Pädagogische Cloud Infrastruktur

20. März 2026

Rahmenbedingungen Pädagogische Infrastruktur-Cloud (PCI)

(PCI-Rahmenbedingungen)

Version 1.0

Pädagogische Cloud Infrastruktur

Inhaltsverzeichnis

1 Präambel und Geltungsbereich

1.1 Diese Vertragsbedingungen (nachfolgend „PCI-Rahmenbedingungen“) regeln die Nutzung der Pädagogischen Cloud-Infrastruktur (nachfolgend „PCI“). Die PCI ist ein länderübergreifendes Vorhaben mit dem Ziel, eine souveräne, flexible, stabile und sichere IT-Infrastruktur als Basis für digitale Bildungsangebote zu schaffen. Sie wird von der govdigital eG (nachfolgend „Auftragnehmer*) bereitgestellt.

1.2 Diese PCI-Rahmenbedingungen richten sich an den Auftragnehmer* sowie:

a) die an der PCI als strategische Partner teilnehmenden Länder der Bundesrepublik Deutschland (nachfolgend als „Verbundpartner*“ bezeichnet) und

b) (i.d.R. kommunale) Schulträger*,

welche pädagogischen Anwendungen (nachfolgend „Fachanwendungen*“) auf der PCI betreiben oder betreiben lassen. Verbundpartner* und Schulträger* werden nachfolgend gemeinsam als „Auftraggeber*“ bezeichnet.

1.3 Die Verbundpartner* regeln ihre Zusammenarbeit sowie die strategische Steuerung der PCI in einer Verwaltungsvereinbarung* und der Geschäftsordnung der PCI*, die die Gremien des Steuerungskreises (SK)* und des Verbundkoordinationsbüros (VKB)* einsetzen. Das VKB* agiert dabei als zentrale operative Schnitt-stelle der Verbundpartner* zum Auftragnehmer*.

1.4 Schulträger* können im Regelfall nur dann Auftraggeber* im Sinne dieser PCI-Rahmenbedingungen werden, wenn die Voraussetzungen einer vergaberechtskonformen In-House-Beauftragung des Auftragnehmers* durch den jeweiligen Schulträger* gegeben sind. Nähere Informationen hierzu können der auf dem PCI-Informationsportal* veröffentlichten Checkliste In-House-Fähigkeit entnommen werden. Unabhängig davon ist es die Pflicht des Schulträgers*, zu prüfen, ob und in welchem Umfang er den jeweiligen PCI-Service* vergaberechtskonform bestellen und nutzen darf.

1.5 Für den Anwendungsbetrieb* der Fachanwendungen* auf der PCI-Plattform* können die Auftraggeber* Dritte beauftragen oder diese Aufgaben selbst wahrnehmen (nachfolgend „Anwendungsbetreiber*“). Der Auftraggeber* ist für das Handeln der von ihm beauftragten Anwendungsbetreiber* wie für eigenes Handeln verantwortlich. Ist der Auftraggeber* selbst der Anwendungsbetreiber*, gelten die Regelungen für Anwendungsbetreiber* für ihn entsprechend in dieser Funktion.

Hinweis: Die mit einem * gekennzeichneten Begriffe werden am Ende dieser PCI-Rahmenbedingungen näher erläutert.

1.6 Die (Weiter-)Entwicklung der Fachanwendung* kann durch einen gesonderten Anwendungsentwickler* erfolgen, der im Auftrag des Auftraggebers* oder des Anwendungsbetreibers* handelt.

1.7 Diese PCI-Rahmenbedingungen regeln das Rechtsverhältnis zwischen dem Auftragnehmer* und dem jeweiligen Auftraggeber*. Die Beziehung zwischen den Auftraggebern* und den von ihnen beauftragten Anwendungsbetreibern* sowie die Beziehung zu den Endnutzern* der Fachanwendungen* (insbesondere Lehrkräfte, Schülerinnen und Schüler und Verwaltungspersonal der Schulen) sind nicht Gegenstand dieser PCI-Rahmenbedingungen, werden aber in bestimmten Pflichten der Auftraggeber* adressiert.

1.8 Die PCI zielt darauf ab, eine gemeinsame, nachhaltige und zukunftsfähige IT-Infrastruktur für das Bildungswesen zu etablieren. Dies umfasst die Bereitstellung von standardisierten Cloud-Services (Infrastructure-as-a-Service (IaaS*) und Platform-as-a-Service (PaaS*) und Software-as-a-Service (SaaS*), nachfolgend gemeinsam als „PCI-Services*" bezeichnet), die Entwicklung gemeinsamer technischer Standards und die Nutzung von Synergieeffekten.

2 Vertragsgegenstand und Leistungsumfang des Auftragnehmers*

2.1 Gegenstand dieser PCI-Rahmenbedingungen ist die Regelung der Rechte und Pflichten im Zusammenhang mit der Bereitstellung der PCI-Plattform* und der PCI-Services* durch den Auftragnehmer* an die Auftraggeber* sowie deren Nutzung durch die Auftraggeber* (bzw. die von ihnen beauftragten Anwendungsbetreiber*) für den Betrieb von Fachanwendungen*.

Leistungsumfang des Auftragnehmers*: Der Auftragnehmer* stellt die PCI-Plattform* bereit und erbringt darauf aufbauend die im Service-Katalog* spezifizierten PCI-Services*. Der Leistungsumfang umfasst im Wesentlichen:

- **Bereitstellung und technischer Betrieb der PCI-Plattform:** Dies beinhaltet die Zurverfügungstellung der mandantenfähigen Cloud-Infrastruktur (basierend auf den Services von Cloud-Service-Providern*), die Konfiguration von standardisierten, gesicherten Landing Zones* für jeden Auftraggeber* sowie den Betrieb der zentralen Netzwerkinfrastruktur. Der technische Betrieb umfasst das Monitoring der verantworteten Komponenten, das Patch-Management sowie angemessene Maßnahmen zur Sicherstellung von Verfügbarkeit* und Sicherheit.
- **Zugangsmanagement und Datenbereitstellung:** Einrichtung der initialen Administratorkonten* für den Auftraggeber* und die von ihm benannten Personen. Zudem wird dem Auftraggeber* bzw. dessen Anwendungsbetreiber* Zugriff auf ausgewählte Monitoring-, Logging- und Verbrauchsdaten ermöglicht.

- **Supportleistungen:** Erbringung von technischem Support für die PCI-Plattform* und die PCI-Services* bei Störungen* der vom Auftragnehmer* verantworteten Infrastruktur (3rd Level Help Desk).
- **Optionale Unterstützungsleistungen:** Nach gesonderter Vereinbarung können zusätzliche, ggf. vergütungspflichtige Leistungen erbracht werden. Dazu zählen insbesondere erweiterte Beratungsleistungen, die Unterstützung bei der Migration von Fachanwendungen* auf die PCI-Plattform* sowie die Bereitstellung von Werkzeugen für Deployment-Prozesse.

Die konkreten Beschreibungen, technischen Spezifikationen und Service Levels (SLA*) für die einzelnen PCI-Services* werden in einer gesonderten Service-Dokumentation* detailliert, die Bestandteil des jeweiligen Nutzungsvertrags* wird**.**

2.3 Abgrenzung der Verantwortlichkeiten:

2.3.1 Bei IaaS* (z.B. Netzwerkinfrastruktur, Objektspeicher) umfasst die Verantwortung des Auftragnehmers* die Bereitstellung der gebuchten Infrastruktur bis zum definierten Übergabepunkt* (z.B. der Management-API oder der Storage-Schnittstelle). Für die Installation, Konfiguration, Wartung und Sicherung aller darauf aufsetzender Software innerhalb der bereitgestellten Ressourcen ist ausschließlich der Auftraggeber* verantwortlich.

2.3.2 Bei PaaS* (z.B. gemanagter Kubernetes-Service, Datenbank-as-a-Service) umfasst die Verantwortung des Auftragnehmers* die Bereitstellung und das Management der PaaS-Umgebung bis zum definierten Übergabepunkt* (z.B. der API des Service). Für die Bereitstellung, Konfiguration, Wartung und Sicherung der auf der PaaS-Umgebung betriebenen Anwendungen, Container und Services ist ausschließlich der Auftraggeber* verantwortlich.

2.3.3 Bei SaaS* (z. B. eine vom Auftragnehmer* bereitgestellte Lernplattform) umfasst die Verantwortung des Auftragnehmers* den vollständigen technischen Betrieb der Anwendung bis zum definierten Übergabepunkt* (in der Regel die URL der Anwendung). Dies schließt die Wartung und Sicherung der Anwendung und der zugrundeliegenden Infrastruktur ein. Für die inhaltliche Verwaltung der Anwendung, die Administration von Endnutzer-Konten und die Einhaltung der Nutzungsbedingungen der jeweiligen Software ist jeweils der Auftraggeber* verantwortlich.

2.3.4 Der Auftraggeber* ist verantwortlich für die Entwicklung, den Inhalt, die fachliche Funktionalität und den Anwendungsbetrieb* der Fachanwendungen*.

2.3.5 Die Verantwortung für den gesamten Support gegenüber den Endnutzern* der Fachanwendungen* (insbesondere 1st-, 2nd- und 3rd-Level-Support sowie fachlicher Support) liegt bei dem jeweiligen Auftraggeber*. Der Auftragnehmer* leistet keinen Support hinsichtlich der Fachanwendungen* gegenüber Endnutzern*.

2.3.6 Für die Einhaltung spezifischer rechtlicher Anforderungen, die sich aus dem Inhalt oder der Nutzung einer Fachanwendung* ergeben (z.B. fachspezifische Datenschutzanforderungen für Schülerdaten über die Basissicherheit der Plattform hinaus, Urheberrechte für Inhalte der Fachanwendung*), ist ausschließlich der Auftraggeber* verantwortlich.

3 Anbahnung der Nutzung, Bestellung und Bereitstellung der PCI-Services*

3.1 Bedarfsklärung und Assessment:

3.1.1 Auftraggeber*, die PCI-Services* für den Betrieb einer Fachanwendung* nutzen möchten, treten hierzu mit dem Auftragnehmer* in Kontakt. Der Kontakt kann dabei über das VKB* vermittelt werden.

3.1.2 Zur detaillierten Erfassung der Anforderungen erhält der Auftraggeber* vom Auftragnehmer* einen Fragebogen. Dieser dient der Konkretisierung der benötigten technischen Komponenten (z.B. Rechenleistung, Speicher, Datenbanken), des Mengengerüsts, Art und Umfang sowie Schutzbedarfs der zu verarbeitenden Daten (insbesondere im Hinblick auf Art der Daten und Kategorien betroffener Personen gemäß Anlage 1 – Auftragsverarbeitung) sowie weiterer relevanter Rahmenbedingungen.

3.1.3 Auf Basis des ausgefüllten Fragebogens und ggf. weiterer gemeinsamer Gespräche (Assessment) erfolgt eine Klärung, welche PCI-Services* für den geplanten Einsatzzweck geeignet sind und benötigt werden.

3.2 Service-Auswahl und Bestellung:

3.2.1 Der Auftragnehmer* stellt dem Auftraggeber* einen Service-Katalog* zur Verfügung, der die aktuell verfügbaren PCI-Services* (IaaS*, PaaS*, perspektivisch SaaS*) mit ihren Leistungsmerkmalen und technischen Spezifikationen beschreibt.

3.2.2 Der Auftraggeber* wählt auf Basis des Assessments und des Service-Katalogs* die für seine Fachanwendung* benötigten PCI-Services* aus.

3.2.3 Die verbindliche Bestellung der ausgewählten PCI-Services* erfolgt durch den Auftraggeber* mittels eines vom Auftragnehmer* bereitgestellten Bestellformulars. Mit Einreichung des Bestellformulars bestätigt der Auftraggeber* die Geltung dieser PCI-Rahmenbedingungen sowie der relevanten Teile der Service-Dokumentation*.

3.2.4 Ein Nutzungsvertrag* über PCI-Services* kommt zustande, wenn der Auftragnehmer* die Bestellung des Auftraggebers* annimmt, in der Regel durch eine Auftragsbestätigung in Textform. Erfolgt innerhalb eines Zeitraums von 60 Tagen keine Bestätigung der Bestellung, ist der Auftraggeber* nicht mehr länger an die Bestellung gebunden.

3.3 Bereitstellung, Prüfung und Inbetriebnahme der PCI-Services*:

3.3.1 Nach Annahme der Bestellung gemäß Ziffer 3.2.4 wird der Auftragnehmer* die beauftragten PCI-Services* für den Auftraggeber* bereitstellen. Der Auftraggeber* und die von ihm benannten Vertreter des Anwendungsbetreibers* erhalten die für den Zugriff und die Nutzung erforderlichen Informationen und initialen Zugangsdaten. Ein vom Auftragnehmer* bereitgestellter "Onboarding-Guide" unter-stützt diesen Prozess.

3.3.2 Der Auftraggeber* wird die bereitgestellten PCI-Services innerhalb einer Frist von 10 Werktagen nach Bereitstellung auf wesentliche Abweichungen von der vertraglich geschuldeten Beschaffenheit und Funktionalität prüfen und dem Auftragnehmer* etwaige wesentliche Mängel schriftlich oder in Textform anzeigen.

3.3.3 Die Vergütungspflicht gemäß Ziffer 7 für die PCI-Services* beginnt mit dem Zeitpunkt der Bereitstellung. Etwaige Mängelansprüche des Auftraggebers* bleiben hiervon unberührt und können unabhängig von einer Prüfung oder Mängelanzeige innerhalb der in Ziffer 3.3.2 genannten Frist geltend gemacht werden.

3.3.4 Der Auftragnehmer* wird Mängel beseitigen, soweit es ihm nicht technisch unmöglich oder wirtschaftlich unzumutbar ist und die jeweiligen PCI-Services* erneut bereitstellen. Im Hinblick auf Leistungen, die im Innenverhältnis ein Cloud-Provider erbringt, z.B. STACKIT, hängt die technische Möglichkeit davon ab, ob und wann der Cloud-Provider eine solche Mängelbeseitigung vornimmt, hierauf hat der Auftragnehmer* möglicherweise keinen Einfluss. Erfolgt die Mängelbeseitigung nicht in angemessener Frist, obwohl der Auftragnehmer* diese beim Cloud-Provider unter Fristsetzung eingefordert hat oder ist diese nicht erfolgreich, und kann deshalb der PCI-Service nicht vertragsgemäß bereitgestellt werden, können Auftraggeber* bzw. Auftragnehmer* den Nutzungsvertrag* außerordentlich kündigen. Für die Prüfung der nachgebesserten Leistung gilt die Prüfungsfrist gemäß Ziffer 3.3.2 entsprechend. Details zum Verfahren können in der Service-Dokumentation* geregelt werden.

3.4 Nutzung der PCI-Services* und Betrieb von Fachanwendungen*:

3.4.1 Der Auftraggeber* ist berechtigt, die beauftragten und bereitgestellten PCI-Services* gemäß diesen PCI-Rahmenbedingungen und der Service-Dokumentation* zu nutzen, um Fachanwendungen* für das Bildungszwecke bereitzustellen und betreiben zu lassen (Vertragszweck). Die Parteien können mit Zustimmung des SK* auch andere Vertragszwecke vereinbaren.

Der Auftraggeber* stellt insbesondere sicher, dass die von ihm oder in seinem Auftrag betriebenen Fachanwendungen* sowie deren Betrieb mit den jeweils geltenden gesetzlichen Bestimmungen (insbesondere dem Datenschutzrecht), den in der Service-Dokumentation* festgelegten spezifischen technischen Anforderungen sowie insbesondere den allgemeinen Regeln für den Anwendungsbetrieb* (siehe PCI-Betriebsrichtlinien*) konform sind.

3.4.2 Der Auftraggeber* verpflichtet die von ihm beauftragten Anwendungsbetreiber* und ggf. Anwendungsentwickler* entsprechend der Regelung nach 3.4.1.

3.4.3 Ein wesentlicher Verstoß gegen die Vorgaben gemäß 3.4.1 und 3.4.2, der trotz entsprechender Abmahnung und Fristsetzung nicht eingestellt wird, berechtigt den Auftragnehmer* zur Aussetzung seiner Leistung. Erfolgt der Verstoß wiederholt und schuldhaft, ist der Auftragnehmer* zudem zur Kündigung des Nutzungsvertrages berechtigt. Eine Abmahnung und Fristsetzung vor der Aussetzung der Leistungen ist entbehrlich, sofern durch den Verstoß der Betrieb der PCI oder der Betrieb des Auftragnehmers, seiner Unterauftragnehmer oder Dritter gefährdet wird oder ein vergleichbarer Notfall vorliegt.

4 Zugangsberechtigung, Nutzerverwaltung und Pflichten der Auftraggeber*

4.1 Verantwortung für den Zugang

Der Auftragnehmer* richtet für den Auftraggeber* initiale Administratorkonten* ein. Der Auftraggeber* ist für sämtliche Aktivitäten, die über seine Konten sowie die seiner Beauftragten (z.B. Anwendungsbetreiber*) erfolgen, verantwortlich. Er ist verpflichtet, Zugangsdaten sicher zu verwahren, vor unbefugtem Zugriff zu schützen und jeden Verdacht auf eine unbefugte Nutzung unverzüglich zu melden.

4.2 Ordnungsgemäße Nutzung und Mitwirkung

Der Auftraggeber* stellt sicher, dass die PCI-Services* nicht missbräuchlich genutzt werden, insbesondere nicht für rechtswidrige Zwecke (einschließlich des Hochladens, Speicherns oder Verbreitens rechtswidriger Inhalte durch Endnutzer*) oder in einer Weise, die die Sicherheit der PCI-Plattform* oder der Systeme Dritter gefährdet. Er ist zudem verpflichtet, alle für den Betrieb seiner Fachanwendungen* relevanten Mitwirkungspflichten, wie sie in diesen PCI-Rahmenbedingungen sowie in der Service-Dokumentation* beschrieben bzw. im Einzelfall mit dem Auftragnehmer* vereinbart werden, rechtzeitig und vollständig zu erbringen.

5 Änderungen von PCI-Services*

5.1 Änderungen von PCI-Services* durch den Auftragnehmer*

Der Auftragnehmer* entwickelt die PCI-Services* stetig weiter. Er ist daher berechtigt, Services anzupassen, zu erweitern oder einzustellen, wenn dies aus technischen, wirtschaftlichen oder sicherheitstechnischen Gründen erforderlich oder sinnvoll ist; eine Verpflichtung zur Unterstützung veralteter (z.B. herstellerseitig abgekündigter) Versionen besteht nicht. Über wesentliche Änderungen, die die Nutzung beeinträchtigen, informiert der Auftragnehmer* die Auftraggeber* rechtzeitig (i.d.R. mit einer Frist von mindestens 30 Tagen). Sollten sich daraus erhebliche Nachteile für den Betrieb einer Fachanwendung* ergeben, suchen die Parteien gemeinsam nach einer Lösung.

5.2 Änderungsanfragen (Change Requests) durch den Auftraggeber*

Der Auftraggeber* kann jederzeit Anpassungen der von ihm gebuchten PCI-Services* anfragen (Change Request). Der Auftragnehmer* prüft die Anfrage in angemessener Frist, im Regelfall spätestens binnen 30 Tagen auf technische Machbarkeit und mögliche Auswirkungen und unterbreitet dem Auftraggeber* gegebenenfalls ein Angebot über die Umsetzung und eventuelle Mehrkosten. Sofern die Prüfung mehr Zeit erfordert, insbesondere aufgrund besonderer Komplexität, wird der

Auftragnehmer dies und die voraussichtliche Prüfdauer dem Auftraggeber spätestens in der o.g. Frist mitteilen. Die Änderung wird wirksam, wenn der Auftraggeber* das Angebot innerhalb von 30 Tagen annimmt.

Hinweis: *Die automatische Skalierung von Ressourcen (z.B. bei Lastspitzen) im Rahmen der Konfiguration eines PCI-Service ist kein Change Request im Sinne dieser Ziffer.*

6 Änderungen dieser PCI-Rahmenbedingungen

6.1 Verfahren zur Änderung: Bei Änderungen dieser PCI-Rahmenbedingungen wird unterschieden zwischen folgenden Fällen:

6.1.1 Wesentliche Änderungen: Dies sind Änderungen, die die Rechte und Pflichten der Vertragsparteien grundlegend berühren (z.B. Änderungen der Haftungsregelungen in Ziffer 11, grundlegende Änderungen der datenschutzrechtlichen Rollen in Ziffer 8, Änderungen der Kündigungsmodalitäten in Ziffer 12). Wesentliche Änderungen bedürfen zu ihrer Wirksamkeit sowohl der Zustimmung des Auftragnehmers* als auch eines Beschlusses des SK* gemäß der Geschäftsordnung der PCI.

6.1.2 Nicht-wesentliche Änderungen: Dies sind alle Änderungen durch den Auftragnehmer*, die nicht unter 6.1.1 fallen, insbesondere redaktionelle Anpassungen und Klarstellungen oder Anpassungen an zwingendes Recht, die keine neuen wesentlichen Pflichten für die Auftraggeber* begründen und Änderungen durch den Cloud-Provider, die zu keiner oder nur einer geringfügigen Leistungseinschränkung führen. Nicht-wesentliche Änderungen können durch den Auftragnehmer* unter angemessener Berücksichtigung der Interessen der Verbundpartner* durchgeführt werden. es sei denn der SK* wider-spricht der Änderung binnen 30 Tagen seit der Ankündigung.

6.2 Ankündigung und Inkrafttreten von Änderungen: Änderungen dieser PCI-Rahmenbedingungen werden allen Auftraggebern* durch den Auftragnehmer* mit einer Frist von mindestens 60 Tagen angekündigt. Zum angekündigten Zeitpunkt treten die geänderten PCI-Rahmenbedingungen für alle Auftraggeber* (sowohl Verbundpartner* als auch Schulträger*) einheitlich in Kraft und ersetzen die bisherige Fassung; dies gilt nicht, wenn für eine Änderung gemäß Ziffer 6.1.1 keine Zustimmung des Auftragnehmers* oder des SK* vorliegt bzw. der SK* einer Änderung gemäß Ziffer 6.1.2 fristgemäß widersprochen hat.

6.3 Rechte der Schulträger* bei wesentlichen Änderungen: Schulträger*, die nicht als Verbundpartner* im SK* vertreten sind, haben im Fall einer wesentlichen Änderung gemäß Ziffer 6.1.1 das Recht, die betroffenen Nutzungsverträge* außerordentlich mit einer Frist von 30 Tagen zum Zeitpunkt des geplanten Wirksamwerdens der Änderungen zu kündigen. Der Auftragnehmer* wird die Schulträger* in der Änderungsmitteilung auf dieses Sonderkündigungsrecht hinweisen.

7 Vergütung

7.1 Pilotphase

Die Vergütung für den Aufbau und Betrieb der PCI während der Pilotphase ist in einem gesonderten EVB-IT Dienstleistungsvertrag zwischen den Verbundpartnern* und dem Auftragnehmer* geregelt. Diese PCI-Rahmenbedingungen begründen daher grundsätzlich keine eigenständigen Zahlungsverpflichtungen. Ausnahmen für Leistungen außerhalb des Projektrahmens oder für neu hinzukommende Auftraggeber* werden gesondert vereinbart.

7.2 Regelbetrieb

Regelungen zu Entgelten für die Nutzung der PCI-Services* nach Ende der Pilotphase werden rechtzeitig vor Übergang in den Regelbetrieb in einer gesonderten Anlage (*Arbeitstitel: PCI-Preisliste*) getroffen.

8 Datenschutz, IT-Sicherheit und Vertraulichkeit

Die nachfolgenden Regelungen lassen weitergehende gesetzliche und regulatorische Anforderungen unberührt.

8.1 Allgemeine Datenschutzgrundsätze und Rollenverteilung

8.1.1 Die Parteien werden die bei der Erbringung der Leistung jeweils auf sie anwendbaren Bestimmungen über den Datenschutz in der jeweils geltenden Fassung einhalten, insbesondere der Datenschutz-Grundverordnung (DSGVO) und der weiteren relevanten Datenschutzbestimmungen. Gelten für den Auftraggeber* anstelle der DSGVO Regelungen des BDSG oder eines Landesdatenschutzgesetzes, verstehen sich Verweise auf die DSGVO in dieser Ziff. 8 als Verweise auf die jeweilige Parallelvorschrift des BDSG bzw. des Landesdatenschutzgesetzes.

8.1.2 Für die Verarbeitung personenbezogener Daten im Rahmen der vom Auftraggeber* (oder dessen Anwendungsbetreibern*) auf der PCI betriebenen Fachanwendungen* ist der jeweilige Auftraggeber* stets der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftraggeber* ist allein verantwortlich für die Rechtmäßigkeit der Datenerhebung und -verarbeitung innerhalb seiner Fachanwendungen* sowie für die Wahrung der Rechte der betroffenen Personen.

8.1.3 Soweit der Auftragnehmer* bei der Erbringung der PCI-Services* personenbezogene Daten im Auftrag eines Auftraggebers* verarbeitet, handelt der Auftragnehmer* als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO. Die detaillierten Rechte und Pflichten der

Parteien im Rahmen dieser Auftragsverarbeitung sind in der als **Anlage 1** beigefügten Vereinbarung zur Auftragsverarbeitung (AVV) gemäß 28 DSG-VO geregelt. Diese Anlage ist wesentlicher Bestandteil dieser PCI-Rahmenbedingungen.

8.2 IT-Sicherheit der PCI-Plattform*

8.2.1 Der Auftragnehmer* sorgt dafür, dass für die Bereitstellung der PCI-Plattform ein angemessenes, dokumentiertes Sicherheitskonzept besteht, das dem Stand der Technik entspricht und bei Bedarf überprüft und angepasst wird. Auf Wunsch des Auftraggebers* kann dieses mit angemessener Ankündigungsfrist durch seinen jeweiligen IT-Sicherheitsbeauftragten beim Auftragnehmer* eingesehen werden, wobei der IT-Sicherheitsbeauftragte durch den Auftraggeber*, soweit dies noch nicht der Fall ist, zur Verschwiegenheit über die konkreten Inhalte, auch gegenüber dem Auftraggeber* selbst, zu verpflichten ist.

8.2.2 Der Auftraggeber* ist für die Sicherheit der von ihm auf der PCI betriebenen Fachanwendungen* und der von ihm oder seinen Endnutzern* auf die PCI eingebrachten Daten innerhalb der Fachanwendung* selbst verantwortlich. Dies beinhaltet insbesondere die sichere Konfiguration der Fachanwendung*, das Management von Benutzerberechtigungen innerhalb der Fachanwendung* und den Schutz vor Schadsoftware auf den Endgeräten der Endnutzer* der Fachanwendung*. Der Auftraggeber* beachtet die PCI-Betriebsrichtlinien* und sonstige Richtlinien zur IT-Sicherheit.

8.2.3 Bei Sicherheitsvorfällen, die die PCI-Plattform* betreffen, ergreift den Auftragnehmer* in Zusammenarbeit mit dem Plattformbetreiber* unverzüglich Maßnahmen zur Analyse, Eindämmung und Behebung und informiert die betroffenen Auftraggeber* in angemessener Weise. Bei Sicherheitsvorfällen, die eine Fachanwendung* betreffen, ist der jeweilige Auftraggeber* für die Bearbeitung zuständig und informiert den Auftragnehmer*, wenn der Vorfall Auswirkungen auf die PCI-Plattform* haben könnte.

8.3 Vertraulichkeit:

8.3.1 Die Parteien sind verpflichtet, alle im Rahmen der Vertragsverhältnisse erlangten vertraulichen Informationen, Unterlagen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln, insbesondere nicht an unberechtigte Dritte weiterzugeben oder anders als zu vertraglichen Zwecken zu verwerten. Die vorgenannte Pflicht zur Vertraulichkeit schränkt jedoch keine Partei darin ein, für sie tätige Personen, die Zugang zu vertraulichen Informationen hatten, in anderen Projekten einzusetzen. Der Erfahrungsaustausch der Parteien* mit und innerhalb der öffentlichen Hand bleibt unbenommen, ebenso wie die Erfüllung gesetzlicher Pflichten, solange die Pflichten gemäß Satz 1 dabei eingehalten werden.

8.3.2 Die Verpflichtung zur Vertraulichkeit gilt nicht für Informationen, die den Parteien bereits rechtmäßig bekannt sind oder außerhalb des Vertrages ohne Verstoß gegen eine Vertraulichkeitsverpflichtung bekannt werden, die offenkundig sind oder rechtmäßig von

Dritten erlangt wurden oder aufgrund gesetzlicher oder behördlicher Anordnung offengelegt werden müssen. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Vertragsverhältnisse fort.

8.3.3 Vertrauliche Informationen sind Informationen, die ein verständiger Dritter als schützenswert ansehen würde, die als vertraulich gekennzeichnet sind, oder die ihrer Natur nach als vertraulich anzusehen sind; dies können auch solche Informationen sein, die während einer mündlichen Präsentation oder Diskussion bekannt werden.

8.4 Rechtsfolgen bei Nichteinhaltung:

Der Auftragnehmer* kann den Nutzungsvertrag* ganz oder teilweise innerhalb angemessener Frist kündigen, wenn ein Auftraggeber* seinen Pflichten gemäß dieser Ziffer 8 schuldhaft innerhalb einer gesetzten angemessenen Frist nicht nachkommt oder diese Pflichten vorsätzlich oder grob fahrlässig verletzt. Soweit sich die Pflichtverletzung auch auf andere Nutzungsverträge auswirkt, können auch diese Verträge entsprechend Satz 1 gekündigt werden. Ein Recht zur Kündigung besteht nicht, wenn es sich um eine unwesentliche Pflichtverletzung handelt.

9 Verfügbarkeit und Service Levels (SLA*)

9.1 Verfügbarkeitszusagen für einzelne PCI-Services* werden ausschließlich in der Service-Dokumentation* festgelegt.

9.2 Der Auftragnehmer* und die Verbundpartner* haben sich darauf verständigt, souveräne Cloud-Service-Provider für die PCI-Plattform* einzusetzen. Diese Entscheidung erfolgte bewusst zugunsten souveräner Anbieter mit hohem Erfüllungsgrad bei IT-Sicherheitsanforderungen und digitaler Souveränität trotz aktuell geringerem Funktionsumfang und Leistungsfähigkeit als bei etablierten Hyperscalern.

9.3 Der Auftraggeber* (bzw. der Anwendungsbetreiber*) meldet Störungen* der PCI-Services* unverzüglich über die vom Auftragnehmer* bekanntgegebenen Meldewege (z.B. Service Desk, Ticketsystem). Die Meldung soll eine möglichst genaue Beschreibung der Störung* und der betroffenen PCI-Services* enthalten. Kann die Störungsursache nach der ersten Analyse des Auftragnehmers* nicht eindeutig einem Verantwortungsbereich zugeordnet werden, sind beide Parteien verpflichtet, bei der weiteren Analyse in angemessenem Umfang und nach Treu und Glauben mitzuwirken. Dies umfasst insbesondere den gegenseitigen Aus-tausch von für die Analyse notwendigen Informationen (z. B. Logdateien, Konfigurationsdaten).

9.4 Weitere Service Level, insbesondere Reaktionszeiten und Wiederherstellungszeiten für verschiedene Störungsklassen werden ggf. in der Service-Dokumentation* definiert.

9.5 Der Auftragnehmer* stellt den Auftraggebern* auf Anfrage oder in regelmäßigen Abständen Berichte über die erreichte Verfügbarkeit* der genutzten PCI-Services* gemäß den Festlegungen in der Service-Dokumentation* zur Verfügung.

10 Nutzungsrechte

10.1 Der Auftragnehmer* räumt dem Auftraggeber* mit Bereitstellung der PCI-Services* das nicht-ausschließliche, zeitlich auf die Vertragslaufzeit beschränkte, nicht unterlizenzierbare und nicht übertragbare Recht ein, die PCI-Services* für die Dauer des jeweiligen Nutzungsvertrages* gemäß diesen PCI-Rahmenbedingungen und der Service-Dokumentation*, unter Berücksichtigung etwaiger im Nutzungsvertrag vorgesehener quantitativer Metriken wie Useranzahl, Volumen etc., für den Betrieb von Fachanwendungen* für den Vertragszweck (vgl. Ziffer 3.4.1) zu nutzen. Diese Fachanwendungen* dürfen demgemäß vom jeweiligen Auftraggeber*, und von ihm berechtigten Nutzern genutzt werden, jeweils naturgemäß jedoch nur insoweit, wie auch für die Fachanwendungen* selbst dafür ausreichende Nutzungsrechte bestehen.

10.2 Das Nutzungsrecht umfasst das Recht, die PCI-Services* durch eigene Beschäftigte sowie durch die vom Auftraggeber* beauftragten Anwendungsbetreiber* jeweils für den Vertragszweck (vgl. Ziffer 3.4.1) nutzen zu lassen. Der Auftraggeber* stellt sicher, dass auch diese Personen die Bestimmungen dieser PCI-Rahmenbedingungen, der PCI-Betriebsrichtlinien* sowie der Service-Dokumentation* einhalten.

10.3 Soweit dem Auftragnehmer* im Rahmen der PCI-Services* Softwarekomponenten (z.B. Betriebssysteme, Datenbanksoftware, Management-Tools) bereitgestellt werden, umfasst das Nutzungsrecht das Recht, diese Software im Rahmen der bestimmungsgemäßen Nutzung der PCI-Services* zu installieren (soweit erforderlich und vorgesehen), zu laden, anzuzeigen und ablaufen zu lassen. Die Lizenzbedingungen Dritter für solche Softwarekomponenten, die in der Service-Dokumentation* ausgewiesen sind, sind vom Auftraggeber* zu beachten.

10.4 Der Auftraggeber* ist nicht berechtigt, die PCI-Services* oder Teile davon über die in Ziffern 10.1 bis 10.3 vorgesehenen Zwecke hinaus zu nutzen, sie zu verändern, zu dekompilieren, zu disassemblieren oder Re-verse Engineering zu betreiben, es sei denn, dies ist gesetzlich zwingend gestattet.

10.5 Alle Rechte an der PCI-Plattform* selbst, an den zugrundeliegenden Technologien und an den vom Auftragnehmer* oder in dessen Auftrag entwickelten Softwarekomponenten verbleiben beim Auftragnehmer* bzw. dessen Lizenzgebern. Durch diese PCI-Rahmenbedingungen werden keine über die hierin ausdrücklich eingeräumten Nutzungsrechte hinausgehenden Rechte an geistigem Eigentum übertragen.

10.6 Das Nutzungsrecht ist auf das Hoheitsgebiet der Bundesrepublik Deutschland beschränkt, es sei denn, in der Service-Dokumentation* ist für bestimmte PCI-Services* eine erweiterte territoriale Nutzungsmöglichkeit vorgesehen. Die Verarbeitung von Daten im Rahmen der PCI-Services* erfolgt gemäß den Regelungen in Ziffer 8 (Datenschutz und IT-Sicherheit).

10.7 Weitergehende Nutzungsrechte an individuellen Arbeitsergebnissen für einzelne Auftraggeber*, z.B. aufgrund gesonderter Verträge, z.B. des Vertrages mit dem Auftragnehmer* über die Errichtung der PCI, bleiben unberührt,

10.8 Der Auftraggeber* stellt den Auftragnehmer* von allen Ansprüchen Dritter (einschließlich der Kosten für eine angemessene Rechtsverteidigung) frei, die diese aufgrund einer rechtswidrigen oder missbräuchlichen Nutzung der PCI-Plattform* oder der PCI-Services* durch den Auftraggeber*, seine Beschäftigten, die von ihm beauftragten Anwendungsbetreiber*, Anwendungsentwickler* oder die Endnutzer* seiner Fachanwendungen* oder aufgrund von Datenschutzverstößen oder Urheberrechtsverletzungen im Zusammenhang mit den vom Auftraggeber* betriebenen Fachanwendungen* gegen den Auftragnehmer* geltend machen, es sei denn, der Auftragnehmer hat die Rechtsverletzung selbst zu vertreten. Die Parteien werden sich bei der Abwehr solcher Ansprüche gegenseitig unterstützen.

11 Haftung

11.1 Der Auftragnehmer* haftet für Schäden, die dem Auftraggeber* durch eine vom Auftragnehmer*, ihren gesetzlichen Vertretern oder Erfüllungsgehilfen vorsätzlich oder grob fahrlässig verursachte Pflichtverletzung entstehen, nach den gesetzlichen Bestimmungen.

11.2 Für einfache Fahrlässigkeit haftet der Auftragnehmer* – außer im Falle der Verletzung des Lebens, des Körpers oder der Gesundheit – nur, sofern wesentliche Vertragspflichten verletzt werden. Wesentliche Vertragspflichten sind solche Pflichten, die die Grundlage des Vertrages bilden, die entscheidend für den Abschluss des Vertrages sind und auf deren Erfüllung der Auftraggeber* vertrauen durfte. Dabei haftet der Auftragnehmer* nur für vorhersehbare Schäden, mit deren Eintreten typischerweise gerechnet werden muss.

11.3 Die Haftung des Auftragnehmers* gemäß Ziffer 11.2 dieser PCI-Rahmenbedingungen ist für die in Ziffer 19 der EVB-IT Cloud-AGB in der bei Abschluss des jeweiligen Nutzungsvertrags* aktuellen Fassung vorgesehenen Fälle zudem begrenzt wie dort geregelt.

11.4 Unbeschadet der vorstehenden Regelungen ist die Haftung des Auftragnehmers* für durch ihre Unterauftragnehmer (insbesondere Plattformbetreiber* und Cloud-Service-Provider*) verursachte Schlecht- oder Nichterfüllung von Leistungen auf die Ansprüche beschränkt, die dem

Auftragnehmer* gegenüber dem jeweiligen Unterauftragnehmer zustehen. Etwaige dem Auftragnehmer zustehende Gutschriften des Cloud-Service-Providers aufgrund von SLA-Verletzungen, reicht der Auftragnehmer* an den Auftraggeber* weiter. Eine weitergehende Haftung des Auftragnehmers* besteht nur, wenn und soweit sie eine Pflichtverletzung bei der Auswahl oder Überwachung des Unterauftragnehmers zu vertreten hat.

11.5 Die Haftung nach dem Produkthaftungsgesetz bleibt von den vorstehenden Regelungen unberührt.

11.6 Der Auftragnehmer* haftet nicht für Schäden, die darauf beruhen, dass der Auftraggeber* oder die von ihm beauftragten Anwendungsbetreiber* ihre Pflichten gemäß diesen PCI-Rahmenbedingungen oder der Service-Dokumentation* verletzen, insbesondere nicht für Schäden, die durch unsachgemäße Nutzung, fehlerhafte Konfigurationen durch den Auftraggeber* oder dessen Anwendungsbetreiber* oder durch unzureichende Sicherung der vom Auftraggeber* oder dessen Anwendungsbetreibern* auf die PCI eingebrachten Daten oder Fachanwendungen* entstehen. Die Haftung des Auftraggebers* im Falle eines Mitverschuldens bleibt unberührt.

12 Laufzeit und Kündigung

12.1 Laufzeit

12.1.1 Soweit nicht anders vereinbart, beginnt der Nutzungsvertrag mit der Annahme der Bestellung des Auftraggebers* durch den Auftragnehmer gemäß Ziffer 3.2.4 und läuft auf unbestimmte Zeit, mindestens jedoch sechs Monate, soweit nicht anders vereinbart.

12.1.2 Die Laufzeit eines Nutzungsvertrages* kann in der Service-Dokumentation* oder im jeweiligen Bestellformular abweichend geregelt werden (z.B. andere Mindestlaufzeiten).

12.2 Ordentliche Kündigung

Die ordentliche Kündigung einzelner Nutzungsverträge* durch den Auftraggeber* oder den Auftragnehmer* richtet sich nach den in der Service-Dokumentation* für den jeweiligen PCI-Service* oder im Nutzungsvertrag* festgelegten Kündigungsfristen und -bedingungen. Sind dort keine spezifischen Regelungen getroffen, kann ein Nutzungsvertrag* über PCI-Services* vom Auftraggeber* mit einer Frist von 30 Kalendertagen gekündigt werden. Für die Kündigung durch den Auftragnehmer* gilt eine Frist von 60 Kalendertagen.

12.3 Außerordentliche Kündigung

Das Recht beider Parteien zur außerordentlichen Kündigung einzelner Nutzungsverträge* aus wichtigem Grund bleibt unberührt. Eine Kündigung aus wichtigem Grund kann nur innerhalb einer angemessenen Zeit ab Kenntnis des Kündigungsgrundes erfolgen.

12.4 **Form der Kündigung**: Jede Kündigung bedarf der Textform.

12.5 **Folgen der Kündigung**

12.5.1 Mit Wirksamwerden der Kündigung eines einzelnen Nutzungsvertrags* über PCI-Services* enden die Nutzungsrechte an diesem spezifischen PCI-Service*.

12.5.2 Der Auftragnehmer* wird dem Auftraggeber* nach Beendigung eines Nutzungsvertrags* über PCI-Services* die vom Auftraggeber* auf den betreffenden PCI-Services* gespeicherten Daten (Inhaltsdaten der Fachanwendungen*) zur Verfügung stellen und anschließend löschen oder diese auf Anforderung des Auftraggebers* ohne vorherige Herausgabe löschen. Der Auftraggeber* ist für die rechtzeitige Sicherung seiner Daten vor Vertragsende verantwortlich.

12.5.3 Pflichten, die ihrer Natur nach auch nach Vertragsende fortbestehen sollen (z.B. Vertraulichkeit, Datenschutzpflichten hinsichtlich noch vorhandener Daten), bleiben von der Kündigung unberührt.

12.6 Unterstützung beim Anbieterwechsel (Data Act)

12.6.1 Der Auftragnehmer* wird den Auftraggeber* auf dessen Wunsch bei einem Wechsel zu einem anderen Anbieter aktiv unterstützen. Dies umfasst die Pflicht, alle zumutbaren und technisch möglichen Maßnahmen zu ergreifen, um offensichtliche und verdeckte Hindernisse für den Wechsel zu beseitigen.

12.6.2 Der Auftragnehmer* stellt sicher, dass der Auftraggeber* nach Beendigung eines Nutzungsvertrags* alle von ihm oder in seinem Namen erzeugten exportierbaren Daten, einschließlich Metadaten, in einem gängigen, strukturierten und maschinenlesbaren Format extrahieren kann.

12.6.3 Die Parteien legen in einem gesonderten Übergangsplan die konkreten Unterstützungsleistungen, Verantwortlichkeiten und den Zeitrahmen für den Wechsel fest. Die Unterstützungsleistungen des Auftragnehmers* können nach Aufwand vergütet werden, es sei denn, es handelt sich um gesetzlich unentgeltlich zu erbringende Leistungen.

13 Migration von Fachanwendungen*

13.1 **Allgemeines:** Die Verantwortung für die Planung, Vorbereitung und Durchführung der Migration einer Fachanwendung* auf die PCI liegt grundsätzlich bei dem jeweiligen Auftraggeber*, der die Fachanwendung* betreiben möchte. Der Auftraggeber* kann hierfür Anwendungsbetreiber* und/oder Anwendungsentwickler* beauftragen.

13.2 **Unterstützung durch den Auftragnehmer*:** Der Auftragnehmer* verfügt während der Pilotphase über ein spezialisiertes Migrationsteam (nachfolgend „PCI-Migrationsteam*“), das den Auftraggeber* und dessen Anwendungsbetreiber* sowie ggf. Anwendungsentwickler* bei der Migration von Fachanwendungen* unterstützen kann. Die Mitglieder dieses Teams (nachfolgend „Migrationslotsen*“) erbringen hierfür Beratungsleistungen, stellen Informationen bereit und leisten technische Unterstützung. Der Auftragnehmer* stellt zudem einen Migrationsleitfaden zur Verfügung, der als Teil der Service-Dokumentation* bereitgestellt wird. Art, Umfang sowie die Vergütung der Unterstützungsleistungen des PCI-Migrationsteams* werden gesondert zwischen Auftraggeber* und Auftragnehmer* vereinbart oder können in der Service-Dokumentation* näher spezifiziert sein.

13.3 **Prozess bei beauftragter Unterstützung**: Wird eine Unterstützung durch den Auftragnehmer* gem. Ziffer 13.2 beauftragt, gelten die folgenden Regelungen zum Prozess:

13.3.1 Vor Beginn einer Migration führt der Auftraggeber* (und/oder dessen Anwendungsbetreiber* bzw. Anwendungsentwickler*) mit Unterstützung des PCI-Migrationsteams* eine Analyse (Assessment) der zu migrierenden Fachanwendung* durch. Diese Analyse umfasst insbesondere die technischen Anforderungen der Fachanwendung*, Abhängigkeiten, Datenschutz- und Sicherheitsaspekte sowie den Migrationsaufwand.

13.3.2 Auf Basis der Analyse erstellt der Auftraggeber* (und/oder dessen Anwendungsbetreiber* bzw. Anwendungsentwickler*) mit Unterstützung durch das PCI-Migrationsteam* einen Migrationsplan, der die Zielarchitektur der Fachanwendung* auf der PCI, die einzelnen Migrationsschritte, Verantwortlichkeiten und einen Zeitplan festlegt.

13.3.3 Die Migration erfolgt daraufhin in enger Abstimmung zwischen dem Auftraggeber* (bzw. dessen Anwendungsbetreiber* und/oder Anwendungsentwickler*) und dem Auftragnehmer* (insbesondere dem PCI-Migrationsteam*). Der Auftraggeber* stellt sicher, dass die Fachanwendung* so angepasst und konfiguriert wird, dass sie den technischen und sicherheitstechnischen Vorgaben der PCI (insbesondere den PCI-Betriebsrichtlinien* und der Service-Dokumentation*) entspricht.

13.3.4 Der Auftragnehmer* stellt die gebuchten PCI-Services* und die Landing Zone* für die Migration und den anschließenden Betrieb bereit.

13.4 **Verantwortung des Auftraggebers* bei beauftragter Unterstützung**: Im Fall einer beauftragten Unterstützung gemäß Ziffer 13.2 bleibt der Auftraggeber* insbesondere dafür verantwortlich, dass:

- alle für die Migration erforderlichen Rechte (z.B. Lizenzen für die Fachanwendung* und darin enthaltene Software Dritter) vorliegen;
- die zu migrierenden Daten korrekt und vollständig sind und während der Migration angemessen geschützt werden, sodass Fehler und Datenverluste ausgeschlossen werden;
- die migrierte Fachanwendung* auf der PCI vor der Produktivsetzung durch den Auftraggeber* oder dessen Anwendungsbetreiber* und/oder Anwendungsentwickler* ausreichend getestet wird. Der Auftragnehmer* führt keine fachliche oder funktionale Abnahme der Fachanwendung* selbst durch;
- die Konfiguration der Fachanwendung* und deren Betrieb den PCI-Betriebsrichtlinien*und der Service-Dokumentation* entspricht und
- alle relevanten Stakeholder (z.B. Endnutzer*, Datenschutzbeauftragte) angemessen über die Migration informiert werden.

14 Schlussbestimmungen

14.1 **Anwendbares Recht**: Diese PCI-Rahmenbedingungen und alle auf ihrer Grundlage geschlossenen Vertragsverhältnisse zwischen dem Auftragnehmer* und dem Auftraggeber* unterliegen ausschließlich dem Recht der Bundesrepublik Deutschland.

14.2 **Gerichtsstand**: Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesen PCI-Rahmenbedingungen und den darauf basierenden Vertragsverhältnissen ist Berlin.

14.3 **Übertragung von Rechten und Pflichten**: Die Übertragung von Rechten und Pflichten aus den Vertragsverhältnissen durch den Auftraggeber* auf Dritte bedarf der vorherigen schriftlichen Zustimmung des Auftragnehmers*. Der Auftragnehmer* ist berechtigt, ihre Rechte und Pflichten aus diesem Vertragsverhältnis ganz oder teilweise auf ein mit ihr verbundenes Unternehmen im Sinne des § 15 AktG oder auf einen Rechtsnachfolger zu übertragen, sofern sichergestellt ist, dass der Dritte die vertraglichen Verpflichtungen vollumfänglich erfüllt und die Interessen des Auftraggebers* gewahrt bleiben. Der Auftragnehmer* wird den Auftraggeber* über eine solche Übertragung rechtzeitig informieren. § 354a HGB bleibt unberührt.

15 Begriffsbestimmungen

Glossar

Administratorkonto	Ein Benutzerkonto mit erweiterten Berechtigungen zur Verwaltung von PCI-Services* im Namen eines Auftraggebers* oder Anwendungsbetreibers*. Es gibt verschiedene Arten von Administratorkonten, zum Beispiel für Infrastrukturadministration, und Anwendungsadministration (bspw. Deployment und Konfiguration).
Anwendungsbetreiber	Eine vom Auftraggeber* beauftragte Stelle (z.B. ein IT-Dienstleister oder eine Organisationseinheit des Auftraggebers* selbst), die eine oder mehrere Fachanwendungen* auf der PCI-Plattform* technisch entwickelt, bereitstellt, konfiguriert und/oder den Anwendungsbetrieb* durchführt. Der Auftraggeber* kann auch selbst die Rolle des Anwendungsbetreibers* wahrnehmen.
Anwendungsbetrieb	Die Gesamtheit der in der Verantwortung des Auftraggebers* liegenden technischen und fachlichen Maßnahmen zum Betrieb einer Fachanwendung* auf der PCI-Plattform* ab dem Übergabepunkt*. Dies umfasst insbesondere die Konfiguration der Fachanwendung*, die Verwaltung ihrer Inhalte sowie die Einrichtung und Verwaltung der Endnutzer* einschließlich des Supports gegenüber diesen.
Auftraggeber	Verbundpartner* sowie perspektivisch ggf. weitere Länder* der Bundesrepublik Deutschland sowie (unter den in Ziffer 1.2 genannten Voraussetzungen) Schulträger*, die mit dem Auftragnehmer* einen Vertrag auf Basis dieser PCI-Rahmenbedingungen über die Nutzung der PCI-Plattform* und der PCI-Services* schließt.
Auftragnehmer	Die govdigital eG, die die PCI-Plattform* bereitstellt und die PCI-Services* an die Auftraggeber* erbringt. Sie ist alleinige Vertragspartnerin der Auftraggeber*. Zur Erfüllung ihrer Aufgaben bedient sie sich insbesondere eines Plattformbetreibers* für den technischen Betrieb der PCI-Plattform* sowie der Leistungen der Cloud-Service-Provider für die PCI-Services*.
Ausfallzeit	Der Zeitraum, in dem ein PCI-Service* ungeplant nicht oder nicht mit den in der Service-Dokumentation* zugesagten wesentlichen Funktionen am Übergabepunkt* zur Verfügung steht. Die genaue Definition und

	Berechnungsmethode für Ausfallzeiten* wird in der Service-Dokumentation* festgelegt.
Bedarfsträger	(Dieser Begriff wird in den AGB aktuell nicht verwendet, da die Verantwortung und die vertraglichen Pflichten auf Ebene des Auftraggebers* gebündelt sind. Intern im Projekt kann dieser Begriff weiterhin für spezifische Organisationseinheiten oder Projekte eines Auftraggebers* verwendet werden, die PCI-Services* nutzen).
Cloud-Service-Provider	Ein Drittanbieter von Cloud-Computing-Ressourcen und -Services (z.B. IaaS*-, PaaS*-Angebote), dessen Leistungen der Auftragnehmer* als Unterauftragnehmer für die Bereitstellung der PCI-Services* nutzt.
Endnutzer	Natürliche Personen, die die auf der PCI betriebenen Fachanwendungen* nutzen, insbesondere Lehrkräfte, Schülerinnen und Schüler sowie sonstiges pädagogisches oder administratives Personal an Schulen oder Bildungseinrichtungen.
EVB-IT Cloud AGB	Die EVB-IT Cloud-AGB stehen unter www.cio.bund.de zur Einsichtnahme bereit.
Fachanwendungen	Pädagogische Softwareanwendungen, Lernplattformen, Schulverwaltungssoftware oder sonstige IT-Anwendungen für den Bildungsbereich, die von einem Auftraggeber* (oder in dessen Auftrag von einem Anwendungsbetreiber*) auf der PCI-Plattform* unter Nutzung der PCI-Services* betrieben werden.
Geschäftsordnung der PCI	Die Geschäftsordnung der PCI legt verbindliche Regelungen zwischen den Verbundpartnern* für die Organisation, Steuerung und Umsetzung des PCI-Vorhabens fest, definiert Zuständigkeiten, Entscheidungsprozesse sowie Kommunikationswege, gewährleistet die effektive Umsetzung der Prinzipien der Governance und dient als Leitfaden für die Zusammenarbeit und den Umgang der Verbundpartner* mit Konflikten, Risiken und Veränderungen im Projektverlauf.
Hyper-Care-Phase	Die Hyper Care Phase ist ein befristeter Zeitraum rund um den Go Live eines PCI-Services, der durch eine erhöhte Überwachung und besondere Aufmerksamkeit im Betrieb gekennzeichnet ist. Sie dient dazu, den stabilen Regelbetrieb eines PCI-Services herbeizuführen.

Infrastructure-as-a-Service (IaaS)	Bei IaaS* stellt der Auftragnehmer* grundlegende IT-Infrastrukturressourcen (wie Rechenleistung, Speicher, Netzwerke) als Services zur Verfügung. Ein Auftraggeber* bzw. Anwendungsbetreiber* installiert und betreibt auf diesen Fachanwendungen*.
Landing Zone	Eine durch den Auftragnehmer* vorkonfigurierte, standardisierte und gesicherte Umgebung innerhalb der Cloud-Infrastruktur der PCI, die einem Auftraggeber* für den Betrieb seiner Fachanwendungen* zugewiesen wird. Sie beinhaltet grundlegende Netzwerk-, Sicherheits- und Governance-Einstellungen.
Migrationslotse	Siehe PCI-Migrationsteam*
Nutzungsvertrag	Der zwischen dem Auftragnehmer* und dem Auftraggeber* auf Basis des Bestellformulars und dieser PCI-Rahmenbedingungen zustande kommende Vertrag über die Bereitstellung und Nutzung spezifischer PCI-Services*.
PCI-Betriebsrichtlinien	Richtlinien, welche verbindliche technische und organisatorische Vorgaben und Empfehlungen für den sicheren und konformen Betrieb von Fachanwendungen* auf der PCI-Plattform* enthalten. Die PCI-Betriebsrichtlinien werden als Teil der Service-Dokumentation* bereitgestellt und sind damit Gegenstand der Nutzungsverträge*. Die jeweils aktuelle Fassung der PCI-Betriebsrichtlinien kann zudem unter *Link hinzufügen a*ufgerufen werden.
PCI-Migrationsteam	Ein von dem Auftragnehmer* eingerichtetes, spezialisiertes Team, das Auftraggeber* und deren Anwendungsbetreiber* bei der Migration von Fachanwendungen* auf die PCI-Plattform* unterstützt. Die Mitglieder des PCI-Migrationsteams* werden als „Migrationslotsen*“ bezeichnet.
PCI-Plattform	Die von dem Auftragnehmer* bereitgestellte und betriebene Gesamtinfrastruktur, bestehend aus der zugrundeliegenden Cloud-Umgebung (inkl. der Services der Cloud-Service-Provider*), den eingerichteten Landing Zones*, der zentralen Netzwerkinfrastruktur sowie den übergreifenden Management-, Sicherheits- und Unterstützungswerkzeugen, auf deren Basis die spezifischen PCI-Services* erbracht und von den Auftraggebern* genutzt werden können.

PCI-Services	Die von dem Auftragnehmer* auf Basis der PCI-Plattform* erbrachten und im Service-Katalog* beschriebenen IT-Services, die Gegenstand der jeweiligen Nutzungsverträge* sind. Dies umfasst insbesondere Services der Modelle Infrastructure-as-a-Service (IaaS*), Platform-as-a-Service (PaaS*) sowie perspektivisch Software-as-a-Service (SaaS*).
Pilotphase	Der initiale, zeitlich begrenzte Betriebsabschnitt der PCI, der dem Aufbau der PCI-Plattform* sowie der Erprobung, der Migration und dem Betrieb von ersten Pilotanwendungen dient. Diese Phase ist durch eine spezifische Projektfinanzierung sowie durch gesonderte Unterstützungsleistungen für Pilotanwendungen gekennzeichnet. Die Pilotphase endet mit dem Übergang in den Regelbetrieb.
Platform-as-a-Service (PaaS)	Bei PaaS stellt der Anbieter standardisierte Services mit Schnittstellen zur Entwicklung, Ausführung und Verwaltung von Anwendungen bereit. Bereitgestellt werden typischerweise Betriebssysteme, Laufzeitumgebungen, Datenbanken und Webserver – inklusive Funktionen wie Mandantenfähigkeit, Skalierung, Zugriffskontrolle und Datenbankzugriff. Der Auftraggeber kann darauf eigene Anwendungen betreiben, hat jedoch keinen Zugriff auf die zugrunde liegende Infrastruktur.
Plattformbetreiber	Ein vom Auftragnehmer beauftragter Dritter, der für den Auftragnehmer den technischen Betrieb der PCI-Plattform* oder wesentlicher Teile davon durchführt. Der Plattformbetreiber* handelt im Auftrag und nach Weisung des Auftragnehmers*.
Schulträger	Die für die Errichtung und die sächliche Unterhaltung von einer oder mehreren Schulen verantwortliche juristische Person des öffentlichen oder privaten Rechts. Öffentliche Schulträger sind in der Regel Gebietskörperschaften (z.B. Kommunen, Landkreise), während freie Schulträger z.B. kirchliche oder andere private Organisationen sein können. Ein Schulträger kann gemäß diesen PCI-Rahmenbedingungen unter den in Ziffer 1.4 genannten Voraussetzungen die Rolle eines Auftraggebers einnehmen.
Service Level Agreement (SLA)	Eine Vereinbarung innerhalb der Service-Dokumentation*, die spezifische Qualitätsmerkmale (Service Levels, z.B. Verfügbarkeit*, Reaktionszeiten*) für einen PCI-Service* definiert.

Service-Dokumentation	Sammelbegriff für alle vom Auftragnehmer* bereitgestellten Dokumente, die die PCI-Services* näher beschreiben und konkretisieren, die im Service-Katalog* gelistet sind. Dazu gehören Service-Beschreibungen, technische Richtlinien, PCI-Betriebsrichtlinien* und die Beschreibung der Technischen und Organisatorischen Maßnahmen (TOM*). Die Service-Dokumentation* ist Bestandteil des jeweiligen Nutzungsvertrags*.
Service-Katalog	Ein Verzeichnis der vom Auftragnehmer* angebotenen PCI-Services* (IaaS*, PaaS*, SaaS*) mit Beschreibung der Leistungsmerkmale, Optionen und technischen Spezifikationen.
Software-as-a-Service (SaaS)	Bei Software-as-a-Service stellt der Auftragnehmer* (oder ein von ihr beauftragter Dritter) Softwareanwendungen bzw. deren Funktionen über das Internet zur Nutzung bereit. Die Software läuft auf PCI-Infrastruktur und die Auftraggeber* greifen auf die Software typischerweise über einen Webbrowser oder eine dedizierte Client-Anwendung zu, ohne in Installation, Wartung oder den Betrieb der Software involviert zu sein.
Steuerungskreis (SK)	Das strategische Entscheidungsgremium der Verbundpartner* gemäß der Geschäftsordnung der PCI, das die übergeordneten Ziele und die Ausrichtung der PCI verantwortet.
Technische und Organisatorische Maßnahmen (TOM)	Die von dem Auftragnehmer* gemäß Art. 32 DSGVO getroffenen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten im Rahmen der PCI-Services*, wie in Anlage 2 (TOM) zu diesen PCI-Rahmenbedingungen und ggf. der Service-Dokumentation* näher beschrieben.
Verbundkoordinationsbüro (VKB)	Die gemäß der Geschäftsordnung der PCI eingerichtete operative Schnittstelle der Verbundpartner*, die deren Zusammenarbeit koordiniert und als zentraler Ansprechpartner für den Auftragnehmer* in strategischen und gebündelten operativen Belangen fungiert.
Verbundpartner	Ein Land der Bundesrepublik Deutschland, das als Mitglied des Steuerungskreises* die strategische Entwicklung der PCI mitgestaltet und sich an der Finanzierung des Pilotprojekts beteiligt.
Verfügbarkeit	Der Prozentsatz der Zeit innerhalb eines definierten Messzeitraums, in dem ein PCI-Service* am Übergabepunkt* vertragsgemäß zur Verfügung steht und

	nutzbar ist. Die genaue Definition und Berechnungsmethode werden in der Service-Dokumentation* festgelegt.
Übergabepunkt	Die definierte technische Schnittstelle, an der der Auftragnehmer* die PCI-Services* dem Auftraggeber* zur Nutzung bereitstellt. • Bei IaaS* ist Übergabepunkt regelmäßig die Schnittstelle der bereitgestellten Infrastruktur-Services (adressiert bspw. durch IP-Adresse, DNS, Storage-Mount-Point/Bucket-URL, APIC/CLI (für Management Services)); • Bei PaaS* ist Übergabepunkt regelmäßig die Programmierschnittstelle (API, adressiert bspw. durch IP/DNS) der gemanagten Plattform (z.B. einer Message Queue). • Bei SaaS* ist der Übergabepunkt regelmäßig die URL zur Anwendung. Näheres zum Übergabepunkt ergibt sich aus der Service-Dokumentation*. Die Verantwortung des Auftragnehmers* für den PCI-Service* endet an diesem Übergabepunkt.

16 Anlagenverzeichnis

Anlage 1: Auftragsverarbeitung gemäß Art. 28 DSGVO

Anlage 2: Technische und Organisatorische Maßnahmen (TOM) des Auftragnehmers*