Leistungsbeschreibung

Bereitstellung dOnlineZusammenarbeit 2.0 (Messaging/Audio/Video)

Software as a Service (SaaS)

Inhaltsverzeichnis

1 Einleitung

*Das Dokument bestimmt den zu erbringenden Leistungsgegenstand und die Beschreibung der Leistung für den Service **dOnlineZusammenarbeit 2.0**.*

1.1 Ausgangssituation

Die Anforderungen der Zusammenarbeit haben sich im Zuge von Homeoffice und mobiler Arbeit sowie der COVID19-Pandemie verändert. Auf Grund der Corona Krise in Deutschland ist der Bedarf an schnell skalierbaren Videokonferenz- und Onlinekollaborationslösungen für die Aufrechterhaltung der Arbeitsfähigkeit der öffentlichen Verwaltung der Länder sehr wichtig.

Dataport hat Vorkehrungen getroffen, schnell einer großen Anzahl von Nutzern eine Lösung bieten zu können. Dabei geht es um die Herstellung von virtuellen Klassenräumen und digitalem Unterricht für die Schulen und Sicherstellung von virtuellen Konferenzräumen für die Verwaltung.

Mit **dPhoenixSuite 2.0** und seinen Modulen stellt 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 Leistungsgegenstand

2.1 Beschreibung

dOnlineZusammenarbeit 2.0 (Modul für Messaging/Audio/Video aus **dPhoenixSuite 2.0**) ist eine Lösung zur Kommunikation im Verwaltungs- und Bildungsumfeld. Sie ermöglicht es, vielen Nutzer unkompliziert und ad hoc zu Online-Besprechungen zusammenzukommen. Es beinhaltet die in Matrix/Element integrierte Videolösung Jitsi.

- Dataport bietet eine Audio-/Videokonferenz-Lösung aus der sicheren Umgebung des eigenen Rechenzentrums unter Hinzunahme von Services aus Partner-Rechenzentren in Deutschland.
- Die Lösung lässt sich für die Arbeit aus dem Homeoffice und von verteilten Standorten nutzen, z.B. im Umfeld von Verwaltungen und für den digitalen Unterricht.
- Für die Teilnahme sind keine Installationen auf den Endgeräten notwendig.
- Die Lösung eignet sich auch bei geringen Datenübertragungsraten und ist auf praktisch allen stationären und mobilen Endgeräten (BYOD) Browser-, oder APP-basiert einsetzbar.

2.2 Funktionsumfang

Das Produkt **dOnlineZusammenarbeit 2.0** wird durch Dataport (Auftragnehmer) für den Auftraggeber bereitgestellt. Es erlaubt die digital souveräne Durchführung von Audio- und Videokonferenzen. Zum Einsatz kommt hierbei die Open-Source-Software Jitsi. Jitsi bietet eine sichere und verschlüsselte Audio- und Videokonferenz mittels hop-encryption aus dem sicheren Rechenzentrum von Dataport oder durch Dataport beauftragte Rechenzentren in Deutschland.

dOnlineZusammenarbeit 2.0 unterstützt in allen Protokollen Präsenz- und Sofortnachrichten. Es werden alle gängigen Protokolle bekannter Instant Messenger unterstützt und bei Bedarf im Rahmen der Weiterentwicklung erweitert. In vielen Fällen ist auch Dateiübertragung möglich.

Folgende Funktionen stehen standardmäßig zur Verfügung:

- Desktop-Sharing – Freigabe des eigenen Bildschirmes zur Ansicht und zur Bedienung durch die andere Seite
- Video-/Audiokonferenzen ohne weitere Infrastruktur
- Remote-Konfiguration (Provisioning)
- Direktverbindungen für die Mediendaten P2P über Interactive Connectivity Establishment und Universal Plug and Play (UPnP)

2.3 Merkmale

- Komplett webbasiert, daher Zugriff mit jedem Endgerät,
- Zugriff generell aus allen Netzen möglich,
- Vollständige Nutzung von Open-Source-Software,
- Anwendung ist zu 100 % quelloffen,
- Nutzung der an das Endgerät angebundenen Peripherie für die Kommunikation (z.B. Headsets) möglich

3 Betrieb und Monitoring

Grundsätzlich liegt die Betriebsverantwortung für den Betrieb der Services beim Auftragnehmer. Der Auftraggeber hat keinen administrativen Zugriff auf Server, Datenbanken, Fileservice.

3.1 Sicherheit

- Sicheres Austauschen von Nachrichten sowie das Starten von verschlüsselten Audio- und/oder Videositzungen.
- Benutzerverwaltung mit den Benutzergruppen User oder Administrator
- Anmeldung nur mit Benutzerkennung und Passwort
- Hierarchische Stufen für das Zugriffsrecht
- Protokollierung aller ändernden Zugriffe für den internen Datenschutzbeauftragten möglich
- Der Auftragnehmer stellt sicher, die vom BSI in den IT-Grundschutzkatalogen vorgegebenen A-, B- und C-Maßnahmen, die in den Zuständigkeitsbereich des Auftragnehmers fallen, einzuhalten.
- Die Maßnahmenermittlung und Umsetzung von Sicherheitsmaßnahmen erfolgt auf Basis der Bausteine der IT-Grundschutzkataloge in der beim Auftragnehmer eingesetzten Fassung und unter Einhaltung der für BSI-Zertifizierungen geltenden Übergangsfristen.
- Die für den betrachteten Informationsverbund maßgeblichen Sicherheitsmaßnahmen und der jeweilige Umsetzungsstand werden im Sicherheitskonzept dokumentiert. Sofern

zusätzliche Maßnahmen umgesetzt werden müssen, sind diese gesondert zu beauftragen.

Die Nutzung der Plattform macht organisatorische Regelungen notwendig:

a) Schutzbedarf: Es sollten keine Informationen mit erhöhtem Schutzbedarf über die Plattform ausgetauscht werden. Das Risiko für die (konforme) Nutzung obliegt dem Nutzer und sollte diesem durch den Auftraggeber transparent gemacht werden.

b) Jede Konferenz ist hinsichtlich der Teilnahme unberechtigter Dritter abzusichern. Dies erfolgt zum einen über ein Berechtigungskonzept, das vorsieht, dass nur vorab definierte Personen eine Konferenz eröffnen können. Diese berechtigten Personen müssen dazu verpflichtet werden, ein sicheres Passwort je Videokonferenz zu vergeben. Es muss den handelnden Personen bewusst sein, dass die Vertraulichkeit unmittelbar von der Vergabe eines sicheren Passwortes (und dessen sichere Übertragung an die Teilnehmer) abhängig ist.

c) Der Initiator einer Konferenz sollte auf die eingewählten Teilnehmer achten, die während der Konferenz angezeigt werden und bei unbekannten Teilnehmern nachfragen, wer sich dahinter verbirgt.

d) Es besteht das Risiko, dass Audio-/Videokonferenzen durch Teilnehmer aufgezeichnet werden.

e) Es besteht das Risiko, dass Teilnehmer durch Benutzung der Videofunktion innerhalb ihres Wohnumfeldes ungewollt/unbewusst Informationen preisgeben (z. B. durch Poster an der Wand). Darüber sollten die Teilnehmer vor Teilnahme informiert werden, ebenso über die "Blur"-Funktion, um den Hintergrund unscharf zu zeichnen.

f) Der Einwahlpunkt für die Teilnehmer sollte eindeutig spezifiziert sein, um falsche Einwahlen in möglicherweise öffentliche Videokonferenzräume zu verhindern.

3.2 Zugang

Die **dPhoenixSuite 2.0** ist über das Internet und ggf. über die Landesnetze sowie kommunalen Verwaltungsnetze verfügbar. **dOnlineZusammenarbeit 2.0** kann innerhalb der **dPhoenixSuite 2.0** als Modul aufgerufen werden. Zusätzlich kann es notwendig sein, für den Zugang für die Landesnetze sowie kommunalen Verwaltungsnetze separate Freischaltungen beim Dataport Policy Management einzureichen.

3.3 Netzkommunikation

Die Server des Gesamtsystems können nur untereinander kommunizieren.

3.4 Betriebszeiten

3.4.1 Onlineverfügbarkeit

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

3.4.2 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 das Call-Center des Auftragnehmers informiert.

3.4.3 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.

3.5 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:

	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 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.

3.6 Support

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

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

3.7 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.

3.8 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.
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	Viele Anwender sind betroffen.	Ersatz steht kurzfristig nicht zur Verfügung. Die	Priorität „Hoch“ führt zur bevorzugten Bearbeitung

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

(bisher 2)	Geschäftskritische Systeme sind betroffen. Die Geschäftstätigkeit kann eingeschränkt aufrechterhalten werden.	Tätigkeit, bei der der Incident auftrat, muss kurzfristig durchgeführt werden.	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

3.9 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 (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 erforderlich, die nachfolgend aufgelistet sind:

- Durchführung von Funktionstests

- Kostenübernahme bei mobiler Nutzung
- Bereitstellung von Netzzugängen (Internet)

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 (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 (Überwachter Betrieb) 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.