

**Anlage 2 Leistungsbeschreibung
für die Beschaffung eines erweiterten Arznei-
mittelauskunftssystems (umfassendes Preis-
und Produktverzeichnis zu Arzneimitteln und
weiteren Produkten gem. § 31 SGB V)**

Stand: 10.09.2026

Inhaltsverzeichnis

1. Einleitung.....	3
2. Leistungsgegenstand.....	3
3. Zweck der Leistung	3
4. Allgemeine Rahmenbedingungen.....	4
5. Funktionale Anforderungen	4
6. Nicht-funktionale Anforderungen.....	10

1. Einleitung

Der AOK Bundesverband sucht für sich und im Auftrag für die 11 AOKs (Baden-Württemberg, Bayern, Bremen, Hessen, Niedersachsen, NordOst, NordWest, PLUS, Rheinland-Pfalz/Saarland, Rheinland/Hamburg, Sachsen-Anhalt) ein erweitertes Arzneimittelauskunftssystem (umfassendes Preis- und Produktverzeichnis zu Arzneimitteln und weiteren Produkten gem. § 31 SGB V) für die Mitarbeitenden aus den Bereichen Beratung, Abrechnung, Wirtschaftlichkeitsprüfung, Vertragsverhandlung, Controlling und Analyse von Daten mit Arzneimittelbezug zur Erfüllung der gesetzlichen Aufgaben.

2. Leistungsgegenstand

Leistungsgegenstand ist die Überlassung eines erweiterten Arzneimittelauskunftssystems (umfassendes Preis- und Produktverzeichnis zu Arzneimitteln und weiteren Produkten gem. § 31 SGB V) sowie dessen Support und Pflege durch den Auftragnehmer.

3. Zweck der Leistung

3.1. Ziel und Zweck

Ziel ist die Beschaffung einer Softwarelösung, die alle in dieser Leistungsbeschreibung aufgeführten fachlichen Anforderungen erfüllt und eine vollständige, aktuelle und historische Arzneimittelinformation einschließlich Produkt-, Preis-, Vertragsinformationen und Vergleichsfunktionen bereitstellt.

Alle in diesem Dokument beschriebenen Anforderungen sind MUSS-Anforderungen, sofern nicht ausdrücklich anders gekennzeichnet.

3.2. Geltungsbereich

Das Arzneimittelauskunftssystem wird für die Recherche von Arzneimitteln und weiteren Produkten gem. § 31 SGB V sowie Hilfsmitteln benötigt, um eine fachliche und wirtschaftliche Bewertung vorzunehmen sowie bei der Beratung von Versicherten und Vertragspartnern, Verordnungs- und Abrechnungsprüfung, Wirtschaftlichkeitsprüfung, Vertragsvorbereitung, Controlling und Analyse zu unterstützen.

Das System wird von fachlich spezialisierten Anwendern genutzt und basiert auf strukturierten Datenbeständen (mindestens¹, siehe auch Punkt 5 und 6.1). ABDA Lizenzen sind Bestandteil des Auftragsgegenstandes.

¹ ABDA – Bundesvereinigung Deutscher Apothekerverbände e.V. (Spitzenorganisation der Apotheker in Deutschland), IFA – Informationsstelle für Arzneispezialitäten GmbH (Dienstleister für PZN-Zuweisung und Arzneimitteldaten im deutschen Pharmamarkt).

4. Allgemeine Rahmenbedingungen

- Alle angezeigten Informationen müssen datenstandbezogen, konsistent und nachvollziehbar sein.
- Regionale und kassenspezifische Regelungen müssen vollständig berücksichtigt werden.
- Historische Daten müssen abrufbar bleiben.
- Die Software muss für nicht-technische Anwender klar strukturiert und nachvollziehbar bedienbar sein.

5. Funktionale Anforderungen

5.1. Datenstandverwaltung

Das System muss:

- den aktuellen Datenstand standardmäßig anzeigen (siehe auch Punkt 6 Nicht-funktionale Anforderungen),
- den Datenstand frei wählbar machen (Vergangenheit und – sofern vorhanden – Zukunft),
- bei jedem gewählten Datenstand ausschließlich die zugehörigen Daten anzeigen.

5.2. Regionale und kassenspezifische Parametrisierung

Das System muss folgende Parameter zur Einstellung bereitstellen:

- Bundesland,
- Krankenkasse über IK-Nummer ² mit Vorschlagsliste. Diese Einstellungen müssen sich unmittelbar auswirken auf:
 - die Anzeige von Rabattverträge (inkl. Parenteralia),
 - Zuzahlungs- und Mehrkostenregelungen, inkl. deren Höhe
 - Vertrags- und Mietpreise

5.3. Suchfunktion

5.3.1. Schnellsuche

Das System muss eine Schnellsuche bereitstellen mit folgenden Eigenschaften:

- Suche nach PZN³ (auch ohne führende Nullen),

² (IK-Nummer steht für Institutionskennzeichen. Es handelt sich um eine bundesweit eindeutige, neunstellige Zahl zur Identifikation von Leistungserbringern (Ärzte, Apotheken, Krankenhäuser etc.) im deutschen Gesundheitswesen für Abrechnungen mit gesetzlichen Krankenkassen gemäß § 293 SGB V..

^{3,4} PZN steht für Pharmazentralnummer.

- Suche nach Artikelnamen,
- fehlertolerante Suche bei falscher Schreibweise,
- Wildcard-/Jokersuche,
- Ergebnisanzeige als vollständige Trefferliste,
- Hinweis bei nicht gefundener PZN⁴,
- automatischer Wechsel auf den letzten Datenstand mit vorhandener PZN.

5.3.2. Erweiterte Suche

Das System muss eine kombinierbare Suche nach folgenden Kriterien ermöglichen:

- Artikelname, Packungsgröße,
- Anbieter inkl. Anbieternummer,
- Darreichungsform und -struktur,
- Wirkstoffe (mehrere, inkl. Wirkstoffmenge),
- ATC-Code⁵ (amtlich und Weltgesundheitsorganisation),
- Warengruppe, LV-Gruppe⁶, Hilfsmittelnummer (ohne Trennung),
- Indikation,
- Vertriebsstatus,
- Zuzahlungsbefreiung.

Die Eingabe muss möglich sein durch:

- Direkteingabe,
- Teileingabe mit Vorschlagslisten,
- Baumstrukturen (z. B. ATC⁷).

Mehrfachauswahlen müssen unterstützt werden.

Zusätzlich müssen mindestens Filter verfügbar sein:

- Abgabebestimmungen,

Es handelt sich um eine bundeseinheitliche, achtstellige Identifikationsnummer (7 Ziffern + Prüfziffer) für Arzneimittel, apothekenpflichtige Produkte und Medizinprodukte in Deutschland. Sie dient der eindeutigen Kennzeichnung nach Bezeichnung, Darreichungsform, Wirkstoffstärke und Packungsgröße und wird von der IFA (Informationsstelle für Arzneispezialitäten) vergeben.

^{5 7} ATC-Code steht für Anatomisch-Therapeutisch-Chemisches Klassifikationssystem (engl. Anatomical Therapeutic Chemical Classification System). Es ist ein international standardisiertes Klassifikationssystem der WHO zur Zuordnung von Arzneimitteln in 5 Hierarchieebenen:

1. Ebene: Anatomische Hauptgruppe (Buchstabe, z. B. A = Magen-Darm-System)
- 2.–3. Ebene: Therapeutische/pharmakologische Gruppen (Ziffern/Buchstaben)
- 4.–5. Ebene: Chemische/pharmakologische Untergruppen (Buchstaben/Ziffern)

⁶ LV-Gruppe steht im deutschen Pharmamarkt für Leistungsvorgangsgruppe oder Leistungsgruppe – eine Abrechnungsgruppierung von Arzneimitteln nach Wirkstoff, Indikation oder Therapiegebiet für Zwecke der gesetzlichen Krankenversicherung (GKV). Sie dient der standardisierten Vergütung und Statistik ähnlicher Präparate (z. B. LV-Gruppe 1 = Antidiabetika, LV-Gruppe 8 = Antiadiposita).

- Rabattarzneimittel,
- Original/Import,
- Festbetragsarzneimittel,
- Biologika,
- Nutzenbewertungsverfahren,
- Negativliste.

Kann-Anforderung: Suche nach Hinweissätzen.

5.3.3. Internationale Suche

Schnellsuche

Das System muss eine Schnellsuche für Produkte nach Artikelnamen ermöglichen, welche nicht im deutschen Markt verfügbar sind, sondern nur im Ausland (andere Datenbankgrundlage).

- nur für Artikelname
- Das Ergebnis soll eine Ergebnisliste aller Produkte sein.
- es muss die Funktion einer "Jokersuche"/"Wildcard" geben (z. B. *)
- Schreibfehler müssen toleriert werden, das System muss so lange Buchstaben am Ende "abschneiden" bis ein Produkt gefunden wird (bei Suche nach Artikelname)

Ausführliche Suche

Das System muss zusätzlich eine ausführliche Suche mit diversen Filtermöglichkeiten/Auswahlkriterien ermöglichen, um gezielt ausländische Produkte zu finden.

Vergleichende Suche (Äquivalenzsuche)

Das System muss ausgehend von einem ausländischen Arzneimittel die Möglichkeit anbieten die Austauschprodukte mit gleichem Wirkstoff anzeigen zu lassen, um vergleichbare Produkte benennen zu können.

Es muss eine Suche nach folgenden Kriterien möglich sein: Artikelname, ATC-Code (Baumstruktur), Inhaltsstoff und Wirkstärke.

Detailansicht

Das System muss zu einem ausländischen Produkt, sofern das Produkt verfügbar ist, folgende Informationen anzeigen:

- Basisinformationen mit Klassifikation
- Originaldokumente
- Anbieter
- Pharmazeutische Informationen (Inhaltsstoff, Wirkstoffdossier, ATC-Code Klassifikation, Angaben zur Darreichungsform)

In der Ergebnisliste müssen mindestens die nachfolgenden Felder angezeigt werden:

Artikelname, Darreichungsform, Anbieter, Verkehrsfähigkeit, Land, Wirkstoff, ATC-Code.

5.4. Vergleichende Funktionen

Das System muss vergleichende Suchen ausgehend von einem Produkt ermöglichen, mindestens:

- Aut-idem-Suche,
- Äquivalenzsuche mit frei wählbaren Kriterien,
- Äquivalenzsuche gemäß Rahmenvertrag (§ 129 SGB V),
- Festbetragssuche,
- Importsuche,
- Vergleich innerhalb derselben Warengruppe.

Die Ergebnisse müssen:

- preisgünstige Artikel kennzeichnen,
- die Indikationsübereinstimmung anzeigen,
- einen Vergleich zwischen Ausgangs- und Zielprodukt ermöglichen (Inhaltsstoffe, Indikation).

Kann-Anforderung: Vergleich identischer Wirk- und Hilfsstoffe.

5.5. Ergebnisliste

Nach ausgeführten Suchanfragen muss eine Ergebnisliste ausgegeben werden.

- Die Anzahl der Ergebnisse soll nicht limitiert, sondern muss konfigurierbar sein.
- Die angezeigte Ergebnisliste muss (in Abhängigkeit zum eingestellten Kostenträger) mindestens folgende Felder enthalten:
 - PZN,
 - Artikelname,
 - Zuzahlung und Mehrkosten (gesetzlich und kassenspezifisch),
 - Festbetrag,
 - Abgabepreis des pharmazeutischen Unternehmens (ApU),
 - Apothekeneinkaufspreis (AEK),
 - Apothekenverkaufspreis (AVK),
 - Apothekenrabatt,
 - Gesetzliche Herstellerrabatte (einzeln aufgelistet),
 - Kennzeichen Rabattvertrag,
 - Darreichungsform,
 - Menge und Mengeneinheit,
 - Packungsgröße,
 - Pharmazeutischer Unternehmer,
 - Abgaberegulierung (apothekenpflichtig, ...)
 - Verkehrs- und Vertriebsfähigkeit

5.6. Preis- und Vertragsinformationen

5.6.1. Allgemeine Preise

Das System muss mindestens folgende Preisangaben anzeigen:

- Apothekenverkaufspreis (Endpreis für den Patienten in der Apotheke inkl. Zuzahlung), Apotheken-Einkaufspreis (Preis, zu dem die Apotheke das Arzneimittel beim Großhandel kauft), Abgabepreis des pharmazeutischen Unternehmers (Herstellerabgabepreis an Großhandel/Apotheke), Krankenhaus-Einkaufspreis (Einkaufspreis für Krankenhäuser, oft rabattiert), Unverbindliche Preisempfehlung (vom Hersteller empfohlener Verkaufspreis),
- Festbeträge inklusive Festbetragsstufe,
- Zuzahlung und Mehrkosten (gesetzlich und kassenspezifisch),
- Gesetzliche Herstellerrabatte,
- Erstattungsbeträge inkl. Gültigkeit,
- Umsatzsteuer,
- Kennzeichnung Rabattarzneimittel,
- historische Listenpreise (nicht abrechnungsrelevant).

5.6.2. Vertrags- und Mietpreise

Das System muss:

- Filter nach Bundesland und IK unterstützen,
- Einzelverordnung und Sprechstundenbedarf unterscheiden,
- alle gültigen Preisvarianten anzeigen (z. B. Staffelpreise),
- die jeweils geltenden Konditionen eindeutig kennzeichnen,
- Berechnungslogik, Randbedingungen und Erstattungsbedingungen darstellen.

5.6.3. optionale Zusatzmodule (sofern nicht in der Standardlizenz enthalten)

5.6.3.1. Großhandelsangebotspreis und -einkaufspreis

Sofern die Information vorhanden ist, müssen die Rabatte und Angebotspreise der verschiedenen Großhändler/Anbieter je PZN aktuell zum Abfragedatum angezeigt werden. Ergänzend dazu ist die Mindestbestellmenge, der Angebotspreis und der Zeitraum des Angebotes anzuzeigen. Wenn das Abfragedatum verändert wird, müssen auch die Angebotspreise der Vergangenheit sichtbar sein.

5.6.3.2. Hilfstaxenpreise

Ist für ein Produkt ein Preis in der Hilfstaxe für Apotheken⁸ hinterlegt, so muss das System diesen anzeigen (inklusive Historie).

⁸ Fußnote zu Hilfstaxe: Nach § 4 Abs. 3 und § 5 Abs. 4 und 5 der Arzneimittelpreisverordnung können der Deutsche Apothekerverband e. V. (DAV) und der GKV-Spitzenverband abweichend von den Abrechnungsregelungen der Arzneimittelpreisverordnung Vereinbarungen zur Vergütung von in Apotheken hergestellten Rezepturen treffen. Der nach dieser Ermächtigung geschlossene Vertrag über die

5.7. Detailansichten zu Produkten

Zu jedem Produkt muss eine Detailansicht mit mindestens den folgenden Informationen verfügbar sein:

- Basisdaten, Klassifikationen, Historie,
- Information, ob ein Rabattvertrag nach §130a Abs. 8c SGB V besteht
- Preise inklusive Preishistorie,
- pharmakologische Informationen (Inhalt, Interaktionen, Warnhinweise, um auf Kontraindikationen, Risiken, Allergien oder Wechselwirkungen hinzuweisen.),
- Anbieterinformationen inklusive Historie,
- Beratungshinweise (mindestens Teilbarkeit, Sondenapplikation),
- Originaldokumente inklusive Historie (Fachinformation, Packungsbeilage, wenn vorhanden: Roter-Hand-Brief⁹),
- Verordnungsvorgaben und Nutzenbewertung,
- Wirk- und Hilfsstoffe,
- Lagerung, Haltbarkeit,
- Nachfolge- und Vorgängerprodukte.

Alle Inhalte müssen datenstandbezogen abrufbar sein.

5.8. Hilfsmittel

Für Hilfsmittel müssen mindestens folgende Angaben verfügbar sein:

- Preis,
- Einordnung,
- Hilfsmittelpositionsnummer.

5.9. Historie

Das System muss eine Historie bereitstellen für:

- Preise (tabellarisch, mit Zeitangabe),
- gesetzliche Herstellerabschläge (tabellarisch, mit Zeitangabe, exportierbar),
- sonstige Änderungen (z. B. Darreichung, Klassifikation).

Die Preishistorie muss:

- jede Änderung in einer neuen Zeile abbilden,
- mindestens 10 Jahre rückwirkend verfügbar sein.

5.10. Originaldokumente

Das System muss folgende Originaldokumente anzeigen:

- Fachinformationen,
- Packungsbeilagen,

Preisbildung für Stoffe und Zubereitungen aus Stoffen (§§ 4 und 5 der Arzneimittelpreisverordnung), die sogenannte „Hilfstaxe“, enthält Regelungen zur Preisbestimmung

⁹ Es ist ein dringendes Informationsschreiben deutscher pharmazeutischer Unternehmen an Ärzte, Apotheker und andere Heilberufler über neu erkannte Arzneimittelrisiken, Rückrufe fehlerhafter Chargen, Kontraindikationen oder Wechselwirkungen. Die Schreiben werden über das BfArM veröffentlicht und haben hohe Priorität in der Arzneimittelsicherheit.

- Rote-Hand-Briefe.

5.11. Interaktionscheck

Das System muss ausgehend von einem Arzneimittel potentielle Interaktionen mit ausgewählten Arzneimitteln anzeigen, um Interaktionen erkennen zu können.

5.12. Eigene Erfassungen

Das System muss eine Funktion bereitstellen, um eigene Informationen zu Artikeln zu erfassen und speichern zu können. Diese eigenen Erfassungen sind bei Aufruf des Artikels anzuzeigen.

5.13. Änderungssuche

Übersicht zu PZNs mit Änderungen ggü. dem vorherigen Stand (z.B. Anzeige der Preisangaben mit altem und neuem Wert, Änderung ATC Code etc.) gegenüber dem vorherigen Stand

5.14. Anzeige Rabattverträge für Zubereitungen

Das System muss anzeigen, ob ein Rabattvertrag nach §130a Abs. 8c SGB V besteht

6. Nicht-funktionale Anforderungen

6.1. Datenbasis und deren Aktualisierung

- Die 14-tägige Bereitstellung des ABDA-Artikelstammes sowie eventuell weiterer genutzter Basisdaten ist spätestens am Gültigkeitstag in der Anwendung sicherzustellen.

6.2. Verfügbarkeit der Anwendung

Die SaaS-Lösung muss eine **hohe Verfügbarkeit** gewährleisten, um einen unterbrechungsfreien Betrieb sicherzustellen. Hierfür gilt ein **Service-Level-Agreement (SLA) von mindestens 99 % Verfügbarkeit**, gemessen über einen Zeitraum von **12 Monaten**. Die Verfügbarkeit wird als der **Anteil der Zeit definiert, in der die Anwendung für die Nutzer zugänglich und funktionsfähig ist**, abzüglich geplanter Wartungsfenster. Als **Ausfall** gilt jede **ungeplante Unterbrechung des Dienstes**, bei der die Anwendung für Nutzer nicht oder nur eingeschränkt nutzbar ist. **Geplante Wartungsarbeiten** (z. B. Software-Updates, Sicherheits-Patches) sind von dieser Berechnung ausgenommen, sofern sie **außerhalb der Geschäftszeiten (18–08:00 Uhr MEZ)** durchgeführt werden und der Auftragnehmer die Nutzer **mindestens 48 Stunden im Voraus** über die Wartung informiert.

Der Auftragnehmer muss sicherstellen, dass die **Kernfunktionen der Anwendung** während der Betriebszeit **durchgehend verfügbar** sind. Hierzu zählen insbesondere:

- **Zugang zur Benutzeroberfläche** (Login, Navigation, Hauptfunktionen),
- **Datenabfrage und -bearbeitung** (Lese- und Schreiboperationen),
- **Datei-Downloads.**

Zur **Überwachung der Verfügbarkeit** muss der Auftragnehmer ein **Echtzeit-Monitoring-System** einsetzen, das **Ausfälle automatisch erkennt und dokumentiert**. Die **historischen Verfügbarkeitsberichte der letzten 12 Monate** sind vom Auftragnehmer auf Aufforderung der Auftraggeberinnen nach Vertragsschluss vorzulegen, um die Einhaltung des SLA nachzuweisen.

Im Falle eines **Verstoßes gegen das SLA** (d. h. bei Unterschreitung der 99 %-Verfügbarkeit) hat der Auftragnehmer **Kompensationsregelungen** anzuwenden. Diese können beispielsweise **Gutschriften auf die monatlichen Nutzungsgebühren** umfassen, die sich an der Dauer und Schwere des Ausfalls orientieren. Die genauen Konditionen sind im Kriterienkatalog für Cloudleistungen festgehalten.

6.3. Performance und Skalierbarkeit

Die SaaS-Lösung muss eine hohe Performance und Skalierbarkeit gewährleisten, um den Anforderungen eines unternehmensweiten Einsatzes gerecht zu werden. Hierfür gelten folgende Vorgaben:

Für die Benutzeroberfläche gilt, dass mindestens 95 % aller Seitenaufrufe innerhalb von 2 Sekunden vollständig geladen sein müssen. Zur Sicherstellung dieser Performance ist der Einsatz von Content Delivery Networks (CDN) sowie In-Memory-Caching-Mechanismen wie Redis oder Memcached erforderlich.

Der Auftragnehmer hat die Einhaltung dieser Anforderungen durch Lasttests mit mindestens 1.000 gleichzeitigen Nutzern nachzuweisen und die entsprechenden Testprotokolle oder Benchmark-Berichte auf Aufforderung der Auftraggeberinnen nach Vertragsschluss vorzulegen.

Die Datenbank-Performance muss so ausgelegt sein, dass die Lösung mindestens 1.000 Transaktionen pro Sekunde ohne spürbare Einbußen verarbeiten kann. Hierfür ist ein Datenbank-Benchmark-Test unter Last durchzuführen, dessen Ergebnisse zu dokumentieren sind.

Die Skalierbarkeit der Lösung muss sicherstellen, dass sie mindestens 10.000 gleichzeitige Nutzer ohne Performance-Einbußen unterstützt. Die Lösung muss automatisch skalierbar sein, sowohl horizontal (durch Hinzufügen weiterer Server-Instanzen) als auch vertikal (durch Erhöhung der Ressourcen pro Instanz, z. B. CPU, RAM). Die Skalierungsmechanismen müssen in der Architektur-Dokumentation beschrieben werden. Zudem ist ein Skalierungstest mit schrittweiser Steigerung der Nutzerzahl bis auf 10.000 durchzuführen und die Ergebnisse zu dokumentieren.

6.4. Benutzerfreundlichkeit

Die SaaS-Lösung muss **benutzerfreundlich** gestaltet sein und den Anforderungen an **Barrierefreiheit, Sprachunterstützung, mobile Optimierung sowie Dokumentation und Schulung** gerecht werden.

Zur **Barrierefreiheit** ist die Einhaltung des **WCAG 2.1 AA-Standards** (Web Content Accessibility Guidelines) erforderlich. Dies umfasst unter anderem die **Unterstützung von Screenreadern** für blinde oder sehbehinderte Nutzer, die **Tastaturbedienbarkeit** für Nutzer, die keine Maus verwenden können, sowie **ausreichende Kontrastverhältnisse** (mindestens 4,5:1 für normale Texte und 3:1 für große Texte). Zudem müssen **alternative**

Texte für Bilder und Grafiken bereitgestellt werden. Der Auftragnehmer hat die Einhaltung dieser Anforderungen durch einen **WCAG-Testbericht eines zertifizierten Prüfers** oder eine **Selbsterklärung mit Testprotokollen** nachzuweisen.

Die SaaS-Lösung muss in **Deutsch** verfügbar sein. Dies betrifft die **Benutzeroberfläche (UI)**, **Fehlermeldungen und Systemhinweise** sowie die **Dokumentation** (Handbücher, FAQs, Tutorials).

Die Lösung muss **vollständig responsiv** sein und auf allen gängigen Geräten wie **Desktop-PCs, Notebooks, Tablets** optimal dargestellt werden. Hierfür ist eine **Anpassung an Bildschirmgrößen bis 1920 px oder höher** erforderlich.

Der Auftragnehmer muss **kostenlose Schulungsunterlagen** bereitstellen. Diese müssen mindestens **Grundlagen der Nutzung, erweiterte Funktionen sowie Administration und Konfiguration** abdecken. Zudem ist eine **umfassende Online-Hilfe** bereitzustellen, die **FAQs zu häufigen Problemen, Schritt-für-Schritt-Anleitungen für alle Hauptfunktionen** umfasst. Die Schulungsunterlagen und die Online-Hilfe müssen in **Deutsch** verfügbar sein. Der Auftragnehmer hat **Beispiel-Dokumentationen** auf Aufforderung der Auftraggeberinnen nach Vertragsschluss vorzulegen.

6.5. Browser-Unterstützung

Die SaaS-Lösung **muss** mit den folgenden Browsern **vollständig kompatibel** sein und alle Funktionen ohne Einschränkungen bereitstellen: **Microsoft Edge** (aktuelle Version sowie die zwei vorherigen Major-Releases) und **Mozilla Firefox** (aktuelle Version sowie die zwei vorherigen Major-Releases).

Alle Funktionen der SaaS-Lösung müssen in diesen Browsern **fehlerfrei** funktionieren. Dies umfasst insbesondere die **Benutzeroberfläche (UI)**, **Formulare und Eingabefelder**, **Datenvisualisierungen (z. B. Diagramme, Tabellen)**, **Datei-Uploads/Downloads sowie die Integration mit externen Systemen (z. B. Single Sign-On, APIs)**. Die Performance der SaaS-Lösung darf in den genannten Browsern **nicht signifikant** von den in den Performance-Anforderungen festgelegten Werten abweichen. Der Auftragnehmer hat die Einhaltung dieser Anforderungen durch **Testprotokolle**, die die Funktionalität und Performance in Edge und Firefox bestätigen, nachzuweisen.

Zusätzlich muss der Auftragnehmer sicherstellen, dass die SaaS-Lösung **innerhalb von 30 Tagen** nach der Veröffentlichung eines neuen Major-Releases von Edge oder Firefox **vollständig kompatibel** bleibt. Hierfür ist eine **Kompatibilitätsmatrix** vorzulegen, die die Unterstützung der Browser-Versionen dokumentiert.

Falls ein Nutzer einen **nicht unterstützten Browser** verwendet, muss die SaaS-Lösung eine **klare Warnmeldung** anzeigen. Diese Warnmeldung muss den Nutzer über die **Nicht-Unterstützung** informieren, eine **Liste der unterstützten Browser** bereitstellen und einen **Link zum Download** der unterstützten Browser enthalten.

6.6. Support - Service Level Agreements

Support der Anwendung während der Geschäftszeiten

Der Auftragnehmer muss einen **professionellen Support** für die SaaS-Lösung während der **Geschäftszeiten des Auftraggebers von 08:00 Uhr bis 18:00 Uhr MEZ**

(Montag bis Freitag, an Werktagen in Deutschland) sicherstellen. In diesem Zeitraum muss der Support **vollständig erreichbar** sein und **alle Anfragen zeitnah bearbeiten**.

Der Support umfasst mindestens folgende **Kontaktmöglichkeiten**:

- **Telefonischer Support** (mit einer **kostenfreien Hotline oder Festnetznummer**),
- **E-Mail-Support** (mit einer dedizierten Support-Adresse) sowie
- **Ticket-Support**
- Für die **Bearbeitung von Support-Anfragen** gelten folgende **Reaktionszeiten**:
 - **Priorität 1 (kritische Störungen, z. B. vollständiger Ausfall der Anwendung oder schwerwiegende Sicherheitslücken)**: Reaktionszeit innerhalb von **1 Stunde**, Beginn der Fehlerbehebung **unverzüglich**.
 - **Priorität 2 (erhebliche Beeinträchtigungen, z. B. eingeschränkte Funktionalität oder Performance-Probleme)**: Reaktionszeit innerhalb von **4 Stunden**.
 - **Priorität 3 (geringfügige Probleme, z. B. kleine Fehler oder Fragen zur Bedienung)**: Reaktionszeit innerhalb von **8 Stunden**.

Der Support muss **in deutscher Sprache** erfolgen, um eine reibungslose Kommunikation mit den Nutzern des Auftraggebers zu gewährleisten. Support-Mitarbeiter müssen **technisch kompetent** sein und über **ausreichende Kenntnisse der SaaS-Lösung** verfügen, um Anfragen direkt bearbeiten zu können.

Der Auftragnehmer hat sicherzustellen, dass **alle Support-Anfragen dokumentiert** werden. Hierzu gehört die **Erfassung von Anfragedatum, Priorität, Bearbeitungsstatus und Lösung**. Der Auftraggeber muss **Zugang zu einem Ticket-System** erhalten, in dem er den **Status seiner Anfragen einsehen und nachverfolgen** kann. Zudem sind **monatliche Support-Berichte** vorzulegen, die **Anzahl, Art und Bearbeitungsdauer der Anfragen** zusammenfassen.

Für den Fall, dass eine Support-Anfrage **nicht innerhalb der vereinbarten Reaktionszeit bearbeitet** werden kann, muss der Auftragnehmer den Auftraggeber **proaktiv informieren** und eine **vorläufige Einschätzung der Bearbeitungsdauer** liefern.

Zusätzlich muss der Auftragnehmer einen **dedizierten Ansprechpartner** für den Auftraggeber benennen, der als **Single Point of Contact (SPoC)** für alle Support-Angelegenheiten fungiert. Dieser Ansprechpartner ist für die **Koordination der Support-Aktivitäten** verantwortlich und steht dem Auftraggeber für **regelmäßige Abstimmungen** zur Verfügung.

6.7. Webanwendung

- Die Anwendung soll eine Webanwendung sein.
- Es muss eine aktuelle Server-/Web-Technologie, die dem aktuellen Stand der Technik entspricht, eingesetzt werden.

6.8. IT-Sicherheit

- Es dürfen in der SaaS-Lösung nur kryptographischen Verfahren, Kommunikationsprotokolle, Schlüssellängen und Cipher Suites verwendet werden, die nicht als gebrochen oder unsicher gelten.
- Die Kommunikation muss über TLS 1.2 (mit restriktiver Cipher-Auswahl) oder vorzugsweise TLS 1.3 erfolgen. Veraltete und unsichere Protokollversionen (SSLv2, SSLv3, TLS 1.0, TLS 1.1) sind in der SaaS-Lösung zu deaktivieren.
- Es dürfen nur sichere Cipher Suites eingesetzt werden. Die Konfiguration muss zwingend Forward Secrecy (z. B. mittels ECDHE) unterstützen, um bei einem späteren Kompromittieren des privaten Schlüssels die Vertraulichkeit vergangener Kommunikationen zu gewährleisten.
- Bevorzugt werden AEAD-Cipher (z. B. AES-GCM, ChaCha20-Poly1305). Unsichere Algorithmen (z. B. RC4, DES, 3DES, CBC-Mode-Cipher ohne MAC-then-Encrypt-Schutz) sind zwingend zu deaktivieren.
- Die TLS-Konfiguration muss den aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), insbesondere der BSI TR-03116 (Sichere TLS-Konfiguration) und der BSI TR-02102 (Kryptographische Verfahren), entsprechen
 - Die für die Webanwendung eingesetzten Zertifikate müssen gültig und durch die Auftraggeber verifizierbar sein. Die verwendeten Zertifikate müssen
 - ausreichende Schlüssellängen aufweisen (z. B. RSA $\geq$ 2048 Bit, besser 3072/4096 Bit oder ECC $\geq$ 256 Bit),
 - mit sicheren Hash-Algorithmen signiert sein (mindestens SHA-256),
 - die Zertifizierungsstellen (CAs) müssen von einer öffentlich vertrauenswürdigen vor dem Einsatz der Zertifikate Certificate Authority (CA) ausgestellt sein, deren Root-Zertifikate in den gängigen Trust Stores (z. B. Microsoft, Mozilla, Apple) enthalten sind.
 - Der Auftragnehmer muss auf Verlangen nachweisen, dass die Endpunkte der SaaS-Lösung die genannten Anforderungen erfüllen. Der Auftraggeber behält sich vor, die Konfiguration der SaaS-Endpunkte (FQDNs) mittels etablierter, standardisierter Testverfahren (z. B. Qualys SSL Labs Server Test, testssl.sh oder interne Security-Scanner) zu überprüfen. Es wird eine Bewertung von mindestens "Grade A" (oder äquivalent) vorausgesetzt.

6.8.1. Cloud-Sicherheit, Zertifizierungen und Rechenzentrumsbetrieb

Der Auftragnehmer muss nachweisen, dass die SaaS-Lösung in einem Rechenzentrum betrieben wird, das über die gesamte Vertragslaufzeit mindestens nach ISO/IEC 27001 oder dem BSI C5-Kriterienkatalog (Cloud Computing Compliance Controls Catalogue) zertifiziert ist.

Der Auftragnehmer gewährleistet eine strikte logische Mandantentrennung (Multi-Tenancy-Security), sodass keine Daten oder Metadaten zwischen verschiedenen Kunden (Mandanten) einsehbar oder zugänglich sind.

6.8.2. Patch- und Schwachstellenmanagement

Der Auftragnehmer betreibt während der gesamten Vertragslaufzeit ein dokumentiertes Patch-, Änderungs- und Schwachstellenmanagement für die gesamte SaaS-Lösung (inklusive aller zugrundeliegenden Bibliotheken, Container und Betriebssysteme).

Schwachstellen sind mindestens anhand des Common Vulnerability Scoring System (CVSS) oder eines gleichwertigen, anerkannten Bewertungsverfahrens zu klassifizieren.

Durchgeführte Schwachstellenscans sowie die Identifikation und Behandlung von Schwachstellen müssen dokumentiert und im Zeitverlauf für die gesamte Vertragslaufzeit inkl. etwaiger Vertragsverlängerungen nachgewiesen werden.

Der Auftragnehmer muss für alle Schwachstellen mit einem CVSS-Score ≥ 7 unverzüglich, spätestens jedoch innerhalb von 7 Tagen, eine Fehlerkorrektur bereitstellen. Der Auftragnehmer muss für alle anderen Schwachstellen, welche die Integrität oder Vertraulichkeit der Datenverarbeitung betreffen, spätestens binnen 28 Tagen eine Fehlerkorrektur bereitstellen. Ausgenommen davon sind Schwachstellen, welche auf Grund der vereinbarten Spezifikation unvermeidlich sind.

Schwachstellen mit CVSS-Bewertung ≥ 4 („mittel“) MÜSSEN spätestens 4 Wochen nach öffentlichem Bekanntwerden oder Bekanntgabe durch den Hersteller so behandelt sein, dass eine Ausnutzung nicht mehr möglich ist.

Schwachstellen mit CVSS-Bewertung ≥ 7 („hoch“) MÜSSEN spätestens 3 Tage nach öffentlichem Bekanntwerden oder Bekanntgabe durch den Hersteller so behandelt sein, dass eine Ausnutzung nicht mehr möglich ist.

Sobald eine Schwachstelle mit einem CVSS-Basiswert von mindestens 9 („kritisch“) öffentlich bekannt wird und ein hoher Temporal Score (bspw. Exploit-Code verfügbar, Patch nicht verfügbar) oder ein hoher Environmental Score (bspw. System am Internet exponiert, sensible Daten verarbeitend) vorliegt, muss unverzüglich – spätestens innerhalb von 1 Stunde – eine Risikobewertung durchgeführt werden. In diese Bewertung sind einzubeziehen:

- Die konkrete Erreichbarkeit des Systems (bspw. Erreichbarkeit aus dem Internet, Netzsegmentierung),
- Vorhandene technische Schutzmaßnahmen (bspw. WAF, IDS/IPS, Firewalls),
- Der EPSS-Score (Exploit Prediction Scoring System) als Indikator für Ausnutzungswahrscheinlichkeit,
- Geschäfts- und regulatorische Kritikalität des betroffenen Systems.

Basierend auf dieser Risikobewertung müssen unverzüglich geeignete Sofortmaßnahmen ergriffen werden, um eine Ausnutzung der Schwachstelle zu verhindern oder zumindest signifikant zu erschweren. Dazu zählen insbesondere:

- Temporäre Deaktivierung betroffener Funktionen oder Dienste,
- Netzwerksegmentierung oder Zugriffsbeschränkung,
- Aktivierung verstärkten Monitorings,
- Anwendung dokumentierter Workarounds.

Diese Sofortmaßnahmen müssen spätestens innerhalb von 3 Stunden nach Bekanntwerden der Schwachstelle vollständig umgesetzt sein.

Sobald ein offizieller Patch oder Sicherheitsupdate des Herstellers verfügbar ist, muss dessen Einspielung unverzüglich geplant und priorisiert werden. Die Verfügbarkeit neuer Patches muss mindestens alle 12 h (bzw. mehrfach täglich in kritischen Umgebungen) geprüft werden.

Ist die unmittelbare Installation aus betrieblichen Gründen (bspw. fehlendes Wartungsfenster, Testaufwand) nicht innerhalb von 24 Stunden (bei internetexponierten oder besonders schutzwürdigen Systemen) bzw. 72 Stunden (bei internen, abgeschotteten Systemen) möglich, so müssen:

- die bereits ergriffenen Risikominderungsmaßnahmen dokumentiert und
- deren Wirksamkeit fortlaufend überprüft werden und
- eine formale Risikoakzeptanz durch die zuständigen Stellen (bspw. Informationssicherheitsbeauftragter, Auftraggeber) eingeholt werden.

Die vollständige Behebung (bspw. Patch-Einspielung, Architekturänderung) muss innerhalb der genannten Fristen (24/72 Stunden) erfolgen, es sei denn, eine begründete Ausnahme wurde dokumentiert und von den Auftraggebern akzeptiert.

Der Auftragnehmer muss den Auftraggeber unverzüglich über bekannt gewordene, die Lösung betreffende Schwachstellen informieren. Die Information muss mindestens enthalten: Beschreibung, betroffene Komponenten, CVE-Nummer, CVSS-Basiswert, Risikobewertung, Auswirkungen, empfohlene Gegenmaßnahmen und Zeitplan für die Bereitstellung eines Fixes.

6.8.3. Sicherheitsupdates und Versionsmanagement

Sicherheitsupdates sind während der gesamten Vertragslaufzeit ohne zusätzliche Kosten bereitzustellen.

Die Bereitstellung von Sicherheitsupdates darf nicht an kostenpflichtige Funktionssupgrades, Versionswechsel oder den Wechsel des SaaS-Tarifs gebunden sein.

Sicherheitsupdates müssen vom Auftragnehmer so eingespielt werden, dass keine funktionalen Änderungen erzwungen werden, die für die Behebung der Schwachstelle nicht erforderlich sind. Wartungsfenster für sicherheitsrelevante Updates sind

dem Auftraggeber unter Einhaltung einer angemessenen Frist (z. B. 5 Werktage) anzukündigen, außer bei Gefahr im Verzug.

6.8.4. Transparenz und Software Bill of Materials (SBOM)

Die SaaS-Lösung muss den Einsatz kryptografischer Verfahren entsprechend dem aktuellen Stand der Technik unterstützen.

Alle Datenübertragungen zwischen dem Client des Auftraggebers und der SaaS-Lösung sowie zwischen internen Komponenten des Auftragnehmers müssen ausschließlich über verschlüsselte Protokolle (z. B. TLS 1.2 oder höher) erfolgen.

Daten müssen im Ruhezustand (Data at Rest) verschlüsselt gespeichert werden.

Soweit kryptographische Verfahren verwendet werden, müssen diese den zum Zeitpunkt der Inbetriebnahme geltenden Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), insbesondere den Technischen Richtlinien der Reihe TR-02102, entsprechen. Abweichungen sind vom Auftragnehmer nachvollziehbar zu begründen.

6.8.5. Protokollierung und SIEM-Anbindung

Die SaaS-Lösung muss sicherheitsrelevante Ereignisse (z. B. erfolgreiche/fehlgeschlagene Logins, Rechteänderungen, Konfigurationsänderungen, Datenexporte) in einem manipulationssicheren Audit-Log protokollieren.

Die SaaS-Lösung muss die automatisierte Weiterleitung dieser sicherheitsrelevanten Ereignisse und Nachrichten an ein zentrales SIEM-System des Auftraggebers unterstützen. Hierfür sind standardisierte Schnittstellen (z. B. Syslog, CEF, LEEF oder eine gesicherte REST-API nach dem Stand der Technik) bereitzustellen.

6.8.6. Authentifizierung, Autorisierung und Identitätsmanagement

Die SaaS-Lösung muss sich nahtlos in die bestehende Authentifizierungs- und Autorisierungsinfrastruktur des Auftraggebers integrieren lassen.

Die SaaS-Lösung muss standardisierte Authentifizierungsprotokollen (Single Sign-on (SSO)), mindestens SAML 2.0 und OpenID Connect (OIDC) unterstützen.

Die SaaS-Lösung muss eine Anbindung an einen vom Auftraggeber betriebenen oder beauftragten Identity Provider (z. B. Microsoft Entra ID / ADFS, Keycloak) auf Basis der vorgenannten Standards unterstützen. Die Authentifizierung muss vollständig über diesen zentralen Identity Provider (IdP) erfolgen können.

Die SaaS-Lösung darf keine proprietären Authentifizierungsverfahren voraussetzen. Eine lokale Benutzerverwaltung (Passwort-Login) muss deaktivierbar sein, sofern eine zentrale Authentifizierung aktiv ist.

Die SaaS-Lösung muss die Automatisierung der Benutzerbereitstellung und -deaktivierung unterstützen, vorzugsweise über den SCIM 2.0 (System for Cross-domain Identity Management) Standard.

Rollen und Berechtigungen müssen Benutzern oder Gruppen des zentralen Identity Providers zugeordnet werden können (Role-Based Access Control, RBAC).

Authentifizierungs- und Autorisierungsvorgänge müssen revisionssicher protokolliert und über die oben genannte SIEM-Schnittstelle exportierbar sein.

6.8.7. Compliance und Exit-Management

Der Auftraggeber muss die Möglichkeit haben, seine Daten während der Vertragslaufzeit und bei Vertragsende in einem gängigen, maschinenlesbaren Format (z. B. CSV, JSON, XML) vollständig und strukturiert zu exportieren.

Nach Beendigung des Vertrags muss der Auftragnehmer alle Daten des Auftraggebers innerhalb einer Frist von 90 Tagen unwiederbringlich löschen und dies auf Verlangen schriftlich bestätigen.

6.9. Softwareauslieferung/Hotfix

Die SaaS-Lösung muss der Semantischen Versionierung (Semantic Versioning, Format: Major.Minor.Patch, z. B. 2.1.4) folgen.

Der Auftragnehmer ist verpflichtet, für folgende Änderungen umfassende und strukturierte Release Notes bereitzustellen. Dies gilt zwingend bei:

- Breaking Changes: Änderungen an APIs, Datenmodellen oder Kernfunktionalitäten, die Anpassungen auf Kundenseite erfordern.
- Sicherheitsrelevanten Updates: Behebung von Schwachstellen mit einem CVSS-Score von $\geq 7,0$ (Hoch und Kritisch). Diese müssen zusätzlich als dediziertes Security Advisory (mit CVE-Referenz) ausgewiesen werden.
- Neuen Major- oder Minor-Versionen: Einführung neuer Funktionalitäten, Module oder signifikanter Änderungen an der Benutzeroberfläche (Erhöhung der Major- oder Minor-Ziffer).
- Kritischen Fehlerbehebungen: Behebung von Fehlern, die die Verfügbarkeit, Datenintegrität oder Kernfunktionalität der Software beeinträchtigen.

Die Inhalte der Release Notes müssen mindestens enthalten: Versionsnummer, Veröffentlichungsdatum, detaillierte Beschreibung der Änderungen, behobene Feh-

ler/Sicherheitslücken, bekannte Einschränkungen, erforderliche Konfigurationsanpassungen auf Auftraggeberseite sowie eine klare Kennzeichnung von Breaking Changes.

Für reine Wartungsupdates (Patch-Ebene, z. B. Behebung von Minor-Bugs oder Sicherheitslücken mit CVSS < 7,0), die keine funktionalen Auswirkungen haben, genügt die Bereitstellung eines fortlaufenden, maschinenlesbaren Changelogs.

Sämtliche Release Notes und der Changelog müssen für den Auftraggeber zentral, dauerhaft über das Kundenportal des Auftragnehmers abrufbar sein.

6.10. Anwendungseinstellungen

- Die Anwendungseinstellungen des Users (Userprofil, Anzeigefelder für Ergebnislisten) müssen gespeichert und bei der nächsten Anmeldung wieder geladen werden können.
- Die Steuerung von Zugriffsrechten und Berechtigungen muss zentral durch den Auftraggeber erfolgen.
- Aufgrund der vorgeschriebenen Integration eines zentralen Identity Providers (SSO) darf die SaaS-Lösung im regulären Betrieb keine Passwörter der Endanwender verarbeiten oder speichern.
- Sofern die Lösung aus betrieblichen Gründen lokale Fallback- oder Service-Accounts vorhalten muss, ist die Speicherung von Passwörtern im Klartext oder mit veralteten Hash-Verfahren (z. B. MD5, SHA-1) strikt untersagt. Passwörter müssen ausschließlich mit aktuellen, salted Hash-Verfahren (z. B. Argon2, bcrypt oder PBKDF2 mit ausreichenden Iterationen) gespeichert werden, die den aktuellen Empfehlungen des BSI (TR-02102) entsprechen.

6.11. Vergütungslogik

Für die Nutzung der Software fällt je Lizenz eine monatliche Lizenzgebühr an (vgl. Anlage 03 Preisblatt, Pos. 1). Die Software muss mindestens die funktionalen Anforderungen gemäß Kapitel 5 dieser Leistungsbeschreibung (ausgenommen die optionalen Zusatzmodule gem. 5.6.3 dieser Leistungsbeschreibung) sowie die nicht-funktionalen Anforderungen gemäß Kapitel 6 dieser Leistungsbeschreibung umfassen (Standardlizenz). Erforderliche ABDA Lizenzen **sind** Bestandteil des Auftragsgegenstandes.

Durch den Auftragnehmer sind über die in den Standardlizenzen mindestens enthaltenen funktionalen Anforderungen zudem die Funktionen zur Anzeige von Großhandel- und Einkaufspreisen (vgl. 5.6.3.1 dieser Leistungsbeschreibung) sowie zur Anzeige von Hilfstaxenpreisen (vgl. 5.6.3.2 dieser Leistungsbeschreibung) anzubieten (Sondermodul). Soweit diese Funktionen nicht bereits Teil der Standardlizenz sind, erfolgt eine Vergütung des Sondermoduls „Großhandel- und Einkaufspreisen“ im Rahmen einer monatlichen Lizenzgebühr je Lizenz gemäß Preisblattposition 2 (vgl. Anlage 03 Preisblatt, Pos.

2). Eine Vergütung des Sondermoduls „Hilfstaxenpreise“ erfolgt im Rahmen einer monatlichen Lizenzgebühr je Lizenz gemäß Preisblattposition 3 (vgl. Anlage 03 Preisblatt, Pos. 3).

Die Kosten für Support und Pflege sind in der Vergütung für die Standardlizenzen und Sondermodule enthalten. Eine separate Vergütung hierfür erfolgt nicht.

Die Leistungen der Standardlizenzen und Sondermodule werden auf Abruf gem. Nr. 3.3 des Vertrags (vgl. Anlage 01) erbracht. Die Auftraggeberinnen sind nicht zum Abruf verpflichtet. Eine Mindestabnahmemenge ist nicht vereinbart.