

**Beschaffung einer Screening-Software für Finanzsanktionen so-wie
erweiterter Sanktionslisten inkl. Research Tool im Rahmen des Pro-
jektes WEMASO**

Leistungsbeschreibung Standard IT-Lösung im Bereich Namensscreening

Stand: 09.07.2026

Inhaltsverzeichnis

	Seite
Inhaltsverzeichnis	2
Abkürzungsverzeichnis	5
0 Hinweise zur Leistungsbeschreibung	6
1 Kontext und Zielsetzung	7
1.1 Besonderheiten	7
1.2 Systemkontext	8
1.2.1 Beschreibung der IT-Systemlandschaft der Bundesbank.....	8
1.2.1.1 Beschreibung der Container-Umgebung (OpenShift)	8
1.2.1.2 Logging und Monitoring	9
1.2.1.3 Anwendungskommunikation	9
1.2.1.4 Orchestrierung / Automation	10
1.2.1.5 Entwicklungsumgebung für OpenShift.....	10
1.2.1.6 Datenhaltung	10
1.2.1.7 Identity Access Management.....	11
1.2.1.8 Wartung und Systemaktualisierungen	11
1.2.1.9 Staging.....	12
2 Ausschlusskriterien	13
2.1 Fachliche (funktionale) Anforderungen an den Screening-Kern.....	13
2.1.1 Erkennung sanktionierter Entitäten (Screening)	13
2.1.2 Namensscreening	13
2.1.3 Verarbeitung von strukturierten und semi-strukturierten Daten	13
2.1.4 Batchverarbeitung	13
2.1.5 Verarbeitung von Codierungen und nicht-lateinischen Alphabeten	13
2.1.6 Scoring / Bewertung der Ergebnisse	13
2.1.7 Verarbeitung kurzer Namen	14
2.1.8 Verarbeitung von mindestens 200 Zeichen langen Datensätzen	14
2.1.9 Erkennung trotz Kombination von Abweichungen	14
2.1.10 Konfigurierbarkeit des Namensscreenings / Tuning	14
2.1.11 Konfigurierbarkeit der einbezogenen Datenquellen	14
2.1.12 Parallele (gleichzeitige) und getrennte Auswertung von Datensätzen	14
2.1.13 Prozessdokumentation / Reporting / Audit-Trail	14
2.1.14 Schnittstellen	15
2.1.15 Import relevanter Datenformate	15
2.1.16 Reihenfolge von Namensbestandteilen: Treffer trotz Änderungen	15
2.2 Technische Anforderungen	15
2.2.1 Integration in die IT-Systemlandschaft der Bundesbank	15
2.2.1.1 Integration in die IT-Systemlandschaft der Bundesbank.....	15
2.2.2 Implementierung der Software	16
2.2.2.1 Installation und Grundkonfiguration (Herbeiführung der Betriebsbereitschaft)	16
2.2.3 IT-Sicherheit	16
2.2.3.1 Auswahl geeigneter kryptografischer Verfahren (CON.1.A1).....	16
2.2.3.2 Einsatz von TLS-/SSL-Proxies (DER.1.A10)	16
2.2.3.3 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (DER.1.A6).....	16

2.2.3.4	Grundlegende Absicherung der Kommunikation mit anderen Netzen (NET.1.1.A9)	17
2.2.3.5	Absicherung eingehender Kommunikation vom Internet in das interne Netz (NET.1.1.A11)	17
2.2.3.6	Information bei IT-Schwachstellen (OPS.1.1.1.A20)	17
2.2.3.7	Nachweisbarkeit von administrativen Tätigkeiten (OPS.1.1.2.A5)	17
2.2.3.8	Schutz administrativer Tätigkeiten (OPS.1.1.2.A6)	17
2.2.3.9	Nutzung systemspezifischer Schutzmechanismen (OPS.1.1.4.A2)	18
2.2.3.10	Trennung der Testumgebung von der Produktivumgebung (OPS.1.1.6.A13)	18
2.2.3.11	Durchführung von Penetrationstests (OPS.1.1.6.A14)	18
2.2.3.12	Zertifizierung nach Sicherheitsstandards	18
2.2.4	Datenschutz	19
2.2.4.1	Einhaltung rechtlicher Rahmenbedingungen (OPS.1.1.5.A5 und CON.2.A1)	19
2.2.4.2	Anforderungen aus der KI-Verordnung	19
2.2.5	Benutzerkonten / Zugangsberechtigungen / Rollenkonzept	19
2.2.5.1	Funktionstrennung zwischen unvereinbaren Aufgaben (ORP.1.A4)	19
2.2.5.2	Einrichtung, Änderung und Entzug von Berechtigungen (ORP.4.A2)	19
2.3	Übergeordnete Anforderungen.....	20
2.3.1	Bedienungssprache	20
2.3.2	Schulung an der Software	20
2.3.3	Softwaredokumentation	20
2.3.4	Wartbarkeit	20
2.3.5	Testdatenscreening	20
2.3.6	Teststellung / Testinstallation	21
3	Bewertungskriterien	22
3.1	Fachliche (funktionale) Anforderungen an den Screening-Kern.....	22
3.1.1	Erkennung von weiteren Entitäten	22
3.1.2	Erkennung von Entitäten, bei abweichenden Schreibweisen (Fuzzy-Logik)	22
3.1.3	Hohe Sensitivität	22
3.1.4	Hohe Spezifität	22
3.1.5	Verarbeitung von Zahlungsverkehrsnachrichten	22
3.1.6	Verarbeitung von unstrukturierten Daten	22
3.1.7	Natural language processing (NLP): Einbeziehung von weiteren Informationen	23
3.1.8	Geburtsdaten	23
3.1.9	Einbeziehung von weiteren Informationen aus Sanktionslisten	23
3.1.10	Parametrisierbarkeit/Konfigurierbarkeit der Kontext-Daten	23
3.1.11	Unabhängiges Namensscreening	23
3.1.12	Verarbeitung von nicht-lateinischen Alphabeten	23
3.1.13	Transparenz	24
3.1.14	Begründung der Scores	24
3.1.15	Verarbeitung unbegrenzter Zeichenmengen pro Datensatz	24
3.1.16	Auswahl der zu screenenden Datenfelder	24
3.1.17	Verschiedene Konfigurierungen beim Screening einzelner Datenfelder	24
3.1.18	Erkennung auch ohne externe Zuordnung zum Typ der Entität	24
3.1.19	Häufige Namen	24
3.1.20	Erkennung von verschiedenen Sprachen und differenzierte Verarbeitung	24
3.1.21	Benachrichtigung bei fehlenden, fehlerhaften, inkonsistenten, unerwarteten Daten	25
3.2	Detailanforderungen an den Screening-Kern.....	25
3.2.1	Groß- und Kleinschreibung	25
3.2.2	Umlaute und Sonderzeichen	25
3.2.3	Ergänzungen und Verdopplung von Zeichen	25
3.2.4	Auslassung von Zeichen	25

3.2.5	Phonetische Ähnlichkeiten / Transkriptionsvarianten	25
3.2.6	Verarbeitung von einzelnen Zeichen anderer Alphabete	26
3.2.7	Direkte Verarbeitung von nicht-lateinischen Zeichen	26
3.2.8	Transkription von nicht-lateinischen Zeichen	26
3.2.9	Verarbeitung nicht-lateinischer defektiver Schreibweisen	26
3.2.10	Berücksichtigung von sprachspezifischen Besonderheiten von Namen	26
3.2.11	Männliche vs. weibliche Namen	27
3.2.12	Berücksichtigung besonders häufiger Fehler	27
3.2.13	Auslassung von Namensbestandteilen	27
3.2.14	Abkürzung von Namensbestandteilen	27
3.2.15	Ergänzungen von Namensbestandteilen und Zusätzen	27
3.2.16	Namen verschiedener Personen in einer Zelle	27
3.2.17	Trennzeichen: zusätzliche oder fehlende	28
3.2.18	Sehr lange Namen	28
3.2.19	Sehr kurze Namen	28
3.2.20	Typische Abwandlungen	28
3.2.21	Rechtsformen Erkennung und Verarbeitung	28
3.2.22	Branchen- und geographische Bezeichnungen werden sinnvoll in das Screening einbezogen	29
3.2.23	Erkennung austauschbarer Bezeichnungen	29
3.2.24	Erkennung von Namen trotz Kombination von Fehlern auf der Ebene von Zeichen und / oder Namensbestandteilen	29
3.3	Technische Anforderungen	29
3.3.1	Implementierung der Software	29
3.3.1.1	Integration in ein Shared Cluster	29
3.3.1.2	Konfiguration und Finetuning	30
3.3.2	Performance und Skalierbarkeit	30
3.3.2.1	Verarbeitung großer Datenmengen	30
3.3.2.2	Skalierbarkeit	30
3.3.2.3	Performance-Monitoring	30
3.3.2.4	Wiederaufnahme des Screenings nach Abbrüchen	30
3.3.2.5	Benachrichtigung bei Fehlern und Problemen	31
3.3.3	IT-Sicherheit	31
3.3.3.1	Information bei IT-Schwachstellen (OPS.1.1.1.A20)	31
3.3.3.2	Konfiguration der Protokollierung auf System- und Netzebene (OPS.1.1.5.A3)	31
3.3.4	Datenschutz	31
3.3.4.1	Restriktive Verwendung von Protokollierungsdaten	31
3.4	Übergeordnete Anforderungen	31
3.4.1	Release- und Änderungsdokumentation	31
3.4.2	Benutzerfreundlichkeit	32
3.4.3	Barriere-Freiheit	32
3.4.4	Portabilität	32
3.4.5	Gleichstellungskonform	32

Abkürzungsverzeichnis

Abkürzung	Bedeutung
A-Kriterium	Ausschluss-Kriterium
API	Anwendungsprogrammierschnittstelle
BDSG	Bundesdatenschutzgesetz
BGG	Behindertengleichstellungsgesetz
BGleiG	Bundesgleichstellungsgesetz
BIC	Business Identifier Code
BITV 2.0	Barrierefreie Informationstechnik-Verordnung 2.0
B-Kriterium	Bewertungs-Kriterium
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLI	Command Line Interface
DSGVO	Datenschutz-Grundverordnung
EU	Europäische Union
ISIN	Internationale Wertpapierkennnummer
IWA	Integrated Windows Authentication
LAD	Lösungsarchitekturdokument
OCR	Optical Character Recognition
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SEPA	Single Euro Payments Area
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TLS	Transport Layer Security

0 Hinweise zur Leistungsbeschreibung

Innerhalb der Leistungsbeschreibung und der Bewertungsmatrix, die sich aus mehreren thematisch gegliederten Tabellenblättern zusammensetzt, werden sämtliche von der Anwendung bzw. vom Auftragnehmer zu erfüllende Anforderungen dokumentiert. In der Bewertungsmatrix werden alle Anforderungskriterien getrennt nach Ausschluss- (A-Kriterien) und Bewertungskriterien (B-Kriterien) dargestellt.

- A-Kriterien sind MUSS-Anforderungen: beschreiben eine zwingende Anforderung/Mindestanforderung, die unbedingt erfüllt werden muss. Bereits die Nicht-Erfüllung eines A-Kriteriums führt zum Ausschluss.
- B-Kriterien – SOLL-Anforderungen: bezeichnen Anforderungen, die möglichst zu erfüllen sind. Sofern diese nicht oder nur teilweise erfüllt werden, ist im Angebot darauf hinzuweisen. Es steht dem Auftragnehmer frei, zu diesen Anforderungen Alternativlösungen aufzuzeigen, die dem in der genannten Anforderung verfolgten Ziel gerecht werden können. Diese Kriterien werden bewertet.

Die Gewichtung der einzelnen Anforderungen ist der Bewertungsmatrix zu entnehmen. Für die Vergabe sind die Inhalte der Bewertungsmatrix und die in den Zuschlagskriterien angegebenen Berechnungen maßgeblich.

Im Verlauf des Verfahrens ist beabsichtigt, weitere Mindestanforderungen/A-Kriterien zu ergänzen. Hierbei ist es auch möglich, dass bestehende Anforderungen enger definiert oder zu Ausschlusskriterien verschärft werden. Diese bereits im Vorfeld in Frage kommenden Kriterien sind in der Anlage „C4_L1_Anlage 2_Bewertungsmatrix 25-2000064042_Los 1“ gekennzeichnet.

1 Kontext und Zielsetzung

Die Deutsche Bundesbank kann nach § 23 Abs. 1 und 2 des Außenwirtschaftsgesetzes zur Überwachung der Einhaltung von Finanzsanktionen und der außenwirtschaftlichen Meldepflichten von Auskunftspflichtigen Auskünfte verlangen und Prüfungen bei diesen durchführen. Bestandteil der Prüfungen ist ein softwarebasierter Abgleich („Screening“) der Kunden-, Transaktions- und Handelsfinanzierungsinformationen des geprüften Unternehmens mit Listen von Entitäten (insbesondere natürliche und juristische Personen, Organisationen und Einrichtungen sowie Schiffe, Häfen, Schleusen und Flugzeuge), die nach deutschem und EU-Recht (auch unter Berücksichtigung von Beschlüssen des UN-Sicherheitsrates nach § 5a AWG) Sanktionen unterliegen (Sanktionslisten).

Zur Unterstützung von Prüfungshandlungen ist angedacht, einen neuen Screening-Softwarekern zu beschaffen, welcher in eine bundesbankeigene Prüfungsplattform integriert werden soll.

Gesucht wird ein am Markt vorhandener Screening-Kern, der Namen und Namensähnlichkeiten in strukturierten und semi-strukturierten Daten findet und auch die Volltextsuche in unstrukturierten Daten der geprüften Unternehmen unterstützt. Weitere Merkmale wie Geburtsdaten, Geschlecht, u.ä. sollen hierbei ggf. mitberücksichtigt werden. Zusatzfunktionalitäten zum Screening-Kern, wie ein Case Management System, sind nicht Bestandteil dieser Ausschreibung. Zusätzliche optionale Leistungen können Tools z.B. zum Listenmanagement, zur Datenstandardisierung oder Datenschnittstellen sein.

Anders als beim Einsatz bei Geschäftsbanken soll die Software gegen stichtagsbezogene/historische Sanktionslisten screenen; die Berücksichtigung der Gültigkeit von Sanktionen zu bestimmten Zeitpunkten wird jedoch in einer separaten Anwendung vorgenommen. Die Belieferung von Kundendaten erfolgt hierbei nicht regelmäßig, sondern je nach geprüftem Unternehmen ändern sich die Input-Daten, die Konfiguration sowie die verwendeten Sanktionslisten. Die Aufarbeitung der Sanktionslisten in ein standardisiertes Format bzw. das Listenmanagement erfolgt in einer separaten Anwendung.

Es wird keine Auftragsfertigung, externe Neuentwicklung oder Beratung angefragt.

1.1 Besonderheiten

Durch kontinuierlich wechselnde geprüfte Unternehmen sind mit jedem Batch-Lauf neue und unterschiedliche Daten zu screenen, welche unterschiedliche Herausforderungen mit sich bringen. Der Screening-Kern soll deshalb möglichst flexibel konfigurierbar und parametrisierbar sein, um für jedes Screening unterschiedliche Methoden (z. B. Übereinstimmungsgrad oder Matching-Algorithmen) verwenden zu können. Des Weiteren variiert dadurch das Mengengerüst für die Anzahl an zu screenenden Daten von Jahr zu Jahr. Das Mengengerüst wird erst nach dem Teilnahmewettbewerb offengelegt, wenn eine entsprechende Verschwiegenheitserklärung vom Auftragnehmer unterzeichnet wurde. Hierbei gilt es zu beachten, dass abweichend zur Vorgehensweise bei Geschäftsbanken auch die Kundendaten jeweils nur einmal pro Prüfung gescreent werden.

1.2 Systemkontext

Wie eingangs erwähnt, soll der zu beschaffende Screening-Kern Bestandteil einer Prüfungsplattform werden. Eine separate Anwendung in der Prüfungsplattform empfängt Daten von geprüften Unternehmen, bereitet diese zu einem standardisierten Format auf und übermittelt diese dann über eine Anwendungsprogrammierschnittstelle (API) zusammen mit den Sanktionslisten an die Screening-Software, damit die Daten dann mittels Batch-Lauf gescreent werden. Anschließend sollen die Treffer und zugehörigen Metadaten aus dem Screening an die Plattform zurückübermittelt werden, damit diese weiterverarbeitet werden können. Für unseren Anwendungsfall sollten die Ergebnisse in Listenform in einem maschinenlesbaren Format vorliegen. Die beschriebene Prüfungsplattform befindet sich aktuell noch in der Entwicklung. Der Screening-Kern soll in der Private Cloud der Deutschen Bundesbank betrieben werden können.

1.2.1 Beschreibung der IT-Systemlandschaft der Bundesbank

Im Folgenden wird die IT-Systemlandschaft der Deutschen Bundesbank beschrieben. Die Software muss in die beschriebene Infrastruktur entweder auf einem Standard-Server oder in der OpenShift-Umgebung integriert werden können. Hierbei wird die Integration in die OpenShift-Umgebung bevorzugt.

Im Angebot muss eine Beschreibung der Systemlandschaft des Auftragnehmers erfolgen, in dem insbesondere erläutert wird, wo es Probleme bei der Implementierung geben könnte (ID 5.2).

Im Rahmen der Ausschreibung muss vor Vertragsunterzeichnung eine technische Teststellung erfolgen, in der die Integration in die IT-Systemlandschaft der Deutschen Bundesbank geprüft wird (siehe Abschnitt 2.3.6). Hierbei wird insbesondere geprüft, ob die in diesem Kapitel aufgeführten Rahmenbedingungen und die angebotene Anwendung kompatibel sind.

1.2.1.1 Beschreibung der Container-Umgebung (OpenShift)

Die von der Bundesbank betriebene Container-Plattform basiert auf dem etablierten Cloud-Standard Kubernetes. Konkret wird die Kubernetes-Distribution Red Hat OpenShift genutzt, welche Kubernetes um zusätzliche Unternehmensfunktionen erweitert und gängige Integrationen mit anderen Werkzeugen der IT-Landschaft vereinfacht.

Die Container-Plattform ermöglicht es durch OpenShift Anwendungen in isolierten und portablen Einheiten in Form von Containern zu entwickeln, zu verwalten und zu betreiben. Die Container können innerhalb des Red Hat OpenShift Clusters in einem mandantenfähigen Shared Cluster mit entsprechend eingerichteten Namespaces und Operatoren betrieben werden.

- **Service Mesh:** Das Service Mesh (integrierter Proxy, Loadbalancer, Firewall) zur einheitlichen und vollintegrierten Verwaltung der Kommunikation zwischen Anwendungen ist auf Basis der von OpenShift bereitgestellte Implementierung (Istio) umgesetzt. Wird Service Mesh nicht unterstützt, muss die Verschlüsselung der Cluster-internen Kommunikation anders sichergestellt werden. Wir befinden uns auf Service Mesh Version

3.

- **Storage:** Dynamische Provisionierung und Verwaltung von NFS und Block, der von den Containern zur persistenten Datenhaltung genutzt werden kann.
- **Container Runtime Security:** Das RASP Tool RHACS (Red Hat Advanced Cluster Security) wird als Sicherheitslösung für Kubernetes zur Risikoerkennung und Compliance-Überwachung genutzt.
- **Worker Nodes:** Ein Worker Node verfügt standardmäßig über 40 CPU Cores und 512 GiB RAM, weshalb ein einzelner Pod nicht mehr als 36 CPU Cores und / oder 500 GiB RAM benötigen darf.
- **Namespaces:** In Namespaces der OpenShift Cluster werden die maximal verfügbaren Ressourcen (CPU und RAM) über Leistungsbeschränkungen gesteuert. Es gibt Standardgrößen (von 2 CPU und 8 GiB RAM bis 16 CPU und 64 GiB RAM), es können aber auch individuelle Größen definiert werden.
- **Backup und Restore:** Die Anwendungsdaten werden in Persistent Volumes im Red Hat OpenShift Cluster unter Nutzung des VCF vSAN gespeichert, für Langzeitsicherungen siehe Datenhaltung.

1.2.1.2 Logging und Monitoring

Die Container Plattform ist an die zentrale Logging-Plattform der Deutschen Bundesbank angebunden und überträgt die Application-Logs automatisiert dorthin. Es wird das Produkt Elastic Cloud Enterprise (ECE) genutzt. In den OpenShift Clustern der Container Plattform werden mittels Elastic Agents die Anwendungs-Logs sowie weitere Systeminformationen gesammelt und an Elasticsearch weitergeleitet. Die Anwendungs-Logs müssen hierfür in die Standard-Datenströme *StdOut* und *StdErr* geschrieben werden.

Läuft die Anwendung auf einem Standard-Server, müssen Log-Dateien geschrieben werden.

Für das zentrale Enterprise Monitoring wird das Produkt Dynatrace genutzt. Die OpenShift Cluster der Container Plattform werden mittels Kubernetes API und Prometheus in die Dynatrace Plattform integriert.

Die Standard-Server werden über den Dynatrace Agent angebunden.

1.2.1.3 Anwendungskommunikation

Es ist möglich, mit Dritt-Anwendungen über eine Schnittstelle (z.B. REST-API oder CLI) zu kommunizieren und von dort aus Batch-Läufe anzustoßen.

1.2.1.4 Orchestrierung / Automation

Für die Bereitstellung und Verwaltung von Systemen (OpenShift Cluster und Namespaces), Storage (S3 Buckets, NFS) und Datenbanken (Oracle, Microsoft SQL Server) sowie weitere Komponenten wird das Produkt OpenText Operations Orchestration genutzt.

1.2.1.5 Entwicklungsumgebung für OpenShift

In der OpenShift-Umgebung stehen unter anderem die folgenden Basisdienste zur Verfügung:

- **CodeArtefakt:** Bereitstellung eines Binary Repository Managers unter Nutzung des Produkts JFrog Artifactory
- **CodeDeploy:** Bereitstellung eines Continuous-Deployment-Services, mit dem Anwendungen auf die Container Plattform ausgeliefert werden können. Für das Deployment wird das Produkt OpenShift GitOps bzw. ArgoCD genutzt.

1.2.1.6 Datenhaltung

Datenbankmanagementsysteme (DBMS):

Die DBMS werden auf virtuellen Windows Servern (Microsoft SQL Server) betrieben und somit außerhalb der Container Plattform bereitgestellt.

Storage:

Für temporäre Daten wird Ephemeral Local Storage im Red Hat OpenShift Pod genutzt. Für persistente Daten Persistent Volumes im Red Hat OpenShift Cluster unter Nutzung des VCF vSAN (File RWO/RWX, Block RWO).

Storage Fileservices:

Der Storage Fileservice umfasst Fileservices für Anwendungen und Serversysteme sowie die Bereitstellung persistenter Volumes für Container-Umgebungen:

- Für Standard-Server auf Windows-Basis werden Speicherbereiche über das CIFS-Protokoll bereitgestellt.
- Für Standard-Server auf RHEL-Basis werden über NFS Speicherbereiche freigegeben, die für die Datenhaltung genutzt werden. Da das Stagesystem die Verwaltung des Speicherbereichs übernimmt, können die Datenbereiche ggf. von mehreren Servern genutzt werden.

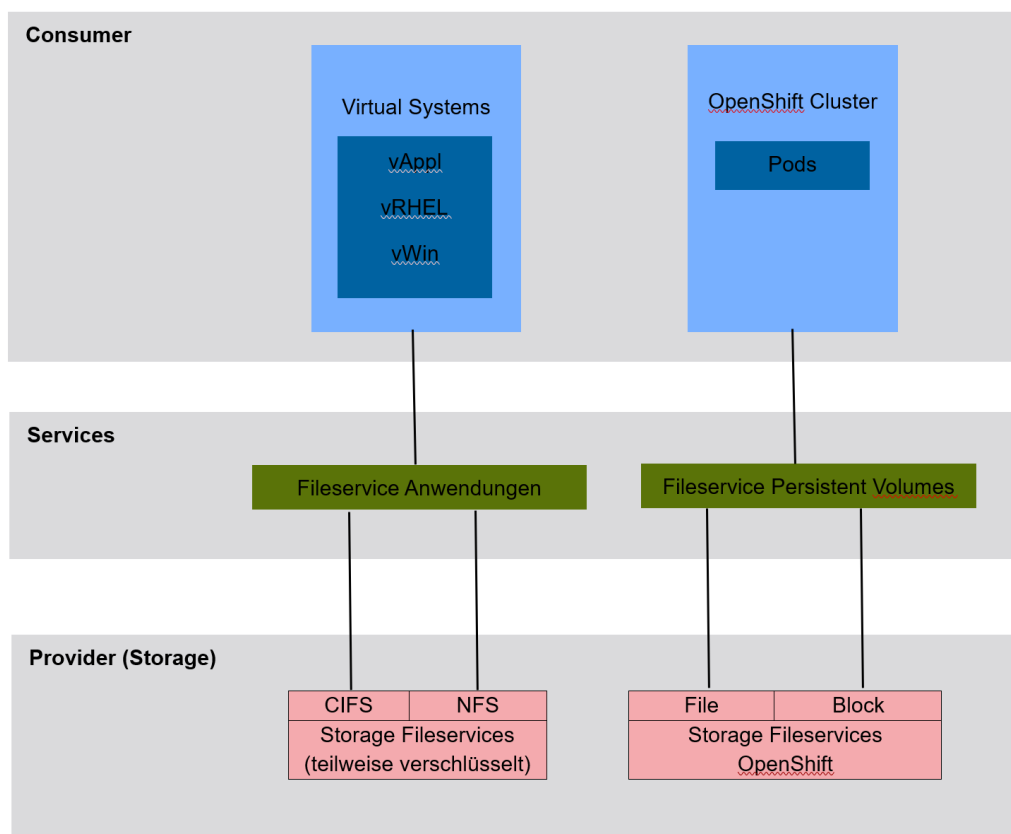


Abbildung 1: Übersicht Fileservices

1.2.1.7 Identity Access Management

Die Benutzer- und Berechtigungsverwaltung in der Deutschen Bundesbank erfolgt derzeit im Active Directory (AD). Die Software muss auf die im AD definierten Benutzer und deren Gruppen zugreifen können, sodass diese zur Autorisierung (Rechte- und Rollenvergabe) genutzt werden können. Die technische Anbindung an das AD erfolgt via LDAP.

Für die Authentifizierung von Benutzern stehen derzeit zwei Varianten zur Verfügung:

- (1) Authentifizierung über das AD mit IWA (Integrated Windows Authentication) unter Nutzung von Kerberos
- (2) Authentifizierung über das AD FS (Active Directory Federation Services) mit SAML

1.2.1.8 Wartung und Systemaktualisierungen

Die Systeme der Private Cloud der Deutschen Bundesbank werden regelmäßig aktualisiert. Für Red Hat OpenShift ist mindestens die vorletzte von Red Hat unterstützte EUS/LTS Version im Einsatz. Aktuell ist das die Version 4.18.

1.2.1.9 Staging

Die Software muss in drei unterschiedlichen Stages deployt werden können (mehr Details im Abschnitt 2.2.3 unter Trennung der Testumgebung von der Produktivumgebung).

2 Ausschlusskriterien

2.1 Fachliche (funktionale) Anforderungen an den Screening-Kern

2.1.1 Erkennung sanktionierter Entitäten (Screening)

Die Software muss Entitäten (insbesondere natürliche und juristische Personen, Organisationen und Einrichtungen) in gelieferten Sanktionslisten mit Entitäten aus den Daten der zu prüfenden Unternehmen anhand verschiedener Merkmale (siehe 2.1.2) abgleichen, Übereinstimmungen und Ähnlichkeiten erkennen, paarweise zuordnen und ausgeben (Screening). Die Wahrscheinlichkeit einer Identität bzw. der Grad der Ähnlichkeit muss als Score¹ angegeben werden. Sowohl die Kunden-/Transaktions-ID als auch die Sanktions-IDs aus den Sanktionslisten müssen mit ausgegeben werden. Die Prüfung muss sowohl natürliche als auch juristische Personen und andere Entitäten umfassen. Dabei soll eine möglichst gute Sensitivität, bei gleichzeitig hoher Spezifität erreicht werden (siehe hierzu 3.1.3 und 3.1.4).

2.1.2 Namensscreening

Die Software muss Entitäten anhand ihrer Namen screenen können. (Zusätzliche Anforderungen zum Namensscreening werden unter Abschnitt 3.2 (B-Kriterien) beschrieben.)

2.1.3 Verarbeitung von strukturierten und semi-strukturierten Daten

Die Software muss einen oder mehrere Screening-Algorithmen verwenden, die den Abgleich von Namen oder Begriffen in strukturierten und semi-strukturierten Daten unterstützen.

2.1.4 Batchverarbeitung

Die Software muss in der Lage sein, Batch-Screenings durchzuführen. (Weitere Anforderungen zur Batchverarbeitung werden unter Abschnitt 3.3.2 (B-Kriterien) beschrieben.)

2.1.5 Verarbeitung von Codierungen und nicht-lateinischen Alphabeten

Die Software muss mindestens Codierungen in UTF-8 und ANSI verarbeiten können.

2.1.6 Scoring / Bewertung der Ergebnisse

Die Software muss die Ergebnisse und Teilergebnisse des Screenings ermitteln und als aussagekräftige und hinreichend differenzierende Bewertung (Score) ausgeben. Der Score muss die Trefferqualität des Namens mit dem Sanktionslisteneintrag angeben. Die Scores bei der Prüfung der weiteren Bestandteile (z.B. Geburtsdatum, Länderangaben) müssen getrennt hiervon ausgegeben werden. Die Treffer eines Namens gegen mehrere Sanktionslisteneinträge müssen getrennt voneinander ausgegeben werden.

¹ Siehe auch 2.1.6

2.1.7 Verarbeitung kurzer Namen

Die Software muss auch kurze Namen (idealerweise ab einem Zeichen) aus den EU-Sanktionslisten beim Screening berücksichtigen können.

2.1.8 Verarbeitung von mindestens 200 Zeichen langen Datensätzen

Die Software muss mindestens 200 Zeichen lange Namen verarbeiten können.

2.1.9 Erkennung trotz Kombination von Abweichungen

Die Software muss sanktionierte Entitäten auch dann treffen können, wenn ihre Namen durch Abweichungen, auch unterschiedlicher Art, verändert sind.

2.1.10 Konfigurierbarkeit des Namensscreenings / Tuning

Die Software muss es den Nutzern ermöglichen, Regeln, Parameter und andere Einstellungen des Namensscreenings flexibel zu konfigurieren, zu entfernen und hinzuzufügen.

Die Software muss es den Nutzern ermöglichen, Screening-Abfragen so einstellen zu können, dass der Nutzer selbst die Kompromisse im Zielkonflikt zwischen Sensitivität und Spezifität festlegen und ändern kann.

2.1.11 Konfigurierbarkeit der einbezogenen Datenquellen

Die Software muss es ermöglichen, dass unterschiedliche Screenings mit unterschiedlichen Sanktionslisten durchgeführt werden können.

2.1.12 Parallele (gleichzeitige) und getrennte Auswertung von Datensätzen

Die Software muss es ermöglichen, dass verschiedene auszuwertende Datensätze auch mit unterschiedlichen Konfigurationen parallel (gleichzeitig) und getrennt voneinander gescannt werden können. Die Daten unterschiedlicher geprüfter Unternehmen müssen dementsprechend strikt getrennt verarbeitet und ausgegeben werden. Der Status (Überblick/Fortschritt) von verschiedenen parallellaufenden Screenings muss einzusehen sein.

2.1.13 Prozessdokumentation / Reporting / Audit-Trail

Der Screening-Prozess sowie mögliche Fehler und Probleme müssen nachvollziehbar und aussagekräftig dokumentiert werden, um auswertbare Hinweise zu den Ursachen von Problemen zu liefern und deren Folgen abschätzen zu können. Dazu gehören:

- alle Änderungen an Systemeinstellungen
- der Batchverlauf (Uhrzeiten, Datenmengen, Aktionen wie z.B. Import von Input-Daten etc.);
- Dokumentation von Problemen, z.B. Programmabbrüche, Fehler beim Laden von Inputdaten, Inkonsistenzen in Daten unterschiedlicher geprüfter Unternehmen (z.B. inkonsistente Datenformate) usw., also Art, Auftreten, Häufigkeit von Fehlern;

- transparente Dokumentation der Konfliktlösung, z.B. wie die Software problematische oder fehlende Inputdaten verarbeitet hat, (z.B. durch Ignorieren der Fehler, Ignorieren der Daten, Verändern der Daten usw.);
- Dokumentation der Folgen von Fehlern oder Problemen (z.B. bei Abbrüchen oder Überspringen von (Teil-)Aufgaben)

2.1.14 Schnittstellen

Die Software muss standardisierte Schnittstellen (z. B. REST) und Konnektoren für gängige Systeme bieten. Dies umfasst auch API-basierte Kommunikation. Die Integration des Screening-Kerns ist unter 1.2 Systemkontext beschrieben. Die Grundmenge an typischen Inputattributen umfasst den Vor- und Nachnamen bei natürlichen Personen, Aliasnamen, Firmennamen und ehem. Bezeichnungen, Datumsangaben, Länderangaben und Identifikationsnummern.

2.1.15 Import relevanter Datenformate

Die Software muss strukturierte Daten laden und verarbeiten können, die in einem gängigen Format vorliegen (mindestens csv, xml oder txt).

2.1.16 Reihenfolge von Namensbestandteilen: Treffer trotz Änderungen

Die Software muss sanktionierte Entitäten auch dann treffen, wenn die Reihenfolge von einem oder mehreren Namensbestandteilen verändert ist (z.B. Vornamen, Familiennamen, Patronymie, Titel, akademische Grade oder entsprechend Bestandteile von Firmennamen oder Organisationen).

2.2 Technische Anforderungen

In diesem Abschnitt werden die technischen Ausschlusskriterien an die Software-Lösung formuliert.

2.2.1 Integration in die IT-Systemlandschaft der Bundesbank

2.2.1.1 Integration in die IT-Systemlandschaft der Bundesbank

Die Software muss in der Private Cloud der Bundesbank betrieben werden können. Dies kann entweder auf Red Hat Enterprise Linux Servern oder Windows Servern erfolgen (abkürzend als „Standard-Server“ bezeichnet) oder in einer Container-Umgebung, die auf einer aktuellen Version der Kubernetes-Distribution Red Hat OpenShift basiert (abkürzend als „OpenShift“ bezeichnet).

Die IT-Systemlandschaft der Bundesbank wird in Abschnitt 1.2.1 beschrieben.

2.2.2 Implementierung der Software

2.2.2.1 Installation und Grundkonfiguration (Herbeiführung der Betriebsbereitschaft)

Der Auftragnehmer muss Unterstützung bei der Installation und Grundkonfiguration der Screening-Software leisten, einschließlich der Anpassung an die spezifischen Anforderungen der Deutschen Bundesbank und der Erstellung des Lösungsarchitekturdokuments (LAD) zur Dokumentation der Systemarchitektur.

2.2.3 IT-Sicherheit

Die verwendeten Kürzel bezeichnen die Abschnitte aus dem IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) der Edition 2023.²

2.2.3.1 Auswahl geeigneter kryptografischer Verfahren (CON.1.A1)

Sämtliche Daten müssen sowohl während der Übertragung ("in transit") als auch im Ruhezustand ("at rest") durch geeignete Verschlüsselungsverfahren geschützt werden. Dies gilt für alle Kommunikationsverbindungen, einschließlich interner Verbindungen (z.B. zur Datenbank), sowie für alle Speicherlösungen.

Zur Verschlüsselung müssen geeignete kryptografische Verfahren mit etablierten Algorithmen verwendet werden. Zu diesen Algorithmen dürfen keine relevanten Sicherheitslücken bekannt sein. Ebenso müssen aktuell empfohlene Schlüssellängen verwendet werden. Die aktuell etablierten Algorithmen und Schlüssellängen, die anzuwenden sind, sind in der Technischen Richtlinie TR-02102-1 des BSI festgelegt.

2.2.3.2 Einsatz von TLS-/SSL-Proxies (DER.1.A10)

Bei Übergängen aus BBk-externen Netzen in das interne BBk-Netz soll die Anwendung mit der Unterbrechung des Datenverkehrs (aufgrund eines Contentscannings, Schemavalidierung sowie Inhaltsvalidierung) ohne weitere Probleme (z.B. ohne Timeouts) umgehen können.

2.2.3.3 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten (DER.1.A6)

Die Software muss Protokolldaten erstellen, die Aktivitäten (wie bspw. Anmeldeversuche, Dateizugriffe, Löschprotokolle, Konfigurationseinstellungen oder Fehlermeldungen) aufzeichnen. Diese Aufzeichnungen dienen dazu, Probleme oder verdächtige Aktivitäten frühzeitig zu identifizieren.

² Siehe: Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html; direkter Link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

2.2.3.4 Grundlegende Absicherung der Kommunikation mit anderen Netzen (NET.1.1.A9)

Die IT-Lösung muss Zugriffe von Benutzern authentifizieren, hier muss eine Multi-Faktor-Authentifizierung (MFA) erfolgen.

Die IT-Lösung muss eine gegenseitige Authentisierung zwischen der IT-Lösung und anderen IT-Lösungen unterstützen.

2.2.3.5 Absicherung eingehender Kommunikation vom Internet in das interne Netz (NET.1.1.A11)

Die IT-Lösung muss sicherstellen, dass alle Zugriffe vom Internet auf das interne Netz über sichere Kommunikationskanäle erfolgen.

Die IT-Lösung muss auch ohne freien Internetzugang funktionsfähig sein.

2.2.3.6 Information bei IT-Schwachstellen (OPS.1.1.1.A20)

Die IT-Lösung muss vom Auftragnehmer vor der Auslieferung auf Schadsoftware/Malware und Backdoors geprüft werden. Ein entsprechendes Prüfergebnis ist dem Auftraggeber zur Verfügung zu stellen.

2.2.3.7 Nachweisbarkeit von administrativen Tätigkeiten (OPS.1.1.2.A5)

Administrative Tätigkeiten müssen nachweisbar sein und in der Software protokolliert werden. Dafür muss mindestens festgehalten werden,

- welche Änderung bei einer Tätigkeit durchgeführt wurde,
- wer eine Tätigkeit durchgeführt hat,
- wann eine Tätigkeit durchgeführt wurde.

Dazu müssen alle Administrierenden über eine eigene Zugangskennung verfügen. Auch Vertretungen von Administrierenden müssen eigene Zugangskennungen erhalten. Jeder Anmeldevorgang (Login) über eine Administrationskennung muss protokolliert werden.

2.2.3.8 Schutz administrativer Tätigkeiten (OPS.1.1.2.A6)

Administrative Schnittstellen und Funktionen dürfen nur berechtigten Personen zur Verfügung stehen. Für diese Schnittstellen und Funktionen müssen geeignete Verfahren zur Authentisierung festgelegt werden. Es muss sichergestellt sein, dass Administrationstätigkeiten nur durchgeführt werden können, falls vorher eine dementsprechende Authentisierung erfolgt ist. Die Administration muss über sichere Protokolle erfolgen.

2.2.3.9 Nutzung systemspezifischer Schutzmechanismen (OPS.1.1.4.A2)

Die Software muss mit den IT-Systemen des Auftraggebers kompatibel sein und deren Schutzmechanismen verwenden, beispielsweise in Bezug auf Logging und Monitoring, das Rollenkonzept, Authentifizierungsmethoden und Firewall-Regeln.

Diese Mechanismen müssen genutzt werden, sofern es keinen mindestens gleichwertigen Ersatz gibt.

2.2.3.10 Trennung der Testumgebung von der Produktivumgebung (OPS.1.1.6.A13)

Die Software muss sich als 3-Stagemodell (Entwicklung, Test, Produktion) aufbauen lassen. Die Testumgebung muss von der Produktivumgebung getrennt betrieben werden können. Der Auftragnehmer sichert zu, dass die technische Konfiguration der IT-Lösung transparent über die Stages ausgeliefert werden kann. Die in der Testumgebung verwendeten Architekturen und Mechanismen müssen dokumentiert werden. Es muss möglich sein, die Stages mit unterschiedlichen Release-Ständen zu betreiben.

2.2.3.11 Durchführung von Penetrationstests (OPS.1.1.6.A14)

Der Auftragnehmer muss sich bereit erklären, dass der Auftraggeber bei Bedarf auf eigene Kosten einen Penetrationstest durchführen darf, um sich von der Sicherheit der bereitgestellten Services selbst überzeugen zu können. Der Auftragnehmer sichert zu, Pentest-Findings gemäß ihrer Kritikalität für den Einsatz in der Deutschen Bundesbank zu beheben.

2.2.3.12 Zertifizierung nach Sicherheitsstandards

Der Auftragnehmer verfügt für die Bereitstellung der Leistung bzw. IT-Lösung über ein angemessenes, implementiertes und dokumentiertes Sicherheitskonzept und Informationssicherheitsmanagementsystem (ISMS) basierend auf ISO-Standard 27001. Für den Betrieb in der Private Cloud Umgebung hat sich das Sicherheitskonzept zudem an ISO 27017 auszurichten. Die IT-Lösung muss gemäß den Standards 200-2 „IT-Grundschutz-Methodik“ sowie 200-3 „Risikomanagement“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bzw. gemäß der angeführten ISO 27001 und ISO 27017 Standards oder alternativen Sicherheitsstandards mit vergleichbarem Sicherheitsniveau, installierbar und betreibbar sein. Die für die IT-Lösung zutreffenden IT-Grundschutzbausteine der aktuellen Edition müssen für die gesamte Vertragslaufzeit anwendbar sein. Zur Erfüllung der Anforderung sind alternativ Nachweise über die Einhaltung vergleichbarer internationaler Standards zu erbringen.

2.2.4 Datenschutz

2.2.4.1 Einhaltung rechtlicher Rahmenbedingungen (OPS.1.1.5.A5 und CON.2.A1)

Die Software muss es ermöglichen, die gesetzlichen Bestimmungen bzw. rechtlichen Vorgaben zum Datenschutz (insbesondere DSGVO, BDSG (Bundesdatenschutzgesetz)) einzuhalten.

Ferner übergibt der Auftragnehmer eine Beschreibung zu seinen implementierten technischen und organisatorischen Schutzvorkehrungsmaßnahmen.

2.2.4.2 Anforderungen aus der KI-Verordnung

Sofern bei der Screening Software auch KI-Komponenten eingesetzt werden sollen, sind neben den Regelungen der DSGVO auch die Regelungen der KI-VO zu beachten.

2.2.5 Benutzerkonten / Zugangsberechtigungen / Rollenkonzept

Die Software muss die Umsetzung eines individuellen Berechtigungskonzeptes ermöglichen. Dazu muss es möglich sein, verschiedene Benutzer anzulegen, den Zugang zu steuern und Nutzeraktionen zu loggen. (Zum Logging und Auslesen von Nutzeraktivitäten siehe 2.2.3.3 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten.)

Die Software muss die Realisierung eines Rollenkonzeptes ermöglichen, das die folgenden Anforderungen erfüllt:

2.2.5.1 Funktionstrennung zwischen unvereinbaren Aufgaben (ORP.1.A4)

Die Software muss es ermöglichen, operative und kontrollierende Funktionen auf verschiedene Personen zu verteilen. Für unvereinbare Funktionen muss eine Funktionstrennung festgelegt und dokumentiert sein. Auch Vertreter müssen der Funktionstrennung unterliegen.

2.2.5.2 Einrichtung, Änderung und Entzug von Berechtigungen (ORP.4.A2)

Die Software muss es ermöglichen, dass Benutzerkennungen und Berechtigungen nur aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden können, also nach dem Prinzip der geringsten Berechtigungen (*Least Privileges*) und Erforderlichkeitsprinzip (*Need-to-know*). Bei personellen Veränderungen müssen die nicht mehr benötigten Berechtigungen entfernt werden können.

Die Software muss Folgendes ermöglichen: Beantragen Mitarbeitende Berechtigungen, die über den Standard hinausgehen, dürfen diese nur nach zusätzlicher Begründung und Prüfung vergeben werden.

Alle Berechtigungen müssen über separate administrative Rollen eingerichtet werden.

2.3 Übergeordnete Anforderungen

2.3.1 Bedienungssprache

Die Software muss in deutscher oder englischer Sprache bedient werden können, wobei die Deutsche Bundesbank eine deutschsprachige Lösung präferieren würde. Auch Systemeinstellungen im Hintergrund, Log-Dateien und weitere Funktionen müssen entweder auf Deutsch oder Englisch verfügbar sein.

2.3.2 Schulung an der Software

Der Auftragnehmer muss Schulungen für die relevanten Mitarbeitenden der Deutschen Bundesbank durchführen. Zum einen sollen Administratoren und technische Integratoren geschult werden, zum anderen sollen Workshops zur Konfiguration und Nutzung der Software durchgeführt werden. Zusätzlich sollen Schulungsmaterialien bereitgestellt werden. Die Schulungen (einschließlich der zugehörigen Materialien) müssen in deutscher oder englischer Sprache gewährleistet werden, wobei die Deutsche Bundesbank eine deutschsprachige Schulung präferieren würde.

2.3.3 Softwaredokumentation

Der Auftragnehmer muss eine umfassende und verständliche Dokumentation der Software bereitstellen. Hierunter zählen ein Benutzerhandbuch für Anwendende, ein Betriebshandbuch für technische Administratoren, eine Schnittstellenbeschreibung für die Integration in die IT-Landschaft der Deutschen Bundesbank sowie eine Beschreibung der Konfigurationsmöglichkeiten (z.B. Prüfregelein, Parameter). Bei Anpassungen der Software muss der Auftragnehmer entsprechende „Release Notes“ mit einer transparenten Beschreibung der Änderungen mitliefern. Die Dokumentation muss in deutscher oder englischer Sprache zur Verfügung gestellt werden, wobei die Deutsche Bundesbank deutschsprachige Dokumentationsmaterialien bevorzugen würde.

2.3.4 Wartbarkeit

Der Auftragnehmer gewährleistet auch notwendige funktionale Anpassungen zusätzlich zu Wartungsarbeiten, die aus Vorkommnissen bezüglich der IT-Sicherheit resultieren (siehe Punkt 2.2.3). Die Software soll so gestaltet sein, dass Updates, Patches und Konfigurationsänderungen mit minimalem Aufwand durchgeführt werden können.

2.3.5 Testdatenscreening

Der Bieter erklärt sich bereit, den vom Auftraggeber zur Verfügung gestellten synthetischen Testdatensatz nach Aufforderung in seinen Systemen fristgerecht zu screenen und die Testergebnisse zur Verfügung zu stellen. In weiteren Verhandlungsrunden haben die ausgewählten Bieter die Möglichkeit ihre Systeme auf die Anforderungen des Auftraggebers einzustellen und zu konfigurieren. Die Testdaten sollten per E-Mail, auf einer CD oder einem vergleichbaren Datenträger, oder per Download von einer Webseite zur Verfügung gestellt werden.

2.3.6 Teststellung / Testinstallation

Der Auftragnehmer erklärt sich bereit, eine Teststellung in Form einer Testinstallation in den Systemen des Auftraggebers durchzuführen, um die technische Realisierbarkeit zu verifizieren. In welchem Umfang diese Testinstallation durchgeführt wird und welche Aspekte dabei betrachtet werden, ergibt sich aus der Beschreibung der technischen Ausgestaltung (ID 5.2). Die Testinstallation wird erst in der Verhandlungsphase durchgeführt.

3 Bewertungskriterien

3.1 Fachliche (funktionale) Anforderungen an den Screening-Kern

3.1.1 Erkennung von weiteren Entitäten

Die Software soll neben natürlichen und juristischen Personen, Organisationen und Einrichtungen auch weitere Entitäten (insbesondere Schiffe, Häfen, Schleusen und Flugzeuge) erkennen können.

3.1.2 Erkennung von Entitäten, bei abweichenden Schreibweisen (Fuzzy-Logik)

Die Software soll verschiedene Variationen eines Namens erkennen können, einschließlich abweichender Schreibweisen, Tippfehler, typischer OCR-Fehler, Transkriptionen, Abkürzungen, Auslassungen und phonetischer Ähnlichkeiten. Die Anforderung wird anhand der Testdaten und den Detailanforderungen unter 3.2 bewertet.

3.1.3 Hohe Sensitivität

Die Software soll beim Screening eine hohe Sensitivität aufweisen. Die Anforderung wird anhand der Testdaten unter 4. der Bewertungsmatrix bewertet.

3.1.4 Hohe Spezifität

Die Software soll beim Screening eine hohe Spezifität aufweisen. Die Anforderung wird anhand der Testdaten unter 4. der Bewertungsmatrix bewertet.

3.1.5 Verarbeitung von Zahlungsverkehrsnachrichten

Die Software soll Namen in SWIFT-, SEPA- und ggf. anderen Zahlungsverkehrsnachrichten direkt (ohne zusätzliche Datenstandardisierung) screenen können. Daher soll die Software alle gängigen SWIFT- und SEPA- und ggf. andere Formate (aktuelle und historische) verarbeiten können. Es soll einstellbar sein, welche Felder innerhalb von Zahlungsverkehrsnachrichten gescreent werden; der Auftragnehmer sichert zu, dass die Software bei Änderungen von Zahlungsverkehrsstandards flexibel angepasst werden kann; der Auftragnehmer sichert zu, dass die Software prinzipiell so konfiguriert oder erweitert werden kann, dass mögliche neue Nachrichtentypen oder Nachrichten weiterer Zahlungsverkehrssysteme gescreent werden können. Hierbei ist zu beachten, dass bei Zahlungsverkehrsnachrichten explizit keine Datenstandardisierung erfolgen soll.

3.1.6 Verarbeitung von unstrukturierten Daten

Zusätzlich zu 2.1.3 soll die Entitätensuche als (unscharfe) Volltextsuche in unstrukturierten Input-Daten (z.B. PDF-Dokumente) möglich sein. Das heißt es sollen auch abweichende Schreibweisen gefunden werden.

3.1.7 Natural language processing (NLP): Einbeziehung von weiteren Informationen

Die Software soll in der Lage sein, im Zusammenhang mit dem Namen auch weitere Informationen in das Screening einzubeziehen. Dazu gehören z. B.:

- Länderangaben,
- Geschlecht,
- Personenart,
- Meta-Daten (z. B. Adressen),

3.1.8 Geburtsdaten

Die Software soll in der Lage sein, im Zusammenhang mit dem Namen auch Geburtsdaten in das Screening einzubeziehen. Der Grad der Übereinstimmung der Geburtsdaten soll konfigurierbar sein. Wenn Geburtsdaten berücksichtigt werden, soll die Software neben dem gregorianischen Kalender verschiedene weitere Kalendersysteme aus Sanktionslisten (insbesondere EU-Verordnungen) korrekt erfassen, umwandeln und abgleichen können. Insbesondere der islamische Mondkalender als auch der islamische Sonnenkalender sollen verarbeitet werden können.

3.1.9 Einbeziehung von weiteren Informationen aus Sanktionslisten

Die Software soll in der Lage sein, unabhängig von Namen auch weitere Informationen in das Screening einzubeziehen. Dazu gehören z.B. Warenlisten, HS-Codes, ISINs, BICs oder andere Informationen aus den Daten der Geschäftsbanken, aus Sanktionslisten oder anderen Quellen.

3.1.10 Parametrisierbarkeit/Konfigurierbarkeit der Kontext-Daten

Die Einbeziehung von weiteren Informationen (siehe 3.1.7) soll parametrisierbar sein.

3.1.11 Unabhängiges Namensscreening

Die Ergebnisse aus dem Namensscreening sollen auch unabhängig von weiteren einbezogenen Informationen ausgegeben werden können.

3.1.12 Verarbeitung von nicht-lateinischen Alphabeten

Die Software soll insbesondere lateinische, kyrillische, arabische, persische, koreanische und chinesische Zeichen verarbeiten können. Die Verarbeitung von weiteren Alphabeten ist von Vorteil. Namen sollen sowohl getroffen werden können, wenn sie in der Originalschrift vorliegen, als auch wenn sie transkribiert wurden. Die Software soll flexibel ohne zusätzliche Kosten erweiterbar sein, so dass weitere Schriften getroffen werden können, wenn auf Grund von Änderungen im Sanktionsrecht Bedarf dazu vorhanden ist (z.B. Birmanisch).

3.1.13 Transparenz

Die Arbeitsweise des Screenings soll offengelegt, nachvollziehbar und plausibel sein. Die verwendeten Algorithmen sind zu erklären. Bei der Verwendung von KI-Modellen soll klar sein, welches Modell verwendet wird. Die Ergebnisse sollen grundsätzlich reproduzierbar sein.

3.1.14 Begründung der Scores

Die Software soll für jedes einzelne Ergebnis nachvollziehbar darstellen, wie der jeweilige Score im Detail ermittelt wurde. So sollen beispielsweise bei Verwendung unterschiedlicher Algorithmen alle Scores ersichtlich sein.

3.1.15 Verarbeitung unbegrenzter Zeichenmengen pro Datensatz

Die Software soll den gesamten Inhalt von Datenattributen screenen können, unabhängig von der Anzahl der enthaltenen Zeichen und dem übermittelten Datentyp. Auch sehr lange Feldinhalte sollen verarbeitet werden können.

3.1.16 Auswahl der zu screenenden Datenfelder

Die Software soll es ermöglichen, einzustellen welche und wie viele Datenfelder pro Datensatz gescreent werden sollen.

3.1.17 Verschiedene Konfigurierungen beim Screening einzelner Datenfelder

Die Software soll gezielt auch unterschiedliche Datenfelder mit verschiedenen Einstellungen screenen können, z.B. verschiedenen Gewichten, Parametern oder Algorithmen. Die Software soll gezielt gleiche Datenfelder auch mit verschiedenen Methoden screenen können.

3.1.18 Erkennung auch ohne externe Zuordnung zum Typ der Entität

Die Software soll sanktionierte Entitäten treffen, unabhängig davon, ob eine Entität in den zu prüfenden Daten überhaupt oder korrekt als natürliche oder juristische Person (bzw. Schleuse, Flugzeug, o.Ä.) ausgewiesen ist.

3.1.19 Häufige Namen

Die Software soll über geeignete Methoden zur Beschränkung falsch-positiver Treffer verfügen, die häufige Namen oder Namensbestandteile berücksichtigen.

3.1.20 Erkennung von verschiedenen Sprachen und differenzierte Verarbeitung

Die Software soll in der Lage sein, Namen aus verschiedenen Sprachen zu erkennen und Prüfregeln differenziert danach anzuwenden. Die Erkennung könnte sowohl nach dem Zeichensatz als auch nach z.B. dem Sanktionsregime erfolgen.

3.1.21 Benachrichtigung bei fehlenden, fehlerhaften, inkonsistenten, unerwarteten Daten

Die Software soll während des Screeningprozesses melden/ausgeben, wenn Auffälligkeiten der Inputdaten (z.B. leere Spalten, falsche Codierung) festgestellt wurden.

3.2 Detailanforderungen an den Screening-Kern

3.2.1 Groß- und Kleinschreibung

Die Software soll sanktionierte Entitäten auch dann treffen, wenn Groß- und Kleinschreibung von Zeichen abweichen.

3.2.2 Umlaute und Sonderzeichen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ihre Namen Umlaute, Sonderzeichen, Akzente, diakritische Zeichen usw. enthalten. Das gilt auch für typische Fehler, die im Zusammenhang mit

- Excel auftreten (z.B. ü → Ä^α);
- Umlauten in anderen Systemen auftreten, z.B. völliger Wegfall von Umlauten oder diakritischen Zeichen, Akzenten etc., Ersetzung durch Leerzeichen, Fragezeichen, Punkte oder Anführungsstriche.

3.2.3 Ergänzungen und Verdopplung von Zeichen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ein oder mehrere Zeichen hinzugefügt sind. Ergänzungen sollen nicht gleich gewichtet werden, besonders häufige Zusätze (z.B. Anführungsstriche, Bindestriche, Klammern) und Zusätze aus Zahlungsverkehrsnachrichten u.Ä. (z.B. 1/, // usw.) sollen ggf. nur gering oder gar nicht berücksichtigt werden.

3.2.4 Auslassung von Zeichen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ein oder mehrere Zeichen ausgelassen sind. Auslassungen sollen nicht gleich gewichtet werden, sondern z.B. nach ihrer Häufigkeit (z.B. fehlende Verdopplungen).

3.2.5 Phonetische Ähnlichkeiten / Transkriptionsvarianten

Die Software soll sanktionierte Entitäten auch dann treffen, wenn die Zeichenfolge an einer oder mehreren Stellen verändert ist. Besteht dabei eine phonetische Ähnlichkeit bzw. Transkriptionsvariante, soll die Abweichung geringer ins Gewicht fallen als bei anderen Abweichungen. Das gilt auch für phonetische Ähnlichkeiten in anderen Sprachen (z.B.: doppelte oder einzelne Buchstaben, i-ie, d-dt usw.).

3.2.6 Verarbeitung von einzelnen Zeichen anderer Alphabete

Bei Namen, die überwiegend im lateinischen Alphabet geschrieben sind, sollen Zeichen aus anderen Alphabeten erkannt werden und beim Abgleich durch die entsprechend lateinischen Zeichen ersetzt werden (z.B.: "B" und "В" in Latein und Kyrillisch). Das gilt entsprechend für Namen, die in anderen Alphabeten geschrieben werden und identisch aussehende Zeichen aus dem lateinischen Alphabet enthalten.

3.2.7 Direkte Verarbeitung von nicht-lateinischen Zeichen

Die Software soll in der Lage sein, nicht-lateinische Zeichen abzugleichen, ohne sie erst ins lateinische Alphabet zu transkribieren. Die sanktionsrelevanten Verordnungen der EU (und ggf. anderer Quelldokumente) enthalten neben lateinischen Buchstaben insbesondere Schriftzeichen des kyrillischen, koreanischen, chinesischen, arabischen und des erweiterten arabischen Alphabets sowie zahlreiche Sonder- und diakritische Zeichen. Diese sollen direkt verarbeitet werden können.

3.2.8 Transkription von nicht-lateinischen Zeichen

Die Software muss sanktionierte Entitäten auch dann treffen, wenn ihre Namen aus nicht-lateinischen Alphabeten transkribiert wurden oder von der Software transkribiert werden müssen. Dabei soll(en):

- nie nur ein einziger Transkriptionsstandard verwendet werden;
- transparent sein, welche Standards eingesetzt werden;
- auch der oder die amtlichen Transkriptionsstandards des Landes verwendet werden, dessen Identifikationsdokumente eine sanktionierte Person nutzen würde;
- die häufigsten in Deutschland gebräuchlichen Transkriptionsstandards verwendet werden;
- die weltweit am häufigsten gebrauchten Standards verwendet werden.

3.2.9 Verarbeitung nicht-lateinischer defektiver Schreibweisen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ihre Namen durch die Transkription aus Konsonantenschriften die dann üblichen Transkriptionsbesonderheiten aufweisen, z.B. bei Namen aus dem Arabischen, Farsi, Urdu und Paschtu. Dabei handelt es sich vor allem um die Auslassung von kurzen Vokalen und von Verdoppelungen, die Umschrift von Stimmabsätzen, die Assimilation und Anbindung von Artikeln.

3.2.10 Berücksichtigung von sprachspezifischen Besonderheiten von Namen

Die Software soll sprachliche Besonderheiten von Namen aus verschiedenen Sprachräumen sinnvoll zur Erhöhung der Trennschärfe in das Screening einbeziehen, z.B. über Häufigkeiten von Namen oder Namensbestandteilen.

3.2.11 Männliche vs. weibliche Namen

Die Software soll in der Lage sein, männliche und weibliche Namensformen bei natürlichen Personen zu erkennen, um dadurch die Zahl falsch-positiver Treffer zu verringern (Bsp. Amin Mohammed vs. Amina Mohammed).

3.2.12 Berücksichtigung besonders häufiger Fehler

Die Software soll sanktionierte Entitäten auch dann treffen, wenn die Zeichenfolge an einer oder mehreren Stellen verändert ist. In bestimmten Fällen sollen die Abweichungen geringer ins Gewicht fallen, insbesondere bei:

- typischen OCR-Fehlern,
- Buchstabendrehern,
- Zeichen, die auf benachbarten Tasten liegen (z.B. O-0),
- phonetischen Ähnlichkeiten

3.2.13 Auslassung von Namensbestandteilen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ein oder mehrere Namensbestandteile ausgelassen sind (insbesondere Vornamen, Familiennamen bzw. Teile von Familiennamen, Patronymie, Titel, akademische Grade oder entsprechend Bestandteile von Firmennamen oder Organisationen).

3.2.14 Abkürzung von Namensbestandteilen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ein oder mehrere Namensbestandteile abgekürzt sind. Das gilt in besonderem Maß für juristische Personen und für Rechtsformen, bei denen alle Namensbestandteile abgekürzt sein können.

3.2.15 Ergänzungen von Namensbestandteilen und Zusätzen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ein oder mehrere Namensbestandteile hinzugefügt sind, z.B.:

- weitere Vor- oder Familiennamen und Patronymie,
- Titel und Ehrenbezeichnungen, akademische Grade,
- Funktionsbezeichnungen, Amtsbezeichnungen usw.,
- Branchenbezeichnungen, geographische Begriffe usw.

Die Software soll sanktionierte Entitäten auch dann treffen, wenn einem Namen ein oder mehrere andere Zusätze beigelegt sind, z.B. Adressdaten, Erläuterungen, Codes (insbesondere bei juristischen Personen).

3.2.16 Namen verschiedener Personen in einer Zelle

Die Software soll sanktionierte Entitäten auch dann treffen, wenn sich die Namen von zwei oder mehreren natürlichen oder juristischen Personen in einer Zelle befinden, z.B. bei Ge-

meinschaftskonten oder in Zahlungsverkehrsdaten. Falls sich die Namen von zwei sanktionierten Personen, Organisationen und Einrichtungen in einer Zelle befinden, sollen beide angezeigt werden. Das gilt auch für angefügte Geburtsnamen oder frühere Namen von juristischen Personen (s. auch unstrukturierte Daten).

3.2.17 Trennzeichen: zusätzliche oder fehlende

Die Software soll sanktionierte Entitäten auch dann treffen, wenn ihre Namensbestandteile fehlerhaft getrennt sind (z.B. durch Leerzeichen, Zeilenumbrüche, Bindestriche, Punkte etc.), z.B. wenn Trennzeichen:

- ganz fehlen,
- teilweise fehlen,
- zusätzliche eingefügt sind,
- in größerer Zahl fehlen oder zusätzlich eingefügt sind und
- Kombinationen dieser Fehler vorliegen.

3.2.18 Sehr lange Namen

Die Software soll auch alle langen Namen aus den Sanktionslisten (insbesondere EU-Sanktionslisten) (mindestens 200 Zeichen) treffen.

3.2.19 Sehr kurze Namen

Die Software soll folgendes gewährleisten:

- ein Screening soll mindestens ab einschließlich 2 Zeichen möglich sein;
- die Mindestzahl der berücksichtigten Zeichen soll konfigurierbar sein;
- es soll auch nach einzelnen Zeichen (insbesondere UTF-8 Zeichen) gescreent werden können, z.B. in chinesischen Datensätzen.

3.2.20 Typische Abwandlungen

Die Software soll Namen auch dann finden können, wenn sie in typischer Weise abgewandelt sind, z.B. Koseformen wie: Sascha statt Alexander, Aleksandr oder Aleksaschka; Dima statt Dimitri oder Dmitrij; Kolja statt Nikolai oder Nikolaj usw.

Die Funktion soll in Abhängigkeit vom Sprachraum oder Sanktionsregime einstellbar sein.

Die Funktion soll nicht für Sprachen aus dem islamischen Kulturkreis eingesetzt werden, da dort Abwandlungen verbreiteter Namen als eigenständige Namen verwendet werden (z.B. Ahmed, Achmad u.a. von Muhammad).

3.2.21 Rechtsformen Erkennung und Verarbeitung

Die Software soll Rechtsformen erkennen und sinnvoll in die Bewertung integrieren, um die Qualität des Screenings zu erhöhen:

- Auch ausländische und fremdsprachliche Bezeichnungen sollen erkannt werden.

- Die Einstellungen sollen konfigurierbar sein.
- Es soll möglich sein, das Screening allein auf den Namenskern (ohne Rechtsform) anzuwenden oder alternativ die Ergebnisse so zu filtern, dass die Rechtsformen nicht berücksichtigt werden.
- Für die Verarbeitung der Rechtsformen sollen sinngemäß dieselben Anforderungen gelten, wie für das Treffen von Namen. Sie sollen z.B. auch dann erkannt werden, wenn Leerzeichen, Tippfehler, Abkürzungen usw. vorliegen. (z.B. Ltd., Ltd, limited, Limited usw.)
- Sehr ähnliche Bezeichnungen sollen dabei erkannt werden (z.B. Ltd., GmbH, OOO (d.h. eine „russische GmbH“) usw.)

3.2.22 Branchen- und geographische Bezeichnungen werden sinnvoll in das Screening einbezogen

Die Software soll Branchen- und geographische Bezeichnungen (z.B. Städtenamen, Länderangaben) erkennen und sinnvoll in das Scoring integrieren, um die Qualität des Screenings zu erhöhen:

- Auch ausländische und fremdsprachliche Bezeichnungen sollen erkannt werden.
- Die Einstellungen sollen konfigurierbar sein.
- Es soll möglich sein, das Screening allein auf den Namenskern anzuwenden oder alternativ die Ergebnisse so zu filtern, dass Branchen- und geographische Bezeichnungen nicht berücksichtigt werden.

3.2.23 Erkennung austauschbarer Bezeichnungen

Die Software soll erkennen können, wenn Unterschiede bei Namensbestandteilen auf sinngemäß gleiche oder sehr ähnliche Begriffe zurückgehen und dies bei der Bewertung der Ähnlichkeit berücksichtigen. Einige Begriffe, die hierunter fallen sind z.B. Handelsbank, Commercial Bank, Banque commerciale und Коммерческий банк. Die Software soll dabei konfigurierbar sein.

3.2.24 Erkennung von Namen trotz Kombination von Fehlern auf der Ebene von Zeichen und / oder Namensbestandteilen

Die Software soll sanktionierte Entitäten auch dann treffen, wenn sie an mehreren Stellen auf der Ebene der Zeichen und / oder der Namensbestandteile oder durch Zusätze verändert sind.

3.3 Technische Anforderungen

3.3.1 Implementierung der Software

3.3.1.1 Integration in ein Shared Cluster

Wird die Software in der Container-Umgebung betrieben, dann soll das Berechtigungskonzept mit einem mandantenfähigen Shared Cluster kompatibel sein und keine Berechtigungsvergabe auf Cluster-Ebene benötigen.

3.3.1.2 Konfiguration und Finetuning

Der Auftragnehmer soll Unterstützungsleistungen bei der Konfiguration von Prüfregeln und Parametern, die Durchführung von Tests zur Validierung der Konfiguration, Schnittstellen und der Datenkonsistenz sowie die Optimierung der Software für die Verarbeitung großer Datenmengen erbringen. Es sollen maximal 900 Millionen Datensätze in einem Batch-Lauf innerhalb von 5 Tagen verarbeitet werden können bzw. ca. 2.100 Transaktionsdatensätze pro Sekunde. Durchschnittlich sind ca. 15 Millionen Datensätze pro Batch-Lauf zu screenen. Die Daten sollen gegen eine Sanktionsliste mit ca. 200.000 Einträgen gescreent werden.

3.3.1.3 Simulationsumgebung

In der Software soll eine zusätzliche Simulationsumgebung existieren, um Konfigurationen verproben zu können.

3.3.2 Performance und Skalierbarkeit

Im vorliegenden Anwendungsfall sind die Datenmengen sehr variabel, insbesondere kommen große Datensätze selten vor, sollen aber aufgrund der Zukunftsfähigkeit der Software verarbeitet werden können.

3.3.2.1 Verarbeitung großer Datenmengen

Das Mengengerüst wird nach dem Teilnahmewettbewerb offengelegt, wenn eine entsprechende Verschwiegenheitserklärung (vgl. Dokument „T13_L1_Verschwiegenheitserklärung_25-2000064042_Los 1.docx“) unterzeichnet und mit dem Angebot eingereicht wurde.

3.3.2.2 Skalierbarkeit

Die Anwendung soll für die Verarbeitung großer Datenmengen temporär skalierbar sein (z. B. durch horizontale Skalierung). Die Software soll in der Lage sein, das 1,5-fache des Mengengerüsts zu verarbeiten, um zukünftige Anforderungen zu erfüllen.

3.3.2.3 Performance-Monitoring

Die Software soll zuverlässig und stabil arbeiten und ein integriertes Performance-Monitoring bieten, um die Systemleistung (z. B. Verarbeitungsgeschwindigkeit, Systemauslastung, Speicherverbrauch) kontinuierlich zu überwachen. Falls erforderlich sollen Optimierungsmaßnahmen zur Verbesserung der Effizienz vorgenommen werden.

In der Container-Umgebung der Deutschen Bundesbank erfolgt das IT-Monitoring mit der Anwendung Dynatrace.

3.3.2.4 Wiederaufnahme des Screenings nach Abbrüchen

Die Software soll in der Lage sein, nach Abbrüchen das Screening an der richtigen Stelle fortzusetzen, ohne dass das gesamte Screening neu durchlaufen muss.

3.3.2.5 Benachrichtigung bei Fehlern und Problemen

Die Software soll die Anwender der Software aktiv bei Abbrüchen, Fehlern und anderen Problemen benachrichtigen, sowie bei fehlenden, fehlerhaften, inkonsistenten und unerwarteten Daten.

3.3.3 IT-Sicherheit

Die verwendeten Kürzel bezeichnen die Abschnitte aus dem IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) der Edition 2023.³

3.3.3.1 Information bei IT-Schwachstellen (OPS.1.1.1.A20)

Der Auftragnehmer soll bei Bekanntwerden von IT-Sicherheitsschwachstellen sowie sicherheitsrelevanten Ereignissen bezogen auf die integrierten bzw. genutzten Technologien dem Auftraggeber diese Information inklusive marktüblicher Security-Einordnung (z.B. CVSS-Scoring) zur Kenntnis geben.

3.3.3.2 Konfiguration der Protokollierung auf System- und Netzebene (OPS.1.1.5.A3)

Der Auftragnehmer soll eine ausführliche Dokumentation zur Analyse der Log-Meldungen zur Verfügung stellen. Der Zugriff auf die Log-Files darf nur gesichert und nur durch besonders Berechtigte erfolgen.

3.3.4 Datenschutz

3.3.4.1 Restriktive Verwendung von Protokollierungsdaten

Es sollen keine User-bezogenen Reports erstellt werden können (wegen Mitbestimmung und Persönlichkeitsrechten). Der Zugriff auf User und personenbezogene Daten in den Logdateien ist restriktiv – nach dem Need-to-know Prinzip zu handhaben.

3.4 Übergeordnete Anforderungen

3.4.1 Release- und Änderungsdokumentation

In Ergänzung zu der in Abschnitt 2.3.3 beschriebenen Softwaredokumentation soll jede neue Version der Software mit einer detaillierten Release-Dokumentation ausgeliefert werden, in der die Änderungen, neue Funktionen und behobene Fehler beschrieben werden. Dies beinhaltet auch Hinweise zur Installation und Konfiguration von Updates.

³ Siehe: Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html; direkter Link: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

3.4.2 Benutzerfreundlichkeit

Die Software soll bei der Erlernbarkeit, Bedienbarkeit und Verständlichkeit ausreichend benutzerfreundlich sein, um Fehler bei der Software-Nutzung und Ergebnisauswertung unwahrscheinlich zu machen.

3.4.3 Barriere-Freiheit

Die Software soll die Anforderungen nach dem Behinderten- und Gleichstellungsgesetz (BGG) und der Barrierefreie-Informationstechnik-Verordnung (BITV 2.0) erfüllen.

3.4.4 Portabilität

Die Software soll an eine neue technische Infrastruktur angepasst werden können (Ggf. auch durch den Auftragnehmer).

3.4.5 Gleichstellungskonform

Die Software und alle bereitgestellten oder während der Vertragslaufzeit zugesandten Dokumente sollen im Sinne des Bundesgleichstellungsgesetzes (BGleG) die Gleichstellung von Frauen und Männern sprachlich zum Ausdruck bringen, wo dies möglich ist.