Teil B Leistungsbeschreibung

(wird bei Zuschlagserteilung Vertragsbestandteil)

Debitkarte 2026-2

Bei der vorliegenden Ausschreibung handelt es sich um die Rückversetzung des Verfahrens 12-26-00011 in die Angebotsphase.

Anlagen:

Anlage 1	Entfällt
Anlage 2	Organisationsstruktur der BA / Lieferantenmanagement
Anlage 3	Technische und organisatorische Maßnahmen (TOM)
Anlage 4	Entfällt
Anlage 5	Angaben zu Software-Nutzungsrechten

Inhaltsverzeichnis

1. Gegenstand und Ziel der Ausschreibung

1.1 Allgemeines

Die Bundesagentur für Arbeit (BA) und die gemeinsamen Einrichtungen (gE) (siehe Anlage 2) zahlen im gesetzlichen Auftrag Geld an Leistungsempfangende aus. Dies erfolgt im Regelfall per Überweisung auf Konten der Zahlungsempfangenden.

Es besteht keine gesetzliche Verpflichtung, Leistungen als Barzahlung auszuzahlen. Jedoch sind rund 4.000 berechtigte Leistungsempfänger (bundesweit) nicht gewillt und auch nicht verpflichtet ein Bankkonto zu führen. Die Fürsorgepflicht der BA erfordert daher eine Versorgung mit Geldmitteln auch über Bargeld oder über ein anderes Zahlungsmittel, das kurzfristig und unkompliziert in Bargeld umgewandelt werden kann.

Für die BA und die gE besteht die gesetzliche Verpflichtung nach § 47 SGB I, Geldleistungen an den Wohnsitz oder gewöhnlichen Aufenthalt einer Person, die nachgewiesen kein Konto erhalten hat, zu übermitteln.

Bargeldauszahlungen in allen Dienststellen der BA oder gE sicher und stets ausreichend zur Verfügung zu stellen, ist bei einer fast ausschließlich unbaren Abwicklung von Sozialleistungen in der BA herausfordernd. Daher hat sich die BA für eine Auszahlungsmöglichkeit von Sozialleistungen an kontolose Personen für die sog. Debitkarten entschieden.

1.2 Ziel

Die BA (nachfolgend Auftraggeber (AG) genannt) und gE benötigen eine Lösung zur Bargeldversorgung von Leistungsempfangenden (Kundinnen und Kunden der BA/gE, die Leistungen nach dem SGB II und SGB III erhalten) ohne Bankkonto.

Die Debitkarte soll den Leistungsempfangenden (im folgenden Kartennutzende genannt) hierbei einen einfachen und diskriminierungsfreien Zugang zu ihren Sozialleistungen ermöglichen und dazu dienen, die weggefallene Auszahlung in Form von Schecks durch eine moderne Kartenlösung zu ersetzen und Leistungen schnell und digital an Leistungsempfangende der BA und der gE ohne Bankkonto im SEPA-Raum auszuzahlen. Die Leistungsempfangenden, die eine Debitkarte erhalten, sind damit Karteninhabende, bzw. Kartennutzende (siehe Glossar).

Dies soll auch die im Arbeitsprogramm des Vorstands angestrebte Stärkung der Nutzung der Digitalisierung („Wir nutzen die Möglichkeiten der Digitalisierung im Interesse unserer Kundinnen und Kunden, Mitarbeiterinnen und Mitarbeiter.“) unterstützen.

Nicht zuletzt stellt die angestrebte Kartenlösung auch eine gleichberechtigte Teilnahme am gesellschaftlichen Leben sicher.

2. Ausschreibungsgegenstand

Während des Leistungszeitraums (s. Kap. 4) sind folgende Leistungen vom Auftragnehmer (AN) zu erbringen, die den Anforderungen gemäß Kapiteln 2 und 3 entsprechen:

Gesamtsystem (nicht-optional):

- Ausgabe von Debitkarten in Form von Consumer Debitcards (s. Kapitel 2.1 und Preisgruppe 1 im Leistungsverzeichnis (LV))
    - Bereitstellung und Betrieb physischer sowie virtueller Debitkarten (+ dazugehöriger Zahlungsinfrastruktur) für ca. viertausend (4.000) Kartennutzende
    - Bundesweiter Versand von Karten in Paketen mit Stückelungen von Einzelkarten an verschiedene Adressen
- Webanwendung für die Verwaltung der Karten für Mitarbeiterinnen und Mitarbeiter der BA und gE (MA) (s. Kap. 2.3.1)

  - Einrichtung und Bereitstellung einer Webanwendung für Mitarbeitende der BA und gE über den Browser (s. Kap. 2.3.1) inkl. Betriebsservices und Support (s. Kap. 2.4).
- Online-Portal und App für Kartennutzende (s. Kapitel 2.3)
  - Bereitstellung eines Online Portals für Kartennutzende (s. Kap. 2.3.2) inkl. Betriebsservices und Support (s. Kap. 2.4)
  - App (iOS und Android) für Kartennutzende um damit den „Kontostand“ einsehen zu können und alle weiteren Funktionen nutzen zu können (s. Kap. 2.3.2) Optional auch für die Nutzung der virtuellen Debitkarte inkl. Betriebsservices und Support (s. Kap. 2.4).

Sonstige nicht optionale Leistungen:

- Qualifizierung/Qualifizierungsmaterial für Mitarbeitende der BA und der gE (s. Kap. 2.7)

Optionale Leistungen:

- Optionales Dienstleistungskontingent (s. Kap. 3.4)

Bei den im LV aufgeführten Mengen handelt es sich um Schätzmengen, aus denen keinerlei Ansprüche durch den AN abgeleitet werden können. Die tatsächlichen Mengen können höher oder niedriger ausfallen. Eine Abrufverpflichtung für die BA besteht nicht.

Die Höchstmenge für diese Beschaffung beläuft sich auf 4.800 Karten. Diese Menge stellt die vergaberechtliche Obergrenze zur Nutzung der Rahmenvereinbarung dar und hat keinen Zusammenhang mit von der BA zugrunde gelegten Schätzmengen oder von der BA vorgesehenen Haushaltsmitteln.

2.1 Bereitstellung Gesamtsystem und Debitkarten-Nutzung

2.1.1 Kartenlieferung

Die initialen Kartenabrufe für die Erstausstattung erfolgen direkt nach Zuschlagserteilung innerhalb von fünf AT.

Die Lieferung hat auf Abruf an von der BA zur Verfügung zu stellende Dienststellenadressen zu erfolgen. Die Lieferung für die Erstausstattung muss sieben AT nach Abruf bei diesen Dienststellenadressen eingegangen sein. Kartennachlieferungen während der weiteren Vertragslaufzeit müssen innerhalb von fünf AT bei der abrufenden Stelle der BA oder der gE eingegangen sein.

Jeder Sendung ist ein Lieferschein mit Angabe der spezifischen Auftragsdaten (mindestens Bestellnummer, Warenempfänger, Belegnummer) beizufügen.

2.1.2 Inbetriebnahme Gesamtsystem

Das Gesamtsystem (bestehend aus SaaS-Lösung s. Kapitel 2.3 und Zahlungsinfrastruktur bzw. Zahlungsdienstleistung/Debitkarten) muss mit dem Start der Ausgabe der Karten unverzüglich funktionieren (konkrete Ausführungen in Kapitel 2.1). Alle zur Kartennutzung erforderlichen Voraussetzungen müssen rechtzeitig ab Vertragslaufzeit erfüllt und die Debitkarten ab Aktivierung vollumfänglich nutzbar sein.

Die jeweils bei Abruf bestimmten Kontingente an physischen Debitkarten sind für den Initialabruf in den dort benannten Zeiträumen (Initialabruf-Lieferfrist 7 AT) an die benannten Stellen zu liefern, bzw. die optional virtuellen Debitkarten bereitzustellen. Die noch nicht aktivierten Blankokarten sind in einem verschlossenen Briefumschlag zur Verfügung zu stellen. Kartennachbestellungen sind mit Lieferfristen von fünf AT auszuliefern

(ausschlaggebend ist der Eingang bei der abrufenden Stelle). Der AN muss sicherstellen, dass im Ausnahmefall bei kurzfristig benötigter Nachbestellung physischer Karten unverzüglich geliefert werden.

Debitkarten müssen unmittelbar nach Anlage des Datensatzes zum Kartennutzenden (in der Webanwendung für MA) aktiviert und anschließend in den Dienststellen direkt an die/den Kartennutzenden ausgegeben werden können. Die Erfassung der Daten erfolgt zur Erfüllung der gesetzlichen Vorgaben im Zusammenhang mit der Erbringung der Zahlungsdienstleistung durch den AN. Physische Karten müssen sowohl ohne Smartphone genutzt werden können als auch virtuell in einer vom AN zur Verfügung gestellten App auch auf dem Smartphone mit den Betriebssystemen iOS und Android nutzbar sein, als auch mit anderen verbreiteten Apps nutzbar sein (z.B. Google Pay, Apple Pay, Samsung Pay).

Die zur Kartennutzung erforderliche PIN wird seitens des AN so zur Verfügung gestellt, dass die Karte umgehend genutzt werden kann und nur die/der Kartennutzende Kenntnis von der PIN erhält.

2.1.3 Design der Debitkarte

Die Debitkarte soll neutral gestaltet sein. Hierbei sind insbesondere Aufdrucke von Logos oder der Name der Karteninhaberin oder des Karteninhabers (ohnehin erst bei Aktivierung bekannt) nicht zugelassen. Neben den rechtlich bzw. von den Schemes vorgeschriebenen Mindestangaben soll auf der Karte nur die dazugehörige Kartennummer ersichtlich sein.

2.1.4 Kartenausgabe

Der AG erhält die Möglichkeit, über eine Webanwendung für MA Debitkarten für Kartennutzende zu aktivieren und diesen verfügbare Geldbeträge zuzuordnen. Die Kartennutzenden sind alleinige Eigentümer/innen und Besitzer/innen der Debitkarte. Der AG bleibt im Nutzungsverhältnis außen vor und trägt nach Ausgabe der Karten dafür keine Verantwortung. Deshalb erhalten Kartennutzende die Vereinbarung und die Datenschutzerklärung des AN bei Aktivierung der Debitkarte. Die Empfangsbestätigung der Zustimmung zur Vereinbarung und der Datenschutzerklärung werden in der BA und den gE dokumentiert und archiviert. Die Vereinbarung muss alle Aspekte zur Nutzung der Debitkarte erklären und für die Kartennutzenden verständlich aufbereitet sein. Die Unterzeichnung der Vereinbarung erfolgt zur Erfüllung der gesetzlichen Vorgaben im Zusammenhang mit der Erbringung der Zahlungsdienstleistung durch den AN. Folgende Aspekte sind aufzunehmen:

- Definition und Aufklärung zu allen wesentlichen Begriffen
- Erklärung, was bei Erhalt und Aktivierung der Karte erfolgen muss
- Beschreibung, wie und wo die Karte verwendet werden kann
- Beschreibung, wie Bargeld mit der Karte ausgezahlt werden kann
- Information, welche Entgelte bei welchen Transaktionen von der Kartennutzerin, vom Kartennutzer zu zahlen sind
- Darstellung, ob Beschränkungen bei Verwendung der Karte bestehen
- Information, wo und wie Informationen zum „Kontostand“ abrufbar sind
- Informationen, was beim Umgang mit der Karte zu beachten ist
- Information, wo und wie Kartennutzendeden Support bei Problemen und Fragen erreichen
- Information, wie ein Sperren der Karte bei Verlust oder defekter Karte möglich ist
- Ggf. Informationen, was nicht in der Verantwortung des Auftragnehmers liegt
- Informationen, wofür der Auftragnehmer und wofür der/die Kartennutzende haftet
- Informationen zur Gültigkeit der Karte

- Informationen zur Beendigung der Vereinbarung
- Informationen zu sonstigen rechtlichen Bestimmungen

Die Datenschutzerklärung muss alle wesentlichen Aspekte beinhalten. Folgende Aspekte sind zwingend (nicht abschließend):

- Allgemeine Hinweise und Rechtsgrundlage (DSGVO)
- Weitere gesetzliche Verpflichtungen und Bestimmungen
- Welche Daten werden verarbeitet
- Wer verarbeitet die Daten und ist dafür verantwortlich
- Wer bekommt die Daten (siehe auch Nutzung von Apps)
- Wie werden die Daten erfasst
- Wofür werden die Daten genutzt
- Vertragliche Pflichten des Auftragnehmers in Bezug auf die Verarbeitung der Daten
- Welche Daten werden bei der Nutzung von Apps (wie Apple Pay oder Google Pay) erhoben oder weitergeben
- Dauer der Speicherung
- Alle Rechte der/des Kartennutzenden

Zudem wird der AG die Kartennutzenden anhand persönlich vor Ort vorgelegter Ausweisdaten identifizieren. Der AN muss keine Kartennutzenden identifizieren. Die Ausweisdaten werden in der Webanwendung für MA eingetragen und gespeichert. Es darf keine Kopie des Ausweisdokuments in BA-Systemen oder in der Webanwendung des AN gespeichert werden. Es muss ausreichend sein, die Ausweisdaten in der Webanwendung abzuspeichern.

Bei der Ausgabe einer physischen Debitkarte händigt der AG der/dem Kartennutzenden eine physische Karte in einem verschlossenen Briefumschlag aus und aktiviert die Debitkarte anhand einer Kartennummer in der Webanwendung für MA. Für Dritte darf die zugehörige PIN nicht einsehbar sein. Den Kartennutzenden wird ein Autorisierungscode mitgeliefert, den sie für die einmalige Registrierung im Online-Portal für Kartennutzende oder in der App benötigen (siehe Kap. 2.3).

Der AN verpflichtet sich, für alle Kartennutzenden nach Übergabe der notwendigen Kunden- und Ausweisdaten und Neuanlage einer Karte, eine individuelle virtuelle IBAN (entspricht einer IBAN ohne Bankkonto) je Debitkarte zur Verfügung zu stellen. Auf diese überweist der AG Geldbeträge, um den Kartennutzenden ein Limit zur Nutzung der Debitkarte in Höhe dieses Geldbetrages verfügbar zu machen. Die Verfügbarkeit von Geldern ist auf die von dem AG überwiesenen Beträge beschränkt, Überziehungsmöglichkeiten für Kartennutzende dürfen nicht bestehen.

Um den Kartennutzenden den bestmöglichen Service bieten zu können, erstellt der AN eine Zusammenfassung auf einer Seite (Onepager) mit den wichtigsten Informationen für den täglichen Gebrauch der Karte in PDF-Format. (z.B. als Flyer: Wie wird die Karte aktiviert? Wie und wo kann damit bezahlt werden? Wie und wo kann damit Bargeld abgehoben werden? Welche Kosten fallen an? Wie kann die Karte gesperrt werden? Wie kann der Kontostand abgefragt werden? Wie kann der Support erreicht werden? Wo und wie kann die App genutzt werden? Was kann mit der Debitkarte nicht gemacht werden, insbesondere Geldeingänge von anderen Konten oder Lastschriften, Wie werden Änderungen z.B. bei der Datenschutzerklärung mitgeteilt?). Dieser Flyer wird bei Kartenausstellung mit der

Vereinbarung und Datenschutzerklärung vom AG ausgedruckt und den Kartennutzenden ausgehändigt.

2.1.5 Kartengültigkeit

Die Laufzeit der Karte soll sich an branchenüblichen Standards orientieren und mindestens 4 Jahre betragen. Die Karte soll danach nicht wieder an den AN oder den AG zur Entsorgung zurückgeschickt werden, sondern verbleibt bei den Kartennutzenden.

2.1.6 Verfügbarkeit der Debitkarte virtuell und physisch

Die Debitkarte muss sowohl als physische, optional auch als digitale, auf dem Smartphone verfügbare (virtuelle) Karte mit NFC (Near Field Communication) ausgegeben werden können.

Die bargeldlose Bezahlfunktion der Debitkarten muss branchen- und handelsüblich ausgestaltet sein (PIN als Missbrauchs- und Diebstahlschutz).

Die Debitkarte muss nach Aufladung einen unkomplizierten und schnellen Zugang zu Geldleistungen und Bargeldabhebungen im Einzelhandel und am Geldautomaten ermöglichen. Die Karte muss auch Bargeldverfügungen bei Einzelhändlern zulassen, die es im Rahmen des Einkaufs ermöglichen, Bargeld abzuheben. Für die Bargeldabhebung im Einzelhandel gelten die Bedingungen der Einzelhändler. Für die Bargeldabhebung an Geldautomaten gelten die Bedingungen der Geldautomatenbetreiber. Die Debitkarte soll als Plastikkarte (die Regel), als auch virtuell, nutzbar sein. Ein Kreditrahmen ist ausgeschlossen. Die Karten können von den Kartennutzenden grundsätzlich nur auf Guthabenbasis eingesetzt werden.

2.1.7 Standardzahlungsprozess

Der AG nutzt die individuelle virtuelle IBAN für die Zahlung von Geldbeträgen zugunsten des jeweiligen Kartennutzenden. Diese können monatlich variieren. Per SEPA-Überweisung (SCT) überträgt die BA den entsprechenden Geldbetrag zugunsten der virtuellen IBAN. Der AN wird nach Zahlungseingang den Geldbetrag der entsprechenden Debitkarte zuordnen und dieser ein entsprechendes Limit einräumen. Es steht keine Überziehungsmöglichkeit zur Verfügung (abgesehen von der Ad-Hoc-Limit-Erhöhung siehe Kap. 2.1.9).

2.1.8 Stornobuchungen

Da die Debitkarte über eine Bezahlfunktion verfügt, muss es möglich sein, dass der Handel Storno- und Rückbuchungen auf die Karte ausführen kann (beispielsweise bei der Rücknahme von Waren).

2.1.9 Ad-hoc-Limit-Erhöhung

Neben dem Standardzahlungsprozess muss für Notfälle die Möglichkeit bestehen, Leistungsempfangenden unverzüglich das Limit auf der Debitkarte erhöhen zu können, ohne zuvor den Geldbetrag überwiesen zu haben. Nach Auswahl der Ad-hoc-Limit-Erhöhung und Eingabe des Wertes in der Webanwendung für MA räumt der AN der entsprechenden Debitkarte unverzüglich ein entsprechendes Limit ein. Die Web-Anwendung und Funktion der Ad-hoc-Limit-Erhöhung muss so gestaltet sein, dass diese über ein Vier-Augen-Prinzip von zwei Anwendenden des AG technisch voneinander getrennt, freigegeben werden muss.

Die **Nutzung eines Sammelkontos**, das vorab von dem AG mit einem Guthaben ausgestattet werden muss, ist **ausgeschlossen**. Gemäß der Verwaltungsvorschrift für Zahlungen, Buchführung und Rechnungslegung (§§ 70 bis 71 sowie 75 bis 80 BHO) - VV-ZBR BHO widerspricht die Verwendung eines Sammelkontos den Grundsätzen der Haushaltsklarheit und -wahrheit. Die Überweisung muss direkt auf die individuelle virtuelle IBAN je Debitkarte erfolgen. Dabei muss der AN in Vorleistung treten. Erst mit einer nachträglichen Ausgleichszahlung auf die individuelle virtuelle IBAN wird dem AN die Vorleistung von der BA, bzw. den gE ausgeglichen (siehe auch Kap. 3.3).

2.1.10 Karten sperren, entsperren und kündigen

Der AG muss in der Lage sein, in der Webanwendung für MA den jeweiligen Status, in dem sich eine Karte befindet, einzusehen (aktiviert, gesperrt, entsperrt, gekündigt). Damit ist keine Berechtigung für Karten sperren, entsperren oder kündigen, verbunden.

Kartennutzende müssen die Möglichkeit haben, die Debitkarte selbst oder durch Inanspruchnahme des Supports des AN (z. B. Kundendienst, Website und/oder App des AN) 24/7 sperren zu können. Es muss sichergestellt sein, dass jede/ jeder Kartennutzende nur die eigene Karte sperren kann.

Nach Setzen der Kartensperre darf keine Transaktion mehr mit der Karte möglich sein. Auf der Karte noch vorhandenes Guthaben verbleibt auf der Karte, ist aber gesperrt. Eine erfolgreiche Sperrung der Karte muss in der Anwendung angezeigt werden.

Muss ggf. Guthaben von einer gesperrten Karte auf eine neue Karte übertragen werden, muss auf Anfrage des AG (BA oder der gE) vom AN das noch vorhandene Guthaben auf eine neue virtuelle IBAN und somit umgehend auf eine neue Karte transferiert werden.

Ebenso muss im Online-Portal für Kartennutzende ein Entsperren durch die Kartennutzenden möglich sein. Die erfolgreiche Entsperrung der Karte muss in beiden Systemen (Online-Portal für Kartennutzende und Webanwendung für MA) angezeigt werden. Nach dem Entsperren muss die Karte direkt wieder vollständig nutzbar sein, damit die Kartennutzenden uneingeschränkt über das vorhandene Guthaben verfügen können.

Sollen dauerhaft keine weiteren Zahlungen auf die ausgestellte Karte überwiesen werden, muss die Debitkarte über das Online-Portal für Kartennutzende gekündigt oder dauerhaft gesperrt werden können. Bei Fällen, in denen die Leistungsempfangenden (Kartennutzenden) aus dem Leistungsbezug des AGs fällt, soll die gleiche Karte später bei erneutem Leistungsbezug wieder nutzbar sein (solange die Laufzeit der Karte noch nicht abgelaufen ist). Solange keine Zahlungen erfolgen, soll die Karte „ruhen“, also weder gekündigt, noch gesperrt werden müssen. Der AN bestätigt, dass für ungenutzte Karten, die nicht monatlich aufgeladen werden, keine monatlichen Gebühren oder sonstige Kosten anfallen.

2.2 Beistellungsleistungen des AG

2.2.1 IBAN Whitelist

Der AG meldet an den AN die IBANs, von denen die Überweisungen zugunsten der ausgegebenen Karten durchgeführt werden. Zur Vermeidung von Geldwäscherisiken und -missbrauch werden nur Zahlungen von den angegebenen IBAN akzeptiert. Die Meldung der IBAN erfolgt 7 AT vor der initialen Inbetriebnahme (siehe Kap. 2.1.2). Nachmeldungen werden spätestens nach 7 AT durch den AN bearbeitet.

2.2.2 IBAN für Rücküberweisungen

Der AG meldet dem AN eine IBAN für mögliche Rücküberweisungen (Zurückführung von Kartenguthaben an den AG). Die Meldung der IBAN hat sieben AT vor der initialen Inbetriebnahme zu erfolgen.

2.2.3 IP-Whitelistung

Für den Zugriff auf die Webanwendung für MA schaltet der AN die IP-Adressen der AG frei. Der AG ist verpflichtet, seine ausgehenden IP-Adressen bzw. IP-Ranges dem AN mitzuteilen. Die Meldung erfolgt 14 AT vor der initialen Inbetriebnahme (siehe Kap. 2.2.1). Nachmeldungen werden innerhalb 2 AT durch den AN bearbeitet.

2.3 Webanwendung für Mitarbeiterinnen und Mitarbeiter, und Online-Portal und App für Kartennutzende (SaaS-Lösung)

Der AN stellt dem AG eine Webanwendung für Mitarbeiterinnen und Mitarbeiter (kurz: MA). als Webanwendung über Browser für die Administration der Debitkarten während des Vertragszeitraums (s. Kapitel 4) zur Nutzung bereit. Die Webanwendung wird als Software-as-a-Service (SaaS) vom AG genutzt. Nähere Anforderungen zur IT-Sicherheit sind in Kap. 6 beschrieben.

Außerdem wird vom AN ein über Browser nutzbares Online-Portal und eine App für Kartennutzende (ebenfalls als SaaS) bereitgestellt. Kartennutzende umfasst alle in Kap 1.2 erwähnten Leistungsempfangenden des AG, die über kein Konto verfügen und dafür die Debitkarte als Kartennutzende und Karteninhaber/innen erhalten.

Produktbezeichnung und -beschreibung, Produkt-Nr.	Lizenzart	Anzahl
Webanwendung für Mitarbeiterinnen und Mitarbeiter (MA) zur Erstellung und Verwaltung von Debitkarten	Unternehmens-lizenz	1
Online-Portal für Kartennutzende	Unternehmens-lizenz	1
App für Kartennutzende	Unternehmenslizenz	1

2.3.1 Webanwendung für Mitarbeiterinnen und Mitarbeiter (MA)

Der AN verantwortet die Bereitstellung und den Betrieb der Webanwendung sowie die zugehörigen Betriebsservices und Support (siehe Kap. 2.4). Der AN übernimmt die technische Verknüpfung der Debitkarten mit der Webanwendung, d.h. diese Tätigkeiten fallen nicht in den Verantwortungsbereich des AG. Der AN muss gewährleisten, dass die vereinbarten Leistungen in der Webanwendung ausgewählt werden können.

Der AN muss alle notwendigen Services zur Verfügung stellen, damit berechtigte MA des AG über eine Webanwendung sämtliche Prozesse rund um die Debitkarte administrieren, verwalten und steuern können. Die Webanwendung muss **min.** folgende Funktionen/Sachverhalte bieten:

- Neue Karte erstellen (Kundendatensatz, inkl. BA/gE interne Kundennummer anlegen)
- Ad-hoc-Limiterhöhungen im Vier-Augen-Prinzip
- Berichtssystem (z.B. Kartenstatus) und statistische Auswertungen (z.B. Einzahlungshistorie, Anzahl aktivierte Karten)
- Ersatzkarte ausstellen inkl. Übertragung von Guthaben von einer Karte auf eine andere Karte
- Kartenumzug von einer Dienststelle in eine andere Dienststelle bei Wechsel der Zuständigkeit für Verwaltung (z.B. aufgrund Umzugs des Leistungsbeziehers)
- Dublettenprüfung und eindeutige Identifizierung

Für die Nutzung sowie für den Betrieb der Anwendung muss ein Rollen- und Berechtigungskonzept und die Betriebsbedingungen vorliegen, unter denen eine Webanwendung ordnungsgemäß funktioniert.

Die Webanwendung für MA darf nur von Personen genutzt werden können, die zuvor als Nutzer (Anwendende oder Admins) eingerichtet worden sind (entsprechende Lese-, Schreib- und Freigaberechte). Mit dem Zugang sind keine weiteren Berechtigungen verbunden. Die jeweiligen Mitarbeitenden sollen durch den AG selbst in der Anwendung des AN administriert,

d. h. angelegt, bearbeitet und gelöscht werden können. Dazu sollten Administratorenrechte vergeben werden können. Dabei erhält der AN die Daten der Admins und pflegt diese erstmalig in der Webanwendung an (zu klären ist, in welchem Format der AN die Daten benötigt, bspw. über ein bereitgestelltes Excel-Template, o.ä.). Zur Authentisierung soll aus der Webanwendung eine Mail an die dienstliche Mailadresse versandt werden, welche durch die Nutzenden zu bestätigen ist.

Allen Nutzenden der Webanwendung für MA muss ein personalisierter, individueller Account zugewiesen werden. Für die Nutzung der Webanwendung sind nur der Vorname, Nachname und die dienstliche E-Mail-Adresse notwendig. Die Erfassung dieser Daten erfolgt im Rahmen einer **Auftragsverarbeitung durch den AN**. Darüber hinaus sind keine weiteren personenbezogenen Daten notwendig oder zu verarbeiten. Die Authentisierung muss, soweit technisch umsetzbar, mit einer dem Stand der Technik entsprechenden Mehr-Faktor-Authentisierung (MFA) erfolgen können.

Sämtliche relevanten Maßnahmen und Zugriffe auf das System des AN müssen mit entsprechenden User-Daten und Zeitangaben protokolliert werden und jederzeit in der Anwendung nachvollziehbar sein. Dabei sind mindestens Nutzername, Anmeldezeitpunkt, Abmeldezeitpunkt, IP-Adresse des sich anmeldenden Gerätes sowie die Aktivitäten des Nutzers zu protokollieren. Die Protokolle müssen für den AG zugänglich und auswertbar sein. Der Zugriff selbst ist ebenfalls zu protokollieren. Zugriffe auf verarbeitete personenbezogene Daten von Mitarbeitenden des AG (hier: Anwendende) durch Mitarbeitende des AG (hier: Admins) sind ebenfalls entsprechend zu protokollieren (beispielsweise bei Wechsel von Nutzenden der Webanwendung).

Inaktive Sitzungen sind nach einem festgelegten Zeitraum (z.B. 15 Minuten) grundsätzlich zu deaktivieren.

Alle Berechtigungsmaßnahmen müssen systemseitig geloggt und aufbewahrt werden.

Der AG (die BA mit 150 Agentur für Arbeit-Dienststellen und die gemeinsamen Einrichtungen mit 300 Dienststellen) ist in insgesamt 450 Dienststellen untergliedert. Die Anzahl kann durch Neustrukturierung zu- oder abnehmen. Die Webanwendung für MA muss diese Untergliederung abbilden und Änderungen (z.B. Zusammenlegung von Dienststellen und demzufolge Zusammenlegung von Karten, Admins und Nutzer) ermöglichen. Das Rollen- und Berechtigungskonzept muss dahingehend eine technische Unterscheidung zwischen den Dienststellen beinhalten. Die Dienststellen werden nach Bezeichnung (Name) und nach Dienststellennummer (bei BA) bzw. Trägernummer (bei gE) unterschieden (Hinweis: Agentur für Arbeit-Dienststellen werden mit Dienststellennummern geführt, aber die gemeinsamen Einrichtungen werden mit Trägernummern geführt). Keine Dienststelle (sowohl Agenturen als auch gE) und deren Admins oder Nutzer dürfen die Kundendatensätze anderer Dienststellen einsehen können oder diese Datensätze verändern können. Sollte Kartennutzende umziehen oder ein örtlicher Wechsel von einer Agentur hin zu einer gE erfolgen, soll die neue zuständige Dienstelle (Agentur oder gE) in der Webanwendung für MA die Karte übernehmen können. Damit kann die neue Dienststelle alle Funktionen für die Verwaltung der Karte nutzen (z.B. Einzahlungshistorie sehen, Ad-hoc-Zahlungen veranlassen). Die Unterscheidung nach Dienststellennummer und Trägernummer soll außerdem für AG-interne Prozesse und Zwecke Berichte und Datenauswertungen ermöglichen. Die Berichte, bzw. Datenauswertungen müssen zwingend folgende Attribute umfassen:

- Dst-/Trägernummer
- Name der Dienststelle, z.B. Agentur für Arbeit Nürnberg
- Name der gE, z.B. Jobcenter Nürnberg
- Anzahl der Karten, die im Monat aktiviert wurden
- IBAN
- Kunden(referenz)nummer

- Ausstellungsdatum der Karte
- Monatliche Aufladegebühr
- Anzahl der Aufladungen, die im Monat je IBAN stattgefunden haben

Die Berichte sind **monatlich mit der Rechnung als Excel-Datei** zur Verfügung zu stellen (siehe Passus Rechnungsstellung in Kap. 3.2).

Der AN muss die Umsetzung der jeweils geltenden Regelungen zur Korruptionsbekämpfung und Geldwäschebekämpfung sicherstellen. Hierzu zählen Überprüfungen der Karteninhaber hinsichtlich Know Your Customer (KYC), politisch exponierter Personen (PEP) und relevanter Sanktionslisten, die vom AN bei Anlage des Datensatzes, d. h. der Stammdaten in der Webanwendung, vorzusehen sind. Dies erfolgt zur Erfüllung der gesetzlichen Vorgaben im Zusammenhang mit der Erbringung der Zahlungsdienstleistung durch den AN.

Allen Nutzenenden der Webanwendung für MA stellt der AN eine benutzerfreundliche Anleitung zum anwendungssicheren Umgang mit dem Verfahren und stattfindende Qualifizierungsangebote zur Verfügung (siehe Kapitel 2.7). Bei Verfahrensänderungen werden diese vom AN aktualisiert.

Zudem bietet der AN einen regelmäßigen virtuellen Austausch (MS-Teams) mit dem AG zu Optimierungsmöglichkeiten, Problemlösungen, Grundsatzfragen, etc. an. Hierbei wird durch AG-interne Regelung ausgeschlossen, dass eine Klärung personenbezogener Daten erfolgt.

Daten der Kartennutzenden (Leistungsempfangende) werden in der Webanwendung für MA mit Namen, Vornamen, Ausweisnummer, Ausweisart und die seitens des AG verwendete Kundennummer gespeichert (Format Kundennummer: Drei Zahlen, Ein Buchstabe, Sechs Zahlen. Bsp. 123A456789). Die Angabe der Daten der Kartennutzenden erfolgt zur Erfüllung der gesetzlichen Vorgaben im Zusammenhang mit der Erbringung der Zahlungsdienstleistung durch den AN. Zwischen Kartennutzenden und Auftragnehmer wird bei Kartenübergabe eine entsprechende Vereinbarung geschlossen. Die Erfassung der vorgenannten Daten erfolgt durch den AG lediglich im Auftrag der Kartennutzenden.

2.3.2 Online-Portal und App für Kartennutzende

Damit sich die Kartennutzenden jederzeit über ihren „Kontostand“ und die Kontobewegungen informieren können (zur Erfüllung der gesetzlichen Vorgaben im Zusammenhang mit der Erbringung der Zahlungsdienstleistung durch den AN), muss ein Online-Portal, sowie eine App des AN für Kartennutzende zur Verfügung gestellt werden. Das Online-Portal sowie die App werden ebenfalls als Software-as-a-Service (SaaS) betrieben. Mit der Angebotsabgabe muss dargelegt werden, von wem und wie die zugrundeliegende Cloud-Infrastruktur betrieben wird (siehe Kap. 5 und 6). Nach der Registrierung im Online-Portal hat die/der Kartennutzende Zugriff auf alle Informationen, die der AN zur Erfüllung der gesetzlichen Vorgaben im Zusammenhang mit der Erbringung der Zahlungsdienstleistung bereitstellen muss. Ihre/Seine Kartenumsätze, den Verfügungsrahmen sowie den Zugang zum Kundensupport bei Fragen und Problemen (z.B. PIN wurde vergessen, Karte ist verloren gegangen und muss gesperrt werden). Sollten Änderungen oder Anpassungen bei der Datenschutzerklärung notwendig sein, muss diese Änderung und ggf. eine neue Datenschutzerklärung zur Erfüllung der gesetzlichen Vorgaben im Online-Portal und der App sichtbar angezeigt werden. Die einzugebenden Daten werden im Zusammenhang mit der Erfüllung der Zahlungsdienstleistung durch den AN von den Kartennutzenden eingegeben.

Kartennutzerinnen und Kartennutzer, die zusätzlich ihr Smartphone benutzen möchten, um die Funktionen und Informationen einsehen zu können, können dazu die App des AN nutzen. Weitere Funktionen muss die App nicht bereitstellen.

2.4 SaaS-Betriebsservices und Support

Die nachfolgenden Betriebsservices sind integraler Bestandteil der geschuldeten Leistung und umfassen insbesondere:

- Fehlerbehebung: Analyse und Behebung technischer Störungen, Fehlfunktionen oder sicherheitsrelevanter Schwachstellen innerhalb der Reaktions- und Wiederherstellungszeiten (s. Tabelle 1).
- Regelmäßige Aktualisierung der Software (z. B. durch kostenfreie Produkt-Updates, -Upgrades, -Patches, -Releases, Hotfixes).
    - Updates, welche Auswirkungen auf Nutzende des Systems haben, müssen dem AG vorab (mindestens 10 AT) per E-Mail mitgeteilt werden.
    - AN-seitige Anpassungen an der Webanwendung müssen in der Zeit von 22:00 Uhr bis 06:00 Uhr (MEZ) stattfinden, so dass die Webanwendungsnutzung für die Mitarbeitenden des AG und Kunden nicht eingeschränkt ist.
    - Der AN hat sicherzustellen, dass hinterlegte Daten bei einer Anpassung der Webanwendung (z.B. durch ein Update) nicht verloren gehen und mit der aktualisierten Version weiterhin kompatibel sind.
- Bereitstellung eines deutschsprachigen AN-Supports zur Beantwortung von Fragen des AG oder von Kartennutzern (telefonisch, per E-Mail) im Zeitraum werktags von 08:00 bis 17:00 Uhr (MEZ) mit folgenden Leistungsmerkmalen:
    - Bereitstellung einer Service-Hotline innerhalb der Servicezeiten, welche über eine einzige Rufnummer erreichbar sein muss
    - Bekanntgabe der entsprechenden E-Mailadresse
- Der AN benennt für die gesamte Vertragslaufzeit eine/n umfassend entscheidungsbefugte/n und handlungsbevollmächtigte/n Vertreter/in einschließlich einer Person, die in Vertretungsfällen ansprechbar ist.
- Wartung der zugrundeliegenden Cloud-Infrastruktur

Bei Supportdienstleistungen gegenüber dem AG ist es ausgeschlossen, dass der AN Kenntnis von personenbezogenen Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) erlangt, da sich der Support nur auf die grundsätzliche technische Bereitstellung der Webanwendung bezieht und keine darüber hinausgehenden Daten abgefragt werden. Der AN verpflichtet sich, angemessene Maßnahmen mit dem Ziel zu ergreifen, das Auftreten zukünftiger Störungen des Gesamtsystems zu vermeiden.

Darüber hinaus ist ein technischer Support zu leisten:

- Bereitstellung von technischem Support und Hilfe bei Fragen oder Problemen von Mitarbeitenden des AG oder der Kartennutzenden.
  Im Rahmen von Supportdienstleistungen gegenüber den Kartennutzenden (Kontaktaufnahme durch die Kartennutzenden mit dem AN per Mail oder Anruf) hat der AN nach Eingabe der jeweiligen Kartennummer auch Zugriff auf personenbezogene Daten. Die Verarbeitung von personenbezogenen Daten im Rahmen der Erbringung von Leistungen, welche direkt mit den Tätigkeiten des AN als reguliertes Zahlungsinstitut verbunden sind, erfolgt durch den AN als allein Verantwortlicher nach Art. 4 Nr. 7 DSGVO.

Der AN verpflichtet sich, die vereinbarten Betriebsservices und Supportleistungen während des gesamten Leistungszeitraums zu erbringen.

Der 1st-Level-Support wird vom AN übernommen.

Tätigkeiten durch den AN in den Räumlichkeiten des AG sind nicht möglich.

Ein Remote-Zugriff auf die IT-Systeme des AG ist ebenfalls nicht möglich.

2.5 Verfügbarkeit (Betriebszeit)

Der Betrieb muss während des gesamten Leistungszeitraums kontinuierlich und ohne Unterbrechungen (ausgenommen sind angekündigte AN-seitige Anpassungen an der Webanwendung für MA oder dem Online-Portal für Kartennutzende oder der App in der Zeit von 22:00 Uhr bis 06:00 Uhr (MEZ)) sichergestellt werden.

Der AN gewährleistet eine technische Verfügbarkeit des Gesamtsystems von mindestens 99,5 % (Betrachtungszeitraum ein Vertragsmonat), bezogen auf die produktive Betriebszeit (24/7).

Die Verfügbarkeit wird monatlich durch den AN protokolliert und dem AG auf Anfrage nachgewiesen (als Bericht / Übersicht per Mail).

2.6 Reaktions- und Wiederherstellungszeiten

Der AN hat die im Folgenden definierten Reaktions- und Wiederherstellungszeiten (Tabelle 1) zwingend einzuhalten.

Störungsklasse	Kurzbeschreibung	Reaktionszeit	Wiederherstellungszeit
Prio 1	**Betriebsverhindernde Störung** Ausfall des Systems, Datenschutzpanne, IT-Sicherheitsvorfall *Beispiel:* *Es kann auf die Webanwendung nicht zugegriffen werden.*	Bis zu 1 h	Bis zu 3 h
Prio 2	**Betriebsbehindernde Störung** Negative Beeinträchtigung (z. B. Performance, Funktionalität) *Beispiel:*	Bis zu 2 h	Bis zu 6 h

	Die Funktionen des Administrators bzw. Moderator fallen aus, sodass diese nicht mehr steuernd in die Anwendung eingreifen können.		
Prio 3	**Leichte Störung** Technische Anfragen, Unterstützung, Feature Requests etc. *Beispiel:* *Die Funktionen der Mitarbeiterinnen und Mitarbeiter stehen nicht mehr in vollem Umfang zur Verfügung.*	Bis zu 24 h	Bis zu 48 h

Tabelle 1: Reaktions- und Wiederherstellungszeiten

Explizit ausgeschlossen sind Störungen, die das jeweilige Kartensystem betreffen und nicht in der Verantwortung des AN liegen.
Beispiel: Die Kartenzahlung bei bestimmten Händlern ist ausgefallen.

Die Fehlerpriorität wird durch die Zentrale des AG festgelegt und bei Eröffnung einer Supportanfrage angegeben. Der AN hat die Möglichkeit, die Fehlerpriorität in Abstimmung mit dem AG zu ändern. Die Schlussbewertung obliegt dem AG.

Die Reaktionszeit beginnt mit dem Eingang einer Störungsmeldung (der Zentrale des AG, der Dienststellen oder der gE) beim AN (telefonisch, per Mail, per Post). Der AN hat unverzüglich – spätestens jedoch bis zum Ablauf der o.g. Zeitangaben – auf diese Meldung zu reagieren. Unter Reaktion ist dabei eine Kontaktaufnahme mit der den Fehler meldenden Stelle zur Abstimmung des weiteren Vorgehens zu verstehen (i.d.R. die Zentrale des AG).

Die Wiederherstellungszeit beginnt ebenfalls mit Eingang der Störungsmeldung beim AN und endet mit deren Behebung. Die Behebung muss dem AG vom AN per E-Mail gemeldet werden.

Der AN muss den AG eigenständig über Meilensteine der Störungsbeseitigung (per E-Mail) informieren. Weiterhin muss ein Statusupdate (per E-Mail) erfolgen, sofern ein Mitarbeitender des AG dieses anfordert.

Die Reaktions- und Wiederherstellungszeiten laufen innerhalb der Servicezeiten (s. Glossar).

2.7 Qualifizierungsmaßnahmen

Zur Qualifikation der involvierten Mitarbeitenden des AG sind geeignete Online-Qualifizierungsmaßnahmen durch den AN zu planen, vorzubereiten und durchzuführen.

Zusätzlich zu den Qualifizierungsmaßnahmen sind durch den AN entsprechende Arbeitsmittel zum Selbststudium zur Verfügung zu stellen.

Da die Prozessschritte und ggf. einzusetzende Hilfsmittel vom AN ausgestaltet werden, obliegen ihm die Vorbereitung und Durchführung der Qualifizierungsmaßnahmen.

Durch AG-interne Regelungen wird ausgeschlossen, dass in diesen Maßnahmen eine Klärung personenbezogener Daten erfolgt.

Qualifizierungsmaßnahme	
Teilnehmerkreis:	ca. 5.000 Mitarbeitende des AG (BA und der gE)
Teilnehmeranzahl pro Einweisungs-/ Schulungstag:	max. 1.000 TN
Anzahl und Dauer der Maßnahmen:	20 Maßnahmen jeweils ca. 60 Minuten (+ angemessene Dauer für Rückfragen, z.B. weitere 15-30 Minuten)
Ort der Leistungserbringung:	Virtuell via MS-Teams
Unterlagen:	Handbuch für die Webanwendung für MA, Zugriff auf FAQ, Präsentationsunterlagen, Zugriff auf ein Test- und Schulungssystem
Übergabe Unterlagen:	Der AG erhält zum Abschluss der Qualifizierungsmaßnahme die Unterlagen in digitaler Form.

Tabelle 2 Einweisung / Schulung

Hinsichtlich der Vorbereitung und Durchführung der Qualifizierungsmaßnahmen hat der AN folgende Anforderungen zu erfüllen:

- Die inhaltliche und zeitliche **Planung** der Qualifizierungsmaßnahmen wird durch den AN vorgenommen und mit der Zentrale des AG abgestimmt.
- Der AN wird die Qualifizierungsmaßnahmen ausschließlich online durchführen und nutzt hierfür MS-Teams als Kommunikationsplattform.
- Vom AN sind erstmalige Qualifizierungsmaßnahmen im Zeitraum von 12 AT ab Zuschlag durchzuführen. Anzahl und Termine werden in Abstimmung mit der Zentrale des AG festgelegt (max. 20 Maßnahmen). Eine Abrufverpflichtung seitens des AG besteht nicht. Die Abrechnung erfolgt nach tatsächlich erbrachtem Aufwand. Weitere **Nachqualifizierungen** sollen bei Bedarf während der gesamten Vertragsdauer erbracht werden können. Nachqualifizierungsbedarf kann im Falle von Änderungen der Abläufe und Hilfsmittel bestehen. Anzahl und Zeitpunkt wird in Abstimmung mit der Zentrale des AG festgelegt (anzunehmen ist die offene Differenz zwischen 20 und der tatsächlich durchgeführten Erstqualifizierungen. Bsp. sollten 18 Erstqualifizierungen durchgeführt worden sein, verbleiben 2 als Nachqualifizierung).
- Das Handbuch muss alle Funktionen in benutzerfreundlicher Sprache und mit Screenshots beinhalten, für den täglichen Gebrauch geeignet sein und die Funktionen mit Schritt-für-Schritt Anleitungen erklären. Folgende Aspekte müssen **mindestens** vorhanden sein:
    - Login auf die Webanwendung
    - Rechte- und Rollen inkl. die Durchführung der jeweiligen Prozesse (z.B. Welche Prozesse können von Admins wie und wo durchgeführt werden)
    - Funktionen:
        - Neue Karte ausstellen
        - Karte(n) verwalten (Kartenstatus, Einzahlhistorie, Ersatzkarte, Kartenübernahme aus anderer Dienststelle)
        - Ad-hoc Limit-Erhöhungen
        - Auswerten und Erstellen von Berichten zum Kartenbestand, verschiedene Such- und Filterfunktionen im Kartenbestand

- Weitere Funktionen für die Verwaltung einer Karte/Nutzenden (Bearbeiten eines Datensatzes)
- Sonderfälle (z.B. Karte für Minderjährige)

- Support für Mitarbeiterinnen und Mitarbeiter
  - Wie und wo ist der Mitarbeiter-Support zu erreichen
  - Wo sind FAQs und die Anleitung zu finden
- Welche Informationen bietet die Webanwendung für MA
  - Alle Elemente auf der Webanwendung müssen erklärt werden
- Einweisung in das Testsystem
  - Wie und wo gelangt man zum Testsystem

Bei Änderungen der Prozesse sind die Qualifizierungsunterlagen entsprechend anzupassen (auch bei Ergänzungen der Beschreibungen bestehender Funktionen) sowie geeignete Einweisungs-/Schulungsmaßnahmen sicherzustellen.

3. Weitere Anforderungen

3.1 Allgemeine Anforderungen

Das Gesamtsystem als auch die unmittelbare Distribution der Debitkarten muss unverzüglich nach Zuschlagserteilung zur Verfügung stehen.

Der AN muss eine Webanwendung für MA zur Ausgabe und Verwaltung der Debitkarten bereitstellen.

Das Gesamtsystem muss als Stand-Alone-System außerhalb der Infrastruktur des AG vollständig und ohne technische Anbindung an diese funktionieren.

Das System muss an das Visa- oder das Mastercard-Zahlungssystem oder ein vergleichbares Netz von Akzeptanzstellen angeschlossen sein. Die Karte muss im gesamten SEPA-Raum nutzbar sein (an Bankautomaten, im stationären und elektronischen Handel). Eine Vereinbarung zwischen dem AG und den Akzeptanzstellen ist nicht vorzusehen.

Es muss gewährleistet sein, dass Leistungsempfangende über den auf der Karte hinterlegten Betrag selbständig und unabhängig verfügen können. Sowohl Karte als auch aufgeladener Betrag liegen in der Verfügungsgewalt der Karteninhaber/innen. Der AG ist nicht verantwortlich für den sorgsamen und rechtskonformen Einsatz der Karte durch die Karteninhaber/innen.

Die Bereitstellung von Kartenguthaben erfolgt seitens des AG ausschließlich per SEPA-Überweisung. Jeder einzelnen Debitkarte muss deshalb eine eineindeutige virtuelle IBAN zugeordnet werden, auf die ausschließlich die Überweisungen des AG erfolgen können. Eine Weitergabe der IBAN an Dritte ist nicht vorgesehen. Für das Aufladen der Karte muss der zur Beladung vorgesehene Geldbetrag auf die virtuelle IBAN je Debitkarte, welche unverzüglich nach Erstellung einer Karte zur Verfügung gestellt werden muss, durch den AG überwiesen werden können.

3.2 Kostenabrechnung

Anfallende Kosten werden nach Eingang einer prüfbaren Rechnung im Original kalendermonatlich nachträglich abgerechnet. Mit der Übersendung der Rechnung ist auch eine Auswertung der verursachten Kosten (Berichte) gemäß dem oben beschriebenen Dienststellenmodell (Kap 2.3.1) bis spätestens zum 6. jedes Folgemonats mitzuliefen.

3.3 Aufsichtsbehörde

Der AN muss von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder einer anderen vergleichbaren Aufsichtsbehörde innerhalb der EU lizenziert und reguliert sein und wird daher auch entsprechend bei der IT-Sicherheit und Verfügbarkeit von der zuständigen

Finanzaufsicht überwacht. Die Vorgaben der BaFin für den deutschen Aufsichtsbereich sind mandatorisch. Um das geforderte Ad-hoc Verfahren (siehe Kap. 2.1.9) mit nachträglicher Ausgleichszahlung erfüllen zu können, muss der AN bestätigen, dass er bei der Vorleistung dem AG einen „Kredit“ gewährt, und dass dieses Verfahren von einer Aufsichtsbehörde für den deutschen Geltungsbereich genehmigt und reguliert wird. In diesem Zusammenhang müssen Mindestanforderungen an das Risikomanagement (MA-Risk) erfüllt sein.

3.4 Optionales Dienstleistungskontingent

3.4.1 Umfang der Dienstleistungsunterstützung

Die zu erbringenden Dienstleistungen sollen den AG in die Lage versetzen, Optimierungen und Weiterentwicklungen am System vorzunehmen.

Hierfür ist ggf. eine Dienstleistungsunterstützung erforderlich. Die geschätzte Abrufmenge über den gesamten Leistungszeitraum hinweg beträgt ca. ca. **240** Personenstunden (PS).

Bitte beachten Sie, dass es sich hierbei lediglich um eine Schätzgröße handelt, Abweichungen sind möglich. Eine voraussichtliche jährliche Verteilung kann nicht angegeben werden.

Die geschätzte Abrufmenge kann, abhängig von den fachlichen Notwendigkeiten und den haushaltsmäßigen Gegebenheiten, über- oder unterschritten werden. Eine Abrufverpflichtung seitens des AG besteht nicht. Die Abrechnung erfolgt nach tatsächlich erbrachtem Aufwand auf Basis des angebotenen Stundensatzes.

Der Auftragnehmer hat dafür Sorge zu tragen, dass entsprechend qualifiziertes Personal für die beauftragte Dienstleistung zur Verfügung gestellt wird.

Die Dienstleistungsunterstützung erfolgt im folgenden Kontext:

- Digitalisierung der Geschäftsprozesse im Zusammenhang mit der Übersendung von Berichten und Reportings z.B. bei der Rechnungsbearbeitung (siehe Kap 3.2, bzw. 2.3.1).

Bei optionalen Dienstleistungsunterstützungen ist es ausgeschlossen, dass der AN Kenntnis von personenbezogenen Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) und ähnlicher sensibler Daten erlangt.

3.4.2 Ort und Zeiten der optionalen Dienstleistungserbringung

Die Erbringung der optionalen Dienstleistungsunterstützung erfolgt grundsätzlich nur nach Abruf durch den AG und findet remote statt. Hierbei sind die Regelungen zum Datenschutz (s. Kap. 5.7) und die technisch-organisatorischen Maßnahmen (TOM, siehe Anlage 3 zur Leistungsbeschreibung) zwingend einzuhalten.

Für die Erbringung der optionalen Dienstleistungen werden folgende Servicezeiten definiert:

Montag bis Freitag von 08:00 bis 17:00 Uhr (MEZ).

Nacht-/Wochenend-/Feiertagsarbeit findet nicht statt.

Der Personaleinsatz des Auftragnehmers erfolgt nach Bedarf in Absprache zwischen dem AG und dem dauerhaften Ansprechpartner des Auftragnehmers gemäß Kapitel 2.4.

3.5 Barrierefreiheit

Als Körperschaft des öffentlichen Rechts müssen alle in der BA eingesetzten IKT-Anwendungen sowie interne und externe Websites, Apps, grafische Oberflächen,

elektronische Aktenführung und Dokumente die gesetzlichen Anforderungen an barrierefreie Informationstechnik gemäß BITV 2.0 sowie EN 301 549 in ihrer jeweils gültigen Fassung entsprechen, und diese uneingeschränkt erfüllen.

Die BA als Arbeitgeberin beschäftigt zahlreiche Mitarbeitende mit Behinderungen. Alle intern eingesetzten IKT-Anwendungen und -Produkte werden auch auf Arbeitsplätzen von Mitarbeitenden mit Schwerbehinderung oder Gleichstellung eingesetzt, und müssen barrierefrei sein und die Anforderungen gemäß BGG, BITV 2.0 und EN 301 549 erfüllen.

Die Barrierefreiheit der zu beschaffenden IKT-Lösung ist im Rahmen der Entwicklung und Programmierung von Beginn an konsequent, umfassend und uneingeschränkt zu berücksichtigen. Die IKT-Lösung muss auch für Menschen mit behinderungsbedingten Einschränkungen (Nutzung ohne oder mit eingeschränktem Sehvermögen, ohne oder mit eingeschränktem Hörvermögen, ohne oder mit eingeschränktem Sprachvermögen, mit eingeschränkter Reichweite, Handhabung oder Kraft, ohne Risiko epileptischer Anfälle, mit eingeschränkten kognitiven, sprachlichen oder Lernfähigkeiten; siehe EN 301 549, Abschnitt 4.2) barrierefrei zugänglich und nutzbar sein. Hierzu sind die Anforderungen zur Barrierefreiheit, die sich aus den einschlägigen technischen Standards (insbesondere EN 301 549, DIN EN ISO 9241-171 und DIN ISO 14289-1) und aus der BFIT-Bund Handreichung: Barrierefreie Gestaltung von User Interface-Elementen ergeben, einzuhalten und umzusetzen.

Der AG behält sich vor zu beschaffende IKT-Lösungen (Webanwendung für die Mitarbeitenden des AG, des Online-Portals und der App für die Kartennutzende sowie der weiteren Dokumente gem. dieser Leistungsbeschreibung) sowie entwickelte IKT-Lösungen einer Überprüfung gemäß den gesetzlichen Anforderungen (gemäß BITV 2.0, EN 301 549, DIN ISO 14289-1 etc.) zu unterziehen, gemäß den Anforderungen der BFIT-Bund Handreichung: Qualitätskriterien für die Begutachtung der Barrierefreiheit. Diese Prüfung der Vereinbarkeit mit der BITV 2.0 erfolgt im Rahmen einer neutralen, unabhängigen Begutachtung durch entsprechend zertifizierte externe Prüfstellen.

Die Anforderungen an die Barrierefreiheit an die IT-Lösung müssen über die gesamte Vertragslaufzeit erfüllt werden. Hierin eingeschlossen sind Versionswechsel, Wartung und Pflege der IT-Lösung. Sollten Barrieren bestehen, müssen diese im weiteren Verlauf behoben werden.

4. Vertragslaufzeit und Dauer der Leistung

4.1 Beginn und Dauer

Der Vertrag beginnt mit Zuschlag. Ein Zuschlagstermin wird ab August 2026 angestrebt.

Der Leistungszeitraum beginnt ebenfalls mit Zuschlag und endet nach 4 Jahren, gleichzeitig mit der Vertragslaufzeit, ohne dass es einer Kündigung bedarf.

Die ersten Abrufe erfolgen voraussichtlich umgehend nach Zuschlagserteilung.

Für den AG besteht die Option, den Vertrag nach 24 Monaten bzw. nach 36 Monaten zu kündigen, jeweils unter Einhaltung einer Kündigungsfrist von 3 Monaten.

4.2 Exit-Management: Verpflichtungen zum Ende des Vertrags

Der Auftragnehmer verpflichtet sich, zu Vertragsende einen möglichst reibungslosen Übergang auf einen möglicherweise nachfolgenden Auftragnehmer zu gewährleisten.

Dies beinhaltet insbesondere die Datenmigration sowie, sofern der nachfolgende Auftragnehmer das gleiche Zahlungssystem nutzt, die Prüfung der Möglichkeit zur Überführung der ausgegebenen Karten auf den neuen Auftragnehmer, damit der AG nach Möglichkeit die ausgegebenen Karten nicht austauschen muss.

Spätestens sechs Monate vor Vertragsablauf wird der Auftraggeber zur Datenmigration ein strukturiertes Template vorgeben, in das die Daten zu befüllen sind. Hierbei handelt es sich um eine vertragliche Mitwirkungsleistung im Zuge der Datenmigration zu einem oder mehrere nachfolgenden Dienstleister(n).

Abhängig davon, ob es nachfolgend einen einheitlichen Dienstleister geben wird oder mehrere nachfolgende Dienstleister, ist der Export je nach Zieldienstleister einzeln oder gesammelt vorzunehmen. Je nachdem, ob der oder die nachfolgenden Dienstleister die gleiche Zahlungsinfrastruktur nutzen (z.B. Master oder Visa) überträgt der Auftragnehmer die Karten auf das oder die nachfolgenden Unternehmen, sofern die rechtliche und tatsächliche Möglichkeit für eine Übertragung besteht.

5. Datenschutz / Auftragsverarbeitung

Bei diesem Auftrag ist nicht ausgeschlossen, dass der AN Kenntnis von personenbezogenen Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) sowie Betriebs- und Geschäftsgeheimnissen im Sinne von § 35 Abs. 4 Erstes Buch Sozialgesetzbuch (SGB I) erlangt.

Die Verarbeitung von personenbezogenen Daten im Rahmen der Erbringung von Leistungen, welche direkt mit den Tätigkeiten des AN als reguliertem Zahlungsinstitut verbunden sind, erfolgt durch den AN als allein Verantwortlicher nach Art. 4 Nr. 7 DSGVO. Abweichend davon erbringt der AN die unter 5.1.1 aufgeführten Leistungen als **Auftragsverarbeiter**.

Der Auftragnehmer sichert zu, dass die Verarbeitung der Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfindet. Der Datentransfer in einen Drittstaat ist unzulässig. Dies gilt auch bei der Beauftragung von weiteren Auftragnehmern oder der Inanspruchnahme von Cloud-Diensten.

Die Erfassung der Kartennutzer-Daten erfolgt zur Erfüllung der gesetzlichen Vorgaben im Zusammenhang mit **der Erbringung der Zahlungsdienstleistung** durch den AN.

5.1 Gegenstand und Dauer der Verarbeitung

5.1.1 Gegenstand der Verarbeitung

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den AN:

- Bereitstellung der Webanwendung für die Mitarbeiterinnen und Mitarbeiter des AG zum Zweck der Steuerung der Prozesse rund um die Debitkarte;
- Protokollierung innerhalb der Webanwendung;
- technischer Support für die Mitarbeitenden des AG;

5.1.2 Dauer der Verarbeitung

Die Dauer dieses Auftrags (Laufzeit) ist ab Zuschlagserteilung befristet auf Vier Jahre. Für den AG besteht die Option, den Vertrag nach 24 Monaten bzw. nach 36 Monaten zu kündigen, jeweils unter Einhaltung einer Kündigungsfrist von 3 Monaten. (siehe Kap. 4.1).

5.2 Konkretisierung des Auftragsinhalts

5.2.1 Art der Verarbeitung

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des AN:

Für die Webanwendung für Mitarbeiterinnen und Mitarbeiter (MA) (s. Kap. 2.3, 2.3.1 und 2.4) erfolgt die Verarbeitung in folgender Art:

Erfassen, Organisation, Speicherung, Vertragsmäßige Verwendung, Löschung von Daten.

5.2.2 Zweck der Verarbeitung

Die Verarbeitung dient folgendem Zweck:

Zur Nutzung der Webanwendung durch die Mitarbeitenden des AG (BA und gE) sind diese mit Vornamen, Name und dienstlicher E-Mailadresse zu hinterlegen. Die Mitarbeitenden des AG können dann die Zuordnung einer Debitkarte zu einer/einem Kartennutzenden und Ad-hoc-Limiterhöhungen vornehmen.

5.2.3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien) (s. Kap. 2.3, 2.3.1 und 2.4):

☒ Personenstammdaten von Mitarbeitenden des AG (BA und gE) (Name, Vorname)

☒ Kommunikationsdaten (dienstliche E-Mail-Adresse von Mitarbeitenden der BA und gE)

☐ Daten zur Vermittlung/Integration in Arbeit und Beratung (Lebenslauf, Nachweis über Abschlüsse, Angaben zu Kenntnissen und Fähigkeiten)

☐ Daten auf Grundlage der Beauftragung von Dritten (z. B. Maßnahmeträger, Fachdienste)

☐ Dokumentation der Kundenkontakte und Entscheidungen (Beratungsvermerke)

☒ Weitere/Sonstige: technische Daten (Logging-Daten: Nutzername, Anmeldezeitpunkt, Abmeldezeitpunkt, IP-Adresse des sich anmeldenden Gerätes sowie die Aktivitäten des Nutzers)

5.2.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden

☒ Mitarbeiter

☐ Lieferanten

☐ Ansprechpartner

☐ Weiter/Sonstige:

5.3 Technische und organisatorische Maßnahmen und deren Kontrolle

Der AN hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und der Zentrale der BA zur Prüfung zu übergeben. Bei Akzeptanz durch die Zentrale der BA werden die dokumentierten Maßnahmen Grundlage des Auftrags. Die Vertragsparteien vereinbaren die in der Anlage 3 zu dieser Leistungsbeschreibung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Die Anlage 3 ist Gegenstand dieser Leistungsbeschreibung. Soweit die Prüfung/ein Audit der BA einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der AN hat die Sicherheit gem. Art. 28 Abs. 3 lit. c), 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die

unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 3].

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in der Anlage 3 festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5.4 Berichtigung, Einschränkung und Löschung von Daten

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung der BA unmittelbar durch den AN sicherzustellen.

5.5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragnehmer

Qualitätssicherung und sonstige Pflichten des AN

Der AN hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO [Einzelheiten in Anlage 3]
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber der BA im Rahmen ihrer Kontrollbefugnisse nach Nr. / § XXX des Vertrages.

5.6 Mitteilung bei Verstößen des Auftragnehmers

Der AN unterstützt die BA bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

- die Unterstützung der BA für deren Datenschutz-Folgenabschätzung
- die Unterstützung der BA im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

5.7 Regelungen bei Remote-Zugriff und Tele-/Heimarbeit

Der Auftraggeber behält sich vor, bei Bedarf die Erbringung von Leistungen mit Remote-Zugriff anzufordern bzw. Tele-/Heimarbeit zuzulassen (s. Kap. 3.4).

Nachfolgend sind die Regelungen zu Remote-Zugriff und Tele-/Heimarbeit beschrieben:

Die Erbringung der optionalen Dienstleistungsunterstützung erfolgt grundsätzlich nur nach Abruf durch den AG und findet remote statt.

Dienstleister-/innen des Auftragnehmers, die im Rahmen der Leistungserbringung die Leistungen über einen Remote-Zugriff außerhalb der Geschäftsräume des Auftraggebers erbringen, tragen eine besondere datenschutzrelevante Verantwortung. Sie verpflichten sich zur Einhaltung der geltenden Datenschutzbestimmungen, insbesondere zur Wahrung des Sozialgeheimnisses und des Sozialdatenschutzes (§ 35 SGB I in Verbindung mit §§ 67 ff. SGB X).

Der Remote-Zugriff bzw. die Tele-/Heimarbeit darf ausschließlich im Hoheitsgebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat im Sinne des Abkommens über den Europäischen Wirtschaftsraum stattfinden. Dies gilt auch für etwaige weitere Auftragsverarbeiter.

Der Remotearbeitsplatz muss den datenschutzrechtlichen Anforderungen entsprechen. Voraussetzung ist, dass die Arbeitsbedingungen des Remotearbeitsplatzes mit einem separaten, verschließbaren Arbeitsbereich vergleichbar sind. Ein gesondertes Zimmer zur ausschließlichen Nutzung für die Remotearbeit bzw. Tele-/Heimarbeit ist dabei nicht erforderlich, vielmehr muss ein getrennter, verschließbarer Bereich zum Arbeiten zur Verfügung stehen.

Der Transport dienstlicher Unterlagen muss in einem verschlossenen Behältnis (z. B. verschließbarer „Pilotenkoffer“) erfolgen. Außerhalb der Aufgabenerledigung sind dienstliche Unterlagen in der Arbeitsstätte verschlossen und gegen den Zugriff Dritter, dies gilt auch für Familienangehörige und Haushaltsangehörige, gesichert aufzubewahren.

Fehlausdrucke dürfen nicht im Hausmüll entsorgt werden, sondern sind in der Dienststelle einer datenschutzkonformen Vernichtung durch Einwurf in die entsprechenden Behälter zuzuführen.

Bei unrechtmäßiger Kenntniserlangung von Sozialdaten durch Dritte ist dies durch die/den jeweiligen IT-Dienstleister-/in des Auftragnehmers unverzüglich anzuzeigen und über ihren/den Teamleiter des Auftragnehmers sofort der Datenschutzbeauftragten des Auftraggebers (Stabsstelle Datenschutz der Zentrale) mitzuteilen (Informationspflicht).

6. Anforderungen der IT-Sicherheit

6.1 Sicherheitsnachweise

Mindestanforderungen an die Cloud-Sicherheit (C5-Kriterien)
Technische Spezifikationen / Mindestanforderungen
Die angebotenen Cloud-Leistungen müssen ein Sicherheitsniveau aufweisen, das den Anforderungen des BSI C5-Standard oder einem gleichwertigen, international anerkannten Standard (z.B. SOC 2 Type 2 basierend auf Trust Services Criteria) entspricht.

Nachweisführung mit dem Angebot:
1. Der Bieter hat mit dem Angebot ein gültiges C5-Testat (Typ 2) oder einen gleichwertigen, unabhängigen Prüfbericht (z.B. SOC 2 Type 2) vorzulegen, der die Wirksamkeit der Kontrollen für einen Zeitraum von mindestens 6 Monaten bestätigt.
2. Sofern zum Zeitpunkt der Angebotsabgabe noch kein Testat über die Wirksamkeitsprüfung (Typ2) vorliegt, ist ersatzweise ein Nachweis über die Angemessenheit der Kontrollgestaltung vorzulegen (z.B. C5 Typ 1, SOC 2 Type 1 oder ein detailliertes Audit-Testat eines unabhängigen Dritten).
3. Die Gleichwertigkeit eines anderen Standards als BSI C5 ist vom Bieter im Angebot schlüssig darzulegen. Der Auftraggeber behält sich die Prüfung der Gleichwertigkeit vor.

6.2 IT-Sicherheitskonzept

Der Auftragnehmer hat vor Beginn der Auftragsverarbeitung ein IT-Sicherheitskonzept nach BSI-Standard 200-2 unter Verwendung des IT-Grundschutz-Kompendiums (aktuelle Edition) oder vergleichbar konform der Standard-Absicherung zu erstellen und dem AG die Mitwirkungspflichten von umzusetzenden Anforderungen (und daraus resultierenden Maßnahmen) für eine durchgängige Informationssicherheit zu benennen und deren Umsetzung entsprechend nachzuweisen.
Das Sicherheitskonzept ist auf der Grundlage der Systemarchitektur, der zu erhebenden, verarbeitenden und zu nutzenden Daten zu erstellen, umzusetzen und regelmäßig an den aktuellen Stand der Technik anzupassen.

Eine Aktualisierung des IT-Sicherheitskonzepts ist mindestens einmal jährlich oder bei Änderungen durchzuführen und dem AG zu übergeben.

Die Abnahme des IT-Sicherheitskonzepts erfolgt durch den AG.

6.3 Voraussetzung für eine sichere Bereitstellung/Nutzung

Kryptographische Protokolle, Formate und Algorithmen zum Schutz schützenswerter Informationen sind zum Einsatz zu bringen. Alle eingesetzten kryptographischen Protokolle, Formate und Algorithmen müssen den aktuellen Vorgaben des BSI (entsprechend der technischen Richtlinien respektive direkt vom BSI anerkannten Drittdokumenten) entsprechen.

Die technischen Sicherheitsfunktionalitäten hinsichtlich der Authentifizierung/Autorisierung müssen nach aktuellem Stand der Technik innerhalb der Software in geeigneter Weise implementiert sein.

- Mandantentrennung von anderen Kunden des SaaS-Dienstes
- Serverseitige Zugriffskontrolle
- Umgesetzte Benutzerverwaltung mit einem Rollensystem
- Useradministration ist in Eigenadministration durch den AG möglich
- Authentifizierungs- und Authentisierungsmaßnahmen für User sind implementiert
- Eine Sperre von Aktivitäten ohne Benutzer-Authentifizierung ist integrierbar
- Es sind Richtlinien hinsichtlich der Verwendung und Charakteristik von Passwörtern sowie deren Gebrauch und Schutz nach Stand der Technik definierbar
- Ein Brute-Force-Schutz ist implementiert

Der AG behält sich das Recht vor, Dokumentationen, die als Nachweise für die Implementierung der Funktionalitäten herangezogen werden können, anzufordern.

Der Auftragsgegenstand muss frei von Schadcode (Malware, Spyware), Hintertüren oder sonstigen nicht dokumentierten Funktionen (z.B. unautorisierte Datenweiterleitung) sein und zum Zeitpunkt der Auslieferung dürfen keine bekannten Sicherheitsmängel enthalten sein. Auf Anfrage müssen Nachweise über durchgeführte Sicherheitstests vorgelegt werden.

6.4 Protokollierung

Es muss eine Protokollierungsfunktion implementiert werden, um z.B. Handlungen, Aktivitäten oder dergleichen aufzuzeichnen und/oder nachzuvollziehen.

6.5 Auditrecht

Der AG ist nach ISO 27001 auf Basis IT-Grundschutz zertifiziert. Des Weiteren ist die Zentrale des AG als Betreiber kritischer Infrastruktur verpflichtet, für einen sicheren und zuverlässigen Betrieb ihrer IT-Systeme und Einrichtungen zu sorgen und die Verfügbarkeit der kritischen Dienstleistungen uneingeschränkt zu gewährleisten.

Aus diesen Gründen ist eine Dienstleistersteuerung durch den AG notwendig. Die Umsetzung erfolgt in regelmäßigen Security-Reifegradaudits. Diese finden im Regelfall remote statt.

Ziel soll es sein, dass die externen Dienstleistenden jährlich überprüft werden und Abweichungen frühzeitig dokumentiert und abgestellt werden können. Dadurch soll das erreichte Sicherheitsniveau des AG mindestens gehalten und sogar verbessert werden. Die Prüfgrundlage orientiert sich dabei an den vertraglich vereinbarten Sicherheitsanforderungen, den Anforderungen des IT-Grundschutz-Kompendiums in der aktuellen Edition, den

Richtlinien zur Informationssicherheit des AG und weiteren, welche im Rahmen der Erbringung der externen Dienstleistung notwendig sein können.

Zur Durchführung der Audits erteilt der Auftragnehmer der Zentrale des AG ein Auditrecht in Bezug auf den Ausschreibungsgegenstand.

6.6 Verschlüsselung

Der AN sichert die Verschlüsselung für den Austausch bzw. die Übertragung von Daten des AG zu. Der AN übernimmt die Verantwortung für die Datenübertragung, sobald sie außerhalb der von dem AG kontrollierten Systeme erfolgt.

Ruhende Daten des AG werden vom AN verschlüsselt, während sie im Cloud-Service gespeichert werden.

6.7 Ort der Verarbeitung der Daten

Der Sitz des Cloud-Anbieters und die Standorte aller Rechenzentren befinden sich im EWR. Für Unterauftragnehmer gilt dies in gleicher Weise.

6.8 Datenrückgabe und Datenlöschung

Der AN stellt die elektronische Rückgabe und die vollständige und nicht wiederherstellbare Löschung von Daten des AG mittels standardisiertem Verfahren (z.B. VSITR-Standard des Bundesamtes für Sicherheit/Informationstechnik (BSI)) bei Vertragsende oder auf Anforderung des AG sicher und reicht einen Nachweis darüber nach.

6.9 Penetrationstests

Der AN führt Penetrationstests durch und richtet interne Richtlinien ein, die bestimmen, wie der Cloud Service proaktiv getestet wird. Der AN gewährt dem AG auf Anforderung Einblick in die Dokumentation der durchgeführten Tests. Der AG hat das Recht in Abstimmung mit dem AN eigene PEN-Tests durchzuführen.

6.10 Einschränkung des Zugangs Dritter

Als "Dritte" gelten im Zuge der Anforderung alle bei dem und für den AN tätigen Personen, welche Zugriff auf vom AG genutzte Cloud-Services bzw. die verarbeiteten Daten haben können.

Der AN muss durch technische und organisatorische Maßnahmen die Einhaltung der nachfolgenden Punkte für Support-Zugriffe sicherstellen, oder vertraglich durch den Cloud-Anbieter sicherstellen lassen:

- Support-Zugriffe sind nur nach expliziter Freigabe durch den AG möglich.
- Rechte für Support-Zugriffe werden nach dem Least-Privilege-Prinzip vergeben.
- Support-Zugriffe werden zeitlich auf einen minimal notwendigen Rahmen eingeschränkt.
- Die Nachvollziehbarkeit aller Support-Tätigkeiten (welche Tätigkeiten Dritte innerhalb dieses Zeitraums durchgeführt haben) muss gewährleistet werden.
- Zugriffe erfolgen ausschließlich über verschlüsselte, sichere Verbindungen.

6.11 Weitere Sicherheitsanforderungen an den AN

Im Folgenden sind weitere Sicherheitsanforderungen an den AN benannt:

- Der AN sichert zu, dass die Subauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und dass zugesicherte Prüfrechte sich auch auf Subauftragnehmer beziehen.
- Es muss ein durchgehender und deutschsprachiger Support sichergestellt sein.
- Der AN verpflichtet sich, sicherheitsrelevante Vorfälle, die die Daten des AG betreffen, unverzüglich dem AG zu melden.
- Für den Fall eines freiwilligen oder unfreiwilligen Provider-Wechsels muss die Portabilität und Interoperabilität sichergestellt werden.

7. Abkürzungen / Glossar

Begriff	Bemerkung
AA	Agentur für Arbeit, Arbeitsagentur.
AN	Auftragnehmer
Anleitung	Synonym mit Handbuch zu verwenden. Bestandteil der Qualifizierungsunterlagen
AG	Auftraggeber
Arbeitstage	Montag bis Freitag, außer an bundeseinheitlichen und an nicht bundeseinheitlichen Feiertagen am Erfüllungsort sowie am 24. Dezember und 31. Dezember.
BA	Bundesagentur für Arbeit
Barrierefreiheit	Gesetzliche Vorgaben gemäß → BITV 2.0
BITV 2.0	Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung)
Dienststelle	Sammelbegriff für alle Lokationen der BA u. a. Arbeitsagenturen und Geschäftsstellen. Hier werden auch die gE mit gemeint.
Feiertag	Als Feiertage gelten bundeseinheitliche Feiertage am Erfüllungsort (Nürnberg), sowie der 24. Dezember und der 31. Dezember
gE	Jobcenter in der Form einer gemeinsamen Einrichtung. Abzugrenzen und nicht in dieser LB betroffen sind Jobcenter in Form als zugelassene kommunale Träger (zkT).
Gesamtsystem	Umfasst die SaaS-Lösung s. Kapitel 2.3 und Zahlungsinfrastruktur
IKT	Informations- und Kommunikationstechnik
Karteninhaber/-nutzer bzw. Kartennutzende	Kundinnen und Kunden der BA und gE. Personen, die Leistungen nach dem SGB II und SGB III via Debitkarte empfangen -> Hier synonym mit Leistungsempfangende. Die Karteninhaber sind gleichzeitig auch Kartennutzende.
Kundinnen und Kunden	Bezeichnung für Menschen, die Leistungen nach dem SGB II und SGB III von den Jobcentern (gE) und Agenturen erhalten. In dieser LB bezogen auf diejenigen Kundinnen und Kunden ohne Konto. Hier gleichzusetzen mit Karteninhabern/-nutzenden und Leistungsempfangenden.
Leistungsempfangende	Sachliche Bezeichnung für Menschen die Leistungen nach dem SGB II und SGB III empfangen. Umfasst auch Minderjährige oder Menschen ohne deutschen Pass. - > Leistungsempfangende. In dieser LB bezogen auf diejenigen Leistungsempfangenden ohne Konto. Hier gleichzusetzen mit Karteninhabern/-nutzenden und Kundinnen und Kunden.
RD	Regionaldirektion bzw. Regionaldirektionsbezirk (Zuständigkeitsbereich einer RD).

MFA	Mehrfach-Faktor Authentifizierung
MS-Teams	Microsoft Teams
Online-Portal	Umfasst eine Webanwendung mit allen Funktionen für Kundinnen und Kunden der BA und der gE bzw. für die Kartennutzenden. Z.B. Höhe des aktuellen Limits einsehen.
Qualifizierungsunterlagen	Umfasst die Anleitung (Handbuch), FAQs und die Präsentationsunterlagen aus den durchgeführten Schulungen
Remote	Leistungen unter Inanspruchnahme von technischen Einrichtungen zur Fernkommunikation von einem Standort außerhalb des Einsatzortes der Leistungen.
SaaS-Lösung	Umfasst die Webanwendung für Mitarbeiterinnen und das Online-Portal für Kartennutzende sowie die App
Scheme	Visa oder Mastercard als Betreiber des jeweiligen Kartenzahlungsnetzwerks
Servicezeiten	Montag bis Freitag von 08:00 Uhr bis 17:00 Uhr, ausgenommen sind → Feiertage
Träger	Jobcenter in Form von gemeinsamen Einrichtungen.
Webanwendung für Mitarbeiterinnen und Mitarbeiter der BA und gE	Das Stand-Alone-System zur Verwaltung der Karten für die Mitarbeiterinnen und Mitarbeiter ohne technische Anbindung in die BA-Systeme. Zugriff nur für berechtigte Mitarbeiterinnen und Mitarbeiter der BA und gE. Z.B. Neue Karte anlegen.