

Anforderungskatalog Datenschutz und IT-Sicherheit

1. Einleitung & Struktur des Katalogs

Dieser Anforderungskatalog definiert die zwingenden rechtlichen, funktionalen und technischen Mindestanforderungen an den Plattformanbieter (Auftragnehmer) zum Schutz personenbezogener Daten und zur Gewährleistung der Informationssicherheit.

Die Anforderungen sind nach dem datenschutzrechtlichen **Drei-Ebenen-Modell** strukturiert:

- **Ebene 1 (Organisatorisch-prozessuale Governance):** Anforderungen an Prozesse, Verträge und Zusammenarbeit.
- **Ebene 2 (Fachapplikation - Softwareebene):** Funktionale und logische Anforderungen an die Softwarearchitektur der Plattform.
- **Ebene 3 (Technische Infrastruktur - Hosting-Ebene):** Anforderungen an die Server, Netzwerke, Verschlüsselung und den Cloud-Betrieb.

2. Ebene 1: Vertragliche Governance & Organisatorische Anforderungen (GOV)

ID	Meilensteinzuordnung	Anforderungsbeschreibung
GOV-01	Meilenstein 1	Abschluss des Muster-AVV: Der Bieter verpflichtet sich unwiderruflich, mit jeder dem Rahmenvertrag beitretenden regionalen IHK unverzüglich und ohne inhaltliche Abweichungen eine direkte Vereinbarung zur Auftragsverarbeitung auf Basis des als Anlage beigefügten Muster-AVV (Art. 28 DSGVO) abzuschließen.

GOV-02	Meilenstein 1	Subdienstleister-Anzeige (UAV): Der Auftragnehmer muss jede geplante Änderung, Einbindung oder den Austausch von Unterauftragsverarbeitern (UAV) mindestens sechs (6) Wochen vor dem geplanten Einsatz schriftlich an die zentrale Koordinierungsstelle (DIHK-Geschäftsstelle) melden.
GOV-03	Meilenstein 1	Sonderkündigungsrecht bei UAV-Widerspruch: Dem Auftraggeber (den regionalen IHKs) ist vertraglich das Recht einzuräumen, dem Einsatz eines neuen UAV aus wichtigem datenschutzrechtlichem Grund zu widersprechen. Kann der Auftragnehmer den Widerspruch nicht durch technische Maßnahmen (z. B. Mandantenausschluss) heilen, steht der betroffenen IHK ein sofortiges, kostenfreies Sonderkündigungsrecht für die Plattformnutzung zu.
GOV-04	Meilenstein 1	Unterstützung bei der Datenschutz-Folgenabschätzung (DSFA): Der Bieter ist verpflichtet, die DIHK bei der Erstellung der Muster-

		DSFA) durch Bereitstellung aller erforderlichen technischen Dokumentationen, Risikoanalysen und Nachweise (z. B. Architekturdiagramme, Datenflussbeschreibungen) kostenfrei zu unterstützen.
GOV-05	Meilenstein 1	Zentralisiertes Auditierungsrecht: Der Auftragnehmer muss dulden und vertraglich zusichern, dass die IHK-Organisation (vertreten durch den Lenkungskreis) einmal jährlich ein gemeinsames, umfassendes Datenschutz- und Sicherheitsaudit durch einen unabhängigen, zertifizierten Prüfer durchführen lässt. Audits sollen vorrangig auf Basis von Zertifikaten und Testaten des Auftragnehmers und seiner Nachunternehmer bzw. Auftragsverarbeiter erfolgen, Vor-Ort-Kontrollen müssen aber möglich bleiben, wenn sie gesetzlich erforderlich sind.
GOV-06	Meilenstein 1	Schulung und Dokumentation: Der Bieter muss detaillierte, leicht verständliche Administrations- und

		Benutzerhandbücher in deutscher Sprache bereitstellen.
--	--	--

3. Ebene 2: Fachapplikation - Softwarebezogene Anforderungen (APP)

3.1 Mandantentrennung & Zugriffskontrolle (RBAC)

ID	Klassifizierung	Anforderungsbeschreibung
APP-01	Meilenstein 1	Strikte logische Mandantentrennung (Multi-Tenancy): Die Applikation muss so konzipiert sein, dass Datenströme, Abfragen und Speicherbereiche streng mandantenspezifisch (nach der jeweiligen IHK-Mandanten-ID) isoliert verarbeitet werden. Mandantenübergreifende SQL-Abfragen oder Datenzugriffe müssen systemseitig im Quellcode technisch unmöglich sein (<i>Tenant-aware Design</i>).
APP-02	Meilenstein 1	Rollenbasierte Zugriffskontrolle (RBAC): Die Software muss eine strikte, feingranulare Funktionstrennung auf Basis vordefinierter Rollen (Prüfling, Prüfer, Aufsicht,

		IHK-Mitarbeiter, Systemadministrator) erzwingen (<i>Need-to-know-Prinzip</i>).
APP-03	Meilenstein 1	Multi-Faktor-Authentifizierung (MFA): Für alle privilegierten Rollen (Prüfer, Aufsichten, IHK-Mitarbeitende, Administratoren) muss eine starke Zwei-Faktor-Authentifizierung (2FA) applikationsseitig erzwungen werden.
APP-04	Meilenstein 1 / Meilenstein 2a	Automatisches Sitzungs-Timeout: Aktive Softwaresitzungen müssen bei Inaktivität automatisch beendet werden (Timeout nach maximal 10 Minuten bei Aufsichtskonten, 15 Minuten bei Prüferkonten).

3.2 Datensparsamkeit & Pseudonymisierung

ID	Klassifizierung	Anforderungsbeschreibung
APP-05	Meilenstein 2a	Pseudonymisierte Korrekturmaske: Die Applikation muss standardmäßig neben einer Verarbeitung von personenbezogenen Daten als Klardaten auch eine vollständig

		pseudonymisierte Bewertung von Freitextaufgaben unterstützen. (im letzteren Fall dürfen Prüfer bei der Korrektur keine Klarnamen oder demografischen Daten der Prüflinge sehen, sondern ausschließlich eine temporäre Prüfungs-ID.
APP-06	Meilenstein 2a	Kapselung der Identitätszuordnung: Die Zuordnungstabelle zwischen der temporären Prüfungs-ID und dem Klarnamen des Prüflings muss softwareseitig streng gekapselt sein. Der Zugriff ist auf die Rollen "Prüfungsaufsicht vor Ort" (zeitlich beschränkt auf die Durchführung) und die interne "IHK-Prüfungsorganisation" (zur Notenverbuchung) zu beschränken.
APP-07	Meilenstein 1	Ausschluss der Mitarbeiterüberwachung: Eine softwareseitige Auswertung von Nutzungs- und Bearbeitungsdaten der Prüferinnen, Prüfer und Aufsichten zur personal-, arbeits- oder dienstrechtlichen Leistungs- und Verhaltenskontrolle muss technisch und

		organisatorisch ausgeschlossen sein.
--	--	--------------------------------------

3.3 Datenintegrität & Revisionssicherheit

ID	Klassifizierung	Anforderungsbeschreibung
APP-08	Meilenstein 2a	Kryptografische Abgabesicherung: Unmittelbar bei der Abgabe der Prüfung durch den Prüfling muss die Applikation automatisch eine kryptografische Prüfsumme (SHA-256-Hash oder höher) über alle abgegebenen Antworten generieren, um nachträgliche Manipulationen detektierbar zu machen.
APP-09	Meilenstein 1 / Meilenstein 2a	Lückenloser fachlicher Audit Trail: Alle administrativen und bewertungsrelevanten Aktionen (z. B. manuelle Notenkorekturen, Gewährung von Schreibzeitverlängerungen) müssen revisionssicher, lückenlos und unmanipulierbar protokolliert (historisiert) werden. Ein direktes Überschreiben ohne Historienbildung ist

		unzulässig.
APP-10	Meilenstein 1	Eingabe-Validierung (WAF-Konformität): Alle Eingabefelder der Applikation müssen gegen Einschleusung von Schadcode (SQL-Injection, Cross-Site-Scripting/XSS) geschützt sein.

3.4 Ausfallsicherheit & Offline-Caching

ID	Klassifizierung	Anforderungsbeschreibung
APP-11	Meilenstein 3	Offline-Caching auf Endgeräten: Die Software muss über eine lokale, verschlüsselte Zwischenspeicherung (z. B. via <i>IndexedDB</i> im Kiosk-Browser) auf dem Endgerät des Prüflings verfügen. Bei Netzunterbrechungen muss die Prüfung unterbrechungsfrei offline fortführbar sein; Antworten müssen bei Netzzurückkehr automatisch im Hintergrund synchronisiert werden.
APP-12	Meilenstein 1	Prüfungsstarts und sonstige Spitzenlasten Die Applikationslogik muss so konzipiert sein, dass bei bundesweiten Lastspitzen

		eine reibungsloser Prüfungsbetrieb sichergestellt ist.
--	--	--

3.5 Betroffenenrechte (Export & Sperrung)

ID	Klassifizierung	Anforderungsbeschreibung
APP-13	Meilenstein 2a / bereits ab Meilenstein 1 muss eine Möglichkeit bestehen Betroffenen nach Anforderung einen Datenexport/ bzw. eine Datenkopie zur Verfügung zu stellen	Automatisierter Datenkopie-Export (Art. 15 DSGVO): Die Applikation muss eine Funktion bereitstellen, die es IHK-Mitarbeitenden ermöglicht, auf Knopfdruck eine vollständige, strukturierte Datenkopie aller über einen Prüfling gespeicherten Daten (inkl. Klickprotokolle, Antworten, Bewertungen) in einem gängigen Format zu generieren.
APP-14	Meilenstein 3	Schwärzungsfunktion im Export: Das Datenkopie-Exporttool muss eine integrierte Schwärzungsfunktion aufweisen, um schutzwürdige Rechte Dritter (z. B. die Identität von Prüfern nach Art. 15 Abs. 4 DSGVO) vor der Aushändigung zu zensieren.

APP-15	Meilenstein 1	Sperr-Flags: Es müssen Datenstatus-Merkmale (z. B. "Gesperrt wegen Widerspruchsverfahren") implementiert sein, um Daten manuell von automatisierten Löschrufen auszunehmen.
APP-16	- <i>(Nur relevant, falls die Lösung des Bieters eine Nachteilsausgleichsfunktion enthält, auf die diese Anforderung zutrifft.)</i>	Getrennte Verarbeitung der Nachteilsausgleichsparameter. Die Umsetzungsparameter eines bewilligten Nachteilsausgleichs sind in einem eigenen, gesondert verschlüsselten Datenbereich mit eigenem Rollenprofil zu führen. Der Zugriff ist auf namentlich autorisierte Beschäftigte der zuständigen IHK zu beschränken. Prüferoberflächen, Korrekturmasken und Standard-Exportansichten dürfen auf diesen Bereich keinen Zugriff haben. Aufsichten erhalten ausschließlich die zur Durchführung zwingend erforderliche Angabe, insbesondere eine veränderte Bearbeitungszeit, nicht aber Grund oder Anlass des Ausgleichs. Für den Datenbereich ist gesondertes Schlüsselmaterial zu

		verwenden.
APP-17	= <i>(Nur relevant, falls die Lösung des Bieters eine Nachteilsausgleichsfunktion enthält, auf die diese Anforderung zutrifft.)</i>	Beschränkung auf Umsetzungsparameter Die Applikation darf für den Nachteilsausgleich ausschließlich abstrakte Umsetzungsparameter aufnehmen, etwa „Schreibzeitverlängerung 25 %“, „Screenreader-Kompatibilität“ oder „Einzelraum“. Datenfelder für Diagnosen, Attest-Inhalte, Grad der Behinderung oder sonstige medizinische Angaben sind nicht vorzusehen. Der Upload medizinischer Nachweise auf die Plattform ist technisch zu unterbinden. Freitextfelder im Kontext des Nachteilsausgleichs sind auf ein Minimum zu reduzieren und mit einem Hinweis zu versehen, dass Gesundheitsangaben nicht einzutragen sind.
APP-18	Meilenstein 1	Einwilligungs- und Widerrufsmanagement Für optionale Zusatzdienste, die auf einer Einwilligung beruhen, muss die Applikation ein granulares, nachweisbares Einwilligungs- und Widerrufsmanagement

		bereitstellen, das die Anforderungen des Art. 7 DSGVO und des § 25 Abs. 1 TDDDG erfüllt (Konzept Ziff. 5.2). Einwilligungen sind je Zweck getrennt einzuholen, mit Zeitpunkt und Textfassung zu protokollieren und jederzeit mit gleichem Aufwand widerrufbar. Der Widerruf muss die betroffene Funktion unverzüglich deaktivieren. Voreingestellte Zustimmungen und Kopplungen an die Prüfungsteilnahme sind ausgeschlossen. Für Minderjährige unter 16 Jahren ist der Einbezug der gesetzlichen Vertreter vorzusehen.
--	--	---

4. Ebene 3: Technische Infrastruktur & Cloud-Betrieb (INF)

4.1 Geografische & Administrative Souveränität

ID	Klassifizierung	Anforderungsbeschreibung
INF-01	Meilenstein 1	Datenverarbeitung ausschließlich in EU/EWR: Sämtliche personenbezogenen Daten

		(als <i>data at rest</i> und <i>data in use</i>) müssen in zertifizierten (mindestens ISO 27001 oder gleichwertig) Rechenzentren innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) gespeichert und verarbeitet werden. Dies gilt für die gesamte Unterauftragsverarbeiterkette.
INF-02	Meilenstein 1	Ausschluss von Drittstaatensupport (Remote-Zugriff): Jegliche Support-, Wartungs-, Administrations- und Remotezugriffe auf die Plattform und die Hosting-Infrastruktur müssen physisch aus der EU/dem EWR heraus erfolgen. Ein <i>Follow-the-Sun-Support</i> aus Drittländern ist vertraglich und technisch auszuschließen.

4.2 Technische Zusatzmaßnahmen bei Public-Cloud-Nutzung

(Nur relevant, falls der Bieter eine US-geprägte Public-Cloud-Infrastruktur wie AWS, Azure oder Google Cloud anbietet. Diese Maßnahmen müssen kumulativ erfüllt sein):

ID	Klassifizierung	Anforderungsbeschreibung
INF-03	Meilenstein 1	Hold Your Own Key (HYOK): Alle sensiblen

		Daten müssen im Ruhezustand (<i>data at rest</i>) mit AES-256 (oder höher) verschlüsselt sein. Die Schlüsselverwaltung (External Key Management) muss physisch und logisch außerhalb des Zugriffsbereichs des Cloud-Anbieters im exklusiven Einflussbereich der IHK-Organisation liegen.
INF-04	Meilenstein 1	Präsentieren eines TIAs: Der Bieter muss ein detailliertes, lückenloses <i>Transfer Impact Assessment</i> (TIA) vorlegen, das die technischen Risiken unbefugter Datenzugriffe durch Drittstaatenbehörden analysiert und die Wirksamkeit der implementierten TOMs nachweist.

4.3 Netzwerksicherheit & Verschlüsselung

ID	Klassifizierung	Anforderungsbeschreibung
INF-05	Meilenstein 1	Verschlüsselung im Transit (Data in Transit): Alle Datenübertragungen

		müssen ausnahmslos über verschlüsselte Kommunikationskanäle mittels TLS 1.3 unter Nutzung sicherer Cipher Suites erfolgen. Die interne Server-Kommunikation im Rechenzentrum ist über mTLS oder IPSec abzusichern.
INF-06	Meilenstein 1	Netzwerksegmentierung: Die Rechenzentrums Umgebung muss konsequent logisch segmentiert sein (z. B. mittels VLANs und Micro-Segmentation) zur strikten Trennung von Webservern, Applikationsservern und Datenbanksystemen.

4.4 Backup, Protokollierung & Desasterschutz

ID	Klassifizierung	Anforderungsbeschreibung
INF-07	Meilenstein 1	Georedundantes Backup-Konzept: Täglich automatisierte Datensicherungen müssen georedundant in mindestens zwei physisch getrennten, zertifizierten Rechenzentren (Mindestabstand gemäß BSI-Vorgaben) aufbewahrt werden.

INF-08	Meilenstein 2a	Automatisiertes Recovery-Testing: Mindestens vierteljährlich müssen automatisierte Wiederherstellungstests (Restore-Tests) zur Überprüfung der definierten Wiederanlaufzeiten (RTO/RPO) durchgeführt und dokumentiert werden.
INF-09	Meilenstein 2a	Schreibgeschützter Logserver: Alle technischen Logfiles und Revisionsdaten müssen in Echtzeit an einen dedizierten, schreibgeschützten Protokollserver (SIEM-System) außerhalb der administrativen Domäne der Produktiv-Infrastruktur übertragen werden. IP-Adressen in Zugriffsprotokollen sind nach 7 Tagen automatisiert zu löschen.

5. Incident- & Sicherheitsmanagement (INC)

ID	Klassifizierung	Anforderungsbeschreibung
INC-01	Meilenstein 1	Zentraler 24/7 Security Incident Service: Der Auftragnehmer muss ein rund um die Uhr besetztes

		Security Incident Management (SOC) zur Erkennung, Abwehr und Dokumentation von IT-Sicherheitsvorfällen bereitstellen.
INC-02	Meilenstein 1	Der Auftragnehmer verpflichtet sich vertraglich, jeden Sicherheitsvorfall oder jede vermutete Datenpanne auf der Plattform unverzüglich, spätestens aber binnen 24 Stunden zu melden, auch um es den IHKs zu ermöglichen, ihre Meldungen untereinander zu koordinieren.
INC-03	Meilenstein 1	Verwendung des Standard-Meldetemplates: Für die Meldung hat der Auftragnehmer ein vordefiniertes Meldetemplate (in Absprache mit dem Auftraggeber) zu nutzen, welches zwingend alle notwendigen Informationen nach Art. 33 Abs. 3 DSGVO strukturiert enthält.
INC-04	Meilenstein 1	Automated Incident Response: Die Fachapplikation muss über automatisierte Mechanismen zur

		Angriffserkennung und -eindämmung verfügen (z. B. automatische temporäre Sperrung von Konten bei Brute-Force-Angriffen oder Sperrung von APIs bei atypischen Massenabrufen).
INC-05	Meilenstein 1	Isolations-Architektur bei Kompromittierung: Im Falle der Kompromittierung eines einzelnen IHK-Mandanten muss die Applikationslogik eine sofortige Quarantäne dieses Mandanten ermöglichen, sodass eine Ausbreitung (<i>Lateral Movement</i>) auf die übrigen 78 Mandanten technisch ausgeschlossen ist.

6. Datenlöschung & Exit-Szenarien (EXT)

ID	Klassifizierung	Anforderungsbeschreibung
EXT-01	Meilenstein 1	Zweistufiges Löschverfahren mit Karenzzeit: Nach erfolgreicher Datenquittierung durch die IHK sind die Daten zunächst für den regulären Zugriff zu sperren (Sperrung). Die endgültige, physische Löschung (BSI-konformes

		Überschreiben) auf den Servern und Backups darf erst nach einer Karenzzeit von 90 Tagen erfolgen.
EXT-02	Meilenstein 1	Interoperables Datenexportformat (Exit-Fall): Im Falle eines Exits oder Systemwechsels ist der Auftragnehmer verpflichtet, alle personenbezogenen Daten (inkl. Ergebnisse und Audit Trails) in einem strukturierten, gängigen und maschinenlesbaren Format (JSON oder XML) sowie das vollständige Datenbankschema (<i>Data Dictionary</i>) in deutscher Sprache kostenfrei zu übergeben.
EXT-03	Meilenstein 1	Granularer Teil-Exit: Die Plattform muss technisch in der Lage sein, die Daten eines einzelnen Mandanten vollständig und isoliert zu exportieren und anschließend unwiderruflich zu löschen, ohne den Betrieb der übrigen Mandanten zu beeinträchtigen.
EXT-04	Meilenstein 1	Qualifiziertes Löschprotokoll: Der Auftragnehmer hat die unwiderrufliche Löschung der Daten nach einem Exit

		durch ein qualifiziertes Löschprotokoll pro Mandanten-ID nachzuweisen.
--	--	--

7. Anforderungen an den Einsatz von KI-Systemen (KI)

(Relevant, falls optionale KI-gestützte Funktionen in der Lösung des Bieters enthalten sind):

ID	Klassifizierung	Anforderungsbeschreibung
KI-01	-	Ausschluss verbotener KI-Praktiken (Art. 5 KI-Verordnung): Der Einsatz von KI-Systemen zur Erkennung von Emotionen im Bildungs- und Prüfungsumfeld, zur biometrischen Kategorisierung sensibler Merkmale oder zur Verhaltensmanipulation ist auf der gesamten Plattform technisch und organisatorisch ausgeschlossen.
KI-02	-	Menschliches Korrektiv (Human-in-the-Loop): Eine rein automatisierte Einzelfallentscheidung (Art. 22 DSGVO) bei der Notenermittlung ist unzulässig. Die Applikation muss eine Workflow-Schranke erzwingen, wonach jeder KI-generierte

		Bewertungsvorschlag zwingend durch den menschlichen Prüfungsausschuss geprüft und manuell freigegeben werden muss.
KI-03	-	Erklärbarkeit der KI (Explainable AI): Das KI-System muss in der Lage sein, seine Bewertungsvorschläge anhand der hinterlegten Musterlösungen und Bewertungskriterien transparent und für den menschlichen Prüfer nachvollziehbar zu begründen.
KI-04	-	Souveräne Mandantensteuerung (Opt-In / Opt-Out): Die Aktivierung von KI-Funktionen muss auf Ebene der Fachapplikation mandantenspezifisch steuerbar sein. Ist die Funktion für eine IHK deaktiviert, darf kein Datentransfer an die KI-Schnittstellen erfolgen.
KI-05	-	Striktes KI-Trainingsverbot: Eine Übertragung personenbezogener Daten von Prüflingen oder Prüfern zum Zwecke des Trainings, des Finetunings oder der

		Weiterentwicklung der KI-Modelle des Betreibers oder von Drittanbietern ist strikt verboten.
KI-06	-	Nachweis der Daten-Governance (Bias-Minimierung): Der Bieter muss die Herkunft, Struktur und Repräsentativität der genutzten Trainingsdaten dokumentieren und nachweisen, wie algorithmische Diskriminierungen (Bias) ausgeschlossen werden.
KI-07	-	KI-Sicherheitsarchitektur: Der Bieter muss die Robustheit der KI-Infrastruktur gegen spezifische Angriffe wie <i>Data Poisoning</i> und <i>Prompt Injection</i> nachweisen.