

Anhang 2 – Glossar

Akte: Strukturierte Zusammenfassung von Dokumenten und zugehörigen Metadaten zu einem fachlichen Objekt (z. B. Vertrag, Unternehmen, Person).

API (Application Programming Interface): Technische Schnittstelle, über die Systeme standardisiert Daten austauschen oder Funktionen gegenseitig aufrufen können.

Audit-Trail: Lückenlose, nachvollziehbare Protokollierung aller wichtigen Änderungen und Aktionen im System (z. B. wer was wann geändert hat).

AVV (Auftragsverarbeitungsvertrag): Vertrag, der regelt, wie ein Dienstleister personenbezogene Daten im Auftrag verarbeiten darf.

BPMN (Business Process Model and Notation): Standardisierte Darstellungsform, um Abläufe und Prozesse grafisch zu beschreiben.

Check-in / Check-out: Verfahren zur kontrollierten Bearbeitung von Dokumenten. Beim „Check-out“ wird ein Dokument zur Bearbeitung reserviert, beim „Check-in“ wieder eingecheckt und als neue Version gespeichert.

Cold Storage / Hot Storage: Speicherklassen: Hot = schnell/teurer für häufig genutzte Daten; Cold = langsamer/günstiger für selten genutzte Daten (z. B. Archive).

Compliance: Einhaltung von gesetzlichen, regulatorischen und internen Vorgaben.

Commvault Backup & Recovery: Backup-/Wiederherstellungssoftware, die Daten regelmäßig sichert und bei Bedarf zurückspielen kann (Restore).

Conditional Access: Zugriffsregeln für Anmeldungen, z. B. nur von bestimmten Geräten/Standorten oder nur mit MFA; blockiert riskante Logins.

Confidential Computing: Sicherheitsansatz, bei dem Daten nicht nur gespeichert und übertragen, sondern auch während der Verarbeitung besonders geschützt werden.

CSV (Comma Separated Values): Tabellenbasiertes Textformat mit Komma-getrennten Werten für den Datenaustausch, insbesondere für Excel.

Dashboard: Übersichtsseite mit wichtigen Kennzahlen, Statusinformationen oder Auswertungen auf einen Blick.

Dead-Letter-Queue (DLQ): Auffang-Warteschlange für fehlgeschlagene Nachrichten/Jobs; ermöglicht sichere Nachbearbeitung ohne Datenverlust.

Deployment: Geregelter Bereitstellung von Konfigurationen, Anpassungen oder neuen Funktionen in einer Systemumgebung.

DMS (Dokumentenmanagementsystem): System zur strukturierten Verwaltung von Dokumenten, Akten und zugehörigen Informationen über ihren gesamten Lebenszyklus hinweg.

DoD (Definition of Done): Abnahmekriterium für Meilensteine/Arbeitspakete – legt fest, wann etwas als „fertig“ gilt.

Drill-Down: Möglichkeit, aus einer Übersicht schrittweise in detailliertere Informationen zu wechseln.

DSGVO: Datenschutz-Grundverordnung, zum Schutz personenbezogener Daten.

Entra ID / SSO: Microsoft-Dienst für Identitäten/Anmeldung (früher „Azure AD“). SSO = einmal anmelden, mehrere Systeme nutzen.

ERP-System (Enterprise Resource Planning): Zentrales Softwaresystem zur Unterstützung und Verwaltung von Geschäftsprozessen und Stammdaten in einer Organisation.

ESS (EVA Service Schicht): Webservice-/Schnittstellschicht von EVA, über die andere Systeme (z. B. DMS) Daten abfragen oder übergeben können.

EVA (Erweiterte Verwaltungsanwendung): In diesem Lastenheft das fachlich führende Verwaltungssystem/Stammdatensystem der IHK, aus dem bestimmte Daten und Kontexte für das DMS bereitgestellt werden.

Facettierte Suche: Suchfunktion, bei der Ergebnisse zusätzlich über auswählbare Filter (z. B. Dokumenttyp, Datum oder Status) eingegrenzt werden können.

Failover: Automatischer Wechsel auf ein Ersatzsystem oder eine Ausweichkomponente, wenn der reguläre Betrieb ausfällt.

GoBD: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff.

Governance: Verbindliche Regeln, Zuständigkeiten und Kontrollmechanismen für den geordneten Betrieb und die Weiterentwicklung eines Systems.

Graph API: Microsoft Schnittstelle, um auf M365/Entra Daten und Funktionen zuzugreifen (z. B. Nutzer, Gruppen, Mail, Teams/SharePoint – je nach Freigabe).

Hardening: Technische Absicherung eines Systems durch gezielte Sicherheitsmaßnahmen, um Angriffsflächen zu verringern.

HSTS (HTTP Strict Transport Security): Browser erzwingen verschlüsselte Verbindungen (HTTPS) und verhindern unsichere Umleitungen.

Hybridbetrieb / Hybridmodell: Betriebsform, bei der Teile einer Lösung lokal und andere Teile in der Cloud betrieben werden.

Indexierung: Aufbereitung von Dokumentinhalten und Metadaten, damit sie über die Suche schnell gefunden werden können. Re-Indexierung: Erneute Erstellung oder Aktualisierung des Suchindex, z. B. nach Änderungen an Dokumenten oder Suchregeln.

Instanzstabilität: Eigenschaft eines Systems, laufende Prozesse oder Vorgänge auch bei Änderungen an Konfigurationen oder Workflows zuverlässig weiterzuführen.

JSON (Javascript Object Notation): Strukturiertes Textformat für Systeme/APIs.

Klassifizierungs-Queue: Definierte Bearbeitungsliste für Dokumente, die nicht automatisch oder nicht eindeutig zugeordnet werden konnten.

Kontextzugriff / kontextbezogener Zugriff: Direkter Zugriff auf Dokumente oder Akten aus dem fachlichen Zusammenhang heraus, z. B. aus einem Fachverfahren oder einer bestimmten Akte.

KPI (Key Performance Indicator): Messgröße, mit der Leistung oder Qualität nachgewiesen wird (z. B. Antwortzeit).

KVM / Proxmox: KVM = Virtualisierungstechnologie (führt virtuelle Maschinen aus); Proxmox = Plattform zur Verwaltung von Virtualisierung und Infrastruktur.

LDAP / AD (Active Directory): LDAP ist ein Standard-Protokoll für Verzeichnisdienste; AD ist Microsofts Verzeichnisdienst für Benutzer/Gruppen.

Low-Code / No-Code: Methoden, mit denen Prozesse, Masken oder Regeln mit wenig oder ganz ohne Programmierung angepasst werden können.

Mandantenfähigkeit: Fähigkeit eines Systems, mehrere organisatorisch getrennte Bereiche oder Kunden innerhalb derselben Lösung sauber voneinander getrennt zu verwalten.

Metadaten: Strukturierte Zusatzinformationen zu einem Dokument oder einer Akte, z. B. Dokumenttyp, Datum, Vertragsart oder verantwortliche Stelle.

Metadatenmodell: Festgelegte Struktur, nach der Metadatenfelder, Pflichtfelder und Auswahlwerte im System definiert sind.

Monitoring: Laufende Überwachung des Systemzustands, der Auslastung und wichtiger Betriebsereignisse.

MFA (Multi-Faktor-Authentifizierung): Sicherheitsverfahren, bei dem zur Anmeldung mehrere Nachweise erforderlich sind, z. B. Passwort und zusätzlicher Bestätigungscode.

NAS / SAN: Speicherarten: NAS = Dateispeicher über Netzwerk (Files/Ordner); SAN = blockbasierter Storage über Netzwerk (z. B. für Datenbanken/VM Disks).

NetApp: Hersteller/Plattform für Storage Systeme (Speicherlösungen), oft für Fileservices, Performance Storage und Datenmanagement genutzt.

OAuth2: Standardverfahren, mit dem Anwendungen zugriffsberechtigt werden, ohne Passwörter weiterzugeben. Stattdessen nutzt man zeitlich begrenzte Tokens, um auf eine API/ressource zuzugreifen (z. B. „App darf Daten lesen“).

OIDC (OpenID Connect): Standard für sichere Anmeldung (SSO) über Token; baut auf OAuth2 auf und liefert Identitätsinformationen.

OCR (Optical Character Recognition): Texterkennung – macht gescannte Seiten durchsuchbar.

On-Prem (On-Premises): Betrieb in der eigenen Infrastruktur des Auftraggebers (im eigenen Rechenzentrum).

OpenAPI / Swagger: Standard und Werkzeuge, um REST-APIs verständlich zu beschreiben, zu testen und zu pflegen.

OTC (Open Telekom Cloud): Vom Auftraggeber genehmigte Cloud-Infrastruktur (Deutschland), in der das DMS betrieben werden darf.

P95 (95. Perzentil): Zeitwert, den 95 % aller gemessenen Aufrufe höchstens erreichen.

Parametrisierung: Anpassung eines Systems über Einstellungen und Parameter, ohne den Programmcode zu verändern.

PDF/A: Spezielles PDF-Format für die langfristige, standardisierte Archivierung elektronischer Dokumente.

Perfect Forward Secrecy (PFS): Eigenschaft moderner Verschlüsselung: Auch wenn ein Schlüssel später bekannt wird, bleiben alte Verbindungen sicher.

Private Cloud: Cloud-Umgebung, die für eine Organisation exklusiv bereitgestellt und kontrolliert betrieben wird.

Release: Geplante Veröffentlichung einer neuen oder geänderten Version einer Software oder Konfiguration.

Release-Fähigkeit: Eigenschaft einer Lösung, Änderungen oder Erweiterungen kontrolliert, wartbar und updatesicher in neue Versionen zu übernehmen.

Release-Management: Geordneter Prozess zur Planung, Freigabe und Einführung neuer Software-Versionen oder Systemänderungen.

Release-Roadmap: Übersicht geplanter Weiterentwicklungen, Versionen und Einführungsschritte über einen bestimmten Zeitraum.

REST-APIs: Web-Schnittstellen (HTTP) mit klaren Regeln (GET/POST/PUT/DELETE) für den automatisierten Datenaustausch.

Revisionssicher / Revisionssicherheit: Eigenschaft von Daten oder Dokumenten, unveränderbar, vollständig und nachvollziehbar gespeichert zu sein, sodass sie auch später als verlässlicher Nachweis dienen können.

Round-Robin: Verteilverfahren, bei dem neue Aufgaben reihum nacheinander an mehrere Personen oder Stellen vergeben werden.

RPO (Recovery Point Objective): Maximal erlaubter Datenverlust im Notfall (z. B. höchstens Daten der letzten 4 Stunden).

RTO (Recovery Time Objective): Maximal erlaubte Wiederherstellungszeit (z. B. System ist innerhalb von 8 Stunden wieder nutzbar).

SaaS (Software as a Service): Bereitstellung einer Software als Dienst über das Internet, ohne dass sie lokal installiert und selbst betrieben werden muss.

SAML 2.0: Standard für die sichere Anmeldung und Authentifizierung zwischen verschiedenen Systemen, häufig für Single Sign-on genutzt.

Schwärzung (Redaktion): Technische Unkenntlichmachung sensibler Inhalte in einer Dokumentkopie, sodass diese Inhalte bei Weitergabe nicht mehr sichtbar oder auslesbar sind.

SIEM-Anbindung: Anschluss an ein Sicherheits-Monitoring-System (Security Information and Event Management), das Ereignisse sammelt, auswertet und alarmiert.

SLA (Service Level Agreement): Vereinbarte Service-Niveaus, z. B. Reaktions-/Lösungszeiten bei Störungen.

Team-Queue: Gemeinsame Aufgaben- oder Bearbeitungsliste eines Teams, aus der berechtigte Personen Vorgänge übernehmen oder bearbeiten können.

Testmigration: Probeweise Durchführung einer Datenübernahme in eine Testumgebung, um Vollständigkeit, Struktur und Qualität vor der echten Migration zu prüfen.

Test / Prod: Getrennte Systemumgebungen – Test zum Prüfen/Abnehmen, Prod (Produktion) für den echten Betrieb.

TOMs (Technische und organisatorische Maßnahmen): Dokumentierte Sicherheitsmaßnahmen (z. B. Zugriffsrechte, Verschlüsselung, Backups).

VDI (Virtuelle Desktop Infrastruktur): Nutzer arbeiten auf einem zentral bereitgestellten virtuellen Arbeitsplatz; Citrix stellt dafür die Zugriffs-/Bereitstellungsplattform.

Versionierung: Nachvollziehbare Verwaltung verschiedener Bearbeitungsstände eines Dokuments oder einer Konfiguration.

Vorgang: Zeitlich und sachlich zusammenhängende Bearbeitungseinheit im Zusammenhang mit einem konkreten fachlichen Anliegen. Ein Vorgang ist regelmäßig einer Akte zugeordnet. Die fachliche Führung erfolgt in der Regel im Fachverfahren; das DMS dient insbesondere der Dokumentation und Nachvollziehbarkeit.

Workflow: Systemgestützt definierter Ablauf von Bearbeitungsschritten, Zuständigkeiten und Entscheidungen. Ad-hoc-Workflow: Kurzfristig ausgelöst, nicht dauerhaft fest definierter Bearbeitungsablauf für einen konkreten Einzelfall.

Workflow-Engine: Technische Komponente eines Systems, die Workflows ausführt, steuert und überwacht.

WORM (Write Once Read Many): Speicherart: einmal schreiben, danach nicht mehr verändern – schützt vor Manipulation (z. B. bei Protokollen).

XJustiz: Standardisiertes Datenformat im Justizumfeld für den strukturierten Austausch von Verfahrensdaten/Dokumenten zwischen Systemen.

Zero-Trust: Sicherheitsprinzip, nach dem keinem Zugriff automatisch vertraut wird; jeder Zugriff muss geprüft und freigegeben werden.