Leistungsbeschreibung

Bereitstellung dPhoenixSuite 2.0

Software as a Service (SaaS)

Inhaltsverzeichnis

1 Einleitung

Dataport stellt Auftraggebern mit **dPhoenixSuite 2.0** 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. Insbesondere können die eingesetzten Open-Source-Lösungen auch vollständig ausgetauscht werden, um das Funktionsmodul um weitere Funktionen zu erweitern oder um einen wirtschaftlicheren oder performanteren Betrieb zu ermöglichen. Die **dPhoenixSuite** wird dazu versioniert.

2 Leistungsgegenstand

2.1 dPhoenixSuite 2.0 Funktionsumfang

Mit der **dPhoenixSuite 2.0** stellt Dataport Dataport einen cloudbasierten Web-Arbeitsplatz für den öffentlichen Sektor (Verwaltung, Schulen, Universitäten, Kultur, …) als Service bereit. Zur Wahrung der digitalen Souveränität unserer Auftraggeber werden dabei Alternativen zu den marktbeherrschenden Produkten evaluiert sowie eine On-Premise-Lösung erstellt und optimiert.

2.1.1 Modul dPhoenixPortal (Web-Front-End)

Die **dPhoenixSuite 2.0** wird den Endanwendern und Administratoren mit einem zentralen Portal **(dPhoenixPortal)** als Web-Anwendung bereitgestellt.
Alle verfügbaren Module sind nach erfolgreicher Anmeldung im Front-End aufrufbar. Der Link, über den der Zugang erfolgt, wird dem Auftraggeber gesondert mitgeteilt.

Im Portal werden zudem Anwendungsdokumentationen für die einzelnen Funktionsmodule sowie FAQs für den Endbenutzer bereitgestellt. Zudem bietet das Portal folgende Möglichkeiten zur Selbstverwaltung:

- Endanwender editieren Meta-Informationen zur eigenen Identität
- Endanwender editieren persönliche Gruppen
- Passwortänderung sowie -rücksetzung durch Endbenutzer

2.1.1.1 Identity und Access Management (Benutzerverwaltung / IAM)

Mit dem **integrierten IAM** stellt die **dPhoenixSuite 2.0** einen Verzeichnisdienst für die zentrale und dezentrale Benutzerverwaltung zur Verfügung.

- Single Sign-On modulübergreifend
- User-Self-Service: Möglichkeit der Änderung seiner persönlichen Attribute

2.1.1.2 Administratoren-Funktion

Dem Auftraggeber wird ein Administratoren-Zugang für das Web-Front-End (**dPhoenixPortal**) zur Verfügung gestellt.

Dieser ermöglicht folgende Einstellungen:

- Anlegen, Editieren und Löschen von Identitäten, Rollen, Rechten und Gruppen durch Systemadministratoren innerhalb der eigenen Organisation
- User Helpdesk unterstützt z.B. beim Passwortwechsel
- Administratoren editieren Rollen und Berechtigungen

2.1.2 Modul dPhoenixFileShare

dPhoenixFileShare stellt einen Cloudspeicher zum Bearbeiten, Versionieren und Teilen von Dateien bereit.
Jeder Benutzer erhält einen Speicherort für Dateien. Auf diese kann über den Browser zugegriffen werden. Der Zugriff findet immer über das Internet statt. Der Benutzer kann hier Dateien ablegen und in Ordnern organisieren. Sowohl Dateien als auch Ordner können mit anderen Benutzern 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 Benutzer wiederhergestellt werden. Ebenso werden gelöschte Dateien zuerst in einen Papierkorb verschoben, von dem aus diese vom Benutzer wiederhergestellt werden können. Versionen und gelöschte Dateien werden 30 Tage vorgehalten und dann automatisch gelöscht. Die Versionen und der Papierkorb zählen mit in das Speicherquota des Benutzers.

2.1.2.1 Teilmodul dPhoenixOffice (Web-Office)

Das **Teilmodul dPhoenixOffice** ist innerhalb des Moduls **dPhoenixFileShare** integriert. Hierbei können Benutzer Dateien aus dem Modul **dPhoenixFileShare** in einer Web-Office-Funktion erstellen und online bearbeiten. Sowohl die Echtzeit-Kollaboration mit mehreren Benutzern als auch Einzelbearbeitung von Dokumenten wird unterstützt.

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

Die Funktionen umfassen Textverarbeitung, Tabellenkalkulation und Präsentationen.
Hierbei können Benutzer bestimmte Dateien im Browser direkt aus dem Cloudspeicher heraus anlegen und bearbeiten. Unterstützt werden Textdateien, Präsentationen und Tabellenkalkulationen.

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

Folgende Dateien können lesend geöffnet werden:

- Bilder (JPEG, PNG, ...)
- Videos (MP4, ...)
- PDF/ PDF/A

2.1.3 Modul dPhoenixMail (Groupware / E-Mail, Kalender, Kontakte)

Mit dem Modul **dPhoenixMail** stellt die **dPhoenixSuite 2.0** einen vollwertigen E-Maildienst zur Verfügung. Dies umfasst die gängigen Funktionen der E-Mailkommunikation, Drag & Drop, Threading sowie Standardfunktionen eines E-Mail-Clients. Mit einem Groupware-Konto erhält ein Benutzer ein personenbezogenes Postfach, Zugriff auf das zentrale Adressbuch, einen persönlichen Kalender sowie die Aufgabenfunktion. Der Zugriff auf **dPhoenixMail** erfolgt ausschließlich über einen Internetbrowser.

Folgende Funktionen stehen zur Verfügung:

- Import, Anlage und Verwaltung persönlicher Kontaktlisten
- Freigabe von Kontaktlisten an Benutzer 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 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 z.B. Präsentationen zu teilen, Dateien auszutauschen oder gemeinsam an einem Whiteboard zu arbeiten.

2.1.5 Datensicherung und Backup

Die Infrastrukturkomponenten werden 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 24 Stunden
- Versionierung von gespeicherten Dateien in **dPhoenixFileShare** mit einer maximalen Speicherfrist von 30 Tagen

3 Betrieb und Monitoring

3.1 Sicherheit

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

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
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**

3.2 Virenschutz

Der Auftragnehmer gewährleistet für die Bereitstellung des Gesamtsystems einen Virenschutz.

Aufgaben und Zuständigkeiten	Auftrag-nehmer	Auftrag-geber
Betrieb und Betreuung des Virenschutzes der Infrastruktur	**V, D, B**	**I**

Die Server innerhalb des Gesamtsystems unterliegen einem Monitoring (Event-, Trend- und Log-Monitoring).

3.3 Zugang

Die **dPhoenixSuite 2.0** ist über das Internet und ggf. über die Landesnetze sowie kommunalen Verwaltungsnetze verfügbar. Aus der **dPhoenixSuite 2.0** lassen sich alle Module und Funktionen aufrufen und nutzen. Zusätzlich kann es notwendig sein, für den Zugang für die Landesnetze sowie kommunalen Verwaltungsnetze separate Freischaltungen beim Dataport Policy Management einzureichen.

3.4 Netzkommunikation

Die Server des Gesamtsystems können nur untereinander kommunizieren.

3.5 Verschlüsselung

Es wird eine Transportwegverschlüsselung nach den gängigen Sicherheitsstandards eingesetzt.

3.6 Löschung von Daten

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

Unabhängig vom Kündigungsgrund und von der Vertragspartei, welche die Kündigung ausgesprochen hat, löscht der Auftragnehmer alle Daten des Auftraggebers 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 vom Auftragnehmer zu Abrechnungszwecken über diese Frist hinaus benötigt werden oder soweit sie einer gesetzlichen Aufbewahrungspflicht unterliegen.

3.7 Betriebszeiten

3.7.1 Onlineverfügbarkeit

Die zentrale Infrastruktur steht ganztägig zur Verfügung, d.h. an sieben Tagen in der Woche (Verfügbarkeit 95 %) – ausgenommen der in Kapitel 3.8 angegebenen Einschränkungen (z.B. Wartungsfenster, akutes Einspielen von Sicherheitsupdates).

3.7.2 Servicezeit – Betreuter Betrieb[1]

- 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 Administratoren des Auftragnehmers. Es stehen Ansprechpartner mit systemtechnischen Kenntnissen für den Betrieb und zur Störungsbehebung zur Verfügung. Im Problem- und Störungsfall wird das entsprechende Personal des Auftragnehmers über den User Help Desk (UHD) des Auftragnehmers informiert.

3.7.3 Betriebszeit – Überwachter Betrieb

- alle Zeiten außerhalb des betreuten Betriebes

Auch außerhalb des betreuten Betriebes stehen die Systeme den Anwendern grundsätzlich zur Verfügung. Die zentrale Infrastruktur wird automatisiert überwacht. Festgestellte Fehler werden automatisch in einem Trouble Ticket System hinterlegt. Ansprechpartner stehen während des überwachten Betriebes nicht zur Verfügung.

3.8 Wartungsarbeiten

Die regelmäßigen, periodisch wiederkehrenden Wartungs- und Installationsarbeiten erfolgen i. d. R. außerhalb der definierten Servicezeiten des betreuten Betriebes. Derzeit ist ein Wartungs-fenster wie folgt definiert:

	Zeitraum
Standard-Wartungsfenster	Dienstag 19:00 Uhr bis Mittwoch 06:00 Uhr
Besondere Wartungsfenster	In Ausnahmefällen (z.B. wenn eine größere Installation erforderlich ist) werden diese Arbeiten nach vorheriger

[1] Gilt nicht für gesetzliche Feiertage des Landes Schleswig-Holstein sowie 24.12. und 31.12.

	Ankündigung (mindestens 2 Wochen vorher) an einem Wochenende vorgenommen.
Wartungsfenster Datensicherung	Täglich 0:00 Uhr bis 06:00 Uhr

In dieser Zeit werden Wartungsarbeiten durchgeführt und das Arbeiten ist ggf. nur eingeschränkt möglich.

3.9 Support

Der Auftragnehmer übernimmt den Support für die Infrastruktur sowie dazugehörige Komponenten. Der Auftragnehmer ist berechtigt für die Leistungserbringung Subunternehmen einzusetzen.

3.10 Störungsannahme[2]

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

Die Rufnummer ist 040 428 46 1904.

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

3.11 Incident-Management

Betriebsstörungen werden als 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 unterbrochen durch höhere Gewalt oder durch Ereignisse, die durch den Auftraggeber oder den Nutzer zu verantworten sind (z.B. Warten auf Zusatzinformationen durch den Nutzer, Unterbrechung auf Nutzerwunsch, etc.).

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

Priorität	Auswirkung	Dringlichkeit	Bearbeitung
Niedrig (bisher 4)	Incident betrifft einzelne Benutzer. Die Geschäftstätigkeit ist nicht eingeschränkt.	Ersatz steht zur Verfügung und kann genutzt werden, oder das betroffene System muss aktuell nicht genutzt werden. Tätigkeiten, deren Durchführung durch den Incident behindert werden, können später erfolgen.	Priorität „Niedrig“ führt zur Bearbeitung durch den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.

[2] Gilt nicht für gesetzliche Feiertage des Landes Schleswig-Holstein sowie 24.12. und 31.12.

Mittel (bisher 3)	Wenige Anwender sind von dem Incident betroffen. Geschäftskritische Systeme sind nicht betroffen. Die Geschäftstätigkeit kann mit leichten Einschränkungen aufrechterhalten werden.	Ersatz steht nicht für alle betroffenen Nutzer 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 den Auftragnehmer und unterliegt der Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Hoch (bisher 2)	Viele Anwender sind betroffen. Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann eingeschränkt 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 den Auftragnehmer und unterliegt besonderer Überwachung des Lösungsfortschritts. Die Reaktionszeit (Beginn der Bearbeitung oder qualifizierter Rückruf) ergibt sich aus der Serviceklasse.
Kritisch (bisher 1)	Viele Anwender 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 den Auftragnehmer 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

3.12 Rollendefinition

Die allgemeine Zuordnung von Aufgaben zu Rollen ist wie folgt definiert:

Rolle	Rollendefinition
Auftraggeber (AG)	Rolle des Auftraggebers im Sinne der DSGVO
Auftragsverabeiter (AV)	Zentraler Betrieb, Auftragsverarbeiter im Sinne der DSGVO
Auftragsberechtigte (AB)	Abruf von im Vertrag definierten Services des Auftragverarbeiters Der Abruf erfolgt durch vom Auftraggeber benannte autorisierte Auftragsberechtigte. Der Auftraggeber benennt diese Personen und pflegt die Liste der autorisierten Auftragsberechtigten.
Nutzer	Nutzer sind alle Endanwender, die das Verfahren nutzen. Nutzer müssen nicht Mitarbeiter des Auftraggebers sein.

4 Protokollierung

Innerhalb des Systemverbunds 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	technisch,	10 Tage, 10 Tage

(Detailinformationen)	personenb., mandant	
Abrechnungsinformationen (aggregierte Billing Informationen)	personenb., mandant	2 Jahre, 2 Jahre

5 Mitwirkungsleistungen und Pflichten des Auftraggebers

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

- Durchführung von Funktionstests

Der Auftragnehmer weist darauf hin, dass das BSI die Erstellung einer Sicherheitsrichtlinie für Cloud-Nutzer durch den Auftraggeber empfiehlt.

Zusätzlich gelten für den Auftraggeber folgende Pflichten:

- Der Auftraggeber 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 Auftraggeber benennt einen Ansprechpartner mit Vertretung.

6 Erläuterungen

6.1 Begriffsfestlegungen

Betriebsmodus	Begriffsdefinition
Onlineverfügbarkeit	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) vom Auftragnehmer 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) vom Auftragnehmer 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 Auftraggeber nutzbar sind. Sollte in Sonderfällen ein größeres oder weiteres Wartungszeitfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggeber. Der Auftraggeber wird nur in begründeten Fällen die Durchführung von

	Wartungsmaßnahmen einschränken. Der Auftragnehmer 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 Dienstleister bzw. Meldung einer Störung durch den Auftraggeber über den vereinbarten Weg (Service Desk) bis zum Beginn der Störungsbeseitigung. Die Reaktionszeit beginnt mit der Aufnahme der Störung in das Ticketsystem des Auftragnehmers.

6.2 Erläuterung VDBI

V = Verantwortlich	“V” bezeichnet denjenigen, der für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
D = Durchführung	“D” bezeichnet denjenigen, der 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.