Leistungsbeschreibung

Bereitstellung dPhoenixSuite 3.0 APP Umgebung

Software as a Service (SaaS)

Inhaltsverzeichnis

1. Einleitung

Dataport stellt Auftraggebern mit dPhoenixSuite 3.0 eine Software-Lösung as a Service [SaaS], mit unterschiedlichen Funktionsmodulen, zur Verfügung.

Alle Module basieren auf Open-Source-Lösungen und werden durch Dataport gemanagt und betrieben.

Jedes Funktionsmodul kann durch Dataport ganz oder teilweise verändert werden, soweit die hier zugesicherten Eigenschaften nicht beeinträchtigt werden.

1.1. Beschreibung der APP-Umgebung

Die Dataport-eigene Umgebung [PX-Umgebung genannt] besteht aus zwei weitestgehend identischen Umgebungen]: der PROD- [Production] und der APP-Umgebung [Approval]. In dieser Umgebung können interessierte Kunden die Software kennenlernen und erproben.

Die APP-Umgebung ist identisch zur PROD-Umgebung. Die Administration der APP erfolgt durch die Qualitätssicherung des Programms Phoenix.

Daten, die zu einem Account gehören [E-Mails, Office-Dokumente usw.] sind grundsätzlich nur für diesen einen Account sicht- und zugreifbar. Nach den Phasen der Einrichtung und Freischaltung kann die Umgebung somit produktiv im Rahmen Ihrer Erprobung genutzt werden.

Ausnahmen sind:

- Nutzer*innen können sich andere Nutzer*innen in Form von Vor- und Nachname sowie Profilbild [wenn vorhanden] anzeigen lassen.

- Nutzer*innen können sich gegenseitig Dateien und Daten freigeben.

1.2. Unterschiede zwischen APP- und PROD-Umgebung im Hinblick auf den Schutzbedarf „Normal“

Ziel ist es, im Dialog mit Kunden Fortentwicklungen und beispielsweise Updates gemeinsam im Kundenumfeld zu erproben und so einen ständigen Optimierungsprozess sicherzustellen, bevor in einem zweiten Schritt diese für den Wirkbetrieb auf der PROD- Umgebung ausgerollt werden. Die Betriebsprozesse der APP-Umgebung entsprechen grundsätzlich - mit den nachfolgenden Ausnahmen bzw. Einschränkungen - denen der PROD-Umgebung.

- Die Daten sind wie in der Produktionsumgebung nach Grundschutz gesichert und damit ohne aktives Wirken der Nutzer*innen nicht für Unbefugte zugänglich. Die Daten sind jedoch pro Kunde in der APP-Umgebung physisch nicht von- einander getrennt. Eine Nutzer*in kann einer Nutzer*in aus einer anderen Organisation, die ebenfalls einen Account auf dieser Umgebung besitzt, Daten zur Verfügung stellen, wenn sie diese entsprechend frei gibt

- Die Benutzerverwaltung obliegt Dataport. Benutzer*innen können nur über Dataport zugelassen, gelöscht oder geändert werden. Benutzer*innen können nicht eigenständig Einträge vornehmen. Damit behält Dataport die Kontrolle über die angelegten Zugänge.

- Wartungsfenster für die Umgebung sind fest vorgegeben und können nicht pro Kunde geändert werden. Es ist damit nicht möglich, auf individuelle Anforderungen einzelner Organisationen einzugehen.

- Datensicherung und -wiederherstellung werden für die komplette Approval-Umgebung durchgeführt, nicht pro Kunde. Es ist damit nicht möglich, auf individuelle Anforderungen einzelner Organisationen [Kunden] einzugehen.

- Das „Branding“ der APP-Umgebung ist vorgegeben. Es ist nicht möglich, auf individuelle Anforderungen einzelner Organisationen [Kunden] einzugehen.

- Nutzer*innen können nicht ihre berufliche beziehungs- weise organisatorische E-Mail-Adresse verwenden, sondern müssen die vordefinierte Domain „@app.px.dphoenixsuite.de“ verwenden. Die Mail-Domain entspricht damit nicht der „normal“ genutzten E-Mail Adresse.

Die Schutzbedarfsfeststellung ist analog der PROD-Umgebung für Schutzbedarf NORMAL durchgeführt. Ein gesondertes Sicherheitskonzept für die Approval Umgebung ist nicht vorgesehen. Die Umsetzung nach BSI wird entsprechend der IT-Strukturanalyse für die PROD-Umgebung maßnahmenbezogen dokumentiert und regelmäßig überprüft.

1.3. Organisatorische Maßnahmen, die die entstehende Gefahr für den Schutzbedarf minimieren

- Anlegen der Accounts mit einem speziellen Präfix für die Benutzernamen [[organisation.]vorname.nachname]:

In dPhoenixSuite wird an verschiedenen Stellen eine Komfortfunktion verwendet, die eine Vorschlagsliste von bestehenden Accounts auf der APP-Umgebung anzeigt. Wenn beispielsweise eine Datei zur Bearbeitung durch eine andere Nutzer*in freigegeben werden soll, schlägt das System während der Eingabe der ersten Buchstaben passende Nutzer*innen-Accounts vor. Diese Liste wird aus den Anfangsbuchstaben des Benutzernamens, mit dem man sich einloggt, generiert.

Mit der Verwendung eines Präfixes wird sichergestellt, dass in der Vorschlagsliste ausschließlich Accounts der eigenen Organisation aufgeführt sind, so dass das Risiko einer versehentlichen Freigabe für Personen außerhalb der eigenen Organisation stark minimiert wird.

Die Anlage der Nutzer*innen mit Präfix ist gesondert zu beantragen, ansonsten wird kein Präfix automatisch verwendet.

- Alle Benutzer*innen sollten über die Risiken, des versehentlichen weitergeben von Daten, informiert werden

- Alle Benutzer*innen sollten über die Risiken eines Datenverlusts, durch beispielsweise ein versehentliches permanentes Löschen, informiert werden

- Alle Benutzer*innen sollten angewiesen werden, keine Daten in der APP-Umgebung mit höherem Schutzbedarf für die Erprobung verwenden.

1.4. Darstellung des Restrisikos

Eine individuelle Wiederherstellung von gesicherten Daten kann in der APP-Umgebung nicht durchgeführt werden. Es kann lediglich ein Backup der gesamten Umgebung zurückgespielt werden. Zudem könnten Daten, die beispielsweise versehentlich von Nutzer*innen freigegeben worden sind, von Nutzer*innen anderer Organisationen eingesehen und gegebenenfalls verändert werden.

2. Leistungsgegenstand

2.1. Funktionsumfang

Mit der dPhoenixSuite 3.0 stellt Dataport einen cloudbasierten Web-Arbeitsplatz für den öffentlichen Sektor [Verwaltung, Schulen, Universitäten, Kultur, …] als Service bereit. Zur Wahrung der digitalen Souveränität unserer Auftraggeber*innen, werden dabei Alternativen zu den marktbeherrschenden Produkten verwendet.

2.1.1. Modul dPhoenixPortal [Web-Front-End]

Die dPhoenixSuite 3.0 wird dem / der Endanwender*in mit einem zentralen Portal [dPhoenixPortal] als Web-Anwendung bereitgestellt. Alle beauftragten Module sind aufrufbar. Der Link, über den der Zugang erfolgt, wird dem/der Auftraggeber*in gesondert mitgeteilt. Im Portal werden zudem Anwendungsdokumentationen für die einzelnen Funktionsmodule, sowie FAQs für den / die Endanwender*in bereitgestellt. Zudem bietet das Portal folgende Möglichkeiten zur Selbstverwaltung:

_ Endanwender*innen editieren Meta-Informationen zur eigenen Identität

_ Passwortänderung sowie Zurücksetzung durch Endanwender*innen

2.1.1.1. Identity und Access Management [Benutzerverwaltung / IAM]

Die dPhoenixSuite 3.0 stellt einen Verzeichnisdienst [IAM] für die zentrale Benutzerverwaltung zur Verfügung:

_ Modulübergreifendes Single Sign-on

_ User-Self-Service: Möglichkeit der Änderung seiner persönlichen Attribute

2.1.2. Modul dPhoenixOffice

dPhoenixOffice stellt über den dPhoenixFileShare einen Cloudspeicher zum Bearbeiten, Versionieren und Teilen von Dateien bereit. Jede:r Benutzer*in erhält einen Speicherort für Dateien. Auf diese kann über den Browser zugegriffen werden.

Der Zugriff findet immer über das Internet statt. Der / die Benutzer*in kann hier Dateien ablegen und in Ordnern organisieren. Sowohl Dateien als auch Ordner können mit anderen Benutzer*innen geteilt werden. Die Freigaben können sowohl zeitlich begrenzt als auch unbegrenzt erteilt und / oder durch ein Passwort geschützt werden. Die gespeicherten Dateien werden durch Versionierung und durch einen Papierkorb vor dem versehentlichen Ändern bzw. Löschen bewahrt. Wenn Dateien verändert werden, werden alte Versionen der Datei weiter vorgehalten und können durch den / die Benutzer*in wiederhergestellt werden. Ebenso werden gelöschte Dateien zuerst in einen Papierkorb verschoben, von dem aus diese von dem / der Benutzer*in wiederhergestellt werden können. Versionen und gelöschte Dateien werden 30 Tage vorgehalten und dann automatisch gelöscht. Die Versionen und der Papierkorb zählen mit in die Speicherquota der Benutzer*innen.

In dem Teilmodul dPhoenixOffice können Benutzer*innen Dateien aus dem Modul dPhoenixFileShare in einer Web-Office-Funktion erstellen und online bearbeiten. Sowohl die Echtzeit-Kollaboration mit mehreren Benutzer*innen als auch Einzelbearbeitung von Dokumenten wird unterstützt.

Die Bearbeitung kann durch alle Personen stattfinden, die schreibenden Zugriff auf die jeweilige Datei haben. Die Funktionen umfassen Textverarbeitung, Tabellenkalkulation und Präsentationen. Es ist möglich, Dateien herunterzuladen und in andere Formate zu exportieren.

Folgende Dateitypen werden unterstützt:

_ Power-Point-Präsentationen [pptx, potx]

_ Excel-Tabellen [xlsx, xlst, csv]

_ Word-Dateien [docx, dotx]

_ OpenDocument Text [odt, ott]

_ OpenDocument Tabelle [ods, ots]

_ OpenDocument Präsentation [odp]

_ Markdown Documentation File [md]

_ Plain-Text-Datei [txt]

_ Rich Text [rtf]

_ HTML

_ Zeichnungen [odg]

Folgende Dateien können lesend geöffnet werden:

_ Gängige Bildformate [wie z. B. JPG, PNG und GIF]

_ Gängige Videoformate [wie z. B. MP4, MOV und WebM]

_ PDF, PDF/A

2.1.3.Modul dPhoenixMail [Groupware / E-Mail, Kalender, Kontakte]

Mit dem Modul dPhoenixMail stellt die dPhoenixSuite 3.0 einen vollwertigen E-Mail-Dienst zur Verfügung. Dies umfasst die gängigen Funktionen der E-Mail-Kommunikation, Drag & Drop, Freigabe und gleichzeitiges Bearbeiten von Objekten sowie Standardfunktionen eines E-Mail-Clients. Mit einem Groupware-Konto erhält ein:e Benutzer*in ein personenbezogenes Postfach, Zugriff auf das zentrale Adressbuch, einen persönlichen Kalender sowie die Aufgabenfunktion. Der Zugriff auf dPhoenixMail erfolgt ausschließlich über einen Browser.

Folgende Funktionen stehen zur Verfügung:

_ Import, Anlage und Verwaltung persönlicher Kontaktlisten

_ Freigabe von Kontaktlisten an Benutzer*innen der eigenen Organisation

_ Anlegen, Verwalten und Freigeben persönlicher Verteilerlisten

_ Import, Anlage, Verwaltung und Freigabe eigener und / oder externer Kalender [z. B. Feiertage, Ferien]

_ Freigabe von Ordnern oder Postfächern an Benutzer*innen aus der eigenen Organisation

_ Erstellung, Bearbeitung, Zuweisung und Statusverfolgung von Aufgaben

2.1.4.Modul dOnlineZusammenarbeit 2.0 [Messaging, Audio, Video]

Das Modul dOnlineZusammenarbeit 2.0 ist eine Plattform für die digitale Zusammenarbeit. Es umfasst unter anderem eine Video- und Audiokonferenzlösung sowie eine Chat-Funktion und die Möglichkeit, Bildschirminhalte, wie beispielsweise Präsentationen, zu teilen, Dateien auszutauschen oder gemeinsam an einem Whiteboard zu arbeiten. Der Zugriff auf dOnlineZusammenarbeit 2.0 erfolgt ausschließlich über einen Browser.

2.1.5.Datensicherung und Backup

Die Infrastrukturkomponenten sind redundant ausgelegt, um Ausfällen aufgrund von Hardwareversagen vorzubeugen. Die gespeicherten Daten werden täglich gesichert. Diese Sicherungen dienen ausschließlich der Systemwiederherstellung.

_ Konsistentes Backup des Gesamtsystems [Alle Module; mindestens einmal am Tag]

_ Maximaler Datenverlust 24 Stunden

_ Maximale Wiederherstellungszeit der Daten 24 Stunden

_ Versionierung von gespeicherten Dateien in dPhoenixOffice mit einer maximalen Speicherfrist von 30 Tagen

3. Betrieb und Monitoring

3.2. Sicherheit

Durch umfangreiche technische und organisatorische Maßnahmen stellt die Auftragnehmer*in [Dataport] den sicheren Betrieb des Gesamtsystems sicher. Für das Update- und Patchmanagement der Infrastrukturkomponenten ist die Auftragnehmer*in verantwortlich. Dies gilt auch für ggf. eingesetzte Subunternehmer*innen.

Aufgaben und Zuständigkeiten	Auftragnehmer*in	Auftraggeber*innen
Betrieb der Infrastruktur	V, D, B	I
Sicherer Betrieb des Gesamtsystems nach Bereitstellung, inkl. Einspielung von Patches und Updates	V, D, B	I
Planung und Durchführung von systemspezifischen Wartungsarbeiten an der Infrastruktur	V, D	I

3.3. Virenschutz

Die Auftragnehmer*in gewährleistet für die Bereitstellung des Gesamtsystems einen Virenschutz.

Aufgaben und Zuständigkeiten	Auftragnehmer*in	Auftraggeber*innen
Betrieb und Betreuung des Virenschutzes der Infrastruktur	V, D, B	I

Die Server innerhalb des Gesamtsystems unterliegen einem Monitoring [Event-, Trend- und Log-Monitoring].

3.4. Zugang

Die dPhoenixSuite 3.0 ist über das Internet verfügbar. Aus der dPhoenixSuite 3.0 lassen sich alle beauftragten Module und Funktionen aufrufen und nutzen. Zusätzlich kann es notwendig sein, für den Zugang über Landesnetze sowie kommunalen Verwaltungsnetze separate Freischaltungen beim Dataport Policy Management einzureichen.

3.5. Netzkommunikation

Die Server des Gesamtsystems können nur untereinander kommunizieren.

3.6. Verschlüsselung

Es wird eine Transportwegverschlüsselung nach den gängigen Sicherheitsstandards eingesetzt.

3.7. Löschung von Daten

Im Falle einer Vertragskündigung ist der / die Auftraggeber*in dafür verantwortlich, die von ihm / ihr gespeicherten Daten, rechtzeitig, vor Beendigung des Vertrages, anderweitig zu sichern.

Unabhängig vom Kündigungsgrund und von der Vertragspartei, welche die Kündigung ausgesprochen hat, löscht die Auftragnehmer*in alle Daten der Auftrageber*innen, einschließlich eventuell noch vorhandenen Datensicherungen, spätestens 30 Tage nach Beendigung des Vertrages.

Eine Wiederherstellung von Daten ist nach dieser Löschung ausgeschlossen. Ausgenommen von der Löschung sind Daten, die von der Auftragnehmer*in zu Abrechnungszwecken über diese Frist hinaus benötigt werden oder soweit sie einer gesetzlichen Aufbewahrungspflicht unterliegen.

3.8. Betriebszeiten

3.8.6. Versions- und Funktionsupdates

Die Auftragnehmer*innen werden den Auftraggeber*innen innerhalb sieben bis vierzehn Tage vor Veränderungen in den Systemen über diese informieren. Davon ausgenommen sind Sicherheitsupdates.

3.8.7. Onlineverfügbarkeit

Die zentrale Infrastruktur steht ganztägig zur Verfügung, d. h. an sieben Tagen in der Woche [Verfügbarkeit 95 %] – ausgenommen der in Kapitel 3.9 Wartungsarbeiten angegebenen Einschränkungen [z. B. Wartungsfenster, akutes Einspielen von Sicherheitsupdates].

3.8.8. Servicezeit – Betreuter Betrieb

_ Montag bis Donnerstag: 08.00 Uhr bis 17.00 Uhr

_ Freitag: 08.00 Uhr bis 15.00 Uhr

In diesen Zeiten erfolgt die Überwachung und Betreuung der Systeme durch Administrator*innen der Auftragnehmerin. Es stehen Ansprechpartner*innen mit systemtechnischen Kenntnissen für den Betrieb und zur Störungsbehebung zur Verfügung. Im Problem- und Störungsfall wird das entsprechende Personal der Auftragnehmer*in über den User-Help-Desk [UHD] der Auftragnehmer*in informiert.

3.8.9. Betriebszeit – Überwachter Betrieb

_ Alle Zeiten außerhalb des betreuten Betriebes

Auch außerhalb des betreuten Betriebes stehen die Systeme den Anwender*innen grundsätzlich zur Verfügung.

Die zentrale Infrastruktur wird automatisiert überwacht.

Ansprechpartner*innen stehen während des überwachten Betriebes nicht zur Verfügung.

3.9. Wartungsarbeiten

Die regelmäßigen, periodisch wiederkehrenden Wartungs- und Installationsarbeiten erfolgen i. d. R. außerhalb der definierten Servicezeiten des betreuten Betriebes.

Derzeit ist ein Wartungsfenster wie folgt definiert:

Wartungsfenster	Zeitraum
Standard	Dienstag 19.00 Uhr bis Mittwoch 06.00 Uhr
Datensicherung	Täglich 0.00 Uhr bis 06.00 Uhr

In diesen Zeiten werden Wartungsarbeiten durchgeführt und das Arbeiten ist ggf. nur eingeschränkt möglich.

3.10. Support

Die Auftragnehmer*in übernimmt den Support für die Infrastruktur sowie dazugehörige Komponenten. Die Auftragnehmer*in ist berechtigt, für die Leistungserbringung Subunternehmen einzusetzen.

3.11. Störungsannahme

Die Meldung von Störungen durch meldeberechtigte Personen erfolgt grundsätzlich über das Call-Center oder den User-Help-Desk des Auftragnehmers.

Die Rufnummern lauten:

_ 040 428 46 1904

_ 0421 361 4444 [Trägerland Bremen]

Im Rahmen der Störungsannahme werden grundsätzlich Meldedaten sowie die Störungsbeschreibung erfasst und ausschließlich für die Störungsbehebung gespeichert. Der Störungsabschluss wird der meldenden Person bekannt gemacht.

3.12. Incident-Management

Betriebsstörungen werden als so genannte Incidents im zentralen Trouble Ticket System [TTS] aufgenommen. Jeder Incident und dessen Bearbeitungsverlauf werden im TTS dokumentiert.

Generell unterbrechen die Zeiten außerhalb des betreuten Betriebes die Bearbeitungszeit. Ebenso wird die Störungsbearbeitung durch höhere Gewalt oder durch Ereignisse, die durch die Auftraggeber*innen oder den Nutzer*innen zu verantworten sind, unterbrochen [z. B. Warten auf Zusatzinformationen durch den / die Nutzer*in, Unterbrechung auf Nutzerwunsch, etc.].

Folgende Prioritäten werden für die Störungsbearbeitung im Rahmen der beauftragten Leistungen auf der folgenden Seite definiert:

Priorität	Auswirkung	Dringlichkeit	Bearbeitung
Niedrig [bisher 4]	Incident betrifft einzelne Anwender*innen. Die Geschäftstätigkeit ist nicht eingeschränkt.	Ersatz steht zur Verfügung und kann genutzt werden oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchfüh- rung durch den Incident behindert werden, können später erfolgen.	Priorität „Niedrig“ führt zur Bearbeitung durch die Auftragnehmer*in und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit [Beginn der Bearbeitung oder qualifizierter Rückruf] ergibt sich aus der Serviceklasse.
Mittel [bisher 3]	Wenige Anwender*innen sind von dem Incident betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.	Ersatz steht nicht für alle betroffenen Anwender*innen zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann später oder auf anderem Wege evtl. mit mehr Aufwand durchgeführt werden.	Priorität „Mittel“ führt zur standardmäßigen Bearbeitung durch die Auftragnehmer*in und unterliegt der Überwachung des Lösungs- fortschritts. Die Reaktionszeit [Beginn der Bearbeitung oder qualifizierter Rückruf] ergibt sich aus der Serviceklasse.
Hoch [bisher 2]	Viele Anwender*innen sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann ein- geschränkt aufrechterhalten werden.	Ersatz steht kurzfristig nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, muss kurzfristig durchgeführt werden.	Priorität „Hoch“ führt zur bevorzugten Bearbeitung durch die Auftragnehmer*in und unterliegt besonderer Überwachung des Lösungsfortschritts. Die Reaktionszeit [Beginn der Bearbeitung oder qualifizierter Rückruf] ergibt sich aus der Serviceklasse.
Kritisch [bisher 1]	Viele Anwender*innen sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann nicht aufrechterhalten werden.	Ersatz steht nicht zur Verfügung. Die Tätigkeit, bei der der Incident auftrat, kann nicht verschoben oder anders durchgeführt werden.	Priorität „Kritisch“ führt zur umgehenden Bearbeitung durch die Auftragnehmer*in und unterliegt intensiver Überwachung des Lösungsfortschritts. Die Reaktionszeit [Beginn der Bearbeitung oder qualifizierter Rückruf] ergibt sich aus der Serviceklasse.

Es gelten einheitlich folgende Reaktionszeiten bei Störungen [je Störungspriorität und während der Supportzeit]:

Priorität	Reaktionszeit
Niedrig [bisher 4]	4 Stunden
Mittel [bisher 3]	2 Stunden
Hoch [bisher 2]	1 Stunde
Kritisch [bisher 1]	0,5 Stunden

3.13. Rollendefinition

Die allgemeine Zuordnung von Aufgaben zu Rollen ist wie folgt definiert

Rolle	Rollendefinition
Auftraggeber*innen [AG]	Rolle der Auftraggeber*innen im Sinne der DSGVO
Auftragsverabeiter*innen [AV]	Zentraler Betrieb, Auftragsverarbeiter*innen im Sinne der DSGVO
Auftragsberechtigte:r [AB]	Abruf von im Vertrag definierten Services der Auftragverarbeiter*innen. Der Abruf erfolgt durch von dem / der Auftraggeber*in benannte autorisierte Auftragsberechtigte. Der / die Auftrag- geber*in benennt diese Personen und pflegt die Liste der autorisierten Auftrags- berechtigten.
Anwender*innen	Anwender*innen sind alle Endanwen- der*innen, die das Verfahren nutzen. Anwender*innen müssen nicht Mitarbei- ter*innen des / der Auftraggebers/in sein.

4. Protokollierung

Innerhalb der IT-Infrastruktur des Produktes dPhoenixSuite findet eine Protokollierung statt.

Eine regelmäßige Auswertung erfolgt nicht, sondern nur im Bedarfsfall, wie zum Beispiel dem Verdacht, dass ein Sicherheitsrisiko vorliegt. Standardmäßige Löschfristen sind:

Typ	Inhalt	Aufbewahrungsfrist	Löschfrist
Infrastruktur-Protokollierung [Adminplattform, Cloud-Manager]	technisch, personenb., mandant	12 Monate	12 Monate
System-Protokollierung [Betriebssystem, Basissoftware]	technisch	1 Monat	1 Monat
Audit-Protokollierung [Betriebssystem]	technisch, personenb.	12 Monate	12 Monate
Applikations-Protokollierung [Phoenix Softwarestack]	technisch, personenb., mandant	3 Monate	3 Monate
Protokollierung der Nutzeraktionen [Detailinformationen]	technisch, personenb., mandant	10 Tage	10 Tage
Nutzungsinformationen [aggregierte Reporting Informationen]	personenb., mandant	2 Jahre	2 Jahre
Protokollierung der Verbindungsdaten [Detailinformationen]	technisch, personenb., mandant	10 Tage	10 Tage
Abrechnungsinformationen [aggregierte Billing Informationen]	personenb., mandant	2 Jahre	2 Jahre

5. Mitwirkungsleistungen und Pflichten des Auftraggebers

Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers / der Auftraggeberin erforderlich, die nachfolgend aufgelistet sind:

_ Durchführung von Freigabetests, d.h. der Prüfung des Systems auf Gebrauchsfähigkeit in Anlehnung an die Anforderungen.

Die Auftragnehmer*in weist darauf hin, dass das BSI die Erstellung einer Sicherheitsrichtlinie für Cloud-Nutzer*innen durch den / die Auftraggeber*in empfiehlt.

Zusätzlich gelten für den / die Auftraggeber*in folgende Pflichten:

_ Der/die Auftraggeber*in prüft eigenverantwortlich die Einhaltung aller für ihn im Zusammenhang mit der Nutzung der Leistung relevanten und anwendbaren rechtlichen Vorschriften, Gesetze und Verordnungen und stellt deren Einhaltung sicher.

_ Der / die Auftraggeber*in benennt eine:n Ansprechpartner*in mit Vertretung.

6. Erläuterungen

6.1. Begriffsfestlegungen

Betriebsmodus	Begriffsdefinition
Online-verfügbarkeit	Onlineverfügbarkeit beschreibt Zeiträume, in denen definierte Basisleistungen und Services zur Verfügung stehen und automatisiert überwacht werden.
Servicezeit [Betreuter Betrieb]	Die Servicezeit „Supportzeit [betreuter Betrieb]“ beschreibt die Zeiträume, in denen die Ressourcen, Funktionen und Module [Basisleistungen] von der Auftragnehmer*in bedient und Störungen und Anfragen bearbeitet werden.
Betriebszeit [Überwachter Betrieb]	Die Betriebszeit ist der Zeitraum, in der die vereinbarten Server, Ressourcen, Funktionen und Module [Basisleistungen] von der Auftragnehmer*in zur Verfügung gestellt und automatisiert überwacht werden.
Wartungsfenster	Regelmäßiges Zeitfenster für Wartungsarbeiten an den Systemen, in dem die Systeme nicht oder nur eingeschränkt für den / die Auftraggeber*in nutzbar sind. Sollte in Sonderfällen ein größeres oder weiteres Wartungszeitfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem / der Auftraggeber*in. Der / die Auftraggeber*in wird nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Die Auftragnehmer*in wird in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informieren.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne, innerhalb der vereinbarten Servicezeiten, zwischen der Feststellung einer Störung durch den / die Dienstleister*in bzw. Meldung einer Störung durch den / die Auftraggeber*in über den vereinbarten Weg [Service Desk], bis zum Beginn der Störungsbeseitigung. Die Reaktionszeit beginnt mit der Aufnahme der Störung in das Ticketsystem der Auftragnehmerin.
Speicherquota	Hierbei handelt es sich um die Begrenzung des Speicherplatzes auf einem Datenspeicher für einen einzelnen Benutzer oder eine Benutzergruppe. Ziel ist es, eine technische Grenze für Speicherplatzverbrauch zu setzen, um sicherzustellen, dass alle Benutzer die zur Verfügung stehenden Systemressourcen bestmöglich nutzen können.

6.2. Erläuterung VDBI

Bezeichnung	Erläuterung
[V] Verantwortlich	“V” bezeichnet denjenigen / diejenige, der / die für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
[D] Durchführung	“D” bezeichnet denjenigen / diejenige, der / die für die technische Durchführung verantwortlich ist.
[B] Beratung	“B” bedeutet, dass die Partei zu konsultieren ist und z. B. Vorgaben für Umsetzungsparameter setzen oder Vorbehalte formulieren kann. „B“ bezeichnet somit ein Mitwirkungsrecht bzw. eine Mitwirkungspflicht.
[I] Information	“I” bedeutet, dass die Partei über die Durchführung und / oder die Ergebnisse des Prozessschritts zu informieren ist. „I“ ist rein passiv.