf Servern gespeichert werden, die sich **in der Europäischen Union** befinden, Deutschland wird hierbei als bevorzugter Speicherort festgelegt. Die Verschlüsselung muss dem Standard AES-256 entsprechen, sowohl für Daten im Ruhezustand (at-rest) als auch für Daten in der Übertragung (in-transit) mit TLS 1.3 oder neuer. Die Auftragnehmerin schließt hierfür einen EVB-IT Cloud Service Vertrag mit der Auftraggeberin ab.

Einhaltung der IT-Sicherheitsleitlinien des Bundes: Die Lösung muss den höchsten Anforderungen an die IT-Sicherheit und den Datenschutz genügen. Maßgeblich sind die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die fünfte Kernleistung besteht in einer **umfassenden Schulung der Nutzer und Administratoren**. Die Auftragnehmerin ist verpflichtet, Schulungen in deutscher Sprache durchzuführen, diese in Präsenzform vor Ort bei der Bundespolizei zu veranstalten und die Schulungsunterlagen in editierbarem Format barrierefrei zur Verfügung zu stellen, damit die Bundespolizei diese intern weitergeben kann. Schulungsreisekosten sind im Angebotspreis begriffen.

Die sechste Kernleistung besteht in der **Gewährleistung von Support und der Reparaturverfügbarkeit der bereitgestellten Hardware sowie des dazugehörigen SaaS-Dienstes**. Die Auftragnehmerin garantiert, dass für die Vertragslaufzeit der Rahmenvereinbarung sechs Jahre ab Lieferung Reparaturen und Wartung durchgeführt werden können, dass notwendige Ersatzteile verfügbar sind und dass ein Hotline-Support in deutscher Sprache verfügbar ist (nähere Details finden Sie in den Kapiteln 3.6 - Reparatur und Wartung sowie 5 - Service und Support).

Hinweis bzgl. Marktreife/Serienerzeugnis: Es dürfen ausschließlich serienreife Standardprodukte angeboten werden, die zum Zeitpunkt der Angebotsabgabe bereits regulär im kommerziellen Vertrieb des Herstellers etabliert und frei am Markt erhältlich sind. Prototypen, Vorserienmodelle, Test- oder Laborversionen sowie kunden- oder verfahrensspezifische Neuentwicklungen (Sonderanfertigungen für dieses Vergabeverfahren) sind ausdrücklich von der Antragstellung ausgeschlossen. Dies gilt gleichermaßen für die Hardware (Bodycams, Dockingstationen) wie für die Kernfunktionen der Cloud-Software (SaaS). Diese Anforderung wird als Mindestkriterium M93 – Marktreife/Serienerzeugnis festgelegt.

Nachweis: Der Bieter hat mit dem Angebot offizielle, unveränderte Produktdatenblätter oder einen Auszug aus dem regulären Produktkatalog des Herstellers einzureichen, aus dem die kommerzielle Verfügbarkeit (z. B. Angabe einer globalen Artikelnummer/EAN oder eines bestehenden Seriennummernkreises) zweifelsfrei hervorgeht.

3. Anforderungen an die Bodycam-Hardware

Dieses Kapitel beschreibt sämtliche technischen und physischen Anforderungen an die zu liefernden Bodycam-Systeme einschließlich des zugehörigen Zubehörs. Die Anforderungen orientieren sich an den spezifischen Einsatzbedingungen der Bundespolizei, insbesondere an den Anforderungen des 24/7-Schichtbetriebs, der Notwendigkeit zur ergonomischen Integration in die bestehende Einsatzausrüstung sowie an den rechtlichen und taktischen Anforderungen an die Gefahrenabwehr und Beweissicherung.

3.1 Grundlegende Eigenschaften und Einsatzumgebung

3.1.1 Gewicht und Tragbarkeit

Die Bodycam muss unter Berücksichtigung der operativen Realität der Bundespolizei ausgelegt sein. Bundespolizeibeamte tragen bereits umfangreiche Ausrüstung, bspw. Gürtel mit Dienstwaffe, Handschellen, Funkgerät, Taschen und weitere taktische Ausrüstung. Eine zusätzliche Bodycam darf nicht zu einer unnötigen Belastung werden, die den Beamten behindert oder körperlich ermüdet. Aus diesem Grund ist das maximale Gewicht (M1 – Gewicht der Bodycam (max. 255g)) einer betriebsbereiten Bodycam, einschließlich des installierten Akkus, als Ausschlusskriterium auf 255 Gramm festgelegt. Dies entspricht etwa dem Gewicht eines mittelgroßen Smartphones und stellt sicher, dass eine robuste mechanische Ausstattung ohne übermäßige physische Last gewährleistet ist.

Um die ergonomische Belastung für die Einsatzkräfte so gering wie möglich zu halten, wird ein besonders niedriges Eigengewicht innerhalb des zulässigen Rahmens positiv bewertet (B1 – Gewicht der Bodycam). Ein geringeres Gewicht erhöht die Trageakzeptanz und minimiert die Hebelwirkung auf die Uniform bei dynamischen Bewegungen. Die Einhaltung der Gewichtsvorgaben wird im Rahmen der Qualitätssicherung mittels einer Präzisionswaage (Genauigkeit ± 1 Gramm) überprüft. Bei einem Gesamtgewicht von < 200 Gramm werden 5 Punkte vergeben. Beträgt das Gesamtgewicht 200 Gramm oder mehr (jedoch maximal 255 Gramm) werden 0 Punkte vergeben.

3.1.2 Befestigung und Kompatibilität mit Uniformteilen und Ausrüstungsgegenständen

Die Bodycam muss auf vielfältige Weise befestigt werden können, um den unterschiedlichen Einsatzbedingungen und persönlichen Vorlieben der Beamten gerecht zu werden. Die Grundvariante ist die Befestigung an der Uniform, typischerweise auf der Brust oder dem Schulterbereich.

Die Bodycam muss mit dem in der Bundespolizei verwendeten modularem Wechselsystem (MOLLE – Modular Lightweight Load-carrying Equipment) der taktischen Wechselhülle der ballistischen Schutzweste kompatibel sein (M2 – Kompatibilität zu MOLLE). MOLLE ist ein standardisiertes Befestigungssystem, das auf Kampfwesten, taktischen Rucksäcken und anderen Ausrüstungsgegenständen verwendet wird und eine flexible Anbringung an verschiedenen Positionen ermöglicht. Die Auftragnehmerin muss einen MOLLE-Adapter bereitstellen.

Des Weiteren muss die Bodycam über ein Klipp-Modul verfügen, mit dem eine sichere jedoch schnell wechselbare Anbringung auf verschiedenen Ausrüstungs- bzw. Uniformteilen (z.B. Körperschutzausstattung, schwere ballistische Weste, Einsatzjacke) ermöglicht wird, bspw. durch ein Adaptersystem. Die uneingeschränkte Bedienbarkeit muss dabei weiterhin gewährleistet sein. Die Substanz der Bekleidung oder des Ausrüstungsgegenstandes darf dabei nicht beschädigt werden. Die Auftragnehmerin muss hierzu notwendiges Zubehör entwickeln und liefern.

Alle erforderlichen Befestigungsadapter und -vorrichtungen müssen im Lieferumfang der jeweiligen Bodycam enthalten und als Zubehör erhältlich sein.

Soweit für die sichere und uneingeschränkte Nutzung der Bodycam weitere Adapter-, Halte- oder Verbindungselemente erforderlich sind, sind auch diese Bestandteil des Lieferumfangs der jeweiligen Bodycam und im Preis des Bodycam-Komplettsystems einzupreisen.

3.1.3 Intuitive Bedienbarkeit und Nutzerführung

Die Akzeptanz des Systems im täglichen Dienstbetrieb hängt maßgeblich von einer intuitiven und selbsterklärenden Bedienlogik ab. In sämtlichen Einsatzlagen der Bundespolizei müssen Beamte in der Lage sein, das Gerät unter Stress sicher zu bedienen, ohne langwierige Bedienmenüs oder komplexe Tastenkombinationen konsultieren zu müssen. Eine Bodycam ist für den polizeilichen Einsatz nur dann zweckmäßig, wenn ihre Kernfunktionen auch von Personal, das lediglich eine kurze Einweisung erhalten hat oder das Gerät nach längerer Zeit wieder nutzt, sofort und fehlerfrei bedient werden können.

Die Auftragnehmerin muss daher ein Bedienkonzept bereitstellen, welches die logische Abfolge von Bedienschritten unterstützt und den Gerätestatus (z. B. Betriebsbereitschaft, laufende Aufnahme, Energiestatus) jederzeit eindeutig signalisiert. Dies umfasst sowohl die haptische Anordnung der Bedienelemente als auch die visuelle oder akustische Rückmeldung des Gerätes. Die Validierung dieser Eigenschaft erfolgt durch eine unvoreingenommene Teststellung mit Einsatzkräften ohne vorherige intensive Schulung (B2 - Intuitive Menüführung ohne Schulung).

Werden alle definierten Grundaufgaben (Einschalten, Start/Stop der Aufnahme, Prüfung des Akkuladestands, Ausschalten) von einem ungeschulten Testbeamten ohne fremde Hilfe erfolgreich abgeschlossen, gibt es 15 Punkte. Sollte der Testbeamte zur Erfüllung der Aufgaben Unterstützung benötigen oder kann diese nicht innerhalb des vorgegebenen Zeitrahmens von 5 Minuten abschließen, werden 0 Punkte vergeben.

3.1.4 Bedienbarkeit mit und ohne Handschuhe

Ein kritischer Aspekt für die Feldtauglichkeit ist die Bedienbarkeit unter allen Bedingungen. Beamte der Bundespolizei tragen in der überwiegenden Anzahl an Einsatzlagen (taktische) Handschuhe (teilw. mit Schnittschutz an den Hand- und Fingerinnenflächen) oder Hygienhandschuhe. Auch bei Außeneinsätzen in den Wintermonaten muss eine Bedienbarkeit mit dicken Handschuhen aus Materialien wie beispielsweise Wolle, Leder oder technischen Kunststoffen gewährleistet sein. Eine Bodycam ist vollkommen unbrauchbar, wenn der Beamte die Aufnahme nicht starten, stoppen oder andere wichtige Funktionen durchführen kann, ohne die Handschuhe auszuziehen.

Touch-Screens erfüllen in diesem Zusammenhang nicht den einsatztaktischen Bedarf, da sie regelmäßig erfordern, dass die Einsatzkraft auf den Bildschirm schauen muss, um die richtige Einstellung anzuvisieren, anstatt diese intuitiv (blind) zu finden und den Blick auf die Einsatzsituation gerichtet zu lassen. Daher muss die Bedienung aller für den Einsatz erforderlichen Funktionen ohne Touch-Screen möglich sein.

Die Auftragnehmerin hat durch geeignete Designansätze sicherzustellen, dass alle notwendigen Bedienelemente, wie beispielsweise Hauptschalter, Aufnahmetaste, Menütasten, TR/IA-Kennzeichnungstasten mit dicken Handschuhen betätigt werden können. Dies kann durch verschiedene Designansätze erreicht werden: übergroße Tasten, taktile Unterscheidung zwischen Tasten. Dieses Kriterium wird im Rahmen der praktischen Teststellung bewertet (B3 - Bedienbarkeit mit dicken Handschuhen, siehe Kapitel). Für eine absolut sicher und intuitive Bedienung (Einschalten, Start/Stop, Markieren, Ausschalten) mit dicken Winterhandschuhen (mind. 3 mm Materialstärke) werden 5 Punkte vergeben. Ist die Bedienung mit Handschuhen erschwert, führt zu Fehlbedienungen oder erfordert das Ausziehen der Handschuhe werden 0 Punkte vergeben.

3.1.5 Schutzklasse und Widerstandsfähigkeit

Die Bodycam wird in rauen Umgebungen eingesetzt, hierzu gehören neben Regen, Schnee und Staub auch gröbere Verschmutzungen wie bspw. ölige Stoffe, Farbe, Matsch, menschliche Sekrete. Die Verwendung im Rahmen von Wasserwerfer-Einsätzen erfordert ebenfalls eine hinreichende Beständigkeit. Sie kann auf den Boden fallen, gegen Gegenstände stoßen, oder in Gewalt-

Situationen (durch körperliche Gewalt, Bewurf, Schläge) beschädigt werden. Eine angemessene Schutzklasse gegen Eindringen von Feststoffen und Flüssigkeiten ist daher essentiell.

Der Standard IP67 wird als Minimalanforderung (M3 – Schutzklasse IP67) festgelegt. Diese Schutzklasse bedeutet, dass die Bodycam staubdicht ist (erste Ziffer: 6 = Schutz gegen Eindringen von Staub und Schmutz) und zeitweise Untertauchen in Wasser bis zu 1 Meter Tiefe für maximal 30 Minuten unbeschädigt überstehen kann (zweite Ziffer: 7 = Schutz gegen Untertauchen). Dies ist ein bewährter Standard für mobile Geräte im polizeilichen Einsatz.

Oberhalb dieser Minimalanforderung werden bessere Schutzklassen akzeptiert, werden aber nicht erwartet. Ein Hersteller, der IP68 (permanentes Untertauchen in Wasser) oder sogar IP69K (Hochdruckwasserstrahlen) anbietet, würde damit eine höhere Robustheit demonstrieren, was jedoch nicht explizit gefordert wird.

3.1.6 Falltests und mechanische Robustheit

Die Bodycam wird unweigerlich fallen, entweder aus Unachtsamkeit, durch Sturz des Beamten (stolpern, im Handgemenge, etc.) oder durch die Gewalt einer Auseinandersetzung. Die Auftragnehmerin muss daher Bodycams liefern, die Stürze unbeschädigt überstehen.

Als Mindestanforderung ist festgelegt, dass die Bodycam einen Fall aus einer Höhe von 1 Meter auf harten Untergrund (etwa Beton oder Hartholzboden) ohne jede Beschädigung überstehen muss (M4 – Robustheit (Falltest aus 1m)). Diese Anforderung wird durch wiederholte Falltests validiert: Mindestens fünf Wiederholungen pro Gerät, jeder Fall aus 1 Meter Höhe auf denselben harten Untergrund, mit vollständiger Funktionsprüfung danach.

Zusätzlich ist ein Falltest aus 1,5 Metern als Bewertungskriterium (B4 – Robustheit (Falltest aus 1,5m)), siehe Kapitel 7.3.1) definiert. Bieter, deren Bodycams einen Fall aus 1,5 Metern ohne Funktionsbeeinträchtigung überstehen, erhalten 10 zusätzliche Bewertungspunkte.

3.1.7 Temperaturbereich

Die Bundespolizei ist ganzjährig 24/7 im Einsatz. Sowohl bei Maßnahmen unter direkter Sonneneinstrahlung sowie bei Frost, jeweils über mehrere Stunden hinweg, muss die Funktionsfähigkeit der Einsatzmittel gewährleistet sein. Die Bodycam muss daher über einen breiten Betriebstemperaturbereich funktionieren.

Die Mindestanforderung lautet: Betriebstemperaturbereich von -20 °C bis +50 °C oder größer (M5 – Temperaturbereich (-20 °C bis +50 °C)). Dies bedeutet, dass die Bodycam bei einer Außentemperatur von -20 °C (etwa -4 °F) einsatzbereit sein muss, zum Beispiel für Einsätze an (Grenz-) Kontrollstellen im Winter. Auch bei Temperaturen von +50 °C (122 °F) muss die Bodycam funktionieren. Zum Beispiel in geparkten Fahrzeugen.

3.1.8 Display und visuelle Deeskalation

Für die taktische Einsatzbewältigung hat die Koppelungsfunktion der Bodycam mit weiteren Führungs- und Einsatzmitteln (FEM) grundsätzlich Vorrang und ist im Zweifelsfall einem integrierten Front-Display vorzuziehen.

Es ist jedoch im Sinne einer vollumfänglichen einsatztaktischen Bedarfsdeckung in höchstem Maße wünschenswert, wenn die angebotene Bodycam sowohl über die Möglichkeit zur Koppelung mit weiteren FEM als auch über ein integriertes Front-Display zur visuellen Deeskalation verfügt.

Sofern die angebotene Bodycam über ein solches Front-Display verfügt, sollte dieses in Aufnahme-richtung (zum polizeilichen Gegenüber) ausgerichtet sein und in der Lage sein, das aktuell aufgezeichnete Videobild in Echtzeit wiederzugeben ("Live-View"). Diese Funktion dient dazu, dem polizeilichen Gegenüber das eigene Verhalten unmittelbar vor Augen zu führen ("Spiegel-Effekt"). Durch die visuelle Konfrontation mit dem eigenen Handeln soll eine mäßigende Wirkung auf aggressive Personen erzielt und die Transparenz der polizeilichen Maßnahme erhöht werden. Um die taktische Flexibilität in diesem Fall zu gewährleisten, sollte bei einer Bildwiedergabe auf dem Front-Display durch den Nutzer oder über eine zentrale Konfiguration steuerbar sein:

- **Standard-Modus:** Das Display ist während der Aufnahme aktiv und zeigt das Live-Bild.
- **Stealth-/Opferschutz-Modus:** Das Display ist bei Bedarf manuell am Gerät oder dauerhaft per Konfiguration deaktivierbar sein (Dunkelschaltung). Dies ist erforderlich für verdeckte Maßnahmen, Einsätze bei Dunkelheit (verdeckte Annäherung) oder in Situationen, in denen die Bildwiedergabe kontraproduktiv wäre.

Zudem sollte ein solches Display grundlegende Statusinformationen (z. B. Aufnahmestatus, Uhrzeit) anzeigen können, um allen Beteiligten transparent zu machen, dass die konkrete Aufnahme zur aktuellen Zeit erfolgte.

Das Vorhandensein eines Front-Displays stellt ein Bewertungskriterium dar (B5 – Frontdisplay). Verfügt die angebotene Bodycam zusätzlich zur präferierten Koppelungsfunktion mit weiteren FEM über ein Front-Display, welches die oben genannten Anforderungen (Live-View, umschaltbare Modi) erfüllt, erhält der Bieter hierfür 15 Punkte in der qualitativen Wertung. Wird kein Gerät mit entsprechendem Display angeboten, führt dies nicht zum Angebotsausschluss, es werden in diesem Kriterium jedoch 0 Punkte vergeben.

3.1.9 Schnellregistration von Einsatzkraft und Bodycam (RFID)

Einsatzkräfte der Bundespolizei sind überwiegend im Drei-Schicht-System 24/7 eingesetzt. Die Ausstattung von Bodycam erfolgt im Rahmen einer Pool-Ausstattung, sodass die in einer Dienststelle vorhandenen Geräte grundsätzlich von Schicht zu Schicht und damit von Einsatzkraft zu Einsatzkraft übergeben werden. Dies muss ohne Zeitaufwand und mit geringstmöglichem Handlungsaufwand erfolgen. Eine Registratur über ein RFID-System o.ä. ist daher eine Mindestanforderung (M6 – Schnellregistration (RFID)).

3.1.10 Automatisierte Auslösung beim Ziehen von weiteren Führungs- und Einsatzmitteln (FEM, Distanz-Elektroimpulsgerät sowie dienstlicher Schusswaffe) aus dem Holster

Zur Sicherstellung der Eigensicherung und einer umfänglichen einsatztaktischen Bedarfsdeckung in hochdynamischen Einsatzsituationen ist die Koppelungsfähigkeit der Bodycam mit weiteren Führungs- und Einsatzmitteln (FEM) zwingend erforderlich. Die angebotene Bodycam muss über eine verlässliche Schnittstelle bzw. Koppelungsfunktion (z. B. Bluetooth oder vergleichbare Nahbereichsfunktechnologie) verfügen, um mit weiteren FEM sowie deren Tragesystemen kommunizieren zu können.

Insbesondere muss das System die automatisierte Auslösung der Bodycam-Aufzeichnung beim Einsatz von Zwangsmitteln, insbesondere Waffen, unterstützen. Hierzu muss die Bodycam in der Lage sein, sich mit entsprechenden Signalgebern/Sensoren an den Holstern von weiteren FEM (konkret dem Distanz-Elektroimpulsgerät (DEIG) sowie der dienstlichen Schusswaffe P30) zu koppeln. Sobald das jeweilige Einsatzmittel aus dem Holster gezogen wird, muss durch diese Koppelung zwingend und verzögerungsfrei eine automatisierte Auslösung der Bodycam (Start der Video- und Audioaufzeichnung inkl. Pre-Recording) erfolgen, ohne dass die Einsatzkraft die Bodycam zusätzlich manuell bedienen muss.

Um diese Funktionalität praxistauglich umzusetzen und den unterschiedlichen Trage- und Holstersystemen Rechnung zu tragen, sind geringe Abmessungen der hierfür erforderlichen Auslöse-/Koppelungskomponenten erforderlich. Entsprechende Signalgeber, Sensoren oder Koppelungsplatten für Holster sind zudem als eigenständiges Zubehör zu konzipieren und müssen separat sowie in höherer Stückzahl als die eigentlichen Bodycams beschaff- und austauschbar sein.

Diese Funktionalität stellt eine Mindestanforderung (M7 – automatisierte Aufnahme bei Nutzung von FEM) dar und garantiert die lückenlose Dokumentation und Beweissicherung in kritischen Situationen, in denen die manuelle Aktivierung der Kamera durch die Einsatzkraft aufgrund der Stress- oder Gefahrenlage nicht möglich ist.

Sämtliche für die Grundausstattung der ausgeschriebenen Bodycam-Systeme erforderlichen Auslöse-, Koppelungs-, Signalgeber-, Sensor- oder funktional gleichwertigen Komponenten sind im Preis des Bodycam-Komplettsystems einzupreisen. Dies gilt unabhängig davon, ob die technische Umsetzung über klassische Holstermodule, sonstige Triggereinheiten oder andere funktional gleichwertige technische Lösungen erfolgt. Darüber hinausgehende zusätzliche Bedarfe, Ersatz- oder Erweiterungsbeschaffungen bleiben gesondert abrufbar.

3.1.11 Firmware-Pflege und Update-Management

Die kontinuierliche Wartung und Weiterentwicklung der Geräte-Firmware ist Bestandteil der Leistung, um die IT-Sicherheit und Funktionsfähigkeit über die gesamte Nutzungsdauer zu gewährleisten. Die Auftragnehmerin verpflichtet sich, für die angebotenen Bodycams für einen Zeitraum von mindestens 6 Jahren nach Abnahme jeder Charge Firmware-Updates bereitzustellen (M8 – Firmwarebereitstellung). Diese Updates müssen folgende Bereiche abdecken:

- Schließen von Sicherheitslücken und Anpassung an aktuelle kryptografische Standards. Kritische Sicherheitsupdates sind unverzüglich nach Bekanntwerden der Lücke bereitzustellen.
- Behebung von Funktionsstörungen, Stabilitätsproblemen oder Fehlern in der Aufnahmequalität.
- Sicherstellung der Kompatibilität mit der Backend-Software (SaaS-Dienst) und den Dockingstationen.

Da ein manuelles Update einzelner Geräte im operativen Betrieb nicht durchführbar ist, muss das System eine zentrale Verteilung der Firmware unterstützen ("Remote Device Management").

- Der Administrator muss in der Lage sein, Firmware-Updates zentral in die Verwaltungssoftware (SaaS-Dienst) einzuspielen.
- Die Updates sollen automatisch auf die Bodycams übertragen werden (M9 – Firmwareupdate der Bodycams), sobald diese in die Dockingstation eingesteckt werden (via LAN/WLAN) oder, sofern technisch verfügbar "Over-the-Air" (OTA) via WLAN/LTE. Firmware-Updates dürfen nicht während einer laufenden Video- oder Audioaufzeichnung gestartet oder installiert werden, sofern hierdurch die Funktionsfähigkeit der Bodycam eingeschränkt oder eine laufende Aufnahme unterbrochen würde. Die Installation der Updates hat daher grundsätzlich nur in Phasen ohne laufende Aufnahme, vorzugsweise beim Einstellen der Bodycam in die Dockingstation nach Abschluss und Upload sämtlicher Aufnahmen, zu erfolgen. Hierbei muss aber sichergestellt werden, dass ein Firmwareupdate keine operativen Einsätze gefährdet/die Bodycam nicht einsatzfähig ist.
- Es muss administrativ steuerbar sein, wann welche Gerätegruppe das Update erhält (z. B. erst Testgruppe, dann Rollout für alle), um Einsatzrisiken zu minimieren.

Alle Firmware-Updates (Sicherheit und Bugfixes) müssen in den Lizenz- oder Wartungskosten enthalten sein. Es dürfen keine separaten Kosten pro Update entstehen.

Firmware-Updates sollten vorab gegenüber der Bundespolizei angekündigt und ihr Inhalt nachvollziehbar dargestellt werden (z. B. Ursache/Problem, Lösung, Verfahrensprozess, etwaige Einschränkungen)

3.2 Speicher und Datenverwaltung

3.2.1 Interner Speicher und Backup

Die Bodycam muss über einen ausreichend großen internen Speicher verfügen, um mehrere Stunden Videomaterial unabhängig von einer Cloud-Verbindung lokal zu speichern. Dies ist kritisch, da die Bodycam in unterirdischen Bahnhöfen, in dicken Betongebäuden oder in Fahrzeugen eingesetzt wird, wo WiFi- oder Mobilfunkverbindungen nicht immer verfügbar sind. Der Beamte muss die Gewissheit haben, dass Aufnahmen lokal gesichert sind, auch bei Netzwerkunterbrechungen.

Als Mindestanforderung ist festgelegt, dass die Bodycam über einen internen Speicher von mindestens 64 Gigabyte verfügen muss (M10 – Speicherausstattung). Bei einer Aufnahmequalität von

1080p und 25 Bildern pro Sekunde mit H.264-Kompression entspricht dies etwa 20-24 Stunden kontinuierlicher Aufnahmezeit, je nach Kompressionseinstellungen. Dies deckt mehrere Schichten ab und puffert kurzzeitige Netzwerkstörungen.

Ein unmittelbarer Upload der Aufnahmen (Live-Streaming) in die Cloud wird nicht gefordert. Stattdessen ist ein Upload über das Einstecken in die Ladestation (Dockingstation) nach der Aufnahme ausreichend. Die Bodycam muss jedoch grundsätzlich mobilfunkfähig sein (z. B. LTE), wobei die tatsächliche Nutzung optional bleibt.

Die Auftragnehmerin kann auch höhere Speicherkapazitäten anbieten (etwa 128 GB oder 256 GB), was positiv bewertet wird, da es den Beamten mehr Flexibilität gibt (B6 – Speicherausstattung).

3.2.2 GNSS/GPS und Geo-Tagging

Die Fähigkeit zur Georeferenzierung **von Aufnahmen** ist von großer Bedeutung für die operative Lagebildanalyse, die Nachbetrachtung von Einsatzlagen, sowie insbesondere für die Ermittlungs- und Prozessführung. Wenn ein Polizeieinsatz sich über mehrere Örtlichkeiten fortsetzt, ist es wertvoll zu wissen, an welchem genauen Ort eine bestimmte Aufnahme gemacht wurde, sowohl im Rahmen der nachfolgenden Ermittlungen als auch als beweiskritischer Faktor im gerichtlichen Verfahren (Stichwort: Beweislast und Glaubhaftigkeit von Aussagen).

Die Auftragnehmerin muss daher ein integriertes GNSS-System (Global Navigation Satellite System), typischerweise GPS, in die Bodycam einbauen (M11 – Integriertes Global Navigation Satellite System). Dieses muss eigenständig funktionieren, unabhängig von Mobilfunkmodems (LTE/5G), und weltweit verfügbar sein. Die Georeferenzierung muss automatisiert in unveränderbaren Metadaten jeder Aufnahme hinterlegt werden und darf nicht deaktivierbar sein (M12 – Georeferenzierung in Aufnahmen).

Die Visualisierung in einer Karte des SaaS-Dienstes oder die Möglichkeit der Ausleitung/Export (im Format GeoJSON bzw. GPX) und Übernahme in einer bundespolizeieigenen Karte (BPOLMaps) im Nachgang der Einsatzlage ist zwingend erforderlich (M13 – Visualisierung in einer Karte (SaaS-Dienst) oder Export (BPOLMaps)).

Die Fähigkeit einer anlassbezogenen und auf den Einzelfall beschränkten live-Ortungsmöglichkeit der Bodycam-Träger und geobasierter Darstellung in einer digitalen Karte ist dagegen nicht erforderlich.

Sofern diese Funktion im Gesamtsystem Bodycam beinhaltet sein sollte, ist es aus Datenschutzgründen essentiell, dass die Bundespolizei in der Lage sein muss das Geo-Tagging nur dann zu aktivieren und es in sensiblen Situationen zu deaktivieren, wenn es rechtlich oder operativ notwendig ist. Diese Funktionalität wäre sodann durch Berechtigte rollenbasiert und ausschließlich über die Software individuell für jedes Gerät zu- und abschaltbar.

Darüber hinaus muss im Falle dieser Funktionalität die Option bestehen, dass dieses GNSS-System zusätzlich zentral durch den Systemadministrator oder Fachadministrator der Bundespolizei

aktiviert und deaktiviert werden kann. Dies wird über die Cloud-Verwaltungssoftware erfolgen und gilt für alle im Einsatzgebiet eingesetzten Geräte gleichzeitig.

3.2.3 Manipulationssicherer Zeitstempel

Der Zeitstempel, der in jede Videoaufnahme eingeblendet wird, ist eine kritische Information. In einem Gerichtsverfahren können genaue zeitliche Abläufe entscheidend sein. Wenn ein Beamter den Zeitstempel manipuliert, könnte dies die Glaubwürdigkeit der gesamten Aufnahme kompromittieren.

Daher ist eine Mindestanforderung, dass der Zeitstempel manipulationssicher ist (M14 – Manipulationssichere Zeitstempel). Dies bedeutet: Der Zeitstempel kann von dem Beamten nicht auf dem Gerät selbst manuell eingestellt werden. Stattdessen wird der Zeitstempel automatisch vom Gerät gesetzt, basierend auf einer zentralen Zeitquelle (typischerweise Network Time Protocol (NTP) von Internet-Zeitservern).

Alle Bodycams müssen zentral synchronisiert werden, etwa über eine WiFi-Verbindung mit einem zentralen Zeitserver, wenn sie an die Cloud-Infrastruktur angebunden werden. Dies stellt sicher, dass alle Geräte eine konsistente Zeit verwenden und dass keine manuelle Einstellung auf dem Gerät selbst möglich ist.

3.2.4 Schutz gegen unbefugten Zugriff und Datenlöschung

Die Bodycam speichert sensible Daten, nicht nur Videoaufnahmen von Einsätzen, sondern insbesondere auch personenbezogene Daten in Bild und Ton. Die Bundespolizei hat hinsichtlich dieser einen datenschutzkonformen Umgang schon von Rechtswegen zu gewährleisten. Ein angemessenes Sicherheitsmodell ist daher essentiell.

Die Auftragnehmerin muss das Gerät so konfigurieren, dass die auf der Bodycam gespeicherten Daten durch folgende Mechanismen geschützt sind (M15 – Schutz gegen unbefugten Zugriff und Datenlöschung):

- Die Daten müssen so verschlüsselt sein, dass jemand, der das physische Gerät in die Hand bekommt, die Videos nicht ohne den richtigen Schlüssel abspielen kann.
- Die Löschung von Videos direkt auf der Bodycam darf nicht möglich sein. Dies verhindert, dass ein Nutzer, dessen Aufnahmen möglicherweise problematisch sind, diese löscht. Stattdessen können Videos nur über die zentralisierte Cloud-Software mit entsprechenden Berechtigungen und Audit-Trails gelöscht werden.
- Nach erfolgreichem Upload hat eine automatisierte Löschung vom Gerätespeicher der Bodycam zu erfolgen.
- Es darf kein Nutzer Videos vom Gerät auf einen USB-Stick oder externe Datenträger kopieren.
- Mittels TR/IA-Kennzeichnungstasten müssen entsprechende Aufzeichnungen seitens des Nutzers zu kennzeichnen sein.

Diese Funktionen sind seitens der Auftragnehmerin durch Software-Kontrolle zu unterbinden.

3.2.5 Pre-Event-Recording (Vorlaufaufnahme)

Die Kamera muss über einen Pufferspeicher verfügen, der im Standby-Modus permanent aufzeichnet. Bei Aktivierung müssen mindestens 30 Sek. (seitens eines Systemadministrators individuell aber einheitlich für alle Geräte der Bundespolizei einstellbar, auch über 30 Sekunden hinaus) Videomaterial vor dem Auslösezeitpunkt gespeichert werden. Das Pre-Event-Recording muss am Gerät durch den Nutzer aktivierbar und deaktivierbar sein. Sofern keine Aktivierung des Aufnahme-modus erfolgt, sind die jeweils vorlaufenden 30 Sekunden (sodann die jeweils 31. Sekunde) rückstandslos zu löschen/zu überschreiben. Bei einer aktiven Aufnahme, ergänzen sie die eigentliche Aufnahme um die 30 vorangestellten Sekunden (M16 – Pre-Event-Recording).

Dahingehend abgestufte Betriebsmodi (bspw. Ruhe-/ Stand-By- (Pre-Recording deaktiviert) sowie Bereitschafts- (alle Funktionen aktiviert) Modus) stellen dahingehend eine Grundforderung dar.

3.3 Videoqualität und Aufnahmeformat

3.3.1 Auflösungsoptionen und Bildwiederholfrequenz

Die Videoaufnahmequalität muss ausreichend sein, um bei der Wiedergabe der Aufnahmen Gesichter nach einer typischen Einsatzsituation zu identifizieren (auch, wenn die Aufnahmen in Umgebungen mit schlechten oder wechselnden Lichtbedingungen erfolgten). Zudem muss es auch wirtschaftlich, im Hinblick auf Speicherung und Upload-Bandbreite, sein. Höhere Auflösung führt zu größeren Dateien und längeren Upload-Zeiten.

Die Auftragnehmerin muss daher flexible Aufnahmeoptionen bieten. Sowohl 720p-Auflösung (1280 × 720 Pixel) als auch 1080p-Auflösung (1920 × 1080 Pixel) müssen von der Auftraggeberin/Bedarfsträgerin rollenspezifisch (Admin) wählbar sein (M17 – Videoqualität (720/1080p, 25 FPS)).

Die Bildwiederholfrequenz (Anzahl der Einzelbilder pro Sekunde) muss mindestens 25 FPS (Frames Per Second) betragen. Dies ist ausreichend für flüssiges, identifizierbares Video. Die Auftragnehmerin muss dem Nutzer rollenbezogen die Möglichkeit geben, die Bildwiederholfrequenz anzupassen. Etwa auf 30 FPS oder 60 FPS, um je nach Situation und Einsatzbereich die optimale Bildwiederholfrequenz einstellen zu können.

Kann eine höhere Auflösung von min. 4k eingestellt werden, so wird dies mit 5 zusätzlichen Punkten bewertet (B7 – Videoqualität (4k+)).

3.3.2 Video-Codec und Kompression

Die Dateigrößen müssen managebar bleiben, damit die Cloud-Speicherung wirtschaftlich bleibt.

Das H.264-Format (auch bekannt als MPEG-4 Part 10) ist ein bewährter Standard, der eine gute Balance zwischen Kompression und Kompatibilität bietet. Die Bodycam muss H.264 als Standard unterstützen (M18 – Video-Codec (H.264)).

Zusätzlich wird das neuere H.265-Format (HEVC – High Efficiency Video Coding) als Bewertungskriterium angeboten. H.265 erreicht etwa die gleiche Videoqualität wie H.264, benötigt aber etwa 50 % weniger Speicherplatz. Bieter, die H.265-Aufnahmen unterstützen, erhalten 10 zusätzliche Bewertungspunkte (B8 – Video-Codec (H.265)).

3.3.3 Bildstabilisierung

Aufnahmen, die aus der Bewegung heraus, insbesondere bei Laufschritten oder dynamischen Einsatzlagen, entstehen, unterliegen naturgemäß starken Erschütterungen. Diese Verwacklungen können die Analyse des Videomaterials erheblich beeinträchtigen und die zweifelsfreie Identifizierung von Personen oder handlungsrelevanten Details erschweren.

Um die Verwertbarkeit des Beweismaterials auch unter solchen Bedingungen sicherzustellen, muss die Bodycam über eine wirksame Technologie zur Bildstabilisierung verfügen. Hierbei kommen sowohl elektronische Bildstabilisatoren (EIS), die durch Software-Algorithmen und Gyrosensoren Bewegungen ausgleichen, als auch optische Bildstabilisatoren (OIS/Gimbal), die Erschütterungen mechanisch kompensieren, in Betracht (M19 – Bildstabilisierung).

3.3.4 Sichtfeld und Kamera-Schwenkbereich

Das horizontale Sichtfeld (die seitliche Breite dessen, was die Kamera sehen kann) ist essentiell für eine polizeiliche Einsatz-Dokumentation. Ein zu enges Sichtfeld führt dazu, dass wichtige Details außerhalb des aufgezeichneten Bereichs liegen.

Eine Mindestanforderung ist ein horizontales Sichtfeld von mindestens 110 Grad (M20 – Horizontales Sichtfeld der Kamera (min. 110 Grad)). Dies ist ein bewährter Wert, der in vielen professionellen Action-Kameras und Bodycams verwendet wird. Es erfasst genug von der Umgebung, ohne zu großen Sichtverzerrungen zu führen.

Ein horizontales Sichtfeld im Bereich von 120 bis 130 Grad wird positiv bewertet. Dieser Bereich erfasst das Sichtfeld eines Menschen (hier: Einsatzkraft) und ist entscheidend, um das Geschehen festzuhalten, dass der Nutzer tatsächlich wahrnehmen kann. Bieter, die dies anbieten erhalten 10 Punkte (B9 – Horizontales Sichtfeld der Kamera (im Bereich 120 bis 130 Grad)). Darüber hinaus gehende Winkel werden nicht bepunktet, da aus Gründen der Beweislast auf die Abbildung von seitens des Trägers nicht erfassbaren Bereichen abzusehen ist.

Zusätzlich können fortgeschrittene Lösungen eine horizontal schwenkbare Kameralinse bieten, das heißt, der Beamte kann die Kamera nach links und rechts drehen, um bspw. eine links oder rechts an der Brust getragene Bodycam wieder zentral auszurichten (B10 – Kamera horizontal schwenkbar). Dies ist optional und wird mit 10 Punkten bewertet, wenn angeboten. Ebenso wird eine vertikal neigbare Kameralinse mit 10 Punkten bewertet (B11- Kamera vertikal schwenkbar). Diese Funktionen ermöglichen maximale Flexibilität bei der Anpassung auf die Physiognomie des Nutzers (bspw. besonders große oder kleine Körpergröße der Einsatzkraft), um die Aufnahmewinkel an die sich aus der Körpergröße und aus der steten Kopfneigung und -hebung ergebende Perspektive des Nutzers anzupassen bzw. diese auszugleichen.

3.3.5 Mikrofonanforderungen und Audioqualität

Die auditive Dokumentation ist für die Beweissicherung von entscheidender Bedeutung. Neben der rein visuellen Ebene sind der exakte Wortlaut sowie die Tonalität verbaler Konfrontationen essenziell, um eine vollständige und gerichtsfeste Rekonstruktion des Einsatzgeschehens zu gewährleisten. Eine Bodycam ohne funktionale Tonaufzeichnung stellt daher einen erheblichen Minderwert dar.

Daher werden folgende Mindestanforderungen an die Tonaufzeichnung gestellt:

- **Hardware:** Das Gerät muss über mindestens zwei integrierte Mikrofone verfügen. (M21 – Zwei Mikrofone). Eine Lösung mit mehr als zwei Mikrofonen ist ausdrücklich zulässig, sofern die geforderte Audioqualität vollumfänglich sichergestellt ist. Die Platzierung muss so gewählt sein, dass die Mikrofone durch gängige Halterungssysteme (MOLLE, Klick-Adapter) nicht verdeckt werden. Eine Platzierung auf der Geräterückseite ist unzulässig.
- **Basiskonfiguration (60–70 dB):** Das Mikrofonsystem muss zwingend eine klare und zweifelsfrei verständliche Sprachaufzeichnung in normalen Einsatzumgebungen bei einer Umgebungslautstärke von ca. 60 bis 70 dB gewährleisten. M22 – Klare Sprachaufzeichnung (bei 60–70 dB).

Folgende Anforderung ist darüber hinaus wünschenswert und geht in die Bewertung ein:

- **Aktive Filterung von Geräuschen:** Sollte das Gerät eine aktive Filterung von Umgebungsgeräuschen (z.B. Wind oder Sirenenrauschen, Hall in Unterführungen, fahrende Züge etc.) ermöglichen, so wird dies mit 10 zusätzlichen Punkten bewertet (B12)
- **Lärmbelastete Umgebungen (> 85 dB):** Über die Mindestanforderung hinaus wird die Sprachverständlichkeit in extremen Lärmszenarien bewertet. Bietet das Gerät eine klare und gut verständliche Klangqualität bei einer Umgebungslautstärke von **mehr als 85 dB** (z. B. bei Großveranstaltungen/Menschenmengen oder direktem Straßen-/ Zugverkehr), ohne dass die Aufnahme übersteuert, werden hierfür 10 Zusatzpunkte vergeben (B13 – Klare Sprachaufzeichnung (bei >85 dB)).

3.3.6 Akustisches Startsignal

Wenn ein Beamter eine Bodycam aktiviert und die Aufnahme beginnt, muss es ein klares, erkennbares akustisches Signal geben, ein Piepton oder ähnliches. Dieses Signal dient mehreren Zwecken:

- Erstens informiert es den Beamten selbst, dass die Aufnahme tatsächlich begonnen hat. Dies ist besonders wichtig, wenn das Gerät in einer Umgebung mit vielen Reizen verwendet wird, wo visuelle oder haptische Rückmeldungen möglicherweise übersehen werden.
- Zweitens informiert es die Personen in der Umgebung (den Adressaten polizeilicher Maßnahmen, Zeugen oder beteiligte/unbeteiligte Personen), dass eine Videoaufnahme läuft.

Das Signal muss laut genug sein, um in einer lauten Umgebung aus mindestens 1 Meter Entfernung noch deutlich gehört zu werden (M23 – Akustisches Startsignal (1m Entfernung)).

3.3.7 Optische und andere Benachrichtigungen

Neben akustischen Signalen muss die Bodycam mehrere optische und haptische Rückmeldungen bieten:

- Während einer aktiven Aufnahme muss eine LED (Light Emitting Diode) blinken oder leuchten, oder bei Geräten mit Display muss eine Anzeige auf dem Display erfolgen. Dies visualisiert für den Beamten und für Personen in der Umgebung, dass eine aktive Aufnahme läuft (M24 – LED-Statusanzeige (Aufnahme)).
- Der Akku-Ladestand muss zu jeder Zeit erkennbar sein, entweder durch LED-Indikatoren (beispielsweise grünes Licht = gut geladen, gelbes Licht = mittelmäßig geladen, rotes Licht = niedrig bzw. durch mehrere Punkte oder Striche) oder durch eine digitale Anzeige (M25 – Statusanzeige (Akkuladezustand)).
- Der Speicherplatz muss überwacht werden. Wenn der verfügbare Speicher knapp wird, muss das Gerät eine Warnung geben, visuell (LED oder Display), akustisch (Piepton) und/oder haptisch (Vibration) (M26 – Warnmeldung visuell, akustisch oder haptisch (Speicherplatzknappheit)).

Als Bewertungskriterium sind weitere Status-Anzeigen definiert:

- Wenn das Gerät mit einem WiFi-Netzwerk verbunden ist, sollte dies angezeigt werden. Dies wird mit 5 Punkten bewertet (B14 – Statusanzeige (mit Wifi verbunden)).
- Wenn das Gerät LTE/5G-Mobilfunkverbindung hat, sollte dies angezeigt werden. Dies wird mit 5 Punkten bewertet (B15 - Statusanzeige (mit LTE/5G verbunden)).
- Wenn das Gerät über Bluetooth mit anderen Geräten verbunden ist, sollte dies angezeigt werden. Dies wird mit 5 Punkten bewertet (B16 - Statusanzeige (mit Bluetooth verbunden)).
- Wenn das Gerät über ein Display verfügt, sollten Datum und Uhrzeit angezeigt werden. Dies wird mit 5 Punkten bewertet (B17 – Statusanzeige (Datum und Uhrzeit)).
- Wenn Debug-Informationen wie Firmware-Version und Gerätetype im Display angezeigt werden, wird dies mit 5 Punkten bewertet (B18 – Statusanzeige (Debug-Information)).

3.4 Schnittstellen und Konnektivität

3.4.1 USB-C Anschluss

Die Auftragnehmerin muss einen USB-C Anschluss in die Bodycam integrieren (M27 – USB-C (Anschluss vorhanden)). USB-C ist ein moderner, standardisierter Anschluss, der folgende Funktionen unterstützt:

- Der USB-C Anschluss ermöglicht das Aufladen des Akkus der Bodycam über ein Standard-Ladekabel und -netzteil. Dies ist das primäre Ladesystem, sofern keine gleichzeitige Ladung über eine Dockingstation und damit gleichzeitigem Upload der Aufzeichnungen vorgesehen ist (M28 – USB-C (Ladefunktion)). Dieser (USB-C Anschluss) muss zuverlässig funktionieren.

- Über USB-C können Videos und andere Dateien vom Gerät auf einen Computer übertragen werden (M29 – USB-C (Dateiübertragung)). Dies ist eine Backup- und Wiederherstellungsmöglichkeit, falls die Cloud-Infrastruktur nicht verfügbar ist. Wobei hier auch auf die jeweiligen Rollen inkl. der jeweiligen Berechtigungen geachtet werden muss. Der Transfer muss nicht zwingend direkt am PC per Kabel erfolgen, sondern kann per Dockingstation oder über einen herstellerspezifisch abgesicherten USB-C-Datenpfad realisiert werden.
- Über USB-C können administrative Änderungen, Kalibrierungen und Firmware-Updates durchgeführt werden (M30 – USB-C (administrative Änderungen)).

3.4.2 WiFi-Konnektivität

WiFi ist ein Standard-Kommunikationsprotokoll und essentiell für die Cloud-Integration. Die Bodycam muss WiFi 802.11ac, 802.11b, 802.11g, und 802.11n unterstützen (M31 – WiFi-Konnektivität). Dies sind etablierten Normen, die eine weitverbreitete Kompatibilität gewährleisten.

Der Beamte oder Administrator muss in der Lage sein, das WiFi-Modul ein- und auszuschalten, um Energie zu sparen, wenn WiFi nicht benötigt wird, oder um die Verbindung zu unterbrechen, wenn datenschutz sensible Aufnahmen gemacht werden, die nicht automatisch hochgeladen werden sollen, sofern ein live-Upload vorgesehen ist.

3.4.3 Automatischer Cloud-Upload

Das System muss einen vollautomatisierten Upload der erfassten Aufnahmen in die Speicherinfrastruktur (SaaS-Dienst) gewährleisten, sobald sich das Gerät in einer definierten Upload-Umgebung befindet. Als Mindeststandard wird der Upload über eine Dockingstation (kabelgebundenes LAN oder WLAN) gefordert, der gleichzeitig mit dem Ladevorgang erfolgt (M32 – Automatischer Cloud-Upload).

Um Datenverlust vorzubeugen, muss der Upload-Prozess zwingend fehlertolerant ausgelegt sein. Bei Verbindungsabbrüchen (z. B. Entnahme des Geräts aus dem Dock, Netzwerkschwankungen) muss das System den Upload zu einem späteren Zeitpunkt an exakt der unterbrochenen Stelle fortsetzen oder die Datei neu übertragen, ohne dass es zu Datenkorruption oder -verlust kommt (M33 – Automatischer Cloud-Upload (Fortsetzung nach Unterbrechung)). Der Status des Uploads muss für den Anwender am Gerät oder an der Station erkennbar sein (z. B. durch LED-Statusanzeige oder Display) (M34 – Statusanzeige bei automatischem Cloud-Upload).

3.4.4 Mobile Netzwerk-Unterstützung und Live-Streaming

Die Fähigkeit zur Datenübertragung unabhängig von stationärer Infrastruktur wird als qualitativer Mehrwert betrachtet.

Autarke Mobilfunk-Anbindung (LTE/5G): Bieter erhalten 15 Punkte, wenn die Bodycam über ein integriertes Mobilfunkmodem (SIM/eSIM) verfügt (B19 – Mobile Netzwerkunterstützung (LTE/5G)).

Dies muss technisch ermöglichen:

- Den sofortigen Upload von kritischen Beweisvideos bereits im Einsatzgebiet ("Field-Upload"), ohne dass ein Tethering mit einem Smartphone oder Router notwendig ist.
- Die Unabhängigkeit von lokalen WLAN-Netzwerken.

Live-Streaming (Real-Time Situational Awareness): Zusätzlich wird bewertet, ob das System in der Lage ist, das Videobild und Audio in Echtzeit an die Cloud-Software zu übertragen, um Einsatzleitern oder dem Kommandostab einen Live-Einblick in die Lage zu ermöglichen (B20 - Live-Streaming (Real-Time Situational Awareness)). Diese Funktion wird mit 20 Punkten aufgrund der Komplexität bewertet.

Die Nutzung dieser Funktion setzt zwingend folgende technische und organisatorische Sicherheitsmechanismen voraus, die vom Bieter vollständig zu implementieren sind:

- **Erheblichkeitsschwelle:** Die Live-Übertragungsfunktion darf ausschließlich in Situationen ab einer definierten Erheblichkeitsschwelle aktiviert werden (z. B. lebensbedrohliche Einsatzlagen). Eine Aktivierung im Regelbetrieb außerhalb solcher Lagen ist grundsätzlich nicht vorgesehen. Daher muss eine Möglichkeit bestehen diese Funktion technisch zu unterbinden oder eine Aktivierung zumindest automatisiert zu dokumentieren.
- **Rollenbasierte Zugangsbeschränkung:** Der Zugriff auf laufende Live-Übertragungen muss technisch auf einen eng begrenzten, berechtigten Personenkreis (z. B. Dienstgruppenleitung, Leitstelle, Polizeiführer) beschränkt sein. Dies muss über das Rollen- und Berechtigungskonzept der Cloud-Software (siehe Kapitel 4.4) einzustellen und zu differenzieren sein.
- **Übertragungsweg:** Der Live-Abruf muss entweder direkt zwischen der Bodycam und dem berechtigten Empfänger oder über die Cloud-Plattform erfolgen können. Beide Varianten setzen eine Echtzeit-Übertragung (Upload) der laufenden Aufzeichnung voraus.

Da die einsatztaktische Priorität dieser Funktion als nachrangig eingestuft wird, erfolgt die Bewertung ausschließlich als qualitativer Mehrwert. Eine Erfüllung dieser Anforderung ohne vollständige Implementierung der vorstehenden Sicherheitsmechanismen wird nicht bewertet

3.4.5 Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten

Die Bundespolizei nutzt für die taktische Kommunikation Digitalfunkgeräte des Standards TETRA (BOS-Digitalfunk). Zur Steigerung der Eigensicherung der Beamten sowie zur signifikanten Verbesserung der Dokumentationsqualität stellt die Interoperabilität zwischen den angebotenen Bodycams und diesen Funkgeräten eine erweiterte Anforderung dar. Die technische Umsetzung muss dabei zwingend kompatibel zu den bei der Auftraggeberin/Bedarfsträgerin vorhandenen Bestandsgeräten der Hersteller **Motorola Solutions (insbesondere MTP6000-Serie und MXP600)** sowie, wenn möglich, zusätzlich **Sepura (STP- und SC-Serie)** sein.

Mindestanforderungen: Die Bodycam muss über eine integrierte, drahtlose Bluetooth-Schnittstelle verfügen, die eine Kopplung mit den genannten Digitalfunkgeräten Funkgeräten des Herstellers Motorola Solutions (Serien MTP6000/MXP600) ermöglicht. Hierbei ist zwingend sicherzustellen, dass die IT-Sicherheit durch eine verschlüsselte Bluetooth-Strecke (mindestens Standard Bluetooth 4.2 mit Secure Simple Pairing oder höher) gewährleistet ist. Die Kopplung darf die Primärfunktion des Funkgeräts, insbesondere die Sprachkommunikation im BOS-Netz, zu keinem Zeitpunkt beeinträchtigen oder stören. Die Auftragnehmerin hat sicherzustellen, dass die Positionierung der Bluetooth-Antenne in der Bodycam so gewählt ist, dass eine stabile Verbindung auch bei verdeckter Tragweise des Funkgerätes unter Einsatzwesten/Bekleidung gewährleistet bleibt (M35 – Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten).

Bewertungskriterien: Über die Mindestanforderungen hinaus werden Lösungen mit einer tiefergehenden funktionalen Integration wie folgt positiv bewertet:

- **Automatische Aktivierung (Trigger-Funktion):** Als Bewertungskriterium ist eine Automatisierung des Aufnahmestarts in kritischen Situationen definiert. Wenn ein Beamter über das gekoppelte Digitalfunkgerät einen Notruf absetzt (z. B. durch Drücken der Notruftaste oder durch einen automatischen Statuswechsel wie „Man-Down“), muss die Bodycam unverzüglich und vollautomatisch die Videoaufzeichnung aktivieren. Diese Funktion dient der Entlastung des Beamten in Stresssituationen von der manuellen Bedienung und stellt sicher, dass Eskalationslagen zuverlässig dokumentiert werden. Die erfolgreiche Umsetzung dieser Trigger-Funktion wird mit 15 Punkten bewertet (B21 - Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten (Trigger-Funktion)).
- **Bluetooth-Konnektivität zu Sepura (STP- und SC-Serie):** Als Bewertungskriterium wird eine Konnektivität zu Bestandsgeräten der Auftraggeberin/Bedarfsträgerin des Herstellers Sepura festgelegt. Die erfolgreiche Umsetzung dieser Funktion wird mit 15 Punkten bewertet (B22 - Bluetooth-Schnittstelle zu Geräten des Herstellers Sepura (STP- und SC-Serie)).
- **Erweiterte Audio-Dokumentation (Sprachaufzeichnung):** Darüber hinaus werden Systeme bevorzugt, die mittels der verschlüsselten Bluetooth-Verbindung nicht nur Steuersignale empfangen, sondern auch eine bidirektionale Übertragung von Audiodaten ermöglichen. In dieser Ausbaustufe muss die Bodycam den über das Funkgerät geführten Sprechfunkverkehr (sowohl eingehende Funksprüche als auch das eigene Gesprochene) als zusätzliche Tonspur synchron zum Video aufzeichnen. Dies ermöglicht eine lückenlose Rekonstruktion des Einsatzablaufes inklusive der taktischen Kommunikation. Die Bereitstellung dieser synchronen Audio-Dokumentation wird mit weiteren 15 Punkten bewertet (B23 - Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten (Sprachaufzeichnung)).

Die Überprüfung der tatsächlichen Kompatibilität und Funktionstiefe erfolgt im Rahmen der praktischen Erprobung in der Teststellung. Hierzu werden dem Bieter Referenzgeräte der Bundespolizei zeitlich begrenzt zur Verfügung gestellt, um das Pairing sowie die Trigger- und Audiofunktionen unter realistischen Bedingungen während eines Labortests nachzuweisen.

3.5 Akku und Ladeinfrastruktur

3.5.1 Akku-Anforderungen

Der Akku ist das Herzstück der Bodycam, ohne einen zuverlässigen, langlebigen Akku ist das Gerät unbrauchbar. Die Auftragnehmerin muss daher folgende Spezifikationen erfüllen.

Der Akku muss wiederaufladbar sein, das heißt, er kann mindestens eintausend Mal auf- und entladen werden, nicht nur einmal verwendet und dann entsorgt werden. Dies ist aus ökologischen und wirtschaftlichen Gründen essentiell (M36 – Akku wiederaufladbar).

Der Akku muss eine dauerhafte Aufnahmezeit von mindestens 10 Stunden bei 1080p-Auflösung und 25 FPS bereitstellen. Ein Beamter muss während einer 12h+-Schicht mit einem Akku-Ladezyklus auskommen (Stand-by-Betrieb), ohne dass der Akku während der Schicht gewechselt oder bei festverbautelem Akku die Bodycam geladen werden muss (M37 – Akkulaufzeit (Aufnahmezeit min. 10h)). Lösungen mit fest integriertem Akku sind ausdrücklich zulässig, bilden jedoch den spezifischen operativen Bedarf der Bundespolizei hinsichtlich der taktischen und logistischen Flexibilität im dynamischen 24/7-Einsatzgeschehen (Sicherung des ununterbrochenen Streifendienstes im Feld ohne zeitaufwändige Rückkehr zur Dienststelle) schlechter ab. Sofern die Mindestanforderung M37 erfüllt wird, ist seitens der Bieter solcher Fest-Akku-Systeme zwingend ein vollumfängliches logistisches Versorgungskonzept mit definierten Austausch- und Reparaturfristen darlegt, das die dauerhafte Einsatzbereitschaft über die Vertragslaufzeit sicherstellt.

Ein Akku, der werkzeuglos wechselbar ist, wird positiv mit zusätzlichen 10 Punkten bewertet (B24 – Akkuwechsel). Aufgrund des taktischen Bedarfs an maximaler Autonomie im Feld vergibt die Auftraggeberin diese qualitativen Zusatzpunkte ausschließlich für physisch und werkzeuglos im laufenden Betrieb durch die Einsatzkraft entnehmbare Akkus. Systeme mit fest integriertem Akku können diesen operativen Mehrwert konzeptionell nicht erbringen und erhalten im Kriterium B24 zwingend 0 Punkte.

Ein Bieter, der einen Akku mit einer Laufzeit von mehr als 12 Stunden Aufnahmezeit bietet, wird positiv mit zusätzlichen 10 Punkten bewertet (B25 - Akkulaufzeit (Aufnahmezeit > 12h)). Zudem werden Ladestationen/Dockingstationen die eine Schnellladefunktion und somit eine vollständige Ladung der Akkus innerhalb < 4h bieten mit zusätzlichen 5 Punkten bewertet (B26 – Ladestation/Dockingstation mit Schnellladefunktion (Akku innerhalb < 4h vollgeladen)).

Energiekonzept

Die Bodycam muss über ein belastbares Energiekonzept verfügen, das eine verlässliche Nutzung im polizeilichen Schichtbetrieb gewährleistet. Die Sicherstellung der geforderten Einsatzverfügbarkeit ist unabhängig von der technischen Ausgestaltung des angebotenen Systems geschuldet. Zulässig sind daher sowohl Lösungen mit wechselbaren Akkus als auch Lösungen mit fest integrierten Akkus oder funktional gleichwertigen Versorgungskonzepten, sofern die weiteren Anforderungen dieser Leistungsbeschreibung vollumfänglich erfüllt werden. Sämtliche Kostenbestandteile, die für die Grundausstattung der ausgeschriebenen Bodycam-Systeme zur Sicherstellung der

Energieversorgung und Einsatzverfügbarkeit erforderlich sind, sind im Preis des Bodycam-Komplettsystems einzupreisen. Dies umfasst insbesondere, je nach angebotenen System, Akkus, Ersatz- oder Reserveakkus, Lade- oder Wechselkomponenten, Vorhalte- oder Austauschgeräte sowie sonstige Bestandteile eines zur Erfüllung der Leistungsbeschreibung erforderlichen Versorgungskonzepts.

3.5.2 Externe Akku-Ladeinfrastruktur (Stand-Alone)

Ergänzend zur im vorherigen Kapitel positiv bewerteten Wechselbarkeit der Energiespeicher sollte, sofern vom Bieter umgesetzt, eine Ladeinfrastruktur bereitgestellt werden, die das unabhängige Aufladen von Reserve-Akkus außerhalb der Bodycam ermöglicht (z.B. für Pool-Akkus oder längere Einsätze) und wird im Rahmen der qualitativen Bewertung mit 10 Punkten berücksichtigt (B27 – Stand-Alone-Ladestation).

Hierbei gilt folgende Vorgabe:

- Die Ladestationen/Dockingstationen sollten einen separaten Akku sicher aufnehmen und laden, ohne dass eine Bodycam als "Ladewirt" benötigt wird.

Um die permanente Einsatzbereitschaft im Schichtdienst logistisch und dezentral abzusichern, bewertet die Auftraggeberin das Vorhandensein einer solchen stand-alone-fähigen Ladeinfrastruktur für Zusatz-Energiespeicher positiv. Ein logistisches Austausch- oder Poolgerätekonzept für vollständige Kamerasysteme im Werk stellt im operativen und dezentralen Dienstbetrieb keinen gleichwertigen Ersatz für das direkte, standortunabhängige Vorhalten und Wechseln von Akkumulatoren dar. Für Systeme mit fest integriertem Akku können die Zusatzpunkte im Kriterium B27 sowie im darauffolgenden Kriterium B28 (Multi-Port-Ladestation) daher nicht vergeben werden. Diese Systeme werden in den Kriterien B27 und B28 pauschal und zwingend mit 0 Punkten bewertet.

3.5.3 Multi-Dockingstationen und Kombi-Ladefunktion

Die Dockingstation dient als zentrale Schnittstelle für den Schichtwechsel (Upload & Laden). Um die in Kapitel 3.5.1 geforderte Effizienz beim Akku-Management zu unterstützen, wird die Funktionalität der Dockingstationen wie folgt gefordert und bewertet:

Mindestanforderung:

- Bereitstellung von Ladestationen/Dockingstationen mit EU-Standardstecker (Typ F/C, 230V, 50Hz) (M38 – Ladestation/Dockingstation mit EU-Standardstecker (Typ F/C, 230V, 50Hz)). Gleichzeitiges Laden und Datenübertragung (Upload) für mehrere eingesteckte Bodycams (M39 – Dockingstation (gleichzeitiges Laden und Datenübertragung)).

- Integrierter Überhitzungsschutz für die Ladefunktion (M40 – Dockingstation (integrierter Überhitzungsschutz)). Bei Systemen mit wechselbaren Akkus umfasst der Überhitzungsschutz sowohl die Bodycams als auch die separat geladenen Zusatzakkus.
- Visualisierung des Status (Laden/Fertig/Upload) (M41 – Dockingstation (Statusanzeige: Laden/Fertig/Upload)). Die Dockingstation oder die angedockte Bodycam muss den Status (Ladevorgang, Abschluss des Uploads) klar visualisieren. Eine Anzeige direkt über das Display der Bodycam im angedockten Zustand ist zulässig, sofern der Status auf einen Blick und ohne Interaktion (kein Tastendruck, kein Aufwecken des Displays erforderlich) erkennbar ist.

Im Falle eines wechselbaren Akkus wäre die Bereitstellung von Multi-Port-Stationen, die neben der Bodycam auch gleichzeitig mindestens sechs (6) Zusatzakkus laden können, wünschenswert und wird im Rahmen der qualitativen Bewertung mit 10 Punkten berücksichtigt (B28 – Multi-Port-Ladestation)

3.5.4 Firmware-Updates über Dockingstation

Die Dockingstation fungiert als zentraler Verteilungspunkt für Software-Wartung und Firmware-Updates.

Sobald ein Firmware-Update zentral durch die System-/Fachadministration freigegeben wurde, muss die Dockingstation dieses Update automatisch auf die eingesteckten Bodycams übertragen und installieren. Dieser Prozess muss interventionsfrei ("Zero-Touch") erfolgen, d. h. der Anwender (Polizeibeamte) darf keine manuellen Bestätigungen am Gerät vornehmen oder Menüs bedienen müssen (M42 – Dockingstation (automatische Firmwareupdates)).

Firmware-Updates dürfen die Einsatzbereitschaft im laufenden Dienst nicht beeinträchtigen.

Ein Update während des Tragens im Einsatz oder während einer laufenden Aufzeichnung darf nicht zu einer Unterbrechung der Aufnahme oder zu einem Funktionsverlust führen. Läuft ein Update dennoch parallel im Hintergrund, muss systemseitig sichergestellt sein, dass dies zu keinem Fehlerzustand sowohl bei den Aufzeichnungsdateien als auch beim Update führt und der Vorgang bei erneutem Einstellen in die Dockingstation nahtlos fortgesetzt oder wiederholt werden kann (M43 – Firmwareupdates während der Nutzung (ohne Beeinträchtigung)).

Der Update-Vorgang soll vorzugsweise parallel zum Ladevorgang und Daten-Upload stattfinden und darf die Einsatzbereitschaft zum nächsten Schichtbeginn nicht gefährden (z. B. durch intelligente Zeitsteuerung oder Priorisierung des Ladevorgangs).

Ein Status-Indikator (z. B. LED an der Station oder am Gerät) muss klar erkennbar signalisieren, dass ein Update läuft oder noch nicht abgeschlossen ist, um ein verfrühtes Entnehmen zu verhindern und dem Nutzer eine verlässliche Einschätzung der Einsatzbereitschaft zu ermöglichen (M44 – Statusanzeige bei Firmwareupdate)

3.6 Reparatur und Wartung

3.6.1 Langfristige Versorgungs- und Reparatursicherheit

Zur Sicherung der Investition ist eine langfristige Nutzbarkeit der Hardware gefordert.

Die Auftragnehmerin gewährleistet die Verfügbarkeit von Ersatzteilen, Reparaturdienstleistungen und Service-Support für einen Zeitraum von mindestens 6 Jahren ab dem Zeitpunkt der Lieferung (M45 – Versorgungs- und Reparatursicherheit).

Für diesen Zeitraum wird ein entsprechender Instandsetzungs- bzw. Servicevertrag als Teil der Ausschreibung abgeschlossen.

Sollte eine Reparatur oder die Beschaffung identischer Ersatzteile aufgrund von Obsoleszenz (End-of-Life von Komponenten) innerhalb dieses Zeitraums technisch oder wirtschaftlich unmöglich werden, ist die Auftragnehmerin berechtigt und verpflichtet, einen Austausch gegen ein technisch gleichwertiges oder höherwertiges Nachfolgemodell vorzunehmen. Dabei muss die volle Kompatibilität zur bestehenden Peripherie (Dockingstationen, Software-Backend) sichergestellt bleiben oder, falls dies nicht möglich ist, die notwendige Peripherie für die Austauschgeräte kostenneutral mitgeliefert werden.

Soweit das angebotene System zur Sicherstellung der Einsatzverfügbarkeit auf Austausch-, Vorabtausch-, Ersatzgeräte- oder vergleichbare Versorgungskonzepte angewiesen ist, müssen diese für denselben Zeitraum in den Instandsetzungs- und Serviceprozess einbezogen sein. Die hierfür für die Grundausstattung erforderlichen Leistungen und Kosten sind Bestandteil des angebotenen Systems.

3.6.2 Kommunikation in deutscher Sprache

Jegliche Kommunikation zwischen Auftraggeberin/Bedarfsträgerin und der Auftragnehmerin (Abrufe, Supportanfragen, Reparaturberichte, Rechnungen, Dokumentation etc.) muss in deutscher Sprache erfolgen. Die Auftragnehmerin muss deutschsprachige Mitarbeiter beschäftigen oder Verträge mit Dienstleistern haben, um diese Anforderung zu erfüllen.

3.6.3 Hotline-Support und Reaktionszeiten

Die Auftragnehmerin muss für Hardwarefragen (Bodycams, Akkus, Lade- und Dockingstationen sowie sonstiges Zubehör) eine Hotline bieten, erreichbar Montag bis Freitag, von 08:00 bis 17:00 Uhr deutscher Zeit (inkl. jeglicher Feiertage). Die Hotline muss via Telefon, E-Mail und Ticketsystem verfügbar sein. Ein Beamter oder Administrator kann die Hotline anrufen oder ein Ticket einreichen, wenn ein Hardwareproblem auftritt (z.B. Defekt einer einzelnen Bodycam, Ladeproblem an der Dockingstation oder auffälliges Verhalten eines Akkus).

Die Reaktionszeit, die Zeit vom Eingang der Meldung bis zur ersten Antwort durch eine technisch qualifizierte Person, richtet sich nach der Auswirkung auf die Einsatzfähigkeit der Hardware:

- Für hochgradig problematische Fälle (Ausfall mehrerer Bodycams oder einer Dockingstation, die von der Dienststelle im Schichtbetrieb genutzt wird) ist eine Reaktionszeit innerhalb des nächsten Werktages von 4 Stunden akzeptabel.
- Für mittel-prioritäre Probleme (z. B. Display- oder Gehäuseproblem einer einzelnen Bodycam) ist eine Reaktionszeit innerhalb des nächsten Werktages von 8 Stunden akzeptabel.
- Für kosmetische oder niedrig-prioritäre Probleme ist eine Reaktionszeit innerhalb des nächsten Werktages von 24 Stunden akzeptabel.

Kritische Vorfälle im Sinne eines Ausfalls oder Angriffs auf die Cloud-Software, die Upload- und Speicherinfrastruktur oder den Zugriff auf Aufnahmen werden nicht unter dieser Ziffer, sondern in den Service-Level-Vereinbarungen zum SaaS-Dienst (siehe Kapitel 5 - Service und Support) geregelt.

3.6.4 Instandsetzung und Austausch-Service (RMA-Prozess)

Zur Minimierung von Ausfallzeiten wird ein effizienter Prozess für Defektgeräte gefordert.

1. Reaktionszeit und Vorab-Austausch (SLA)

Im Falle eines Hardware-Defekts muss die Einsatzfähigkeit der Dienststelle priorisiert wiederhergestellt werden. Meldet die Auftraggeberin/Bedarfsträgerin ein Gerät als defekt (RMA-Eröffnung), muss die Auftragnehmerin innerhalb von 5 Werktagen ein voll funktionsfähiges Austauschgerät (gleicher Typ und Konfiguration) an die betroffene Dienststelle versenden. Dies gilt unabhängig davon, ob das defekte Gerät bereits bei der Auftragnehmerin eingegangen ist.

2. Reparatur vs. Austausch

Es steht der Auftragnehmerin frei, ob sie das defekte Gerät repariert und zurücksendet oder das bereitgestellte Austauschgerät dauerhaft bei der Auftraggeberin/Bedarfsträgerin verbleibt ("Gerätetausch"). Im Falle einer Reparatur muss diese innerhalb von 15 Werktagen (inkl. Versandwege) abgeschlossen sein.

3. Kosten und Abwicklung

Innerhalb der Gewährleistung/Garantie erfolgt der Austausch/Reparatur kostenfrei (inkl. Hin- und Rückversand). ~~Bei Beschädigungen außerhalb der Garantie (z.B. Gewaltschäden) gelten die im Preisblatt vereinbarten Reparaturpauschalen.~~ Sämtliche Leistungen im Zusammenhang mit dem RMA-Prozess (Fehleranalyse, Austauschgerät, Reparatur, Geräte austausch, Ersatzteile, Hin- und Rückversand sowie sonstige Maßnahmen zur Wiederherstellung der Betriebsbereitschaft) sind durch die Instandhaltungspauschale (siehe Pos. 2 im Preisblatt) abgegolten, eine gesonderte Vergütung erfolgt nicht. Ein individueller Kostenvoranschlag ist nur auf ausdrückliche Anforderung der Auftraggeberin/Bedarfsträgerin (bei Totalschaden) zu erstellen, um Verwaltungsprozesse schlank zu halten.

4. Ersatzteil-Qualität

Verbaute Ersatzteile oder Austauschgeräte müssen technisch neuwertig und voll funktionsfähig sein. Der Einsatz von werksüberholten Komponenten ("Refurbished") ist zulässig, sofern diese den gleichen Qualitätsstandards und Garantiebedingungen wie Neuteile entsprechen.

5. Datenschutz und Datensicherheit im RMA-Prozess

Die Auftragnehmerin darf auf im internen Gerätespeicher gespeicherte Aufnahmen zu keinem Zeitpunkt zugreifen. Ein technischer Zugang im Rahmen der Reparatur ist durch geeignete Maßnahmen (z. B. verschlüsselte Speicherung, s. Kapitel 3.2.4) auszuschließen. Daher hat vor der Rücksendung eines defekten Geräts an die Auftragnehmerin die Auftraggeberin/Bedarfsträgerin dafür Sorge zu tragen, dass alle im internen Speicher der Bodycam befindlichen Bild- und Tonaufzeichnungen gesichert und anschließend vollständig vom Gerät gelöscht sind. Der Nachweis der erfolgreichen Löschung ist vom zuständigen Fachadministrator zu dokumentieren.

Sollte eine vollständige Löschung vor Einsendung aufgrund des Defekts technisch nicht möglich sein, ist dies der Auftragnehmerin unverzüglich zu melden. Die Auftragnehmerin muss dann ein datenschutzkonformes Verfahren anbieten, z. B.

- Sofortiger physischer Speichermodul-Austausch vor jeder Reparatur (der defekte Speicher wird ungelöscht an die Auftraggeberin/Bedarfsträgerin zurückgesendet oder zerstört, nach vorheriger Absprache).
- Nachweisbare Blindlöschung oder Überbrennung des Speichers unter Aufsicht der Bundespolizei.

Das weitere Vorgehen ist gemeinsam abzustimmen.

Die Auftragnehmerin verpflichtet sich, empfangene Geräte nicht auf vorhandene Daten zu analysieren oder auszulesen, und hat dies durch geeignete technische und organisatorische Maßnahmen (TOMs) sicherzustellen und nachzuweisen (z. B. durch unabhängige Audit-Berichte).

Die im Rahmen dieses Prozesses erforderlichen Leistungen und Kosten sind, soweit sie für die Grundausstattung des angebotenen Systems erforderlich sind, im Preis des Bodycam-Komplettsystems zu berücksichtigen.

4. Cloud-Software und SaaS-Modell

Dieses Kapitel beschreibt sämtliche Anforderungen an die cloudbasierte Software-Infrastruktur, die als Software-as-a-Service (SaaS) bereitzustellen ist. Die Cloud-Software bildet die zentrale Plattform für die Verwaltung, Speicherung, Archivierung und Verarbeitung aller durch die Bodycams erfassten Aufnahmen. Sie ist damit ein gleichrangig kritischer Bestandteil der Gesamtlösung wie die Hardware selbst.

4.1 Grundlegende Prinzipien und Anforderungen

Die Cloud-Software ist das zentrale Verwaltungs- und Analysewerkzeug für alle erfassten Bodycam-Videos. Sie muss nicht nur funktional, sondern auch sicher, benutzerfreundlich, konform mit deutschen und europäischen Datenschutzgesetzen sein und möglichst barrierearm sein.

4.1.1 Digitale Souveränität und Vendor-Lock-In-Vermeidung

Die Bundespolizei muss die volle Kontrolle über ihre Daten bewahren. Dies bedeutet, dass die Bundespolizei nicht in einen Zustand geraten darf, in dem sie an einen Anbieter so stark gebunden ist, dass ein Wechsel zu einer anderen Software oder Cloud praktisch unmöglich ist.

Die Auftragnehmerin muss daher mehrere Maßnahmen treffen, um Digitale Souveränität zu gewährleisten:

- Die Auftragnehmerin muss Standard-Technologien verwenden, nicht proprietäre oder undokumentierte Technologien. Beispiele für offene Standards (M46 – SaaS - Verwenden von Standardtechnologie (REST, JSON, XML etc.):
 - REST-basierte APIs,
 - Standard-Videoformate (MP4),
 - Standard-Dateiformate (JSON, XML) für Metadaten.
- Die Bundespolizei muss in der Lage sein, ihre Daten vollständig aus dem System zu exportieren. Dies bedeutet, dass die Auftragnehmerin umfassende Datenexport-Funktionen bieten muss, mit denen Videos, Metadaten, Benutzer- und Berechtigungsinformationen in standardisierten, nicht-proprietären Formaten exportiert werden können (M47 – SaaS – Datenexport).
- Die Auftragnehmerin muss eine vollständige, öffentliche Dokumentation der REST-API bereitstellen, sodass die Bundespolizei oder andere Dienstleister Integrationen oder Anpassungen durchführen können (M48 – SaaS – Dokumentation der REST-API).

Diese Prinzipien sind Mindestanforderungen und müssen ohne Ausnahme erfüllt werden.

4.1.2 IT-Sicherheit und Verschlüsselung

Die Videos, die in der Cloud gespeichert werden, sind sensible Daten. Sie enthalten Bilder und damit personenbezogene Daten von Personen in Konfrontationen mit der Polizei, potenziell verletzte Personen, der Einsatzkräfte selbst und möglicherweise auch unbeteiligter Dritte. Ein hohes Niveau von IT-Sicherheit ist daher essentiell und ein datenschutzkonformer Umgang wird seitens der Bundespolizei erwartet.

Die Auftragnehmerin muss folgende Sicherheitsstandards einhalten:

- Die angebotene SaaS-Lösung muss nach dem Stand der Technik und unter Berücksichtigung der für Cloud-Dienste einschlägigen Vorgaben und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) konzipiert, betrieben und fortlaufend

weiterentwickelt werden. (M49 – SaaS – BSI Empfehlungen). Die Auftragnehmerin muss hierfür mindestens ein dokumentiertes Informationssicherheitskonzept vorhalten, das insbesondere folgende Bereiche abdeckt:

- Berechtigungs- und Rollenkonzept, einschließlich Mehr-Faktor-Authentisierung für privilegierte Zugänge,
- Mandantentrennung und Zugriffsschutz,
- Protokollierung sicherheitsrelevanter Ereignisse,
- Schwachstellen-, Patch- und Änderungsmanagement,
- Backup-, Wiederherstellungs- und Notfallmanagement,
- Incident-Response-Prozesse,
- Verschlüsselungskonzept für Datenübertragung und Datenspeicherung,
- sichere Administratorzugänge sowie technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten.

Als Mindestanforderung gilt, dass die Auftragnehmerin mit dem Angebot ein belastbares IT-Sicherheitskonzept einreicht, aus dem die Umsetzung der vorstehenden Anforderungen nachvollziehbar hervorgeht.

Der Nachweis kann erbracht werden durch:

- ein aktuelles BSI-C5-Testat oder einen vergleichbaren unabhängigen Prüfbericht oder
- eine gleichwertige, prüffähige Dokumentation, aus der die Umsetzung der oben genannten Sicherheitsanforderungen eindeutig hervorgeht.

Die Auftraggeberin/Bedarfsträgerin behält sich vor, ergänzende Unterlagen zum Nachweis der Gleichwertigkeit anzufordern.

- Alle Videos und Metadaten, die auf Servern gespeichert sind, müssen mit AES-256-Verschlüsselung verschlüsselt sein (M50 – SaaS – AES-256 Verschlüsselung).
- Alle Daten, die über das Netzwerk übertragen werden, etwa wenn ein Beamter ein Video von seiner Bodycam zur Cloud hochlädt, müssen verschlüsselt sein. Mindestanforderung: TLS 1.3 oder höher (M51 – SaaS – TLS1.3 oder höher).
- Die Auftragnehmerin muss Mechanismen implementieren, die sicherstellen, dass nur autorisierte Personen auf Daten zugreifen können. Dies wird durch Benutzername/Passwort, Multi-Faktor-Authentifizierung, und rollenbasierte Zugriffskontrolle erreicht (siehe Kapitel 4.4).

4.1.3 Barrierefreiheit nach BITV 2.0

Die Bundesrepublik Deutschland hat sich verpflichtet, öffentliche digitale Dienste barrierefrei zu gestalten. Dies ist in der Barrierefreien Informationstechnik-Verordnung 2.0 (BITV 2.0) geregelt.

Die Auftragnehmerin muss die Cloud-Software so gestalten, dass sie möglichst barrierefrei ist. Dies bedeutet:

- Alle Funktionen müssen mit Tastatur allein bedienbar sein, nicht nur mit Maus.
- Blinde oder sehbehinderte Nutzer sollten die Software mit Hilfe eines Screen Readers (ein Programm, das Text vorliest) nutzen können. Die Auftragnehmerin muss hierzu alt-Attribute und semantische HTML verwenden.
- Die Textfarbe muss sich hinreichend von der Hintergrundfarbe abheben, damit Menschen mit Farbenblindheit oder niedriger Sehkraft den Text lesen können.
- Nutzer sollten die Textgröße vergrößern können, ohne dass die Seite in ihrer Darstellung beeinträchtigt wird.

Dies sind Anforderungen, die während der Feldtestung und bei der schriftlichen Bewertung des Angebots mittels BITV 2.0 Test-Zertifikat überprüft werden (M52 – SaaS – Barrierefreiheit (BITV 2.0 Testat)).

Hinweis: Als Nachweis der Konformität zur BITV 2.0 wird ein Prüfbericht auf Basis der EN 301 549 (WCAG 2.1) akzeptiert. Während Verwaltungsfunktionen vollumfänglich barrierefrei sein müssen, wird für rein visuelle Bearbeitungsfunktionen (z. B. Verpixelung) anerkannt, dass eine vollumfängliche Barrierefreiheit technisch nicht in jedem Punkt umsetzbar ist. Der Bieter muss etwaige Abweichungen in einem Konformitätsbericht detailliert begründen.

4.1.4 Server-/Speicherort in der Europäischen Union

Alle Videos und Metadaten müssen auf Servern gespeichert werden, die sich in der Europäischen Union befinden (M53 – SaaS – Server-/Speicherstandort). Deutschland ist der bevorzugte Speicherort. Gründe für diese Anforderung:

- Die Europäische Union hat strengere Datenschutzgesetze als viele andere Regionen. Die Allgemeine Datenschutzverordnung (GDPR) bietet mehr Schutz für die Daten von EU-Bürgern.
- Die Bundesrepublik möchte sicherstellen, dass ihre Daten unter deutscher und europäischer Kontrolle bleiben.
- Speicherung in Deutschland bedeutet niedrige Latenz (kurze Übertragungszeiten), was besser für Live-Streaming und schnelle Abrufe ist.

4.2 SaaS-Betriebsmodell und Verantwortlichkeiten

4.2.1 Definition des SaaS-Modells

Software as a Service (SaaS) bedeutet, dass die Software als Dienst über das Internet bereitgestellt wird, nicht als ein Produkt, das die Bundespolizei kauft und eigenständig betreibt. Die Auftragnehmerin trägt die volle Verantwortung für den Betrieb.

Dies unterscheidet sich fundamental von anderen Modellen:

- On-Premises: Die Auftragnehmerin liefert Software, die die Bundespolizei auf ihren eigenen Servern installiert und selbst verwaltet.

- Infrastructure as a Service (IaaS): Die Auftragnehmerin stellt nur die Infrastruktur (Server, Speicher, Netzwerk) bereit, die Bundespolizei installiert und verwaltet die Software selbst.
- Platform as a Service (PaaS): Die Auftragnehmerin stellt Infrastruktur und Betriebssystem bereit, die Bundespolizei installiert die Anwendung.

Im SaaS-Modell verwaltet die Auftragnehmerin alles.

4.2.2 Verantwortlichkeiten der Auftragnehmerin

Die Auftragnehmerin trägt folgende Verantwortlichkeiten:

- Die Auftragnehmerin sorgt für Server, Speicherkapazität, Netzwerk-Infrastruktur, und Rechenzentrums-Betrieb. Die Infrastruktur muss redundant ausgelegt sein, sodass kein Einzelausfall den gesamten Service unterbrechen kann.
- Die Auftragnehmerin installiert regelmäßig Updates ihrer eigenen Software sowie Sicherheits-Patches für Drittkomponenten (etwa die Betriebssystem-Komponenten des Servers).
- Die Auftragnehmerin ist verantwortlich dafür, dass Daten wie oben beschrieben verschlüsselt sind.
- Die Auftragnehmerin führt regelmäßige Sicherungen durch und verfügt über einen etablierten Prozessablauf zur Wiederherstellung von Daten, sofern dies erforderlich wird (interner/externer Angriff auf die Daten, Ausfall eines Rechenzentrums, unberechtigte Löschung etc.).
- Die Auftragnehmerin stellt sicher, dass die Software jederzeit (24/7, 365 Tage im Jahr) erreichbar und funktionsfähig ist (siehe Kapitel 5.1 - Service-Level-Agreements (SLAs)).
- Datenzugriffsverbot: Die Auftragnehmerin hat keinen Zugriff auf die in der Cloud gespeicherten Daten der Bundespolizei (Bild- und Tonaufzeichnungen sowie zugehörige Metadaten). Technische Zugangsberechtigungen im Rahmen von Infrastrukturmaßnahmen, Wartungsarbeiten oder Updates sind durch geeignete technische und organisatorische Maßnahmen (TOMs) auf das absolut notwendige Minimum zu beschränken und auszuschließen. Wo ein technischer Zugang zur Infrastruktur unvermeidbar ist (z. B. bei Sicherheitsarbeiten), darf dieser ausschließlich auf Infrastrukturebene erfolgen und keinen inhaltlichen Zugriff auf Aufnahmen oder Metadaten begründen.
- Protokollierung von Infrastrukturmaßnahmen: Sämtliche durch die Auftragnehmerin vorgenommenen Maßnahmen an der Infrastruktur (z. B. Updates, Sicherheitsarbeiten, Konfigurationsänderungen, Datenbankzugriffe) sowie mit ausdrücklicher Zustimmung der Bundespolizei vorgenommene Maßnahmen sind lückenlos zu protokollieren. Diese Protokolle sind der Bundespolizei auf Verlangen unverzüglich zur Verfügung zu stellen.
- Dateibasierte Protokollierung in der Software: Die bereitgestellte Cloud-Software muss eine automatische und unveränderbare Protokollierung für jede einzelne Datei gewährleisten. Diese Protokollierung muss jeden Zugriff und jede Änderung abbilden (wer hat wann was gemacht) und darf weder durch die Auftragnehmerin noch durch Nutzer nachträglich verändert oder gelöscht werden können. Die Originaldatei muss dabei stets unverändert erhalten

bleiben. Bearbeitungen werden ausschließlich an einer automatisiert erstellten Kopie vorgenommen, die als solche gekennzeichnet ist. Es muss die Möglichkeit bestehen, die Metadaten sowie die Protokolle auch nach Löschung der eigentlichen Bild- und Tondatei für einen von der Auftraggeberin/Bedarfsträgerin (Bundespolizei) definierten Zeitraum zu speichern.

4.2.3 Verantwortlichkeiten der Bundespolizei

Die Bundespolizei trägt folgende Verantwortlichkeiten:

- Die Bundespolizei verwaltet Passwörter und Zwei-Faktor-Authentifizierung ihrer Nutzer.
- Die Bundespolizei entscheidet, welche Beamte welche Rollen haben (Standard-Nutzer, Fachadministrator, etc.) und damit welche Zugriffsberechtigungen und Bearbeitungsberechtigungen jeweils übertragen werden.
- Die Bundespolizei legt Richtlinien fest, wie lange Videos aufbewahrt werden, wann sie automatisch gelöscht werden, und unter welchen Bedingungen auf Videos zugegriffen werden darf. Die Umsetzung dieser Festlegungen muss zentral seitens eines Administrators mit entsprechender Berechtigung für die Bundespolizei einstellbar sein.
- Die Bundespolizei stellt sicher, dass die Nutzung der Cloud-Software in Übereinstimmung mit deutschen Datenschutzgesetzen erfolgt.

4.2.4 Personelle Sicherheit und Geheimschutz

Da im Rahmen des SaaS-Betriebsmodells sowie bei der Erbringung von Support- und Wartungsdienstleistungen (sowohl Remote als auch im Falle einer Vor-Ort-Betreuung) potenziell Zugriff auf sensible und sicherheitsrelevante Daten der Bundespolizei erlangt werden kann, gelten für die Auftragnehmerin strenge personelle Sicherheitsanforderungen. Die Auftragnehmerin muss organisatorisch und technisch sicherstellen, dass in diesen Fällen vertrauliche Informationen, Videodaten und Systemzugänge jederzeit ausschließlich befugtem Personal zur Kenntnis gelangen.

Aufgrund der internen Sicherheitsbestimmungen der Sicherheitsbehörden des Bundes wird gefordert, dass alle für die Leistungserbringung notwendigen Mitarbeiter der Auftragnehmerin, welche administrativen oder anderweitig Zugriff auf die Daten der Bundespolizei oder die Cloud-Software haben, zwingend sicherheitsüberprüft sein müssen. Für dieses Personal ist **spätestens zur Aufnahme des Wirkbetriebes** eine erfolgreich abgeschlossene einfache Sicherheitsüberprüfung (SÜ1) gemäß Sicherheitsüberprüfungsgesetz (SÜG) in Verbindung mit der Verschlusssachenanweisung (VSA) zwingend erforderlich (M54 – Sicherheitsüberprüftes Personal (SÜ1)).

Die Auftragnehmerin verpflichtet sich daher:

- Die geforderten Sicherheitsüberprüfungen (mindestens SÜ1 für den Wirkbetrieb) rechtzeitig vornehmen zu lassen.
- Aktuelle und gültige Nachweise über die erfolgreich bestandenen Sicherheitsüberprüfungen der eingesetzten Mitarbeiter vorzuhalten und unverzüglich auf Verlangen der Bundespolizei vorzulegen.

Es ist sicherzustellen, dass alle eingesetzten Mitarbeiter vor Aufnahme ihrer Tätigkeit entsprechende Geheimhaltungserklärungen abgeben.

4.3 Funktionale Anforderungen an die Cloud-Software

4.3.1 Grundlegende Funktionen

Die Cloud-Software muss die folgenden grundlegenden Funktionen bieten:

- **Sichtung und Abruf von Aufnahmen:** Beamte und Administratoren müssen in der Lage sein, Videos abzurufen für deren Einsichtnahme und ggf. Bearbeitung sie aufgrund ihrer zugewiesenen Rolle berechtigt sind. Dies sollte über einen Web-Browser möglich sein, ohne dass spezielle Software installiert werden muss. Nutzer sollten ihre eigenen Videos sehen können (M55 – Software – Anzeige/Abspielen von Videos). Erweiterte Nutzer, Administratoren und Führungskräfte sollten je nach Rolle Videos einsehen oder Bearbeiten können.

- Zum Bearbeiten gehören insbesondere: Schneiden, Benennen von Datei und Sequenzen, Bildverbesserungen, Standbild-Erstellung, Anonymisierung/Verpixelung, Kennzeichnen, etc. (M56 – Software – Bearbeitung der Dateien).

- **Löschen von Aufnahmen:** Videos müssen gelöscht werden können, etwa wenn keine rechtliche Relevanz besteht oder wenn eine gesetzliche Aufbewahrungsfrist abgelaufen ist.

Verschiedene Rollen haben unterschiedliche Lösch-Befugnisse: Ein Standard-Nutzer kann seine eigenen Videos nicht löschen (dies verhindert, dass etwaig problematische Videos gelöscht werden). Ein Fachadministrator kann Videos auf Anfrage eines Berechtigten löschen, aber alle Löschungen werden protokolliert. Eine Speicher- und Löschfristen-Managementfunktion muss vorhanden sein. Dazu zählt die Möglichkeit eine automatisierte Löschfrist für alle Dateien als Grundeinstellung einzustellen sowie diese rollenbasiert manuell auszusetzen und händisch die erforderlichen, sodann individuellen Fristen zu hinterlegen sowie ein Modus zur Fristenkontrolle (M57 – Software – Löschen von Dateien nach Rollenkonzept).

- **Rollenabhängiges Teilen:** Ein Beamter kann beschließen, ein Video mit einem Kollegen, mit einem Vorgesetzten, oder mit einer externen Behörde zu teilen, sofern ein dienstliches Erfordernis hierzu besteht. Die Software muss dies ermöglichen, aber auch Zugriffskontrolle bieten, etwa nur Personen mit bestimmten Berechtigungen können auf das Video zugreifen (M58 – Software – Teilen von Dateien nach Rollenkonzept).

- **Protokollierung:** Jeder Zugriff auf eine Datei und jede vorgenommene Änderung, einschließlich einer letztlichen Löschung, sind in einer Protokolldatei zu hinterlegen. Dies muss auch nach Löschung der Aufnahmen für einen definierbaren Zeitraum für die Bundespolizei abrufbar sein. Bei jeder Änderung muss die Originaldatei stets unverändert erhalten bleiben. Für Änderungen ist sodann eine systemseitige automatisch erstellte Kopie bereitzustellen (M59 – Software - Protokollierung).

- **Export auf USB/CD:** Die Software muss die Möglichkeit bieten, Videodateien in einem standardisierten, abspielkompatiblen Format (z. B. MP4) auf externe Datenträger (USB-Laufwerke, CDs/DVDs) auszuleiten. Dies ist erforderlich für die Übermittlung an externe Behörden (z. B. Staatsanwaltschaft, Gerichte) sowie zur Archivierung. (M60 – Software – Export auf USB/CD).

4.3.2 Erweiterte Such- und Filterfunktionen

Die Software muss folgende Such- und Filterfunktionen zwingend bieten:

- **Filterung nach Datum und Uhrzeit:** Nutzer können Videos abrufen, die in einem definierten Zeitraum aufgenommen wurden (M61 – Software – Filterung nach Datum und Uhrzeit).
- **Filterung nach Bodycam-Nummer:** Abruf aller Videos einer bestimmten Bodycam (M62 – Software – Filterung nach Bodycam-Nummer).
- **Filterung nach Nutzer-ID:** Abruf aller Videos eines bestimmten Beamten (rollenabhängig autorisiert) (M63 – Software – Filterung nach Nutzer-ID).
- **Filterung nach TR/IA-Kennzeichnung** (siehe Kapitel 4.4.1 - Die neun Rollenprofile): Abruf von Videos mit spezifischen Markierungen für Überprüfungs- und Ermittlungszwecke (M64 – Software – Filterung nach TR/IA).

Folgende Funktionen sind optional und werden bei Vorhandensein mit Punkten bewertet:

- Kombinierte Mehrfachfilter (z.B. Datum UND Nutzer UND Kennzeichnung gleichzeitig): 10 Punkte (B29 – Software – Filterung (Mehrfachfilter))
- Volltextsuche in Kommentaren und Metadaten: 10 Punkte (B30 – Software – Filterung (Volltextsuche/Metadaten))

4.3.3 Videobearbeitung und Verarbeitung

Die Software muss grundlegende Videobearbeitungsfunktionen bieten:

- **Schnitt:** Trimmen von Anfang und Ende eines Videos (M65 – Software – Videobearbeitung (Schnitt)).
- **Kommentarfelder:** Hinzufügen von Text-Komentaren zu Videos (M66 – Software – Videobearbeitung (Kommentare einfügen)).
- **Bezeichnung der Datei:** Bspw. Hinterlegung des Aktenzeichens zum Vorgang aus dem polizeilichen Vorgangsbearbeitungssystem oder Einsatznummer (M67 – Software – Videobearbeitung (Bezeichnung der Datei ändern)).

Folgende Funktionen sind optional und werden bei Vorhandensein mit Punkten bewertet:

- **Bildverbesserung:** Anpassung von Helligkeit, Kontrast, Farbsättigung zur Optimierung der Erkennbarkeit: 15 Punkte (B31 – Software – Videobearbeitung (Bildverbesserung))
- **Erweiterte Videobearbeitung** (Unschärfe-Effekte für Datenschutz, Zeitlupen-/Zeitraffer-Funktion): 10 Punkte (B32 – Software – Videobearbeitung (erweiterte Videoverarbeitung))
- **Erzeugen eines Standbildes** 15 Punkte (B33 – Software – Videobearbeitung (Erzeugen von Standbildern))
- Möglichkeit **Kennzeichnungen/Markierungen** vorzunehmen (bspw. farblich unterschiedliche Einkreisung) 15 Punkte (B34 – Software – Videobearbeitung (Kennzeichnung/Markierung -

Einzelbild)) sowie bewegte Markierungen 10 Punkte (B35 – Software – Videobearbeitung (bewegte Markierungen))

Revisionssichere Protokollierung sämtlicher Änderungen und Zugriffe für jede Datei. Die Originaldatei muss dabei stets unverändert erhalten bleiben.

4.3.4 Verwaltungsfunktionen

Die Software muss zwingend folgende Verwaltungsfunktionen bieten:

- **Benutzer- und Geräteverwaltung:** Neue Benutzer hinzufügen, bestehende Benutzer löschen, Berechtigungen ändern, neue Geräte registrieren und Geräte deaktivieren (M68 – Software – Verwaltungsfunktionen (Benutzer- und Geräteverwaltung)).
- **Automatische Lösungsfristen und Fristenmanagement:** Die Software muss konfigurierbare Aufbewahrungsrichtlinien mit automatischer, revisionssicherer Löschung nach Fristablauf unterstützen (M69 – Software – Verwaltungsfunktionen (Automatische Lösungsfristen)). Dabei gilt:
 - Die Auftraggeberin/Bedarfsträgerin muss die Möglichkeit haben zentral eine Standardlöschfrist festzulegen. Diese Frist greift automatisch für alle Aufnahmen, sofern keine abweichende Regelung manuell gesetzt wurde.
 - Es muss die Möglichkeit bestehen, die automatische Lösungsfrist für eine einzelne Datei durch einen berechtigten Nutzer manuell auszusetzen und eine neue, individuelle Frist einzutragen (z. B. bei Aufnahmen, die einem Strafverfahren oder einer verlängerten Aufbewahrungspflicht zugeführt werden).
 - Ein Modus zur aktiven Fristenkontrolle muss vorhanden sein, der berechtigte Nutzer rechtzeitig vor Ablauf einer individuell gesetzten Frist informiert. Automatische Erinnerungen (z. B. per E-Mail oder Systembenachrichtigung) sind als Mindestanforderung zu implementieren.
 - Alle manuellen Eingriffe in Lösungsfristen (Aussetzung, Verlängerung, Neusetzung) sind revisionssicher zu protokollieren (wer hat wann welche Frist für welche Datei geändert).
- **Geräte-Zuordnung:** Zuordnung von Geräten zu Dienststellen, Teams oder Organisationseinheiten zur Abbildung der Struktur (M70 – Software – Verwaltungsfunktionen (Gerätezuordnung)).
- **Revisionssichere Protokollierung** aller administrativen Änderungen (Nutzeranlage, Berechtigungsänderungen, Geräteverwaltung) (M71 – Software – Verwaltungsfunktionen (Protokollierung)).
- **Hierarchische Organisationsstruktur:** Die Software muss Organisationsstrukturen mehrstufig abbilden können (z. B. Direktion → Dienststelle → Team), um eine strukturkonforme Gerätezuordnung und rollenbasierte Sichtbarkeit zu ermöglichen (M72 – Software – Verwaltungsfunktionen (hierarchische Organisationsstruktur)).

4.3.5 Spezielle Funktionen als Bewertungskriterien

Bieter können zusätzliche Funktionen anbieten, die mit Bewertungspunkten honoriert werden.

- **Passwortänderung durch Nutzer** (B36 - Software – Spezielle Funktionen (Passwortänderung durch Nutzer): 10 Punkte. Wenn Nutzer ihre eigenen Passwörter ändern können (selbst-Service), erhöht dies die Sicherheit und reduziert die Last auf die IT-Administratoren.
- **Import externer Medienquellen** (B37 - Software – Spezielle Funktionen (Import externer Medienquellen)): 10 Punkte. Wenn die Software Videos von anderen Quellen (etwa Überwachungskameras, externe Behörden) importieren kann, erhöht dies die operative Versatilität.
- **Geopositionsdaten-Kartendarstellung** (B38 - Software – Spezielle Funktionen (Geopositionsdaten – Kartendarstellung)): 10 Punkte. Wenn die Software Geopositions-Daten der Bodycams auf einer Kartenansicht visualisiert (Aufnahmeort je Datei), ist dies wertvoll für operative und forensische Analyse.
- **Geopositionsdaten-Extraktion ohne Visualisierung** (B39 - Software – Spezielle Funktionen (Geopositionsdaten-Extraktion ohne Visualisierung)): 5 Punkte. Wenn die Software Geopositions-Daten exportieren kann, jedoch keine Kartenvisualisierung bietet, werden 5 Punkte gegeben (Alternative zu B38, keine doppelte Punktevergabe).
- **Gesicherter Link-Versand** (B40 - Software – Spezielle Funktionen (Gesicherter Link-Versand)): Wenn die Software eine gesicherte elektronische Übermittlung von Videodateien an externe Stellen (z. B. Staatsanwaltschaft, Gerichte) per Link ermöglicht, werden 10 Punkte vergeben. Voraussetzung ist die vollständige Umsetzung folgender Sicherheitsmechanismen:
 - Zugriffs-Protokollierung (wer hat wann auf den Link zugegriffen)
 - Zeitlich begrenzte Gültigkeit des Links (konfigurierbare Ablaufzeit)
 - Möglichkeit zum jederzeitigen manuellen Zugriffsentzug (Link-Deaktivierung)
 - Automatische Löschung nach Ablauf der Gültigkeitsdauer
- **Single-Sign-On-Authentifizierung** (B41 - Software – Spezielle Funktionen (Single-Sign-On)): Wenn sich Nutzer mit ihren bestehenden Benutzerkonten anmelden können, über SAML 2.0 oder OIDC in Verbindung mit einem Behörden-IdP wird dies mit 5 Punkten bewertet. Dies erhöht die Benutzerfreundlichkeit.
- **Einfache Gerätezuordnung per RFID/Dongle** (B42 - Software – Spezielle Funktionen (Gerätezuordnung per RFID/Dongle)): Wenn die Software eine einfache und schnelle Registrierung einer Bodycam auf den jeweiligen Nutzer durch Auslesen einer RFID-Karte, eines Dongles oder eines vergleichbaren Identifikationsmediums unterstützt (softwareseitige Verknüpfung von Gerät und Beamten), werden 10 Punkte vergeben. Dies ergänzt die hardwareseitige RFID-Schnellregistrierung (s. Kapitel 3.1.9) um die software- und datenseitige Zuordnung im Schichtbetrieb.

4.4 Rollen- und Berechtigungskonzept

Die Cloud-Software muss ein differenziertes System haben, das verschiedenen Benutzer unterschiedliche Rechte gibt bzw. eine Zuweisung von Rollen und spezifischen Rechten ermöglicht. Dies basiert auf dem "Prinzip der geringsten Berechtigung", jeder Benutzer bekommt nur die Rechte, die er für die Wahrnehmung seiner dienstlichen Aufgaben benötigt, nicht mehr (M73 - Software – Rollenkonzept).

4.4.1 Die neun Rollenprofile

1. Nutzer (Standard): Dies ist die Standard-Rolle für einen Einsatzbeamten.

Ein Nutzer kann:

- Aufzeichnungen in den zentralen Datenspeicher überführen (Up-Load in die Cloud)
- Sein eigenes Videos betrachten
- Kommentare / Anmerkungen hinzufügen oder ändern
- Kopien von Aufzeichnungen (innerhalb der Software) erstellen und diese in der Dauer ändern (schneiden)
- Weitere Berechtigte der Dienststelle zum Zugriff auf die Aufzeichnungen berechtigen
- Von anderen Nutzern zum Zugriff auf deren Aufzeichnungsdaten berechtigt werden, sofern dienstliches Erfordernis besteht
- Eine Aufzeichnung als IA (Interne Angelegenheiten) oder TR (To review) einstufen
- Sein Passwort selbst ändern sofern angeboten, sonst Verwaltung durch Administrator (siehe Kapitel 4.3.1)

Ein Nutzer kann nicht:

- Videos von anderen Beamten ansehen
- Aufzeichnungen herunterladen
- Videos löschen
- administrativen Funktionen ausführen

2. Erweiterter Nutzer: Ein erweiterter Nutzer hat zusätzliche Rechte ggü. dem Nutzer. Er kann:

- sämtliche Videos seiner eigenen Dienststelle ansehen
- Aufzeichnungen Nutzern zuweisen (teilen)
- Aufzeichnungen anderen Dienststellen zuweisen (teilen)
- Eine Aufzeichnung mit Metadaten und Audit-Log herunterladen und anschauen
- Videos bearbeiten (Schnitt, Bildverbesserung, etc.)
- Die automatisch gesetzten Speicher-/Löschfristen aussetzen (manuell) und
- Geräte Nutzern zuweisen

Ein erweiterter Nutzer kann:

- Keine Benutzer-Verwaltung durchführen
- Keine System-/Verwaltungsfunktionen durchführen
- Keine Löschungen vornehmen
- Keine Speicher- und Löschfristen zurücknehmen

3. Fachadministrator: Ein Fachadministrator (ggf. ein IT-Spezialist) bei einer Dienststelle der Bundespolizei. Er kann, zusätzlich zu den Rechten des erweiterten Nutzers:

- Löschungen von Aufzeichnungsdaten (ausgenommen Audit-Log und Metadaten) vornehmen
- In der Software neue Nutzer in der Dienststelle hinzufügen und entfernen
- Rollen von Nutzern ändern und zu vorhanden Rollen zuweisen
- Benutzern die Rollenzuordnung bzw. Rechte entziehen und
- Benutzer löschen
- Geräte registrieren und deaktivieren
- System-/Verwaltungsfunktionen ausführen und
- Sonstige Funktionen ausführen, die mit Aufzeichnungsdaten verbunden sind

Ein Fachadministrator kann:

- Andere Fachadministratoren nicht verwalten
- Keine Audit-Log und Metadaten zu Aufzeichnungsdaten löschen

4. Internal Affairs (IA) – Berechtigte (gem. Ziffer 4.4.3): Internal Affairs ist eine Kennzeichnungsmöglichkeit für besonders sensible Aufnahmen. Ein IA-Berechtigter kann:

- Aufnahmen der eigenen Dienststelle ansehen
- Videos ansehen, die mit IA-Kennzeichnung gekennzeichnet sind
- den Status IA zurücksetzen / revidieren und
- das Löschen von Aufzeichnungen vornehmen

Er ist nicht berechtigt:

- Audit-Log und Metadaten zu Aufzeichnungsdateien zu löschen
- andere administrative System-/Verwaltungsfunktionen durchzuführen
- Systembezogene Protokolldateien zu

5. To Review (TR)-Berechtigter (gem. Ziffer 4.4.3): Ähnlich wie IA, aber für eine andere Zweck: Eine Überprüfung oder ein Review-Prozess. Ein TR-Berechtigter kann:

- Aufnahmen seiner Dienststelle ansehen
- Videos ansehen, die mit TR-Kennzeichnung gekennzeichnet sind

- den Status TR zurücksetzen/revidieren
- diese Videos löschen und bei Bedarf eine Verschiebung in den Bereich IA veranlassen

6. Geräteadministrator: Ein Geräteadministrator verwaltet die physischen Bodycams und Ladeinfrastruktur. Er kann:

- Neue Geräte registrieren (Seriennummern eingeben, Geräte zu Pools zuordnen)
- Defekte Geräte deaktivieren und Geräte aus dem Verwaltungsbereich entfernen
- Firmware-Updates durchführen
- Grundkonfigurationen von Geräten aktualisieren / vornehmen

Ein Geräteadministrator kann:

- keine Videos ansehen
- keine Nutzer verwalten
- keine Löschungen durchführen
- oder sonstige Funktionen ausführen, die mit Aufzeichnungsdaten verbunden sind

7. Systemadministrator: Ein Systemadministrator ist der oberste Administrator, typischerweise bei der Zentral-IT-Abteilung der Bundespolizei. Ein Systemadministrator verfügt über alle Rechte der Anwendung. Er kann zudem:

- System-Einstellungen ändern (Verschlüsselung, Speicherort, Backup-Strategien)
- Alle anderen Administratoren verwalten

8. Audit-Berechtigte: Ein Audit-Berechtigter ist typischerweise jemand, der für Compliance und interne Kontrollen verantwortlich ist. Er kann:

- über das Audit-Modul auf die auf dem Server gespeicherten Protokolldateien aller Nutzer und Dateien zugreifen
- Audit- Dateien (Audit-Log und Metadaten) herunterladen und
- die Audits ansehen und die Logs analysieren

Ein Audit-Berechtigter kann:

- keine Aufnahmen löschen
- keine Aufnahmen verarbeiten oder Änderungen vornehmen
- Berechtigten mit Audit-Rechten müssen situativ weitere Rollen zugewiesen werden können.

9. Link-Sharing-Berechtigte: Ein Link-Sharing-Berechtigter ist jemand, der Videos mit externen Personen teilen muss (etwa mit Gerichten oder anderen Behörden). Er hat die Rechte eines erweiter-ten Nutzers plus die Fähigkeit:

- Videos mit externen Benutzern (außerhalb der Bundespolizei) zu teilen
- Zeitlich begrenzte Zugriffs-Links zu erstellen

4.4.2 Beispielszenarien

Szenario 1: Ein Standard-Beamter möchte sein Video ansehen

Der Beamte loggt sich ein, navigiert zu "Meine Videos", sieht eine Liste seiner Videos sortiert nach Datum. Er wählt ein Video aus und schaut es an. Er kann keine Videos von anderen Beamten sehen.

Szenario 2: Ein Video wird an ein Gericht übermittelt

Das Video ist vor Gericht relevant. Ein Link-Sharing-Berechtigter erstellt einen Freigabe-Link mit 30 Tagen Gültigkeit. Der Link wird an das Gericht gesendet. Das Gericht öffnet den Link in einem Web-Browser und kann das Video ansehen, ohne auf das gesamte Cloud-System zugreifen zu können. Der Zugriff wird protokolliert.

4.4.3 Sonderfunktionen zur Zugriffsberechtigung

Zusätzlich zu den sonstigen Nutzungs- und Verarbeitungstätigkeiten müssen nachfolgende Funktionen zur Verfügung gestellt werden, um besonderen Fallkonstellationen Rechnung zu tragen:

Innere Angelegenheiten (IA) – Beschränkung (M74 - Software – Sonderfunktionen (Innere Angelegenheiten)):

- Erforderlich ist eine Kennzeichnungsmöglichkeit von besonders sensiblen Aufnahmen, die rechtmäßig erhoben und gespeichert wurden, deren Zugriff jedoch nur besonders Berechtigten möglich sein darf.
- Eine solche Aufzeichnung ist daher unverzüglich dem Zugriff normaler Nutzer (einschließlich des ursprünglichen Nutzers) zu entziehen und ausschließlich einem besonders berechtigten Personenkreis zugänglich zu machen.
- Die gesetzlich definierte Standardlöschfrist wird ausgesetzt, eine automatische Löschung somit unterbunden.

To Review (TR) – in Prüfung (M75 - Software – Sonderfunktionen (To Review)):

- Gefordert wird eine Kennzeichnungsmöglichkeit von Aufnahmen, die versehentlich aufgenommen wurden, für deren Speicherung aber keine Rechtsgrundlage vorliegt und daher eine unverzügliche Löschung zu erfolgen hat.
- Diese Aufzeichnungen sind unverzüglich dem Zugriff normaler Nutzer und darüber hinaus (der ursprüngliche Nutzer behält Zugriff) ausschließlich einem besonders berechtigten Personenkreis zugänglich zu machen.
- Die gesetzlich definierte Löschrfrist wird sodann ausgesetzt, die automatisierte Löschung ist zu unterbinden, um händisch eine unverzügliche Löschung zu ermöglichen

Für die Prüfung von IA/TR markierten Aufzeichnungen/Dateien sind eine eigene Rolle für besonders berechtigte Nutzer vorzusehen. (siehe auch Kapitel 4.4 - Rollen- und Berechtigungskonzept).

4.5 Cloud-Infrastruktur und Speicherung

4.5.1 Speicherplatz und Skalierbarkeit

Die Auftragnehmerin muss eine Cloud-Infrastruktur bieten, deren Speicherkapazität dynamisch und bedarfsgerecht skalierbar ist (M76 - Cloud – Speicherkapazität skalierbar). **Berechnung des Speicherbedarfs:**

Bei einer Aufnahmequalität von 1080p @ 25 FPS mit H.264-Kompression liegt die Dateigröße bei etwa 400-500 MB pro Stunde. Mit 10 TB können daher etwa 20.000-25.000 Stunden Video gespeichert werden.

Mindestanforderungen an den Speicher:

Die Basis-Speicherkapazität muss mindestens 10 TB betragen (Mindeststandard bei Vertragsabschluss). Die Infrastruktur muss dynamisch skalierbar sein, d. h. die Auftragnehmerin muss die Kapazität auf Anforderung der Bundespolizei kurzfristig (innerhalb von 5 Werktagen) erweitern können bspw. auf 20, 50, 100 TB oder mehr. Dies hat ohne Unterbrechung des laufenden Betriebs zu erfolgen. Über- und Unterschreitungen des Speicherbedarfs sind durch ein automatisches Monitoring zu erkennen. Die Bundespolizei ist frühzeitig vor Erreichen von Kapazitätsgrenzen zu warnen (s. auch Kapitel 4.5.5 - Warnmeldungen und Speicherverwaltung).

Abrechnung:

Die Speicherkapazität wird als skalierbare Leistung im Preisblatt ausgewiesen (z. B. Preis je TB/Monat). Die Bundespolizei soll nur die tatsächlich genutzte Kapazität vergüten.

Um eine ausgewogene und wirtschaftliche Preisgestaltung sicherzustellen, wird der Angebotspreis für die zusätzliche Speicherbereitstellung (Zusätzliche TB gemäß Preisblatt Pos. 3.4) an den Preis des Basisspeichers (10 TB gemäß Preisblatt Pos. 3.3) gekoppelt. Der vom Bieter angebotene Preis pro Jahr für ein (1) zusätzliches Terabyte (Pos. 3.4) darf maximal 10 % des angebotenen Jahrespreises für das gesamte 10-TB-Basis-speicherpaket (Pos. 3.3) betragen.

Ausschlusskriterium:

Angebote, bei denen der Preis für Position 3.4 die Grenze von 10 % des Jahrespreises der Position 3.3 überschreitet, werden wegen spekulativer Preisgestaltung und unzulässiger Mischkalkulation gemäß § 57 Abs. 1 VgV zwingend vom Verfahren ausgeschlossen.“

4.5.2 Datensicherung und Redundanz

Die Auftragnehmerin muss automatische, regelmäßige Datensicherungen durchführen. Eine Mindestanforderung ist eine tägliche Sicherung mit einer Aufbewahrung von mindestens 4 Wochen. Dies bedeutet, dass wenn ein Video versehentlich gelöscht wird, es aus einer Sicherung wiederhergestellt werden kann, solange das Löschen weniger als 4 Wochen her ist. Hierzu ist ein Antrag/eine

Freigabe der Bundespolizei erforderlich. Eine Protokollierung ist sicherzustellen (M77 – Cloud – Datensicherung (min. einmal täglich)).

Die Infrastruktur muss redundant ausgelegt sein. Dies bedeutet, dass Daten auf mehreren verschiedenen physischen Speichergeräten oder sogar in mehreren verschiedenen Rechenzentren gespeichert sind. Sollte ein Speichergerät ausfallen, sind die Daten noch auf einem anderen Gerät vorhanden (M78 – Cloud – redundante Infrastruktur).

4.5.3 Verschlüsselung nach BSI-Standards

Wie in Kapitel 4.1.2 beschrieben, müssen Daten mit AES-256 verschlüsselt sein. Die Auftragnehmerin muss die Verschlüsselungsschlüssel sicher verwalten. Eine Option ist, dass die Auftraggeberin/Bedarfsträgerin die Schlüssel verwaltet. Eine bessere Option ist ein "Treuhand-Modell" (Escrow), bei dem die Schlüssel bei einem unabhängigen Treuhänder hinterlegt sind, so kann die Bundespolizei im Krisenfall oder bei Insolvenz der Auftragnehmerin noch auf ihre Daten zugreifen.

4.5.4 Protokollierung nach BDSG

Das Bundesdatenschutzgesetz (BDSG) verlangt, dass alle Zugriffe auf sensible Daten protokolliert werden. Die Auftragnehmerin muss daher ein Audit-Log-System implementieren, das protokolliert:

- Wer hat auf ein Video zugegriffen (Benutzer-ID)
- Wann haben sie zugegriffen (Zeitstempel)
- Was haben sie getan (angesehen, heruntergeladen, gelöscht, etc.)
- Von welcher IP-Adresse erfolgte der Zugriff

Diese Logs müssen revisionssicher sein, das heißt, sie können nicht manipuliert oder gelöscht werden. Dies wird typischerweise durch Digitale Signaturen oder durch Speicherung in einem Write-Once-Medium erreicht (M79 – Cloud – Protokollierung nach BDSG).

4.5.5 Warnmeldungen und Speicherverwaltung

Folgende Mindestanforderung gibt es bzgl. Warnmeldungen:

- Das System muss automatische Warnmeldungen an Administratoren ausgeben, wenn der Speicher 80 % Auslastung erreicht (M80 – Cloud – Warnmeldung bei Speicherauslastung).

Folgende Funktionen sind optional und werden bei Vorhandensein mit Punkten bewertet:

- Frühwarnsystem mit mehrstufigen Warnungen (bei 75 %, 85 %, 95 % Auslastung) (B43 – Cloud – Warnmeldung bei Speicherauslastung (mehrstufige Warnungen): **10 Punkte**

Automatische Speicher-Berichte mit Prognosen zur erwarteten Vollausslastung (B44 – Cloud – Warnmeldungen bei Speicherauslastung (automatische Speicher-Berichte)): **5 Punkte**

4.5.6 Datenlöschung nach Vertragsende

Wenn die Rahmenvereinbarung endet, muss die Bundespolizei sicherstellen, dass ihre Daten sicher gelöscht sind und/oder eine Übertragung in ein seitens der Bundespolizei festgelegtes anderes Zielsystem übertragen werden (M81 – Cloud – Datenlöschung nach Vertragsende).

Die Auftragnehmerin muss daher:

- Eine Aufbewahrungsphase von 1 Jahr nach Vertragsende anbieten, während der die Bundespolizei noch auf ihre Daten zugreifen kann.
- Nach dieser 1-Jahres-Frist werden alle Daten vollständig gelöscht, nicht nur logisch (Dateien werden aus dem Dateisystem entfernt), sondern auch physisch (Speichermedia werden mehrfach überschrieben oder zerstört). Vorab der Löschung ist die Auftraggeberin/Bedarfstägerin zur anstehenden Löschung zeitgerecht zu informieren. Sie hat die Löschung freizugeben.
- Die Löschung wird protokolliert und der Bundespolizei wird ein Nachweis ausgestellt, der bescheinigt, dass die Löschung durchgeführt wurde.

4.6 Interoperabilität und Vendor-Lock-In-Vermeidung

4.6.1 REST-API

Die Auftragnehmerin muss eine REST-konforme (Representational State Transfer) API bieten (M82 – SaaS – REST-API). REST ist ein Standard-Architektur-Stil für Web-APIs. Eine REST-API ermöglicht es, über HTTP-Anfragen auf die Cloud-Software zuzugreifen.

Die API muss folgende Funktionen unterstützen:

- **Metadaten-Abruf:** Die Bundespolizei kann eine HTTP-GET-Anfrage stellen und erhält eine Liste aller Videos mit ihren Metadaten (Aufnahmedatum, Aufnahmeort falls GPS verfügbar, aufnehmender Beamter (Kennung, kein Klarname), Länge des Videos, Speicherfrist, Löschung, etc.).
- **Sichere Videodaten-Abrufe:** Videos können über die API heruntergeladen werden, mit voller Berechtigungsprüfung (nur Personen mit entsprechenden Rollen können Videos abrufen).
- **Nutzer- und Geräteverwaltung:** Neue Nutzer können über die API hinzugefügt werden, bestehende gelöscht, Rollen geändert, etc.
- **Audit-Log-Export:** Die Audit-Logs (siehe oben) können über die API exportiert werden, für tiefere Analysen seitens der Bundespolizei.
- Die API muss vollständig dokumentiert sein, mit Beispielen für jeden Endpunkt (jeden verfügbaren Dienst).

4.6.2 Datenexport in standardisierten Formaten

Die Auftragnehmerin muss den Export aller Daten in nicht-proprietären, standardisierten Formaten ermöglichen:

- **Videos:** MP4 oder andere Standard-Video-Formate (H.264 oder H.265 Codec, AAC-Audio).
- **Metadaten:** JSON oder XML-Format, Standard-Web-Formate.
- **Benutzer- und Berechtigungsdaten:** JSON oder XML, zusammen mit einer klaren Dokumentation der Datenstruktur.

Dies stellt sicher, dass wenn die Bundespolizei die Cloud-Software wechseln möchte, sie alle ihre Daten mitnehmen kann und nicht bei einem Anbieter gefangen ist (siehe auch Mindestkriterium M47 – SaaS – Datenexport in Kapitel 4.1.1).

4.6.3 Container-Technologie und Cloud-Portabilität

Folgende Funktionen sind optional und werden bei Vorhandensein mit Punkten bewertet:

- Unterstützung von Container-Technologien (Docker, Kubernetes) für Multi-Cloud- oder Hybrid-Cloud-Betrieb (B45 – Cloud – Unterstützung von Containertechnologien): **15 Punkte**
- Vollständige Infrastruktura-as-Code-Dokumentation für vereinfachte Migration (B46 – Cloud – Infrastruktura-as-Code-Dokumentation): **10 Punkte**

5. Service und Support

Dieses Kapitel regelt die Anforderungen an den laufenden Betrieb der Gesamtlösung nach der initialen Lieferung. Eine zuverlässige Bodycam-Infrastruktur ist nur dann einsatztauglich, wenn sowohl die Hardware als auch der SaaS-Dienst jederzeit verfügbar, aktuell und sicher sind. Dazu verpflichtet sich die Auftragnehmerin zu verbindlichen Service-Level-Agreements (SLAs) für Reaktions- und Wiederherstellungszeiten (5.1) sowie zu einem regelmäßigen und sicherheitskritischen Update-Management für die Cloud-Software (5.2). Alle in diesem Kapitel festgelegten Reaktionszeiten und Verfügbarkeitsgarantien sind Mindestanforderungen und Bestandteil der vertraglichen Leistungspflicht.

5.1 Service-Level-Agreements (SLAs)

Die Auftragnehmerin verpflichtet sich, verbindliche Service-Level-Agreements für den SaaS-Dienst einzuhalten. Diese regeln die Erreichbarkeit des Notfall-Supports sowie die Reaktions- und Wiederherstellungszeiten bei Störungen und Sicherheitsvorfällen. Die SLAs für den Hardware-Support (Bodycams, Akkus, Dockingstationen) sind gesondert in Kapitel 3.6.3 geregelt (M83 - Service und Support – Einhaltung der SLA).

Für sicherheitsrelevante und betriebskritische SaaS-Vorfälle, insbesondere Angriffe auf die Cloud-Infrastruktur, unberechtigte Datenzugriffe oder Datenabflüsse, Ausfälle des Upload-Prozesses

oder der Zugriffsmöglichkeit auf Aufnahmen sowie großflächige Störungen einer Vielzahl von Geräten durch SaaS-Probleme, muss die Auftragnehmerin einen 24/7-Notfall-Support an 365 Tagen im Jahr bereitstellen. Der Notfall-Support ist mindestens über eine dedizierte Notfallrufnummer sowie ein hochverfügbares Ticketsystem erreichbar.

Die Priorisierung und die Reaktions- sowie Wiederherstellungszeiten für SaaS-bezogene Störungen und Sicherheitsvorfälle werden wie folgt verbindlich festgelegt:

Priorität	Beschreibung	Reaktionszeit	Wiederherstellungszeit
Kritisch (P1)	Cloud-Software komplett ausgefallen, kein Upload möglich, Zugriff auf Aufnahmen wesentlich gestört oder Verdacht auf unberechtigten Zugriff/Datenabfluss.	max. 1–2 Stunden, 24/7	max. 4 Stunden
Hoch (P2)	Wesentliche Funktionen (z. B. Videobearbeitung, Export, Suche) gestört (10–50 Nutzer betroffen).	max. 4 Stunden	max. 12 Stunden
Mittel (P3)	Einzelne Funktionen eingeschränkt, operative Arbeit teilweise betroffen (1–10 Nutzer).	max. 8 Stunden	max. 24 Stunden
Niedrig (P4)	Kosmetische Fehler ohne wesentliche Beeinträchtigung.	max. 24 Stunden	max. 72 Stunden

Die Auftragnehmerin garantiert eine Verfügbarkeit des SaaS-Dienstes von mindestens 99,5% im Jahresmittel, gemessen auf Monatsbasis, exklusive angekündigter Wartungsfenster. Geplante Wartungsarbeiten sind der Bundespolizei mindestens zwei Wochen im Voraus anzukündigen und abzustimmen.

5.2 Cloud-Software-Update und Sicherheitsupdates

Die Auftragnehmerin ist verantwortlich dafür, dass die Cloud-Software regelmäßig aktualisiert wird.

Software-Updates: Die Auftragnehmerin installiert regelmäßig Feature-Updates und nimmt Verbesserungen vor. Die Installierung sollte immer in Absprache mit der Bundespolizei erfolgen. Die Auftragnehmerin muss die Bundespolizei zudem zwei Wochen im Voraus informieren, wenn ein Update ansteht, sodass die Bundespolizei ggf. erforderliche Vorkehrungen (technisch wie organisatorisch) treffen kann (M84 – Service und Support – Software-Updates).

Sicherheits-Patches: Falls eine Sicherheitslücke in der Software oder in Drittkomponenten (etwa dem Web-Server) besteht, muss die Auftragnehmerin unverzüglich mit Verfügbarkeit eines Patches diesen installieren (M85 – Service und Support – Sicherheits-Patches). Darüber hinaus ist die Auftraggeberin/Bedarfsträgerin über Art und Ausmaß der Sicherheitslücke und über die getroffenen Maßnahmen sowie prognostische Dauer der Behebung fortlaufend zu informieren.

Bug-Fix-Zyklen: Die Auftragnehmerin führt regelmäßige Bug-Fix-Releases durch, etwa monatlich. Falls ein kritischer Bug entdeckt wird (etwa eine Sicherheitslücke oder etwas, das die Funktionalität verhindert), kann auch ein sofortiges Ad-Hoc-Release erfolgen (M86 – Service und Support – Bug-Fix-Zyklen).

6. Schulung und Dokumentation

Dieses Kapitel regelt die Anforderungen an die Einführung der Gesamtlösung in den operativen Betrieb der Bundespolizei. Technisch hochwertige Systeme entfalten ihren vollen Nutzen nur dann, wenn das eingesetzte Personal die Geräte und die Software sicher und routiniert bedienen kann. Gleichzeitig ist eine vollständige und belastbare Dokumentation Voraussetzung für den langfristigen, wartbaren und rechtssicheren Betrieb der Lösung.

6.1 Schulungsanforderungen

Eine kritische Komponente des Erfolgs dieser Beschaffung ist, dass die Beamten, die die Bodycams nutzen, und die Administratoren, die die Cloud-Software verwalten, entsprechend geschult werden. Die Auftragnehmerin ist verantwortlich dafür, umfassende Schulungen bereitzustellen.

6.1.1 Multiplikator-Schulungen

Das Schulungskonzept basiert auf einem Multiplikator-Modell. Die Auftragnehmerin schult nicht alle tausenden Beamten, sondern schult etwa 50-100 "Multiplikatoren". Erfahrene Beamte und Trainer, die dann diese Schulungen an ihre Kollegen in ihren Dienststellen weitergeben.

Die Schulungen der Auftragnehmerin sind in Präsenzform, nicht online (M87 – Schulungen in Präsenzform). Die Auftragnehmerin muss vor Ort bei der Bundespolizei anwesend sein, in Klassenzimmern oder Schulungsräumen, und das Publikum direkt trainieren. Die Sprache der Schulungen ist deutsch. Die Gruppengröße pro Schulung sollte 10-15 Teilnehmern nicht übersteigen. Dies ermöglicht interaktive Frage- und Antwortsitzungen und persönliche Unterstützung.

Die Schulungen der Multiplikatoren sollten die unterschiedlichen Rollenverteilungen berücksichtigen. Eine Ausrichtung von Schulungen für Multiplikatoren gezielt für spezifische Rollen sollte ermöglicht werden können. Das bedeutet:

- **Für Nutzer und Erweiterte Nutzer sowie IA/TR-Berechtigte (Beamte die Bodycam verwenden oder ihr Führungspersonal):** Fokus auf Bedienung der Bodycam, Funktionen wie

Start/Stop, Einstellungen, Laden des Akkus, Zugang zu/Funktionen der Videobearbeitungssoftware.

- **IA/TR-Berechtigte:** Basis Informationen der Nutzer/erweiterten Nutzer inkl. Einweisung, plus IA/TR-Verfahren und Speicher-/Lösch-/Beteiligungsfunktionalitäten
- **Für Fachadministratoren und Geräteadministratoren der Dienststellen:** Fokus auf Nutzerverwaltung, Berechtigungen, Reparaturabwicklung, Sicherung, API-Zugriff, plus lokales Troubleshooting.
- **Für Datacenter-Administratoren (sog. Systemadministratoren) (zentrale IT):** Fokus auf Cloud-Betrieb, Updates, Infrastruktur-Skalierung, Backup und Recovery, Sicherheit.

6.1.2 Timing und Koordination

Die Schulungen sollten unmittelbar nach Lieferung der Hardware durchgeführt werden, damit die Multiplikatoren die Schulungen möglichst schnell an ihre Kollegen weitergeben können. Schulungstermine haben in Abstimmung mit der Bundespolizei, entsprechend der Verfügbarkeit der Schulungsadressaten, zu erfolgen (M88 – Schulungen unmittelbar nach Lieferung).

6.1.3 Schulungsmaterial

Die Auftragnehmerin muss Schulungsunterlagen in deutscher Sprache zur Verfügung stellen und in editierbarem Format (etwa Microsoft PowerPoint oder Word). Dies ermöglicht es der Bundespolizei, diese Unterlagen an ihre lokalen Bedürfnisse anzupassen und in ihren eigenen Schulungen weiterzugeben. Zusätzliche e-Learning-Formate werden positiv gewertet (M89 – Schulungsunterlagen in deutscher Sprache).

6.1.4 Reisekosten

Alle Kosten für die Anfahrt des Schulungsteams (Flüge, Bahn, Auto) und Übernachtungen in Hotels müssen im Angebotspreis der Auftragnehmerin enthalten sein. Die Bundespolizei trägt keine zusätzlichen Reisekosten.

6.2 Dokumentation und Bedienungsanleitungen

6.2.1 Bodycam-Bedienungsanleitung

Die Auftragnehmerin muss eine Bedienungsanleitung für die Bodycam bereitstellen. Dies kann in Papierform (gedruckt) sein und muss zusätzlich als PDF bereitgestellt werden. Die Anleitung muss in deutscher Sprache verfasst sein und sollte mindestens Folgendes enthalten (M90 – Bedienungsanleitung in deutscher Sprache (Bodycam)):

- Überblick über die Bodycam (Bezeichnung der Tasten und Anschlüsse).
- Akku-Verwaltung (Laden sowie Einsetzen und Wechseln (soweit nicht festverbaut)).
- Ein- und Ausschalten.

- Aufnahme starten und stoppen.
- Grundlegende Einstellungen (Auflösung, Bildrate, Audio).
- Anschluss an WiFi und Docking.
- Troubleshooting für häufige Probleme.

6.2.2 Cloud-Software-Bedienungsanleitung

Die Auftragnehmerin muss eine Bedienungsanleitung für die Cloud-Software, ebenfalls in deutscher Sprache, mit Screenshots der Benutzeroberfläche bereitstellen. Sie sollte die folgenden Themen abdecken (M91 – Bedienungsanleitung in deutscher Sprache (Cloud-Software)):

- Anmeldung und Authentifizierung.
- Navigation und Benutzeroberfläche.
- Videos suchen, ansehen, bearbeiten.
- Fristenkontrolle: automatisierte und manuelle Einstellung von Lösch-/Speicherfristen
- Nutzer- und Geräteverwaltung (für Administratoren).
- Rollen und Berechtigungen: Management sowie rollenbasierte Funktionalitäten.
- API-Zugriff und Datenexport.

6.2.3 Technische Dokumentation

Die Auftragnehmerin muss eine Technische Dokumentation für IT-Administratoren und Entwickler in deutscher Sprache bereitstellen. Sie sollte folgende Themen abdecken (M92 – Technische Dokumentation für IT-Administratoren/Entwickler):

- Systemarchitektur.
- REST-API-Dokumentation mit Beispielen.
- Sicherheit und Verschlüsselung.
- Backup- und Recovery-Prozeduren.
- Audit-Logs und deren Format.

Hinweis: Hochspezifische technische Dokumente, wie API-Referenzen, IT-Sicherheitszertifikate (z. B. BSI-C5-Testate) oder rein entwicklerspezifische Verfahrensbeschreibungen, dürfen in englischer Sprache eingereicht werden.

7. Teststellung und funktionaler Labortest

Dieses Kapitel beschreibt das Verfahren zur praktischen Erprobung der angebotenen Bodycam-Gesamtsysteme vor Zuschlagserteilung. Die Teststellung dient dazu, ausgewählte Bewertungskriterien (B) sowie diejenigen Mindestanforderungen (M), die in Kapitel 8.1 mit dem Zusatz „**Praxistest**“ gekennzeichnet sind, unter einheitlichen Bedingungen zu überprüfen.

Bieter sollen zudem eindeutig erkennen können, welche Kriterien in welcher Form getestet werden und unter welchen Bedingungen hieraus Punkte in der Wertung resultieren.

Die Teststellung ist integraler Bestandteil der qualitativen Bewertung und erfolgt im Rahmen einer zweistufigen Bewertungslogik:

- Schriftliche Erstbewertung aller wertungsfähigen Angebote anhand der mit dem Angebot eingereichten Unterlagen (Datenblätter, Zertifikate, Prüfberichte, Eigenerklärungen).
- Praktische Teststellung (funktionaler Labortest) für die nach der Erstbewertung zwei bestplatzierten Bieter.

Mindestanforderungen, die ausschließlich anhand von Unterlagen nachzuweisen sind, werden nicht im Rahmen der Teststellung geprüft. Mindestanforderungen mit der Kennzeichnung „Praxistest“ werden in der Teststellung ausschließlich auf Erfüllung (bestanden/nicht bestanden) verifiziert und führen bei Nichterfüllung zum Ausschluss des Angebots.

7.1 Gegenstand der Teststellung

Um sicherzustellen, dass die angebotenen Bodycam-Systeme inklusive der dazugehörigen Cloud-Software (SaaS-Dienst) den hohen einsatztaktischen, technischen und ergonomischen Anforderungen der Bundespolizei entsprechen, wird mit den für den Zuschlag in Frage kommenden Bietern eine Teststellung in Form eines funktionalen Labortests durchgeführt.

Gegenstand der Teststellung ist die praktische Verifikation der in den schriftlichen Angeboten zugesicherten Eigenschaften. Die Teststellung dient ausschließlich der Überprüfung der in dieser Leistungsbeschreibung definierten Mindestanforderungen (M-Kriterien) und Bewertungskriterien (B-Kriterien), für die als Prüfmethode der „Praxistest“ vorgesehen ist. Es werden keine neuen Kriterien eingeführt oder bewertet.

7.2 Organisatorische Rahmenbedingungen

7.2.1 Zeitpunkt und Dauer der Teststellung

Die Teststellung findet nach Ablauf der Angebotsfrist, der formalen Angebotsprüfung und der schriftlichen Erstbewertung aller wertungsfähigen Angebote statt. Zur Teststellung werden die nach der schriftlichen Erstbewertung zwei bestplatzierten Bieter eingeladen.

Die Einladung erfolgt elektronisch über das Vergabemanagementsystem mindestens 10 Werktage vor dem jeweiligen Testtermin und enthält insbesondere:

- Testdatum und Zeitfenster,
- Testort und Zugangsinformationen,
- die Anzahl und Konfiguration der bereitzustellenden Geräte, Akkus (soweit wechselbar), Dockingstationen und ggf. Digitalfunkgeräte/Router,
- den Hinweis auf die mitzubringenden Unterlagen (z. B. Zugangsdaten zur SaaS-Testinstanz).

Je Bieter wird ein Testzeitfenster von in der Regel bis zu 6 Stunden vorgesehen, in dem alle Testmodule gemäß Kapitel 7.3 in festgelegter Reihenfolge durchgeführt werden. Es wird sichergestellt, dass alle eingeladenen Bieter unter im Wesentlichen gleichen Bedingungen (Tageszeit, Lichtverhältnisse, Raumsetup) getestet werden.

7.2.2 Testort und Infrastruktur

Die Teststellung findet in von der Bundespolizei benannten Räumlichkeiten statt, die es ermöglichen, die vorgesehenen Szenarien standardisiert durchzuführen. Diese umfassen insbesondere:

- einen Testraum mit Tischen, Stühlen, Stromversorgung, Arbeitsplatzrechnern und gesichertem Netzwerkzugang (LAN/WLAN) zur vom Bieter bereitgestellten SaaS-Testumgebung,
- einen Bewegungsbereich (Flur, Übungsstrecke, ggf. Treppenhaus) für Lauf-, Fall- und Sichtfeld-Tests,
- ggf. Außen- oder Innenbereiche mit variabler Beleuchtung für Video-/Audio-Tests.

Messmittel wie Präzisionswaage, Schallpegelmesser, Maßband sowie ggf. Referenz-Digitalfunkgeräte werden durch die Bundespolizei bereitgestellt, soweit nicht anders in der Einladung beschrieben.

7.2.3 Bereitzustellende Geräte und Zubehör

Jeder Bieter muss zur Teststellung folgende Komponenten in funktionstüchtigem Zustand bereitstellen:

- **Mindestens 5 Bodycam-Einheiten** des angebotenen Modells, vollständig geladen und einsatzbereit. Die Geräte müssen fabrikneu oder neuwertig sein und dem Serienstand entsprechen, der im Falle einer Zuschlagserteilung geliefert werden würde.
- **Alle angebotenen Befestigungssysteme:** sämtlich erwerbbar Befestigungssysteme Adapter, MOLLE-Adapter, Adapter für Körperschutzausrüstung/Bekleidung sowie alle weiteren im Angebot spezifizierten Befestigungslösungen, jeweils in mindestens 3-facher Ausführung.
- **Mindestens 10 vollständig geladene Ersatzakkus (soweit wechselbar) sowie alle angebotenen Ladegeräte und Dockingstationen** in funktionsfähigem Zustand.
- ggf. mobile Router oder weitere Komponenten, sofern diese für angebotene B-Kriterien (z. B. LTE/5G, Live-Streaming) erforderlich sind
- **Zugang zur Cloud-Software (SaaS-Dienst):** Der Bieter muss eine voll funktionsfähige Testumgebung der Cloud-Software bereitstellen, die sämtliche im Angebot beschriebenen Funktionen abbildet. Die Testumgebung muss für die Dauer der Teststellung sowie für mindestens 7 weitere Tage nach Abschluss der Tests verfügbar sein. Es müssen mindestens 10 Nutzerkonten mit unterschiedlichen Berechtigungsstufen (Nutzer, Fachadministrator, Systemadministrator) eingerichtet sein.
- ggf. notwendige Integrationskomponenten zu BOS-Digitalfunkgeräten, RFID, Koppelungsmodule zwischen Bodycam und Zwangsmitteln.

- **Deutschsprachige Dokumentation:** Vollständige Bedienungsanleitung in deutscher Sprache (gedruckt oder digital), technische Spezifikationen, Schnellstartanleitungen und Administratorhandbücher.
- **Optional:** Soweit im Angebot spezifiziert, zusätzliche Komponenten wie externe Mikrofone, Bluetooth-Headsets, Mobilfunk-Module, GPS-Empfänger oder andere Erweiterungen.

Die Bieter sind verpflichtet, die Geräte und Komponenten spätestens am Vortag des Testtermins bis 16:00 Uhr am Testort anzuliefern oder persönlich abzugeben. Die Auftraggeberin/Bedarfsträgerin übernimmt keine Haftung für Beschädigungen, die während der Teststellung im Rahmen der vorgesehenen Tests entstehen. Die Bieter werden jedoch rechtzeitig über die geplanten Robustheitstests (Falltests, Wassertests) informiert.

Fehlen für ein Testmodul erforderliche Komponenten oder sind diese nicht funktionsfähig, wird das betreffende B-Kriterium mit 0 Punkten bewertet. Ein damit verknüpftes Mindestkriterium mit Zusatz „**Praxistest**“ gilt als nicht erfüllt und führt zum Ausschluss aus dem Vergabeverfahren.

7.2.4 Anwesenheit und Mitwirkung der Bieter

Jeder Bieter ist berechtigt, während der gesamten Dauer seiner Teststellung mit maximal 2 Vertretern vor Ort anwesend zu sein. Diese Vertreter dürfen:

- **Technische Unterstützung leisten:** Bei der Konfiguration der Geräte, der Einrichtung der Cloud-Software und der Lösung technischer Probleme assistieren.
- **Fragen beantworten:** Fragen der Testkommission zu Funktionen, Bedienung und technischen Details beantworten.
- **Beobachten:** Den Testverlauf beobachten und protokollieren.

Die Vertreter dürfen nicht:

- In die Bewertung eingreifen oder diese beeinflussen.
- Testdurchläufe wiederholen lassen, es sei denn, es liegt ein technischer Defekt oder ein nachweislicher Fehler in der Testdurchführung vor.
- Die Testumgebung verändern oder manipulieren.

Die Kommunikation während der Teststellung erfolgt ausschließlich über den Testleiter. Die Bietervertreter dürfen nicht direkt mit den Mitgliedern der Testkommission über die Bewertung diskutieren.

Die Bedienung der Bodycams und der Cloud-Software im Rahmen der Testmodule erfolgt grundsätzlich durch von der Bundespolizei benannte Testpersonen, um eine realitätsnahe und bieterunabhängige Bewertung zu gewährleisten.

7.2.5 Testkommission und Bewertungsgremium

Die Durchführung und Bewertung der Teststellung erfolgt durch eine unabhängige Testkommission, die aus **mindestens sechs** Personen besteht:

- **2 Testleiter:**
Mitarbeiter des Beschaffungsamtes des BMI mit Kenntnissen im Vergaberecht und in der Durchführung von Teststellungen. Verantwortlich für Ablaufkoordination, Einhaltung der Testprotokolle und Kommunikation mit den Bietern.
- **2 fachliche Vertreter der Bundespolizei**
Erfahrene Polizeibeamtin/erfahrener Polizeibeamter aus dem operativen Dienst. Bewertet insbesondere Praxistauglichkeit, Ergonomie und Bedienbarkeit.
- **2 IT-/Cloud-Expertin bzw. -Experte**
Mitarbeiter/in mit einschlägiger Erfahrung in IT-Betrieb, Cloud-Software und IT-Sicherheit. Bewertet insbesondere die praktische Umsetzung der Cloud-Software-Funktionen und Konnektivität.

Die Testkommission kann bei Bedarf durch weitere sachkundige Personen (z. B. zusätzlichen IT-Sicherheitsexperten, Protokollführung) ergänzt werden. Alle Mitglieder der Testkommission unterliegen der Neutralitätspflicht und dürfen keine persönlichen oder wirtschaftlichen Beziehungen zu den Bietern haben, eine etwaige Befangenheit ist unverzüglich anzuzeigen.

Die Bewertung erfolgt grundsätzlich im Konsens. Kommt kein Konsens zustande, entscheidet die Mehrheit der Mitglieder der Testkommission. Bei Stimmengleichheit entscheidet die Stimme der Testleiterin/des Testleiters.

7.2.6 Dokumentation und Protokollierung

Die gesamte Teststellung wird lückenlos dokumentiert. Für jeden Bieter wird ein separates Testprotokoll erstellt, das folgende Elemente umfasst:

- **Protokollkopf:** Datum, Uhrzeit (Beginn und Ende), Name des Bieters, anwesende Personen (Bietervertreter und Testkommission), getestete Geräte (Modellbezeichnung, Seriennummern).
- **Checkliste Vollständigkeit:** Bestätigung, dass alle erforderlichen Geräte und Komponenten bereitgestellt wurden.
- **Testablauf:** Chronologische Dokumentation aller durchgeführten Tests mit Zeitstempeln, Testparametern und Testergebnissen.
- **Bewertungsmatrix:** Ausgefüllte Bewertungsbögen für jedes Bewertungskriterium mit vergebenen Punkten und Begründungen.
- **Foto- und Videodokumentation:** Fotografische und videografische Aufzeichnungen relevanter Testvorgänge (z. B. Falltests, Bedienung, Display-Anzeigen, Videoqualität).

- **Bemerkungen und Besonderheiten:** Notizen zu besonderen Vorkommnissen, technischen Problemen, Nachfragen der Bieter oder Abweichungen vom geplanten Testablauf.
- **Unterschriften:** Unterschrift des Testleiters und mindestens zweier weiterer Kommissionsmitglieder zur Bestätigung der Richtigkeit und Vollständigkeit des Protokolls.

Die vollständigen Protokolle sind Bestandteil der Vergabeakte und werden für eventuelle Nachprüfungsverfahren aufbewahrt.

7.3 Testszenarien und Prüfkriterien

Die nachfolgenden Testmodule beschreiben den genauen Ablauf der praktischen Erprobung (Praxistest) im Rahmen der Teststellung. Jedes Modul dient der Verifizierung von Mindestkriterien, die laut Kapitel 8.1 zwingend einen Praxistest erfordern, sowie der Punktevergabe für die in Kapitel 8.2 definierten Bewertungskriterien (B1 bis B46). Die Bieter haben sicherzustellen, dass die bereitgestellten Mustergeräte und Softwareumgebungen die in den folgenden Modulen beschriebenen Anforderungen vollumfänglich demonstrieren können.

7.3.1 Testmodul 1: Hardware – Ergonomie & Robustheit

Zielsetzung: Dieses Modul prüft Gewicht, Tragbarkeit, Bedienbarkeit sowie mechanische Belastbarkeit der Bodycam unter Einsatzbedingungen.

Geprüfte Mindestkriterien und Bewertungskriterien:

- M1 – Gewicht der Bodycam (max. 255g)
- M2 – Kompatibilität zu MOLLE
- M4 – Robustheit (Falltest aus 1m)
- B1 – Gewicht der Bodycam (5 Punkte)
- B2 – Intuitive Menüführung ohne Schulung (15 Punkte)
- B3 – Bedienbarkeit mit dicken Handschuhen (5 Punkte)
- B4 – Robustheit (Falltest aus 1,5m) (10 Punkte)
- B5 – Frontdisplay (15 Punkte)

Maximal erreichbare Punkte in diesem Modul: **50 Punkte**

Testdurchführung:

Vorbereitung: Die Testkommission stellt eine geeichte digitale Waage, eine polizeiliche Einsatzweste mit MOLLE-System, standardisierte polizeiliche Einsatzhandschuhe sowie eine Falleinrichtung (1,5m Höhe, Betonboden) bereit.

Testaufbau: Das Bodycam-Mustergerät liegt im ausgeschalteten Zustand auf dem Prüftisch. Ein ungeschulter Tester der Behörde fungiert als Proband und zieht die Einsatzweste an.

Testdurchgang:

1. Das Gerät wird auf der Waage gewogen (betriebsbereit) (M1, B1).
2. Der Tester befestigt die Bodycam an den MOLLE-System der Weste und prüft den festen Sitz durch schnelles Gehen und abrupte Drehbewegungen (M2).
3. Der Tester navigiert ohne vorherige Einweisung durch das Menü und liest Status-Anzeigen (z.B. Akkustand, Zeit) ab (B2, B5).
4. Der Tester zieht die Einsatzhandschuhe an, ertastet die Tasten, schaltet das Gerät blind ein, startet eine Videoaufnahme und stoppt diese wieder (B3).
5. Der Tester schaltet, sofern vorhanden, das Frontdisplay ein und prüft, ob der Raum vor ihm in einer Live-View auf dem Display angezeigt wird.

Bewertung:

- 5 Punkte (B1): Das Gewicht der betriebsbereiten Bodycam liegt unterhalb des in der Leistungsbeschreibung definierten Optimalgewichts.
0 Punkte (B1): Das Gewicht liegt auf oder über dem definierten Optimalgewicht.
- 15 Punkte (B2): Der Tester kann die Menüführung und Basisfunktionen auf Anhieb fehlerfrei und ohne Handbuch bedienen.
0 Punkte (B2): Der Tester benötigt Hilfe, scheitert an der Menüführung oder muss das Handbuch konsultieren.
- 10 Punkte (B3): Die Tasten lassen sich mit dicken Einsatzhandschuhen zweifelsfrei ertasten und die Aufnahme lässt sich beim ersten Versuch fehlerfrei starten und stoppen.
0 Punkte (B3): Die Tasten sind mit Handschuhen nicht sicher bedienbar oder es kommt zu Fehleingaben.
- 10 Punkte (B4): Nach 3x Falltest aus 1,5 m keine Funktionsbeeinträchtigung (Aufnahme, Menü, Display).
0 Punkte (B4): Jegliche Funktionsstörung nach Falltest.
- 15 Punkte (B5): Frontdisplay zeigt Live-View erkennbar an.
0 Punkte (B5): Frontdisplay nicht vorhanden oder kein Live-View möglich.

Dokumentation: Fotoprotokoll der Wiegung mit sichtbarem Waagen-Display, Tragefotos der Kamera an der MOLLE-Weste, Falltestvideo, Fotoaufnahme des Frontdisplays.

7.3.2 Testmodul 2: Video & Audio

Zielsetzung: Dieses Modul überprüft die Video- und Audioqualität der Bodycam bei Wiedergabe vom Gerät und in der Software unter realistischen Einsatzbedingungen, inklusive Speicherleistung und Kamerafunktionen. **Geprüfte Mindestkriterien und Bewertungskriterien:**

- M10 – Speicherausstattung
- M17 – Videoqualität (720/1080p, 25FPS)
- M18 – Video-Codec (H.264)
- M19 – Bildstabilisierung
- M20 – Horizontales Sichtfeld der Kamera (min. 110 Grad)
- M21 – Zwei Mikrofone
- M22 – Klare Sprachaufzeichnung (bei 60-70 dB)
- M23 – Akustisches Startsignal (1m Entfernung)
- M24 – LED-Statusanzeige (Aufnahme)
- M25 – Statusanzeige (Akkuladezustand)
- M26 – Warnmeldung (Speicherplatzknappheit)
- B6 – Speicherausstattung (10 Punkte)
- B7 – Videoqualität (4k+) (5 Punkte)
- B8 – Video-Codec (H.265) (10 Punkte)
- B9 – Horizontales Sichtfeld der Kamera (120 Grad) (10 Punkte)
- B10 – Kamera horizontal schwenkbar (10 Punkte)
- B11 – Kamera vertikal schwenkbar (10 Punkte)
- B12 – aktive Geräuschfilterung (10 Punkte)
- B13 – Klare Sprachaufzeichnung (bei >85 dB) (10 Punkte)

Maximal erreichbare Punkte in diesem Modul: **75 Punkte**

Testdurchführung:

Vorbereitung: Die Testkommission stellt eine Testszene mit Lärmquelle (85 dB), Schwenkobjekten (horizontal/vertikal), kalibrierte Messgeräte (Field-of-View (FOV), Audio) sowie einen Bewegungsparcours bereit.

Testaufbau: Bodycam auf Weste befestigt. Testszene mit Markierungen für FOV-Messung, Lautsprecher für Sprachtest bei 85 dB, Parcours für Stabilisierung.

Testdurchgang:

1. Speicherkapazität prüfen (B6).
2. 4K-Aufnahme starten (B7),
3. Codec via Metadaten/File-Analyse bestätigen (H.265 vs. H.264, B8).
4. Horizontales FOV messen (Bereich zwischen 120 und 130 Grad, B9), horizontale Schwenk ($\geq 45^\circ$, Objekte erfassen, B10), vertikale Schwenk ($\geq 30^\circ$, B11).
5. Audio bei >85 dB: Standardtext sprechen/lauten Lärm simulieren, Playback prüfen (B12 und B13).
6. Stabilisierung: Aufnahme beim Gehen/Laufen auf Parcours, Verwacklung/Bildschärfe bewerten.

Bewertung:

- 10 Punkte (B6): Speicher ≥ 64 GB, fehlerfreie >1h 1080p-Aufnahme.
0 Punkte (B6): Kapazität <64 GB oder Schreibfehler.
- 5 Punkte (B7): 4K ≥ 30 FPS scharf/flüssig.
0 Punkte (B7): Kein 4K oder Qualitätsdefizite.
- 10 Punkte (B8): H.265-Codec (kleinere Datei/bessere Effizienz als H.264).
0 Punkte (B8): Nur H.264.
- 10 Punkte (B9): $\geq 120^\circ$ horizontales FOV gemessen.
0 Punkte (B9): $< 120^\circ$.
- 10 Punkte (B10): Horizontaler Schwenk $\geq 45^\circ$ ohne Qualitätsverlust.
0 Punkte (B10): Unzureichend/kein Schwenk.
- 10 Punkte (B11): Vertikaler Schwenk $\geq 30^\circ$ (Blick unten/oben).
0 Punkte (B11): Unzureichend/kein Schwenk.
- 10 Punkte (B12): Geräuschfilterung aktiv
0 Punkte (B12): keine Geräuschfilterung
- 10 Punkte (B13): Sprache bei >85 dB klar verständlich.
0 Punkte (B13): Verzerrt/unverständlich.

Dokumentation: Testvideos (4K, Schwenkbereich, Audio), Dateianalysen (Codec, Größe, Metadaten), FOV-Messprotokoll, Audio-Playback-Protokoll, Speichermessung, Stabilisierungs-Vergleichsfotos.

7.3.3 Testmodul 3: Konnektivität & Akku

Zielsetzung: Dieses Modul überprüft Schnittstellen, Netzwerkfunktionen, Statusanzeigen und Akkuleistung der Bodycam inklusive Ladeinfrastruktur.

Geprüfte Mindestkriterien und Bewertungskriterien:

- M27 – USB-C (Anschluss vorhanden)
- M28 – USB-C (Ladefunktion)
- M29 – USB-C (Dateiübertragung)
- M30 – USB-C (administrative Änderungen)
- M31 – WiFi-Konnektivität WiFi 802.11ac, 802.11b, 802.11g, und 802.11n)
- M32 – Automatischer Cloud-Upload
- M33 – Automatischer Cloud-Upload (Fortsetzung nach Unterbrechung)
- M34 – Statusanzeige bei automatischem Cloud-Upload
- M35 – Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten
- M36 – Akku wiederaufladbar
- M37 – Akkulaufzeit (Aufnahmezeit min. 10h)
- M38 – Ladestation/Dockingstation mit EU-Standardstecker (Typ F/C, 230V, 50Hz)
- M39 – Dockingstation (gleichzeitiges Laden und Datenübertragung), sofern Akku wechselbar
- M41 – Dockingstationen (Statusanzeige: Laden/Fertig/Upload)

- B14 – Statusanzeige (mit Wifi verbunden) (5 Punkte)
- B15 – Statusanzeige (mit LTE/5G verbunden) (5 Punkte)
- B16 – Statusanzeige (mit Bluetooth verbunden) (5 Punkte)
- B17 – Statusanzeige (Datum und Uhrzeit) (5 Punkte)
- B18 – Statusanzeige (Debug-Informationen) (5 Punkte)
- B19 – Mobile Netzwerkunterstützung (LTE/5G) (15 Punkte)
- B20 – Live-Streaming (Real-Time Situational Awareness) (20 Punkte)
- B21 – Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten (Trigger-Funktion) (15 Punkte)
- B22 – Bluetooth-Schnittstelle zu Geräten des Herstellers Sepura (STP- und SC-Serie) (15 Punkte)
- B23 – Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten (Sprachaufzeichnung) (15 Punkte)
- B24 – Akkuwechsel (10 Punkte)
- B25 – Akkulaufzeit (Aufnahmezeit > 12h) (10 Punkte)
- B26 – Ladestation/Dockingstation mit Schnellladefunktion (Akku innerhalb < 4h vollgeladen) (5 Punkte)
- B27 – Ladestation (Stand-Alone, Laden ohne Bodycam) (10 Punkte)
- B28 – Dockingstation (Multi-Port) (10 Punkte)

Maximal erreichbare Punkte in diesem Modul: **150 Punkte**

Testdurchführung:

Vorbereitung: Testkommission stellt WLAN, LTE/5G-SIM, Digitalfunkgerät (BOS-kompatibel), Dockingstationen, entladene Akkus, Netzwerk-Monitor bereit.

Testaufbau: Bodycam in Einsatzweste, Testnetzwerke (WiFi/LTE/5G), Funkgerät gekoppelt, Dockingstation an Strom.

Testdurchgang:

1. Statusanzeigen prüfen: WiFi/LTE/Bluetooth verbinden, Datum/Uhrzeit/Debug anzeigen (B14–B18).
2. LTE/5G: Verbindung aufbauen, Datenrate per Eigenerklärung gewährleisten (B19).
3. Live-Streaming: Echtzeit-Übertragung in Cloud prüfen (Latenz <5s, B20).
4. Bluetooth: Mit Funkgerät koppeln, Trigger (Aufnahme-Start), Sprachübertragung testen (B21-B23).
5. Akkutest: Akkuwechsel durchführen ohne Werkzeug, 1080p-Aufnahme >12h simulieren (Teiltests), Ladezeit in Dockingstation <4h messen (B24-B26).
6. USB/Dockingstation: Dateitransfer, paralleles Laden/Upload prüfen (B27/B28).

Bewertung:

- 5 Punkte (B14): Klare WiFi-Verbindungsanzeige (LED/Display).
0 Punkte (B14): Fehlende/unklare Anzeige.
- 5 Punkte (B15): LTE/5G-Status sichtbar.
0 Punkte (B15): Fehlende Anzeige.
- 5 Punkte (B16): Bluetooth-Verbindung angezeigt.
0 Punkte (B16): Fehlende Anzeige.
- 5 Punkte (B17): Datum/Uhrzeit permanent lesbar.
0 Punkte (B17): Nicht verfügbar.
- 5 Punkte (B18): Debug-Infos abrufbar.
0 Punkte (B18): Nicht verfügbar.
- 15 Punkte (B19): Stabile LTE/5G ≥ 50 Mbps Upload.
0 Punkte (B19): < 50 Mbps/unstabil.
- 20 Punkte (B20): Live-Stream flüssig (< 5 s Latenz).
0 Punkte (B20): Verzögerung/Abbrüche.
- 15 Punkte (B21): Bluetooth-Trigger funktioniert fehlerfrei.
0 Punkte (B21): Kein Trigger.
- 15 Punkte (B22): Bluetooth-Schnittstelle vorhanden
0 Punkte (B22): nicht vorhanden
- 15 Punkte (B23): Bluetooth-Sprachübertragung klar.
0 Punkte (B23): Verzerrt/kein Audio.
- 10 Punkte (B24): Akkuwechsel werkzeuglos möglich
0 Punkte (B24): kein eigener Akkuwechsel möglich
- 10 Punkte (B25): > 12 h Aufnahme ohne Akku-Ende.
0 Punkte (B25): ≤ 12 h.
- 5 Punkte (B26): Akku < 4 h voll in Docking.
0 Punkte (B26): ≥ 4 h.
- 10 Punkte (B27): Stand-Alone Ladestation vorhanden
0 Punkte (B27): nicht vorhanden
- 10 Punkte (B28): Dockingstation als Multi-Port vorhanden
0 Punkte (B28): nicht vorhanden

Dokumentation: Netzwerk-Logs (Verbindungen, Raten), Streaming-Videos, Akku-Ladekurven, Bluetooth-Protokolle, Tester-Erklärungen, Fotos der Statusanzeigen.

7.3.4 Testmodul 4: Cloud-Grundfunktionen

Zielsetzung: Dieses Modul überprüft grundlegende Such-, Filter- und Bearbeitungsfunktionen der Cloud-Software in der SaaS-Testinstanz.

Geprüfte Mindestkriterien und Bewertungskriterien:

- M47 – SaaS – Datenexport

- M56 – Software – Bearbeitung der Dateien
- M57 – Software – Löschen von Dateien nach Rollenkonzept
- M58 – Software – Teilen von Dateien nach Rollenkonzept
- M59 – Software – Protokollierung
- M60 – Software – Export auf USB/CD
- M61 – Software – Filterung nach Datum und Uhrzeit
- M62 – Software – Filterung nach Bodycam-Nummer
- M63 – Software – Filterung nach Nutzer-ID
- M64 – Software – Filterung nach TR/IA
- M65 – Software – Videobearbeitung (Schnitt)
- M66 – Software – Videobearbeitung (Kommentare einfügen)
- M67 – Software – Videobearbeitung (Bezeichnung der Datei ändern)
- M68 – Software – Verwaltung (Benutzer-/Geräteverwaltung)
- M69 – Software – Verwaltung (Automatische Löschfristen)
- M70 – Software – Verwaltung (Gerätezuordnung)
- M71 – Software – Verwaltung (Protokollierung)
- M72 – Software – Verwaltung (hierarchische Organisationsstruktur)
- B29 – Software – Filterung (Mehrfachfilter) (10 Punkte)
- B30 – Software – Filterung (Volltextsuche/Metadaten) (10 Punkte)
- B31 – Software – Videobearbeitung (Bildverbesserung) (15 Punkte)
- B32 – Software – Videobearbeitung (erweiterte Videoverarbeitung) (10 Punkte)
- B33 – Software – Videobearbeitung (Erzeugen von Standbildern) (15 Punkte)
- B34 – Software – Videobearbeitung (Kennzeichnung/Markierung - Einzelbild) (15 Punkte)
- B35 – Software – Videobearbeitung (bewegte Markierungen) (10 Punkte)

Maximal erreichbare Punkte in diesem Modul: **85 Punkte**

Testdurchführung:

Vorbereitung: Die Testkommission füllt SaaS-Testinstanz mit 50+ Testvideos (verschiedene Daten, IDs, TR/IA-Markierungen, Nutzer), definiert Testskripte bereit.

Testaufbau: Browser-Zugang zur Cloud-Software mit Testrollen (Nutzer, Admin), vorbereiteter Testdatensatz sichtbar.

Testdurchgang:

1. Datenexport: Vollständigen Export (Video + Metadaten) durchführen (M47, M60).
2. Filtertests: Nach Datum/Bodycam/Nutzer/TR/IA filtern, Mehrfachfilter kombinieren (M61–M64, B29).
3. Volltextsuche: Metadaten/Text durchsuchen (B30).
4. Videobearbeitung: Schnitt/Kommentare/Umbenennen durchführen (M56-M58, M65–M67).

5. Erweiterte Bearbeitung: Bildverbesserung (Kontrast/Helligkeit), erweiterte Verarbeitung (Zoom), Standbild extrahieren (B31–B33).
6. Markierungen: Einzelbild kennzeichnen, bewegte Markierungen zeichnen (B34/B35).
7. Verwaltung prüfen: Alle Änderungen im Audit-Log nachvollziehen (M59, M68-M72).

Bewertung:

- 10 Punkte (B29): Mehrfachfilter (z. B. Datum + Nutzer) präzise, <3s Ergebnis.
0 Punkte (B29): Ungenau/zu langsam.
- 10 Punkte (B30): Volltextsuche in Metadaten/Text funktioniert fehlerfrei.
0 Punkte (B30): Keine/inadequate Suche.
- 15 Punkte (B31): Bildverbesserung (Kontrast/Schärfe) wirksam verbessert Video.
0 Punkte (B31): Kein Effekt.
- 10 Punkte (B32): Erweiterte Verarbeitung (z. B. Stabilisierung/Zoom) nutzbar.
0 Punkte (B32): Fehlend/unwirksam.
- 15 Punkte (B33): Standbilder fehlerfrei extrahierbar (JPEG).
0 Punkte (B33): Fehlend/qualitätsarm.
- 15 Punkte (B34): Einzelbild-Kennzeichnung präzise setzbar/sichtbar.
0 Punkte (B34): Ungenau/fehlend.
- 10 Punkte (B35): Bewegte Markierungen (Tracking) flüssig.
0 Punkte (B35): Fehlend/jittery.

Dokumentation: Screenshots vor/nach Filtern/Bearbeitung, Testskript-Protokoll mit Zeiten, Audit-Logs, exportierte Standbilder/Markierungen, Tester-Bewertung der Bedienbarkeit.

7.3.5 Testmodul 5: Speicher & Warnung

Zielsetzung: Dieses Modul überprüft Speichermanagement, Warnfunktionen und Überwachung in der Cloud-Software.

Geprüfte Mindestkriterien und Bewertungskriterien:

- M80 – Cloud – Warnmeldung bei Speicherauslastung (bei 80%)
- B43 – Cloud – Warnmeldung bei Speicherauslastung (mehrstufige Warnungen) (10 Punkte)
- B44 – Cloud – Warnmeldungen bei Speicherauslastung (automatische Speicher-Berichte) (5 Punkte)

Maximal erreichbare Punkte in diesem Modul: **15 Punkte**

Testdurchführung:

Vorbereitung: Die Testkommission simuliert hohe Speicherauslastung in SaaS-Testinstanz (Upload großer Testvideos), definiert Admin-Rolle mit Warnzugriff.

Testaufbau: Cloud-Software mit Testdaten (ca. 75–95% Auslastung simulieren), Admin angemeldet.

Testdurchgang:

1. Speicherauslastung auf 75/80/85/95% steigern (Upload/Simulation).
2. Warnmeldungen beobachten: Bei 80% (M80), mehrstufig bei 75/85/95% (B43).
3. Automatische Berichte abrufen (Prognose, B44).
4. Backup/Skalierung prüfen: Restore-Testdatei, Redundanz simulieren (Multi-AZ-Status).

Bewertung:

- 10 Punkte (B43): Mehrstufige Warnungen (75/85/95%) per E-Mail/UI, konfigurierbar.
0 Punkte (B43): Nur 80% oder fehlend.
- 5 Punkte (B44): Automatische Berichte mit Prognose (z. B. Vollausslastung in Tagen).
0 Punkte (B44): Keine Berichte/Prognose.

Dokumentation: Screenshots Warnmeldungen/Berichte, Speicherauslastungs-Logs vor/nach, E-Mail-Protokolle, Backup-Restore-Nachweis.

7.3.6 Testmodul 6: Spezielle Features & Interoperabilität

Zielsetzung: Dieses Modul überprüft spezielle Softwarefunktionen, Integrationen und Interoperabilität der Cloud-SaaS-Lösung.

Geprüfte Mindestkriterien und Bewertungskriterien:

- M48 – SaaS – Dokumentation der REST-API
- M73 – Software – Rollenkonzept
- M74 – Software – Sonderfunktionen (Innere Angelegenheiten)
- M75 – Software – Sonderfunktionen (To Review)
- B36 – Software – Spezielle Funktionen (Passwortänderung durch Nutzer) (10 Punkte)
- B37 – Software – Spezielle Funktionen (Import externer Medienquellen) (10 Punkte)
- B38 – Software – Spezielle Funktionen (Geopositionsdaten – Kartendarstellung) (10 Punkte)
- B39 – Software – Spezielle Funktionen (Geopositionsdaten-Extraktion ohne Visualisierung) (5 Punkte)
- B40 – Software – Spezielle Funktionen (Gesicherter Link-Versand) (10 Punkte)
- B41 – Software – Spezielle Funktionen (Single-Sign-On) (5 Punkte)
- B42 – Software – Spezielle Funktionen (Gerätezuordnung per RFID/Dongle) (10 Punkte)
- B45 – Cloud – Unterstützung von Containertechnologien (15 Punkte)
- B46 – Cloud – Infrastructure-as-Code-Dokumentation (10 Punkte)

Maximal erreichbare Punkte in diesem Modul: **80 Punkte**

Testdurchführung:

Vorbereitung: Die Testkommission bereitet SaaS-Testinstanz mit GPS-videos, externen Dateien, Testnutzern/Rollen, SAML-Simulator, RFID-Dongle vor.

Testaufbau: Cloud-Software-Zugang, externe Medien/Export-Tools, IaC-Docs bereit, Container-Umgebung (Docker-Test).

Testdurchgang:

1. Passwort: Nutzer ändert eigenes Passwort (B36).
2. Import: Externe Video-Datei hochladen (B37).
3. GPS: Kartendarstellung/Export von Geo-Daten (B38/B39).
4. Link-Versand: Gesicherten Link erstellen/teilen (Zeitlimit, Logs, B40).
5. SSO: Mit SAML/Simulator anmelden (B41).
6. RFID-Zuordnung: Dongle scannen, Gerät zuordnen (B42).
7. Rollen/Sonder: IA/TR kennzeichnen, Zugriffsrechte prüfen (M73–M75).
8. Interop: REST-API-Call (JSON-Export), Container-Deploy test, IaC-Skripte prüfen (M48, B45/B46).

Bewertung:

- 10 Punkte (B36): Self-Service-Passwortänderung funktioniert.
0 Punkte (B36): Nur Admin möglich.
- 10 Punkte (B37): Externe Medien importiert/indexiert.
0 Punkte (B37): Import fehlend.
- 10 Punkte (B38): GPS-Daten klar auf Karte visualisiert.
0 Punkte (B38): Keine Karte. (Alternative B39: 5 Punkte für Export ohne Karte).
- 10 Punkte (B40): Link mit Zeitlimit/Logs/Deaktivierung.
0 Punkte (B40): Unsicher/fehlend.
- 5 Punkte (B41): SSO (SAML/OIDC) erfolgreich.
0 Punkte (B41): Kein SSO.
- 10 Punkte (B42): RFID/Dongle-Zuordnung instant.
0 Punkte (B42): Manuell/kein Support.
- 15 Punkte (B45): Container (Docker/K8s) deploybar.
0 Punkte (B45): Kein Container-Support.
- 10 Punkte (B46): Vollständige IaC-Docs (Terraform/CloudFormation).
0 Punkte (B46): Fehlend/unvollständig.

Dokumentation: Screenshots (Links, Karten, SSO-Login), API-Response-Logs, IaC-Skripte/Deploy-Proof, Import-Tests, RFID-Protokolle, Tester-Berichte.

7.3.7 Testmodul 7: Integration & Sicherheit

Zielsetzung: Dieses Modul überprüft spezielle Hardware-Integrationen, Sicherheitsfunktionen und Software-Schnittstellen inklusive Praxistests für kritische Mindestkriterien.

Geprüfte Mindestkriterien und Bewertungskriterien:

- M6 – Schnellregistration (RFID)

- M7 – Automatisierte Aufnahme bei Nutzung von FEM
- M11 – Integriertes Global Navigation Satellite System
- M12 – Georeferenzierung in Aufnahmen
- M13 – Visualisierung in einer Karte (SaaS-Dienst) oder Export (BPOLMaps)
- M14 – Manipulationssichere Zeitstempel
- M15 – Schutz gegen unbefugten Zugriff und Datenlöschung
- M16 – Pre-Event-Recording
- M79 – Cloud – Protokollierung nach BDSG

Maximal erreichbare Punkte in diesem Modul: **0 Punkte (lediglich eine Verifizierung der Mindestkriterien)**

Testdurchführung:

Vorbereitung: Die Testkommission stellt RFID-Karten/Dongles, FEM-Holster/Dienstwaffe-Simulator, GPS-Testumgebung (Fenster), entladenes Testgerät, Standardnutzer-Accounts bereit.

Testaufbau: Bodycam in Weste, FEM-Holster mit Dummy-Waffe, Cloud-Software mit Testnutzern/Rollen, GPS-Sicht zum Himmel.

Testdurchgang:

1. RFID-Registrierung: Karte scannen, Nutzerzuordnung prüfen (M6).
2. FEM-Trigger: Waffe ziehen, automatische Aufnahme verifizieren (M7).
3. GPS/Metadaten: Aufnahme mit GNSS starten, Geo-Daten in Cloud prüfen (M11/M12).
4. Kartenvisualisierung/Export: GPS-Videos in Karte anzeigen oder BPOLMaps-Export (M13).
5. Zeitstempel: Lokale Zeit manipulieren, Unveränderbarkeit prüfen (M14).
6. Zugriffs-Schutz: Nicht-Admin-Nutzer versucht USB-Lesen/Löschen (M15).
7. Pre-Event: Aufnahme triggern, Vorlauf prüfen (M16).
8. Protokollierung: Alle Aktionen im BDSG-Audit-Log nachvollziehen (M79).

Bewertung:

Binäre M-Verifizierung (erforderlich/nicht erforderlich):

- M6: RFID-Registrierung erfolgreich in <5s.
- M7: FEM-Trigger löst Aufnahme zuverlässig aus.
- M11/M12: GPS-Daten korrekt in Metadaten.
- M13: Karte/Export funktioniert.
- M14: Zeitstempel manipulationssicher.
- M15: Unbefugter Zugriff blockiert.
- M16: Pre-Event-Vorlauf enthalten.
- M47: Export vollständig (MP4+JSON).
- M73: Rollenrechte korrekt umgesetzt.
- M79: BDSG-Protokollierung vollständig.

Nicht erforderlich → Ausschluss

Dokumentation: Videos (RFID-Scan, FEM-Trigger, Pre-Event), GPS-Metadaten-Export, Zeitstempel-Logs, Zugriffsversuch-Screenshots, Firmware-Update-Protokoll, Rollen-Tests, Audit-Logs, Export-Dateien.

7.4 Bewertung und Punktevergabe

7.4.1 Grundsätze

Für jedes im Rahmen der Teststellung geprüfte B-Kriterium wird nach Maßgabe der vorstehenden Testmodule entweder die volle, in der Bewertungsmatrix festgelegte Rohpunktzahl oder 0 Rohpunkte vergeben. Zwischenwerte sind nur zulässig, wenn dies in der Bewertungsmatrix ausdrücklich vorgesehen ist.

M-Kriterien mit Zusatz „Praxistest“ werden ausschließlich binär beurteilt (erfüllt/nicht erfüllt). Die Nichterfüllung eines solchen Mindestkriteriums führt ungeachtet zuvor erzielter Punkte zum Ausschluss des Angebots.

7.4.2 Zusammenführung mit der schriftlichen Bewertung

Die in der Teststellung erzielten Rohpunkte für B-Kriterien werden mit den Ergebnissen der schriftlichen Bewertung zusammengeführt, indem:

- alle Bodycam-Hardware-B-Kriterien (B1 – B28) mit dem in der Bewertungsmatrix definierten Faktor 0,5 gewichtet werden,
- Alle Software-B-Kriterien (B29 – B46) mit dem in der Bewertungsmatrix definierten Faktor 0,3 gewichtet werden.

Die Teststellung bestimmt dabei ausschließlich, ob ein Kriterium die vorgesehene Rohpunktzahl oder 0 Punkte erhält. Die anschließende Gewichtung erfolgt einheitlich für alle Bieter gemäß des Dokuments „Bewertungsmatrix“. Die so ermittelte Gesamtleistungspunktzahl wird anschließend mit dem Preiskriterium gemäß den Vorgaben im Dokument „01. Hinweise für dieses Verfahren und besondere Bewerbungsbedingungen“ zur Ermittlung des wirtschaftlichsten Angebots kombiniert.

7.4.3 Umgang mit Testausfällen und technischen Problemen

Gerätedefekt vor oder während der Teststellung:

Falls ein Testgerät vor Beginn der Teststellung defekt ist oder während der Teststellung ausfällt, erhält der Bieter die Möglichkeit, ein Ersatzgerät bereitzustellen. Dies ist jedoch nur einmal pro Bieter zulässig und muss innerhalb der laufenden Teststellung erfolgen. Kann kein Ersatzgerät bereitgestellt werden, wird der betroffene Test mit 0 Punkten bewertet.

Testfehler durch Verschulden der Auftraggeberin/Bedarfsträgerin:

Falls ein Test aufgrund eines Fehlers in der Testdurchführung (z. B. defekte Testausrüstung, falsche Testparameter) fehlschlägt, wird der Test wiederholt.

Testfehler durch Verschulden des Bieters:

Falls ein Test aufgrund eines Fehlers des Bieters fehlschlägt (z. B. falsche Konfiguration, Bedienungsfehler), wird der Test nicht wiederholt, es sei denn, der Fehler ist offensichtlich und kann sofort korrigiert werden. In diesem Fall entscheidet der Testleiter über eine Wiederholung.

Unklare Testergebnisse:

Bei unklaren Testergebnissen (z. B. grenzwertige Messungen, divergierende Einschätzungen der Testkommission) wird der Test einmal wiederholt. Bei erneuter Unklarheit entscheidet die Testkommission durch Mehrheitsbeschluss.

8. Liste aller in der Leistungsbeschreibung vorkommenden Kriterien

8.1 Mindestkriterien

In der nachfolgenden Übersicht sind alle Mindestanforderungen dieser Leistungsbeschreibung aufgeführt. Die Spalte „Prüfmethode/Nachweis“ gibt an, ob ein Mindestkriterium ausschließlich durch Unterlagen (zum Beispiel Datenblatt, Zertifikat, Prüfbericht etc.), ausschließlich im Rahmen der Teststellung oder durch eine Kombination aus Unterlagen und Praxistest nachzuweisen ist. Mindestanforderungen, bei denen das Wort „**Praxistest**“ angegeben ist, werden im Rahmen der Teststellung überprüft.

Sofern zu einem Mindestkriterium keine herstellerseitigen Unterlagen (z. B. Datenblätter, Zertifikate, Prüfberichte) vorliegen, kann der Bieter den Nachweis durch eine aussagekräftige Eigenerklärung erbringen. Diese Eigenerklärungen sind in einem **zusammenhängenden PDF-Dokument** darzustellen und eindeutig den jeweiligen Mindestkriterien (z. B. „M32 – Automatischer Cloud-Upload“, Kapitel- und Seitenangabe) zuzuordnen. Die in der Eigenerklärung beschriebenen Eigenschaften werden, sofern in der Tabelle ein Praxistest vorgesehen ist, im Rahmen der Teststellung verifiziert.

Beispiel für eine Eigenerklärung zu M32 – Automatischer Cloud-Upload:

„Die angebotene Lösung unterstützt einen vollautomatischen Upload aller auf der Bodycam gespeicherten Aufnahmen in die Cloud-Software, sobald die Bodycam in eine Dockingstation eingesetzt oder mit dem dienstlichen WLAN verbunden wird. Der Upload erfolgt ohne Benutzereingriff, es werden ausschließlich verschlüsselte Verbindungen gemäß TLS 1.3 genutzt. Der Upload-Status ist am Gerät über eine zweifarbige LED (Blau = Upload läuft, Grün = Upload abgeschlossen) erkennbar.“

Im Praxistest wird dann geprüft, ob sich die Bodycams wie in dieser Eigenerklärung beschrieben verhalten (automatischer Upload, Verschlüsselung, Statusanzeige etc.).

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
Mindestanforderungen, die die Hardware (Bodycams) betreffen			
M1	Gewicht der Bodycam (max.255g)	Hersteller Datenblatt mit Angabe des Gerätegewichts ggf. Prüfbericht/Zertifikat, Eigenerklärung des Bieters zur Einhaltung des Maximalgewichts, Verifizierung im Praxistest durch Wiegen betriebsbereiter Mustergeräte mit Präzisionswaage im Rahmen der Teststellung.	3.1.1, Seite: 11
M2	Kompatibilität zu MOLLE	Herstellereklärung und technische Dokumentation (Zeichnungen/Fotos) zu MOLLE-Kompatibilität. Angabe im Datenblatt Funktionsnachweis im Praxistest durch Anbringen der Bodycam mit gelieferten Adaptern an ballistischer Weste und weiterer Ausrüstung.	3.1.2, Seite: 12
M3	Schutzklasse (IP67)	Prüfbericht oder Zertifikat einer unabhängigen, möglichst akkreditierten Prüfstelle zur erreichten IP-Schutzklasse, Angabe der Schutzklasse im Hersteller Datenblatt.	3.1.5, Seite: 13

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M4	Robustheit (Falltest aus 1m)	Prüfbericht oder Herstellerprotokoll zu Falltests aus 1 m, ggf. Zertifikat einer Prüfstelle, Eigenerklärung des Bieters zur Einhaltung der Anforderung, ergänzender Praxistest im Rahmen des Falltests in Testmodul 1, bei dem sichtbar wird, ob Geräte Stürze ohne Funktionsverlust überstehen	3.1.6, Seite: 14
M5	Temperaturbereich (-20 °C bis +50 °C)	Hersteller Datenblatt mit Angabe des Betriebstemperaturbereichs, Prüfbericht aus einer Klimakammer oder gleichwertigem Testaufbau, ausgestellt von Hersteller oder unabhängiger Prüfstelle.	3.1.7, Seite: 14
M6	Schnellregistration (RFID).	Hersteller Dokumentation zum Registrierungsverfahren (z. B. RFID/NFC-Konzept), Beschreibung des eingesetzten Identifikationsverfahrens, Eigenerklärung, Funktionsnachweis im Praxistest durch praktische Durchführung mehrerer Registrierungsvorgänge mit Testpersonen	3.1.9, Seite: 15

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M7	Automatisierte Aufnahme bei Nutzung von FEM	Hersteller Dokumentation zur Kopplung mit FEM-Holstern (DEIG, Dienstwaffe) und Auslöselogik, Eigenerklärung des Bieters, Funktionsnachweis im Praxistest durch Nachstellen typischer Ziehvorgänge mit gekoppelten Mustern	3.1.10, Seite: 16
M8	Firmwarebereitstellung	Schriftliches Firmware-Lifecycle/Update-Konzept des Bieters, Eigenerklärung zur Bereitstellung von Sicherheits- und Funktionsupdates für den geforderten Zeitraum	3.1.11, Seite: 16
M9	Firmwareupdate der Bodycams	Hersteller-Dokumentation zum Update-Prozess (zentrale Verteilung, Verteilung über Dockingstation/OTA), Eigenerklärung, Angabe im Datenblatt.	3.1.11, Seite: 16
M10	Speicherausstattung	Hersteller-Datenblatt mit Angabe der minimalen Speicherkapazität (z. B. ≥ 64 GB), Eigenerklärung, stichprobenartige Kontrolle im Rahmen der Teststellung durch Auslesen der angezeigten Kapazität an Gerät oder in der Cloud-Software.	3.2.1, Seite: 17

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M11	Integriertes Global Navigation Satellite System	Hersteller-Datenblatt/Technische Dokumentation zum integrierten GNSS/GPS-Modul, Eigenerklärung, Funktionsnachweis im Praxistest durch Aufzeichnung mit GNSS und Auswertung der Positionsdaten in der Cloud-Software.	3.2.2, Seite: 18
M12	Georeferenzierung in Aufnahmen	Hersteller-Dokumentation, dass Positionsdaten automatisiert in unveränderbaren Metadaten jeder Aufnahme gespeichert werden, Eigenerklärung, Praxistest durch Prüfung von Metadaten/Positionsanzeige aufgezeichneter Testvideos.	3.2.2, Seite: 18
M13	Visualisierung in einer Karte (SaaS-Dienst) oder Export (BPOLMaps)	Hersteller-Dokumentation der Kartenvisualisierung bzw. Export-Schnittstelle (Format, Felder), Eigenerklärung, Praxistest in der Testinstanz der Cloud-Software durch Anzeige von Testaufnahmen in der Karte bzw. Export und Import in eine Referenzkarte.	3.2.2, Seite: 18

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M14	Manipulationssichere Zeitstempel	Technische Dokumentation zum Zeitstempel-Konzept (zentrale Zeitquelle, NTP-Synchronisation, Unveränderbarkeit auf dem Gerät), Eigenerklärung, Praxistest durch Versuch, lokale Zeit/Timecodes zu verändern und Überprüfung der Protokollierung/Nicht-Veränderbarkeit.	3.2.3, Seite: 19
M15	Schutz gegen unbefugten Zugriff und Datenlöschung	Sicherheitskonzept (Verschlüsselung, Zugriffsrechte, Löschkonzept), Eigenerklärung, ggf. unabhängiger Sicherheitsbericht, Praxistest: Versuch, mit einem Nutzer ohne Adminrechte Aufnahmen direkt auf der Bodycam oder via USB zu lesen/löschen.	3.2.4, Seite: 19
M16	Pre-Event-Recording	Hersteller-Datenblatt mit Angabe der Vorlaufzeit und Konfigurierbarkeit, Eigenerklärung, Praxistest: Auslösen einer Aufnahme und anschließende Kontrolle, ob die definierte Vorlaufzeit zuverlässig in der Aufnahme enthalten ist.	3.2.5, Seite: 20

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M17	Videoqualität (720/1080p, 25FPS)	Hersteller-Datenblatt mit Angabe der unterstützten Auflösungen und Bildraten, Eigenerklärung, Praxistest: Aufnahmen in 720p/1080p mit 25 FPS, Kontrolle der Metadaten und Sichtprüfung auf ausreichende Bildqualität.	3.3.1, Seite: 20
M18	Video-Codec (H.264)	Hersteller-Datenblatt/Technische Spezifikation mit Angabe des verwendeten Codecs, Eigenerklärung.	3.3.2, Seite: 20
M19	Bildstabilisierung	Hersteller-Dokumentation zur eingesetzten Bildstabilisierung (EIS/OIS), Eigenerklärung, Praxistest: Anhand eines Bewegungsparcours wird der Verwacklungsgrad, die Lesbarkeit von Texten, Erkennbarkeit von Gesichtern und Gegenständen geprüft.	3.3.3, Seite: 21
M20	Horizontales Sichtfeld der Kamera (min. 110 Grad)	Hersteller-Datenblatt mit Angabe des horizontalen Sichtfelds, Eigenerklärung,	3.3.4, Seite: 21

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M21	Zwei Mikrofone	Hersteller-Datenblatt/Blockschaltbild mit Angabe von mindestens zwei Mikrofonen und Rauschfilterung, Eigenerklärung Praxistest: Durch Abhören von Aufnahmen in typischen Umgebungen und Beurteilung der Grundqualität.	3.3.5, Seite: 22
M22	Klare Sprachaufzeichnung (bei 60-70 dB)	Hersteller-Angaben (z. B. Frequenzgang, SNR) im Datenblatt, Eigenerklärung, Gezielter Praxistest mit definierter Geräuschkulisse (ca. 60–70 dB) und standardisiertem Text, Auswertung der Sprachverständlichkeit durch die Testkommission.	3.3.5, Seite: 22
M23	Akustisches Startsignal (1m Entfernung)	Hersteller-Dokumentation zur Signalisierung, Eigenerklärung, Praxistest: Start mehrerer Aufnahmen in normaler und lauter Umgebung, Überprüfung, ob das Startsignal aus 1 m Entfernung klar wahrnehmbar ist.	3.3.6, Seite: 22
M24	LED-Statusanzeige (Aufnahme)	Hersteller-Datenblatt/Fotos mit Angabe der optischen Statusanzeige, Praxistest: Beobachtung der LED/Display-Anzeige beim Start/Stop von Aufnahmen und während laufender Aufzeichnung durch die Testkommission.	3.3.7, Seite: 23

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M25	Statusanzeige (Akkuladezustand)	Hersteller-Datenblatt/Bedienungsanleitung mit Beschreibung der Akku-Statusanzeige, Eigenerklärung, Praxistest: Beobachtung der Anzeige (LED/Display) bei unterschiedlichen Ladeständen an Testgeräten.	3.3.7, Seite: 23
M26	Warnmeldung visuell, akustisch oder haptisch (Speicherplatzknappheit)	Hersteller-Datenblatt/Bedienungsanleitung zur Speicherwarnung, Eigenerklärung, Praxistest: gezieltes Füllen des Speichers bis zum Schwellwert und Kontrolle der ausgelösten Warnungen (optisch/akustisch/haptisch).	3.3.7, Seite: 23
M27	USB-C (Anschluss vorhanden)	Hersteller-Datenblatt und Fotos/Zeichnungen zum USB-C-Port, CE-Konformitätserklärung, Praxistest: Sichtprüfung des Anschlusses und Anschluss eines Standard-USB-C-Kabels an Testrechner/Netzteil.	3.4.1, Seite: 23
M28	USB-C (Ladefunktion)	Hersteller Datenblatt zur Ladefunktion über USB C, Eigenerklärung, Praxistest durch Laden einer nahezu entladenen Bodycam ausschließlich über USB C und Kontrolle, dass der Ladevorgang korrekt startet und endet.	3.4.1, Seite: 23

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M29	USB-C (Dateiübertragung)	Hersteller Datenblatt/Bedienungsanleitung zur Datenübertragung per USB C, Eigenerklärung, Praxistest durch Anschluss der Bodycam an einen Testrechner und erfolgreichen Transfer einer Testaufnahme als Datei.	3.4.1, Seite: 23
M30	USB-C (administrative Änderungen)	Technische Dokumentation zum administrativen Zugriff per USB C (z. B. Konfiguration/Firmware Update), Eigenerklärung.	3.4.1, Seite: 23
M31	WiFi-Konnektivität WiFi 802.11ac, 802.11b, 802.11g, und 802.11n)	Hersteller-Datenblatt mit unterstützten WLAN-Standards Eigenerklärung, Praxistest durch Einbindung in das Test-WLAN und erfolgreichen Verbindungsaufbau/Grundkommunikation.	3.4.2, Seite 24
M32	Automatischer Cloud-Upload	Hersteller-Dokumentation zum Upload-Mechanismus, Eigenerklärung, Praxistest durch Aufnahme mehrerer Sequenzen, Einsetzen in Dockingstation/WLAN-Umgebung und Prüfung, ob Upload automatisch in die Cloud erfolgt.	3.4.3, Seite: 24

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M33	Automatischer Cloud-Upload (Fortsetzung nach Unterbrechung)	Technische Beschreibung zur fehler-toleranten Upload-Fortsetzung, Eigenerklärung, Praxistest durch gezieltes Unterbre-chen eines laufenden Uploads und Kontrolle, ob der Upload später au-tomatisch fortgesetzt/neu gestartet wird.	3.4.3, Seite: 24
M34	Statusanzeige bei automati-schem Cloud-Upload	Hersteller-Datenblatt/Bedienungs-anleitung zur Upload-Statusanzeige (LED/Display), Eigenerklärung, Praxistest durch Beobachtung der Anzeige während Upload, bei er-folgreichem Abschluss und bei Feh-ler/Unterbrechung.	3.4.3, Seite: 24
M35	Bluetooth-Schnittstelle und Integration mit Digitalfunk-geräten	Hersteller-Datenblatt zu Blue-tooth-Version/Sicherheit, Integrationsdokumentation mit auf-geführten BOS-Digitalfunkgeräten, Eigenerklärung, Praxistest durch Koppeln mit Refe-renzfunkgeräten und Test einer stabilen Verbindung.	3.4.5, Seite: 25
M36	Akku wiederaufladbar	Hersteller-Datenblatt mit Angabe von Zelltyp und Ladezyklen, Eigenerklärung, ggf. Prüfbericht (Zyklusfestigkeit) ei-nes Labors.	3.5.1, Seite: 27

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M37	Akkulaufzeit (Aufnahmezeit min. 10h)	Prüfbericht/Messprotokoll zur Daueraufzeichnung bei 1080p/25 FPS unter Referenzbedingungen, Hersteller-Datenblatt, Eigenerklärung.	3.5.1, Seite: 27
M38	Ladestation/Dockingstation mit EU-Standardstecker (Typ F/C, 230V, 50Hz)	Hersteller-Datenblatt (Netzteil/Steckerart, Eingangsspannung), CE-Kennzeichnung, Praxistest durch Sichtprüfung des Steckers und Funktionstest an Standard-230-V-Anschluss am Testort.	3.5.3, Seite 28
M39	Dockingstation (gleichzeitiges Laden und Datenübertragung)	Hersteller-Dokumentation zur Dockingstation-Funktionalität, Eigenerklärung, Praxistest durch gleichzeitiges Laden einer eingesteckten Bodycam und Upload an die Cloud-Software, Kontrolle von Ladezustand und Übertragungsstatus.	3.5.3, Seite: 28
M40	Dockingstation (integrierter Überhitzungsschutz)	Hersteller-Datenblatt/Sicherheitsdokumentation zum Überhitzungsschutz, CE/ggf. GS-Zertifikat.	3.5.3, Seite: 28

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M41	Dockingstation (Statusanzeige: Laden/Fertig/Upload)	Hersteller-Datenblatt/Bedienungsanleitung zu LED/Display-Status, Eigenerklärung, Praxistest durch Beobachtung der unterschiedlichen Statusanzeigen bei Laden, vollem Akku und laufendem Upload an Testgeräten.	3.5.3, Seite: 28
M42	Dockingstation (automatische Firmwareupdates)	Technische Dokumentation zum Zero-Touch-Update über Dockingstation, Eigenerklärung.	3.5.4, Seite: 29
M43	Firmwareupdates während der Nutzung (ohne Beeinträchtigung)	Update-Konzept (Zeitsteuerung, Schutz laufender Einsätze), Eigenerklärung.	3.5.4, Seite: 29
M44	Statusanzeige bei Firmwareupdate	Hersteller-Dokumentation zur Update-Statusanzeige, Eigenerklärung.	3.5.4, Seite: 29
M45	Versorgungs- und Reparatursicherheit	Service-/Instandhaltungskonzept mit zugesicherter Laufzeit, Eigenerklärung.	3.6.1, Seite: 30
Mindestkriterien, die die Software sowie die Cloudinfrastruktur betreffen			

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M46	SaaS – Verwenden von Standardtechnologie (REST, JSON, XML etc.)	Architektur-/Schnittstellendokumentation (Beschreibung der verwendeten Standards), vollständige REST-API-Dokumentation, Eigenerklärung, dass keine proprietären, undokumentierten Formate für Kernfunktionen genutzt werden.	4.14.1.1, Seite: 33
M47	SaaS – Datenexport	Funktionsbeschreibung und Screenshots des Export-Dialogs, REST-/Export-API-Dokumentation (Formate, Felder), Eigenerklärung, Praxistest durch Export eines Testfalls (Videos und Metadaten) in standardisierten Formaten.	4.1.1, Seite: 33
M48	SaaS – Dokumentation der REST-API	Vollständige, versionierte REST-API-Dokumentation (z. B. OpenAPI/Swagger), Eigenerklärung zur Bereitstellung für die Bundespolizei,	4.1.1, Seite: 33

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M49	SaaS – BSI Empfehlungen	IT-Sicherheitskonzept mit Bezug auf relevante BSI-Grundlagen (z. B. BSI-Grundsatz, TR, C5-Testat oder gleichwertige unabhängiger Prüfbericht), Eigenerklärung zur Einhaltung, Audit-/Zertifikatsnachweise (z. B. BSI-C5-Testat), hilfsweise sonstige prüffähige Unterlagen zur Darlegung gleichwertiger Sicherheitsmaßnahmen.	4.1.2, Seite: 33
M50	SaaS – AES-256 Verschlüsselung	Kryptokonzept (At-Rest-Verschlüsselung mit AES-256), Eigenerklärung, ggf. unabhängiger Sicherheitsbericht oder Zertifizierung, der den Einsatz starker Verschlüsselung bestätigt.	4.1.2, Seite: 33
M51	SaaS – TLS1.3 oder höher	Technische Beschreibung der Transportverschlüsselung (TLS-Versionen, Cipher Suites), Eigenerklärung, ggf. SSL-Scan/Report oder unabhängiger Sicherheitsbericht, Plausibilitätsprüfung der Unterlagen.	4.1.2, Seite: 33
M52	SaaS – Barrierefreiheit (BITV 2.0 Testat)	Gültiges BITV-2.0-Testat/Prüfbericht einer anerkannten Prüfstelle,	4.1.3, Seite: 34

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M53	SaaS – Server-/Speicherstandort	Hosting-Vertrag/Architekturdiagramm mit Rechenzentrumsstandorten in der EU (bevorzugt DE), Eigenerklärung, ggf. Rechenzentrums-Zertifikate (z. B. ISO 27001) als Plausibilitätsnachweis.	4.1.4, Seite: 35
M54	Sicherheitsüberprüftes Personal (SÜ1)	Eigenerklärung, dass alle für die Leistungserbringung relevanten Mitarbeiter mindestens S1-Sicherheitsüberprüfung besitzen werden.	4.2.4, Seite: 37
M55	Software – Anzeige/Abspielen von Videos	Hersteller-Dokumentation zur Wiedergabefunktion, Eigenerklärung, Praxistest in der SaaS-Testinstanz durch Abspielen mehrerer Testvideos mit unterschiedlichen Rollen (Nutzer, Administrator).	4.3.1, Seite: 38
M56	Software – Bearbeitung der Dateien	Funktionsbeschreibung der Bearbeitungsfunktionen (Schneiden, Benennen, Kommentieren), Eigenerklärung, Praxistest durch Durchführung typischer Bearbeitungsschritte an Testaufnahmen.	4.3.1, Seite: 38

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M57	Software – Löschen von Dateien nach Rollenkonzept	Rollen- und Löschkonzept (inkl. Fristenmanagement), Eigenerklärung, Praxistest durch Löschkversuche mit unterschiedlichen Rollen (Nutzer, Fachadministrator) und Kontrolle der Protokollierung.	4.3.1, Seite: 38
M58	Software – Teilen von Dateien nach Rollenkonzept	Dokumentation der Sharing-Funktionen und Rechteprüfung, Eigenerklärung, Praxistest durch Teilen von Testaufnahmen zwischen Rollen/Organisationseinheiten und Überprüfung der Zugriffsbeschränkungen.	4.3.1, Seite: 38
M59	Software - Protokollierung	Dokumentation zu Audit-Logs (Inhalt, Unveränderbarkeit, Aufbewahrungsdauer), Eigenerklärung, Praxistest durch typische Aktionen und Einsicht in die automatisch erzeugten Protokolleinträge.	4.3.1, Seite: 38
M60	Software – Export auf USB/CD	Funktionsbeschreibung zum Export (Formate, Integritätsprüfung), Eigenerklärung, Praxistest durch Export eines Testvideos auf bereitgestellten USB-Datenträger und Überprüfung der Abspielbarkeit (z. B. MP4).	4.3.1, Seite: 38

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M61	Software – Filterung nach Datum und Uhrzeit	Dokumentation der Filterfunktionen, Eigenerklärung, Praxistest durch Filtern des Testdatenbestands nach einem definierten Zeitraum und Überprüfung der Vollständigkeit der Treffer.	4.3.2, Seite: 39
M62	Software – Filterung nach Bodycam-Nummer	Dokumentation der Filterfunktion nach Geräte-ID, Eigenerklärung, Praxistest durch Abruf aller Aufnahmen einer bestimmten Bodycam mittels Filter.	4.3.2, Seite: 39
M63	Software – Filterung nach Nutzer-ID	Dokumentation der Filterfunktion nach Nutzerkennung, Eigenerklärung, Praxistest durch Abruf aller Aufnahmen eines bestimmten Nutzers (rollenabhängig) über die Filterfunktion.	4.3.2, Seite: 39
M64	Software – Filterung nach TR/IA	Dokumentation zur Filterung nach TR/IA-Kennzeichnung, Eigenerklärung, Praxistest durch gezielte Filterung nach markierten TR/IA-Fällen im Testdatenbestand.	4.3.2, Seite: 39

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M65	Software – Videobearbeitung (Schnitt)	Funktionsbeschreibung/Bedienungsanleitung zum Trimmen, Eigenerklärung, Praxistest durch Zuschneiden einer Testsequenz und Kontrolle der Protokollierung/Unverändertheit des Originals.	4.3.3, Seite: 39
M66	Software – Videobearbeitung (Kommentare einfügen)	Dokumentation zur Kommentarfunktion, Eigenerklärung, Praxistest durch Hinzufügen und Anzeige von Kommentaren zu Testvideos bei verschiedenen Rollen.	4.3.3, Seite: 39
M67	Software – Videobearbeitung (Bezeichnung der Datei ändern)	Dokumentation zur Umbenennung/Metadatenpflege, Eigenerklärung, Praxistest durch Änderung von Dateibezeichnungen (z. B. Vorgangsnummer) und Kontrolle der Nachvollziehbarkeit in den Logs.	4.3.3, Seite: 39
M68	Software – Verwaltungsfunktionen (Benutzer- und Geräteverwaltung)	Admin-Handbuch zur Nutzer-/Geräteverwaltung, Eigenerklärung, Praxistest durch Anlegen, Ändern und Löschen von Testnutzern sowie Zuordnung von Test-Bodycams.	4.3.4, Seite: 40

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M69	Software – Verwaltungsfunktionen (Automatische Löschfristen)	Dokumentation zum Fristenmanagement, Eigenerklärung, Praxistest durch Konfiguration einer Test-Löschfrist und Überprüfung der geplanten/automatisierten Löschung in der Testumgebung.	4.3.4, Seite: 40
M70	Software – Verwaltungsfunktionen (Gerätezuordnung)	Dokumentation zur Geräte-/Organisationszuordnung, Eigenerklärung, Praxistest durch Zuordnung von Testgeräten zu fiktiven Dienststellen und Sichtprüfung der Auswertungsmöglichkeiten nach Strukturen.	4.3.4, Seite: 40
M71	Software – Verwaltungsfunktionen (Protokollierung)	Dokumentation zu Admin-Protokollen (Nutzeranlage, Rechteänderungen, Geräteverwaltung), Eigenerklärung, Praxistest durch Durchführung typischer Administrationsaktionen und Kontrolle der Protokolleinträge.	4.3.4, Seite: 40
M72	Software – Verwaltungsfunktionen (hierarchische Organisationsstruktur)	Dokumentation zur Abbildung hierarchischer Organisation (Dienststellen, Einheiten), Eigenerklärung, Praxistest durch Anlegen/Ändern einer Beispielstruktur und Prüfung der Zugriffssteuerung entlang der Hierarchie.	4.3.4, Seite: 40

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M73	Software – Rollenkonzept	Rollen-/Rechtemodell-Dokumentation, Eigenerklärung, Praxistest durch Anmeldung mit unterschiedlichen Rollen und Prüfung der jeweils erlaubten bzw. gesperrten Funktionen.	4.4, Seite: 42ff
M74	Software – Sonderfunktionen (Innere Angelegenheiten)	Dokumentation der Sonderrolle/n „Innere Angelegenheiten“ (z. B. separater Datentopf), Eigenerklärung, Praxistest durch Anlegen/Verwalten eines Falls im IA-Kontext und Prüfung der Abschottung gegenüber Standardrollen.	4.4.3, Seite: 45
M75	Software – Sonderfunktionen (To Review)	Dokumentation zur To-Review-Kennzeichnung und zugehörigen Workflows, Eigenerklärung, Praxistest durch Kennzeichnen von Aufnahmen als „To Review“ und Abruf/Liste dieser Fälle in der Testumgebung.	4.4.3, Seite: 45
M76	Cloud – Speicherkapazität skalierbar	Architektur-/Betriebskonzept zur Skalierung (z. B. Cluster/Storage-Scaling), Eigenerklärung,	4.5.1, Seite: 46

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M77	Cloud – Datensicherung (min. einmal täglich)	Backup-Konzept (Frequenz, Medien, Aufbewahrungsfristen), Eigenerklärung, ggf. Audit-/Revisionsberichte,	4.5.2, Seite: 46
M78	Cloud – redundante Infrastruktur	Architekturdiagramme mit Redundanzen (z. B. Multi-AZ, Redundanz von Datenbanken/Storage), Eigenerklärung, ggf. Zertifikate/Auditberichte des Rechenzentrums,	4.5.2, Seite: 46
M79	Cloud – Protokollierung nach BDSG	Dokumentation des Audit-Log-Systems (Inhalte, Revisionssicherheit, technische Umsetzung), Eigenerklärung, ggf. Sicherheits-/Datenschutzgutachten, Praxistest durch Auslösen typischer Aktionen und Prüfung der vollständigen, unveränderbaren Protokollierung.	4.5.4, Seite: 47

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M80	Cloud – Warnmeldung bei Speicherauslastung (bei 80%)	Dokumentation zur Speicherüberwachung und Warnlogik, Eigenerklärung, Praxistest durch Befüllen eines Test-Tenants bis nahe an 80 % Auslastung (oder Simulation per Konfiguration) und Kontrolle der automatisch generierten Warnmeldung an Administratoren.	4.5.5, Seite: 47
M81	Cloud – Datenlöschung nach Vertragsende	Konzept zur Datenlöschung/Migration nach Vertragsende (inkl. 1-Jahres-Übergangsphase und vollständiger physischer Löschung), Eigenerklärung.	4.5.6, Seite: 48
M82	SaaS – REST-API	REST-API-Dokumentation (Endpunkte, Authentifizierung, Datenmodelle), Eigenerklärung.	4.6.1, Seite: 48
Mindestkriterien, die den Service und Support betreffen			
M83	Service und Support – Einhaltung der SLA	SLA-Dokument mit definierten Prioritäten, Reaktions- und Wiederherstellungszeiten, Eigenerklärung zur verbindlichen Einhaltung.	5.1, Seite: 49

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M84	Service und Support – Software-Updates	Update-/Release-Konzept, Eigenerklärung zu Intervallen und Ankündigungsfristen, Muster eines Release-Notes.	5.2, Seite: 50
M85	Service und Support – Sicherheits-Patches	Sicherheits-Patch-Prozessbeschreibung (Reaktionszeiten, Priorisierung), Eigenerklärung, ggf. Auszug aus ISMS-Dokumentation, Plausibilitätsprüfung.	5.2, Seite: 50
M86	Service und Support – Bug-Fix-Zyklen	Konzept zu Bug-Fix-Zyklen (z. B. monatliche Releases, Ad-hoc-Hotfixes), Eigenerklärung.	5.2, Seite: 50
M87	Schulungen in Präsenzform	Schulungskonzept (Präsenz, Zielgruppen, Inhalte), Eigenerklärung.	6.1.1, Seite: 51
M88	Schulungen unmittelbar nach Lieferung	Zeit-/Ressourcenplanung für Schulungswellen, Eigenerklärung.	6.1.2, Seite: 52
M89	Schulungsunterlagen in deutscher Sprache	Muster-Schulungsunterlagen in deutscher Sprache in editierbarem Format (z. B. PPTX/DOCX), Eigenerklärung zur Bereitstellung und Anpassbarkeit.	6.1.3, Seite: 52

ID	Name des Mindestkriteriums	Prüfmethode/Nachweis	Referenz zum Kapitel
M90	Bedienungsanleitung in deutscher Sprache (Bodycam)	Muster-Bedienungsanleitung in deutscher Sprache (Print und PDF) mit allen geforderten Inhalten, Eigenerklärung.	6.2.1, Seite: 52
M91	Bedienungsanleitung in deutscher Sprache (Cloud-Software)	Muster-Bedienungsanleitung der Cloud-Software in deutscher Sprache inkl. Screenshots, Eigenerklärung, Sichtprüfung der Inhalte (Anmeldung, Suche, Bearbeitung, Rollen etc.).	6.2.2, Seite: 53
M92	Technische Dokumentation für IT-Administratoren/Entwickler	Muster der technischen Dokumentation (Architektur, REST-API, Sicherheit, Backup/Recovery, Logformate) in deutscher Sprache, Eigenerklärung.	6.2.3, Seite: 53
M93	Marktreife/Serienerzeugnis	Offizielle, unveränderte Produktdatenblätter, Auszug aus dem regulären Produktkatalog des Herstellers	2.2, Seite: 9

8.2 Bewertungskriterien

ID	Name des Bewertungskriteriums	Punktzahl	Referenz zum Kapitel
Bewertungskriterien, die die Hardware (Bodycams) betreffen			
B1	Gewicht der Bodycam	5	3.1.1, Seite: 11
B2	Intuitive Menüführung ohne Schulung	15	3.1.3, Seite: 12
B3	Bedienbarkeit mit dicken Handschuhen	5	3.1.4, Seite: 13

ID	Name des Bewertungskriteriums	Punktzahl	Referenz zum Kapitel
B4	Robustheit (Falltest aus 1,5m)	10	3.1.6, Seite: 14
B5	Frontdisplay	15	3.1.8, Seite: 15
B6	Speicherausstattung	10	3.2.1, Seite: 17
B7	Videoqualität (4k+)	5	3.3.1, Seite: 20
B8	Video-Codec (H.265)	10	3.3.2, Seite: 20
B9	Horizontales Sichtfeld der Kamera (im Bereich 120 bis 130 Grad)	10	3.3.4, Seite: 21
B10	Kamera horizontal schwenkbar	10	3.3.4, Seite: 21
B11	Kamera vertikal schwenkbar	10	3.3.4, Seite: 21
B12	Aktive Geräuschfilterung	10	3.3.5, Seite: 21
B13	Klare Sprachaufzeichnung (bei >85 dB)	10	3.3.5, Seite: 22
B14	Statusanzeige (mit Wifi verbunden)	5	3.3.5, Seite: 22
B15	Statusanzeige (mit LTE/5G verbunden)	5	3.3.5, Seite: 22
B16	Statusanzeige (mit Bluetooth verbunden)	5	3.3.5, Seite: 22
B17	Statusanzeige (Datum und Uhrzeit)	5	3.3.5, Seite: 22
B18	Statusanzeige (Debug-Informationen)	5	3.3.5, Seite: 22
B19	Mobile Netzwerkunterstützung (LTE/5G)	15	3.4.4, Seite: 24
B20	Live-Streaming (Real-Time Situational Awareness)	20	3.4.4, Seite: 24
B21	Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten (Trigger-Funktion)	15	3.4.5, Seite: 25
B22	Bluetooth-Schnittstelle zu Geräten des Herstellers Sepura (STP- und SC-Serie)	15	3.4.5, Seite: 25
B23	Bluetooth-Schnittstelle und Integration mit Digitalfunkgeräten (Sprachaufzeichnung)	15	3.4.5, Seite: 25

ID	Name des Bewertungskriteriums	Punktzahl	Referenz zum Kapitel
B24	Akkuwechsel	10 bzw. 5	3.5.1, Seite: 26
B25	Akkulaufzeit (Aufnahmezeit > 12h)	10	3.5.1, Seite: 27
B26	Ladestation/Dockingstation mit Schnellladefunktion (Akku innerhalb < 4h vollgeladen)	5	3.5.1, Seite: 27
B27	Ladestation (Stand-Alone, Laden ohne Bodycam)	10	3.5.2, Seite: 27
B28	Dockingstation (Multi-Port)	10	3.5.2, Seite: 28
Bewertungskriterien, die die Software betreffen			
B29	Software – Filterung (Mehrfachfilter)	10	4.3.2, Seite: 39
B30	Software – Filterung (Volltextsuche/Metadaten)	10	4.3.2, Seite: 39
B31	Software – Videobearbeitung (Bildverbesserung)	15	4.3.3, Seite: 39
B32	Software – Videobearbeitung (erweiterte Videoverarbeitung)	10	4.3.3, Seite: 39
B33	Software – Videobearbeitung (Erzeugen von Standbildern)	15	4.3.3, Seite: 39
B34	Software – Videobearbeitung (Kennzeichnung/Markierung - Einzelbild)	15	4.3.3, Seite: 39
B35	Software – Videobearbeitung (bewegte Markierungen)	10	4.3.3, Seite: 39
B36	Software – Spezielle Funktionen (Passwortänderung durch Nutzer)	10	4.3.5, Seite: 41ff
B37	Software – Spezielle Funktionen (Import externer Medienquellen)	10	4.3.5, Seite: 41ff
B38	Software – Spezielle Funktionen (Geopositionsdaten – Kartendarstellung)	10	4.3.5, Seite: 41ff

ID	Name des Bewertungskriteriums	Punktzahl	Referenz zum Kapitel
B39	Software – Spezielle Funktionen (Geopositionsdaten-Extraktion ohne Visualisierung) Hinweis: Dieses Kriterium ist als Alternative zu B38 anzusehen. Es kann nur Punkte für B38 oder B39 geben.	5	4.3.5, Seite: 41ff
B40	Software – Spezielle Funktionen (Gesicherter Link-Versand)	10	4.3.5, Seite: 41ff
B41	Software – Spezielle Funktionen (Single-Sign-On)	5	4.3.5, Seite: 41ff
B42	Software – Spezielle Funktionen (Gerätezuordnung per RFID/Dongle)	10	4.3.5, Seite: 41ff
B43	Cloud – Warnmeldung bei Speicherauslastung (mehrstufige Warnungen)	10	4.5.5, Seite: 47
B44	Cloud – Warnmeldungen bei Speicherauslastung (automatische Speicher-Berichte)	5	4.5.5, Seite: 47
B45	Cloud – Unterstützung von Containertechnologien	15	4.6.3, Seite: 49
B46	Cloud – Infrastruktura-as-Code-Dokumentation	10	4.6.3, Seite: 49