BUNDESRECHTSANWALTSKAMMER

Anlage Nr. 2

LEISTUNGSBESCHREIBUNG

Übernahme, Weiterentwicklung und Betrieb des Systems besonderer elektronischer Anwaltspostfächer

Bundesrechtsanwaltskammer (BRAK)

[redacted]

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung weiblicher, männlicher und diverser Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten für Personen jeglichen Geschlechts.

Inhaltsverzeichnis

1. Rahmenbedingungen

1.1 Beschreibung des Projektes

Die Bundesrechtsanwaltskammer (BRAK) hat nach § 31a Abs. 1 Bundesrechtsanwaltsordnung (BRAO) für jedes im Gesamtverzeichnis gem. § 31 BRAO eingetragene Mitglied einer Rechtsanwaltskammer ein besonderes elektronisches Anwaltspostfach (beA) empfangsbereit einzurichten. Dazu hat sie das beA als Kommunikationsplattform für den Austausch von Nachrichten zwischen Rechtsanwälten, Syndikusrechtsanwälten und der Justiz sowie Behörden und Rechtsanwälten bzw. Syndikusrechtsanwälten untereinander entwickeln lassen (vgl. Umsetzungsfeinkonzept beA-Anwendung, Kapitel 3.6). Sie betreibt das beA-System produktiv seit dem 28.11.2016. Der Gesetzgeber hat seither den Nutzerkreis erweitert. So hat die BRAK beA auch für solche europäische dienstleistende Rechtsanwälte einzurichten, die dies bei der für sie zuständigen Rechtsanwaltskammer beantragen.

Derzeit hat die BRAK zwei Verträge mit Dienstleistern für die zu erbringenden Leistungen abgeschlossen. Der EVB-IT-Erstellungsvertrag regelt die Leistungen für Entwicklung, Weiterentwicklung, Wartung, Pflege und Third-Level-Support der Software. Der Betriebsvertrag enthält die Leistungen für den Betrieb des beA einschließlich der Bereitstellung eines Anwender-Supports für den First- und Second-Level-Support.

Beide Verträge enden zum 31.12.2019, sodass die BRAK in der Pflicht steht, die Leistungen rund um die Weiterentwicklung, Wartung, Pflege und Support der Software sowie den Betrieb des beA und den Anwender-Support neu auszuschreiben. Die Laufzeit neuer vertraglicher Vereinbarungen beginnt am 01.01.2020 und endet am 31.12.2024.

Das System muss technikoffen und zukunftssicher sein. Bei der Weiterentwicklung soll geprüft werden, ob und in welchem Umfang Open-Source-Komponenten Verwendung finden können.

Während derzeit die Rechtsanwälte über beA nur empfangsbereit sein, aber nicht senden müssen, fällt in die Leistungsphase der Übergang in die aktive Nutzungspflicht spätestens ab dem 01.01.2022. Das bedeutet, dass ab dann Gerichte Papier von Rechtsanwälten nicht mehr annehmen werden, sondern dass die Nutzung des elektronischen Rechtsverkehrs über beA die einzige Möglichkeit der rechtskonformen Kommunikation sein wird.

Es besteht ein sehr hohes Interesse der Nutzer an einem System mit nutzerfreundlicher Bedienschnittstelle und geringen Anforderungen an den technischen Sachverstand des Anwenders (Postfachinhaber wie auch seine nichtjuristischen Mitarbeiter). Die Vorgaben des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten und die unverändert geltenden verfahrens- und berufsrechtlichen Vorschriften müssen eingehalten werden. Dazu zählen nach derzeitiger Rechtslage im Besonderen:

- §§ 130a, 130c, 130d, 174 Abs. 3 und 4 Zivilprozessordnung – ZPO (zu erschließen über www.gesetze-im-internet.de),[1]
- §§ 13, 14, 30, 31a, 47, 53, 55 Bundesrechtsanwaltsordnung – BRAO (zu erschließen über www.gesetze-im-internet.de),

[1] Vgl. Vorschriften finden sich auch in den Prozess- und Verfahrensordnungen der freiwilligen Gerichtsbarkeit und der Fachgerichtsbarkeiten.

- Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer – RAVPV (zu erschließen über www.gesetze-im-internet.de),
- Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV (zu erschließen über www.gesetze-im-internet.de),
- Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt – eIDAS-VO (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910),
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG DSG-VO (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679).

Die Nutzer des Systems sind insbesondere Rechtsanwälte, Syndikusrechtsanwälte, ihre nicht juristischen Mitarbeiter in den Kanzleien und Rechtsabteilungen, Zustellungsbevollmächtigte, Abwickler und Vertreter. Der Rechtsanwalt als Postfachbesitzer kann anderen Personen unterschiedlich ausgestaltete Berechtigungen für sein Postfach einrichten. Dies können zum Beispiel andere Rechtsanwälte oder Mitarbeiter sein. Ein Berechtigungs- und Rollenkonzept für das System bildet diese Sachverhalte ab (vgl. Feinkonzept beA-Anwendung). Weitere Beteiligte, wie zum Beispiel die BRAK, die Rechtsanwaltskammern (RAKn), die Anwaltsgerichte besitzen sog. Organisationspostfächer und sind in dem System erreichbar. Der Kreis der Nutzer muss erweiterbar sein.

Das beA-System (vgl. Kapitel 3.6) besteht aus einer Java-basierten Individualsoftware sowie Drittprodukten wie den Governikus Service Components, welche speziell für den sicheren und rechtsverbindlichen Austausch via OSCI-Standard entwickelt wurden. Die Verwaltung der Identitäten im beA erfolgt in einer SAFE-Domain. Für den Empfang von Nachrichten von der Justiz kommt ein OSCI-Intermediär zum Einsatz. Darüber hinaus verwendet das beA die Schnittstellen der OSCI-konformen Intermediäre der Justiz zum Nachrichtenversand an Postfächer der Justiz. Der Austausch strukturierter Daten mit den Teilnehmern am elektronischen Rechtsverkehr erfolgt unter Verwendung des XJustiz-Strukturdatensatzes. Die Governikus Service Components ermöglichen ferner eine sichere Nutzung der Schnittstellen zur Verzeichnisabfrage bzw. zum domainübergreifenden Verzeichnisdienst, dem Virtuellen Attribut Service (VAS) im EGVP-Verbund.

Der Benutzerzugriff auf das beA erfolgt einerseits über eine Webanwendung. Andererseits stellt das System eine Webservice-Schnittstelle bereit, die es insbesondere den Herstellern von Kanzlei-Software-Produkten und sonstigen Fachanwendungen ermöglicht, die wesentlichen Funktionen des beA, den Zugriff auf das Postfach, die dazugehörigen Nachrichten sowie die Administration des Postfachs, in ihre Produkte zu integrieren. Die Webanwendung nutzen insbesondere diejenigen, die in ihren Kanzleien/Rechtsabteilungen keine Fachsoftware einsetzen; dies sind nach Kenntnis der BRAK etwa die Hälfte aller Nutzer. Indes setzen auch Nutzer mit Fachanwendungen auf die Webanwendung des beA-Systems. Die Einzelheiten ergeben sich aus dem Umsetzungsfeinkonzept Kanzleisoftware-Schnittstelle und dem Kanzleisoftware-Toolkit.

Aus der anwaltlichen Verschwiegenheitsverpflichtung, aus den besonderen berufsrechtlichen Rahmenbedingungen der Anwaltschaft sowie aus den zuvor aufgeführten gesetzlichen Grundlagen heraus ergeben sich höchste Anforderungen an Informationssicherheit, Datenschutz und Verfügbarkeit. Der Nutzer muss sich darauf verlassen können, dass Nachrichten auf dem Übertragungsweg nicht unbemerkt verändert werden können. Daher muss die Übermittlung einer Nachricht nachweisbar manipulationsfrei erfolgen.

Der Rechtsanwalt muss sich zur Wahrung seiner Pflicht zur Verschwiegenheit weiterhin darauf verlassen können, dass die Nachricht auf dem Weg zu seinem Postfach von niemandem zur Kenntnis genommen werden konnte. Nachrichten müssen durchgängig verschlüsselt sein. Dies gilt genauso für den umgekehrten Weg, also aus dem Postfach des Rechtsanwalts zur Justiz oder zu einem anderen Beteiligten. In jedem Fall müssen die Inhalte des Postfachs vor dem Zugriff Unbefugter sicher sein.

Um dieses Sicherheitsniveau für das beA-System umzusetzen, ließ die BRAK eine Reihe von Maßnahmen implementieren, z. B. eine Zwei-Faktor-Authentifizierung bei der Anmeldung (§ 31a BRAO) sowie die Nutzung von Hardware-Kryptomodulen für die Verschlüsselung (vgl. technische Systembeschreibung nebst Anlagen, secunet-Gutachten).

In dem System erfolgt die Inbesitznahme des Postfachs mit Hilfe einer Signaturkarte, die auf Antrag des Postfachinhabers ausschließlich die Zertifizierungsstelle der Bundesnotarkammer (BNotK) ausstellt. Nach der Inbesitznahme erfolgt die Anmeldung am System ebenfalls durch eine Zwei-Faktor-Authentifizierung mit Hilfe der Signaturkarte oder über sonstige Zugangs-Token inkl. Softwarezertifikaten, die im System eingebunden sind (vgl. Fachkonzept Client Security).

Das System der beA berücksichtigt verschiedene Übermittlungsarten: Elektronische Dokumente können entweder qualifiziert elektronisch signiert aus dem beA oder einfach signiert bei „eigener Anmeldung des Berufsträgers“ aus dem beA versandt werden (§ 130a Abs. 3 ZPO – sicherer Übermittlungsweg). Den Nachweis über die Nutzung des sicheren Übermittlungswegs gewährleistet der mit den Stellen der Justiz abgestimmte sogenannte VHN =„vertrauenswürdige Herkunftsnachweis“ (vgl. Grobkonzept beA-Anbindung).

Das beA-System bietet zudem weitere Dienste und Schnittstellen an. So wird unter anderem die Kammersoftware der RAKn über einen RESTful Web Service, das Bundesweite Amtliche Anwaltsverzeichnis (BRAV) per Webservice (SPML), das europäische Suchportal für Anwälte (FAL; „Europäisches Justizportal“, https://e-justice.europa.eu/fal/) per Webservice sowie ein Trustcenter über zwei SOAP-Schnittstellen angebunden (vgl. Kapitel 3.6).

Derzeit gilt Folgendes:

Die Daten werden in einem Oracle Real Application Cluster (RAC) gespeichert. Alle Komponenten des beA-Zentralsystems sind Cluster-fähig und werden verteilt in georedundanten Rechenzentren betrieben. Damit ist ein synchroner Betrieb, z. B. als Oracle-RAC, möglich. Die Lastverteilung der vier installierten Produktionslinien (je zwei pro Rechenzentrum) erfolgt über Load-Balancer. Die teilweise virtualisierten Anwendungsserver sind auf mehrere Sub-Netze verteilt. Die Schnittstellen sind auf Sub-Domänen aufgeteilt und werden über (Anwendungs-)Firewalls und Intrusion Prevention Systeme überwacht und geschützt. Neben der Produktionsumgebung (PROD) werden eine Testumgebung für Integrations- und Last-Tests (STA) und eine Schulungs- und Partnertestumgebung (SPT) als Pre-Produktion mit entsprechend geringeren Ressourcen bereitgehalten (vgl. zu vorstehendem Absatz die Betriebsdokumentationen).

Im Rahmen der Entwicklungs- und Betriebsleistungen muss der Auftragnehmer (AN) einen stabilen, hochperformanten und störungsarmen Betrieb des beA-Systems unter Einhaltung der besonderen Anforderungen von höchster Integrität, Verfügbarkeit und Vertraulichkeit der anwaltlichen Daten und Informationen sicherstellen.

Er muss insbesondere sicherstellen, dass

- höchste Verfügbarkeit des beA-Systems,
- eine kurze Entstörungsdauer bei auftretenden Fehlern,
- eine umfängliche Unterstützung der Nutzer bei Problemen und in der Handhabung des beA,
- eine verlustarme Zusammenarbeit mit den IT-Supporteinheiten auf Entwicklungsebene,
- eine hohe Akzeptanz für die Nutzung des beA-Systems,
- eine vollständige Vermeidung von Sicherheitsvorfällen durch proaktive bzw. prädikative Einleitung von Maßnahmen

im laufenden Betrieb des beA-Systems erreicht werden.

Zu den Leistungen, die im Rahmen des Vertrages zu erbringen sein werden, gehören insbesondere:

- Weiterentwicklung des Systems und der Architektur auf Basis neuer Anforderungen, Skalierungsbedürfnisse, Performanz- sowie Sicherheitsanforderungen und/oder technischer Entwicklungen,
- Integration der Individualsoftware-Komponenten mit den eingesetzten Dritt-Produkten in die bestehende und sich weiterentwickelnde Test- und Betriebsumgebung und den EGVP-Verbund inklusive der genutzten Sicherheits-Infrastrukturen,
- Integration in vorhandene Deployment-Umgebungen für Software- und Konfigurationsauslieferungen an der Schnittstelle zum Betrieb,
- Pflege und Wartung der Software,
- User-Dokumentation des beA entsprechend anerkannten Standards, beispielsweise ISO/IEC 26514:2008 und/oder ISO/IEC 26515:2018,
- Bereitstellung der erforderlichen Informationen für Diagnose und Support (Alarme, Log Files, Counter) von funktionalen und nichtfunktionalen Problemen in den Test- und Betriebsumgebungen,
- Bereitstellung und 24/7-Betrieb eines hochverfügbaren, georedundanten Rechenzentrums in Deutschland einschließlich der erforderlichen Rechenzentrum-Infrastruktur und Datenbanken,
- Bereitstellung und Betrieb der notwendigen Storage-, Backup- und Recovery-Infrastruktur gemäß den Verfügbarkeitsanforderungen an die Server-Infrastruktur,
    - Bereitstellung und Betrieb aller netztechnischen Systeme zur sicheren Anbindung der beA-Nutzer an die Rechenzentren des Betreibers über das Internet gemäß Verfügbarkeitsanforderungen,
    - Bereitstellung und Betrieb der Monitoring-Systeme, der Betriebs- und IT-Service-Management-Tools,
- Erstellung, Bereitstellung und Pflege des Betriebshandbuchs und aller notwendigen Dokumentationen,
- Unterbrechungs- und datenverlustfreie Migration des Anwendungsbetriebes, einschließlich der ggf. notwendigen historischen Daten, von dem bisherigen Dienstleister,
- Durchführung des Release- und Patch-Managements,
- Durchführung des beA-Anwendungsbetriebs 24/7 in Deutschland,
- Durchführung des System- und Anwendungs-Supports,
- Regelmäßige Überprüfungen und Reporting der Sicherheit des Gesamtsystems hinsichtlich Integrität, Verfügbarkeit und Vertraulichkeit,
- Regelmäßige Sicherheits-Assessments z. B. durch ein ISO-27001-zertifiziertes Informationssicherheitsmanagement und regelmäßige Sicherheitsprüfungen beispielsweise durch Penetrationstests und Quellcode-Reviews.

1.2 Gegenstand der Vergabe

Gegenstand der Vergabe sind Dienstleistungen über die Gesamtlaufzeit des Vertrages vom 01.01.2020 bis zum 31.12.2024

- zur Übernahme der bestehenden Software,
- zur Weiterentwicklung des beA,
- zur Wartung und Pflege der beA-Software,
- zur Übernahme des Betriebs und des Weiterbetriebs eines OSCI-Intermediärs, einer SAFE-Domain, der Schnittstellen zur Infrastruktur des elektronischen Rechtsverkehrs sowie weiterer Schnittstellen, z. B. zur Kanzleisoftware,
- zum Betrieb der beA-Anwendung, einschließlich der notwendigen Infrastruktur,
- zur Bereitstellung und zum Betrieb eines deutschsprachigen First-, Second- und Third-Level-Supports.

1.3 Mengengerüste

Die BRAK besteht aus 27 regionalen Rechtsanwaltskammern und der Rechtsanwaltskammer beim Bundesgerichtshof:

https://www.brak.de/w/files/04_fuer_journalisten/statistiken/02_ra_mitgliederstatistik_01.01.2019.pdf

Derzeit sind rund 200.000 Postfächer für Rechtsanwälte, Syndikusrechtsanwälte, Abwickler, Vertreter und Zustellungsbevollmächtigte sowie die RAKn eingerichtet. Zusätzlich wird von etwa 300.000 nicht-juristischen Mitarbeitern ausgegangen, die Zugriff auf die Postfächer erhalten. Hinzu kommt eine unbekannte Anzahl von juristischen Mitarbeitern, die keine Rechtsanwälte sind (z. B. wissenschaftliche Mitarbeiter, Referendare). Es ist davon auszugehen, dass in der Kernzeit 7 Nachrichten pro Sekunde über das System übermittelt werden. Das beA-System ist nicht als Nachrichtenarchiv konzipiert. Nachrichten werden gem. § 27 RAVPV nach 90 Tagen automatisch in den Papierkorb verschoben und werden nach weiteren 30 Tagen automatisch gelöscht.

Derzeit werden pro Monat rund 270.000 Nachrichten über das beA versandt und rund 450.000 Nachrichten empfangen. Es ist mit einem raschen Anstieg aufgrund der zunehmenden Einführung der elektronischen Aktenführung in der Justiz und der Anbindung der Behördenpostfächer zu rechnen.

Die Vorgaben hinsichtlich der Zahl der Anlagen zu einer über das beA versandten Nachricht und hinsichtlich der maximalen Größe einer Nachricht (Mengenbegrenzungen) ergeben sich aus den Anforderungen für EGVP-Drittprodukte:

https://egvp.justiz.de/Drittprodukte/EGVP_Infrastruktur_Anforderungen_Teilnahme_von_Drittanwendungen.pdf

Der AN muss davon ausgehen, dass die Mengenbegrenzungen in Zukunft aufgehoben werden.

Die Inanspruchnahme des Supports ergibt sich aus der im Anhang 1 beigefügten Übersicht.

1.4 Projektorganisation

Der AN muss ein Konzept für die Projektorganisation vorlegen.

Das Konzept muss mindestens folgende Eckpunkte enthalten:

- Durchführung von Workshops,
- Regelmäßige Projekt- und Lenkungsausschusssitzungen,
- Dokumentation der Meetings und aller weiteren Festlegungen durch den AN,
- Regelmäßige Abstimmungen zwischen Auftraggeber (AG) und AN in Berlin in den Räumen der BRAK,
- Benennung eines Gesamtprojektleiters und der verschiedenen Projektrollen,
- Zuständigkeiten und Abstimmungsprozesse hinsichtlich Transition, Entwicklung, Betrieb und Support.

Der AN muss die Anzahl und die Qualifikation der für den jeweiligen Leistungsbereich eingesetzten Mitarbeiter verbindlich im Umsetzungskonzept angeben sowie die Namen der Personen in vereinbarten Schlüsselpositionen in der Liste der Servicerollen benennen.

1.5 Release-Management

Der AN muss ein Release-Management für die Weiterentwicklung und Pflege der Software des Systems im Betrieb etablieren. Das Release-Management umfasst die Aufgaben zur Planung, Kontrolle und Steuerung eines Releases über den vollständigen Lebenszyklus eines Releases hinweg – Disziplin-übergreifend von der Anforderungserhebung bis zum Nachweis der erfolgreichen Installation auf der Produktionsumgebung. Das Release-Management berücksichtigt ferner alle Bereitstellungsformen sowie Systemänderungen insbesondere Funktionsänderungen, Fehlerbehebungen, Aktualisierungen von Software- oder Hardware-Komponenten sowie Konfigurationsanpassungen. Das Release-Management umfasst neben den Systemänderungen auch die im Bedarfsfall bereitzustellenden Hotfixes oder Emergency-Changes.

Der AG geht davon aus, dass der AN regelmäßig beispielsweise zweimonatlich funktionserweiternde und/oder fehlerbehebende Releases bereitstellt (agile Entwicklung).

Der AN muss neue Releases der eingesetzten Software des Systems in installationsfertiger Form bereitstellen. Installationsfertig bedeutet, dass die neuen Releases der Software des Systems durch den AN getestet und dem AG bereitgestellt wurden. Neue Versionen werden durch den AN installiert. Der AG wird diese Releases zunächst im Staging-Testsystem (STA) testen (Funktionsüberprüfung). Nach Freigabe durch den AG werden die Schulungs- und Partnertestumgebung (SPT) und die Produktionsumgebung (PROD) aktualisiert. Produktionseinspielungen werden auf der STA oder bei Bedarf auf der SPT getestet. Es erfolgt grundsätzlich keine Installation auf der Produktionsumgebung ohne Test. Nach Installation einer Systemänderung weist der AN die erfolgreiche Installation durch eigene Tests nach.

Als Bestandteil des Release-Managements muss der AN eine Release-Planung erstellen und diese kontinuierlich aktualisieren.

Als Bestandteil des Release-Managements muss der AN alle aus einem neuen Release resultierenden Änderungen des Systems unter Beachtung der Analyseergebnisse gemäß Kapitel 3.6 vollständig dokumentieren.

1.6 Zusammenarbeitsmodell

Der AN muss ein Zusammenarbeitsmodell beschreiben. Dieses muss mindestens enthalten:

- Erstellung von Leistungsnachweisen und Reports, die durch den AN zur Verfügung gestellt werden und Abweichungen von den Sollwerten erkennen lassen müssen,
- Freigaben,
- Kommunikation mit dem AG und ggf. den übrigen Beteiligten (z. B. Justiz, BNotK, Kanzleisoftware-Hersteller [KSW-Hersteller], Kammersoftware-Hersteller, Schnittstellenpartner der Justiz),
- Nutzung von Tools und Services gemeinsam mit dem AG,
- Fortschreibung und Verbesserung der Prozess-, Betriebs-, System- und Anwendungsdokumentation.

1.6.1 Service Reporting

Der AN muss ein monatliches Service Reporting konzipieren, mit dem AG abstimmen und etablieren, welches darauf gerichtet sein muss:

- dem AG eine lückenlose Überprüfung der geforderten Leistungen und der geschuldeten Qualität zu ermöglichen,
- dem AG als Instrument der Leistungssteuerung zu dienen,
- dem AG Entscheidungen über die kurz-, mittel- und langfristige Service-Gestaltung zu ermöglichen.

1.7 Mitwirkungsleistungen des Auftraggebers

Der AN soll die von dem AG zu erbringenden Mitwirkungsleistungen beschreiben.

1.8 Informationssicherheit

Aus Einsatzzweck und -umfeld des beA ergeben sich besondere Anforderungen an Informationssicherheit und Datenschutz. Insbesondere die Pflicht zur anwaltlichen Verschwiegenheit, das besondere berufliche Umfeld, sowie die gesetzliche Festlegung, die ab 01.01.2022 den elektronischen Rechtsverkehr als den einzig rechtskonformen Kommunikationskanal zwischen Anwaltschaft und Gerichten definiert, stellen besondere Anforderungen an die Sicherheitsziele für Weiterentwicklung und Einsatz des beA. Diese sind vom AN im Rahmen der Entwicklung und des Betriebs einzuhalten. Die Einzelheiten, wie er mindestens die im Folgenden genannten Sicherheitsziele einhalten will und welche Maßnahmen er zur laufenden Überprüfung vorsehen wird, ergeben sich aus dem von dem AN im Rahmen des Angebots vorgelegten Konzept.

1.8.1 Sicherheitsziele

Aus den besonderen Anforderungen an Informationssicherheit ergeben sich die folgenden Sicherheitsziele:

- **Vertraulichkeit:** Das System muss eine vertrauliche Speicherung und Übertragung sowohl von Inhaltsdaten als auch von Nutzungsdaten gewährleisten.
- **Verfügbarkeit**: Das System wird zu einem verpflichtenden und grundsätzlich einzigen Kommunikationsmittel mit der Justiz (wobei für Notfälle Ausweichmöglichkeiten oder die Möglich-

keit zur Wiedereinsetzung in den vorigen Stand zur Verfügung stehen). Daher muss grundsätzlich eine maximale Verfügbarkeit zu jedem Zeitpunkt gewährleistet sein, der Datenverlust bei Störungen muss minimiert werden, und das System muss auch bei hoher Last ein stabiles Reaktionsverhalten zeigen.

- **Integrität:** Das System muss eine integre und daher manipulationssichere Übertragung und Speicherung sowohl der Inhaltsdaten als auch der Nutzungsdaten gewährleisten.
- **Authentizität:** Das System muss sowohl die Authentizität aller Benutzer prüfen als auch die Authentizität der Inhalts- bzw. Nutzungsdaten gewährleisten.
- **Nichtabstreitbarkeit:** Das System muss die Nichtabstreitbarkeit sowohl in Bezug auf die Autorenschaft einer Nachricht als auch auf den Kommunikationsvorgang gewährleisten.
- **Zurechenbarkeit:** Das System muss die Zurechenbarkeit in den Bereichen Zugriffskontrolle, Beweissicherung bzw. Protokollierung sowie zeitliche Bestimmtheit sicherstellen.
- **Identifizierung der Benutzer:** Das System stellt sicher, dass jeder Benutzer eindeutig identifiziert werden kann.

Der Rechtsanwalt muss sich weiterhin darauf verlassen können, dass die Nachricht auf dem Weg in sein Postfach von niemandem zur Kenntnis genommen werden konnte. Dies gilt genauso für den umgekehrten Weg, also aus dem Postfach des Rechtsanwalts zur Justiz oder zu einem anderen Beteiligten. In jedem Fall müssen die Inhalte des Postfachs vor dem Zugang Unbefugter sicher sein.

Eine Maßnahme zur Zugangs-, Zugriffs- oder Weitergabekontrolle in vernetzten Systemen ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Zur Absicherung der Übertragung der Nachrichten hat der AN eine durchgängige Verschlüsselung sicherzustellen.

1.8.2 Informationssicherheitsmanagement

Der AN muss ein Informationssicherheitsmanagementsystem betreiben und dies dem AG nachweisen. Den Nachweis kann er durch Zertifizierungen, z. B. nach ISO 27001, erbringen. Für die für den Betrieb des beA-System eingesetzten Rechenzentren muss dies erfolgen.

1.8.2.1 Risikomanagement

Der AN ist verpflichtet, ein Risikomanagement z. B. nach ISO 27001 zu betreiben. Der AN muss das bestehende IT-Sicherheitskonzept fortschreiben und dem AG den jederzeitigen Zugriff darauf ermöglichen.

1.8.3 Allgemeine Anforderungen für Entwicklung und Betrieb

Neben der Verpflichtung des AN, eigenständig Schutzmaßnahmen risikoorientiert zu ermitteln und einzuhalten, sind vom AN übergreifende Maßnahmen zur Gewährleistung einer sicheren Entwicklung, eines sicheren Betriebes einschließlich Support umzusetzen und nachzuweisen. Hierfür sind mindestens folgende Aspekte zu betrachten:

- Einhaltung von Sicherheitsanforderungen durch Mitarbeiter des AN,
- Sicherer Umgang mit Informationen,
- Bewusstsein und Schulungen für Informationssicherheit,
- Informationssicherheit von Unterauftragnehmern.

1.9 Beendigungsunterstützung

Der AN muss bei Vertragsende im Falle eines Wechsels des Auftragnehmers einen zukünftigen Auftragnehmer bei der Vorbereitung und Durchführung der Entwicklungs-, Betriebs- und Supportübernahme aktiv unterstützen. Hierzu gehört insbesondere die Schaffung der notwendigen Voraussetzungen für eine erfolgreiche Transition zur Fortsetzung der Weiterentwicklung und des Betriebs des beA-Systems.

2. Transition nach Vergabe

Der AN muss sein Vorgehen in der Transitionsphase ausführlich beschreiben. Die Darstellung muss über das im Angebot vom AN vorgelegte Transitions-Konzept hinausgehen und mindestens Ausführungen zu folgenden Themen enthalten:

- Schulungen und Trainings,
- Übernahme und Prüfung von Quellcode-Bereitstellungen für das beA-System,
- Aufsetzen einer Build-Umgebung (Infrastruktur, Services, Konfiguration, externer Zugriff) einschließlich Vorschlägen zu den zu verwendenden Tools,
- Auslieferungen,
- Entwicklungsprozesse,
- Übernahme und Prüfung der Online-Hilfe-Bereitstellungen,
- Fehlermeldungs- und -bearbeitungsprozess einschließlich der Zusammenarbeit mit dem AG und Vorschlägen zu den einzusetzenden Tools,
- Aufbau der Systemumgebungen und Betriebsübernahme,
- Umstellung des Betriebs,
- Dokumentation,
- Testaktivitäten.

Der AN muss nach Aufbau der Systemumgebungen die Funktions- und Betriebsfähigkeit nachweisen, bevor die Umstellung des Betriebes einschließlich Datenmigration sowie der erforderlichen Umschaltprozesse erfolgen darf.

2.1 Quellcode und Build

2.1.1 Übernahme und Prüfung von Quellcode-Bereitstellungen für das beA-System

Der AN muss den Quellcode aufgrund von Bereitstellungen des bisherigen AN übernehmen. Dazu gehören zumindest folgende Aufgaben:

- Konsistenzprüfung der gelieferten Quellcode-Dateien und Build-Objekte,
- Vollständigkeitsprüfung,
- Prüfung der Abhängigkeiten (eingesetzte Dritt-Bibliotheken, Zulieferprodukte),
- Beschaffung der eingesetzten Dritt-Bibliotheken und Zulieferprodukte, soweit erforderlich,
- Prüfung der Lizenzbedingungen der Dritt-Bibliotheken und Zulieferprodukte,
- Prüfung der Vulnerabilities.

2.1.2 Aufsetzen der Build-Umgebung (Infrastruktur, Services, Konfiguration, externer Zugriff)

Der AN muss eine Build-Umgebung für das beA-System konzipieren und aufsetzen. Dieses System wird nachfolgend auch als Entwicklungs-System bezeichnet.

Die Konzeption und das Aufsetzen der Build-Umgebung erfolgen in einer Weise, dass berechtigte externe Entwickler, etwa des AG, an der Weiterentwicklung und Wartung des beA-Systems mitwirken können.

Der AN muss diese Build-Umgebung an den AG bereitstellen oder die Code-Generatoren so benennen, dass diese Umgebung auch nach Vertragsende durch den AG im vollen Umfang weiter verwendet werden kann. Zur Bereitstellung gehört auch die Übergabe von administrativen Rechten an den AG.

Bestandteile der aufzusetzenden Build-Umgebung sind zumindest:

- ein Versionskontrollsystem,
- ein einheitliches Build-Tool,
- Funktionen zum zeitgesteuerten oder getriggerten Build,
- Funktionen zum automatisierten Entwicklertest,
- Funktionen zur Einbettung von Drittbibliotheken und Zulieferkomponenten,
- Bereitstellung der erforderlichen Code-Generatoren,
- Bereitstellung von Tools zur automatischen Prüfung der Quell-Code-Qualität,
- Funktionen für Datensicherung, Zugriffskontrolle und Berechtigungsverwaltung.

Der AN integriert die übernommenen Bereitstellungen in die aufgebaute Build-Umgebung. Zu den Aufgaben gehören zumindest:

- Entwicklung (Anpassung, Reverse Engineering) von Build-Scripten für erforderliche Target-Objekte unter Berücksichtigung der Build-Infrastruktur,
- Einbindung der erforderlichen Code-Generatoren,
- Integration von Tools zur automatischen Prüfung der Quellcode-Qualität,
- Qualitätssicherung der Build-Chain für beA-Anwendungskomponenten,
- Integration und Bereitstellung von Default-Werten für Konfigurationsdaten des Zielsystems.

Der AN muss für seine Entwicklungsaktivitäten das hier beschriebene Entwicklungssystem benutzen. Eine versionierte Speicherung von

- Quellen und Build-Scripts für Individual-Software,
- entwicklungsrelevanten Konfigurationsdaten für das beA-System

außerhalb dieses Entwicklungssystems ist nicht zulässig, auch nicht für Entwickler des AG. Alle spezifisch für das beA erzeugten Build-Objekte müssen aus dem Entwicklungssystem heraus gebaut werden.

2.2 Aufbau der Systemumgebungen und Betriebsübernahme

Die bisherige Systemarchitektur wurde auf Basis der durch die beA-Software vorgegebenen Anforderungen definiert und die notwendigen Netz- und Systemkonfigurationen davon abgeleitet (vgl. Betriebsdokumentation). Der AN muss die Systemarchitektur nicht übernehmen.

Die zu installierenden Systeme müssen mindestens die Leistungsanforderungen erfüllen.

Das Konzept des AN soll einen Vorschlag enthalten, wie diese Umgebungen auch nach dem Vertragsende durch den AG in vollem Umfang weiter verwendet werden können.

2.3 Umstellung des Betriebes auf ein neues beA-System

Die Übernahme des laufenden Betriebes muss ohne Datenverlust und unterbrechungsfrei erfolgen. Der AN muss die einzelnen Phasen der Betriebsübernahme und seine Vorgehensweise beschreiben, insbesondere auch die Übernahme der Supportvorgänge.

2.4 Übernahme und Prüfung der Dokumentations-Bereitstellungen

Der AN muss Dokumentations-Bereitstellungen für das beA (vgl. Liste der vorhandenen Dokumentationen, Anhang 2) übernehmen und sie auf formale und inhaltliche Richtigkeit und Vollständigkeit hin überprüfen.

3. Entwicklung

3.1 Grundsätze der Weiterentwicklung

Nach den Feststellungen des AG hat die beA-Webanwendung in der Anwaltschaft und in Unternehmen bei Syndikusrechtsanwälten eine weite Verbreitung auch im parallelen Betrieb neben und in Ergänzung zu den Fachanwendungen gefunden. Der AN muss insbesondere auch vor diesem Hintergrund in den ersten sechs Monaten nach Vertragsschluss ein weitergehendes Konzept zur strategischen Weiterentwicklung des beA-Systems einschließlich der Web-Anwendung erstellen.

Der AG erwartet Überlegungen mindestens zu den folgenden Themen:

- Verbesserung der Benutzerfreundlichkeit der beA Web-Anwendung, z. B. durch Reorganisation und Modernisierung der Oberflächen unter Einbeziehung des Nutzerverhaltens,
- Vereinfachung der Arbeitsabläufe in der Web-Anwendung, z. B. bei der Empfängerauswahl,
- Stapelverarbeitung, z. B. beim Export von Nachrichten,
- Eignung für große Einheiten (Großkanzleien / Rechtsabteilungen),
- konzeptionelle und strategische Bewertung der eIDAS-Verordnung, z. B. im Hinblick auf die Einbindung von Fernsignaturen,
- Einbindung in europäische Justizkommunikation (z. B. eEvidence),
- Nutzung mobiler Endgeräte,
- Anbindung einer Mandantenkommunikation; Einbindung weiterer Kommunikationspartner (z. B. Versicherungswirtschaft, Versorgungswerke),
- Einrichtung von Kanzleipostfächern neben den individuellen Postfächern,
- Abrechnungssysteme.

Bei der Weiterentwicklung soll jeweils geprüft werden, ob und in welchem Umfang Open-Source Komponenten Verwendung finden können.

Der AG schließt eine vollständige Überarbeitung der Softwarearchitektur (auch hinsichtlich der Verschlüsselungsmechanismen) nicht aus, ggf. schon in der Transitionsphase.

3.2 Entwicklungskonzept

Der AN muss in den ersten sechs Monaten nach Vertragsschluss in Abstimmung mit dem AG über das im Rahmen des Angebots bereits erstellte Entwicklungskonzept hinausgehend ein ausführliches Konzept für den Weiterentwicklungsprozess erarbeiten. Dieses Konzept muss mindestens folgende Vorgaben berücksichtigen:

- Der AN muss für seine Entwicklungsaktivitäten das Entwicklungssystem (s. Kapitel 2.1) benutzen.
- Der AN muss in Absprache mit dem AG ein Fehlermeldungssystem verwenden, auf das der AG jederzeit Zugriff hat. Der AG stellt das Fehlermeldungssystem dem AN ggf. zur Verfügung. Eine Verwaltung von Fehlermeldungen außerhalb dieses Systems ist unzulässig.
- Der AN muss in einem Dokument seinen Entwicklungsprozess und die darin vorgesehenen Qualitätssicherungsmaßnahmen unter Berücksichtigung der vom AG gestellten Anforderungen dokumentieren. Speziell muss darin auch dokumentiert werden, wie Zulieferungen zum Source Code durch Externe, etwa Mitarbeiter des AG in der erforderlichen Qualität integriert werden können. Der AN muss das mit dem AG abgestimmte Dokumentationssystem nutzen.
- Bei der Weiterentwicklung soll geprüft werden, ob und in welchem Umfang Open-Source-Komponenten Verwendung finden können.
- Die Prozesse im Zusammenhang mit Entwicklung und Wartung der Software müssen anerkannten Standards entsprechen, beispielsweise ISO/IEC 12207:2008 oder ISO/IEC/IEEE 15288:2015.
- Die Prozesse hinsichtlich Software-Entwicklung und Software-Test müssen anerkannten Standards entsprechen, beispielsweise ISO/IEC 25051:2014.
- Der AN muss die Implementierung und Durchführung der Sicherheitsmaßnahmen gewährleisten (beispielsweise durch die Bereitstellung der Hashwerte über die Java-Script-Dateien).

3.3 Sichere Entwicklung

Der AN muss zur Gewährleistung einer sicheren Entwicklung u. a. Maßnahmen zur Absicherung der Entwicklungsumgebung, zur Absicherung der Entwicklungsprozesse sowie zur Trennung von Entwicklungs-, Test-, und Betriebsumgebungen umsetzen und nachweisen. Diesen Nachweis kann der AN durch eine Zertifizierung, beispielsweise nach ISO 27001:2015, erbringen.

Der AN muss durch geeignete Konzeption, Programmierung und Tests für die Anwendungssicherheit Sorge tragen. Zu diesem Zweck muss er Schutzmaßnahmen entsprechend dem Stand der Technik und anhand etablierter Maßnahmenkataloge (beispielsweise der jeweils aktuelle OWASP Testing Guide, oder NIST 800-160 bzw. Nachfolger) ermitteln und diese in Absprache mit dem AG umsetzen.

Die Einzelheiten ergeben sich aus dem mit dem Angebot vorgelegten Konzept.

3.4 Barrierefreiheit

Die Anforderungen an die Barrierefreiheit sollen beachtet werden. Das System soll den besonderen Anforderungen an die Barrierefreiheit, wie sie durch die Verordnung zur Schaffung barrierefreier In-

formationstechnik nach dem Behindertengleichstellungsgesetz („BITV 2.0“) geregelt sind, entsprechen und sollte im BIK-Selbsttest mindestens 90 Punkte (gut zugänglich) erreichen.

3.5 Anforderungs-Management

Anforderungen an Änderungen des beA-Systems haben verschiedene Quellen, d. h. zumindest:

- rechtliche Rahmenbedingungen (Gesetze, Rechtsverordnungen etc.),
- Änderungsvorschläge der Benutzer des beA-Systems und seiner verschiedenen Schnittstellen (z. B. Benutzer der beA-Webanwendung, KSW-Hersteller, Kammersoftware-Hersteller, Schnittstellenpartner der Justiz),
- Änderungsvorschläge des AN und AG,
- Änderungen an verwendeten Dritt- und Zulieferprodukten (Lizenzbedingungen, Nachfolgeversionen, Einstellung des Supports, Innovationen),
- Erkenntnisse aus Sicherheitsbetrachtungen,
- Erkenntnisse zu Verbesserungspotentialen aus Entwicklung, Betrieb und Support des beA,
- geändertes Benutzerverhalten und damit einhergehende Anforderungen an Durchsatz, Antwortzeitverhalten und Mengengerüste.

Der AN muss sich an den technischen Klärungen zu vorgeschlagenen Änderungsanforderungen beteiligen.

Der AN muss vom AG gestellte funktionale und nichtfunktionale Anforderungen an das beA-System analysieren. Im Rahmen dieser Analyse wird der Änderungsbedarf z. B. an

- beA-Anwendungskomponenten, anderer Software- und Infrastruktur-Komponenten (einschließlich Hardware, Netzwerk, Storage, Firmware),
- externen und internen Schnittstellen des beA-Systems sowie
- relevanten fachlichen internen und externen Abläufen und Prozessen

festgestellt.

Der AN muss den AG auf ggf. erforderliche und/oder dem Stand der Technik entsprechende Änderungen und/oder Detaillierungen an gestellten Anforderungen und an architekturellen Lösungen im Rahmen der Analyse und dem nachfolgenden Entwicklungsprozess ausdrücklich hinweisen.

3.5.1 Technische Anforderungen bei Änderungen am beA-System

Technische Änderungen am beA-System müssen unter Berücksichtigung folgender grundsätzlicher Anforderungen erfolgen, insbesondere:

- Kompatibilität mit externen Maschinenschnittstellen,
- Verhalten der Anwendung beim Software-Update,
- Sicherheitseigenschaften des Systems,
- Barrierefreiheit,
- Durchsatz- und Antwortzeitverhalten,
- Verfügbarkeit,
- Ergonomie der Benutzerschnittstellen,

- Betreibbarkeit.

3.6 Systemarchitektur

Die Systemarchitektur des beA-Systems wird in dem Dokument „Technische Systembeschreibung“ beschrieben, insbesondere durch:

- eine Übersicht über Gesamtarchitektur der beA-Anwendungskomponenten, externen Systeme und Schnittstellen,
- eine Schichtenarchitektur der Software des beA-Systems,
- eine Umsetzungsarchitektur in der Infrastruktur.

Ergänzende Informationen zur Systemarchitektur finden sich in

- Umsetzungsfeinkonzept beA-System,
- Betriebshandbuch,
- Administrationshandbuch,
- Installations- und Administrationshandbuch der Fachapplikation beA,
- Überblick über Schnittstellen und Verantwortung (BRAK beA P Applikation Schnittstellen-Verantwortungsübergang_20180710.pptx).

Eine Liste der vom AG bereitgestellten Dokumentationen findet sich im Anhang 2.

Der AN muss gestellte funktionale und nichtfunktionale Anforderungen an das beA-System analysieren. Im Rahmen dieser Analyse wird insbesondere der Änderungsbedarf an

- der Systemarchitektur im Allgemeinen,
- den beA-Anwendungskomponenten, anderer Software- und Infrastruktur-Komponenten (einschließlich Hardware, Netzwerk, Storage, Firmware),
- den externen und internen Schnittstellen des beA-Systems,
- den relevanten fachlichen internen und externen Abläufen und Prozessen sowie
- der Prozess-, Betriebs-, System- und Anwendungsdokumentation

festgestellt.

Die Analyse des AN muss insbesondere die Auswirkungen auf die nicht-funktionalen Eigenschaften, die Testbarkeit des Systems, den Rollout einschließlich etwaiger Migrationen und Konfigurationsänderungen sowie die Betriebsprozesse enthalten.

Der AN muss Analysedokumente zu den gestellten Anforderungen bereitstellen.

Im Rahmen des Reviews der Analysedokumente beteiligt sich der AN an erforderlichen Abstimmungen mit dem AG und ggf. externen Schnittstellenpartnern.

Der AN weist den AG auf ggf. erforderliche und/oder sinnvolle Änderungen und/oder Detaillierungen an gestellten Anforderungen und an architekturellen Lösungen im Rahmen der Analyse und dem nachfolgenden Entwicklungsprozess ausdrücklich hin.

3.7 Dokumentation

Der AN muss ein Dokumentations-System konzipieren und aufsetzen oder das bisherige Dokumentations-System übernehmen.

Zu dem Dokumentations-System gehören zumindest Infrastruktur, Services, Konfiguration und die Möglichkeit externer Zugriffe. Das Dokumentations-System muss auch Funktionen für Sicherung und Versionierung anbieten.

Das Aufsetzen des Dokumentations-Systems erfolgt in einer Weise, dass Externe, etwa Mitarbeiter des AG, auf das Dokumentations-System lesend und schreibend zugreifen können. Es muss möglich sein, Dokumente komfortabel zu suchen, Dokumente einzeln und als Baumstrukturen aus dem Dokumentations-System herunter zu laden.

Die Dokumentation des beA muss anerkannten Standards, beispielsweise ISO/IEC 26514:2008 und/oder ISO/IEC 26515:2018, entsprechen.

3.8 Auslieferungen

3.8.1 Definition und Abstimmung der Auslieferungs-Schnittstellen

Zu einer Version eines Maintenance- oder Patch-Releases müssen für die Inbetriebnahme Daten über eine Auslieferungs-Schnittstelle bereitgestellt werden. Die bereitgestellten Daten umfassen zumindest:

- gültige Freigabemitteilung gemäß Releasemanagement,
- Informationen zu gelieferten Funktionalitäten (z. B. Change Requests) und korrigierten Fehlern,
- freigegebene Software-Archive,
- freigegebene Online-Hilfe-Archive,
- Dokumentation zu verwendeten Dritt- und Zulieferprodukten,
- Teststatus zur Freigabe aufgrund strukturierter Informationen zu geplanten, ausgeführten, erfolgreichen und nicht erfolgreichen Testfällen,
- KPIs zum Teststatus,
- Zulieferungen zum Installations-Manual,
- Hinweise auf Änderungen in der Infrastruktur,
- Hinweise für den Betrieb und den Support,
- Hinweise auf anzupassende externe Prozesse,
- Hinweise auf geänderte externe Schnittstellen des beA-Systems,
- Hinweise für den Abnahmetest des AG,
- Migrationshinweise,
- den aktuellen Status zu Vulnerabilities (Bewertung und Behandlung).

Der AN muss Auslieferungs-Schnittstellen definieren und mit dem AG abstimmen. Der AG muss jederzeitigen Zugriff auf die Auslieferungsschnittstellen haben. Der AN stellt dem AG Release-Notes (vgl. oben Kapitel 1.5) zur Verfügung.

3.8.2 Aufsetzen der Auslieferungs-Umgebung (Infrastruktur, Services, Konfiguration, externer Zugriff)

Der AN muss eine Auslieferungs-Umgebung für das beA-System entsprechend den mit dem AG abgestimmten Auslieferungs-Schnittstellen aufsetzen.

Zu der Auslieferungs-Umgebung gehören zumindest Infrastruktur, Services, Konfiguration und die Möglichkeit externer Zugriffe.

3.9 Test

Der AN muss ein Konzept für eine Teststrategie in Abstimmung mit dem AG entwickeln und dokumentieren, das u. a. den Testprozess einschließlich der anzuwendenden Testmethoden und die vorgesehenen Qualitätssicherungsmaßnahmen unter Beachtung der gewünschten agilen Softwareentwicklung beinhaltet. Ergänzend gelten die Ausführungen in dem mit dem Angebot vorgelegten Konzept des AN.

Der AN muss die für seine Testaktivitäten erforderlichen Testsysteme konzipieren und beschreiben. Der AN muss die für seine Testaktivitäten erforderlichen Testsysteme aufbauen und in eine eigene Testumgebung einbetten. Die aufgebauten Testsysteme müssen mit externen Testsystemen, etwa der Justiz und der BNotK, soweit erforderlich, kompatibel sein.

Der AN muss zu jedem Release eine Testplanung erstellen und diese mit dem AG abstimmen.

Der AN muss in allen Testphasen Fehler kontinuierlich beheben und Fehlerbehebungen integrieren. Der AN muss mindestens die folgenden Tests für die Transition, Auslieferungen und Freigaben durchführen:

- Modul-Tests für einzelne Anwendungs-Komponenten,
- funktionale Tests im integrierten Gesamtsystem und mit externen Systemen und Schnittstellen, insbesondere mit den externen Schnittstellen zur Justiz, zu den Trustcentern, den Rechtsanwaltskammern sowie zu den Suchdiensten (BRAV und FAL),
- nicht-funktionale Tests (Durchsatz, Antwortzeit, Verfügbarkeit, Sicherheit) im integrierten Gesamtsystem und mit externen Systemen und Schnittstellen,
- Migrations-Tests,
- Installationstests auf der Grundlage der Installationsdokumentation,
- Smoke-Tests,
- Regressionstests.

Der AN muss die Tests eigenständig durchführen, auswerten und die Ergebnisse aufbereitet an den AG berichten.

Der AN muss weiterhin kontinuierliche und automatisierte Regressions- und Build-Tests durchführen. Der Umfang sowie der Fokus dieser kontinuierlichen Tests muss mit dem AG fortlaufend abgestimmt werden.

3.10 Integration

Der AN muss die Integration der Anwendungs-Komponenten mit den eingesetzten Dritt- und Zulieferkomponenten sowie OEM-Komponenten in die bestehende und sich weiterentwickelnde Test- und

Betriebsumgebung sowie den EGVP-Verbund inklusive der genutzten Sicherheits-Infrastrukturen sicherstellen.

Der AN muss somit sicherstellen, dass zum Zeitpunkt der Inbetriebnahme alle notwendigen Maßnahmen (u. a. Dokumentation, Einweisungen, Tool-Anpassungen) umgesetzt wurden, damit das System im Verbund sicher, stabil und performant betrieben werden kann.

Der AN soll darstellen, wie im Rahmen der Installationsverfahren Automatisierung eingesetzt werden kann, mit dem Ziel möglichst weniger Einschränkungen für die Benutzer und einer zeitoptimierten Durchführung.

Die Einzelheiten ergeben sich aus dem von dem AN im Rahmen des Angebots vorgelegten Konzept.

3.11 Pflege und Wartung

Der AN erbringt laufend die Leistungen zur Softwarepflege und Wartung inklusive der Störungsbeseitigung und Fehlerbehebung. Dazu gehören mindestens:

- Störungsbearbeitung und Störungsbeseitigung

  Der AN muss den 3rd Level Support bei der Analyse und Behebung von Störungen und Klärung anderer Anliegen, die spezifische Entwicklungs-Kenntnisse erfordern, gewährleisten. Das Resultat hierbei muss die Befähigung des Supports zur Durchführung von Maßnahmen auf Seiten des Betriebes zum Zweck der Störungsbehebung sein und/oder eine detaillierte Analyse der notwendigen Systemanpassungen zur Störungsbehebung sowie deren Umsetzung und Bereitstellung.

- Schwachstellen-Assessment

  Im Rahmen des Schwachstellen-Assessments muss der AN kontinuierlich die Bekanntmachungen und Hinweise von Common Vulnerabilities and Exposures (CVE) sowie Ankündigungen bzw. Abkündigungen (EoS und EoL) prüfen.

  Zu den relevanten Bekanntmachungen und Hinweisen führt der AN eine Risikobewertung durch, mit dem Ziel, in Abstimmung mit dem AG Maßnahmen und die weitere Vorgehensweise zu definieren.

  Auf dieser Grundlage muss der AN die Aktualisierung oder den Austausch eigener Komponenten des beA-Zentralsystems und von verwendeten Dritt- und Zulieferkomponenten sowie OEM-Komponenten (einschließlich der Betriebssysteme) durchführen.

  In diesem Rahmen führt der AN auch mögliche Anpassungen der Anwendungskomponenten durch, sofern dies eine Voraussetzung für die Aktualisierung oder den Austausch der verwendeten Dritt- und Zulieferkomponenten sowie der OEM-Komponenten ist.

  Ist eine Schwachstelle zum Zeitpunkt der Kenntnisnahme durch den AN oder AG durch Dritte ausnutzbar und geeignet, ein Risiko eintreten zu lassen, muss sie als Sicherheitsvorfall im Rahmen des Incident-Management-Prozesses nach ITIL behandelt werden.

- Aktualisierungs-Assessment

  Der AN muss Aktualisierungen oder den Austausch von Anwendungskomponenten, verwendeten Dritt-und Zulieferkomponenten sowie OEM-Komponenten auf Grundlage einer proaktiven Identifizierung und Bewertung technologischer Weiterentwicklungen und den sich daraus ergebenen Anpassungserfordernissen und Verbesserungspotentialen für das beA-System insbesondere hinsichtlich der nicht-funktionalen Anforderungen durchführen.

  Im Rahmen des Aktualisierungs-Assessments muss der AN mögliche Aktualisierungspotenziale identifizieren, bewerten und eventuelle Maßnahmen formulieren und mit dem AG abstimmen.

Die Einzelheiten ergeben sich aus dem von dem AN im Rahmen des Angebots vorgelegten Konzept.

3.12 Online-Hilfe

Der AN muss Sourcen der Online-Hilfe-Bereitstellungen übernehmen (xar-Archiv für XWiki und generiertes PDF) oder eine neue Online-Hilfe aufsetzen.

Dazu gehören folgende Aufgaben:

- Vollständigkeitsprüfung,
- Konsistenzprüfung,
- Aufsetzen einer Entwicklungs-Umgebung für Online-Hilfe.

Das Aufsetzen der Entwicklungs-Umgebung für die Online-Hilfe erfolgt in einer Weise, dass externe Entwickler, auch des AG, an der Weiterentwicklung der Online-Hilfe mitwirken können.

Der AN muss die Entwicklungs-Umgebung für die Online-Hilfe so bereitstellen, dass diese Umgebung nach Vertragsende durch den AN im vollen Umfang weiter verwendet werden kann. Zu der Bereitstellung an den AG gehört auch die Übergabe administrativer Rechte.

4. Betrieb

4.1 Betrieb beA-System

Der AN übernimmt die Verantwortung für den Betrieb des beA. Dieser setzt sich aus folgenden Services zusammen:

- Systembetrieb
  - Rechenzentrumsleistungen
  - Infrastrukturbetrieb
  - Systemmanagement
  - Patchmanagement
  - Lizenzmanagement
- Anwendungsbetrieb
  - Anwendungs-Support
  - Monitoring der Anwendung
  - Wartung der Anwendung
  - Schlüsselmanagement
  - Messung der Anwendungs-Performance
- beA-Betrieb
  - Prozessüberwachung
  - Funktionsüberwachung
  - Schnittstellenüberwachung
  - Datenkonsistenz

Der AN muss die Leistungsfähigkeit des Systems mit Tests nachweisen.

Die Einzelheiten des Vorgehens ergeben sich aus dem von dem AN im Rahmen des Angebots vorgelegten Konzept.

4.2 Betriebsmanagement

Der AN muss ein Konzept für ein Betriebsmanagement auf Grundlage von ITIL in Abstimmung mit dem AG erarbeiten und umsetzen. Dieses muss Ausführungen zu folgenden Punkten enthalten:

- Change Advisory Board (CAB),
- Notfallmanagement,
- Eskalationsmanagement,
- Kommunikationsplan,
- Asset-Management,
- Dokumentation,
- Konfigurationsdaten,
- Standard-Betriebsabläufe,
- Betriebsprotokolle.

4.3 Systemarchitektur auf System- und Infrastrukturebene

Das beA-Zentralsystem besteht aus einer Reihe von Software-Komponenten und Schnittstellen zu externen Systemen (vgl. die Abbildung im Anhang 3). Für alle im beA System enthaltenen Software-Komponenten muss der AN die dafür erforderlichen Server und Infrastrukturdienste betreiben und den Betrieb der dargestellten Komponenten und der darunterliegenden Software-Server erbringen. Zur näheren Beschreibung der Systemarchitektur vgl. Kapitel 3.6.

Der AN muss ein Konzept für den sicheren Betrieb der beA-spezifischen Komponenten mit mindestens folgenden Inhalten erstellen:

- Load Balancing,
- Firewall Systeme,
- Intrusion Prevention,
- Geeignete Server Betriebssysteme für die verschiedenen Dienste,
- Webserver für die Kommunikationsverbindungen,
- Applikationsserver,
- Datenbankserver,
- Storagekapazitäten,
- Backup- und Restore-Kapazitäten,
- Zeitserver zum Nachweis der in den Journalen protokollierten Zeiten,
- Standard-E-Mail-Server zum Versenden von Standard-E-Mails an die beA-Nutzer,
- Domain Name Service (DNS),
- Remote-Zugang Entwicklung,
- Schutz vor Schadprogrammen.

Der AN muss die Systemarchitektur auf Basis der erfolgten Investitionen, Nutzungsdaten (Auslastungs- und Performancedaten), Anforderungen der Entwicklung als Folge veränderter Funktionalitäten auf Anpassungsbedarf prüfen und die Entwicklung bei Prüfungen jederzeit unterstützen.

Der AN muss regelmäßig die Systemarchitektur auf Basis der erfolgten Investitionen, Nutzungsdaten (Auslastungs- und Performancedaten), Anforderungen der Entwicklung als Folge technischer Entwicklungen auf Verbesserungspotential prüfen, die Ergebnisse qualifiziert und nachvollziehbar dem AG vorlegen und in Abstimmung mit dem AG etwaige Verbesserungsmaßnahmen in das Anforderungsmanagement überführen.

Die beA-Systemlandschaft muss mindestens in drei getrennten beA-Systemumgebungen bestehend aus Produktions-, Staging- und Schulung-/Partnertestumgebung vom AN betrieben werden.

Die einzelnen beA-Systemumgebungen müssen jeweils in mehrere, durch Firewalls getrennte Netzsegmente unterteilt werden.

4.4 Internetanbindung

Der AN muss die beA-Systemumgebungen an das Internet anbinden. Er muss dabei gewährleisten, dass immer so viel Bandbreite für das beA-System zur Verfügung steht, dass auch zu Spitzenlastzeiten die Antwortzeiten nicht durch Bandbreitenengpässe verzögert werden.

4.5 beA-Anwendungskomponenten

Der AN muss alle notwendigen Software-Komponenten betreiben, insbesondere

- beA Anwendung,
- beA-Anwenderhilfe,
- Intermediär der BRAK,
- SAFE Domäne der BRAK,
- SAFE Connector.

4.6 Schnittstellen

Alle im Dokument „BRAK beA Applikation Schnittstellen-Verantwortungsübergang“ aufgeführten Schnittstellen sind durch den AN zu überwachen. Die Logfiles der beA-Anwendung sind bzgl. Session-Abbrüchen und sonstiger Fehlermeldungen zu berücksichtigen. Darüber hinaus sind die Nutzungszahlen auf Basis von historischen Daten auf Abweichungen zu prüfen. Werden im Rahmen von Veränderungen weitere Schnittstellen hinzukommen, so sind diese entsprechend zu überwachen.

Für die Schnittstellen, welche keine Messpunkte zur Überwachung haben, ist eine indirekte Überwachung zu etablieren.

5. Support

Der Support ist bei dem AN in drei Supportstufen zu gliedern. Er hat innerhalb der üblichen Geschäftszeiten der Rechtsanwaltskanzleien alle Anliegen der beA-Anwender (Postfachbesitzer, Mitarbeiter, BRAK etc.) zu bearbeiten einschließlich der Einbindung der Verbundpartner (u. a. RAKn, Europäische Kommission, BNotK, Justiz, KSW-Hersteller). Darüber hinaus ist der Support des AN der Ansprechpartner für die Verbundpartner für Supportthemen, welche Informationen und/oder Maßnahmen in beA einschließlich der KSW-Schnittstelle zur Bearbeitung von Störungen benötigen.

Die Aufgaben und Kompetenzen in der Support-Struktur sind wie folgt:

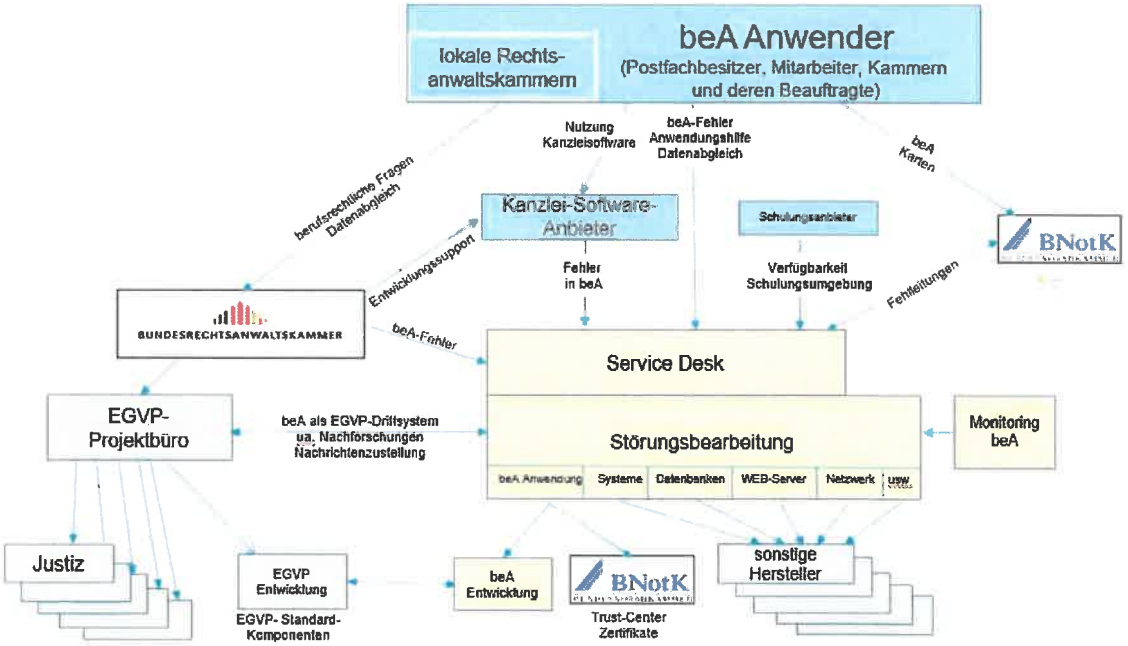
Support-stufe	Aufgaben	Kompetenzen	Zuordnung
1st Level	• Erreichbarkeit für Supportsuchende, eingehende und ausgehende Kommunikation, • Aufnahme der Störungsmeldung in das Ticket-Tool, • Vervollständigung der Daten • Lösung einfacher Störungen und Beantwortung von Anfragen zur Bedienung von beA.	• Bedienung von beA, Installation und Update der Anwendung, • Kenntnisse über die Datenbestände in beA und Betriebsprozesse.	Service Desk
2nd Level	• Prüfung der Zuständigkeiten der Supporteinheiten, • Koordination bei übergreifenden Zuständigkeiten, • Analyse und Qualifizierung der Störungsmeldung, • Vorgabe der Störungsbehandlung durch 1st Level Support, • Anwendung von Workarounds, • Überwachung der internen SLA, • Kommunikation zum AG bzgl. Status und Rückfragen.	• Detailkenntnisse über Abläufe in beA, • Bedienung von beA und der entsprechenden Bedienung durch Anwender, • Datenkorrektur gemäß Vorgaben.	Anwendungs-support
3rd Level	• Detailanalyse und Zuordnung, ob Störung im Betrieb oder Entwicklung gelöst werden muss, • Entwicklung und Bereitstellung von Workarounds (Datenkorrekturen) für Störungen, • Steuerung der Störungsbearbeitung durch Supportgeber außerhalb des Betriebs, • Überführung der Störungsmeldung in ggf. externes Tickettool eines Supportgebers (z. B. Jira-Justiz), • Überwachung von Service Level KPI von Supportgebern.	• Detailkenntnisse der beA-Anwendung, • Detailkenntnisse über das beA Datenmodell, • Abgrenzung der Ursache zwischen Daten und Softwarefunktion, • Script-Entwicklung für betriebliche Unterstützungsmaßnahmen.	Integrationsteam für beA Anwendung

Die durch den AN einzuhaltenden Service-Levels sind in der Anlage zum Vertrag geregelt.

Die Einzelheiten zur Übernahme und zum Aufbau des Supports ergeben sich aus dem von dem AN im Rahmen des Angebots vorgelegten Konzept.

5.1 Supportorganisation

Das beA-System ist als sogenanntes Dritt-System im EGVP-Verbund integriert. Entsprechend muss auch der Support dieses berücksichtigen.



Folgende Schnittstellen sind im Support zu berücksichtigen:

Supportkontakt	Störungsinhalte	Kanäle
Anwender von beA Postfachbesitzer(innen) Mitarbeiter(innen) Rechtsanwaltskammern	Technische Probleme in beA Fragen zur Bedienung / Installation	Telefon E-Mail Portal
Schulungsanbieter	Verfügbarkeit Schulungsumgebung	Telefon E-Mail
Kanzlei- /Kammersoftwareanbieter	Störungen der Kanzleisoftware-Schnittstelle in beA	Telefon E-Mail
Bundesnotarkammer	Störungsfälle, die fehlerhaft dort gemeldet wurden und durch den beA-Support zu lösen sind	E-Mail
AG	Störungen in beA	SM-Tool des AN
EGVP-Projektbüro	Störungen im Datenaustausch zwischen beA und EGVP, einschließlich EGVP-Empfängersuche	Ticket-Tool der Justiz
beA Entwicklung	Weitergabe von Störungsmeldungen, wenn Code-Anpassung notwendig erscheint oder Entwickler-Unterstützung notwendig wird	Intern AN
Bundesnotarkammer (Trust Center Zertifikate)	Funktionalität im Datenaustausch und / oder Dateninhalte	E-Mail Telefon

Grundsätzlich sind alle Störungen und damit verbundene Aktivitäten im Service Management Tool (SM Tool) des AN nachvollziehbar zu dokumentieren. Für die Justiz ist ein eigenes Portal (aktuell auf Basis von Jira) im Einsatz. Für Störungsmeldungen, die vom AN an das EGVP-Projektbüro oder vom EGVP-Projektbüro an den AN erfolgen, ist das entsprechende Tool der Justiz zu benutzen. Der AN führt jeweils eine korrespondierende Fehlermeldung in seinem Tool und synchronisiert die Inhalte zumindest täglich.

Dem AG werden drei Bearbeitungsgruppen in dem Service Management Tool zur Verfügung gestellt, um die eigene Bearbeitung von Störungsmeldungen durchzuführen. Ein Routing zu anderen Bearbeitungsgruppen muss möglich sein.

Der Support ist durch den AN zu erbringen. Er hat alle Anliegen der beA-Anwender (Postfachbesitzer, Mitarbeiter, BRAK) gemäß den Zuständigkeiten zu bearbeiten. Darüber hinaus ist der Support des AN der Ansprechpartner für Partner (Rechtsanwaltskammern, Europäische Kommission, BNotK, Justiz, KSW-Hersteller) für Supportthemen, welche Informationen und/oder Maßnahmen in beA zur Bearbeitung von Störungen benötigen.

Die Entwickler des AN sind in dieser Rolle ausschließlich für Anpassungen der Software und/oder den Anforderungen an den Betrieb einzubinden. Wird dieses Personal für die folgenden Aufgaben des Betriebes eingebunden, so gelten die Prozesse, SLA, Dokumentation und sonstige Anforderungen des Betriebes uneingeschränkt.

5.1.1 Service Desk

Der AN muss einen Service Desk (SD) bereitstellen, der allen beA-Nutzern als zentrale Anlaufstelle (Single Point of Contact) für die Anwendungsunterstützung im Zusammenhang mit der Nutzung von beA dient und den 1st Level Support durchführt. Aufgaben des SD sind die Annahme, Qualifizierung und Lösung jeglicher Störungen, Anforderungen und Anfragen der Nutzer. Der Betrieb des SD und die Kommunikation mit Supportsuchenden muss in deutscher Sprache erfolgen.

Die Kontaktaufnahme mit dem Service Desk ist durch den AN über Telefon, E-Mail und Service Portal zu ermöglichen.

Mindestens die folgenden Aktivitäten müssen durch den AN im Rahmen des SD implementiert, im laufenden Betrieb durchgeführt und ständig verbessert werden:

- Annahme von Calls per Telefon, E-Mail oder über das Service Portal,
- Erfassung jedes Calls in elektronischer Form als Ticket und anschließende Priorisierung des Tickets. Jedes Ticket erhält einen genauen Zeitstempel,
- Übernahme der Ticket-Ownership für die Bearbeitung, Weiterleitung bzw. weitere Verfolgung eines Tickets und bis einschließlich dessen Abschluss,
- Weitergabe aller für die Ticketbearbeitung relevanten Kerninformationen an alle an der Ticketbearbeitung beteiligten Personen bzw. Parteien. Benötigt der AN zur Leistungserbringung zusätzliche Tickets, erstellt der AN diese Tickets ohne Mitwirkung des Nutzers,
- Das vom AN verwendete Ticketsystem muss in der Lage sein, automatisch eine Ticket-Eingangsmail mit eindeutiger Ticketnummer, Call-Beschreibung (Langtext), Priorität, Servicelevel und Aufnahmezeitstempel zu generieren,
- Sind für die Umsetzung der Anforderungen mehrere Tickets erforderlich, muss der AN diese in der zusätzlichen Kommunikation zum Nutzer zusammenfassen (z. B. eine E-Mail mit tabellarischer Übersicht der Einzeltickets). Anfragen der Nutzer zu einzelnen Tickets innerhalb dieser zusammengefassten Kommunikation müssen weiterhin möglich sein und müssen beantwortet werden,
- Aufbau einer Wissensdatenbank mit bekannten Fehlern und deren Behebung,
- Bereitstellung einer Telefonnummer für die Kontaktaufnahme mit dem SD,
- Bereitstellung einer E-Mail-Adresse für die Erreichbarkeit des SD,
- Bei Massenstörungen: Unverzügliche Information des AG insbesondere über betroffene Nutzer, Details der jeweiligen Störung und eingeleitete Maßnahmen. Darüber hinaus muss der AN die unverzügliche Information der Nutzer durch Schalten von Bandansagen für Anrufer beim SD und durch Meldungen im Service Portal sicherstellen. Der AN muss die Bandansagen bzw. Meldungen im Portal laufend aktualisieren. Nach Störungsbeseitigung muss der AN die Nutzer entsprechend informieren.

Mindestens folgende Fähigkeiten muss der AN im Rahmen der Störungsbearbeitung abdecken:

- Bedienung von beA, Installation und Update der Anwendung
- Kenntnisse über die Datenbestände in beA und Betriebsprozesse.

5.1.2 Störungsbearbeitung

Kann der SD gemeldete Störungen und/oder Anfragen nicht direkt beantworten, so muss der AN die Störung im Incident Management innerhalb der vereinbarten Service Level weiter bearbeiten.

Auch durch das Monitoring erkannte Abweichungen sind als Störung zu dokumentieren und diese innerhalb der vereinbarten Service Level zu beheben.

Der AN muss einen Anwendungsbetrieb bereitstellen, der alle vom SD nicht direkt gelösten Störungsmeldungen übernimmt. Zudem werden hier die Monitoring-Ergebnisse zusammengeführt. Folgende Aufgaben muss der Anwendungsbetrieb mindestens durchführen:

- Prüfung der Zuständigkeiten der Supporteinheiten, sofern eine Weiterleitung notwendig ist. Dies beinhaltet auch die Klärung von Unstimmigkeiten des Verständnisses am Support beteiligter Stellen.
- Koordination mit Dritten oder anderen Supporteinheiten, wenn die Störungsbehebung nur mit einer übergreifenden Zusammenarbeit möglich ist.
- Steuerung der Störungsbearbeitung durch Supportgeber außerhalb des Betriebs. Überwachung der entsprechenden Service Level KPI.
- Eine weitergehende Analyse und Qualifizierung der Störungsmeldung ist durch den AN durchzuführen.
- Auf Basis der eigenen Erkenntnisse und/oder Informationen aus der Entwicklung oder Dritten sind Vorgaben zur Störungsbehandlung durch den SD zu erstellen.
- Entwicklung, Bereitstellung und Anwendung von Workarounds (Datenkorrekturen) für Störungen.
- Verantwortung für die Korrektur von Daten und Prüfung von Abweichungen zu Anforderungen.
- Wiederherstellung des Normalbetriebes nach Ausfällen einschließlich Datenrecovery und Koordination der Datenkorrekturen. Dies beinhaltet die Folgen von SW-Fehlern und der Korrektur fehlerhafter Daten.
- Analyse von Problemen und Koordination von Anforderungen zur Risiko-Minimierung.
- SLA von nachgelagerten Serviceorganisationen (Hersteller, Dienstleister, Entwicklung etc.) sind zu überwachen und bei Überschreitung der AG aktiv zu informieren.
- Durchführung der Kommunikation zum AG bzgl. Status und Rückfragen von Störungsbearbeitungen.
- Überführung der Störungsmeldung in ggf. externes Tickettool eines weiteren Supportgebers (z. B. Jira-Justiz).

Mindestens folgende Fähigkeiten muss der AN im Rahmen der Störungsbearbeitung abdecken:

- Detailkenntnisse über Abläufe in beA einschließlich dem Datenaustausch mit Dritten und Prüfmöglichkeiten auf Konsistenz und Integrität der Daten,
- Bedienung von beA und der entsprechenden Bedienung durch Anwender,
- Datenkorrektur gemäß Vorgaben,
- Detailkenntnisse der beA-Anwendung,
- Detailkenntnisse über das beA Datenmodell,
- Abgrenzung der Ursache zwischen Daten und Softwarefunktion.

5.1.3 Remote Support

Der AN muss im Rahmen der Nutzerbetreuung einen zentralen Remote Support zur Nutzerunterstützung und zur Lösung von Incidents erbringen. Der Remote Support muss den Anforderungen an die anwaltliche Verschwiegenheitspflicht entsprechen, insbesondere also die in dieser Leistungsbeschrei-

bung aufgeführten Sicherheitsvorgaben sowie die sonstigen datenschutzrechtlichen Bestimmungen einhalten.

Der AN muss die notwendigen Hard- und Software-Infrastruktur für die Erbringung der Remote Services bereitstellen und betreiben.

Der AN muss alle im Rahmen des Remote Supports tätigen Mitarbeiter auf das Datengeheimnis insbesondere im Hinblick auf die Anforderungen an die anwaltliche Verschwiegenheitspflicht gem. § 43a Abs. 2 BRAO sowie unter Hinweis auf die straf- und ordnungswidrigkeitsrechtlichen Konsequenzen (u. a. § 203 StGB) verpflichten.

Der Remote Support muss von einem Standort des AN aus erfolgen, wobei eine Remote Support-Software für die Übernahme und Bedienung des Arbeitsplatzsystems verwendet wird, um dem Supportpersonal des AN die Nutzerunterstützung bzw. Störungsfeststellung und Störungsbeseitigung zu ermöglichen. Der Remote Support muss unter Berücksichtigung der folgenden Sicherheitsvorgaben durchgeführt werden:

- Der Nutzer muss vor der Übernahme der Steuerung des Endgerätes durch den Support-Mitarbeiter des AN aktiv zustimmen.
- Während der Remote-Übernahme durch den AN muss der Nutzer genau verfolgen können, welche Arbeiten vom Remote Support auf seinem Endgerät durchgeführt werden.
- Der Nutzer muss die Remote Support-Sitzung jederzeit beenden können.
- Die Verbindung zwischen AN und dem Endgerät des Nutzers muss verschlüsselt sein.
- Bei jeder Nutzung des Remote Supports muss der Support-Mitarbeiter den Anrufenden auf die Verantwortung des Anrufenden für den Mandantenschutz hinweisen und empfehlen, ggf. alle Fenster auf der Benutzeroberfläche, die vertrauliche Daten oder Informationen enthalten, vor Aufbau der Remote Verbindung zum Endgeräte des Nutzers zu schließen.
- Der AN muss sicherstellen, dass es dem Support-Mitarbeiter untersagt ist, von den Endgeräten der Nutzer Screenshots zu erzeugen oder Downloads von Daten durchzuführen.

5.1.4 Service Portal

Der AN muss im Web-basierten Service Portal eine Funktion bereitstellen, die dem Nutzer erlaubt, Tickets zu eröffnen und so Störungen, Anforderungen und Anfragen mit geringer Priorität an den Service Desk zu übermitteln. Gleichzeitig muss der Nutzer den Verlauf und den aktuellen Bearbeitungsstatus durch den Service Desk abfragen können.

Darüber hinaus muss der AN mindestens folgende Möglichkeiten im Service Portal für den Nutzer bereitstellen:

- Status-Informationen zur Verfügbarkeit von beA und Informationen zu aktuellen Störungen, Einschränkungen oder Wartungsarbeiten,
- Hinweise an den AG zur Optimierung der Online Hilfe zur Nutzung und Verwaltung von beA,
- Nutzung einer Wissensdatenbank mit bekannten Fehlern und deren Beseitigung.

5.1.5 Reporting

Folgende Mess- und Berichtsgrößen muss der AN mindestens monatlich bereitstellen:

5.1.5.1 Leistungsrelevante Größen

- Erreichbarkeit,
- Lösungsquote des Service Desk,
- Lösungsquote nachgelagerter Supporteinheiten,
- Anzahl Eingänge über Telefon, Online Portal oder E-Mail mit Reaktionszeit größer als Vorgaben,
- Kundenzufriedenheit.

5.1.5.2 Statistische Größen

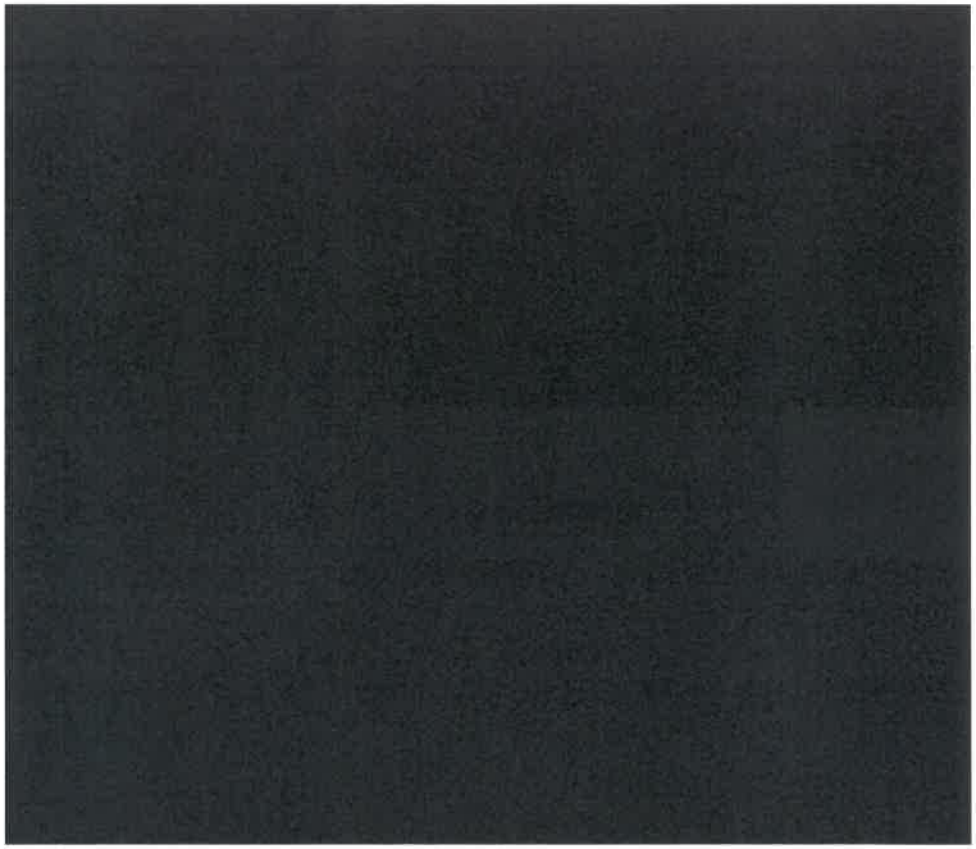
- Anzahl Anrufe (angenommen, verloren, abgebrochen etc.),
- Anzahl der Tickets gegliedert nach Störungen (Incidents), Anforderungen (Service Request), Anfragen (Request for Information) und Problems,
- Anzahl E-Mail Eingänge,
- Anzahl Online Portal Eingänge,
- Anzahl der Langläufer Tickets >7 Tage sowie >3 Monate,
- Anzahl Tickets “closed”, “open”, “reopened”, und „suspended“,
- Anzahl der in den Anwendungssupport weitergeleiteten Tickets.

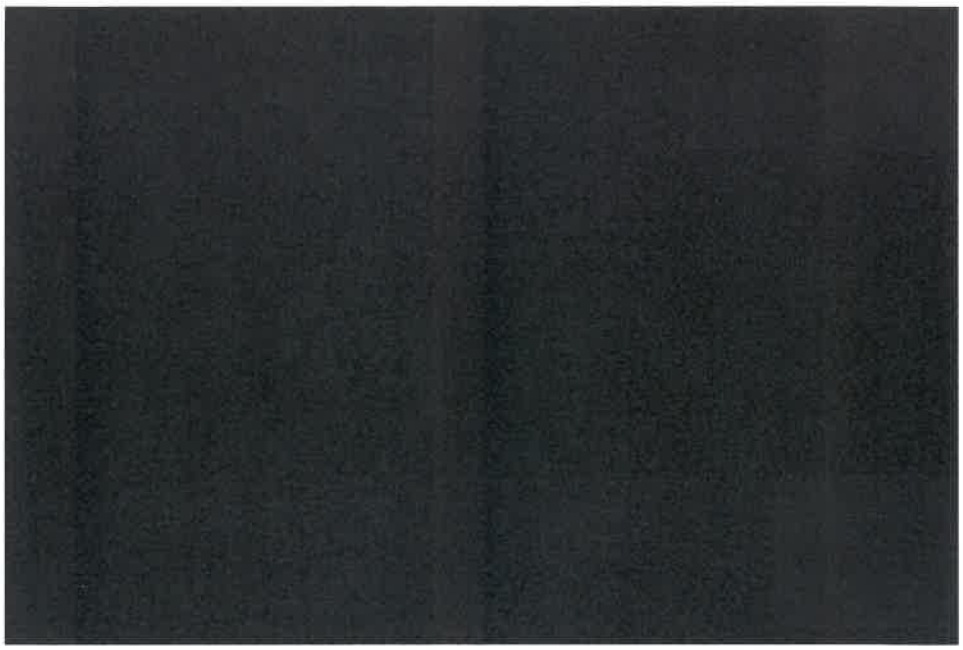
5.1.6 Abgrenzung

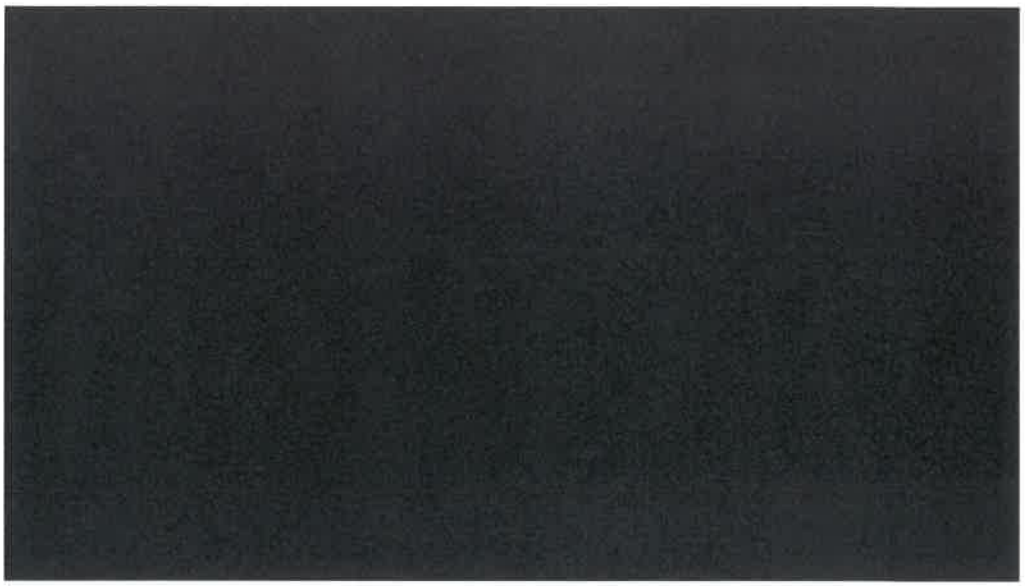
Folgende Aktivitäten sind nicht Bestandteil der Nutzerunterstützung durch den Service Desk:

- Anlegen oder Löschen von Postfächern. Dies erfolgt durch einen automatisierten Prozess im beA unter der Verantwortung der Rechtsanwaltskammern,
- Verwaltung von angelegten Postfächern. Dies erfolgt durch den Postfachbesitzer oder den Systemverwalter der BRAK,
- Unterstützung bei der Nutzung von Kanzleisoftware,
- Entstörung der Nutzer-Endgeräte, insbesondere in Bezug auf Hardware, Betriebssystem, Peripheriegeräte wie Kartenleser, Drucker, Tastatur oder Maus,
- Initiierung und Steuerung von Onsite Support Einsätzen zur Entstörung von Nutzer Endgeräten oder Nutzer Peripheriegeräte.

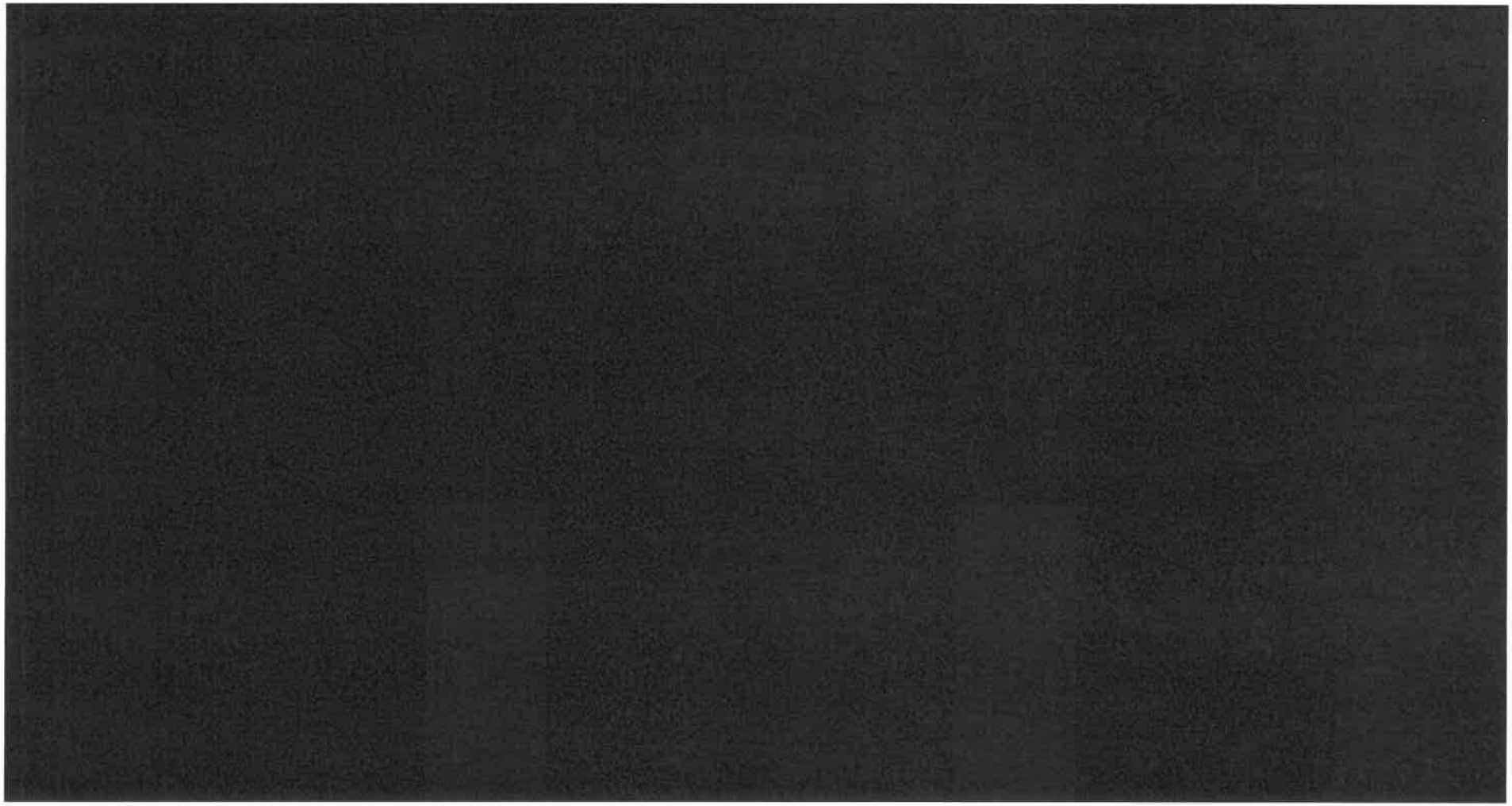
Anhang 1 zur Leistungsbeschreibung:

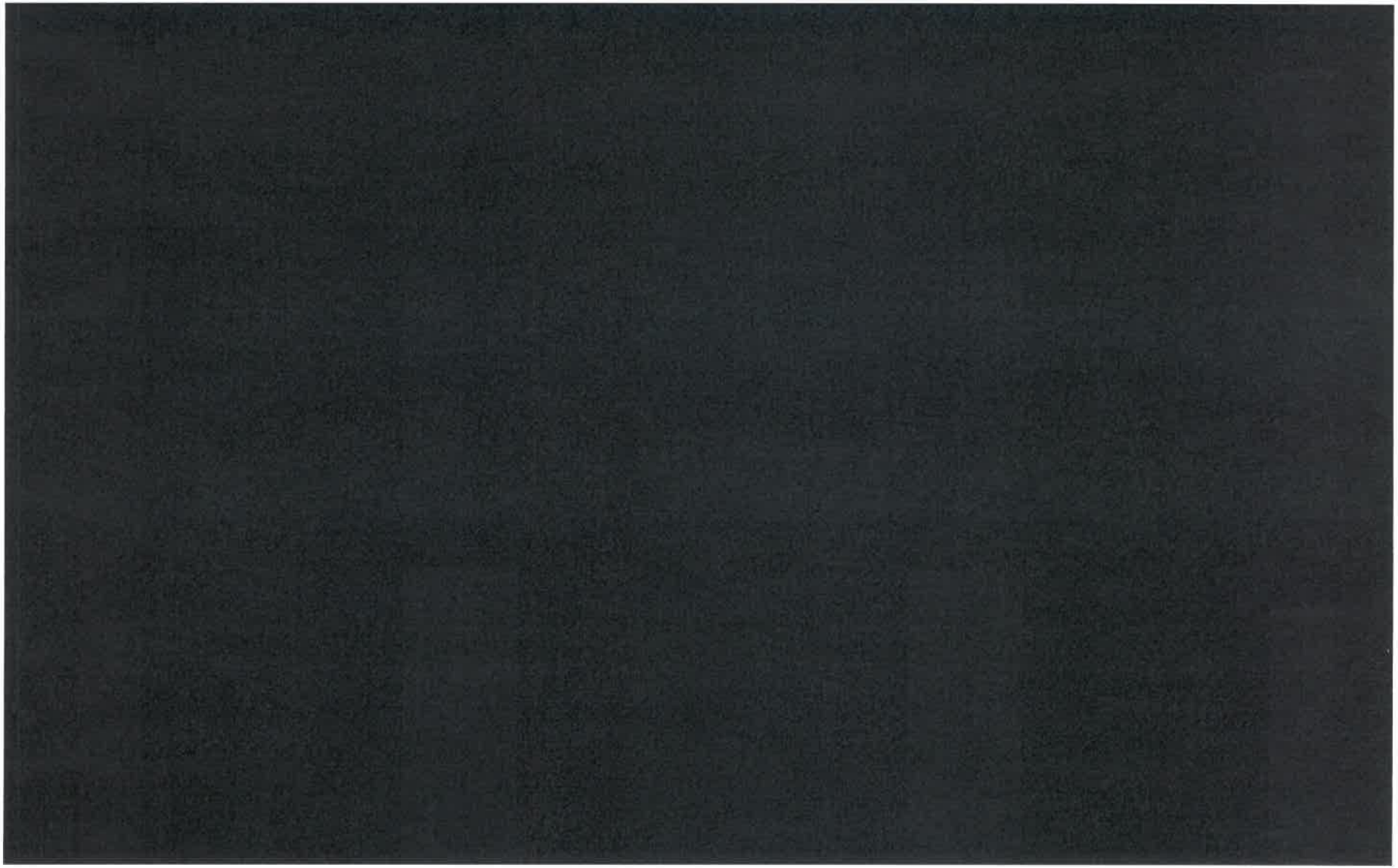


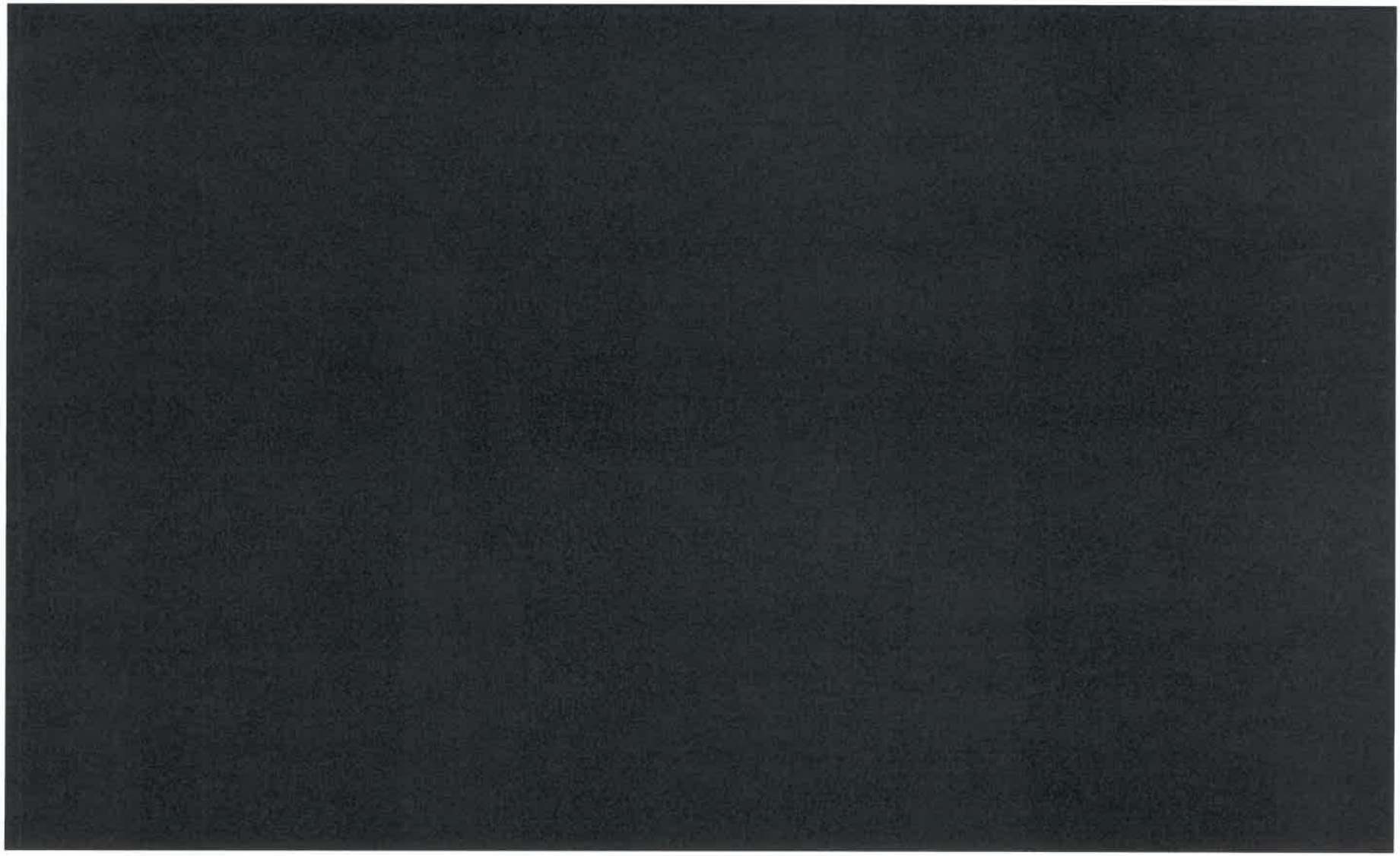


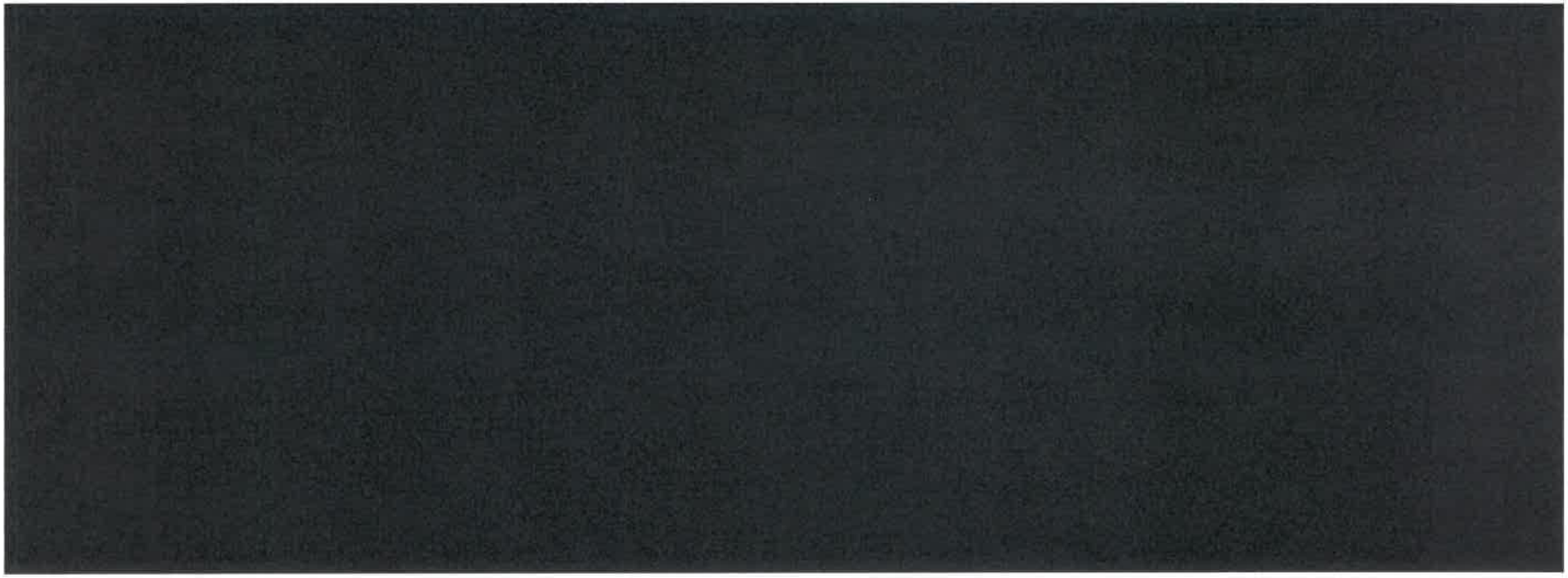


Anhang 2 zur Leistungsbeschreibung:









Anhang 3 zur Leistungsbeschreibung: