

## **Leistungsbeschreibung**

**Bereitstellung dOnlineZusammenarbeit 2.0  
(Messaging/Audio/Video)**

**Software as a Service (SaaS)**

## Inhaltsverzeichnis

---

<b>1</b>	<b>Einleitung</b> .....	<b>3</b>
1.1	Ausgangssituation.....	3
<b>2</b>	<b>Leistungsgegenstand</b> .....	<b>3</b>
2.1	Beschreibung .....	3
2.2	Funktionsumfang .....	3
2.3	Merkmale .....	4
<b>3</b>	<b>Betrieb und Monitoring</b> .....	<b>4</b>
3.1	Sicherheit .....	4
3.2	Zugang .....	5
3.3	Netzkommunikation .....	5
3.4	Betriebszeiten .....	5
3.4.1	Onlineverfügbarkeit.....	5
3.4.2	Servicezeit – Betreuter Betrieb .....	6
3.4.3	Betriebszeit – Überwachter Betrieb .....	6
3.5	Wartungsarbeiten.....	6
3.6	Support.....	6
3.7	Störungsannahme.....	7
3.8	Incident-Management .....	7
3.9	Rollendefinition .....	7
<b>4</b>	<b>Protokollierung</b> .....	<b>8</b>
<b>5</b>	<b>Mitwirkungsleistungen und Pflichten des Auftraggebenden</b> .....	<b>9</b>
<b>6</b>	<b>Erläuterungen</b> .....	<b>10</b>
6.1	Begriffsfestlegungen .....	10
6.2	Erläuterung VDBI .....	11

## 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 Nutzer\*innen 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 3.0** und seinen Modulen, darunter auch dOnlineZusammenarbeit 2.0, stellt Dataport einen cloudbasierten Web-Arbeitsplatz für den öffentlichen Sektor (Verwaltung, Schulen, Universitäten, Kultur, ...) als Service bereit. Zur Wahrung der digitalen Souveränität unserer Auftraggeber werden dabei Alternativen zu den marktbeherrschenden Produkten evaluiert.

## 2 Leistungsgegenstand

---

### 2.1 Beschreibung

**dOnlineZusammenarbeit 2.0** (Modul für Messaging/Audio/Video aus **dPhoenixSuite 3.0**) ist eine Lösung zur Kommunikation im Verwaltungs- und Bildungsumfeld. Sie ermöglicht es, vielen Nutzer\*innen, unkompliziert und ad hoc zu Online-Besprechungen zusammenzukommen.

- 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 unterstützten Plattformen einsetzbar.

### 2.2 Funktionsumfang

Das Produkt **dOnlineZusammenarbeit 2.0** wird durch Dataport (Auftragnehmer) für die Auftraggebenden 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-By-Hop-Protokolls 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. Die unterstützten Protokolle werden im Rahmen der Weiterentwicklung ausgebaut. In vielen Fällen ist auch Dateiübertragung möglich.

Folgende Funktionen stehen standardmäßig zur Verfügung:

- Desktop-Sharing – Freigabe des eigenen Bildschirms zur Ansicht 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

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

## 3 Betrieb und Monitoring

---

Grundsätzlich liegt die Betriebsverantwortung für den Betrieb der Services bei dem/der Auftragnehmer\*in. Der/die Auftraggeber\*in haben keinen administrativen Zugriff auf Server, Datenbanken, Fileservice.

### 3.1 Sicherheit

- Sicheres Austauschen von Nachrichten sowie das Starten von verschlüsselten Audio- und/oder Videositzungen.
- 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: Die Plattform ist nicht für den Austausch von Daten mit erhöhtem Schutzbedarf ausgelegt. Das Risiko für die (konforme) Nutzung obliegt den Nutzer\*innen und sollten diesen durch den/die Auftraggeber\*in 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\*innen) abhängig ist.
- c) Der Initiator einer Konferenz sollte auf die ausgewählten Teilnehmer\*innen achten, die während der Konferenz angezeigt werden und bei unbekanntem Teilnehmer\*innen nachfragen, wer sich dahinter verbirgt.
- d) Es besteht das Risiko, dass Audio-/Videokonferenzen durch Teilnehmer\*innen aufgezeichnet werden.
- e) Es besteht das Risiko, dass Teilnehmer\*innen durch Benutzung der Videofunktion innerhalb ihres Wohnumfeldes ungewollt/unbewusst Informationen preisgeben (z. B. durch Poster an der Wand). Darüber sollten die Teilnehmer\*innen vor Teilnahme informiert werden, ebenso über die "Blur"-Funktion, um den Hintergrund unscharf zu zeichnen.
- f) Der Einwahlpunkt für die Teilnehmer\*innen sollte eindeutig spezifiziert sein, um falsche Einwahlen in möglicherweise öffentliche Videokonferenzräume zu verhindern.

## **3.2 Zugang**

Die **dOnlineZusammenarbeit 2.0** ist über das Internet und ggf. über die Landesnetze sowie kommunalen Verwaltungsnetze verfügbar. 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<sup>1</sup>

- \_ 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 des Auftragnehmers. Es stehen Ansprechpartner\*innen mit systemtechnischen Kenntnissen für den Betrieb und zur Störungsbehebung zur Verfügung. Im Problem- und Störfall 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 Anwender\*innen grundsätzlich zur Verfügung.

Die zentrale Infrastruktur wird automatisiert überwacht. Festgestellte Fehler werden automatisch in einem Trouble-Ticket-System hinterlegt. Ansprechpartner\*innen 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.

<sup>1</sup> Gilt nicht für gesetzliche Feiertage des Landes Schleswig-Holstein sowie 24.12. und 31.12.

### 3.7 Störungsannahme<sup>2</sup>

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

**Die Rufnummern lauten 040 428461904 und 0421 361 4444 [Trägerland Bremen].**

Im Rahmen der Störungsannahme werden grundsätzlich Melderdaten sowie die Störungsbeschreibung erfasst und ausschließlich für die Störungsbehebung gespeichert. Der Störungsabschluss wird der meldenden Person 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/die Auftraggeber\*in oder den/der Nutzer\*in zu verantworten sind (z.B. Warten auf Zusatzinformationen durch den/die Nutzer\*in, Unterbrechung auf Wunsch des/der Nutzer\*in etc.).

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
Auftraggebender (AG)	Rolle des Auftraggebers im Sinne der DSGVO
Auftragsverarbeitende (AV)	Zentraler Betrieb, Auftragsverarbeitende im Sinne der DSGVO
Auftragsberechtigte (AB)	Abruf von im Vertrag definierten Services des Auftragsverarbeitenden Der Abruf erfolgt durch die von den Auftraggeber*innen benannte autorisierte Auftragsberechtigten. Der/die Auftraggeber*in benennt diese Personen und pflegt die Liste der autorisierten Auftragsberechtigten.
Nutzer	Nutzer*innen sind alle Endanwender*innen, die das Verfahren nutzen. Nutzer*innen müssen nicht Mitarbeiter*innen des Auftraggebers sein.

<sup>2</sup> Gilt nicht für gesetzliche Feiertage des Landes Schleswig-Holstein sowie 24.12. und 31.12.

## 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 Löschrufen sind:

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

## 5 Mitwirkungsleistungen und Pflichten des Auftraggebenden

---

Es sind Mitwirkungs- und Bereitstellungsleistungen der Auftraggebenden erforderlich, die nachfolgend aufgelistet sind:

- Durchführung eines Abnahmetests
- Kostenübernahme bei mobiler Nutzung
- Bereitstellung von Netzzugängen (Internet)

Die Auftragnehmenden weisen darauf hin, dass das BSI die Erstellung einer Sicherheitsrichtlinie für Cloud-Nutzer\*innen durch den Auftraggebenden empfiehlt.

Zusätzlich gelten für den Auftraggebenden folgende Pflichten:

- Der Auftraggebende prüft, eigenverantwortlich, die Einhaltung aller im Zusammenhang mit der Nutzung der Leistung relevanten und anwendbaren rechtlichen Vorschriften, Gesetze und Verordnungen und stellt deren Einhaltung sicher.
- Die Auftraggebenden benennen einen Ansprechpartner\*in 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 (Überwacher Betrieb)	Die Betriebszeit (Überwacher 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 Auftraggebenden nutzbar sind.  Sollte in Sonderfällen ein größeres oder weiteres Wartungszeitfenster beansprucht werden, so erfolgt dies in direkter Absprache mit dem Auftraggebenden. Die Auftraggebenden werden nur in begründeten Fällen die Durchführung von Wartungsmaßnahmen einschränken. Die Auftragnehmer werden in diesen Fällen unverzüglich über sich ggf. daraus ergebenden Mehraufwand und Folgen informiert.
Reaktionszeit	Die Reaktionszeit ist die Zeitspanne innerhalb der vereinbarten Servicezeiten zwischen der Feststellung einer Störung durch den Dienstleister bzw. Meldung einer Störung durch den Auftraggebenden 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

<b>V</b> = Verantwortlich	„V“ bezeichnet denjenigen, der für den Gesamtprozess verantwortlich ist. „V“ ist dafür verantwortlich, dass „D“ die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
<b>D</b> = Durchführung	„D“ bezeichnet denjenigen, der für die technische Durchführung verantwortlich ist.
<b>B</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.
<b>I</b> = Information	„I“ bedeutet, dass die Partei über die Durchführung und/oder die Ergebnisse des Prozessschritts zu informieren ist. „I“ ist rein passiv.