

Security, Vertrag und Exit prüfen

Nachweisliste und Freigabebogen für Cloud-, Kanzlei- und KI-Software vor Vertragsabschluss.

So wird die Unterlage verwendet

Die Felder werden im Auswahlteam gemeinsam vorbereitet, von Testpersonen zunächst unabhängig bewertet und anschließend in einer dokumentierten Entscheidung zusammengeführt. Leere Felder sind Absicht: Die Unterlage soll mit eigenen Nachweisen gefüllt werden.

Skala: 0 = nicht erfüllt oder nicht belegt · 1 = schwach · 2 = teilweise · 3 = solide · 4 = gut · 5 = vollständig belegt und im Szenario bestätigt.

1. Anbieter und Governance

ID	Prämissen	Erwarteter Nachweis / Text	Status	Owner
G1	Vertragspartner, Konzernstruktur und verantwortliche Betriebseinheiten sind eindeutig.	Impressum, Organigramm, Vertragsparteien	☐ offen	
G2	Unterauftragnehmer, Leistungen und Datenstandorte sind vollständig benannt.	Aktuelle Subprozessorenliste	☐ offen	
G3	Änderungen bei Unterauftragnehmern werden rechtzeitig angekündigt.	Vertragsklausel und Widerspruchsprozess	☐ offen	
G4	Anforderungen aus § 43e BRAO sind in Textform adressiert.	Vertragsanlage Verschwiegenheit/Zweckbindung	☐ offen	
G5	AV-Vertrag, Weisungsrechte und Kontrollunterstützung sind geregelt.	AVV und TOM-Anlage	☐ offen	
G6	Zertifikate gelten für Produkt, Standorte und Betrieb im angebotenen Scope.	Zertifikat plus Scope Statement	☐ offen	

2. Identitäten, Zugriffe und Verschlüsselung

ID	Prämissen	Erwarteter Nachweis / Test	Status	Owner
I1	SSO und Multifaktor-Authentisierung sind für alle relevanten Rollen verfügbar.	Live-Test und Konfigurationsnachweis	[] offen	
I2	Rollen folgen dem Minimalprinzip und sind mandatsbezogen einschränkbar.	Rollenmatrix und Live-Test	[] offen	
I3	Support- und Adminzugriffe sind genehmigt, protokolliert und zeitlich begrenzt.	Privileged-Access-Prozess und Logbeispiel	[] offen	
I4	Joiner, Mover und Leaver werden ohne Verlust offener Aufgaben verarbeitet.	Live-Test mit drei Rollenwechseln	[] offen	
I5	Daten sind bei Transport und Speicherung zeitgemäß verschlüsselt.	Architektur- und Kryptografiebeschreibung	[] offen	
I6	Schlüsselverwaltung ist vom Datenspeicher getrennt und kontrolliert.	KMS-Konzept, Rotation, Zuständigkeiten	[] offen	
I7	Mandanten- und Kanzleidaten sind technisch voneinander getrennt.	Tenant-Isolation und Testnachweis	[] offen	
I8	Sicherheitsrelevante Aktionen sind manipulationsgeschützt protokolliert.	Audit-Log-Spezifikation und Aufbewahrung	[] offen	

3. Entwicklung, Schwachstellen und Vorfälle

ID	Prüfungsausschuss	Erwarteter Nachweis / Test	Status	Owner
S1	Ein unabhängiger Penetrationstest deckt den angebotenen Produktumfang ab.	Management Summary, Datum, Scope, Status	☐ offen	
S2	Kritische Befunde haben definierte Behebungsfristen.	Vulnerability-SLA und Beispieltracking	☐ offen	
S3	Abhängigkeiten und Komponenten werden auf Schwachstellen überwacht.	SCA/SBOM-Prozess oder gleichwertiger Nachweis	☐ offen	
S4	Es gibt einen erreichbaren Responsible-Disclosure-Prozess.	Security.txt oder Meldekanal und Ablauf	☐ offen	
S5	Sicherheitsupdates werden getestet und kontrolliert ausgerollt.	Patchprozess, Frequenz, Notfallverfahren	☐ offen	
S6	Vorfälle werden erkannt, eingestuft, eingedämmt und nachbereitet.	Incident-Response-Plan und Übungsnachweis	☐ offen	
S7	Die Kanzlei wird innerhalb einer verbindlichen Frist informiert.	Vertragsfrist, Inhalt und Kommunikationsweg	☐ offen	
S8	Forensische Daten und Ansprechpartner stehen im Ernstfall bereit.	Logumfang, Aufbewahrung, Eskalationsmatrix	☐ offen	

4. Backup, Verfügbarkeit und Wiederanlauf

ID	Prüfungsausschuss	Erwarteter Nachweis / Test	Status	Owner
B1	Backups sind vom Produktivsystem getrennt und gegen Veränderung geschützt.	Backup-Architektur und Zugriffskonzept	[] offen	
B2	Verschlüsselung von Backups nutzt ein zeitgemäßes Verfahren.	Kryptografiebeschreibung und Schlüsselprozess	[] offen	
B3	RPO und RTO sind definiert, messbar und zum Kanzleibetrieb passend.	SLA, Messmethode und Statusbericht	[] offen	
B4	Wiederherstellungen werden regelmäßig vollständig getestet.	Letzter Restore-Test mit Ergebnis	[] offen	
B5	Notbetrieb für Fristen, Aktenzugriff und Kommunikation ist beschrieben.	Business-Continuity-Plan	[] offen	
B6	Statusseite und Eskalation funktionieren auch bei Totalausfall.	Externer Kommunikationskanal und Kontaktliste	[] offen	

5. Vertrag und Leistungsänderungen

ID	Prüfungsausschuss	Erwarteter Nachweis / Text	Status	Owner
V1	Leistung, enthaltene Module und Limits sind eindeutig beschrieben.	Leistungsbeschreibung und Angebotsanlage	☐ offen	
V2	Verfügbarkeit und Wartungsfenster haben eine klare Messmethode.	SLA mit Ausschlüssen und Service Credits	☐ offen	
V3	Supportprioritäten bilden fristkritische Kanzleifälle ab.	Prioritätsmatrix und Reaktionszeiten	☐ offen	
V4	API, Integrationen und Export sind nicht nur unverbindliche Roadmap.	Vertragliche Leistungszusage	☐ offen	
V5	Wesentliche Funktionsänderungen werden angekündigt und dokumentiert.	Change-Klausel und Releaseprozess	☐ offen	
V6	Preisanpassungen, Zusatzkosten und Speicherstaffeln sind kalkulierbar.	Preisblatt und Anpassungsformel	☐ offen	
V7	Change of Control löst Informations- und gegebenenfalls Kündigungsrechte aus.	Vertragsklausel	☐ offen	
V8	Haftung und Versicherung passen zu realistischen Schadensbildern.	Haftungsklausel und Versicherungsnachweis	☐ offen	

6. Datenexport und Exit

ID	Prämissen	Erwarteter Nachweis / Test	Status	Owner
E1	Dokumente werden im Originalformat samt Versionen exportiert.	Probeexport mit Hash-/Vollständigkeitsprüfung	☐ offen	
E2	E-Mails enthalten Anhänge und Headerinformationen.	Probeexport und Importtest	☐ offen	
E3	Aktenstruktur, Beteiligte, Aufgaben, Fristen und Notizen bleiben erhalten.	Datenmodell und Mappingdatei	☐ offen	
E4	Abrechnungs-, Zeit- und Buchungsdaten sind maschinenlesbar.	Formatspezifikation und Beispieldatei	☐ offen	
E5	Audit- und Änderungsprotokolle sind im erforderlichen Umfang enthalten.	Logexport und Dokumentation	☐ offen	
E6	Ein Gesamtexport ist während der Vertragslaufzeit testbar.	Vertragliches Testrecht und durchgeführter Test	☐ offen	
E7	Dauer, Kosten und Unterstützung des Exits sind vorab festgelegt.	Exit-Anlage mit Tagessätzen und Fristen	☐ offen	
E8	Übergangsbetrieb ist lange genug und lesend nutzbar.	Transition Service Agreement	☐ offen	
E9	Produktivdaten, Backups und Supportkopien werden definiert gelöscht.	Löschkonzept und Fristen	☐ offen	
E10	Die Löschung wird schriftlich bestätigt und ist prüfbar.	Löschbestätigung und Verantwortlicher	☐ offen	

7. Zusätzliche Prüfung für KI-Funktionen

ID	Prüfung	Erwarteter Nachweis / Test	Status	Owner
A1	Basismodell, Betreiber und Modellregion sind bekannt.	Systembeschreibung und Datenfluss	[] offen	
A2	Training mit Kanzleidata ist vertraglich ausgeschlossen oder kontrolliert.	Vertrag und Produktkonfiguration	[] offen	
A3	Prompts, Dateien, Ergebnisse und Logs haben definierte Speicherfristen.	Retention-Matrix	[] offen	
A4	Mandats- und Mandantenrestriktionen bleiben technisch wirksam.	Live-Test mit gesperrtem Mandat	[] offen	
A5	Ausgaben zeigen Quellen oder erlauben eine belastbare Nachprüfung.	Szenariotest mit Referenzdokumenten	[] offen	
A6	Modell- und Funktionsänderungen lösen eine kontrollierte Neubewertung aus.	Change-Prozess und Versionsprotokoll	[] offen	
A7	Automatisierte Aktionen haben Freigaben, Limits und Abbruchwege.	Workflow- und Kontrollbeschreibung	[] offen	
A8	Fehler, Beschwerden und Korrekturen werden nachvollziehbar erfasst.	Incident-/Quality-Log	[] offen	

8. Freigabeentscheidung

Produkt / Anbieter: _____

Entscheidungsfeld	Status	Begründung, Auflage, Owner und Termin
Ausschlusskriterien	☐ erfüllt ☐ verletzt ☐ Ausnahme dokumentiert	
Security Evidence Pack	☐ vollständig ☐ teilweise ☐ nicht ausreichend	
Vertragliche Restpunkte	☐ keine ☐ mit Frist und Owner ☐ entscheidungskritisch	
Probeexport	☐ bestanden ☐ mit Auflagen ☐ nicht bestanden	
Gesamtentscheidung	☐ Go ☐ Go mit Auflagen ☐ No-Go ☐ vertragt	

Quellen und Vertiefung

BRAK-Leitfaden: https://www.brak.de/fileadmin/service/publikationen/Handlungshinweise/BRAK_Leitfaden_mit_Hinweisen_zum_KI-Einsatz_Stand_12_2024.pdf

BSI Cloud-Auswahlcheckliste: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-checkliste-auswahl-cloud-dienst.pdf>

CCC-Analyse: <https://www.ccc.de/de/updates/2026/kanzleisoftware-in-der-cloud-lasst-daten-regnen>

Hinweis: Diese Unterlage strukturiert die Prüfung. Sie ersetzt keine rechtliche, datenschutzrechtliche oder technische Einzelfallberatung.