Specification of services

Provision of dOnlineZusammenarbeit 2.0 (messaging/audio/video)

Software as a Service (SaaS)

Content

1 Introduction

The document determines the scope of services to be provided and describes ***dOnlineZusammenarbeit 2.0****.*

1.1 Starting point

The requirements of collaborative work have changed: working from home and mobile work have become more commonplace, partly due to the COVID 19 pandemic. Due to the Covid crisis, the need for quickly scalable video conferences and online collaboration solutions have become very important – also for maintaining the working capacity of the public administration in the German federal states.

Dataport has done everything it can to be able to swiftly offer a solution to a large number of users. This involved creating virtual classrooms and digital lessons for schools and securing virtual conference rooms for administrative purposes.

With **dPhoenixSuite 3.0** and its modules – including dOnlineZusammenarbeit 2.0, Dataport now provides a cloud-based web workspace for the public sector [administration, schools, universities, culture, ...]. It is designed as a service. In order to maintain the digital sovereignty of our clients, Dataport is evaluating alternatives to the leading products on the market.

2 Product

2.1 Description

dOnlineZusammenarbeit 2.0 (module for messaging/audio/video from **dPhoenixSuite 3.0**) is a solution for communicating in the administrative and educational environment. It enables many users to come together for online meetings in a straightforward and ad hoc manner.

- Dataport offers an audio/video conference solution from the secure environment of its own datacentre with additional services from partner datacentres in Germany.
- The solution can be used for working from home and from other locations, e.g. in the administrative environment or for digital teaching.
- To take part, no installations are required on the terminals used.
- The solution is also suitable for low data transmission rates and can be used on supported platforms.

2.2 Range of functions

The product **dOnlineZusammenarbeit 2.0** is provided by Dataport (contractor) for the client. It allows users to conduct digitally sovereign audio and video conferences. To this end, the open-source software Jitsi is used. Jitsi offers a secure and encrypted audio and video conference by using a hop-by-hop protocol from Dataport's secure datacentre or datacentres commissioned by Dataport in Germany.

dOnlineZusammenarbeit 2.0 supports presence and instant messaging across all protocols. All common protocols of popular instant messengers are supported. As the service develops further, the supported protocols will be expanded. Often, file transfer is also possible.

The following functions are available as standard:

- Desktop sharing – sharing your own screen so it can be viewed by other participants
- Video/audio conferences without additional infrastructure
- Remote configuration (provisioning)
- Direct connections for media data P2P via Interactive Connectivity Establishment (ICE) and Universal Plug and Play (UPnP)

2.3 Features

- Completely web-based,
- Access generally possible from all networks,
- Full use of open-source software,
- Application is 100 % open source,
- Use of peripherals connected to the terminal (e.g. headsets) is supported

3 Operation and monitoring

As a rule, the operational responsibility for the operation of the services lies with the contractor. The client has no administrative access to servers, databases or file services.

3.1 Security

- Securely exchange messages and start encrypted audio and / or video sessions.
- Registration only with user ID and password
- Hierarchical levels for the right of access
- Logging of all data concerning changes made can be made available to the internal data protection officer
- The contractor ensures compliance with the A, B and C measures specified by the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) in the IT baseline security catalogues.
- The determination of measures and the implementation of security measures are based on the modules of the IT baseline security catalogues in the version used by the contractor and in compliance with the transitional periods that apply to BSI certifications.
- The security measures relevant to the information network and the respective implementation status are documented in the security concept. If additional measures have to be implemented, these must be ordered separately.

The use of the platform requires organisational regulations:

a) Protection requirements: The platform is not designed for the exchange of data that requires increased protection. The risk for the (compliant) use is the responsibility of the

users – the client should explain this.

b) Each conference must be secured against the participation of unauthorised third parties. One way to ensure this is via an authorisation concept that allows only pre-defined people to start a conference. These authorised persons must choose a secure password for each video conference. The persons involved must be aware that confidentiality is key to keeping the password secure (and that a secure transmission of the password to the participants is also vital).

c) The host of a conference should pay attention to the dialled-in participants of his or her event and ask unknown participants who they are.

d) There is a risk that audio/video conferences will be recorded by participants.

e) There is a risk that participants will unintentionally / unknowingly disclose personal information about their living environment by using the video function (e.g. through posters on the wall). The participants should be informed about this before participating, as well as about the “blur” function that blurs the background.

f) The host should clearly specify the dial-in point for the participants to prevent incorrect dial-ins into possibly public video conference rooms.

3.2 Access

d**OnlineZusammenarbeit 2.0** is available via the internet and, where applicable, via the networks of the German federal states and municipal administrations. For access via state networks and municipal administration networks, it may be necessary to submit separate activation requests to Dataport Policy Management.

3.3 Network communication

The servers of the overall system can only communicate with each other.

3.4 Operating hours

3.4.1 Online availability

The central infrastructure is available 24/7 (availability 95 %) – except in certain circumstances (e.g. maintenance window, urgent installation of security updates).

3.4.2 Service times – supervised operation[1]

- Monday to Thursday 08.00 am to 05.00 pm
- Friday 08.00 am to 03.00 pm

During these times, the systems are monitored and supervised by the contractor's administrators. Contact persons with knowledge of the systems technology are available for consultation and troubleshooting. Should a problem or fault arise, an expert in the matter in hand will be informed via the contractor's call centre.

3.4.3 Operating hours – monitored operation

- All times outside of the supervised operation

Generally, the systems are also available to users outside of the times when operation is supervised.

The central infrastructure is monitored automatically. Any faults that have been detected are automatically stored in a trouble ticket system. Contact persons are not available during the hours of monitored operation.

3.5 Maintenance work

As a rule, the regular, periodically recurring maintenance and installation work is carried out outside the hours of supervised operation. Currently, a maintenance window is defined as follows:

Window Typ	Period
Standard maintenance window	Tuesday 07:00 pm to Wednesday 06:00 am
Special maintenance windows	In exceptional cases (e.g. if a more substantial installation is required), this work will be carried out over a weekend (those affected are informed about the measure at least 2 weeks in advance).
Maintenance window data backup	Daily between midnight and 06:00 am

During these times, maintenance work is carried out and work may only be possible to a limited extent.

3.6 Support

The contractor provides the support for the infrastructure and all associated components. The contractor is entitled to use subcontractors to provide this service.

[1] Does not apply on bank holidays in the state of Schleswig-Holstein and on 24 December and 31 December.

3.7 Malfunction helpdesk[2]

Malfunctions should be reported by persons authorised to do so – either by phoning the call centre or contacting the contractor's user help desk.

The telephone numbers are 040 428461904 and 0421 361 4444 [provider state Bremen].

As part of the process, data concerning the malfunction and a description of the fault are recorded and stored exclusively for troubleshooting purposes. The person who reported the malfunction will be informed once it has been remedied.

3.8 Incident management

Malfunctions are recorded as so-called incidents in the central trouble ticket system (TTS). Each incident and its processing history are documented in the TTS.

Incidents are generally not dealt with outside the times of supervised operation and may be suspended until supervised operation resumes. Likewise, the processing of incidents may be interrupted by force majeure or by events for which the clients or the users are responsible (e.g. waiting for additional information from the user, interruption at the request of the user etc.).

In case of incidents, the following response times apply (depending on incident priority and only during support times):

Priority	Response time
Low (previously 4)	4 hours
Medium (previously 3)	2 hours
High (previously 2)	1 hour
Critical (previously 1)	0.5 hours

3.9 Role definition

Roles and the tasks people fulfil in those roles are defined as follows:

Role	Role definition
Client (Auftraggebender, AG)	Role of the client within the meaning of the GDPR
Data processor (*Auftragsverarbeitende*, AV)	Central operations, role of data processor within the meaning of the GDPR
Authorised person (*Auftragsberechtigte*, AB)	Access to the services of the data processor as defined in the contract. Access is granted to authorised persons named by the client. The client appoints these authorised persons and maintains a list of said persons.
User	Users are all end users who use the system. Users do not necessarily have to be employees of the client.

[2] Does not apply on bank holidays in the state of Schleswig-Holstein and on 24 December and 31 December

4 Logging

Logging takes place within the infrastructure of systems.

There is no regular evaluation. Evaluations only take place when necessary, e.g. in case of a suspected security risk. Standard retention periods are:

Type	Content	Retention period, period after which data is deleted
Infrastructure logging (admin platform, cloud manager)	technical, personal client	12 months, 12 months
System logging (operating system, basic software)	technical	1 month, 1 month
Audit logging (operating system)	technical, personal	12 months, 12 months
Application logging (Phoenix software stack)	technical, personal, client	3 months, 3 months
Logging of user actions (detailed information)	technical, personal client	10 days, 10 days
User information (aggregated reporting information)	personal, client	2 years, 2 years
Logging of connection data (detailed information)	technical, personal, client	10 days, 10 days
Billing information (aggregated billing information)	personal, client	2 years, 2 years

5 Contributions and duties of the client

See below for the contribution and provision services the client needs to provide:

- Performing an acceptance test
- Bearing the costs for mobile use
- Providing web access (internet)

The contractor would like to point out that the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) recommends that the client compile a security guideline for cloud users.

The client also has the following duties:

- The client is responsible for checking and ensuring compliance with all relevant and applicable legal provisions, laws and ordinances in connection with the use of the service.
- The client shall nominate a contact person and a deputy contact person.

6 Explanatory notes

6.1 Terms

Operating mode	Definition of the term
Online availability	Online availability describes periods of time in which defined basic services are available and monitored automatically.
Service times (supervised operation)	The term service time or (supervised operation) describes the periods in which the resources, functions and modules (basic services) are operated by the contractor and faults and inquiries are processed.
Operating hours (monitored operation)	The operating hours (monitored operation) are periods in which the agreed servers, resources, functions and modules (basic services) are made available and monitored automatically by the contractor.
Maintenance window	Regular time slot for maintenance work on the systems, during which the client cannot use the systems, or they can only be used to a limited extent. If, in exceptional cases, a larger or additional maintenance window is required, the client will be consulted. The client shall only restrict the implementation of maintenance measures if this can be justified. In such cases, the contractor shall inform the client immediately of any resultant additional work and consequences.
Response time	The response time is the period of time, within the agreed service times, between the detection of a fault by the service provider or the reporting of a fault by the client via the agreed channel (service desk) and the start of troubleshooting. The response time begins with the recording of the fault in the contractor's ticket system.

6.2 What does VDBI stand for?

Responsible (*Verantwortlich*, **V**)	“V” denotes the person responsible for the overall process. “V” is responsible for ensuring that “D” successfully carries out the implementation of the process step.
Implementation (*Durchführung*, **D**)	“D” designates the person responsible for the technical implementation.
Consultation (*Beratung*, **B**)	“B” means that the parties involved need to be consulted and that they can, for instance, define specifications for implementation parameters or voice reservations. “B” thus designates a right to participate or a duty to cooperate.
Information (*Information*, **I**)	“I” means that the parties need to be informed about the implementation and / or the results of the process step. “I” is purely passive.