Preisblatt dPhoenixSuite 2.0
(öffentlich-rechtliche Einrichtungen)

Für die vereinbarten Leistungen zahlt der Auftraggeber folgende aufwandsbezogenen Preise:

1 Dienstleistungen

Artikelbezeichnung	Menge	Mengen-einheit	Einzelpreis
Einführungsworkshop	1	**Stück**	**800,00 €**
Schulung Anwendende / Administrierende	1	**Stunde**	**98,00 €**
Administrationssupport für Technik / Software	1	**Stunde**	**98,00 €**

2 Software (monatlich)

Benötigte User:

Artikelbezeichnung	Menge	Mengen-einheit	Einzelpreis
dPhoenixSuite 2.0 inkl. 1GB/User Speicherpaket	1	**User**	**20,00 €**

Erweiterung Speicherpaket auf:*

Artikelbezeichnung	Menge	Mengen-einheit	Einzelpreis
3 GB/User	1	**Paket**	**2,50 €**

* Es ist nur das benannte Speicherpaket buchbar, keine Zwischengrößen.

Die Abrechnung der bestellten Benutzerlizenzen und des gebuchten Speicherpaketes erfolgt auf der Grundlage der im laufenden Monat gebuchten höchsten Anzahl an Usern und des größten Speicherpaketes.

Die Abrechnung erfolgt nach Aufwand.

Die Rechnungsstellung erfolgt kalendermonatlich nachträglich.

3 Einmalige Einrichtung

Artikelbezeichnung	Menge	Mengen-einheit	Einzelpreis
dPhoenixSuite 2.0 – Einrichtung	1	**Stück**	**980,00 €**

Die Rechnungsstellung des einmaligen Festpreises erfolgt nach erbrachter Leistung.

Die genannten Entgelte sind Nettopreise. Für jede weitere Beauftragung gilt das jeweils gültige auf www.dPhoenixSuite.de veröffentlichte Preisblatt.

10.09.2021

Inhaltsverzeichnis

1 Kündigung

Der Vertrag ist kündbar mit einer Frist von 2 Wochen zum Monatsende.

2 Rechnungstellung

Die Rechnungstellung erfolgt gemäß Preisblatt.

3 Umsatzsteuer

3.1 Umsatzsteuer für Leistungen, die bis zum 31.12.2022 erbracht werden

Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen in Ansehung ihrer Art, des Zwecks und der Person des Auftraggebers zum Zeitpunkt des Vertragsschlusses nicht der Umsatzsteuer. Sollte sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde eine Umsatzsteuerpflicht ergeben und der Auftragnehmer insoweit durch eine Steuerbehörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, gegebenenfalls auch rückwirkend.

3.2 Umsatzsteuer für Leistungen, die ab dem 01.01.2023 erbracht werden

Die aus diesem Vertrag seitens des Auftragnehmers zu erbringenden Leistungen unterliegen ab dem 01. Januar 2023 der Umsatzsteuer, soweit sie nicht aufgrund einer gesetzlichen Bestimmung (Bsp. § 20 Abs. 3 FVG oder § 126 GBO) nur von juristischen Personen des öffentlichen Rechts erbracht werden dürfen (§ 2b Abs. 3 Nr. 1 UStG).

Der Auftragnehmer hat die Option gem. § 27 Abs. 22 UStG zur Anwendung des § 2b UStG genutzt, so dass die Anwendung des bisherigen Rechts (§ 2 Abs. 3 in der am 31. Dezember 2015 geltenden Fassung) zum 31. Dezember 2022 ausläuft. Der Auftragnehmer wird die Umsatzsteuer für alle Leistungen ausweisen, für die keine gesetzliche Grundlage der Nichtsteuerbarkeit ab dem 01. Januar 2023 vorliegt.

Sollte der Auftragnehmer Leistungen ohne Umsatzsteuer ausgewiesen haben und sich durch Änderungen tatsächlicher oder rechtlicher Art oder durch Festsetzung durch eine Steuerbehörde dennoch eine Umsatzsteuerpflicht ergeben und der Auftragnehmer insoweit durch eine Steuerbehörde in Anspruch genommen werden, hat der Auftraggeber dem Auftragnehmer die gezahlte Umsatzsteuer in voller Höhe zu erstatten, gegebenenfalls auch rückwirkend.

4 Auftragsverarbeitung

Es gelten die Besonderen Vertragsbedingungen zur Verarbeitung personenbezogener Daten im Auftrag für das Produkt dPhoenixSuite 2.0 von Dataport.

5 Mitgeltende Regelungen

Es gelten die Allgemeinen Vertragsbedingungen Teil I von Dataport.

6 Haftungsbeschränkung

Die Haftung der Vertragsparteien pro Vertrag ist, gleich aus welchem Rechtsgrunde, auf insgesamt 10 % des jährlichen Leistungsentgeltes beschränkt. Ist die Laufzeit oder Mindestlaufzeit kürzer, so ist das auf diesen Zeitraum entfallende Leistungsentgelt maßgeblich. Die vorstehenden Beschränkungen gelten nicht bei Vorsatz, grober Fahrlässigkeit, bei der Verletzung des Lebens, des Körpers, der Gesundheit oder soweit das Produkthaftungsgesetz zur Anwendung kommt.

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-	Auftrag-
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-	Auftrag-
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.

Besondere Vertragsbedingungen zur Verarbeitung personenbezogener Daten im Auftrag für das Produkt dPhoenixSuite 2.0

1 Definitionen

In diesen Vertragsbedingungen werden bezeichnet als

Auftraggeber: Der im Vertrag als Auftraggeber Genannte.

Vertrag; Auftrag: Der zwischen dem Auftraggeber und Dataport geschlossene Vertrag zur Bereitstellung (Einräumung der Nutzung, Verfahrensbetrieb, Support) des Produktes dPhoenixSuite 2.0 und der damit verbundenen Verarbeitung personenbezogener Daten einschließlich der im Vertrag in Bezug genommenen oder diesem beigefügten Anlagen.

Verarbeitungstätigkeit; Produkt
Das Produkt dPhoenixSuite 2.0 nach Maßgabe der jeweils gültigen Produkt- bzw. Leistungsbeschreibung einschließlich der Nebenleistungen (z. B. Support).

Kundendaten
Die von Dataport auf der Grundlage und nach Maßgabe des Vertrages im Auftrag verarbeiteten Daten, einschließlich Text-, Ton-, Video- oder Bilddateien, darunter personenbezogene Daten oder besondere personenbezogene Daten, welche anlässlich oder durch die Nutzung des Produkts durch den Auftraggeber als Verantwortlicher oder durch weitere Verantwortliche, denen der Auftraggeber die Nutzung des Produktes ermöglicht, zur Verfügung gestellt werden, und für welche der Auftraggeber Auftragsverarbeiter ist.

Weitere Auftragsverarbeiter: Nachunternehmer bzw. Dienstleister von Dataport, derer sich Dataport bei der Auftragsverarbeitung als weitere Auftragsverarbeiter bedient.

Sonstige Begriffe

Für die verwendeten Begriffe personenbezogene Daten, besondere personenbezogene Daten, Verantwortlicher, Auftragsverarbeiter, weiterer Auftragsverarbeiter gelten die Definitionen der DSGVO.

2 Geltungsbereich und Geltungsvorrang dieser besonderen Vertragsbedingungen

2.1 Diese besonderen Vertragsbedingungen sind Bestandteil des Vertrages. Sie gelten für jede Auftragsverarbeitung von Kundendaten durch Dataport im Rahmen des Produktes dPhoenixSuite 2.0, soweit es sich um personenbezogene Daten handelt.

2.2 Im Falle eines Konfliktes oder Widerspruches gehen diese besonderen Vertragsbedingungen den Bestimmungen des Vertrages, den AVB von Dataport und den Regelungen sonstiger Vertragsbestandteile vor.

2.3 Ermöglicht der Auftraggeber auf Basis des mit Dataport abgeschlossenen Vertrages Dritten, welche ihrerseits Verantwortliche sind, die Nutzung des Produktes, stellt der Auftraggeber durch vertragliche Regelung oder durch ein anderes, geeignetes Rechtsinstrument sicher, dass die sich aus diesen Besonderen Vertragsbedingungen für den Verantwortlichen ergebende Rechte und Pflichten auf die Dritten übertragen werden.

3 Gegenstand und Dauer der Auftragsverarbeitung

Die Angaben zum Vertragsgegenstand, insbesondere zu Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und den Kategorien betroffener Personen sowie zur Dauer der Verarbeitung sind im Vertrag bzw. dessen weiteren Anlagen enthalten.

4 Verantwortung des Auftraggebers

4.1 Der Auftraggeber ist bezüglich der Verarbeitung der Kundendaten für die Einhaltung der gesetzlichen Datenschutzbestimmungen verantwortlich. Er ist insbesondere verantwortlich für

a) die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten, mit deren Verarbeitung er Dataport beauftragt,
b) die Angabe von für die Verarbeitung im Auftrag maßgeblichen Datenschutzanforderungen, soweit sich diese nicht aus der Verordnung (EU) 2016/679 (DSGVO) ergeben,
c) die Einholung und Dokumentation von Einwilligungserklärungen, sofern die Verarbeitung auf der Grundlage einer Einwilligung erfolgt, sowie für die Dokumentation von Widerrufserklärungen und die Umsetzung der im Falle eines Widerrufs erforderlichen Maßnahmen,
d) die Feststellung des Schutzbedarfes der im Auftrag zu verarbeitenden Daten,
e) die Prüfung, ob eine Datenschutz-Folgeabschätzung durchzuführen ist, und falls ja, für die Durchführung derselben,
f) Test und Freigabe des Produktes für den Einsatz in seinem Verantwortungsbereich,
g) die Dokumentation der zum Schutz der Daten getroffenen Maßnahmen,
h) die Maßnahmen zur Wahrung der Rechte der betroffenen Personen insbes. des Rechts auf Berichtigung, Löschung, Einschränkung, sowie die Erfüllung der Informationspflichten,

i) die Einhaltung von Löschfristen und zulässiger Speicherdauer auf der Anwendungsebene,
j) die Erstellung und Aktualisierung des vom Auftraggeber zu führenden Verzeichnisses aller Verarbeitungstätigkeiten.

4.2 Benötigt Dataport zur Erstellung und Aktualisierung des von Dataport als Auftragsverarbeiter gem. Art. 30 Abs.2 DSGVO zu führenden Verzeichnisses der Verarbeitungstätigkeiten Angaben des Auftraggebers oder von Verantwortlichen, für welche der Auftraggeber Auftragsverarbeiter ist, stellt der Auftraggeber Dataport diese Angaben zur Verfügung.

4.3 Hat der Auftraggeber als Verantwortlicher eine Datenschutz-Folgenabschätzung durchzuführen, stellt er Dataport das Ergebnis einschließlich der daraus von ihm abgeleiteten Maßnahmen zur Verfügung. Dataport setzt die Maßnahmen nach Maßgabe des erteilten Auftrages um.

4.4 Beauftragt der Auftraggeber Dritte unmittelbar mit der Verarbeitung der Kundendaten, die Gegenstand des Vertrages mit Dataport sind, so erfolgt diese Beauftragung und deren Verarbeitung in ausschließlicher Verantwortung des Auftraggebers bzw. des jeweiligen Dritten.

5 Verpflichtungen und Unterstützungsleistungen Dataports

5.1 Dataport verarbeitet die Daten und unterstützt den Auftraggeber bei der Wahrnehmung seiner gesetzlichen Verpflichtungen nach Maßgabe der gesetzlichen Bestimmungen im Rahmen des Vertrages und den nachfolgenden, ergänzenden Regelungen. Dies gilt insbesondere hinsichtlich der gesetzlichen Anforderungen:

a) an die Verarbeitung ausschließlich auf dokumentierte Weisung,
b) an die Gewährleistung der Vertraulichkeit,
c) an die erforderlichen Maßnahmen zum Schutz personenbezogener Daten,
d) an die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters,
e) den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte betroffener Personen nachzukommen,
f) den Verantwortlichen bei der Einhaltung seiner Pflichten zum Nachweis der Sicherheit und Ordnungsgemäßheit der Verarbeitung, der Melde- und Informationspflichten bei Verletzungen des Schutzes personenbezogener Daten und der Erstellung einer Datenschutzfolgenabschätzung zu unterstützen,
g) an Löschung oder Rückgabe der Daten nach Abschluss der Erbringung der Verarbeitungsleistung,
h) an die Zurverfügungstellung aller erforderlichen Informationen zum Nachweis der Ordnungsgemäßheit der Verarbeitung,
i) an die Ermöglichung und Unterstützung bei Prüfungen des Auftraggebers.

5.2 Die eigene Verantwortung Dataports für die Einhaltung der für Dataport als Auftragsverarbeiter unmittelbar geltenden Datenschutzbestimmungen bleibt hiervon unberührt.

6 Weisungsrechte des Auftraggebers; Bindung an den Auftrag

6.1 Dataport verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers und im Rahmen des Auftrages, es sei denn, dass Dataport nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist. Die im Vertrag und dessen Anlagen enthaltenen Regelungen stellen Weisungen des Auftraggebers dar. Weisungen im Einzelfall (Einzelauftrag) sind durch den Auftraggeber schriftlich oder in einem elektronischen Format zu erteilen. Werden Weisungen wegen Eilbedürftigkeit mündlich erteilt, sind sie unverzüglich schriftlich oder in einem elektronischen Format zu bestätigen.

6.2 Dataport unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber durch den Vertrag oder gesondert nach Vertragsabschluss in anderer Weise erteilte Weisung nach Auffassung von Dataport zu einem Verstoß gegen datenschutzrechtliche Vorschriften führen kann. Dataport ist berechtigt, die Datenverarbeitung bzw. die Umsetzung der Weisung solange auszusetzen, bis die Weisung durch den Auftraggeber schriftlich oder in einem elektronischen Format bestätigt oder geändert wird.

7 Wahrung der Vertraulichkeit

7.1 Dataport macht die mit der Durchführung der Arbeiten Beschäftigten mit den maßgeblichen Bestimmungen des Datenschutzes vertraut und verpflichtet sie schriftlich unter Hinweis auf die ordnungswidrigkeits- und strafrechtlichen Folgen zur Einhaltung dieser Bestimmungen, insbesondere zur Wahrung der Vertraulichkeit und des Datengeheimnisses, soweit sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.2 Kopien und Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Kopien, soweit dies zur Einhaltung gesetzlicher Aufbewahrungspflichten oder zur Befolgung einer gerichtlichen Anordnung erforderlich ist.

7.3 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von schutzwürdigen Sachverhalten und Daten (insbes. Geschäftsgeheimnisse, Sicherheitsmaßnahmen, als intern oder vertraulich gekennzeichnete Unterlagen, Vertragsinhalte, Leistungsentgelte) vertraulich zu behandeln. Eine Kenntnisgabe oder Übermittlung an Dritte ist nur

nach vorheriger, durch Dataport schriftlich oder in einem elektronischen Format erteilten Einwilligung zulässig; dies gilt nicht für die Kenntnisgabe oder Übermittlung an öffentliche Stellen im Rahmen der Ausübung von gesetzlichen Aufsichts- oder Prüfungshandlungen und an mit der Durchführung solcher Handlungen von öffentlichen Stellen beauftragte Dritte. Die Übermittlung an Dritte durch den Auftraggeber aufgrund für ihn geltender gesetzlicher Bestimmungen und nach Maßgabe der hierfür jeweils geltenden Bestimmungen zum Datenschutz, zur Geheimhaltung und zur Wahrung der Vertraulichkeit bleibt unberührt.

7.4 Ist der Auftraggeber gegenüber einer öffentlichen Stelle oder einer betroffenen Person verpflichtet, Auskünfte über die Verarbeitung von Daten zu geben, so wird Dataport den Auftraggeber darin unterstützen, diese Auskünfte zu erteilen.

7.5 Dataport legt Daten, welche im Auftrag verarbeitet werden, nicht gegenüber Dritten offen, außer auf Weisung des Auftraggebers, oder wenn Dataport nach deutschem Recht oder nach Unionsrecht hierzu verpflichtet ist.

7.6 Dataport legt Daten, welche im Auftrag verarbeitet werden, nicht gegenüber Vollzugsbehörden oder Gerichten offen, außer Dataport ist hierzu nach deutschem Recht oder nach Unionsrecht und/oder auf der Grundlage einer hoheitlichen Maßnahme (z.B. Anordnung zur Beschlagnahme oder Durchsuchung) verpflichtet. Wird Dataport zur Offenlegung von im Auftrag verarbeiteten Daten durch eine hoheitliche Maßnahme verpflichtet, informiert Dataport den Auftraggeber hierüber unverzüglich und stellt ihm eine Kopie der Anordnung zur Verfügung, es sei denn, dies ist Dataport gesetzlich oder im Einzelfall durch eine gerichtliche Anordnung verboten.

7.7 Wird Dataport von einer betroffenen Person zur Herausgabe von Daten oder zur Auskunft über diese Person gespeicherten Daten oder zu deren Sperrung, Berichtigung oder Löschung aufgefordert, wird Dataport die betroffene Person an den Auftraggeber verweisen.

8 Ort der Datenverarbeitung; Datenübermittlung in Drittländer

Die Verarbeitung der ruhenden Kundendaten erfolgt ausschließlich innerhalb der EU bzw. des EWR. Eine Datenübermittlung in Drittländer findet nicht statt.

9 Technische und Organisatorischen Maßnahmen zum Datenschutz und Nachweis der datenschutzkonformen Verarbeitung

9.1 Dataport trifft unter Berücksichtigung des Stands der Technik sowie der einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

9.2 Dataport betreibt ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 auf der Basis von IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik. Dieses umfasst alle IT-Infrastrukturen und –dienste, die Dataport eigenverantwortlich betreibt. Für das Produkt dPhoenixSuite 2.0 erstellt Dataport ein Sicherheitskonzept als Nachweis für die Umsetzung technischer und organisatorischer Maßnahmen auf Grundlage von BSI-Grundschutz und als Nachweis für die erforderlichen Maßnahmen zum Schutz personenbezogener Daten.

9.3 Im Rahmen des Betriebes der IT-Infrastrukturen und –dienste werden alle administrativen Zugriffe auf durch Dataport im Auftrag verarbeitete Daten gemäß den gesetzlichen Anforderungen und gemäß den Anforderungen gemäß BSI-Grundschutz protokolliert. Die Protokollierung umfasst insbesondere die Informationen über die betroffenen Daten, den Zeitpunkt, den Anlass und die Art des Zugriffs sowie die Identifikation der jeweiligen Person, durch welche der Zugriff erfolgt. Die Protokollierung von Nutzerzugriffen im Rahmen des Verfahrensbetriebes erfolgt nach Maßgabe des verfahrensspezifischen Protokollierungskonzeptes.

9.4 Dataport ist hinsichtlich der in seinem Verantwortungsbereich liegenden technischen und organisatorischen Maßnahmen nach eigenem, pflichtgemäßen Ermessen berechtigt, diese durch andere, gleichwertige Maßnahmen zu ersetzen, sowie berechtigt und verpflichtet, diese der technischen und organisatorischen Weiterentwicklung anzupassen. Hierbei darf das Sicherheitsniveau der ursprünglich vereinbarten Maßnahmen nicht unterschritten werden. Änderungen werden von Dataport dokumentiert.

10 Meldung von Verletzungen des Schutzes personenbezogener Daten

10.1 Wird Dataport eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet Dataport diese dem Auftraggeber unverzüglich. Dataport stellt dem Auftraggeber

a) die Informationen zur Verfügung, welche von diesem für die Beurteilung benötigt werden, ob durch ihn eine Meldung an die zuständige Aufsichtsbehörde oder an die betroffene(n) Person(en) zu erfolgen hat,

b) die Informationen zum Sachverhalt zur Verfügung, welche vom Auftraggeber in der Meldung aufgrund datenschutzrechtlicher Bestimmungen anzugeben sind. Hierzu gehören insbesondere

(1) eine Beschreibung der Art des Vorfalls, Kategorien und ungefähre Anzahl der betroffenen Personen und Daten,
(2) eine Beschreibung der wahrscheinlichen Folgen des Vorfalls,
(3) eine Beschreibung der ergriffenen Sofortmaßnahmen zur Behebung oder Abmilderung der Verletzung,
(4) Ansprechpartner für weitere Informationen.

Liegen diese Informationen nicht gleichzeitig vor, kann eine Meldung schrittweise erfolgen.

10.2 Dataport ergreift unverzüglich angemessene Maßnahmen zur Identifikation und zur Beseitigung der Ursache sowie zur Minderung möglicher nachteiliger Folgen für betroffene Personen. Kann aufgrund der Dringlichkeit über die Maßnahmen das Benehmen mit dem Auftraggeber nicht vorab hergestellt werden, setzt Dataport diesen unverzüglich darüber in Kenntnis.

11 Rückgabe und Löschung von Daten

11.1 Personenbezogene Daten, welche für die Durchführung der Dataport im Rahmen der Auftragsverarbeitung obliegenden Tätigkeiten nicht mehr benötigt werden, werden durch Dataport datenschutzgerecht gelöscht bzw. sofern es sich um nicht in elektronischer Form vorliegende Daten handelt, datenschutzgerecht entsorgt. Gleiches gilt für Test- und Ausschussmaterial.

11.2 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 gemäß SLA, Teil B, 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.

12 Weitere Auftragsverarbeiter

1.1 Dataport ist berechtigt, zur Erfüllung seiner vertraglich geschuldeten Leistungen Dienstleister als weitere Auftragsverarbeiter nach vorheriger, in schriftlicher oder in elektronischer Form erteilten Genehmigung durch den Auftraggeber einzusetzen. Dienstleister, welche lediglich Wartungs- oder Reparaturleistungen erbringen, mit denen ein Zugriff auf Kundendaten nicht möglich ist, gelten nicht als weitere Auftragsverarbeiter.

1.2 Dataport überträgt seine im Verhältnis zum Auftraggeber geltenden vertraglichen Pflichten und die für Dataport unmittelbar geltenden gesetzlichen Pflichten zum Schutz der Kundendaten vertraglich in entsprechendem Umfang auf seine weiteren Auftragsverarbeiter.

1.3 Dataport teilt dem Auftraggeber die weiteren Auftragsverarbeiter im Vertragsangebot mit. Die Annahme des Vertragsangebotes durch den Auftraggeber gilt als Genehmigung dieser weiteren Auftragsverarbeiter.

1.4 Sind zum Zeitpunkt der Angebotserstellung bzw. der Annahme des Angebotes weitere Auftragsverarbeiter noch nicht bekannt oder ist eine Änderung bezüglich bereits genehmigter weiterer Auftragsverarbeiter erforderlich, teilt Dataport dem Auftraggeber den oder die weiteren Auftragsverarbeiter zwecks Einholung der Genehmigung unverzüglich mit. Der Auftraggeber teilt Dataport innerhalb eines Monats nach Zugang der Mitteilung die Genehmigung oder den Einspruch unter Angabe von Gründen mit. Erfolgt innerhalb dieser Frist keine Mitteilung des Auftraggebers an Dataport, gilt die Genehmigung als erteilt.

1.5 Versagt der Auftraggeber die Genehmigung zum Einsatz eines weiteren Auftragsverarbeiters oder erhebt er gegen den Einsatz eines weiteren Auftragsverarbeiters Einspruch, sind beide Vertragsparteien berechtigt, den Vertrag außerordentlich zu kündigen. Unbeschadet des Kündigungsrechts werden die Vertragsparteien eine einvernehmliche Lösung anstreben.

1.6 Erfolgt der Einsatz eines bestimmten weiteren Auftragsverarbeiters durch Dataport auf Verlangen des Auftraggebers als Bestandteil des Dataport vertraglich erteilten Auftrages, stellt dieser Auftrag zugleich die Genehmigung des Auftraggebers dar.

1.7 Der Einsatz weiterer Auftragsverarbeiter unmittelbar durch den Auftraggeber für Tätigkeiten, welche nicht Bestandteil der von Dataport vertraglich zu erbringenden Leistungen sind, ist nicht Gegenstand der in dieser Nr. 12 getroffenen Regelungen. Der Auftraggeber trägt in diesem Fall die alleinige Verantwortung für den Einsatz dieser weiteren Auftragsverarbeiter.

13 Informations-, Mitwirkungs- und Unterstützungspflichten Dataports

13.1 Dataport informiert den Auftraggeber unverzüglich über schwerwiegende Betriebsstörungen.

13.2 Werden Anträge betroffener Personen auf Geltendmachung von Betroffenenrechten an Dataport gerichtet, wird Dataport die Antragsteller an den Auftraggeber verweisen.

13.3 Dataport unterstützt den Auftraggeber bei der Erstellung des vom Auftraggeber zu führenden Verzeichnisses der Verarbeitungstätigkeiten und bei der Erstellung einer Datenschutz-Folgenabschätzung jeweils hinsichtlich der Beschreibung der technischen und organisatorischen Maßnahmen.

13.4 Dataport unterstützt den Auftraggeber bei Konsultationen mit der Aufsichtsbehörde.

14 Prüfungsrechte des Auftraggebers

14.1 Der Auftraggeber ist berechtigt, nach Vorankündigung mit angemessener Frist und während der üblichen Geschäftszeiten von Dataport die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen zu überprüfen (Kontrollen, Audits).

14.2 Im Rahmen der Überprüfung ist der Auftraggeber insbesondere zur Einsichtnahme in die in seinem Auftrag betriebenen Datenverarbeitungsprogramme, zum Zugang zu den Arbeitsräumen oder zum Mitlesen an Kontrollbildschirmen bei Ausführung der Arbeiten im Rahmen administrativer Tätigkeiten oder des Fernwartungs-Zugriffs durch Dataport sowie zur Einholung von Auskünften berechtigt. Eine Störung des Betriebsablaufs bei Dataport ist dabei nach Möglichkeit zu vermeiden.

14.3 Der Auftraggeber kann mit der Kontrolle Dritte beauftragen, soweit diese nicht in einem Wettbewerbsverhältnis zu Dataport stehen und die Gefahr eines Interessenkonflikts nicht besteht. Die aufgrund des Hamburgischen Sicherheitsüberprüfungsgesetzes geltenden Zutrittsbeschränkungen zu Sicherheitsbereichen sind zu beachten, sofern Prüfungshandlungen von Personen durchgeführt werden sollen, für welche eine Sicherheitsüberprüfung nicht nachgewiesen wird.

14.4 Unterstützungsleistungen Dataports für den Auftraggeber im Rahmen von Audits und Prüfungen von in dessen Auftrag betriebenen Verfahren, welche über die Bereitstellung einer auftragsgemäßen verfahrensbezogenen Dokumentation, die Erteilung von schriftlichen oder mündlichen Auskünften oder die Vorlage von Abrechnungsunterlagen hinaus gehen, werden von Dataport auf der Grundlage gesondert zu erteilender Aufträge bereitgestellt.

14.5 Dataport stellt dem Auftraggeber Nachweise über von Dataport veranlasste Zertifizierungen für die von Dataport eigenverantwortlich betriebene Infrastruktur oder für die von Dataport eigenverantwortlich betriebenen Verfahren auf Anforderung zur Verfügung.