



Leistungsbeschreibung Fachprogramm für die Schuldner- und Verbraucherinsolvenzberatung

Die Verbraucherzentrale NRW beabsichtigt für ihre 12 anerkannten Verbraucherinsolvenzberatungsstellen ein neues Fachprogramm zur Bearbeitung der Fälle anzuschaffen.

Die in der Leistungsbeschreibung als Mindestanforderung gekennzeichneten Anforderungen sind vom Bieter zu erfüllen. Die als Wertungskriterien gekennzeichneten Anforderungen, die über die Mindestanforderungen hinausgehen werden nach Maßgabe der Bewertungsmatrix bewertet.

1. Hintergrund

Seit Einführung der Insolvenz-Ordnung in Deutschland bietet die Verbraucherzentrale NRW Schuldner- und Verbraucherinsolvenzberatung an. Derzeit in 12 anerkannten Stellen mit ca. 24 Beratungs- und 4 Verwaltungskräften. Zur Unterstützung der Beratung und verschiedener Berichtspflichten ist ein Fachprogramm unerlässlich.

2. Ziel

Das Fachprogramm soll die komplette Fallbearbeitung mit Aktenführung digital ermöglichen. Für die Nutzer soll die größtmögliche Anwenderfreundlichkeit gegeben sein. Cloudhosting und Wartung des Programms wird durch den Anbieter gewährleistet werden.

3. Aufgabenstellung

Das Fachprogramm dient der Bearbeitung eines Falles von der Aktenanlage, über Stellen des Insolvenzantrags bis zur Auswertung und Abgabe der Statistik an Destatis ermöglichen. Insbesondere sind folgende Funktionalitäten erforderlich (**Mindestanforderungen**):

- Erfassung von Gläubiger – und Schuldnerdaten
- Forderungs – und Gläubigerverzeichnis
- Erstellen von Plänen und Musterbriefen
- Kommunikation mit Schuldnern und Gläubigern per E-Mail
- umfassende Erstellung des Antrags auf Eröffnung der Verbraucherinsolvenz
- Schnittstelle zu Destatis zur Versendung der Bundesstatistik
- Praktikables Benutzerhandbuch
- Einführungsschulungen an mehreren Terminen
- Regelmäßige Wartung und Updates

- Service-Hotline zu üblichen Dienstzeiten erreichbar
- Microsoft Edge ist als perspektivischer Standardbrowser vollständig zu unterstützen.
- Verschlüsselung sämtlicher Verbindungen zwischen Client und Cloud-Dienst mittels aktueller TLS-Versionen.
- Verschlüsselung ruhender Daten in der Cloud-Applikation.
- Betrieb der Datenverarbeitung mindestens in Rechenzentren innerhalb der Europäischen Union, vorzugsweise in Deutschland.
- Offenlegung sämtlicher Datenstandorte und Unterauftragnehmer.
- Abschluss einer Vereinbarung zur Auftragsverarbeitung, sofern personenbezogene Daten verarbeitet werden.
- Bereitstellung geeigneter Nachweise zur Informationssicherheit, zum Beispiel ISO-27001-Zertifizierung, SOC-2-Berichte oder vergleichbare Prüfberichte.
- Regelmäßige Schwachstellenprüfungen oder Penetrationstests.
- Dokumentierte Verfahren zum Umgang mit Sicherheitsvorfällen.
- Unterstützung zentral auswertbarer Audit- und Protokolldaten.

Folgende Kriterien sind wünschenswert (**Wertungskriterien**):

- Zentrale Adressdatenbank mit Konsolidierungsfunktion
- Versendung von Serienbriefen per E-Mail
- Adminfunktion, z.B. zum Anlegen von Benutzern bzw. Wechsel von Benutzern in andere Beratungseinheiten bei Bedarf - zur Vertretung auch außerhalb der eigenen Beratungsstelle
- Einfaches Einpflegen von Klientendokumenten in das Programm
- Bedarfsorientierte Auswertungen
- Bei Bedarf Schnittstellen zum Gericht/ Insolvenzverwalter ermöglichen – Stichwort Behördenpostfach
- zentrale Zuweisung von Änderungen z. B. in Textbausteinen/Musterbriefen sollte möglich sein
- Löschfunktion gemäß DSGVO
- Nach Möglichkeit Unterstützung von **Customer Managed Keys** oder **Bring Your Own Key**, insbesondere bei besonders schutzbedürftigen Daten.

4. Eignungskriterien

4.1 Erfahrung mit der Betreuung von Organisationen mit mehreren Standorten

Der Bieter muss über nachweisbare Erfahrung mit der Bereitstellung und Betreuung eines mit dem ausgeschriebenen Fachprogramm vergleichbaren Systems für Organisationen mit mehreren Standorten sowie über entsprechende Erfahrung in der Betreuung einer größeren Anzahl von Anwenderinnen und Anwendern verfügen.

Hierzu sind mindestens folgende Anforderungen zu erfüllen:

Der Bieter weist mindestens eine vergleichbare Referenz über die Bereitstellung und Betreuung einer Fachanwendung für einen Vertragspartner mit mindestens **fünf räumlich getrennten Standorten** nach. Zusätzlich weist er anhand dieser Referenz oder weiterer Referenzen nach, dass er innerhalb der letzten drei Jahre insgesamt mindestens **50 Anwenderinnen und Anwender** solcher Anwendungen über jeweils mindestens 6 Monate betreut hat.

Für jede herangezogene Referenz sind Auftraggeber, Leistungsgegenstand, Leistungszeitraum, Zahl der betreuten Standorte und Zahl der betreuten Anwenderinnen und Anwender anzugeben. Noch laufende Aufträge können berücksichtigt werden, wenn die maßgebliche Leistung bei Ablauf der Angebotsfrist seit mindestens sechs Monaten erbracht wird

4. 2 Nachweise zur Informationssicherheit

Der Bieter muss geeignete Nachweise zur Informationssicherheit, zum Beispiel ISO-27001-Zertifizierung, SOC-2-Berichte oder vergleichbare Prüfberichte vorlegen. Aus dem Nachweis müssen der geprüfte Geltungsbereich, der Prüfzeitraum bzw. die Gültigkeit und der Bezug zu den angebotenen Hosting- und Betriebsleistungen hervorgehen

5. Anzahl Lizenzen

Insgesamt werden **30 Lizenzen** (inklusive einer Lizenz für die Fachabteilung – nur zu Testzwecken, keine echte Klientenbearbeitung) benötigt. Unter der Annahme, dass mit einer Lizenz an zwei Standorten gearbeitet werden kann.

6. Technische Umgebung

Anforderungen an die Integration fremdgehosteter Cloud-Applikationen

Fremdgehostete Cloud-Applikationen müssen sich in die bestehende und perspektivisch geplante IT-Zielarchitektur des Auftraggebers integrieren lassen. Die Unternehmensstrategie sieht mittelfristig eine weitgehende Verlagerung von Infrastruktur, Identitäten, Kommunikationsdiensten und Daten in Richtung **Microsoft Azure** und **Microsoft 365** vor. Lösungen sind daher so auszuwählen und bereitzustellen, dass eine spätere vollständige Integration in diese Zielarchitektur ohne grundlegende Neuimplementierung möglich ist.

Cloud-Applikationen sollen bevorzugt als reine browserbasierte Anwendungen bereitgestellt werden. Zusätzliche Clientinstallationen, Browser-Plug-ins oder lokale Komponenten sind möglichst zu vermeiden und bedürfen einer gesonderten Begründung.

Identitäts- und Zugriffsmanagement

Die Cloud-Applikation muss perspektivisch an die zentrale Benutzerverwaltung des Auftraggebers angebunden werden können. Zielsystem für die zentrale Authentifizierung und Benutzerverwaltung ist **Microsoft Entra ID**.

Die Anbindung muss mindestens über eines der etablierten Standardverfahren **SAML 2.0** oder **OpenID Connect/OAuth 2.0** möglich sein. Eine proprietäre oder ausschließlich anbieterinterne Authentifizierungslösung ist nur als temporäre Übergangslösung zulässig.

Die Lösung muss folgende Anforderungen erfüllen:

- Unterstützung von **Single Sign-on** über Microsoft Entra ID.
- Unterstützung rollen- und gruppenbasierter Berechtigungen.
- Möglichkeit zur automatisierten oder teilautomatisierten Benutzerbereitstellung, zum Beispiel über **Just-in-Time-Provisioning** oder vergleichbare Verfahren.
- Kompatibilität mit Microsoft-Mechanismen wie **Conditional Access**, insbesondere zur Durchsetzung von Mehr-Faktor-Authentifizierung, Standort- oder Gerätekontexten.
- Nachvollziehbare Trennung von Benutzeridentität, Rolle und Berechtigung innerhalb der Anwendung.

Übergangsstrategie bei initial fehlender Entra-ID-Anbindung

Sollte eine direkte Anbindung an Microsoft Entra ID zum Zeitpunkt der Einführung noch nicht möglich sein, muss der Anbieter eine belastbare Übergangsstrategie bereitstellen.

Für diesen Übergangsbetrieb gelten folgende Mindestanforderungen:

- Die Cloud-Applikation darf temporär eine autarke Benutzerverwaltung verwenden, sofern diese technisch und organisatorisch abgesichert ist.
- Bereits bei der initialen Anlage der Benutzer muss sichergestellt werden, dass ein späterer Wechsel auf Microsoft Entra ID **ohne Neuanlage der Benutzerobjekte** möglich ist.
- Die Benutzerobjekte müssen eindeutig auf spätere Entra-ID-Identitäten abbildbar sein, beispielsweise über UPN, E-Mail-Adresse oder eine andere stabile eindeutige Kennung.
- Benutzerrollen, Berechtigungen, Historien, Auditdaten und personenbezogene Zuordnungen müssen beim späteren Wechsel auf die zentrale Benutzerverwaltung erhalten bleiben.
- Für die Übergangszeit ist zwingend eine **autarke Mehr-Faktor-Authentifizierung** innerhalb der Cloud-Applikation bereitzustellen.
- Die autarke Benutzerverwaltung ist als befristete Übergangslösung zu betrachten und muss durch den Anbieter technisch dokumentiert werden.
- Der Anbieter hat darzustellen, wie der spätere Schwenk auf Microsoft Entra ID erfolgt, welche Voraussetzungen dafür erfüllt sein müssen und welche Auswirkungen dies auf bestehende Benutzerkonten, Rollen und Berechtigungen hat.

Eine dauerhafte autarke Benutzerverwaltung ist aus Sicherheits- und Betriebsgründen nicht Zielbild des Auftraggebers.

Zugriff durch Clients und Browser

Der Zugriff auf die Cloud-Applikation muss grundsätzlich über einen verschlüsselten Browserzugriff erfolgen. Die Kommunikation zwischen Client und Cloud-Applikation muss ausschließlich über aktuelle, sichere TLS-Verfahren erfolgen.

Folgende Anforderungen gelten:

- Zugriff ausschließlich über **HTTPS/TLS**.
- Unterstützung des jeweils aktuellen **Microsoft Edge** als strategischem Standardbrowser.
- Unterstützung der **Mozilla Firefox Consumer-Variante** als Alternativbrowser.
- Keine zwingende Installation zusätzlicher lokaler Clientsoftware.
- Keine zwingende Nutzung von Browser-Plug-ins oder unsignierten Erweiterungen.

- Kompatibilität mit Windows-11-Clients.
- Unterstützung einer zentralen Browserkonfiguration über vorhandene Softwareverteilungs- und Richtlinienmechanismen.

Microsoft Edge ist als perspektivischer Standardbrowser vollständig zu unterstützen. Einschränkungen im Betrieb mit Edge sind vom Anbieter offenzulegen.

Mailgateway und Mailarchivierung

Die Cloud-Applikation muss sich in die bestehende E-Mail-Infrastruktur und die vorhandenen Archivierungsprozesse integrieren lassen.

Das bestehende Mailgateway bzw. die vorhandene Mailarchivierung ist weiterhin zu berücksichtigen. Aktuell eingesetzte Archivierungslösungen, insbesondere **Reddoox**, müssen weiterhin angebunden bzw. berücksichtigt werden können.

Perspektivisch ist eine Integration in **Exchange Online** vorgesehen. Der Anbieter muss daher darstellen, wie die Cloud-Applikation mit Exchange Online, zentraler Mailarchivierung und gegebenenfalls Journaling- oder Archivschnittstellen zusammenwirkt.

Folgende Punkte sind zu berücksichtigen:

- Sicherstellung der bestehenden Mailarchivierung.
- Anbindung an das vorhandene Mailgateway.
- Perspektivische Kompatibilität mit Exchange Online.
- Unterstützung nachvollziehbarer Mailflüsse.
- Dokumentation relevanter Schnittstellen, Weiterleitungen, Journaling-Mechanismen oder API-basierten Archivierungsverfahren.
- Keine Umgehung bestehender Archivierungs- oder Compliance-Anforderungen durch direkte, nicht nachvollziehbare Mailzustellung.

Sicherheit und Compliance

Die Cloud-Applikation muss dem aktuellen Stand der Technik hinsichtlich Informationssicherheit, Datenschutz und Compliance entsprechen.

Mindestens folgende Anforderungen sind zu erfüllen:

- Verschlüsselung sämtlicher Verbindungen zwischen Client und Cloud-Dienst mittels aktueller TLS-Versionen.
- Verschlüsselung ruhender Daten in der Cloud-Applikation.
- Betrieb der Datenverarbeitung mindestens in Rechenzentren innerhalb der Europäischen Union, vorzugsweise in Deutschland.
- Offenlegung sämtlicher Datenstandorte und Unterauftragnehmer.
- Abschluss einer Vereinbarung zur Auftragsverarbeitung, sofern personenbezogene Daten verarbeitet werden.
- Regelmäßige Schwachstellenprüfungen oder Penetrationstests.
- Dokumentierte Verfahren zum Umgang mit Sicherheitsvorfällen.
- Unterstützung zentral auswertbarer Audit- und Protokolldaten.

Sofern der Auftraggeber regulatorischen Anforderungen wie NIS2, DORA oder branchenspezifischen Compliance-Vorgaben unterliegt, muss der Anbieter darlegen, wie die Lösung diese Anforderungen unterstützt.

Netzwerk und Perimeterschutz

Der Anbieter muss dokumentieren, wie die Cloud-Applikation netzwerkseitig erreichbar ist und welche Sicherheitsmechanismen zur Absicherung des Zugriffs bestehen.

Folgende Anforderungen sind zu berücksichtigen:

- Dokumentation aller benötigten Zieladressen, Ports, Protokolle und Dienste.
- Unterstützung des Betriebs hinter bestehenden Proxy- oder Firewall-Infrastrukturen.
- Möglichkeit zur Einschränkung des Zugriffs über IP-Adressbereiche, sofern fachlich und technisch sinnvoll.
- Nach Möglichkeit Unterstützung privater oder eingeschränkter Anbindungsmodelle, zum Beispiel über dedizierte Endpunkte oder vergleichbare Sicherheitsmechanismen.
- Keine unkontrollierte Kommunikation der Clients mit unbekannten Drittzielen.
- Bereitstellung einer vollständigen Übersicht über externe Abhängigkeiten, CDN-Dienste, APIs und Drittanbieterkomponenten.

DNS-, Proxy- und Zertifikatsanforderungen sind durch den Anbieter vollständig zu dokumentieren.

Datenintegration, Schnittstellen und Exit-Strategie

Die Cloud-Applikation muss über dokumentierte Schnittstellen verfügen, um Datenintegration, Auswertung, Migration und spätere Ablösung der Lösung sicherzustellen.

Folgende Anforderungen gelten:

- Bereitstellung dokumentierter APIs oder Exportfunktionen.
- Unterstützung strukturierter Exportformate wie CSV, JSON, XML oder vergleichbarer offener Formate.
- Export von Stamm-, Bewegungs-, Konfigurations- und Protokolldaten, soweit fachlich relevant.
- Erhalt von Metadaten, Zeitstempeln, Benutzerzuordnungen und Historien.
- Dokumentation von Limits, API-Versionen, Authentifizierungsverfahren und Änderungshistorien.
- Rechtzeitige Ankündigung von API-Änderungen oder Abkündigungen.
- Sicherstellung eines vollständigen Datenexports bei Vertragsende oder Anbieterwechsel.

Der Anbieter muss ein nachvollziehbares Exit-Konzept bereitstellen. Dieses muss beschreiben, wie Daten vollständig, lesbar, strukturiert und innerhalb eines angemessenen Zeitraums aus der Cloud-Applikation exportiert werden können.

Backup, Wiederherstellung und Notfallvorsorge

Für die Cloud-Applikation ist ein anpassbares und nachvollziehbares Backupkonzept bereitzustellen.

Das Backupkonzept muss mindestens folgende Punkte umfassen:

- Regelmäßige Sicherung relevanter Daten und Konfigurationen.

- Definition von Sicherungsintervallen.
- Definition von Aufbewahrungszeiten.
- Schutz vor versehentlicher oder absichtlicher Löschung.
- Möglichkeit zur Wiederherstellung einzelner Objekte oder Datenstände, sofern technisch möglich.
- Beschreibung von Wiederherstellungsprozessen.
- Angabe von Recovery Time Objective und Recovery Point Objective.
- Regelmäßige Tests der Wiederherstellbarkeit.

Backups sollen logisch und organisatorisch so abgesichert sein, dass ein kompromittiertes Administratorkonto nicht ohne Weiteres zur vollständigen Löschung von Produktivdaten und Sicherungen führen kann.

Verfügbarkeit, Betrieb und Lifecycle

Der Anbieter muss die Betriebs- und Verfügbarkeitsanforderungen der Cloud-Applikation transparent beschreiben.

Folgende Punkte sind mindestens darzustellen:

- Service Level Agreement zur Verfügbarkeit.
- Geplante Wartungsfenster.
- Kommunikationswege bei Störungen.
- Reaktions- und Wiederherstellungszeiten.
- Eskalationswege.
- Release- und Änderungsmanagement.
- Vorankündigung wesentlicher Funktionsänderungen.
- Vorankündigung sicherheits- oder schnittstellenrelevanter Änderungen.
- Dokumentation von bekannten Einschränkungen.

Bitte legen Sie uns ein Angebot für 30 Lizenzen (inklusive Fachabteilung) sowie Cloudhosting für 12 Standorte vor. Die Lizenz der Fachabteilung soll nur zu Test- und Schulungszwecken dienen.

7. Zeit- und Ablaufplanung

Gewünschter Ablauf ca.

Bereitstellung des Fachprogramms	spätestens bis 31.12.2026
Datenmigration von Tau Office – soweit möglich	Zieltermin bis 31.12.2026
Schulung der Beratungskräfte	1. Quartal 2027, bevorzugt Januar/ Februar

8. Zuschlagskriterien

Der Zuschlag wird auf das wirtschaftlichste Angebot aufgrund der nachstehenden Kriterien und Gewichtung erteilt.

Kriterien:

- Preis 30 %
- Leistung 70 % (siehe Bewertungsmatrix)

Als Bewertungsmethode wird die "Lineare Interpolation mit dem zweifachen niedrigsten Angebotspreis" angewandt. Weitere Informationen zur Bewertungsmethodik entnehmen Sie bitte der beigefügten "Allgemeinen Erläuterung zur Bewertungsmethodik".

Das wirtschaftlichste Angebot ist das Angebot mit der höchsten Punktzahl aus den Kriterien Angebotspreis und Leistung.

Kriterien:

- Passgenauigkeit mit den Zuschlagskriterien der Aufgabenbeschreibung der Leistungsbeschreibung (40%),
- Technische Umgebung (30%),
- Support und Service (30%).

9. Vertrag und Rechnungsstellung

Nach Angebotsannahme wird ein EVB-IT Vertrag geschlossen, der die beiderseitigen Rechte und Pflichten vereinbart.

Eine Preiserhöhung um bis zu 10 % ist im Abstand von jeweils zwei Jahren zulässig, sofern die Notwendigkeit der Preisanpassung vom Auftragnehmer nachvollziehbar nachgewiesen wird, beispielsweise aufgrund gestiegener Personal- oder Ressourcenkosten.

Die Rechnung wird unter Angabe der Auftragsnummer in digitaler Form erbeten an:
rechnung@verbraucherzentrale.nrw und in Kopie an kredit@verbraucherzentrale.nrw