Rahmenvertrag EVB-IT
Projekt: Umsetzungsprojekt DAP

zwischen

govdigital eG

Charlottenstr. 65

10117 Berlin

- nachfolgend „Auftraggeber“ genannt -

Und

Dataport

Anstalt des öffentlichen Rechts

Altenholzer Straße 10-14

24161 Altenholz

- nachfolgend „Auftragnehmer“ genannt -

- Auftraggeber und Auftragnehmer nachfolgend einzeln auch „Partei“ oder gemeinsam „Parteien“ genannt –

Präambel

Der Auftraggeber beabsichtigt zukünftig den Lehrkräften des Landes Baden-Württemberg im Rahmen der Digitalen Bildungsplattform des Landes Baden-Württemberg den Zugang zu einem Digitalen Arbeitsplatz (kurz: DAP) zu ermöglichen und zur Nutzung bereit zu stellen. Der DAP soll klassische Funktionalitäten von Büroprogrammen bestehend aus Textverarbeitung, Tabellenkalkulation, E-Mail-Programm, Präsentations-Software und Kollaborations-Tools umfassen.

Die dem DAP zugrundeliegende Software soll zur Vermeidung von Marktabhängigkeiten auf Basis der auf Open Source Software basierenden Web-Arbeitsplatz-Lösung dPhoenixSuite zur Nutzung bereitgestellt, betrieben und gepflegt werden. Der Auftragnehmer bietet die Weiterentwicklung und den Betrieb dieser Lösung über seine, für das Projekt wesentliche und insofern garantierte, Unterauftragnehmerin Dataport (AöR). Im Rahmen eines Pilotprojektes wurde die dPhoenixSuite auf die fachlichen, technischen und organisatorischen Anforderungen des Bildungssektors in Baden-Württemberg bereits geprüft. Im Endausbau sollen zukünftig alle Schulen im Geschäftsbereich des Ministeriums für Kultus, Jugend und Sport in Baden-Württemberg die Dienste und Services des DAP in Baden-Württemberg nutzen. Ein hochverfügbarer, sicherer und datenschutzkonformer Betrieb des DAP ist daher wesentlich für die Beauftragung der Leistungen an den Auftragnehmer.

Die Unterauftragnehmerin Dataport ist eine IT-Dienstleisterin für Länder und Kommunen. Als solche bietet Dataport die besten Lösungen für die speziellen Anforderungen von Verwaltungsprozessen öffentlicher Stellen. Dataport entwickelt innovative IT-Services, welche für die besonderen Verwaltungsprozesse von Behörden geeignet und auf die speziellen Erfordernisse angepasst sind. Neue Technologien werden auf Herz und Nieren geprüft und für den Einsatz im öffentlichen Sektor optimiert. Dataport verfügt über fundierte Erfahrungen bei der Erbringung von IT-Services im Bereich der digitalen öffentlichen Verwaltung, insbesondere auch im Bereich der Softwareentwicklung und des Betriebs von IT-Services für Schulen, und bietet sichere IT-Infrastrukturen und -Services für die digitale Souveränität von Staat und Verwaltung, welche insbesondere auch für den Schutz sensibler personenbezogener Daten geeignet sind.

Art, Ziel und Zweck des DAP sind Dataport aus dem bereits durchgeführten Pilotprojekt sowie Aufbauprojekt zur Konzeptionierung des DAP bekannt. Ziel dieses Vertrags ist es, das im Rahmen des Aufbauprojektes entwickelte Konzept für das Umsetzungsprojekt umzusetzen und den Betrieb des DAP zu erbringen.

Als Behörde verfügt der Auftraggeber nicht über die für dieses anspruchsvolle Projekt notwendigen Kenntnisse und Fähigkeiten, insbesondere im Bereich von IT-Services und Projektmanagement, und bedarf daher der Unterstützung, des Schutzes und der Hilfe durch den Auftragnehmer. Der Auftragnehmer versichert, dass er bereit und in der Lage ist, die Verantwortung für die Leistungserbringung gemäß den Vereinbarungen dieses Vertrages zu übernehmen.

Diese Zusammenarbeit der Vertragspartner beruht auf den Grundsätzen von

a) Partnerschaft

b) Leistungstransparenz

c) Kostentransparenz

d) kontinuierlicher Verbesserung der IT -Prozesse

e) gemeinsamer Zielorientierung auf ein dynamisches Volumen der Geschäftsvorfälle des Ministeriums für Kultus, Jugend und Sport in Baden-Württemberg und auf Analyse der Kostenoptimierungsmöglichkeiten, insbesondere aufgrund von Standardisierung und Produktivitätsgewinnen.

Dies vorausgeschickt, schließen die Vertragspartner den nachfolgenden Vertrag, wobei zwischen den Parteien Einigkeit besteht, dass auch die Regelungen in der Präambel Gegenstand des Vertrags selbst sind:

Leistungsverzeichnis

1. Vertragsbestandteile und Geltungsbereich

1.1 Die Rechte und Pflichten beider Parteien werden durch das gesamte Vertragswerk („Vertrag“) geregelt. Es besteht aus:

a) diesem Rahmenvertrag und alle Anhänge des Vertrages

b) dem EVB-IT Cloudvertrag Nr. V21511 und dessen Anlagen

c) dem EVB-IT Systemvertrag Nr. V21489 und dessen Anlagen

1.2 Das Vertragswerk stellt eine sachliche, wirtschaftliche und rechtliche Einheit dar. Dieser Vertrag gilt auch

(a) für vorvertragliche Leistungen der Parteien, die unter diesem Vertrag fertig gestellt werden sollen, einschließlich insbesondere der Leistungen aus der vertraglichen Nebenabrede vom 18.10.2023, soweit die vertragliche Nebenabrede auf diesen Vertrag Bezug nimmt.

(b) für alle sonstigen Vereinbarungen, die zwischen Auftraggeber und Auftragnehmer in Bezug auf den in der Präambel genannten Gegenstand bis zum Beendigungszeitpunkt abgeschlossen werden.

1.3 Allgemeine Geschäftsbedingungen der Parteien werden auch dann nicht Bestandteil von Vereinbarungen, die unter diesem Rahmenvertrag abgeschlossen werden, wenn diese durch eine Partei widerspruchslos während der Laufzeit eingeführt werden.

2. Vertragsgrundsätze und Vertragsziele

Der Auftraggeber beauftragt den Auftragnehmer, das Umsetzungsprojekt „DAP“ nach Maßgabe dieses Vertrages durchzuführen. Projektplanung, Projektdurchführung und Ergebnisverantwortung liegen beim Auftragnehmer. Der Auftragnehmer haftet für die Leistungen seiner Unterauftragnehmer wie für seine eigenen Leistungen.

3. Projektziel

Ziel des Projektes ist die Bereitstellung des DAP auf der vom Auftragnehmer bereitgestellten IT-Infrastruktur und dessen anschließenden Betrieb für den Bildungssektor.

4. Geschäftsgrundlage

4.1 Die Leistungen aus dem Aufbauprojekt sowie den Vorverträgen (nachfolgend „Vorleistungen“) bilden für den Auftraggeber die Grundlage für den Aufbau und den Betrieb eine wirtschaftliche Einheit, weil die festgelegten funktionalen und technischen Anforderungen an einen DAP nur mit erfolgreichem Abschluss dieser Vorleistungen erreicht werden können. Die fristgerechte und erfolgreiche Umsetzung der Vorleistungen stellt deshalb die Geschäftsgrundlage für die Beauftragung der weiteren Leistungen des Umsetzungsprojektes unter dem Vertrag dar. Die Geschäftsgrundlage für die Beauftragung des Umsetzungsprojektes entfällt nachträglich, wenn die Vorleistungen nicht bis zum

07.09.2024 (Datum der Fertigstellung der Vorleistungen) erfolgreich abgeschlossen ist, es sei denn, der Auftragnehmer (oder dessen Unterauftragnehmer) hat dies nicht zu vertreten.

4.2 Bei nachträglichem Wegfall der Geschäftsgrundlage für die Beauftragung des Umsetzungsprojektes ist der Auftraggeber berechtigt, die Beauftragung des Umsetzungsprojektes zu kündigen. Der Auftragnehmer wird im Falle der Kündigung alle bis dahin erstellten und noch nicht gelieferten Leistungsgegenstände unverzüglich liefern. Die bis zur Kündigung vom Auftragnehmer erbrachten Vorleistungen sind vom Auftraggeber gemäß den vereinbarten Preisen, gegebenenfalls anteilig, zu vergüten.

5. Vertragsgegenstand

5.1 Sämtliche durch den Auftragnehmer zu erbringenden Leistungen, einschließlich optional durch den Auftraggeber abzurufende Leistungen, ergeben sich insbesondere aus dem EVB-IT Systemvertrag, dem EVB-IT Cloudvertrag, den jeweiligen Leistungsbeschreibungen sowie aus diesem Vertrag.

5.2 Mit Vertragsschluss ist zunächst die betriebsbereite Bereitstellung eines über das Internet nutzbaren DAP auf Basis der dPhoenixSuite auf Basis des EVB-IT Systemvertrages Nr. V21489 geschuldet (Umsetzungsprojekt). Dazu gehört insbesondere die Erstellung einer SCIM-Schnittstelle für die Nutzerprovisionierung, die Skalierung der Cloudinfrastruktur für bis zu 130.000 Nutzer, Umsetzung des Konzepts zur Nutzergruppentrennung, das Theming/Branding der Nutzeroberfläche sowie die Übernahme der Betriebsverantwortung für den DAP. Der Aufbau der IT-Infrastruktur erfolgt in fünf (5) verschiedenen Projektphasen, die die Befähigung der dPhoenixSuite zum Betrieb mit bis zu 130.000 Nutzenden durch phasenweise Skalierung als Zielsetzung haben.

5.3 Der Auftragnehmer übernimmt jeweils nach Abschluss der einzelnen Projektphasen für das Mengengerüst der Ausbaustufe sowie im Anschluss an das Umsetzungsprojekt für ein Mengengerüst von bis zu 130.000 Nutzenden den Applikationsbetrieb des DAP im Rahmen des Cloud-Hostings auf Basis und i.S.d. des EVB-IT Cloudvertrages Nr. V21511.

5.4 Die Leistungen unter dem Vertrag bilden eine sachliche, wirtschaftliche und rechtliche Einheit. Für den Auftraggeber ist von vertragswesentlicher Bedeutung, dass der Auftragnehmer die in diesem Vertrag vereinbarten Leistungen ordnungsgemäß erbringt und alle dafür erforderlichen Schritte vornimmt.

5.5 Die Nutzbarkeit, Pflege, Fortentwicklung sowie Anpassung von Standard- und Individualsoftware sind von diesem Vertrag umfasst.

6. Projektmanagement, Projektorganisation und Projektstruktur

6.1 Die Parteien vereinbaren für Projektmanagement, Projektorganisation und Projektstruktur verbindlich ein jeweils leistungsspezifisches Vorgehensmodell gemäß den Vorgaben der Leistungsbeschreibungen.

6.2 Projektdokumentation, Reporting und Monitoring entsprechen dem Standard des vereinbarten Vorgehensmodells.

6.3 Im Rahmen des Umsetzungsprojekts werden Abgrenzungen und Verantwortlichkeiten in Form von VDBI-Matrizen festgehalten. Die Abgrenzungen zwischen Auftragnehmer und Auftraggeber werden im Rahmen der jeweiligen Arbeitspakete im Einzelnen festgelegt.

Die Parteien legen folgende Definitionen zu Grunde:

Bezeichnung	Erläuterung
[V] Verantwortlich	"V" bezeichnet denjenigen / diejenige, der / die für den Gesamtprozess verantwortlich ist. „V" ist dafür verantwortlich, dass „D" die Umsetzung des Prozessschritts auch tatsächlich erfolgreich durchführt.
[D] Durchführung	"D" bezeichnet denjenigen / diejenige, der / die für die technische Durchführung verantwortlich ist.
[B] Beratung	"B" bedeutet, dass die Partei zu konsultieren ist und z. B. Vorgaben fürUmsetzungsparameter 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.

7. Allgemeine Leistungsanforderungen

7.1 Die Lieferungen und Leistungen des Auftragnehmers entsprechen über die gesamte Laufzeit des Vertrages

a) dem Stand der Technik

b) den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) öffentlich bekannt gemachten oder anerkannten IT-Sicherheitsstandards.

c) der Konformität mit allen gesetzlichen und allgemein anwendbaren behördlichen Entscheidungen.

d) der Konformität entsprechend den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).

e) Individualsoftware sowie Änderungen und Erweiterungen des auf Open Source Software basierenden Dienstes „dPhoenixSuite" sind so erstellt und dokumentiert, dass sie die Anforderungen an Zeitverhalten, Ergonomie, Fehlertoleranz, Wartbarkeit und Interoperabilität erfüllt und durch möglichst einfache und möglichst standardisierte Schnittstellen mit

der angrenzenden Software verbunden sind (Sicherung der Kompatibilität zu künftigen Ständen der Software).

7.2 Änderungen in den regulatorischen Anforderungen werden zeitnah umgesetzt, so dass die entsprechende Umsetzung zu Beginn der Periode zur Verfügung steht, zu der die entsprechende Anforderung in Kraft tritt.

8. Servicelevel für Nacherfüllung

Servicelevel für Nacherfüllung im Rahmen der Gewährleistung und Incident Management im Rahmen von Betriebsleistungen

Die gemäß den Leistungsbeschreibungen der EVB-IT Verträge vereinbarten Service Level gelten für Leistungen des Auftragnehmers im Rahmen der Nacherfüllung der Werkleistungen sowie für solche des Incident-Managements und Supports im Rahmen von Betriebsleistungen.

9. Unterauftragnehmer

9.1 Dataport Anstalt des öffentlichen Rechts, Altenholtzer Str. 10-14, 24161 Altenholz, ist wesentlicher und garantierter Unterauftragnehmer im Sinne eines Erfüllungsgehilfen gemäß § 278 BGB des Auftragnehmers. Der Austausch von Dataport als Unterauftragnehmer bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

9.2 Der Auftraggeber stimmt den zum Zeitpunkt des Vertragsschlusses gemäß Anhang zum Rahmenvertrag von Dataport eingesetzten und benannten weiteren Auftragsverarbeitern gem. DSGVO (nachfolgend „Auftragsverarbeiter“ genannt) zu. Die bei Vertragsschluss gültige Liste der Auftragsverarbeiter der Dataport gemäß Anhang zum Rahmenvertrag enthält den Firmennamen, die Anschrift und die Rolle jedes eingesetzten Auftragsverarbeiter. Sofern der Auftragsverarbeiter in die Verarbeitung personenbezogener Daten eingebunden ist, ist zusätzlich der Ort der Datenverarbeitung anzugeben. Der Auftragnehmer bleibt für die Vertragserfüllung verantwortlich und hat sicherzustellen, dass die Auftragsverarbeiter der Dataport sämtliche für den Auftragnehmer geltenden Vertragsbestimmungen einhalten.

9.3 Dataport erhält hiermit eine vorherige allgemeine schriftliche Genehmigung des Auftraggebers, die Leistungen unter den nachfolgenden Voraussetzungen auf Auftragsverarbeiter zu übertragen:

(a) der Auftragnehmer beauftragt Auftragsverarbeiter im Rahmen schriftlicher Verträge (einschließlich elektronischer Form), die mit den Bestimmungen des Vertragswerkes sowie, soweit die Verarbeitung von personenbezogenen Daten betroffen ist, der Auftragsverarbeitungsvereinbarung in Bezug auf die Verarbeitung personenbezogener Daten durch die Auftragsverarbeiter über-einstimmen. Der Auftragnehmer haftet für etwaige Verstöße durch den Auftragsverarbeiter gemäß den Bestimmungen des Vertragswerkes; und

(b) Dataport wird die Sicherheits- und Vertraulichkeitsmaßnahmen sowie, sofern die Verarbeitung personenbezogener Daten betroffen ist, Datenschutzmaßnahmen eines Auftragsverarbeiters vor dessen Auswahl bewerten, um festzustellen und sicherzustellen, dass der Auftragsverarbeiter in der Lage ist, dass in diesem Vertragswerk geforderte Schutzniveau zu bieten; und

(c) Der Einsatz von Auftragsverarbeitern erfolgt nach Ermessen der Dataport unter der Voraussetzung, dass folgende Regelungen eingehalten werden:

Dataport informiert den Auftraggeber (per E-Mail) über jegliche Ausschreibungsverfahren hinsichtlich der Hinzufügungen oder Ersetzungen von Auftragsverarbeiter, sobald diese öffentlich bekannt gemacht wurden. Unverzüglich, nachdem der Zuschlag erteilt wurde, informiert der Auftragnehmer den Auftraggeber (per E-Mail) über die Hinzufügung oder Ersetzung des Auftragsverarbeiters, einschließlich des Namens, der Anschrift und der Rolle des neuen Auftragsverarbeiters sowie den Zeitpunkt des Leistungsbeginns. Sofern der Auftragsverarbeiter in die Verarbeitung personenbezogener Daten eingebunden ist, ist zusätzlich der Ort der Datenverarbeitung anzugeben.; und

Der Auftraggeber kann solchen Änderungen gemäß Abschnitt d) widersprechen.

(d) Sofern der Auftraggeber wegen Verstoß gegen vertragliche Vereinbarungen durch Einsatz des neuen Auftragsverarbeiters oder auf Grund des Datenschutzrechts einen berechtigten Grund hat, der Einbeziehung, insbesondere wegen der Verarbeitung personenbezogener Daten durch den neuen Auftragsverarbeiter, zu widersprechen, kann er den Vertrag ganzheitlich durch schriftliche Erklärung gegenüber dem Auftragnehmer mit Wirkung zum Zeitpunkt des Beginns der Leistungserbringung des neuen Auftragsverarbeiters kündigen. Kündigt der Auftraggeber nicht bis zum Beginn der Leistungserbringung des neuen Auftragsverarbeiters, so gilt der neue Auftragsverarbeiter als durch den Auftraggeber genehmigt.

Innerhalb des Zeitraums ab dem Datum der Mitteilung der Dataport an den Auftraggeber, in der der Auftraggeber über den neuen Auftragsverarbeiter informiert wird, bis zum Leistungsbeginn des neuen Auftragsverarbeiters kann der Auftraggeber verlangen, dass die Vertragspartner sowie Dataport in gutem Glauben zusammenkommen und eine Lösung des Widerspruchs besprechen. Diese Besprechungen verlängern die Kündigungsfrist nicht und berühren nicht das Recht der Dataport, den/die neuen Auftragsverarbeiter zum mitgeteilten Leistungsbeginn in Dienst nehmen zu dürfen.

Jede Kündigung des Auftraggebers nach dieser Ziffer 9.3 (d) wird von beide Vertragspartnern als unverschuldet betrachtet und unterliegt den Bestimmungen des Vertragswerkes. Kündigt der Auftraggeber den Vertrag aufgrund des Widerspruchs gegen die Verwendung eines neuen Auftragsverarbeiters gem. Ziffer 9.3 (d), sind vom Auftraggeber die von dem Auftragnehmer bis zum Zeitpunkt der Vertragsbeendigung tatsächlich erbrachten Leistungen zu vergüten. Etwaige vom Auftraggeber bereits im Voraus geleistete Vergütung ist von dem Auftragnehmer zurückzuerstatten, soweit die Leistungen bis zum Zeitpunkt der Vertragsbeendigung nicht erbracht wurden. Die Haftung des Auftragnehmers wird dadurch nicht ausgeschlossen.

(e) Dataport kann einen Auftragsverarbeiter ohne vorherige Mitteilung austauschen, wenn sich der Grund für den Austausch der zumutbaren Kontrolle der Dataport entzieht und der umgehende Austausch aus Sicherheits- oder anderen dringenden Gründen erforderlich ist. In diesem Fall informiert Dataport den Auftraggeber über den neuen Auftragsverarbeiter unverzüglich nach seiner Ernennung. Ziffer 9.3 (d) gilt entsprechend.

9.4 Eine weitere Auslagerung durch den Auftragsverarbeiter und alle weiteren Auftragsverarbeiter in der Kette unterliegt ebenfalls den Bedingungen der Ziffern 9.2. und 9.3.

10. Leistungen bei Vertragsende

Mit Wirksamwerden einer Kündigung (gleich aus welchem Grund) hat der Auftragnehmer dem Auftraggeber auf Verlangen sämtliche im Rahmen des gekündigten Vertrages erbrachten (Teil-) Leistungen sowie die dazugehörigen Daten und Dokumente in der jeweils aktuellen Version zu übergeben und das Eigentum daran zu übertragen, sofern die Leistung auch unter dem Vertrag zur Herausgabe vorgesehen war. Hinsichtlich der Nutzungsrechte gelten die jeweiligen Reglungen der in Ziffer 1.1 des Rahmenvertrages genannten EVB-IT Verträge. Darüber hinaus gelten die Festlegungen zu Leistungen bei Vertragsende, die in den in Ziffer 1.1 des Rahmenvertrages genannten EVB-IT Verträgen getroffen wurden.

11. Vertragsdauer

11.1 Dieser Rahmenvertrag sowie die damit gemäß Ziffer 1.1 verbundenen EVB-IT Verträge treten mit Unterzeichnung durch beide Parteien rückwirkend zum 1. Februar 2024 in Kraft. Der Rahmenvertrag wird auf unbestimmte Zeit geschlossen. Der Rahmenvertrag endet mit Beendigung des letzten der in Ziffer 1.1 des Rahmenvertrages genannten EVB-IT Verträge automatisch, ohne dass es einer gesonderten Kündigung bedarf.

11.2 Das Recht beider Parteien zur außerordentlichen Kündigung dieses Rahmenvertrages oder einer der in Ziffer 1.1 des Rahmenvertrages genannten EVB-IT Verträge aus wichtigem Grund bleibt unberührt. Die außerordentliche Kündigung des oder der Rücktritt von dem EVB-IT Systemvertrag/s bewirkt

ebenfalls die Beendigung des EVB-IT Cloudvertrages. Ein wichtiger, den Auftraggeber zu einer außerordentlichen Kündigung berechtigender Grund liegt insbesondere vor, wenn

a) über das Vermögen des Auftragnehmers oder seines wesentlichen Unterauftragnehmers das Insolvenzverfahren bzw. ein vergleichbares gesetzliches Verfahren eröffnet oder dessen Eröffnung mangels Masse abgelehnt wird;

b) sich die Vermögensverhältnisse des Auftragnehmers oder seines wesentlichen Unterauftragnehmers wesentlich verschlechtern und der Auftragnehmer nicht innerhalb von dreißig (30) Kalendertagen nach entsprechender Aufforderung durch den Auftraggeber angemessene Sicherheit für die Erfüllung seiner Pflichten unter diesem Vertrag erbringt;

c) der Auftragnehmer oder sein wesentlicher Unterauftragnehmer eine wesentliche Pflicht unter diesem Vertrag trotz Abmahnung und Setzung einer angemessenen Frist zur Abhilfe nicht erfüllt oder trotz Abmahnung und Setzung einer angemessenen Frist zur Abhilfe fortgesetzt gegen sonstige Vertragspflichten verstößt (einschließlich fortgesetzter Schlechtleistung);

d) erkennbar ist, dass die Erfüllung der Vertragsleistungen, insbesondere auch die Einhaltung der Meilensteine und Termine, wegen mangelnder Leistungsfähigkeit des Auftragnehmers oder seines wesentlichen Unterauftragnehmers gefährdet ist; mangelnde Leistungsfähigkeit wird insbesondere angenommen, wenn der Auftragnehmer oder sein wesentlicher Unterauftragnehmers mit Vertragsleistungen ganz oder teilweise in Verzug gerät; Voraussetzung der außerordentlichen Kündigung im Falle des Verzuges ist, dass der Auftraggeber dem Auftragnehmer erfolglos eine Frist von 7 Werktagen zur Leistung gesetzt hat. Das Fristsetzungserfordernis gilt nicht hinsichtlich eines vereinbarten Vertragserfüllungstermins.

e) der Auftragnehmer oder dessen Mitarbeiter, Vertreter, Beauftragte oder Nachunternehmer, insbesondere sein wesentlicher Unterauftragnehmer, im Zusammenhang mit der Erbringung der Vertragsleistungen in erheblichem Umfang gegen straf- und/ oder bußgeldbewehrte Rechtsvorschriften verstoßen;

f) ein Dritter oder mehrere gemeinsam handelnde Dritte unmittelbar oder mittelbar mehr als 50 % der Geschäftsanteile und/ oder Stimmrechte des Auftragnehmers oder seines wesentlichen Unterauftragnehmers oder wesentliche Teile des Geschäftsbetriebs des Auftragnehmers oder seines wesentlichen Unterauftragnehmers erwerben;

g) eine Anordnung einer Aufsichtsbehörde, insbesondere des Landesbeauftragten für Datenschutz und Informationsfreiheit in Baden-Württemberg, die Durchführung dieses Vertrags erschwert oder verhindert;

h) die Gefahr von Reputationsrisiken für den Auftraggeber besteht; Die Gefahr von Reputationsrisiken liegt insbesondere in folgenden Fällen vor:

- Wenn die Summe wesentlicher Pflichtverletzungen oder sonstiger Verstöße des Auftragnehmers oder dessen garantierter Unterauftragnehmer gegen diesen Vertrag so erheblich ist, dass die Vertrauensbasis zwischen den Vertragsparteien nachhaltig gestört ist; einer weiteren Abmahnung und Setzung einer angemessenen Frist zur Abhilfe bedarf es in diesem Fall nicht; oder

- Wenn der Auftragnehmer oder der garantierte Unterauftragnehmer trotz voriger Aufforderung seinen Kooperationspflichten, insbesondere der Erfüllung von Obliegenheiten, der Mitwirkung und der gegenseitigen Information, nicht nachkommt. Die vorige Aufforderung ist entbehrlich, sofern der Auftragnehmer oder der garantierte Unterauftragnehmer die Kooperationspflichten erkannte oder hätte erkennen müssen; oder

- Jedes sonstige schuldhafte Verhalten des Auftragnehmers oder dessen garantierter Unterauftragnehmer, durch das der Vertragszweck gefährdet, so dass es der Auftraggeberin nicht mehr zugemutet werden kann, an der Fortsetzung des Vertrags festzuhalten; eine vorherige Fristsetzung mit Kündigungsandrohung ist in diesem Fall entbehrlich;

und

- aufgrund diesbezüglicher nachhaltiger negativer öffentlicher Berichterstattung und/oder Wahrnehmung das Ansehen des Auftraggebers beeinträchtigt wird; und/oder

- dadurch eine fachlich fundierte Gegendarstellung zu öffentlichen Vorwürfen, die den Vertrag zwischen den Vertragsparteien betreffen, dem Auftraggeber nicht möglich ist.

i) die weitere Durchführung des Vertrages für den Auftraggeber nach Abwägung der beiderseitigen Interessen der Parteien aus sonstigen Gründen unzumutbar erscheint.

11.3 Jede Kündigung dieses Rahmenvertrages hat schriftlich zu erfolgen.

11.4 Im Falle der Beendigung dieses Rahmenvertrages oder eines hierunter vereinbarten EVB-IT Vertrages, gleich aus welchem Rechtsgrund diese erfolgt, erbringt der Auftragnehmer Leistungen zur Beendigungsunterstützung gemäß Ziffer 10.

11.5 Hat der Auftragnehmer die Beendigung des Vertrages zu vertreten, sind tatsächlich erbrachte Vertragsleistungen nur insoweit zu vergüten, wie der Auftraggeber für diese Verwendung hat bzw. diese nicht den Anlass zu einer außerordentlichen Kündigung gegeben haben. Im Falle einer Beendigung nach Ziffer 4.3 gelten die dort getroffenen Festlegungen vorrangig.

11.6 Reicht der Regelungsgehalt einzelner Vorschriften dieses Rahmenvertrages über die Laufzeit dieses Rahmenvertrages hinaus, bleiben diese Vorschriften auch nach Beendigung des Rahmenvertrages wirksam.

12. Datenschutz

Der AN gewährleistet, personenbezogene Daten nur in Übereinstimmung mit allen jeweils geltenden datenschutzrechtlichen Bestimmungen der Bundesrepublik Deutschland, insbesondere

- Bundesdatenschutzgesetz (BDSG neu) bzw. die DSGVO
- Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) soweit zutreffend

zu verarbeiten und zu nutzen. Der Auftragnehmer ist verpflichtet, bei der auftragsmäßigen Verarbeitung und Nutzung der Daten des Auftraggebers das Datengeheimnis gemäß DSGVO und in Bezug auf Telekommunikationsdienstleistungen das Fernmeldegeheimnis gemäß § 3 TTDSG zu wahren.

Der Auftragnehmer verarbeitet die vom Auftraggeber zum Zweck der Erbringung der vertragsgegenständlichen Leistungen übergebenen Daten im Wege der weisungsgebundenen Auftragsdatenverarbeitung (Art. 28 DSGVO) für den Auftraggeber. Der Auftraggeber behält die volle Kontrolle über die vom Auftragnehmer für den Auftraggeber zu erhebenden, zu verarbeitenden und zu nutzenden Daten. Im Verhältnis der Vertragspartner stehen sämtliche vom Auftragnehmer für den Auftraggeber erhobenen, verarbeiteten oder genutzten Daten ausschließlich dem Auftraggeber zu; ein Zurückbehaltungsrecht des Auftragnehmers besteht hieran nicht. Der Auftragnehmer wird Weisungen des Auftraggebers, welche sich auf die Beachtung der Vorschriften der DSGVO oder sonstiger einschlägiger datenschutzrechtlicher Vorschriften entsprechend dieser Ziffer 12 beziehen, beachten. Die Regelungen zur Auftragsverarbeitung gemäß §Art. 28 DSGVO sind in der entsprechenden Anlage 1 - Vereinbarung zur Auftragsverarbeitung geregelt und gelten fortdauernd, wenn sie nicht durch die Vertragspartner verändert, werden

13. Ort der Leistungserbringung

Die Leistungserbringung, insbesondere Verarbeitung personenbezogener Daten, findet ausschließlich innerhalb des EWR statt.

14. Sprache

Die Kommunikation gegenüber dem Auftraggeber erfolgt in deutscher Sprache. Der Auftragnehmer gewährleistet, dass alle im Rahmen des gesamten Umsetzungsprojektes eingesetzten Mitarbeiter*innen, die in direktem Kontakt mit dem Auftraggeber stehen, befähigt sind auf Deutsch mit dem Auftraggeber zu kommunizieren.

15. Schlussbestimmungen

15.1 Änderungen oder Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für Änderungen dieser Schriftformklausel. Mündliche Nebenabreden sind nicht getroffen.

15.2 Sollte eine Bestimmung dieses Rahmenvertrages ganz oder teilweise unwirksam oder undurchführbar sein, werden die Wirksamkeit und Durchsetzbarkeit aller übrigen Bestimmungen des jeweiligen Vertrages davon nicht berührt. Die unwirksame oder undurchführbare Bestimmung ist durch diejenige wirksame und durchsetzbare Bestimmung als ersetzt anzusehen, die dem von den Parteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt. Dasselbe gilt für etwaige vertragliche Lücken.

Altenholz	27.03.2024		
Ort	Datum	Ort	Datum
Auftragnehmer		Auftraggeber	

[redacted]

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

als Anlage zum Vertrag/ zur Leistungsbeschreibung vom 01.02.2024

- nachfolgend „Leistungsvereinbarung“ –

zwischen

Auftraggeber

govdigital eG
Charlottenstr. 65, 10117 Berlin

(nachfolgend "**Auftraggeberin**" genannt)

und

Auftragnehmer

Dataport
Anstalt des öffentlichen Rechts
Altenholzer Straße 10-14
24161 Altenholz

(nachfolgend "**Auftragnehmer**" genannt)

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Auftragsverarbeitungsvereinbarung

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

Präambel

Der Auftraggeber hat den Auftragnehmer mit Leistungen im Bereich der Bereitstellung eines digitalen Arbeitsplatzes für Lehrkräfte in Baden-Württemberg beauftragt. Die Leistungen werden von den jeweiligen Lehrkräften und weiteren, vom Auftraggeber definierte Personengruppen, die an öffentlichen und privaten Schulen in Baden-Württemberg oder an öffentlichen Einrichtungen im Geschäftsbereich des Auftraggebers tätig sind, (nachfolgend „Nutzungsberechtigte“) genutzt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 Datenschutzgrundverordnung (DSGVO) gilt in diesem Zusammenhang nicht der Auftraggeber, sondern die jeweilige öffentliche oder private Schule oder öffentliche Institution. Im Verhältnis zwischen den Parteien soll diese Vereinbarung ein ausreichendes Datenschutzniveau bei der Ausführung der durch den Auftraggeber beauftragten Leistungen sicherstellen.

Im Verhältnis zwischen Auftragnehmer und dem Auftraggeber konkretisiert diese Vereinbarung die datenschutzrechtlichen Rechte und Pflichten gemäß Art. 28 Abs. 3 Datenschutzgrundverordnung (DSGVO) im Zusammenhang mit dem Umgang des Auftragnehmers oder von ihm unterbeauftragte Dritte mit personenbezogenen Daten zur Durchführung der Leistungsvereinbarung. Die Erfüllung der Auftragsverarbeitungsvereinbarung wird nicht gesondert vergütet.

Es werden die Begriffsdefinitionen der DSGVO zugrunde gelegt.

§ 1

Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeitende des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die die Auftraggeberin selbst gegenüber dem gemäß Art. 4 Nr. 7 DS-GVO Verantwortlichen als Auftragsverarbeiterin tätig ist.

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

§ 2

Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Applikationsbetrieb des Digitalen Arbeitsplatzes für Lehrkräfte (kurz „DAP“).

(2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung oder sofern die Leistungsvereinbarung keine Dauer vorsieht zur einmaligen Ausführung.

(3) Die Auftraggeberin kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine Weisung der Auftraggeberin nicht ausführt oder der Auftragnehmer Kontrollrechte der Auftraggeberin vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 3

Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten (Art. 4 Nr. 2 DS-GVO) sind in der Leistungsvereinbarung niedergelegt.

(2) Folgenden Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragnehmer (Art. 4 Nr. 1 DS-GVO):

a) Name, Vormane

b) E-Mail-Adresse

c) (Be-)Nutzername und Passwort (verschlüsselt)

d) IP-Adresse

e) Benutzer ID

f) Session ID (temporärer Sitzungsschlüssel)

g) FQDN des SMTP Clients

h) Meldungstext der Lage

i) Cookie Einstellungen

➔ Device: Browser auf Endgerät

➔ Session: Sitzung des Anwenders

j) Grundsätzliche Inhaltsdaten entsprechend den fachlichen Einsatzzenarien

➔ Hochgeladene, bearbeitete und gespeicherte Daten

➔ Kommentare und Nachrichten im Zuge der Dateibearbeitung

➔ E-Mail und deren Inhalt

➔ Empfänger- und Versenderinformationen

➔ Kalendersaten und andre Attribute

➔ Daten aus dem Kontaktmanagement

(3) Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst:

- Beschäftigte und externe Dienstleister des Auftraggebers

- Nutzer der verantwortlichen Stelle
  - z.B. Lehrer, Schüler, Erziehungsberechtigte, externe Kommunikationspartner, etc.

- alle vom Vertrag umfassten Personenkreise

(4) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss, Binding Corporate Rules oder Standardvertragsklauseln). Die nachträgliche Verlagerung ins EU-Ausland bedarf der vorherigen Zustimmung der Auftraggeberin.

§ 4

Verantwortlichkeit und Weisungsbefugnis

(1) Die Auftraggeberin ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung gegenüber dem für die Datenverarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO verantwortlich. Sie kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen. Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(2) Der Auftragnehmer darf Daten ausschließlich im Rahmen der Weisungen der Auftraggeberin erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung der Auftraggeberin. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von der Auftraggeberin danach in der Regel schriftlich oder in einem dokumentierten elektronischen Format durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(3) Der Auftragnehmer hat die Auftraggeberin unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange

auszusetzen, bis sie durch den Verantwortlichen bei der Auftraggeberin bestätigt oder geändert wird.

(4) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch die Auftraggeberin erteilen.

(5) Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Eine Kenntnisgabe oder Übermittlung an Dritte ist nur nach vorheriger, durch den Auftraggeber 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 Auftragnehmer 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.

(6) Der Auftragnehmer legt Daten des Auftraggebers nicht gegenüber Dritten offen, außer er 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 der Auftragnehmer zur Offenlegung von Daten des Auftraggebers durch eine hoheitliche Maßnahme verpflichtet, informiert er den Auftraggeber hierüber unverzüglich und stellt ihm eine Kopie der Anordnung zur Verfügung, es sei denn, dies ist ihm gesetzlich verboten.

(7) Kopien und Duplikate werden ohne Wissen der Auftraggeberin nicht erstellt. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggeberin berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(8) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung der Auftraggeberin unmittelbar durch den Auftragnehmer sicherzustellen.

(9) Der Auftragnehmer stellt der Auftraggeberin auf deren Wunsch Informationen zur Aufnahme in das von ihr zu führende Verarbeitungsverzeichnis zur Verfügung.

(10) Soweit die Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Mitarbeitenden des Auftragnehmers) verarbeitet werden, sind auch in diesem Fall die Maßnahmen nach Art. 32 DS-GVO sicherzustellen.

§ 5

Beachtung zwingender gesetzlicher Pflichten durch den Auftragnehmer

(1) Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragnehmer die nachfolgenden gesetzlichen Pflichten.

(2) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten de Auftraggeberin befassten Mitarbeitenden die Vertraulichkeit der Daten gemäß Art 28 Abs. 3, 29, 32 DS-GVO wahren und diese entsprechend auf das Datengeheimnis verpflichtet und in die für sie relevanten Bestimmungen zum Datenschutz eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(3) Sofern der Auftragnehmer verpflichtet ist nach den anwendbaren Vorschriften einen Datenschutzbeauftragten zu bestellen, wird er die Kontaktdaten des Datenschutzbeauftragten der Auftraggeberin zum Zwecke der direkten Kontaktaufnahme mitteilen.

(4) Der Auftragnehmer informiert die Auftraggeberin unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde wegen Verletzungen gegen datenschutzrechtliche Bestimmungen bei dem Auftragnehmer ermittelt.

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

§ 6

Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Er ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragnehmer wird der Auftraggeberin auf Anforderung die zur Wahrung ihrer Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Für einen Zutritt zu den Geschäftsräumen des Auftragnehmers ist eine Ankündigung mit einem Vorlauf von mindestens drei Werktagen erforderlich. Aufgrund der Kontrollverpflichtung der Auftraggeberin vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich die Auftraggeberin von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer der Auftraggeberin auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

(4) Die Auftraggeberin kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen.

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

(5) Die in § 6 (3) und (4) genannten Überprüfungsrechte stehen ebenfalls dem für die Datenverarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO zu.

§ 7

Mitteilung bei Verstößen durch den Auftragnehmer

(1) Der Auftragnehmer unterstützt die Auftraggeberin bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO des für die Datenverarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.

(2) Zu den Pflichten, bei denen der Auftragnehmer die Auftraggeberin unterstützt gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an die Auftraggeberin zu melden;

c) die Verpflichtung, die Auftraggeberin im Rahmen der Informationspflicht des für die Datenverarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO gegenüber dem Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung der Auftraggeberin für die Datenschutz-Folgenabschätzung sowie

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

e) die Unterstützung der Auftraggeberin im Rahmen vorheriger Konsultationen des des für die Datenverarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO mit der Aufsichtsbehörde.

§ 8

Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum der Auftraggeberin oder des für die Datenverarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten der Auftraggeberin beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändungen oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer die Auftraggeberin unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist ausgeschlossen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch die Auftraggeberin, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung der Auftraggeberin datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist der Auftraggeberin auf Anforderung vorzulegen.

(3) Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende der Auftraggeberin übergeben.

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

§ 9

Subunternehmer

(1) Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit vorheriger ausdrücklicher schriftlicher Genehmigung der Auftraggeberin vergeben werden. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen der Auftraggeberin und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden und die Verantwortlichkeiten klar abgrenzt sind. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

(3) Der Auftraggeberin sowie dem für die Datenverarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist die Auftraggeberin berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten.

(4) Der Auftragnehmer haftet gegenüber der Auftraggeberin dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

(5) Es gelten im Übrigen die Bestimmungen der Ziffer 9.3 des Rahmenvertrages.

§ 10

Nebenleistungen

Die §§ 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 11

Datenschutzkontrolle

Der Auftragnehmer verpflichtet sich, dem/ der behördlichen Datenschutzbeauftragten der Auftraggeberin zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

§ 12

Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Der Anhang „Technisch-organisatorische Maßnahmen“ ist Bestandteil dieser Vereinbarung.

Auftragsverarbeitungsvereinbarung

Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT

Altenholz, 27.03.2024

Datum, Ort

[redacted]

Auftragnehmer: Dataport
Verfahren: dPhoenixSuite

Technische und Organisatorische Maßnahmen zur Datensicherheit (TOM)

gemäß Art. 32 Abs. 1 und Art. 25 Abs. 1 DS-GVO

hier:

Generischer Ansatz nach Art. 32 DS-GVO zur IT-Sicherheit

Inhalt

1 Allgemeines

Der Auftraggeber als Verantwortlicher i.S.d. DSGVO (AG oder Kunde) und der Auftragnehmer und Auftragsverarbeiter i.S.d. DSGVO (AN oder Dataport) haben unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den Vorgaben der DSGVO erfolgt.

Das Verfahren dPhoenixSuite wird von Auftragnehmer betrieben und zur Verfügung gestellt; die implementierten technischen und organisatorischen Maßnahmen sind an den Risiken eines Schutzbedarfs „normal“ ausgerichtet. Der Kunde ist dafür verantwortlich Daten mit einem höheren Schutzbedarf nicht im Verfahren dPhoenixSuite abzulegen oder zu speichern. Ferner sind die Anforderungen des Datenschutzes an Technikgestaltung und datenschutz-freundliche Voreinstellung zu berücksichtigen.

Der Aufbau des Dokuments und die Auswahl Technischer und Organisatorischer Maßnahmen orientieren sich an den 7 Gewährleistungszielen des Standard-Datenschutzmodells (SDM, Version 2.0b vom April 2020) – d. h.

- Vertraulichkeit (siehe Kapitel 3.1)
- Integrität (siehe Kapitel 3.2)
- Verfügbarkeit (siehe Kapitel 3.3)
- Transparenz (siehe Kapitel 3.4)
- Nichtverkettung (siehe Kapitel 3.5)
- Datenminimierung (siehe Kapitel 3.6)
- Intervenierbarkeit (siehe Kapitel 3.7).

Auf die wiederholte Aufzählung von Maßnahmen, die mehrere Gewährleistungsziele abdecken, wird verzichtet. Die Maßnahmen werden in diesem Fall dem Gewährleistungsziel zugeordnet, bei dem sie am meisten zur Zielerreichung beitragen.

Unter Verfahren wird in diesem Sinne die anlässlich der Nutzung des webbasierten Dienstes dPhoenixSuite erfolgende Datenverarbeitung betrachtet.

Bei den eingesetzten Softwarebestandteilen handelt es sich ausschließlich um Open-Source-Software (OSS), die technisch und organisatorisch in einem gebündelten Softwarestack als webbasierte Kommunikations- und Kollaborationssoftware vom Auftragnehmer dem Auftraggeber bereitgestellt wird. Die dPhoenixSuite beinhaltet die folgenden Dataportprodukte und Funktionalitäten:

- dOnlineZusammenarbeit 2.0: Audio- und Videokonferenzplattform mit Meesenger-Funktionalität
- dPhoenixCloud und dPhoenixOffice: Fileshare- und Weboffice-Dienst zur Speicherung und Bearbeitung von Dateien und Dokumenten
- dPhoenixMail: Mail- und Groupware-Dienst

Die Leistungserbringung erfolgt grundsätzlich nach den Vorgaben des Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Dataport hat ein Informations- und Sicherheitsmanagement (ISMS) nach BSI Grundschutz produktiv eingeführt.

Dataport verpflichtet sich gegenüber dem Kunden und Nutzer (AG) zur Einhaltung nachfolgender TOM, die zur Einhaltung der anzuwendenden Datenschutzvorschriften bei der Nutzung des Verfahrens erforderlich sind.

2 Rechenzentren

Die Leistungserbringung erfolgt generell digital souverän in deutschen Rechenzentren.

Die Dienste werden in Rechenzentren der Nachunternehmen TelemaxX und Equinix erbracht, für die eine Zertifizierung nach ISO 27001:2013 vorliegt.

3 Technische und Organisatorische Maßnahmen

Dataport verpflichtet sich gegenüber dem Auftraggeber zur Umsetzung der folgenden Technischen und Organisatorischen Maßnahmen (TOM).

3.1 Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

3.1.1 Zutrittskontrolle

Dies umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen:

- Alarmanlage
- Automatisches Zugangskontrollsystem für Systemräume
- Zwei-Faktor-Systeme, wie z. B. Chipkarten oder Transpondersysteme
- Zusätzlich manuelle Schließsysteme für Systemschränke
- Sicherheitsschlösser
- Vergitterung von Zugangsschächten
- Türen mit Blindknauf
- Klingelanlage mit Videoüberwachung und Gegensprechanlage
- Videoüberwachung der Gebäude
- Betriebsgeländeabsicherung, wie z. B. Zäune, Stacheldraht etc.

Organisatorische Maßnahmen:

- Regelungen für Schlüsselausgabe
- Rezeptions- bzw. Pförtnerdienste
- Besucherprotokolle, dabei: generell nur begleitende Besuche im Objekt
- Mitarbeiterausweis mit Ablauf und Erneuerungsmodus, angekoppelt an Prozess „Einstellung/Ausstellung/Hausverbot“
- Schriftliche Regelung bzgl. der Begleitung von Besuchern in bestimmten Sicherheitszonen
- Sicherheitsüberprüfung auch für Wach-, Reinigungs- und Empfangspersonal und eigene wie fremde Mitarbeiter im IT-Bereich
- Bildung von Sicherheitszone(n) für verschiedene Gebäudebereiche

3.1.2 Zugangskontrolle

Dies umfasst Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ und „sicheren“ Passworts).

Technische Maßnahmen:

- Zugangskontrolle zu Systemen mindestens mit Benutzernamen und Passwort
- Zugangskontrolle zu Systemen mit Zwei-Faktor-Authentifizierung für Administratoren
- Teilweise automatische Überprüfung der Passwortqualität
- Einsatz von Anti-Malware-Systemen, Endpointprotection oder Integritätssicherung von Softwarekomponenten
- Firewall zur Separierung von Sicherheitszonen
- Einsatz von verschlüsselter Kommunikation bei administrativen Zugängen
- Verschlüsselung von Datenträgern
- Hardware-Absicherung durch passwortgeschützte Firmware-Konfiguration
- Sperre von externen Schnittstellen auf Servern (z. B. USB)
- Automatische Bildschirmsperre
- Teilweise Administration über Jump-Hosts / Administrationsplattform

Organisatorische Maßnahmen:

- Verwaltung und Dokumentation von Benutzerberechtigungen

- Regelmäßige Überprüfung der Benutzerberechtigungen
- Zuweisen von Berechtigungen mit klar definierten Rollenprofilen
- Zentrale Passwortvergabe
- Vorgaben zur Passwortqualität
- Vorgaben für sicheres Löschen und Vernichten
- Richtlinie „Clean Desk“
- Richtlinie für Datenschutz und Informationssicherheit
- Verschlüsselte Kommunikation mit dem Kunden zur Auftragsabwicklung
- Vermeidung der Nutzung von SuperAdmin-Kennungen in der Regeladministration
- Hinterlegung von Notfallkennungen und Zugangsdaten, sichere Verwaltung dieser Daten und technisch abgesicherten Prozess zur Änderung nach Entnahme einer Kennung im Notfall
- Regelungen wurden etabliert, so dass die Nutzung von Administrationskennungen nur für die notwendigen Aufgaben genutzt werden und nicht für andere Arbeiten oder z. B. Internetzugriffe
- Umfängliches Schutzkonzept der Endgeräte von Administratoren durch Anti-Malware-Agenten, Sperren von nicht freigegebenen Programmen, Internetzugriff nur per Proxy, Einschränkung der Betriebssystemrechte, Deaktivieren nicht benötigter Betriebssystemfunktionen etc.
- Prozesse für die Durchführung eines Lifecycle-Managements für Endgeräte mit Ausgabe, Betrieb, überwachter Löschung und überwachter fachgerechter Entsorgung

3.1.3 Zugriffskontrolle

Dies umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen:

- Aktenentsorgung nach DIN 66399
- Physische Löschung oder Vernichtung von Datenträgern
- Protokollierung von Administrationstätigkeiten
- Protokollierung von Anwendertätigkeiten

- Eventbasierte automatische Kontrolle der Protokolldaten
- Auswahl und Festlegung der verwendeten Kryptographie-Algorithmen
- Nur verschlüsselte Zugriffe für die Anwender
- Speicherung der Passwörter unter Nutzung von kryptographischen Verfahren
- Administrative Fernzugriffe nur über verschlüsselte Verbindungen
- Aufzeichnung aller administrativer Tätigkeiten von externen Dienstleistern
- Zeitverzögerung zwischen einzelnen Login-Versuchen / Temporäre Kontosperrung bei Fehlversuchen des Zugriffs auf administrative Konten

Organisatorische Maßnahmen:

- Berechtigungskonzepte für Administratoren und Benutzer je Anwendung
- Begrenzung der Anzahl der Personen mit administrativen Berechtigungen
- Trennung der Benutzerkennung für Administratoren
- Der Mitarbeiter (Benutzer) muss für nicht-administrative Tätigkeiten eine andere Benutzerkennung verwenden
- Freigabeprozess für das Ändern von Benutzerrechten nach dem 4-Augen-Prinzip
- Verbot der Weitergabe von Passwörtern und Mehrfachnutzung von Passwörtern
- Kein Einsatz von Gruppenkennungen, alle Kennungen sind individualisiert
- Automatische Sperrung von Benutzerkennungen bei zu vielen Falscheingaben des Passworts
- Konfiguration der Teilsysteme (z. B. Router, Webserver etc.) unter Einhaltung von Sicherheitsvorgaben (wie. z. B. TLS Version, Parameter etc.)
- Verpflichtendes Härten von System (wie z. B. Server, Switches etc.)
- Regelmäßiges Patchen von allen beteiligten Komponenten
- Schwachstellenmanagement der Systeme
- Teilweise verpflichtendes Patchen von Systemen / Zwangsinstallation von Patches
- Sicherung und Versionierung von Konfigurationseinstellungen
- Gültige Wartungs- und Supportverträge mit Software- und Hardwareherstellern
- Transparenz der fehlgeschlagenen Anmeldeversuche
- Änderung der Default Sicherheitseinstellung von Softwareherstellern (wie z. B. Passwörter)

3.1.4 Trennungskontrolle

Dies umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen:

- Trennung durch Stages mit Produktiv-, Test- usw. -umgebungen
- Trennung von Frontend und Backend (z. B. Datenbank)
- Sicherheitszonen mit unterschiedlichen Kommunikationsanforderungen (eine Sicherheitszone pro Kunde)
- Mandantentrennung wird auf mehreren Ebenen (Systeme, Netzsegmente, Speicherbereiche) vollzogen
- Kein Einsatz von WLAN im Bereich des Verfahrens ohne zusätzliches VPN

Organisatorische Maßnahmen:

- Stage-Umgebungen werden mit den gleichen Sicherheitsanforderungen betrieben, wie produktive Kundenumgebungen
- Unterschiedliche Benutzerkennung für administrative Aufgaben
- Beschränkung des Zugangs zu produktiv genutzten Source-Code-Versionen

3.1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen:

- Teilweise Möglichkeit zur Nutzung von pseudonymisierten Benutzerkennungen für Gäste, so dass kein Personenbezug für die Dataport Mitarbeiter möglich ist.

Organisatorische Maßnahmen:

- Sicheres Löschen von Daten nach Vertragsende bzw. Löschungsbeauftragung

3.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.2.1 Weitergabekontrolle

Dies umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network (VPN) eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. bei der Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen:

- Einsatz von Verschlüsselung bei der Kommunikation über Dataport-fremde Netze
- Einsatz von Festplattenverschlüsselung
- Protokollierung der Zugriffe und Abrufe
- Protokollierung der administrativen Aufgaben
- Protokollierung der durchgeführten Backups
- SSL/TSL-Verschlüsselung der E-Mail-Übertragung (SMTP) von und zu entfernten Mailservern, sofern diese Verschlüsslung unterstützen.

Organisatorische Maßnahmen:

- Definition und Dokumentation von Löschfristen
- Nachweise von Betroffenenanfragen bzgl. Betroffenenrechte
- Besucherprotokolle von Rechenzentren und Besucherregelungen (Begleitung durch Mitarbeiter)
- Beschränkung des Zutritts zum Rechenzentrum auf autorisierte Personen
- Restriktive Zutrittsgestaltung zu Serverräumen (Sicherheitszone)
- Sicherung des Zutritts durch 2 Faktoren
- Unterscheidung zwischen fest zugewiesenen und beim Sicherheitsdienst zur Abholung hinterlegten Zutrittsberechtigungen; im letzten Fall Autorisierung durch Kontrolle des Personalausweises/Firmenausweises; Hinterlegung zutrittsberechtigter Personen beim Sicherheitsdienst
- Nutzung von Videoüberwachung im Rechenzentrum, insbesondere beim Zutritt zu Sicherheitsbereichen
- Sicherung von Zutrittskontrollsystemen über Netzersatzanlage gegen Stromausfall
- E-Mails mit personenbezogenen Daten werden von Mitarbeitern nur verschlüsselt versandt
- Ein Transport von Datenträgern erfolgt im regulären Betriebsablauf nicht
- Nutzung von Open-Source-Produkten – Transparenz in der Nutzung von Verschlüsselung/Krypto-Algorithmen sowie Anti-Privacy-Komponenten
- Verzeichnis der verarbeitenden Personen
- Keine Webtracking- und/oder Analyse-Werkzeuge
- Nur funktionell essentielle Cookie-Einstellungen
- Einhaltung der Meldepflicht bei Datenpannen und Security-Ereignissen

3.2.2 Eingabekontrolle

Dies umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch

Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen:

- Protokollierung der Zugriffe und Abrufe
- Protokollierung der administrativen Aufgaben
- Auslagerung der Protokolle auf spezialisiertem Logserver mit Trennung der administrativen Berechtigungen
- Überprüfung der Benutzerdaten auf Malware

Organisatorische Maßnahmen:

- Dedizierte Bereiche für die Ablage der Daten von Benutzern

3.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.3.1 Verfügbarkeitskontrolle

Dies umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Einsatz von RAID-Systemen (0 bis 5) etc.

Technische Maßnahmen:

- Feuer- und Rauchmeldeanlage
- Feuerlöschanlage
- Klimatisierung der Rechenzentren
- USV
- RAID-Systeme
- HighAvailability-Systeme (HA)
- Videoüberwachung der Rechenzentren
- Unterbringung der Server in spezialisierten, separat verschlossenen Schränken
- Nutzung eines umfassenden DDoS-Schutz (Denial-of-Service)

Organisatorische Maßnahmen:

- Backup-Konzept
- Disaster-Recovery-Konzept
- IT-Notfallmanagement

- Regelmäßige Überprüfung des Notfallplans mit aktiver organisationsweiter Notfallübung (mind.1x jährlich)
- Regelmäßige Tests des Backup-Konzeptes auf Funktionsfähigkeit
- Ablage des Backups an zwei redundanten Rechenzentren
- Lagerung eines Backups offline, damit es vor Verschlüsselung durch Schadsoftware geschützt ist
- Keine Versorgungsleitungen in den Rechenzentren
- Brandschutz-Konzept
- Brand- und Rauchmeldeanlagen
- Unterteilung in Brandabschnitte mittels Brandschottung
- Automatische Löschanlagen
- Einbruchshemmende Türen und Fenster nach DIN EN 1627
- Keine brandaktiven Materialien in den Rechenzentren
- Dynamisches Kapazitäts-Management der beteiligten Systeme
- Abnahme- und Systemtest vor dem produktiven Betrieb
- Incident- und Problem-Management von existierenden Störungen bzw. Fehlern
- Test- und Freigabeverfahren z. B. bei Einführung neuer Soft- oder Hardware
- Beachtung der Hochwasser- und Erdbebenkritikalität
- Redundante Auslegung der operativen Leistungskomponenten (Storage Systeme, Netzwerktechnik)
- Nutzung von fehlertoleranten Massenspeicher-Systemen
- Tägliche Sicherung aller Serversysteme, Datenbanken
- Redundante Auslegung der Netzwerk-Infrastruktur und Firewall-Systeme
- Überwachung der Systeme mit Alarmierung
- Dokumentation von Infrastrukturen und Veränderungen gem. ITIL-Standard V3

3.4 Transparenz (Art. 5 Abs. 1 lit. a DSGVO)

Der Auftragnehmer hat keine Möglichkeiten die Anwender über Details der Dienstenutzung direkt zu informieren. D. h. der Kunden muss die Transparenzpflicht gegenüber der natürlichen Person (in der Regel der Anwender) übernehmen. Grundlegende Informationen zur Kommunikation mit dem Portal und zum Umgang mit den bei der Nutzung des Dienstes verarbeiteten Metadaten werden vom Auftragnehmer bereitgestellt.

Technische Maßnahmen:

- Cookie-Banner beim Besuch des Portals mit Datenschutzhinweisen

Organisatorische Maßnahmen:

- Prozesse für die Unterstützung und Beantwortung von Datenschutzanfragen
- Besetzung der Rolle „Datenschutzbeauftragter“

- Für dOnlineZusammenarbeit existieren Betriebshandbücher, Notfallpläne und Kontrollen für die Einhaltung der Sicherheitsvorgaben

3.5 Nichtverkettung (Art. 5 Abs. 1 lit. b DSGVO)

Die Nichtverkettung leitet sich aus der Zweckbindung ab. Die Zwecke der personenbezogenen Daten sind uns nicht bekannt, sofern die Daten vom Anwender bei der Dienstnutzung erzeugt oder abgelegt werden. Dennoch ist der Auftragnehmer bemüht Maßnahmen zu etablieren, die diese Forderung unterstützen.

Technische Maßnahmen:

- Trennung von Datenpräsentation und Datenhaltung
- Einteilen der Systeme in unterschiedliche Sicherheitszonen
- Trennung von administrativer und normaler Benutzerkennung

Organisatorische Maßnahmen:

- Möglichkeit der Pseudonymisierung von Benutzerkennungen

3.6 Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

Die personenbezogenen Daten, die verarbeitet werden, werden vom Kunden bzw. dessen Anwendern zur Verfügung gestellt. D. h. der Kunde ist dafür verantwortlich, welche Daten im Dienst dPhoenixSuite abgelegt und damit verarbeitet werden.

3.7 Intervenierbarkeit (Art. 5 Abs. 1 lit. d DSGVO)

Die Umsetzung von Betroffenenrechten ist Aufgabe des Auftraggebers. Der Auftragnehmer verpflichtet sich den Auftraggeber bei der Umsetzung von Betroffenenrechten im jeweils erforderlichen Umfang zu unterstützen.

Organisatorische Maßnahmen:

- ITIL-konforme Prozesse für Anfragen, Änderungen und Fehlerbehebung im Bereich von dPhoenixSuite
- Prozesse zur Erkennung und Nachverfolgung von Datenschutzvorfällen

3.8 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

3.8.1 Datenschutz-Management

Dies umfasst Maßnahmen, die gewährleisten, dass die Maßnahmen zur Sicherheit der personenbezogenen Daten regelmäßig auf Angemessenheit, Wirksamkeit und Vollständigkeit geprüft werden.

Technische Maßnahmen:

- Zentrale Ablage alle betriebsrelevanten Dokumentationen
- Sicherheitszertifizierung eines ISMS nach BSI IT-Grundschutz (Dokumentation des ISMS beim AN mittels HiScout)
- Überprüfung der Wirksamkeit der Schutzmaßnahmen mind. einmal innerhalb von 12 Monaten im Rahmen von IT-Grundschutz-Checks

Organisatorische Maßnahmen:

- Berufung und Stellung eines Datenschutz-Beauftragten
- Regelmäßige Mitarbeiterschulung im Bereich Datenschutz und Informationssicherheit
- Berufung eines Informationssicherheits-Beauftragten
- Bedarfsbedingte Durchführung einer Datenschutz-Folgeabschätzung (DSFA)
- Prozess zur Bearbeitung von Anfragen von Betroffenenrechten
- Regelmäßige Durchführung von Pentests
- Regelmäßige Durchführung von Audits
- Veröffentlichung, Pflege und regelmäßige Kontrolle einer Informationssicherheitsrichtlinie
- Führung des ISMS nach dem PDCA-Zyklus (plan/do/check/act)
- Festschreibung der Rollen- und Verantwortlichkeiten im Bereich Sicherheitsmanagement
- Aktive und ständige Mitarbeiterqualifikationsmaßnahmen für Mitarbeiter mit Verantwortung im Sicherheitsbereich
- Regelungen etablieren, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist
- Archivdaten müssen nach Ablauf der Aufbewahrungsfrist wirksam gelöscht werden
- Keine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind (z. B. wiederbeschreibbare DVDs)
- Aufbewahrung von Archivdaten in spezialisierten Archivsystemen
- Verschlüsselung von Archivdaten
- Nutzung von spezialisierten Datenformaten für die Archivierung von Daten, damit eine langfristige Lesbarkeit der Daten gewährleistet ist
- Software und Prozesse für zentral automatisiertes Life-Cycle-Management
- Bearbeitungsschnittstellen und Zugriff über zentrale IPA

3.8.2 Sicherheitsvorfall-Management

Dies umfasst die Unterstützung bei der zeitnahen Bearbeitung von Sicherheitsvorfällen.

Technische Maßnahmen:

- Regelmäßiges Patchmanagement
- Einsatz von Proxies
- Einsatz von Anti-Malware-Lösungen
- Netzwerksegmentierung mit bedarfsgerechten Kommunikationsbeziehungen

Organisatorische Maßnahmen:

- Prozess zur Erkennung und Meldung von Sicherheitsvorfällen
- Richtlinien für die Mitarbeiter zur verpflichtenden Meldung von Sicherheitsvorfällen
- Prozess für die Nachverfolgung und kontinuierliche Verbesserung von Sicherheitsvorfällen
- Abschluss von Third-Level-Verträgen mit den Herstellern
- Eskalationspfade für Sicherheitsvorfälle und Notfälle

3.8.3 Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DSGVO)

Es gilt für alle Verarbeitungstätigkeiten der Grundsatz des Datenschutzes durch Technikgestaltung („Data protection by Design“) und datenschutzfreundlicher Voreinstellungen („Data protection by Default“).

Technische Maßnahmen:

- Verpflichtende Verschlüsselung für den Benutzer
- Default-Einstellung für Firewalls ist „drop-all“
- Fehlende Möglichkeit der Aufzeichnung von Videokonferenzen (siehe Modul „Videokommunikation“)

Organisatorische Maßnahmen:

- Prozess bei Einführung von neuen Funktionen zur Überprüfung der Voreinstellung auf Sicherheit

3.8.4 Auftragskontrolle (Outsourcing an Dritte)

Diese Maßnahmen gewährleisten dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer diese im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets zu regeln.

Technische Maßnahmen:

- 2-Faktor-Authentifizierung für administrative Zugriffe

- getrennte Datenbankeninstanzen pro Kunde
- Trennung der Nutzerkonten der verarbeitenden Systeme mittels IPA und ACLs
- Trennung der Nutzerverwaltung von Betriebskonten und Anwenderkonten; Kunden verwalten ihre eigenen Benutzerkonten jeweils in einem eigenen LDAP

Organisatorische Maßnahmen:

- Vertragliche Zusicherung der Sicherheitsmaßnahmen
- Definition und Dokumentation der Verantwortlichkeiten bei den Sicherheitsmaßnahmen
- Abschluss von Auftragsverarbeitungsverträgen
- Verpflichtung zur Geheimhaltung
- Sicherheitsüberprüfung der Mitarbeiter und externer Unterstützung
- Fortlaufende Inventarisierung der Versionen von Software und Komponenten
- Bezug von Standardsoftware nur aus vertrauenswürdigen Quellen
- Überprüfung der Wirksamkeit von Maßnahmen bei Dienstleistern mittels Zertifizierungen (z. B. ISO/IEC 27001) oder Durchführung von eigenverantworteten Audits
- Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung
- Der Auftragsverarbeiter muss Prozesse bei der Erkennung von Datenschutzverletzungen haben und diese unverzüglich dem Verantwortlichen im Sinne der DSGVO melden
- Trennung der Datenhaltung in Test-, Qualitätssicherungs- und Produktivsysteme
- Keine Webtracking und/oder Datenanalysewerkzeuge
- Nur technisch essentielle Cookie-Einstellungen für Zwecke des Sitzungsmanagements und der Speicherung von Geräteeinstellungen (Kamera und Mikrofon)

4 Management und Organisation

Mangelhafte Sicherheitsstrukturen beim AN können den reibungslosen Betriebsablauf erheblich gefährden. Es werden deshalb beim AN zur Abwehr spezifische Fachkompetenzen organisatorisch bereitgestellt – dies ist neben dem IT-Verantwortlichen dPhoenixSuite

- der Datenschutzbeauftragte (DSB) – aktuell Herr Dr. Schmid wie auch
- der Informationssicherheitsbeauftragte (ISB) – aktuell Herr Dr. Meints.
- Für Rückfragen zum Thema Informationssicherheit stehen als Sicherheitskoordinatoren Herr Hendrik Jaß und Herr Lutz Seemann bereit

Beide Rollen sind beim AN eingerichtet, aktiv fachlich besetzt und mit Rollen und Verantwortlichkeiten versehen.

Technische Maßnahmen:

- dynamischer Wissenstransfer (fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen)
- Möglichkeiten zur aktiven Fortbildung des DSB und ISB
- Security Reporting: Dokumentation bei Sicherheitsvorkommnissen

Organisatorische Maßnahmen:

- Ständige Stellung eines DSB und eines ISB mit Rollen und Verantwortlichkeiten (Rollen-/Rechtekonzept)
- Organisatorische Angliederung von ISB und DSB als Stabsstellen mit der Möglichkeit direkt an die Unternehmensleitung/Vorstand zu berichten.
- Durchführung von regelmäßigen Audits des DSB IT-Grundschutz-Checks zur Überprüfung der nach Art. 32 DSGVO zur Sicherheit der Verarbeitung umgesetzten Anforderungen (Internes Kontrollsystem)
- Aktive Unterstützung der Zusammenarbeit des DSB mit dem ISB durch die Unternehmensleitung/Vorstand
- Kontakt des DSB mit der zuständigen Landesdatenschutzbehörde, auch zur Meldung und Abstimmung von Datenschutzvorfällen nach Art. 33 und 34 DSGVO (Verletzung der Sicherheit)

Änderungen bedürfen einer schriftlichen Festlegung. Das Dokument wird regelmäßig fortgeschrieben.