Specification of services

Provision of dPhoenixSuite 3.0 APP environment

Software as a Service (SaaS)

Content

1 Introduction

With dPhoenixSuite 3.0, Dataport provides customers with a software solution as a service [SaaS] with various function modules.

All modules are based on open-source solutions and are managed and operated by Dataport.

Dataport can change each function module, either in whole or in part, as long as the guaranteed properties are not affected.

1.1. Description of the APP environment

Dataport's own environment [called PX environment] consists of two largely identical environments: the PROD [production] and the APP [approval] environment. Interested customers can get to know and test the software in the latter environment.

The APP environment is identical to the PROD environment. The administration of the APP environment is carried out by the Phoenix programme quality assurance.

Data associated with an account [emails, Office documents etc.] is generally only visible and accessible through this one account. After the setup and activation phases, the environment can be used productively as part of your testing period.

Exceptions are:

_ Users can view other users in the shape of their first and last name as well as their profile picture [where available].

_ Users can share files and data with each other.

1.2. Differences between the APP and PROD environment with regard to "normal" safety requirements

The aim is to test developments and updates together with the customer, thereby ensuring a constant optimisation process. Once tried and tested, the updates are then rolled out for active use in the PROD environment. The operating processes of the APP environment largely correspond to those of the PROD environment – with the following exceptions and restrictions:

_ Just like in the production environment, all data is secured in accordance with the basic safety requirements and is therefore not accessible to unauthorised persons without the active approval of the user. However, in the APP environment, the data for each customer is not physically separated from one another. A user can make data available to a user from another organisation who also has an account in this environment, should they wish to do so.

_ User management is the responsibility of Dataport. Users can only sign up, have their account deleted or changed through Dataport. Users cannot make entries independently. This way, Dataport retains control over the accesses that have been created.

_ Maintenance windows for the environment are fixed and cannot be changed per customer. It is therefore not possible to respond to the individual requirements of individual organisations.

_ Data backup and recovery is performed for the complete approval environment, not per customer. It is therefore not possible to respond to specific requirements of individual organisations [customers].

_ The “branding” of the APP environment is pre-set. It is not possible to respond to specific requirements of individual organisations [customers].

_ Users cannot use their professional email address or an email address linked to their organisation but must use the predefined domain “@app.px.dphoenixsuite.de”. Thus, the email domain does not correspond to the email address “normally” used.

NORMAL security requirements are determined in the same way as in the PROD environment. There are no plans for a separate security concept for the approval environment. As per the German Federal Office for Information Security [BSI], the implementation is documented and regularly checked in accordance with the IT structure analysis for the PROD environment.

1.3. Organisational measures that minimise threats and security needs

_ Creating the accounts with a special prefix for the usernames [[organisation.]firstname.lastname]:

In dPhoenixSuite, a convenience function that displays a suggested list of existing accounts in the APP environment is used in various places. For example, if a file is to be shared for editing with another user, the system will suggest possible user accounts as you enter the first few letters. This list is generated from the first few letters of the username people use to log in.

By using a prefix that is unique to your own organisation, the list will be made up exclusively of accounts from your own organisation so that the risk of accidentally sharing files with outsiders is greatly reduced.

A separate request needs to be made if you want to create users with a prefix. The default setting is without a prefix.

_ All users should be made aware of the risks of accidentally sharing data.

_ All users should be made aware of the risks of data loss, for example through accidental permanent deletion.

_ All users should be told that when testing the APP environment, they should not use data that requires higher security levels.

1.4. Residual risk

Individual recovery of backed up data cannot be performed in the APP environment. Only a backup of the entire environment can be performed. In addition, data that has, for instance, been accidentally shared by users may be viewed and possibly changed by users from other organisations.

2 Product

2.1. Range of functions

With dPhoenixSuite 3.0, Dataport 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 offering alternatives to the leading products on the market.

2.1.1. dPhoenixPortal module [web front end]

With dPhoenixSuite 3.0, the end user is provided with a central portal [dPhoenixPortal] as a web application. This allows the user to access all modules he or she has ordered. The link, through which access is provided, is communicated separately to the client. Application documentation for every function module and FAQs for the end user are also provided in the portal. In addition, the portal offers the following options for self-administration:

_ End users can edit meta information about their own identity

_ End users can change and reset their password

2.1.2. Identity and access management [user management / IAM]

dPhoenixSuite 3.0 provides a directory service [IAM] for the central user administration:

_ Cross-module single sign-on

_ User self-service: users may change their personal attributes

2.1.3. dPhoenixOffice module

dPhoenixOffice provides cloud storage space for editing, versioning and file-sharing via dPhoenixFileShare. Every user receives a storage space for files. This can be accessed via the browser.

To gain access, the user needs an internet connection. The user can store files in his or her storage space and organise them in folders. Both files and folders can be shared with other users. Access to files and folders can be granted for a limited period of time or indefinitely and / or can be protected by a password. The stored files are protected from accidental modification or deletion thanks to versioning and a recycle bin. If files are changed, old versions of the file are kept on hand and can be restored by the user if necessary. Likewise, deleted files are first moved to a recycle bin from where they can be retrieved by the user, should this become necessary. Versions and deleted files are retained for 30 days and then automatically deleted. The versions and the recycle bin count towards the user's storage allocation.

In the dPhoenixOffice module, users can create files from the dPhoenixFileShare module in a web office function and edit them online. Both real-time collaboration with multiple users and individual editing of documents is supported.

Anyone with write access to the respective file may edit it. Features include word processing, compiling spreadsheets and creating presentations. It is possible to download files and export them to other formats.

The following file types are supported:

_ PowerPoint presentations [pptx, potx]

_ Excel spreadsheets [xlsx, xlst, csv]

_ Word files [docx, dotx]

_ OpenDocument texts [odt, ott]

_ OpenDocument charts [ods, ots]

_ OpenDocument presentations [odp]

_ Markdown documentation files [md]

_ Plain text files [txt]

_ Rich Text Format files [rtf]

_ HTML

_ OpenDocument graphics [odg]

_ The following file types can be opened for reading:

_ Common image formats [e.g. JPG, PNG and GIF]

_ Common video formats [e.g. MP4, MOV and WebM]

_ PDF, PDF/A

2.1.4. dPhoenixMail module [groupware / email, calendar, contacts]

With the dPhoenixMail module, dPhoenixSuite 3.0 provides a full-featured email service. This includes the usual functions of email communication, drag & drop, file-sharing and collaborative editing of files as well as standard functions of an email client. With a groupware account, each user receives a personal mailbox, access to the central address book, a personal calendar and the task function. dPhoenixMail can only be accessed via a browser.

The following functions are available:

_ Importing, creating and managing personal contact lists

_ Sharing contact lists with users of your own organisation

_ Creating, managing and sharing personal email distribution lists

_ Importing, creating, managing and sharing own and / or external calendars [e.g. bank holidays, holidays]

_ Sharing folders or mailboxes with users from your own organisation

_ Creating, editing, assigning and status tracking of tasks

2.1.5. dOnlineZusammenarbeit 2.0 module [messaging, audio, video]

The dOnlineZusammenarbeit 2.0 module is a platform for digital collaboration. It includes, among other things, a video and audio conference solution, a chat function, the option of sharing screen content, such as presentations, exchanging files or working together on a whiteboard. dOnlineZusammenarbeit 2.0 can only be accessed via a browser.

2.1.6. Data storage and backup

The infrastructure components are designed redundantly to prevent downtimes due to hardware failure. The stored data is backed up daily. These backups are for system recovery only.

_ Consistent backup of the entire system [all modules; at least once a day]

_ Maximum data loss: 24 hours

_ Maximum data recovery time: 24 hours

_ Retention period of versioned files saved on dPhoenixOffice: 30 days

3 Operation and monitoring

3.1. Security

Thanks to sophisticated technical and organisational measures, the contractor [Dataport] is able to guarantee a safe operation of the entire system. The contractor is responsible for the update and patch management of the infrastructure components. This also applies to any subcontractors used.

Tasks and responsibilities	Contractor	Clients
Operation of the infrastructure	V, D, B	I
Safe operation of the entire system after deployment incl. installation of patches and updates	V, D, B	I
Planning and implementation of system-specific maintenance work on the infrastructure	V, D	I

3.2. Virus protection

The contractor guarantees virus protection for the entire system provided.

Tasks and responsibilities	Contractor	Clients
Operation and support of the virus protection for the infrastructure	V, D, B	I

The servers within the overall system are subject to monitoring [event, trend and log monitoring].

3.3. Access

dPhoenixSuite 3.0 is available over the internet. All modules and functions can be accessed and used via dPhoenixSuite 3.0. For access via state networks and municipal administration networks, it may be necessary to submit separate activation requests to Dataport Policy Management.

3.4. Network communication

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

3.5. Encryption

A transport route encryption in accordance with the latest security standards is used.

3.6. Deleting data

Should the contract be terminated, the client is responsible for backing up his or her data and storing it elsewhere before the end of the contract.

Irrespective of the reason for the termination and of who initiated it, the contractor will delete all of the client's data, including any remaining data backups, no later than 30 days after the end of the contract.

Recovering data after this deletion is impossible. Excluded from the deletion is data that is required by the contractor for billing purposes beyond this period or any data subject to a statutory obligation to preserve records.

3.7. Operating hours

3.7.1. Version and function updates

The contractors will inform the clients about changes in the systems within seven to fourteen days. This does not apply to security updates.

3.7.2. Online availability

The central infrastructure is available 24/7 [availability 95 %] – except for see Chapter 3.9 Maintenance work [e.g. maintenance window, urgent installation of security updates].

3.7.3. Service times – supervised operation

_ 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 user help desk [UHD].

3.7.4. 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.

Contact persons are not available during the hours of monitored operation.

3.8. 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:

Maintenance window	Period
Standard	Tuesday 07.00 pm to Wednesday 06.00 am
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.

3.9. Support

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

3.10. Malfunction helpdesk

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:

_ 040 428 46 1904

_ 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.

3.11. 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.].

Incident processing takes place in accordance with the following priority guidelines:

Priority	Effect	Urgency	Processing
Low [previously 4]	Incident affects individual users. Business operations are not hampered.	A replacement is available and can be used or the affected system does not currently need to be used. Activities that would be hampered by the incident can be performed later.	The designation “Low Priority” leads to processing by the contractor, and the solution progress is monitored. The response time [start of processing or qualified call-back] depends on the service class.
Medium [previously 3]	Few users are affected by the incident. Systems critical for business are not affected. Business operations can continue with minor restrictions.	Not all users affected can get replacements. The activity during which the incident occurred can be carried out later or in another way, possibly with more effort.	The designation “Medium Priority” leads to processing by the contractor, and the solution progress is monitored. The response time [start of processing or qualified call-back] depends on the service class.
High [previously 2]	Many users are affected. Systems critical for business are affected. Business operations can continue with certain restrictions.	There is no short-term replacement available. The activity during which the incident occurred needs to be suspended for a short time.	The designation “High Priority” leads to processing by the contractor, and the solution progress is closely monitored. The response time [start of processing or qualified call-back] depends on the service class.
Critical [previously 1]	Many users are affected. Systems critical for business are affected. Business operations cannot continue.	There is no replacement available. The activity during which the incident occurred needs to be suspended and cannot be performed in another way.	The designation “Critical Priority” leads to processing by the contractor, and the solution progress is monitored extremely closely. The response time [start of processing or qualified call-back] depends on the service class.

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

3.12. Role definition

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

Role	Role definition
Clients [Auftraggeber*innen, AG]	Role of the clients within the meaning of the GDPR
Data processors [Auftragsverabeiter*innen, AV]	Central operations, role of data processors within the meaning of the GDPR
Authorised persons [Auftragsberechtigte, AB]	Access to the services of the data processors 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.
Users	Users are all end users who use the system. Users do not have to be employees of the client.

4 Logging

Logging takes place within the IT infrastructure of dPhoenixSuite.

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

_ Carrying out release tests, i.e. testing the system for usability based on the specified requirements.

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 “support time [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 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.
Storage quota	This is the limitation of storage space on a data repository for a single user or a group of users. The aim of limiting storage space usage is to ensure that all users can make the best possible use of the available system resources.

6.2. What does VDBI stand for?

Term	Explanation
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.