ERLEBEN, WAS VERBINDET.

# Vertrag
# über IT- Leistungen
# im Projekt
# Corona Warn App

zwischen

der Bundesrepublik Deutschland,
vertreten durch das Bundesministerium für Gesundheit,
Friedrichstraße 108,
10117 Berlin

- nachfolgend "Kunde" genannt -

und

T-Systems International GmbH
Hahnstraße 43
60528 Frankfurt am Main

- nachfolgend "Telekom" genannt -

- nachfolgend gemeinsam "Vertragsparteien" genannt -

## Einleitung

(1) Die Unterbrechung von Infektionsketten ist der wesentliche Mechanismus zur Bekämpfung der weiteren Ausbreitung des Corona-Virus. Digitale Anwendungen können hierbei einen erheblichen Beitrag bei der Identifikation und Information möglicher Kontaktpersonen leisten.

(2) Ein vielversprechender Ansatz hierbei ist die Identifikation und Dokumentation relevanter Kontakte mittels Smartphone/ Bluetooth LE. Die Telekom und SAP Deutschland SE & Co. KG ("SAP") haben sich als Auftragnehmer bereit erklärt, die bisherigen Forschungsergebnisse in ein die fachlichen Anforderungen sowie die Vorgaben an Datenschutz und Informationssicherheit erfüllendes Endprodukt zur überführen und dessen infrastrukturellen Betrieb über die Entwicklungsphase hinaus zu gewährleisten ("Projekt Corona Warn App"). Hierbei besteht ausdrücklich die Offenheit der beiden Auftragnehmer, das Produkt mit weiteren gebotenen Nachentwicklungen auf Basis fachlicher Anforderungen voran zu treiben.

(3) Zusätzlich zu diesem Projektvertrag haben der Kunde und SAP einen Vertrag über Entwicklungs- und Supportleistungen im Projekt Corona Warn App und die Parteien mit SAP eine dreiseitige Abstimmungsvereinbarung geschlossen ("Abstimmungsvereinbarung").

## § 1 Leistungen der Telekom

(1) Die Telekom erbringt für den Kunden die im **Anhang 1** (Leistungsbeschreibung Corona Warn App) zu diesem Vertrag näher beschriebenen IT-Leistungen und den in der Abstimmungsvereinbarung definierten Allgemeinen Anforderungen. Wesentliche Leistung der Telekom ist die Bereitstellung eines Systembetriebs und einer Hotline nach dieser Maßgabe. Die Vertragsparteien sind sich bewusst, dass die Entwicklung und der Betrieb der Corona Warn App sowohl hinsichtlich der spezifischen Anforderungen, der Einbindung Dritter als auch aufgrund der zeitlichen Kritikalität besondere Herausforderungen nicht nur an die Vertragsparteien, sondern an alle an diesem Projekt unmittelbar oder mittelbar Beteiligten stellt und ohne ein zügiges und konstruktives Zusammenwirken aller Beteiligten nicht abgeschlossen werden kann. In der Entwicklungsphase haben die Vertragsparteien aufgrund der zeitlichen Kritikalität und dem fehlenden Projektplanungsvorlauf eine agile Projektvorgehensweise gewählt.

(2) Zur Herstellung der Betriebsbereitschaft gehören auch alle Nebenleistungen, die hierfür erforderlich sind und dem Verantwortungsbereich der Telekom bis zu den jeweils vereinbarten Schnittstellen zuzuordnen sind, d.h. nicht in den Verantwortungsbereich von SAP fallen (Ziffer 1.2 der Leistungsbeschreibung) oder nach diesem Vertrag dem Kunden als Mitwirkungs- oder Beistellungsleistung obliegen oder durch einen Dritten (insbesondere RKI, BSI, BfDI, Labore, Google, Apple) zu erbringen sind.

(3) Die Leistungserbringung setzt die Mitwirkung Dritter voraus, so beispielsweise die anforderungsgerechte Öffnung der Schnittstellen von Seiten der Unternehmen Apple und Google für ihre jeweiligen Betriebssysteme. Soweit und solange die in der Leistungsbeschreibung zu diesem Vertrag beschriebenen Leistungsvoraussetzungen nicht gegeben sind, richten sich die Rechtsfolgen nach § 2 Abs. 1 des Vertrages.

(4) Gehört gemäß **Anhang 1** (Leistungsbeschreibung Corona Warn App) IT-Infrastruktur beziehungsweise Software zum Leistungsumfang, verbleibt diese im Eigentum der Telekom, sofern nachfolgend nicht abweichend geregelt.

(5) Die Telekom setzt bei der Realisierung des Vertrages auch technische Lösungen ein, die auf Basis allgemein angebotener Netzplattformen der Telekom und dritter, insbesondere konzernzugehöriger, Unternehmen produziert werden und bei denen Produkte und Leistungsmerkmale einer ständigen Weiterentwicklung und Überprüfung unterliegen.

(6) Soweit an einzelnen Leistungsmerkmalen der Produkte oder der diesen zugrundeliegenden Netzplattformen technische Modifikationen vorgenommen werden oder Netzdienste, Produkte oder einzelne Leistungsmerkmale nicht mehr zur Verfügung stehen, kann die Telekom verlangen, dass diese Änderungen auch in diesem Vertrag umgesetzt werden. Die Telekom wird den Kunden informieren. Die Umstellung der Leistungen durch die Telekom ist für den Kunden entgeltneutral und darf den vertraglich vereinbarten Leistungsumfang nicht beeinträchtigen. Insbesondere darf durch solche Änderungen der Betrieb des Gesamtsystems nicht beeinträchtigt werden und es darf sich kein Änderungsbedarf hinsichtlich der von SAP und/ oder dem Kunden beizustellenden Teile ergeben, insbesondere nicht hinsichtlich der Corona Warn App und der von SAP entwickelten Teile des Back-Ends.

(7) Die Telekom darf zur Erbringung von Leistungen, die qualitativ oder quantitativ für die Gesamtleistung wesentlich sind, Subunternehmer nur einsetzen oder eingesetzte Subunternehmer nur auswechseln, wenn der Kunde dem ausdrücklich zustimmt. Die Zustimmung des Kunden kann nicht aus sachwidrigen Gründen verweigert werden und hat unverzüglich zu erfolgen, wenn sich unter Berücksichtigung des neuen Subunternehmers anstelle des alten Subunternehmers keine andere Zuschlagsentscheidung ergeben hätte. Die Einarbeitung des neuen Subunternehmers erfolgt auf Kosten der Telekom. Für die folgenden benannten Subunternehmer sowie die Einbindung von verbundenen Unternehmen der Telekom gemäß §§ 15 ff. AktG gilt die Zustimmung des Kunden vorsorglich als erteilt, unabhängig davon, ob diese einen wesentlichen Leistungsanteil erbringen:

acticom GmbH – Engineering / Softwareentwicklung

arago GmbH – Konzeptentwicklung / technische Architektur

Axivas Deutschland GmbH – Call-Center-Dienstleistungen

BS software development GmbH & Co. KG - Laboranbindung

Loodse GmbH – DevOps Engineering für Operations

The Boston Consulting Group GmbH - Projekt- und Prozessmanagement

Die Telekom oder von ihr beauftragte Subunternehmer erbringen die vereinbarten Leistungen, soweit nicht abweichend geregelt, in den Ländern der Europäischen Union. Die Telekom oder von ihr beauftragte Subunternehmer können den Ort der Leistungserbringung nur mit vorheriger Zustimmung des Kunden in Länder außerhalb der Europäischen Union verlagern, soweit Bedingungen dieses Vertrages, insbesondere die Regelungen zum Datenschutz, der Verlagerung nicht entgegenstehen; auf die Zustimmung besteht kein Anspruch.

(8) Service- und Reaktionszeiten

Die Servicezeiten und Reaktionszeiten sind in der Leistungsbeschreibung definiert.

(9) Dokumentations- und Berichtspflichten

Die Telekom dokumentiert die durchgeführten Leistungen zeitnah in angemessener Art und Weise gemäß dem in **Anlage 4 (Dokumentation)** der Abstimmungsvereinbarung vereinbarten Umfang in einem üblichen elektronischen Format und macht sie dem Kunden zu den dort vereinbarten Zeitpunkten zugänglich. Die Telekom ist verpflichtet, zu jeder Zeit Einblick in den aktuellen Stand der Dokumentation zu gewähren.

Auf Verlangen erstattet der Telekom dem Kunden während der Vertragsdauer Bericht über den Stand der Leistungen.

(10) Personal der Telekom

Die zur Erbringung der Leistungen eingesetzten Personen müssen vereinbarungsgemäß, unabhängig davon jedoch mindestens dem Vertragszweck und der Aufgabenstellung entsprechend, qualifiziert sein. Soweit vereinbart, ist die Telekom verpflichtet, für die Erbringung von ggf. geschuldeten Leistungen vor Ort nur Personen einzusetzen, welche bereit sind, sich aufgrund des Verpflichtungsgesetzes verpflichten zu lassen. Die Kommunikation mit dem Kunden erfolgt in deutscher Sprache.

Die Telekom darf zur Vertragserfüllung eingesetzte Personen auch ohne Einwilligung des Kunden, jedoch unter angemessener Berücksichtigung der Interessen des Kunden, durch eine qualifizierte Ersatzperson auswechseln.

Die Ersatzperson gilt nur dann als qualifiziert, wenn sie mindestens über die vertraglich vorausgesetzte Eignung verfügt. Eine für die Leistungserbringung nicht erforderliche höhere Qualifikation der Ersatzperson begründet keinen Anspruch auf Erhöhung der Vergütung. Dies gilt insbesondere auch dann, wenn die Ersatzperson einer teureren Kategorie zuzuordnen wäre. Die durch den Austausch und die Einarbeitung der Ersatzperson entstehenden Kosten gehen zu Lasten der Telekom.

Telekom erklärt sich bereit, die zur Erbringung der Leistungen eingesetzten Personen auf Verlangen des Kunden einer Sicherheitsprüfung zu unterziehen, deren Anforderungen durch den Kunden genehmigt werden müssen. Telekom wird die betroffene Person nur dann mit Diensten zur Erbringung von Leistungen betrauen, sofern diese Sicherheitsprüfung eine volle Unbedenklichkeit der betroffenen Person bescheinigt. Sofern notwendig, wird Telekom die dafür notwendige Zustimmung der betroffenen Person einholen.

(11) Zusammenarbeit der Parteien / Ausschluss von Arbeitnehmerüberlassung und Scheinselbständigkeit

Die Parteien werden durch organisatorische Maßnahmen gewährleisten, dass die im Rahmen der Leistungserbringung eingesetzten Mitarbeiter der Telekom ausschließlich deren jeweiligem Direktionsrecht und Disziplinargewalt unterstehen. Es erfolgt keine Eingliederung des zur Leistungserbringung eingesetzten Mitarbeiters der Telekom in die Organisation des Kunden.

Telekom bestimmt grundsätzlich Ort und Zeit der Leistung selbst. Jedoch sind zeitliche, räumliche und fachliche Anforderungen zu beachten, soweit sie sich aus den zwischen den Parteien abgestimmten Termin- oder Leistungsplänen ergeben oder zur Erreichung des Zwecks der Beauftragung erforderlich sind. Für die zur Erbringung der Leistungen notwendigen Arbeitsmittel ist die Telekom jeweils selbst verantwortlich, soweit nicht anders vereinbart.

## § 2 Mitwirkungsleistungen und Beistellungen des Kunden

(1) Der Kunde wird die in diesem Vertrag beschriebenen sowie die insbesondere aufgrund der agilen Projektvorgehensweise zur ordnungsgemäßen Leistungserbringung erforderlichen Mitwirkungs- und Beistellungsleistungen unentgeltlich erbringen. Die jeweiligen Mitwirkungs- und Beistellungsleistungen ergeben sich im Wesentlichen aus den Anhängen zu diesem Vertrag und den nachfolgenden Absätzen.

(2) Der Kunde wird der Telekom die erforderlichen Informationen und Unterlagen aus seiner

Sphäre rechtzeitig zur Verfügung stellen. Der Kunde wird den Mitarbeitern der Telekom Zugang zu seinen Räumlichkeiten und der dort vorhandenen informationstechnischen Infrastruktur rechtzeitig gewähren und die bei ihm vorhandenen Dokumentationen rechtzeitig übergeben, jeweils soweit dies zur Erbringung der Leistung erforderlich ist und die gesetzlichen und vereinbarten persönlichen Voraussetzungen (z.B. Sicherheitsüberprüfungen nach Sicherheitsüberprüfungsgesetz - SÜG -) erfüllt sind. Kommt der Kunde seinen Mitwirkungsleistungen trotz Aufforderung durch die Telekom nicht, nicht rechtzeitig oder unvollständig nach, kann die Telekom ein Angebot unterbreiten, diese Leistungen (soweit möglich) selbst anstelle des Kunden zu erbringen. Sonstige Ansprüche der Telekom bleiben unberührt.

(3) Die Datensicherung obliegt der Telekom als Teil der unter diesem Vertrag zu erbringenden Leistungen nach Maßgabe der Leistungsbeschreibung.

(4) Die Telekom haftet nicht für eine Beeinträchtigung der Leistungen, insbesondere eine nur eingeschränkte oder verspätete Leistung sowie die Einhaltung von Service Levels, soweit und solange dies darauf beruht, dass der Kunde seine Mitwirkungs- oder Beistellungsleistungen nicht, nicht ordnungsgemäß oder nicht rechtzeitig erfüllt. Verbindlich vereinbarte Termine und Meilensteine verschieben sich um einen angemessenen Zeitraum, soweit vereinbarte Mitwirkungs- oder Beistellungsleistungen nicht, nicht ordnungsgemäß oder nicht rechtzeitig erfüllt werden. Die Telekom ist gleichwohl bemüht, die betroffenen Leistungen gegen Erstattung der hierdurch entstehenden nachgewiesenen Mehraufwände vertragsgemäß zu erbringen, und wird den Kunden unverzüglich nach Erkennen darauf hinweisen, wenn vereinbarte Mitwirkungs- oder Beistellungsleistungen nicht, nicht ordnungsgemäß oder nicht rechtzeitig erfüllt werden.

(5) Sofern eine Mitwirkung des Kunden nicht in zwischen den Parteien abgestimmten Zeit- oder Projektplänen festgehalten ist, hat die Telekom den Kunden so rechtzeitig auf die zu erbringende Mitwirkung hinzuweisen, dass die vereinbarte Leistungserbringung nicht gefährdet wird. Sofern eine Mitwirkung des Kunden nach Auffassung der Telekom nicht oder nicht rechtzeitig oder nicht ordnungsgemäß erfolgt und diese für die vereinbarte Leistungserbringung wesentlich ist, wird die Telekom den Kunden hierauf hinweisen.

## § 2A Auditrechte des Kunden

(1) Der Kunde ist berechtigt, bei Telekom Prüfungen in Bezug auf die Einhaltung der vertraglichen Pflichten und den Anforderungen an Datenschutz und Datensicherheit sowie die Vergütung und Abrechnung selbst oder durch von ihm beauftragte Prüfer vorzunehmen ("**Audit**"). Alle Audits werden, sofern der Zweck eines Audits nicht ein anderes Vorgehen zwingend erfordert und zwischen den Parteien vereinbart wurde, während der für Telekom üblichen Geschäftszeiten (09:00 Uhr - 17:00 Uhr, Montag - Freitag, ausgenommen bundeseinheitliche Feiertage und Feiertage des Bundeslandes, in dem das Audit durchgeführt werden soll) durchgeführt. Der Prüfungsablauf wird zwischen den Parteien vorab mit einer Frist von mindestens drei (3) Wochen vereinbart. Das Audit ist unter Angabe des Orts und des Prüfungsgegenstands mindestens vier (4) Wochen vorher schriftlich anzukündigen.

(2) Telekom hat alle Audits gemäß ihrem Verantwortungsbereich gegenüber dem Kunden bezüglich ihrer operativen, infrastrukturellen, system- und fachbezogenen sowie prozessualen Aufgaben und Kenntnisse sowie in einer der Zielsetzung des jeweiligen Audits hinreichenden Weise und Umfänglichkeit zu unterstützen, soweit gesetzliche Gründe, Rechte Dritter, insbesondere hinsichtlich des Schutzes personenbezogener Daten, oder andere berechtigte Gründe wie beispielsweise Geschäftsgeheimnisse einer Bereitstellung von Informationen nicht entgegenstehen. Insbesondere ist der Zugriff auf Plattformen ausgeschlossen, die auch für Dritte

genutzt werden, soweit der Zugriff auf Informationen Dritter nicht mit angemessenem Aufand ausgeschlossen werden kann. Die Verpflichtung zur Bereitstellung von Informationen schließt nicht die Pflicht zur Übergabe von Unterlagen, Dokumentationen etc. ein. Es genügt vielmehr die Gewährung der Einsicht in diese Unterlagen, Dokumentationen etc. und die Möglichkeit, Kopien anzufertigen.

(3) Die Mitwirkungen der Telekom beim Audit werden nach Aufwand vergütet.

(4) Soweit ein vom Kunden beauftragter Auditor nicht von Berufs wegen zur Verschwiegenheit verpflichtet ist, kann die Gewährung des Zutritts zum Betrieb oder die Bereitstellung von Informationen von einer zuvor vereinbarten Verpflichtung zur vertraulichen Behandlung der gewährten Informationen abhängig gemacht werden; alternativ kann der Kunde erklären, dass er für den von ihm beauftragten Auditor als seinen Erfüllungsgehilfen haftet. Gegenüber direkten Wettbewerbern der Telekom kann die Gewährung des Zutritts und die Bereitstellung von Informationen verweigert werden.

(5) Die Parteien stellen innerhalb ihrer Verantwortungsbereiche sicher, dass alle Audits in einer die Geschäftsabläufe der Telekom schonenden Weise durchgeführt werden.

## § 3 Demonstration der Betriebsbereitschaft

(1) Vor der Aufnahme des Wirkbetriebs erfolgt nach der Betriebsbereitschaftserklärung der Telekom eine Funktionsprüfung des Gesamtsystems durch den Kunden unter Beiziehung von SAP als Entwickler der Corona Warn App, des Bundesdatenschutzbeauftragten, des Bundesamtes für Informationssicherheit (BSI) sowie des Robert-Koch-Instituts (RKI); der Kunde kann verlangen, dass weitere Parteien sowie Bundes- oder Landesbehörden beigezogen werden. Bei der Demonstration der Betriebsbereitschaft werden die in der Leistungsbeschreibung beschriebenen Kriterien für die Betriebsbereitschaft geprüft. Eine Aufnahme des Wirkbetriebs erfolgt erst nach Abschluss der Prüfung und der Freigabe durch den Kunden. Die Details sind in der Abstimmungsvereinbarung geregelt.

(2) Das Gesamtsystem im Sinne dieser Regelung umfasst nicht nur die Leistungen der Telekom, sondern die Beistellungen des Kunden nach § 3 sowie der in der Leistungsbeschreibung beschriebenen, für den Betrieb der Corona Warn App erforderlichen Systemkomponenten Dritter.

(3) Die Prüfung des Gesamtsystems führt zu keiner Erweiterung der Leistungspflichten der Telekom nach § 1, insbesondere resultiert aus ihr keine Gesamtverantwortung der Telekom für die Betriebsbereitschaft des Gesamtsystems. Auch stellt die Prüfung des Gesamtsystems keine Abnahme nach § 640 BGB dar.

(4) Die Leistungen von SAP sind vom Kunden im Rahmen der Funktionsprüfung des Gesamtsystems gegenüber SAP abzunehmen. Die Telekom unterstützt und berät den Kunden bei der Abnahme der Leistungen gegenüber SAP. Insbesondere wird die Telekom die in der Leistungsbeschreibung vereinbarten Tests durchführen und den Kunden bei der Durchführung von Funktions- und Abnahmetests gegenüber SAP, einschließlich vorbereitender Tests im Rahmen der Entwicklung und Herstellung der Betriebsbereitschaft beraten und unterstützen. Die Telekom übernimmt es ferner, festgestellte Mängel und Fehlfunktionen der von SAP entwickelten Teile des Gesamtsystems direkt an SAP zu melden, deren Behebung durch SAP zu überwachen und die Korrekturen für die Übernahme in die Produktivumgebung freizugeben (einschließlich Test in einer Nicht-Produktivumgebung) und die Übernahme der korrigierten Leistungsbestandteile in das Produktivsystem technisch abzuwickeln. Der Kunde ist dabei über alle wesentlichen Schritte zu informieren und muss dem Abruf kostenpflichtiger Leistungen von SAP im Voraus

zustimmen, sofern der Kunde oder SAP die Telekom auf die Kostenpflicht hinweisen.

## § 4 Nutzung durch Dritte

Eine - auch teilweise - Untervermietung von IT-Infrastruktur oder sonstige Gebrauchsüberlassung an Dritte ist nur mit Erlaubnis der Telekom gestattet, soweit dies nicht dem Zweck der vereinbarten Leistungen entspricht. Die Erlaubnis ist zu erteilen, wenn die Nutzung durch Dritte für Zwecke der Bekämpfung der Covid-19-Pandemie zweckdienlich ist und darf im Übrigen nur aus wichtigem Grund verweigert werden. Die Telekom behält sich vor, die Erlaubnis aus wichtigem Grund zu widerrufen. Die Nutzung durch die Corona Warn App–Nutzergruppe gemäß § 5 Abs. 1 dieses Vertrags ist unwiderruflich gestattet. Die Übertragung der Durchführung dieses Vertrags an das RKI gilt nicht als Untervermietung oder Gebrauchsüberlassung im vorstehenden Sinn.

## § 5 Nutzungsrechte an Software

(1) Definition der Corona Warn App–Nutzergruppe

Zu der Corona Warn App-Nutzergruppe gehören alle Ministerien und Behörden des Bundes, der Länder und der Kreise und Kommunen, alle bestimmungsgemäßen Nutzer der App sowie alle anzuschließenden Testlabore und die beteiligten anderen Dienstleister einschließlich SAP.

(2) Nutzungsrechtseinräumung durch Kunden an beigestellter Software

Der Kunde räumt der Telekom das nicht ausschließliche, nicht übertragbare, an Subunternehmer unterlizenzierbare, örtlich unbeschränkte und zeitlich auf die Dauer dieses Vertrages beschränkte Recht ein, die vom Kunden auf der bereitgestellten IT-Infrastruktur eingesetzte oder der Telekom beigestellte Software bzw. einzelne Elemente derselben (hierzu zählen ebenfalls z.B. Lichtbilder oder Marken) und die vom Kunden bzw. den bestimmungsgemäßen Nutzern der Corona Warn App und der Corona Warn App-Nutzergruppe auf der bereitgestellten IT-Infrastruktur gespeicherten Daten und Inhalte im Rahmen der Erfüllung der vertraglichen Leistungspflichten zu nutzen, insbesondere zu vervielfältigen. Vervielfältigungen und die Nutzung der angefertigten Kopien dürfen vor allem zu Sicherungs- und Backup-Zwecken vorgenommen werden.

Soweit der Kunde auf der bereitgestellten Infrastruktur Software einsetzt oder der Telekom beistellt, die unter Anwendung einer Open-Source-Lizenz entwickelt wurde, gelten die Bestimmungen der Open-Source-Lizenz auch im Verhältnis zwischen dem Kunden und der Telekom, sofern die Lizenzbedingungen der Telekom bekannt gegeben wurden. Der Telekom ist bekannt, dass die von SAP entwickelten Teile unter der Open Source-Lizenz Apache 2.0 veröffentlicht werden.

Soweit die Telekom für den Kunden eine Internet-Website hostet, räumt der Kunde der Telekom das nicht ausschließliche, nicht übertragbare, weltweite, zeitlich und auf die Dauer dieses Vertrages beschränkte Recht zur Übermittlung der Daten und Inhalte, der Website oder einzelner Elemente der Website über die Telekommunikationsanbindung an die Öffentlichkeit in der Weise ein, dass Dritte zu jeder von ihnen beliebig gewählten Zeit und von jedem beliebig von ihnen gewählten Ort Zugang hierzu haben.

Die Telekom ist nicht berechtigt, die vom Kunden beigestellte Software über die nach Maßgabe dieses Vertrages erlaubte Nutzung hinaus zu nutzen oder von sonstigen Dritten nutzen zu lassen. Die Telekom ist außerdem nicht berechtigt, die Software über die nach Maßgabe dieses

Vertrages erlaubte Nutzung hinaus sonstigen Dritten oder der Öffentlichkeit zugänglich zu machen. Insbesondere ist es der Telekom nicht gestattet, die Software oder Teile davon zu veräußern oder zeitlich begrenzt zu überlassen, vor allem nicht zu vermieten oder zu verleihen.

(3) Nutzungsrechtseinräumung an von Telekom bereitgestellter Software

Soweit der Kunde von Telekom bereitgestellte Software nutzt und in den Anhängen keine abweichende Regelung erfolgt, gilt Folgendes:

Serverbasierte Software:

a.) Die bestimmungsgemäßen Nutzer der Corona Warn App und die Corona Warn App-Nutzergruppe erhalten das nicht ausschließliche, auf die Nutzungszeit bzw. Vertragslaufzeit beschränkte Recht, auf die Softwarefunktionalitäten via Internet oder sonstiger Telekommunikationsverbindung zuzugreifen. Darüberhinausgehende Rechte erhält der Kunde nicht.

b.) Der Kunde ist nicht berechtigt, die Software über die nach Maßgabe dieses Vertrages erlaubte Nutzung hinaus zu nutzen oder von Dritten nutzen zu lassen oder Dritten zugänglich zu machen. Insbesondere ist es dem Kunden nicht gestattet, die Software oder Teile davon zu vervielfältigen oder zu veräußern.

c.) Der Kunde hat auch die Preise zu zahlen, die durch die befugten Nutzer entstanden sind. Gleiches gilt im Fall der unbefugten Nutzung durch sonstige Dritte, wenn und soweit der Kunde diese Nutzung zu vertreten hat.

Clientbasierte Standardsoftware für Corona Warn App:

a.) Der Kunde erhält das nicht ausschließliche, auf die Vertragslaufzeit beschränkte Recht, den in die Corona Warn App integrierten Softwareclient durch Unterlizenzierung an die bestimmungsgemäßen Nutzer der Corona Warn App auf deren Endgerät zur Nutzung über die Appstores von Apple und Google (oder deren Nachfolgeeinrichtungen) zur Verfügung zu stellen und zu verbreiten. Der Kunde erhält ferner alle Rechte, die ggf. darüber hinaus erforderlich sind, um die Appstores zu nutzen und die Corona Warn App unter iOS und Android zu veröffentlichen und zu nutzen.

b.) Der Kunde wird das RKI (als Herausgeber der Corona Warn App) dazu verpflichten, die Corona Warn App zum Ende der Vertragslaufzeit aus den Appstores von Apple und Google zu löschen.

(4) Nutzungsrechtseinräumung an für den Kunden erstellte Individualsoftware

Soweit nach § 1 zum Leistungsumfang der Telekom die Erstellung einer Software für den Kunden vorgesehen ist (Individualsoftware), wird die Individualsoftware unter Anwendung einer Open Source Lizenz (Apache 2.0) erstellt. Der Kunde erhält die Rechte entsprechend den zugrundeliegenden Open-Source Lizenzbestimmungen.

## § 6 Rechte Dritter

Macht ein Dritter gegenüber dem Kunden Ansprüche wegen der Verletzung von Schutzrechten durch die Leistungen der Telekom geltend und wird deren Nutzung hierdurch beeinträchtigt oder untersagt, haftet die Telekom im Rahmen der Haftungsgrenzen gemäß § 9 unbeschadet der sonstigen Rechte des Kunden wie folgt:

(1) Die Telekom kann nach ihrer Wahl und auf ihre Kosten entweder die Leistungen so ändern oder ersetzen, dass sie das Schutzrecht nicht verletzen, aber im Wesentlichen

doch den vereinbarten Funktions- und Leistungsmerkmalen in für den Kunden zumutbarer Weise entsprechen, oder den Kunden von Ansprüchen gegenüber dem Schutzrechtsinhaber im Rahmen der Haftungsgrenzen gemäß § 9 freistellen.

(2) Ist die Änderung und der Ersatz der Telekom unmöglich oder nur zu unverhältnismäßigen Bedingungen möglich, hat sie das Recht, die betroffenen Leistungen gegen Erstattung der entrichteten Vergütung zurückzunehmen. Die Telekom hat dem Kunden dabei eine angemessene Auslauffrist zu gewähren, es sein denn, dies ist nur zu unzumutbaren rechtlichen oder sonstigen Bedingungen möglich.

(3) Die Parteien werden sich wechselseitig unverzüglich über geltend gemachte Ansprüche Dritter verständigen. Der Kunde wird die behauptete Schutzrechtsverletzung nicht anerkennen und jegliche Auseinandersetzung einschließlich etwaiger außergerichtlicher Regelungen entweder der Telekom überlassen oder nur im Einvernehmen mit der Telekom führen. Die Telekom erstattet dem Kunden notwendige Verteidigungskosten und sonstige Schäden, soweit dem Kunden aus Rechtsgründen die geeigneten Abwehrmaßnahmen und Vergleichsverhandlungen vorbehalten bleiben bzw. bleiben müssen. Der Kunde hat in diesem Fall Anspruch auf einen Vorschuss in Höhe der geschätzten Verteidigungskosten.

(4) Soweit der Kunde die Schutzrechtsverletzung selbst zu vertreten hat, sind Ansprüche gegen die Telekom ausgeschlossen.

Dieser § 6 einschließlich des Verweises auf die Haftungsgrenzen gemäß § 9 gilt entsprechend, wenn Dritte gegenüber der Telekom Ansprüche wegen der Verletzung von Schutzrechten durch die vertragsgemäße Verwendung von Mitwirkungs- oder Beistellungsleistungen des Kunden durch die Telekom geltend machen und deren Nutzung hierdurch beeinträchtigt oder untersagt wird.

## § 7 Entgelt und Zahlungsmodalitäten

(1) Der Kunde zahlt für die Leistungen der Telekom die in dem **Anhang 2** (Leistungsverzeichnis) zu diesem Vertrag festgelegten Entgelte zuzüglich Umsatzsteuer in der jeweils gesetzlich bestimmten Höhe.

(2) Eine Aufrechnung ist nur mit unbestrittenen oder rechtskräftig festgestellten Ansprüchen möglich. Ein Zurückbehaltungsrecht kann nur wegen Gegenansprüchen aus diesem Vertragsverhältnis geltend gemacht werden.

(3) Soweit eine Vergütung nach Aufwand vereinbart ist, gilt Folgendes:

(a) Es wird lediglich der Zeitaufwand vergütet. Reisezeiten, Reisekosten, Materialkosten und/oder Nebenkosten werden entsprechend der vertraglichen Vereinbarung gegen Nachweis vergütet. Vom Kunden zu vertretende Wartezeiten der Telekom werden wie Arbeitszeiten vergütet. Die Telekom muss sich jedoch das anrechnen lassen, was sie durch die Nichterbringung seiner Leistung erspart oder durch anderweitige Verwendung seiner Dienste erwirbt oder zu erwerben böswillig unterlässt. Die Zahlung einer Vergütung nach Aufwand setzt von der Telekom geführte Nachweise über die Leistungen und die weiteren geltend gemachten Kosten, z.B. entsprechend **Anhang 5** (Muster Leistungsnachweis) voraus.

(b) Es werden nur die für die jeweilige Leistung vereinbarten bzw. abgerufenen Kategorien vergütet. Ist für eine Leistung keine bestimmte Kategorie vereinbart, werden nur die Kategorien vergütet, die zur Erfüllung erforderlich sind. Satz 1 und 2 gelten auch dann,

wenn die Leistung durch eine Person erbracht wird, die einer teureren als der erforderlichen Kategorie zuzuordnen ist.

(c) Ist bei Vergütung nach Aufwand eine Obergrenze vereinbart, teilt die Telekom dem Kunden jeweils im Rahmen der Rechnungsstellung unaufgefordert die bislang in Rechnung gestellte Summe der Vergütung und die verbleibende Differenz zur vereinbarten Obergrenze mit. Unabhängig hiervon ist der Telekom auch bei Überschreitung der Obergrenze zur vollständigen Erbringung der vereinbarten Leistung verpflichtet. Dies gilt nicht, wenn die Telekom die Überschreitung nicht zu vertreten hat. Die Telekom ist jedoch in diesem Fall verpflichtet, die vereinbarte Leistung gegen zusätzliche Vergütung nach Aufwand zu den vereinbarten Sätzen vollständig zu erbringen, sofern der Kunde dies über das Change Request-Verfahren gemäß § 13 verlangt.

(d) Je Kalendertag wird nicht mehr als ein Tagessatz vergütet, soweit nichts anderes vereinbart ist.

(e) Ein vereinbarter Tagessatz kann nur dann in Rechnung gestellt werden, wenn mindestens acht Zeitstunden geleistet wurden. Werden weniger als acht Zeitstunden pro Tag geleistet, sind diese anteilig in Rechnung zu stellen. Ist ein Stundensatz vereinbart, werden angefangene Stunden anteilig vergütet.

(f) Soweit der Kunde nicht ausdrücklich zugestimmt hat oder etwas anderes vereinbart wurde, sind Leistungen nur in den Zeiten zu erbringen, für die weder ein Zuschlag noch ein anderer erhöhter Vergütungssatz vereinbart ist. Wird die Telekom ohne eine solche Zustimmung oder Vereinbarung tätig, kann sie weder einen Zuschlag noch einen erhöhten Vergütungssatz verlangen. Für Leistungen bis zum Go-Live gilt die Zustimmung des Kunden bis auf Weiteres als erteilt.

(4) Eine fällige Vergütung ist innerhalb von 30 Tagen nach Zugang einer prüffähigen Rechnung zu zahlen, soweit nichts anderes vereinbart ist.

(5) Eine Erhöhung der Vergütung kann erstmalig 12 Monate nach Vertragsbeginn, weitere Erhöhungen frühestens jeweils 12 Monate nach Wirksamwerden der vorherigen Erhöhung erfolgen. Die Erhöhung hat angemessen und nicht entgegen der für die Leistung relevanten Markttendenz zu sein und darf maximal 3% der zum Zeitpunkt der Ankündigung der Erhöhung geltenden Vergütung betragen.

## § 8 Mängelansprüche

(1) Telekom gewährleistet die Funktionsfähigkeit der Leistungen nach diesem Vertrag mit ihren in den Leistungsbeschreibungen benannten Eigenschaften und im Einklang mit den in der Abstimmungsvereinbarung definierten Allgemeinen Anforderungen für die Vertragslaufzeit.

(2) Bei mangelhafter Leistung stellt die Telekom den vertragsgemäßen Zustand nach ihrer Wahl durch Neulieferung oder Nachbesserung gemäß den Regelungen der einschlägigen Leistungsbeschreibung wieder her. Nicht vertragsgemäß erbrachte Leistungen sind vertragsgemäß nachzuholen, sofern das jeweils noch möglich ist.

(3) Der Kunde ist für den Fall der Überschreitung vereinbarter Reaktionszeiten berechtigt, für jeweils angefangene 25% Überschreitung der Reaktionszeit innerhalb der Servicezeiten sowie jeweils für den Fall einer Unterschreitung von einer vereinbarten Verfügbarkeit um 10% eine Vertragsstrafe in Höhe von 1% der monatlichen Vergütung der betroffenen Leistungsgruppe maximal jedoch 5% der monatlichen Vergütung der betroffenen Leistungsgruppe pro Ver-

zugsfall bzw. Unterschreitungsfall zu verlangen. Dies gilt nicht, soweit die Telekom die Überschreitung nicht zu vertreten hat. Insgesamt darf die Summe der aufgrund dieser Regelung pro Monat zu zahlenden Vertragsstrafe nicht mehr als 10% der monatlichen Gesamtvergütung betragen.

§ 341 Abs. 3 BGB findet mit der Maßgabe Anwendung, dass die Strafe bis zum Ablauf von drei Monaten seit ihrer Verwirkung geltend gemacht werden kann. Die Summe aller zu zahlenden Vertragsstrafen beträgt maximal 5% des Auftragswertes. Die Vertragsstrafen werden auf Minderungsansprüche angerechnet.

(4) Bei Unterschreitung der vereinbarten Verfügbarkeit um mehr als 10%, steht dem Kunden darüber hinaus ein Recht zur angemessenen Minderung der Vergütung der jeweils betroffen Leistung bis zu maximal 50% der vereinbarten monatlichen Vergütung in dem Monat der Unterschreitung zu.

(5) Für Zwecke der Absätze (3) und (4) gelten folgende Definitionen:

| | |
|---|---|
| Auftragswert | Der Auftragswert ist die Summe aller Vergütungen aus dem Vertrag. |
| Leistungsgruppe | Die unter Ziff. 3 des Anhangs 1 (Leistungsbeschreibung Corona-Warn-App) unter den Ziff. 3.1 bis Ziff. 3.9 bezeichneten Leistungen stellen jeweils eine Leistungsgruppe dar. |
| Reaktionszeit | Zeitraum, innerhalb dessen die Telekom mit der Leistung zu beginnen hat. Der Zeitraum beginnt mit dem Zugang der entsprechenden Meldung oder Eintritt des vereinbarten Ereignisses während der vereinbarten Servicezeiten und läuft ausschließlich während der vereinbarten Servicezeiten. Geht eine Meldung außerhalb der vereinbarten Servicezeiten ein oder tritt das vereinbarte Ereignis außerhalb der Servicezeiten ein, beginnt die Reaktionszeit mit Beginn der nächsten Servicezeit. |
| Servicezeit | Zeiten, innerhalb derer der Kunde Anspruch auf vertraglich geschuldete Leistungen durch die Telekom hat. |
| Verfügbarkeit | Wie in den Leistungsbeschreibungen definiert. |

(6) Angaben zu Eigenschaften der Leistungen, technische Daten und Spezifikationen in diesem Vertrag und seinen Anhängen dienen allein der Beschreibung der jeweiligen Leistung. Sie sind nicht als Garantie (oder zugesicherte Eigenschaft) im Sinne des Bürgerlichen Gesetzbuches anzusehen. Garantieversprechen werden von der Telekom nicht abgegeben.

(7) Mängelansprüche nach diesem Vertrag verjähren 1 (ein) Jahr nach Beginn der gesetzlichen Gewährleistungsfrist.

(8) Für die Haftung auf Schadensersatz gelten die nachstehenden Bestimmungen gemäß § 9.

## § 9 Haftung

Die Haftung der Telekom, gleich aus welchem Rechtsgrund, für alle Ansprüche auf Schadens- und Aufwendungsersatz sowie Freistellungsansprüche aus und im Zusammenhang mit diesem Vertrag, ist wie folgt begrenzt:

(1) Die Telekom haftet bei Vorsatz unbeschränkt.

(2) Bei grob fahrlässig verursachten Schäden haftet die Telekom jedoch insgesamt maximal wie folgt:

(a) Für Schäden, die bis GOLIVE verursacht werden, bis zur Höhe der für Leistungen im Zeitraum bis zum GOLIVE zu zahlenden Vergütung.

(b) Für Schäden, die im Zeitraum ab GOLIVE bis zum 31.05.2021 verursacht werden, bis zur Höhe der für Leistungen in diesen Zeitraum zu zahlenden Vergütung.

(c) Für Schäden, die in einem der Verlängerungszeiträume verursacht werden, bis zur Höhe der für Leistungen im jeweiligen Verlängerungszeitraum zu zahlenden Vergütung.

(d) Für Schäden, die nach Vertragende verursacht werden, bis zu maximal EUR 5 Mio.

Maßgeblich ist dabei jeweils der Zeitpunkt des schadensverursachenden Ereignisses (Handlung oder Unterlassen), nicht der Zeitpunkt des Schadenseintritts.

(3) Bei einfach fahrlässig verursachten Schäden gilt Abs. (2) entsprechend mit der Maßgabe, dass die jeweiligen Haftungshöchstbeträge um 50% reduziert werden.

(4) Die Haftung für entgangenen Gewinn ist ausgeschlossen.

(5) Ein Schadensereignis bezeichnet auch mehrere Schäden aus derselben Ursache oder Schäden aus Ursachen, die in einem unmittelbaren zeitlichen und räumlichen Zusammenhang stehen, wobei es sich jedoch um eine einheitliche Einwirkung handeln muss.

(6) Ansprüche nach dem Produkthaftungsgesetz werden ausschließlich nach den Bestimmungen dieses Gesetzes geregelt.

(7) Für den Verlust von Daten haftet Telekom nur, soweit der Kunde seine Daten in anwendungsadäquaten Intervallen in geeigneter Form sichert, damit diese mit vertretbarem Aufwand wiederhergestellt werden können; dies gilt nicht, soweit die Telekom vertraglich zur Sicherung der Daten verpflichtet ist.

(8) Zahlungen nach dem Produkthaftungsgesetz werden auf eventuelle Schadensersatzansprüche angerechnet, soweit sie auf dasselbe Schadensereignis zurückzuführen sind.

(9) Der Kunde ist verpflichtet, Schäden, Verluste und Mängel unverzüglich schriftlich anzuzeigen.

(10) Die Beschäftigten der Vertragsparteien haften der anderen Vertragspartei persönlich nur bei Vorsatz.

## § 10 Vertragsbeginn, -laufzeit und –beendigung, Rücktritt

(1) Der Vertrag tritt mit seiner Unterzeichnung durch beide Vertragsparteien rückwirkend zum 1. April 2020 in Kraft. Details der Leistungsbereitstellung werden in den Anhängen geregelt.

(2) Der Vertrag hat eine Laufzeit bis zum 31.05.2021. Der Kunden erhält die Option, den Vertrag zweimal um jeweils weitere 12 Monate zu verlängern. Die Optionen müssen jeweils spätestens vier Monate vor Ablauf der jeweiligen Vertragslaufzeit durch schriftliche Mitteilung ausgeübt werden.

(3) Das Recht einer Vertragspartei, den Vertrag aus wichtigem Grund vorzeitig zu kündigen, bleibt unberührt.

Als wichtiger Grund gilt insbesondere, wenn über das Vermögen einer Vertragspartei das Insolvenzverfahren beantragt oder eröffnet oder die Eröffnung des Insolvenzverfahrens oder eines vergleichbaren Verfahrens nach der Insolvenzordnung mangels Masse abgelehnt wird.

(4) Alle Kündigungen nach diesem Vertrag haben schriftlich und mittels eingeschriebenen Briefes

zu erfolgen.

(5) Soweit in den Anhängen keine abweichende Regelung getroffen wurde, wird die Telekom bei Beendigung dieses Vertrages alle im Rahmen der Datensicherung zu sichernden Daten für den Kunden dreißig Kalendertage zur Abholung bereithalten. Der Kunde wird drei Werktage vor Abholung dem Ansprechpartner der Telekom schriftlich mitteilen, wer die zur Abholung bestimmte Person ist. Sollte der Kunde innerhalb der vorgenannten Frist die Daten nicht abholen, wird die Telekom die Daten auf allen Datenträgern vernichten. Die Datensicherungspflicht der Telekom endet in jedem Fall mit Beendigung dieses Vertrages.

(6) Pflichten nach Vertragsende

(a) Mit Vertragsende hat die Telekom unverzüglich und auf Anforderung des Kunden sämtliche vom Kunden erhaltenen Daten, physischen Unterlagen, Hilfsmittel, Materialien oder Gegenstände herauszugeben, die ihm zum Zwecke der Vertragsausführung bestimmungsgemäß nicht dauerhaft überlassen wurden. Dies gilt auch für alle Kopien. Des Weiteren sind alle Leistungsergebnisse und im Auftrag verarbeiteten Daten in jeder Form an den Kunden auf Anforderung zu übergeben, soweit nicht bereits geschehen.

(b) Der Kunde ist berechtigt, an Stelle der Herausgabe ganz oder teilweise die sichere Löschung oder Vernichtung zu verlangen, soweit technisch möglich und zumutbar. Diese ist dem Kunden auf Verlangen und nach seiner Wahl durch entsprechende Erklärung oder anderweitig nachzuweisen. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

(c) Die Telekom unterstützt den Kunden auf Anfrage in angemessenem Umfang gegen Vergütung nach Aufwand bei der Überführung des Betriebs auf einen Nachfolgedienstleister, insbesondere in Bezug auf die Migration des Gesamtsystems und der Daten.

## § 11 Höhere Gewalt

(1) Für Ereignisse höherer Gewalt, die der Telekom die vertragliche Leistung wesentlich erschweren, die ordnungsgemäße Durchführung des Vertrages zeitweilig wesentlich behindern oder unmöglich machen, haftet die Telekom nicht, soweit diese unvorhersehbar, schwerwiegend und durch die Telekom unverschuldet sind, nach Abschluss dieses Vertrages eintreten und soweit die Behinderung oder Unmöglichkeit nicht durch angemessene, dem anerkannten Stand der Technik entsprechende Vorkehrungen seitens der Telekom hätte verhindert werden können. Als höhere Gewalt gelten insbesondere Naturkatastrophen, Regierungsmaßnahmen, Behördenentscheidungen, Blockaden, Krieg und andere militärische Konflikte, Mobilmachung, innere Unruhen, Terroranschläge, Streiks, Aussperrungen und andere Arbeitsunruhen, Beschlagnahmen sowie Embargos. Pandemien können grundsätzlich ebenfalls ein Ereignis höherer Gewalt darstellen. Die Covid-19 Pandemie gilt jedoch in dem bei Vertragsschluss bekannten Ausmaß nicht als höhere Gewalt. Dies gilt auch für zukünftige Beschränkungen aufgrund der Covid-19 Pandemie in dem bisherigen Umfang und Ausmaß, auch wenn diese bei Vertragsschluss bereits wieder aufgehoben waren.

(2) Soweit eine der Vertragsparteien an der Erfüllung ihrer vertraglichen Verpflichtungen gehindert wird und nach Absatz (1) nicht haftet, gilt dies nicht als Vertragsverstoß, und die im Vertrag oder aufgrund des Vertrages festgelegten Fristen werden entsprechend der Dauer des Hindernisses angemessen verlängert. Gleiches gilt in Bezug auf Vorleistungen Dritter, soweit

die Telekom auf die Vorleistung Dritter angewiesen ist.

(3) Jede Vertragspartei wird alles in ihren Kräften stehende unternehmen, was erforderlich und zumutbar ist, um das Ausmaß der Folgen, die durch die höhere Gewalt hervorgerufen worden sind, zu mindern. Die von der höheren Gewalt betroffene Vertragspartei wird der anderen Vertragspartei den Beginn und das Ende des Hindernisses jeweils unverzüglich schriftlich anzeigen.

(4) Minderungsansprüche und Einreden des Kunden bleiben von diesem § 11 unberührt. Sobald feststeht, dass die höhere Gewalt länger als 6 (sechs) Monate andauert, ist jede Vertragspartei berechtigt, den Vertrag zu kündigen.

## § 12 Governance

Es gelten die Bestimmungen der Abstimmungsvereinbarung.

## § 13 Vertragsänderungsverfahren (Change Request Verfahren)

(1) Es gelten die Bestimmungen der Abstimmungsvereinbarung.

(2) Sofern Telekom erkennen kann, dass Grundannahmen gemäß Ziff. 1.4 des Anhangs 1 (Leistungsbeschreibung Corona-Warn-App) voraussichtlich überschritten werden, informiert Telekom den Kunden unter Nennung der näheren Umstände sowie der angenommenen Folgen und stellt einen Change Request gemäß Ziff. 7.2 der Abstimmungsvereinbarung.

(3) Zur Klarstellung: Telekom ist zur fortlaufenden Leistungserbringung innerhalb der in Ziff. 1.4 des Anhangs 1 (Leistungsbeschreibung Corona-Warn-App) definierten Volumina auch bei Überschreitung der Grundannahmen während eines laufenden Change Request-Verfahrens verpflichtet.

## § 14 Vertraulichkeit, Datenschutz und Datensicherheit

(1) Die Vertragsparteien werden die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz beachten. Die Telekom wird insbesondere die Verpflichtung der Mitarbeiter auf Vertraulichkeit und das Fernmeldegeheimnis nach § 88 TKG vornehmen.

Soweit Telekom für den Kunden personenbezogene Daten im Auftrag gemäß Art. 28 Datenschutzgrundverordnung (Auftragsverarbeitung) verarbeitet, gelten die Regelungen der Vereinbarung zur Auftragsverarbeitung gemäß Anhang 4.

(2) Die der anderen Vertragspartei übergebenen Unterlagen, Kenntnisse und Erfahrungen dürfen ausschließlich für die Zwecke dieses Vertrages verwendet werden. Darüber hinaus vereinbaren die Vertragsparteien Vertraulichkeit über den Inhalt dieses Vertrages und über die bei dessen Abwicklung gewonnenen Erkenntnisse zu wahren.

(3) Die Vertragsparteien verpflichten sich, geheim zu haltende Informationen nicht Dritten gegenüber zu offenbaren. Keine Dritten sind verbundene Unternehmen der Vertragspartner i.S.d. §§ 15 ff AktG, sowie Subunternehmer, sofern diese zu entsprechender Geheimhaltung verpflichtet wurden.

(4) Die Verpflichtung zur Geheimhaltung und Nichtverwertung der gegenseitig mitgeteilten Informationen entfällt,

(a) gegenüber der SAP, dem RKI, dem BSI, dem BfDI sowie weiteren nach den Regelungen in der Abstimmungsvereinbarung in die Projektorganisation einbezogenen Dritten,

(b) soweit diese der informierten Vertragspartei vor der Mitteilung nachweislich bekannt waren, oder der Öffentlichkeit vor der Mitteilung bekannt oder allgemein zugänglich waren,

(c) oder der Öffentlichkeit nach der Mitteilung ohne Mitwirkung oder Verschulden der informierten Vertragspartei bekannt oder allgemein zugänglich werden,

(d) oder im Wesentlichen Informationen entsprechen, die der informierten Vertragspartei zu irgendeinem Zeitpunkt von einem berechtigten Dritten offenbart oder zugänglich gemacht wurden,

(e) oder kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet worden ist bzw. zur Durchsetzung von Rechtsansprüchen dient. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens, die zur Offenlegung vertraulicher Informationen führen könnten, bestehen, wird die an dem Verfahren beteiligte Vertragspartei die andere Vertragspartei – wenn und soweit rechtlich zulässig - hierüber unverzüglich informieren und – wenn und soweit rechtlich zulässig - eine Offenlegung der vertraulichen Information nicht ohne eine solche vorherige Information durchführen.

(f) oder seit der Beendigung dieses Vertrags 2 (zwei) Jahre verstrichen sind.

(5) Die Telekom gewährleistet eine ordnungsgemäße Datenverarbeitung sowie die Einhaltung technischer und organisatorischer Maßnahmen zur Datensicherheit gemäß der bei Telekom eingesetzten Standards und Technologien, mindestens aber gemäß des jeweils anerkannten Stands und der jeweils anerkannten Regeln der Technik, insbesondere zur Sicherstellung der Vertraulichkeit und Integrität der verwendeten Daten. Auf Wunsch des Kunden wird ihn die Telekom über die Maßnahmen näher informieren. Weitergehende Pflichten gemäß der Leistungsbeschreibung bleibt unberührt.

(6) Der Kunde ist nicht berechtigt, Zugang zu den Räumlichkeiten der Betriebsstätten zu verlangen. Hiervon unberührt bleiben gesetzliche und gesonderte vertragliche Kontrollrechte des Kunden.

(7) Der Kunde erklärt sich damit einverstanden, als Referenz genannt zu werden.

(8) Telekom stimmt einer Veröffentlichung der Vertragseckdaten inklusive der vereinbarten Vergütung in einem Amtsblatt zu.

## § 15 Außenwirtschaftsbestimmungen

(1) Die Vertragsparteien sind sich einig, dass die Leistungen unter dieser Vereinbarung den jeweils geltenden Bestimmungen des deutschen Außenwirtschaftsrechts, der europäischen Außenwirtschaftsverordnungen und US-Amerikanischen Exportregularien unterliegen können. Die Vertragsparteien verpflichten sich, die anwendbaren exportrechtlichen Bestimmungen in ihrem jeweiligen Verantwortungsbereich zu beachten und ggf. notwendige Genehmigungen eigenverantwortlich einzuholen.

(2) Werden notwendige Genehmigungen nicht oder verspätet durch die Außenwirtschaftsbehörden erteilt, ist - soweit gesetzlich möglich - eine Haftung der Telekom für daraus resultierende Schäden sowie sonstige Ansprüche ausgeschlossen. Im Falle der Nichterteilung von Genehmigungen entfällt die Leistungsverpflichtung der Telekom. Im Falle der verspäteten Erteilung von

Genehmigungen werden die im Vertrag als verbindlich vereinbarten Termine und Meilensteine entsprechend der Verspätung angemessen verlängert.

(3) Auf Anfrage werden die Vertragsparteien der jeweils anderen Partei erforderliche Dokumente und Informationen zur Erteilung außenwirtschaftsrechtlich notwendiger Genehmigungen zur Verfügung zu stellen.

## § 16 Schlussbestimmungen

(1) Für die vereinbarten Beziehungen gilt deutsches Recht unter Ausschluss des UN-Kaufrechtes.

(2) Sämtliche Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag oder über dessen Gültigkeit ergeben, wird als ausschließlicher Gerichtsstand Bonn vereinbart, sofern keine gesetzlichen ausschließlichen Gerichtsstände bestehen.

(3) Frühere mündliche oder schriftliche Vereinbarungen zwischen den Vertragsparteien in Bezug auf den Vertragsgegenstand sind mit dem Inkrafttreten dieses Vertrages gegenstandslos.

Dieser Vertrag umfasst die gesamten bis zum Vertragsabschluss zwischen den Vertragsparteien bezüglich des Vertragsgegenstandes getroffenen Vereinbarungen. Die Rechte und Pflichten der Vertragsparteien sind insoweit ausschließlich in dem Vertrag und seinen Anhängen festgelegt.

(4) Die Übertragung dieses Vertrags oder von Rechten und Pflichten aus diesem Vertrag ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig. Die Vertragsparteien sind sich darüber einig, dass die vorgenannte Zustimmung nicht unbillig verweigert werden darf. Die Abtretung von Geldforderungen der Telekom bedarf weder der Anzeige noch der Zustimmung des Kunden. Das Bundesministerium für Gesundheit kann die Durchführung dieses Vertrages durch schriftliche Mitteilung an die Telekom an das RKI übertragen und wieder an sich ziehen, ohne dass dies der Zustimmung der Telekom bedarf. Hierzu wird Telekom – soweit erforderlich – die Zugänge, Benutzergruppen und Rechtestrukturen einrichten, bestehende Dokumentation an RKI übergeben und Vertreter des RKI in die Dokumentation einweisen sowie weitere Unterstützungsleistungen in angemessenem Umfang erbringen.

(5) Die Anhänge sind Teil des Vertrages. Im Falle von Widersprüchen zwischen den Anhängen und einer der Bestimmungen des Hauptteils dieses Vertrages (Vertragsregelungen) gelten die Vertragsregelungen vorrangig; dies gilt nicht in Bezug auf Anhang 1 (Leistungsbeschreibung) und Anhang 4 (Vereinbarung zur Auftragsverarbeitung), die im Fall von Widersprüchen den Vertragsregelungen vorgehen. Im Falle von Widersprüchen zwischen diesem Vertrag und der Abstimmungsvereinbarung gilt die Abstimmungsvereinbarung vorrangig.

(6) Änderungen oder Ergänzungen des Vertrages oder seiner Anhänge zum Vertrag bedürfen der Schriftform und sind von beiden Vertragsparteien zu unterzeichnen. Dies gilt auch für diese Schriftformvereinbarung selbst.

(7) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen dadurch nicht berührt. Die Vertragsparteien werden die unwirk-

same Bestimmung unverzüglich durch eine solche wirksame ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt. Entsprechendes gilt im Falle einer Vertragslücke.

(8) Dieser Vertrag ist in 2 (zwei) Exemplaren, von denen jede Vertragspartei eines erhält, ausgefertigt. Die Vertragsparteien dürfen den Vertrag übersetzen, jedoch ist die deutsche Originalfassung maßgebend.

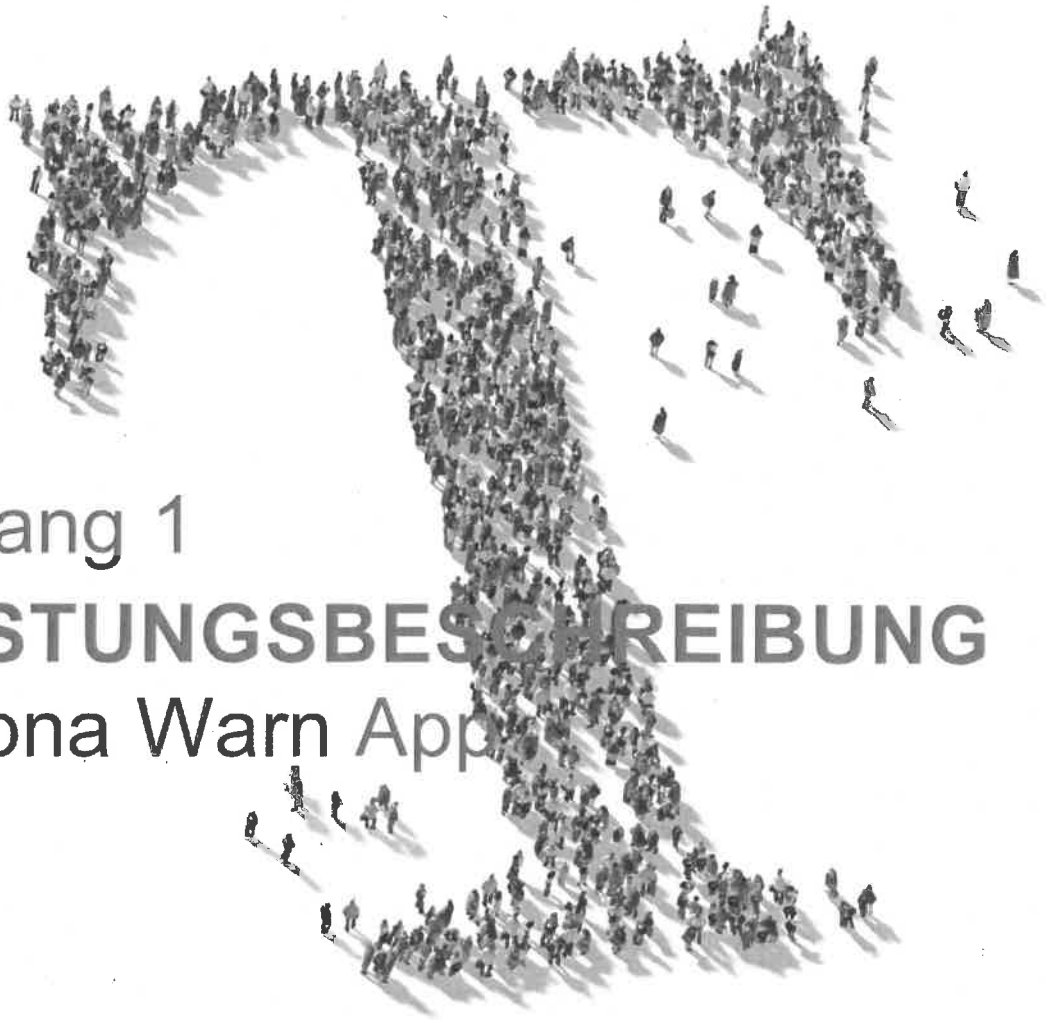
Anhänge:

Anhang 1 – Leistungsinformation Corona Warn App
Anhang 2 – Vergütung
Anhang 3 – [entfallen]
Anhang 4 – Vereinbarung zur Auftragsverarbeitung
Anhang 5 – Muster Leistungsnachweis

BMG

| Kunde | Telekom |
|---|---|
| Berlin 11.06 2020 | |
| Ort, Datum | Ort, Datum |
| i.V. | Adel Al-Saleh Digital unterschrieben von Adel Al-Saleh Datum: 2020.06.09 10:41:59 +02'00' |
| Unterschrift | Unterschrift |
| Dr. Thomas Steffen | |
| Name | Name |

| | |
|---|---|
| | Ort, Datum |
| | Peter Lorenz Digital unterschrieben von Peter Lorenz Datum: 2020.06.09 09:39:59 +02'00' |
| | Unterschrift |
| | Name |



# Anhang 1
# LEISTUNGSBESCHREIBUNG
# Corona Warn App

**Empfänger**
Bundesministerium für Gesundheit

von T-Systems International GmbH

**Angebotsnummer:** 1000820722
**Angebotsdatum:** 05.06.2020

T · · Systems ·

# Informationen zum Angebot

| | |
|---|---|
| An | Bundesministerium für Gesundheit<br>Friedrichstraße 108, 10117 Berlin |
| Über | Leistungsinformation Corona Warn App |
| Von | T-Systems International GmbH<br>BA Public & Healthcare<br>Hahnstr.43<br>60528 Frankfurt am Main |

| **Ansprechpartner** | |
|---|---|
| Kontakt | [redacted] |
| Telefon | [redacted] |
| Fax | [redacted] |
| E-Mail | [redacted] |

| | |
|---|---|
| **Angebotsnummer** | 1000820722 |
| **Angebotsdatum** | 05.06.2020 |

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# 1 EINLEITUNG

Die Telekom bietet dem Bundesministerium für Gesundheit (BMG) im Rahmen der Eindämmung der Corona Pandemie folgende Leistungen im Zusammenhang mit der Erstellung und dem Betrieb einer Corona Warn App an.

- Development Verifikation
- Betriebs- und Netzwerkleistungen
- Hotline-Services
- IT-Sicherheit und Datenschutz
- Projektmanagement
- Beratungsleistungen Europäische Interoperabilität

Die Spezifikation der Systemarchitektur des Gesamtsystems der Corona-Warn-App, für das die Telekom Teilleistungen erbringt, ist als Anlage 1 zur Abstimmungsvereinbarung beigefügt und gilt ergänzend zu dieser Leistungsbeschreibung.

## 1.1 Leistungserbringung

Die Telekom entwickelt und betreibt den Verifikationsserver, Lab Server und Portal Server und erbringt Betriebs- und Netzleistungen sowie Hotline-Services. Neben den weiteren Beteiligten wie dem RKI, dem BSI und dem Bundesdatenschutzbeauftragten ist hier von besonderer Bedeutung die SAP AG als weiterer Vertragspartner des BMG. Die Telekom berücksichtigt diese Struktur in ihrer Projektorganisation.

Für die Leistungspakete der Telekom werden neben den Leistungspflichten auch Annahmen und Rahmenbedingungen, Mitwirkungsleistungen und Beistellungen des Kunden sowie Dritter detailliert beschrieben.

## 1.2 Abgrenzung der Leistungsanteile Telekom / SAP

Die Abgrenzung der Leistungserbringung zwischen Telekom und SAP ist in folgendem Übersichtsbild auf Komponentenebene dargestellt.

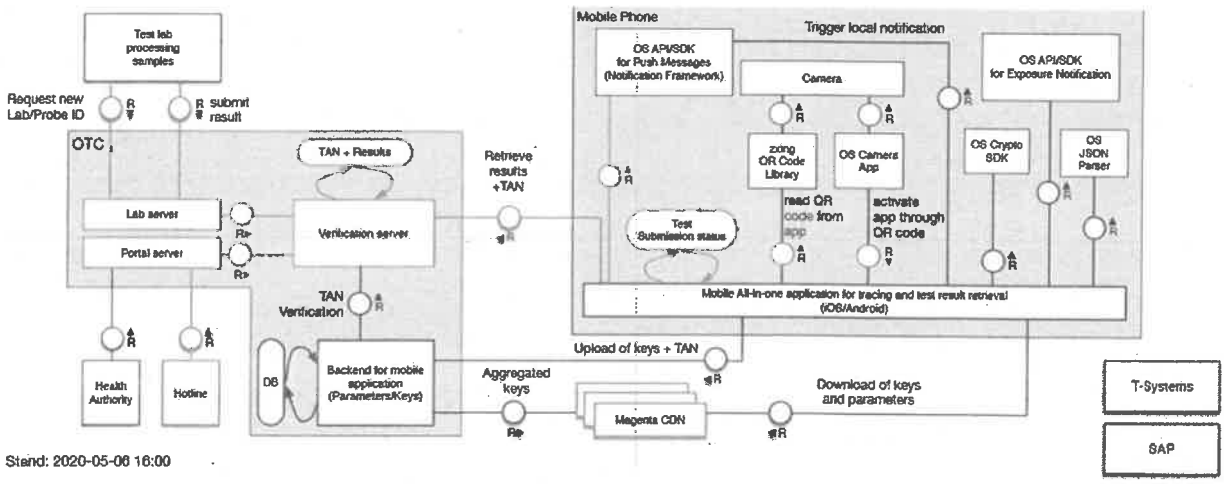



Abbildung 1: Übersicht Gesamtarchitektur

Die magenta gekennzeichneten Leistungskomponenten werden durch die Telekom erbracht.

Die blau gekennzeichneten Leistungen werden durch den Partner SAP erbracht und sind nicht Bestandteil dieser Leistungsinformationen.

## 1.3 Derzeitige zeitliche Planung

Der folgende Zeitplan stellt den vorläufigen Zeitplan unter Berücksichtigung der Planungen der SAP dar. Eine detaillierte Unterscheidung der Leistungen einschließlich Abhängigkeiten und Bedingungen wie zum Beispiel Zulieferungen und Mitwirkungen der Beteiligten ist hier nicht abgebildet. Eine Detaillierung wird im weiteren Projektverlauf stattfinden.

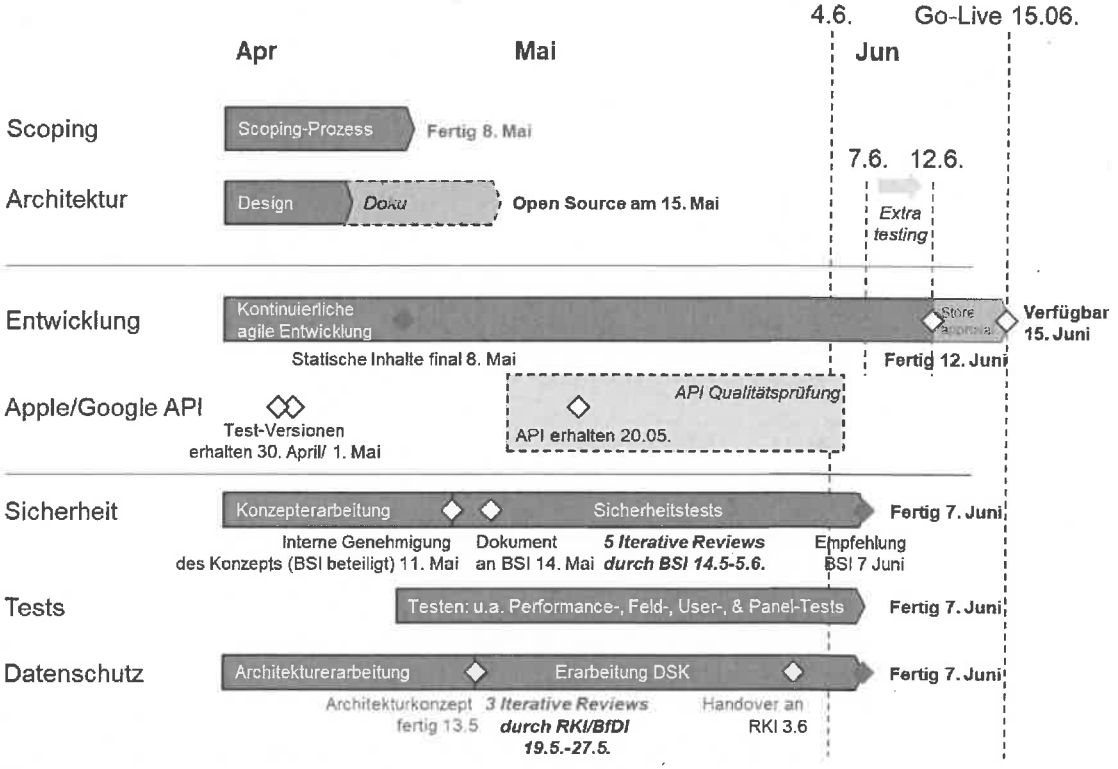



Abbildung 2: Zeitplan bis GOLIVE

Der Leistungszeitraum umfasst zwei Phasen, von Projektstart bis zum GOLIVE Termin und die Zeit nach dem GOLIVE Termin. Eine weitere Planungsprämisse ist nach derzeitigem Stand (5.6.2020), dass die Corona Warn App am 15.06.2020 öffentlich zur Verfügung steht.

## 1.4 Grundannahmen

| Grundannahme | Dimensionierung |
|---|---|
| Anzahl Nutzer | 25 Mio. |
| Anzahl an Infizierten pro Tag für die Netzwerkdimensionierung | max 10.000 |
| Monatliches Datenvolumen je Smartphone | 264 MB |
| Tägliches gesamtes Datenvolumen | 210 TB |
| Spitzenlast im CDN | 48 Gbit/s |
| Spitzenlast zu den Netzbetreibern | 20 Gbit/s |
| Durchschnittliche Last | 20 Gbit/s |
| Anzahl anzubindender Testeinrichtungen | 300 Labore, Krankenhäuser, Uni-Institute, etc. |
| Hotfixe und Updates von Standardkomponenten | 2 pro Monat |
| Häufigkeit Datensicherung | 1 Mal täglich |
| Anzahl Calls pro Tag Technische Hotline | 3000 |
| Dauer pro Call in der Technischen Hotline | 10 Minuten |
| Servicezeit Technische Hotline | Mo-Sa, 7-22 Uhr, nicht an gesetzlichen Feiertagen |
| Anzahl Calls pro Tag Verifikations-Hotline | 1000 |
| Dauer pro Call in der Verifikations-Hotline | 10 Minuten |
| Servicezeit Verifikations Hotline | 7 x 24 Stunden |
| Sprachen der Technischen Hotline | Deutsch, Englisch;<br>sowie Türkisch (3 Monate nach GOLIVE) |
| Sprachen der Verifikations Hotline | Deutsch, Englisch und Türkisch |

Die Dimensionierung der Netzwerkverbindungen basieren auf der Annahme, dass die Gesamtlösung hinsichtlich der maximalen Datenraten, die E2E abgestimmten Bandbreiten vor allem mit Blick auf die deutschen Mobilfunknetze nicht überschreiten. Seitens der Gesamtlösung wird davon ausgegangen, dass man das Gesamtvolumen im Falle von drohender Überlast der Mobilfunknetze kontrolliert begrenzen kann.

Bei der Dimensionierung gehen wir von folgender Berechnungsgrundlage aus:

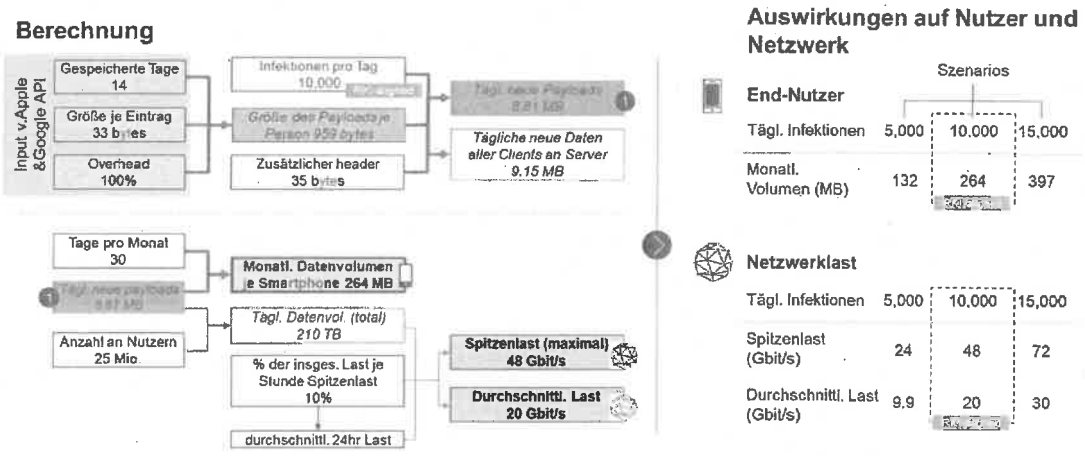



Abbildung 3: Dimensionierung der Netzwerkverbindungen basierend auf den abgestimmten Eingangsparametern

# 2 LEISTUNGEN BIS GOLIVE

## 2.1 Development Verifikation bis GOLIVE

Unter Berücksichtigung der Gesamtarchitektur und einer möglichen zukünftigen Ausrichtung wird der Verifikationsprozess durch die Telekom umgesetzt. Innerhalb der Verifikation erfolgt die Verifizierung / Falsifizierung einer gemeldeten Infektion. Dies wird über einen Vergleich von potenziell infizierten Menschen mit Testergebnissen aus Laboren erreicht und ist nachfolgend beschrieben.

### 2.1.1 Leistungsbeschreibung

Über die Telekom wird die Abbildung des automatischen Laborprozesses inkl. der Anbindung der Testlabore zur Verfügung gestellt. Im Fall des manuellen Prozesses liefert die Telekom innerhalb des Verifikationsprozesses die Verbindung zur Hotline und Abbildung des gesamten TAN Verifikationsprozesses. Mit dem Start des Verifikationsprozesses wird eine Transaktionsberechtigung erzeugt und eine Transaktionsnummer (TAN) generiert. Diese wird an die positiv getestete Person übermittelt. Der Proximity Identifier wird jetzt, sobald ein Anwender positiv getestet wurde, in einen Diagnosis Key umgewandelt. Der Diagnosis Key und die TAN werden jetzt an den Corona Contact Tracing Server (CTS) automatisch übermittelt. Der Ablauf wird dabei für den Nutzer transparent und nachvollziehbar durch die Corona Warn App vorgenommen.

Proximity Identifiers ohne TAN oder mit ungültiger TAN werden verworfen. Nach der Übermittlung der Diagnosis Keys wird die zugehörige TAN im System gelöscht und wird für die Zukunft ungültig. Die Diagnosis Keys werden täglich allen Smartphones, die das Corona Contact Tracing aktiviert haben zur Verfügung gestellt.

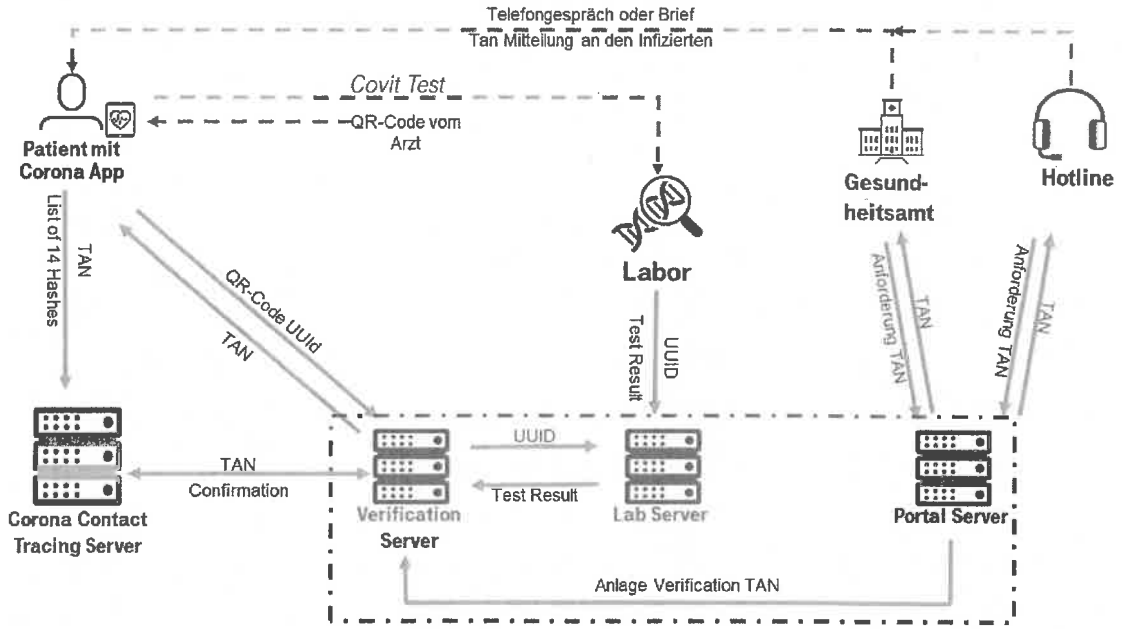



Abbildung 4: Übersicht Verifikationsprozess und beteiligte Komponenten

Das Verifikationssystem gemäß Abbildung 1 ist durch ein punktiertes Rechteck gekennzeichnet, bestehend aus 3 Komponenten, die für jeweils unterschiedliche Aufgaben verantwortlich sind. Eine klare Trennung zwischen Testergebnissen und Verifikationsverfahren wird durch Aufteilung in unterschiedliche Sicherheitszonen erreicht. Diese drei Komponenten werden nachfolgend in ihrer Funktion beschrieben.

Die Telekom entwickelt die folgenden 3 Verifikation Komponenten und realisiert sie auf der Open Telekom Cloud:

**1. Verifikationsserver**

Der Verifikationsserver (VS) prüft die Berechtigung eines infizierten Nutzers zum Upload seiner Diagnosis Keys. Ausschließlich infizierte Nutzer werden durch die vom Verifikationsserver erzeugte TAN berechtigt, ihre Diagnosis Keys dem CTS zu übermitteln. Für diese Prüfung bedient er sich der Auskunft des Labor Test Result Service. Das Verfahren arbeitet nur mit Pseudonymen der betroffenen Personen im System. Pseudonyme Daten werden an keiner Stelle im Verifikationsservice gespeichert. TANs werden auf dem Verifikationsserver gespeichert, bis sie

a. Durch Ablauf einer vorher festgelegten Zeitspanne ungültig werden oder

b. Durch eine Verifikationsanfrage vom CTS entwertet werden

**2. Lab Server**

Der Lab Testresult Server speichert pseudonymisierte Testergebnisse von angeschlossenen Laboren und läuft in einem vom Verifikationssystem getrennten Sicherheitskontext. Er teilt auf dessen Anfrage dem Verifikationsserver ein von einem Labor ermitteltes Testergebnis mit. Telekom stellt eine Schnittschnelle zu den Laboren bereit. Die Anbindung und die Zulieferung der Testergebnisse einschließlich der Berechtigung, diese an Telekom zu liefern, obliegt den Laboren.

**3. Portal Server**

Diese Komponenten dient dem manuelle Freigabeprozess von infizierten Nutzern für den Upload ihrer Diagnosis Keys. Freigaben sollte nur durch die Gesundheitsämter oder vergleichbarer autorisierter Instanzen auf Basis dort verfügbarer Unterlagen und Diagnosen erfolgen. Eine Freigabe, d.h. die Generierung einer neuen TAN für eine infizierte Person erfolgt über ein Web-Portal. Das Webportal dient dem Verifikations-Hotline-Mitarbeiter als Frontend zum Abruf der nächsten gültigen TeleTAN. Der Prozess generiert eine personenunabhängige, zeitlich begrenzt gültige TAN, welche dem Nutzer mitgeteilt wird. Aufgrund der hohen Sensibilität des Verfahrens, ist der Zugang zum Portal nur über ein Authentifizierungsverfahren möglich. Wir empfehlen, zusätzliche, noch abzustimmende Methoden einzusetzen, die sicherstellen, dass sich der Systemzugang bei Nicht- oder Fremdbenutzung automatisch sperrt.

Alle Serverkomponenten werden in der sicheren Open Telekom Cloud in Deutschland betrieben. Dabei sind die Serverkomponenten so konzipiert, dass sie entsprechend der Lastanforderungen durch konkurrierende Benutzerzugriffe automatisch skalieren können, um die Antwortzeiten des Systems kurz zu halten.

**Sicherheitsaspekte des TAN Verfahrens**

Die TANs berechtigen einen Nutzer zum Upload seiner Diagnosis Keys.

Anforderung an die TAN:

1. Eine vom System akzeptierte gültige TAN ist nicht per Trial & Error generierbar
2. Die TAN hat eine zeitlich begrenzte Gültigkeit und kann nur einmal verwendet werden
3. Eine TAN kann nach der Erzeugung keiner Person mehr zugeordnet werden.

Eine TAN ist durch den Nutzer als geheimer Schlüssel zu behandeln, vergleichbar zu einer EC-Karten PIN. Der Nutzer muss durch den Kunden entsprechend darauf hingewiesen werden.

**Manuelle Verifikation**

Manuelle Verifikation dient der Freigabe der Proximity Daten der Corona Warn App infizierter Nutzer, welche auf Grund unterschiedlichster Ursachen nicht im automatischen Verifikationsprozess freigegeben werden können. Hierfür ist durch das BMG/RKI zu klären, welche Instanz solche Freigaben verifizieren und erteilen darf, und wer den Zugang, also das User-Management der freigabeerteilenden Personen übernimmt.

Telekom liefert hierzu eine technische Schnittstelle und ein Web-Portal für die Generierung von TANs als Repräsentation einer Freigabeentscheidung.

Für die technische Anbindung stellt die Telekom ausschließlich eine Schnittstelle bereit, welche die Anbindung der Labore über clientseitige Zertifikate absichert und einen Import der Testdaten ermöglicht.

## 2.2 Testing bis GOLIVE

### 2.2.1 Leistungsbeschreibung

Innerhalb des Projektes und der Vergütung gemäß Leistungsverzeichnis erbringt die Telekom die in der Anlage 5 der Abstimmungsvereinbarung beschriebenen konzeptionellen und operativen Testleistungen. Die Testaktivitäten laufen in mehreren Teststufen ab, die sich zeitlich und inhaltlich voneinander unterscheiden und haben jeweils einen voneinander unterschiedlichen Testfokus mit klar definierten Testkriterien. Das ganze Testvorgehen wird in einem Testkonzept konkret beschrieben. In der Testvorbereitung werden für jede Teststufe Testfälle in Jira/X-Ray spezifiziert und mit den Anforderungen verknüpft. Ziel ist es, die fachlichen Anforderungen vollständig durch Testfälle abzudecken. In der Testdurchführung werden die Durchführungen der Testfälle ebenfalls in Jira/X-Ray protokolliert. Treten bei der Durchführung SW-Fehler auf, werden sie ebenfalls dort dokumentiert und deren Behebung nachverfolgt.

In den nachfolgenden Tabellen werden die Teststufen beschrieben.

| **Teststufe** | **Compatibility-Test Mobile-App** |
|---|---|
| **Testziel** | Kompatibilitätstests der Mobile-App prüfen die korrekte Funktionalität ausgewählter User-Stories auf verschiedenen Endgeräten unterschiedlicher Hersteller mit unterschiedlichen Betriebssystemen in unterschiedlichen festgelegten und abgestimmten Versionen |
| **Testgegenstand** | Testgegenstand ist die lauffähige mobile App (bluetooth tracing ist möglich) integriert mit den Backendsystemen.<br>Die Kompatibilität der Mobile-App wird mit verschiedenen Endgeräten mittels der Mobile Device Cloud überprüft. Es werden dabei iOS Geräte in Version 13.5 sowie Android ab 6. Major Releases bis zu Android 10 als testbare mobile Betriebssystemversionen herangezogen.<br>Mit geeigneten Automatisierungstools (bspw. Appium) wird die App für iOS und Android automatisiert. Dieser Test kann durch zeitliche oder technische Trigger ausgelöst werden.<br>Die Kernfunktionalitäten im Bereich:<br>▪ Anbahnung und Installation (Onboarding-Prozess)<br>▪ Informationen und Instruktionen zur Nutzung der Applikation<br>▪ Nutzung im Regelprozess<br>sind gemäß der Abdeckung im mobilen Compatibility-Test mitberücksichtigt. |
| **Abgrenzung** | Es werden nur Funktionen des Frontend der App auf dem einzelnen Mobilfunkgerät getestet. |

| Teststufe | E2E-Test |
|---|---|
| **Testziel** | Funktionaler E2E-Test des integrierten Systems<br>Ziel des E2E-Tests aus Geschäftsprozesssicht ist die Prüfung funktionaler Korrektheit der Geschäftsprozessketten in einem integrierten Gesamt-IT-Verbund mit vollständig angebundenen Komponenten und Applikationen.<br>Basis für die Testspezifikation sind die Userstories und die daraus abgeleiteten Geschäftsprozesse sowie die fachlichen Schnittstellenspezifikation zwischen den Applikationen und Komponenten. |
| **Testgegenstand** | Testgegenstand des E2E-Tests ist die gesamte angebundene IT-Landschaft, bestehend aus allen im Testscope definierten und technisch im Verbund angebundenen und beteiligten Komponenten. Der Testfokus liegt auf dem korrekten und vollständigen Ablauf der E2E-Prozesse durch diese IT-Landschaft wie z.B.:<br>▪ Meldung eines positiven Testergebnisses über Labor/Hotline<br>▪ Mitteilung eines positiven Testergebnisses über Mobile-App<br>▪ Download und Matching der relevanten Keys und Benachrichtigung des App-Users<br>Zur Durchführung des E2E-Tests wird der gesamte IT-Verbund inkl. die externen Systemkomponenten wie z.B. der Laborserver als Black-Box betrachtet. Es wird anhand von Testfallketten die Korrektheit der applikationsübergreifenden Prozessierung von Geschäftsprozessen durch die gesamte IT-Landschaft geprüft. Beispielweise werden ausgewählte Kontaktszenarien zur Erzeugung unterschiedlicher Risiko-Level für den App-User hergestellt.<br>Eingaben über den Lab-Server, Portal-Server und die Mobile-App werden durch die Tester vorgenommen. |
| **Abgrenzung** | Der E2E-Test erfolgt mit dem für die Produktion vorgesehenen Parametersatz. Tests von unterschiedlichen Parametersätzen sind nicht geplant.<br>Der E2E-Test erfolgt mit wenigen Kontaktszenarien, die zu unterschiedlichen Risiko-Leveln und Meldungen für den App-User führen. |

| Teststufe | Load- and Availability Test |
|---|---|
| **Testziel** | Test der Applikation auf produktionsnahen Systemen der OTC hinsichtlich Lastfähigkeit, Skalierbarkeit und Hochverfügbarkeits-Eignung. Es wird das Verhalten des Systems unter wechselnder Last bewertet, üblicherweise zwischen zu erwartender niedriger, typischer sowie Spitzenlast. |
| **Testgegenstand** | Last- und Performancetest<br>▪ Lasttests mit den erwarteten Mengengerüsten für die Produktion<br>▪ Skalierungstest mit wechselnder Belastung zur Überprüfung der Skalierfähigkeit der Komponenten<br><br>Availability Test<br>▪ Ausfalltests für einzelne Komponenten (Software, Hardware) zur Überprüfung der Hochverfügbarkeitsmechanismen<br>Upload/Download von Keys, Request von IDs und Submit/Retrieve von Results werden mit Lasttesttools auf HTTPS-Ebene simuliert. |
| **Abgrenzung** | Ein Netzlasttest ist nicht geplant.<br>Eine Anbindung externer Partnersysteme ist nicht geplant. |

| Teststufe | User Tests |
|---|---|
| **Testziel** | Funktionaler Test auf Basis der User Stories und der abgestimmten Testkriterien.<br>Dabei werden die Nutzbarkeit des Gesamtsystems sowie Funktionsfähigkeit bestehender E2E-Geschäftsprozesse geprüft. |
| **Testgegenstand** | Funktionale Tests auf Basis der in den User Stories definierten Testkriterien.<br>Soweit Szenarien bereits im E2E-Test abgedeckt sind, wird auf die vorliegenden Ergebnisse aufgesetzt. Wenn weitere Szenarien erforderlich sind, werden diese soweit möglich im E2E-Test aufgenommen. |
| **Abgrenzung** | Ein Test unterschiedlicher Parametersätze oder eine breite Abdeckung unterschiedlicher Kontaktszenarien und Kontakthistorien über die im E2E-Test geplanten Konstellationen ist nicht vorgesehen. |

Die Telekom führt Kompatibilitätstests der auf GitHub veröffentlichten App mit den gängigsten Mobiltelefonmodellen gemäß der Mobiltelefonliste aus Anlage 4 der Abstimmungsvereinbarung durch.

## 2.3 System Operations und Hosting bis GOLIVE

### 2.3.1 Leistungsbeschreibung

Die Telekom stellt dem BMG bereits vor dem GOLIVE eine Managed „Platform as a Service" (PaaS) zur Verfügung. Die Umgebungen werden in der Onboarding Phase geplant und aufgebaut. Dabei fallen initiale Kosten für den Setup der IT Infrastruktur an. Bis zum GOLIVE werden die Umgebungen genutzt, um die Anwendungen und Umgebungen entsprechend anzupassen und zu testen. Dazu ist der Aufbau eines "Continous Integration" und "Continous Delivery" (CI/CD) Prozesses notwendig. Im Rahmen eines agilen CI/CD Service Betriebs stellen wir die Überwachung des Prozesses via Monitoring-Tools sicher. Zur Begleitung der durch den Auftraggeber geforderten Sicherheitsüberprüfungen erfolgen individuelle Security Anpassungen.

Für den Betrieb der Anwendungen erfolgt vor dem GOLIVE eine Transition- und Transformation in 3 Phasen (Pre-check,Transition, Testing – siehe Kapitel 3 des Leistungsbeschreibung CNAO_CI/CD). Die erfolgreiche Umsetzung dieser 3 Phasen ist die grundlegende Voraussetzung für den reibungslosen Ablauf in unserem agilen Betrieb. Für den Betrieb der Anwendung wird ein Betriebshandbuch sowie ein Rechte- und Rollenkonzept erstellt.

Eine detaillierte Beschreibung des Services „Managed PaaS" ist dem beigefügten Leistungsschein zu entnehmen.

### 2.3.2 Annahmen und Rahmenbedingungen

Die Managed PaaS Plattformen für Entwicklung, Test, Pre-Produktion und Produktion werden sukzessive in Betrieb genommen und bis zum GOLIVE stehen alle 4 Umgebungen zur Verfügung.

Für jeden Cluster wird ein Logging Stack auf Basis EFK/EFG (ElasticSearch, Fluentd, Kibana/Graylog) entsprechend einer angepassten Konfiguration bereitgestellt (siehe Anlage 2, Kapitel 1.3 in Leistungsschein Managed PaaS)

### 2.3.3 Mitwirkungsleistungen und Beistellungen SAP

Die Definition der Überwachungsmetriken und KPIs, wie in Kapitel 4.2.1 der Leistungsbeschreibung CNAO_ CI/CD (Anlage 1) beschrieben erfolgt in Abstimmung mit den Applikationsverantwortlichen der SAP spätestens 5 Tage vor GOLIVE.

Die Definition der Runbooks, wie in Kapitel 4.2.2 der Leistungsbeschreibung CNAO_CI/CD (Anlage 1) beschrieben erfolgt in Abstimmung mit den Applikationsverantwortlichen der SAP spätestens 5 Tage vor GOLIVE.

## 2.4 IT-Sicherheit bis GOLIVE

Die Telekom liefert ein angemessen hohes IT-Sicherheitsniveau für alle Komponenten im Angebotsumfang. Alle angebotenen Leistungen genügen den marktüblichen „Security Best Practices", konkret den Technischen Sicherheitsrichtlinien der Telekom[1], die sowohl während der Entwicklung und Bereitstellung erbracht werden als auch während der

[1] https://www.telekom.com/resource/blob/314436/4ba45c4dd017c1652e61daddab7679a9/dl-technische-sicherheitsanforderungen-data.zip

anschließenden Betriebsphase in Form von Managed Services. Die Telekom ist vollumfänglich nach ISO 27001 zertifiziert.

Die Leistungen im Bereich IT-Sicherheit in der Entwicklungsphase gliedern sich in Einzelleistungen, die im Folgenden beschrieben werden.

### 2.4.1 Teilprojektleitung IT-Sicherheit

In diesem Leistungspaket erfolgt die Steuerung der verschiedenen Aktivitäten, die im Bereich IT-Sicherheit geleistet werden. Dies umfasst:

- Koordinieren der verschiedenen IT-Sicherheitsthemen
- Abstimmung der inhaltlichen Anforderungen des Auftraggebers
- Abstimmung der inhaltlichen Anforderungen mit weiteren Auftragnehmern des Kunden bzw. Partnern
- Abstimmung der inhaltlichen Anforderungen mit dem BSI
- Abstimmung der Anforderungen an die Dokumentation der Sicherheitsleistungen

### 2.4.2 IT-Sicherheitsberatung

In Kooperation mit den Partnern werden im Rahmen der Anforderungsanalyse die IT-Sicherheitsanforderungen an das zu entwickelnde System aus Geschäftssicht formuliert (synonym: IT-Sicherheitsziele, ; Leitfrage: Wozu braucht der Auftraggeber denn IT-Sicherheit?). In dieser Aktivität wird auch der Schutzbedarf der verarbeiteten Daten festgestellt. Die IT-Sicherheitsanforderungen geben die Grundlagen für IT-Sicherheitstests vor und sind im Grundsatz technologieunabhängig.

Beratend wird zusammen mit den Partnern eine Spezifikation der Architektur, der Prozesse und der Protokolle erarbeitet.

- Es werden IT-sicherheitskritische Themen identifiziert sowie passende IT-Sicherheitsmaßnahmen (IT-Sicherheitsdienste) und deren erforderliche Stärke (Widerstandsfähigkeit) spezifiziert, um mögliche Verwundbarkeiten zu mitigieren.
- Als konkrete Maßnahmen soll hier das Threat Modelling, das Bewerten der identifizierten Threats (Bedrohungen) und die Ableitung von Risiko-minimierenden Maßnahmen erwähnt werden.
- Im Rahmen der Implementierung der erarbeiteten Spezifikation kann erwartet werden, dass es notwendige Änderungen an dieser Spezifikation geben wird. Solche Änderungen müssen ebenfalls aus Sicht der IT-Sicherheit bewertet werden. Im Falle identifizierter Schwachstellen werden Vorschläge erarbeitet, um diese identifizierten Schwachstellen zu vermeiden oder zu mitigieren.

### 2.4.3 IT-Sicherheitskonzepte

Die Telekom begleitet die Implementierung verschiedener Komponenten (Lab Server, Verifikation Server, Portal Server), die für das Funktionieren der Corona Warn App erforderlich sind, mittels des in der Telekom eingeführten IT-Sicherheitsverfahrens, dem PSA (Privacy and Security Assessment[2]).

[2] https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/details/privacy-and-security-assessment-verfahren-342724

Im PSA-Verfahren werden IT-Sicherheitsanforderungen, die an die zu erstellende Komponente gestellt werden müssen, identifiziert und mit der implementierenden Fachseite abgestimmt. Diese IT-Sicherheitsanforderungen adressieren alle relevanten Ebenen der implementierten Komponente, angefangen bei den verwendeten Betriebssystemen, den Datenbanken bis zu den Applikations- und Web Servern. Ebenfalls stehen Themen wie Architektur, Netze, Monitoring und Administration im Fokus. Neben einem Bestand an standardisierten IT-Sicherheitsanforderungen werden im Zuge des PSA-Verfahrens auch projektspezifische Anforderungen erstellt und abgestimmt.

Die IT-Sicherheitseigenschaften der Komponenten werden im Rahmen des parallel zur Entwicklung erstellten SDSK („Standardisiertes Datenschutz- und Sicherheitskonzept", Telekom-interne Bezeichnung) dokumentiert und mit einem IT-Sicherheitsexperten abgestimmt.

Nach Abschluss der Implementierung überprüft der IT-Sicherheitsexperte die erstellte Dokumentation und stellt fest, ob die vorab identifizierten IT-Sicherheitsziele aus den IT-Sicherheitsanforderungen erreicht worden sind.

### 2.4.4 Penetration Testing

Ziel eines Penetrationstests ist es, Schwachstellen im System zu identifizieren, die ein Angreifer nutzen kann, um Systeme oder die darauf gespeicherten Daten zu kompromittieren, Einsicht in vertrauliche Informationen zu erhalten oder die Verfügbarkeit von Diensten zu beeinträchtigen.

Die Telekom wird die App und die Backends („Verification Server", „Backend for mobile application"), mit denen die App kommuniziert, einem Penetrationstest unterziehen. Ebenso werden die Backend-Server „Lab server" und „Portal server" einem Penetrationstest unterzogen.

In Anlehnung an die OWASP Testing Standards führt die Telekom bei Webapplikationen eine Reihe von Überprüfungen durch, die speziell darauf abzielen, typische Schwachstellen in diesen Anwendungen zu identifizieren. Diese werden auf Basis des OWASP „Web Security Testing Guide" durchgeführt. Für die Smartphone-Apps wird analog der OWASP „Mobile Security Testing Guide" angewandt.

Die Tests werden im White-Box-Verfahren durchgeführt, d. h. es liegen Detailinformationen zum Aufbau der zu testenden Anwendungen und Systeme vor.

Für die Durchführung eines Penetrationstests wird eine ganze Reihe spezialisierter Werkzeuge benötigt. Die Ergebnisse der Penetrationstests werden dokumentiert.

### 2.4.5 IT-Sicherheits-Review

Die Leistungen von der Telekom werden vor Inbetriebnahme in einer beratenden Tätigkeit einem Review unterzogen, in dem die erstellte IT-Sicherheitsdokumentation nochmals auf Korrektheit und Vollständigkeit geprüft wird. Alle im Rahmen von IT-Sicherheitstests identifizierten Schwachstellen, die nicht vollständig beseitigt werden konnten, werden bewertet und wenn nötig, weitere mitigierende Maßnahmen sowie Restrisikobeschreibungen erarbeitet.

Am Ende des IT-Sicherheits-Reviews sind alle bekannten Risiken verstanden und dokumentiert.

### 2.4.6 Onboarding des Monitorings, inklusive Implementierung im Magenta SIEM

Vor GOLIVE werden die Detektionsarchitektur sowie die Alarmbearbeitung festgelegt und dokumentiert. Dazu gehören insbesondere:

- Festlegung der Detektionsszenarien (Use Case Definition)
- Technische Anbindung der Logquellen
- Entwicklung applikationsspezifischer Parser
- Implementierung der Alarm-Regeln für die Use Cases im Security Information and Event Management System (SIEM)
- Entwicklung der Runbooks für die Reaktion durch die Level 1- und Level 2-Analysten im Security Operations Center.

Diese Tätigkeiten sind Vorarbeiten für die Security Operations Center (SOC)-Leistungen im Abschnitt 3.4.1.

### 2.4.7 Leistungsabgrenzung

- Die Telekom erstellt je verantworteter Teilkomponente der Lieferleistung ein Sicherheitskonzept (SDSK-Terminologie) nach Telekom-internen Standards (PSA).
- Es wird kein IT-Sicherheitskonzept nach BSI IT-Grundschutz oder ISO 27001erstellt. Dessen Erstellung ist Bestandteil der IT-Sicherheitstätigkeiten nach GOLIVE (siehe Abschnitt 3.4.4.
- Die IT-Sicherheit inklusive Dokumentation von Teilkomponenten, die von anderen Auftragnehmern des Kunden erstellt werden, wird durch diese selbst verantwortet. Insbesondere sind Software-Sicherheitsarchitektur (App und Backend) und Kryptokonzept inklusive Anonymisierung/Pseudonymisierung nicht in der Verantwortung der Telekom.
- Im Rahmen der Penetrationstests auf die betriebene IT-Infrastruktur testet die Telekom die Teilkomponenten, die von anderen Auftragnehmern erstellt werden, mit. Diese Penetrationstests ersetzen nicht die von anderen Auftragnehmern im Rahmen eines „Secure Software Development Lifecycle" (SSDLC) selbst vorzunehmenden IT-Sicherheitstests.

### 2.4.8 Mitwirkungspflichten und Beistellungen des Kunden

- Der Auftraggeber muss Prozesse, die außerhalb der hier beschriebenen IT Systeme stattfinden, festlegen und bestimmen, wie diese mit den IT Systemen interagieren sollen (Beispiel: Abläufe in den Laboratorien). Die Telekom wird als Teil der Beratung eine Empfehlung erstellen.
- Für Penetrationstests ist eine Einverständniserklärung des Auftraggebers und ggf. weiterer Auftragnehmer und eine Festlegung der Rahmenbedingungen (auch „Rules of Engagement" genannt) erforderlich.

## 2.5 Netzwerk bis GOLIVE

Als Teil der Leistungserbringung wird hier das Thema Netzwerkverbindungen der in der OTC gehosteten Backend-Applikation und den verschiedenen Endsystemen entwickelt und deren Realisierung geplant. Dazu zählen neben der reinen Anbindung auch die Themen Schutz der Schnittstellen und Realisierung der Auslieferung an die Endkunden über die Layer 1-4. Die Telekom stellt einen DDoS Backbone-Schutz bereit, der hochvolumige Angriffe abwehrt, um die Stabilität des bereitgestellten Service zu ermöglichen. Ziel ist es möglichst auf eigenen Produkten aufzusetzen, um die Prozesse und damit die Betreibbarkeit und Stabilität der Lösung zu optimieren.

Die Telekom übernimmt hier die komplette Beschreibung und Umsetzung der Netzanbindungen. Die technische Parametrisierung erfolgt in Abstimmung mit den Architekten, den Applikationsentwicklern und der Sicherheit.

Es werden keine dedizierten Verbindungen zu Netzen außerhalb von Deutschland betrachtet.

Als Leistung bis GOLIVE gehört hierbei ebenso zum Aufbau des Netzwerkbetriebes das Set-up des Content Delivery Network (CDN). Mit diesem CDN Service bieten wir die Auslieferung von statischen Inhalten auf Basis der DT CDN Plattform an die Kunden der Deutschen Netzbetreiber an. Die Lösung ist dafür konzipiert, statische Objekte mit niedriger Latenz und hoher Übertragungsgeschwindigkeit mittels HTTP und HTTPS auszuliefern. Durch die integrierte Möglichkeit des Cachings der Inhalte wird die Datenquelle entlastet und die Quality of Experience für die Endkunden wesentlich verbessert. Durch die redundante Plattform Architektur, die deutschlandweit verteilten Standorten als auch die massive Kapazität der DT CDN Plattform bieten wir höchste Verfügbarkeit der Inhalte.

Die CDN Plattform der Deutsche Telekom (DT) nutzt das IP Backbone der DT (DT IP Backbone) zur Auslieferung der Inhalte. Durch das DT IP Backbone können die Inhalte an alle Endgeräte via Fest- und Mobilfunknetze der DT als auch aller anderen Netzbetreiber ausgeliefert werden. Die umfangreichen, geo-redundanten Verbindungen des DT IP Backbone mit den verschiedenen Netzbetreibern in Deutschland ermöglichen den Zugang jedes Endgerät zu den Inhalten.

Untersuchungen zu den möglichen konkreten Auswirkungen auf die betroffenen Mobilfunknetze (MNOs) in Deutschland werden nicht durchgeführt. Die Deutsche Telekom informiert, basierend auf den aktuellen Annahmen des RKI (siehe Abbildung 3: Dimensionierung der Netzwerkverbindungen basierend auf den abgestimmten Eingangsparametern), die MNOs über die aktuell zu erwartenden Verkehrsvolumen, die die Netze erwarten können.

### 2.5.1 Mitwirkungspflichten und Beistellungen des Kunden

Der Auftraggeber muss frühzeitig über Entwicklungen informieren, die zu einer Veränderung des zu erwartenden Verkehrsvolumen führen können.

## 2.6 Hotline Services bis GOLIVE

Zur angemessenen Vorbereitung des GOLIVE der Hotlines wird eine Ramp-Up Phase vorgeschaltet. Diese Phase hat die Bereiche Personal und Technik im Fokus und ist Grundlage für den erfolgreichen GOLIVE. Im Einzelnen umfasst sie die nachfolgenden Bestandteile:

**0800 + IVR**

Einrichtung der vom RKI beauftragten 0800 Nummern jeweils für die technische und Verifikations Hotline. Aufbau und Einrichtung der IVR (Interactive Voice Response) gemäß den Vorgaben von BMG/RKI hinsichtlich Auswahloptionen, Texte und Aufnahme/Einspielung der danach produzierten Ansagen.

**Technische Hotline**

Um die Forderung nach einer eigenen, lediglich RKI-internen Technischen Hotline nachzukommen, werden wir die Technische Hotline vor dem eigentlichen Produktivstart der App aktivieren müssen.

Des Weiteren fallen Leistungen im Zusammenhang mit Ramp-up, Einrichtung für die Hotline, Tests mit Auftraggeber sowie Schulungs- und Trainingskosten für die Hotline Agenten an.

**Verifikationshotline**

Hier werden ebenfalls vor Produktivstart weitere Leistungen anfallen, wenngleich zeitlich etwas später, wie Ramp-up, Einrichtung für die Hotline, Tests mit Auftraggeber sowie Schulungs- und Trainingskosten für die Hotline Agenten.

### 2.6.1 Mitwirkungsleistungen und Beistellungen des Kunden

| Mitwirkung / Beistellung | Organisationseinheit |
|---|---|
| Freigabe und Beauftragung der Ansagetexte in der IVR | BMG |

### 2.6.2 Mitwirkungsleistungen und Beistellungen Dritter

| Mitwirkung / Beistellung | Dritter |
|---|---|
| Zulieferung zu CoronaWarnApp Dokumentationen für die Erstellung von Frage-/Antwort-Katalogen | SAP |
| Zulieferung für die Bereitstellung von FAQs | SAP |

# 3 LEISTUNGEN NACH GOLIVE

In der Betriebsphase (nach dem GOLIVE) sind die Leistungen der Projektphase in eine stabile Leistungserbringung überführt, werden konstant erbracht und gemonitort. Darüber hinaus werden etwaige Angriffe auf die Plattform (OTC) gemäß den getroffenen Vereinbarungen unterbunden. Neue Anforderungen an das System, z.B. aus dem Live-Betrieb werden bewertet sowie nach Priorisierung und Entscheidungsfindung werden erforderliche Anpassungen am System vorgenommen.

Änderungen an der von Telekom zu betreibenden Software sowie der Schnittstellen zu Google und Apple, die zu höherem Aufwand bei der Leistungserbringung nach GOLIVE führen, werden im Rahmen des Change-Request-Verfahren bewertet.

## 3.1 Development Verifikation nach GOLIVE

Die Entwicklung der Verifikationskomponenten wird in der Phase bis GOLIVE abgeschlossen. Nach GOLIVE benötigt die Telekom mit einem Vorlauf von 14 Tagen eine Beauftragung für weitere Entwicklungstätigkeiten.

## 3.2 Testing nach GOLIVE

Nach dem GOLIVE werden kontinuierlich Hotfixe und Updates von Standardkomponenten in die Produktion eingespielt. Um dies abzusichern, sind 2 Regressionstests pro Monat maximal vorgesehen. Tests von fachlichen Erweiterungen sind gesondert zu beauftragen.

Es wird ein Test durchgeführt, dass auf den Endgeräten die gespeicherten Bluetooth IDs nach 2 Wochen nicht mehr verfügbar sind.

## 3.3 System Operations und Hosting nach GOLIVE

Die Telekom stellt dem BMG nach dem GOLIVE eine Managed „Platform as a Service" (PaaS) zur Verfügung. Alle hierzu notwendigen Infrastrukturkomponenten und Softwarelizenzen (Red Hat Enterprise Linux und Red Hat OpenShift Container Platform (OCP)) werden seitens Telekom bereitgestellt.

Managed PaaS beinhaltet virtuelle Infrastruktur und virtuelle Netzwerkkomponenten auf der Open Telekom Cloud (OTC) und erlaubt das Erzeugen, das Management, sowie die Orchestrierung von Docker Containern.

Es wird ein agiler und zuverlässiger Applikationsbetrieb für die entwickelten Applikationen als „Cloud Application Operation" vor dem GOLIVE vorbereitet. Dieser umfasst ab dem GOLIVE auch die proaktive Überwachung (24*7), das Troubleshooting, das Schnittstellen-management als auch weitere Services wie Nutzermanagement, Reporting und Deep-Analysis.

Übergabepunkt für alle Leistungen der Managed PaaS ist der Übergabepunkt der Managed PaaS in das Internet, bzw. in das Netzwerk des BMG (z. B. VPN, MPLS).

### 3.3.1 Managed PaaS

Managed PaaS umfasst die gemanagten Dienste des Kernsystems mit den folgenden Leistungen:

- Dediziertes RH OCP Cluster (PaaS Instanz) in aktueller Version

- OpenShift-Web-Konsole (Self-Service Portal)
- Überwachung der Plattformverfügbarkeit
- Metrics Stack
- Logging Stack ElasticSearch, Fluentd, Kibana/Graylog

Zur Sicherstellung eines agilen CI/CD Service Betriebs stellen wir die kontinuierliche Überwachung und Erweiterung via Monitoring-Tools sicher.

Eine detaillierte Beschreibung des Service „Managed PaaS" sowie die dazugehörigen Service Level ist der beigefügten Leistungsbeschreibung (Anlage 2) zu entnehmen.

### 3.3.2 Cloud Application Operation

Entsprechend der Kritikalität und der Komplexität der Anwendungen stellen wir einen Applikationsbetrieb der Leistungsklasse „Application Service" (vgl. Anlage 1, Kapitel 2 Leistungsbeschreibung CNAO_CI/CD) für die Verifikation Komponenten und die Mobile Backend Komponente von SAP zur Verfügung.

Dieser beinhaltet die proaktive Überwachung und Verwaltung der Applikationen, die als Backend-Dienst der App auf der Managed PaaS Plattform in der OTC gehostet werden. Neben dem klassischen Monitoring und Management-Reporting beinhaltet das Cloud Application Operation auch eine Echtzeitansicht- und Übersicht über den Zustand und die Verfügbarkeit der Applikation sowie ihrer Komponenten. Im Service ebenfalls enthalten ist die Bearbeitung von Störfällen. Im Betrieb werden Störfälle durch das Betriebsteam erkannt oder in Form eines Support Tickets bekannt gemacht.

Es wird standardmäßig ein tägliches Backup der Nutzdaten bzw. Anwendungsdaten auf der Open Telekom Cloud angelegt. Als Teil des Anwendungsbetriebs werden die Datenbanken und der Object-Storage gesichert.

Teil des Applikationsbetriebs ist ein CI/CD Toolchain Service. Im Rahmen dieses Services ermöglichen wir Ihnen durch die Einführung und Umsetzung unseres CI/CD-Toolchain Services eine automatisierte Entwicklungs-, Integrations-, Test- und Produktionsumgebung. Dazu wird die CI/CD Toolchain konfiguriert mit den dazugehörigen automatisierten Tools in der Cloud.

Eine detaillierte Beschreibung des Service „Cloud Application Operation" sowie die dazugehörigen Service Level werden in der beiliegenden separaten Leistungsbeschreibung (Anlage 1) ausgeführt.

### 3.3.3 Leistungsspezifizierung

Für die Datenbank stehen in der Entwicklungsumgebung 1 Instanz, in der Testumgebung 2 Instanzen, in der Pre-Produktionsumgebung 4 Instanzen und in der Produktionsumgebung stehen ebenfalls 4 Instanzen zur Verfügung. Der Speicherplatz der Datenbank beträgt in der Test- und Entwicklungsumgebung jeweils 50GB und in den Pre-Produktions- und Produktionsumgebungen jeweils 100GB.

Für jeden Cluster wird ein Logging Stack auf Basis EFK/EFG (ElasticSearch, Fluentd, Kibana/Graylog) entsprechend der angepassten Konfiguration bereitgestellt. (siehe Anlage 2, Kapitel 1.3 in Leistungsschein Managed PaaS)

Die Plattform wird über 3 Verfügbarkeitszonen hinweg, ohne Absicherung für den K-Fall und eine Desaster Recovery angeboten.

Eine Erweiterung des Ressourcenbedarfs wie in Kapitel 1.3 Leistungsschein Managed PaaS beschrieben ist unter den gegebenen Grundannahmen, wie in Kapitel 1.4 beschrieben nicht notwendig.

Der OTC Service Web Application Firewall wie in Kapitel 1.2.1.2 im Leistungsschein Managed PaaS beschrieben, ist nicht Vertragsgegenstand.

Ein kritischer Fehler gemäß Leistungsschein Managed PaaS (Kapitel 3.1) und Leistungsschein CNAO_CICD (Kapitel 4.4.5) tritt ein, wenn eine der für den Verifikationsprozess notwendigen Backend-Anwendungen (Verifikation Server, Lab Server, Portal Server) oder das Backend for Mobile Application (Corona Contact Tracing Server) dem Endnutzer an der vereinbarten Schnittstelle nicht zur Verfügung steht.

Für den Applikationsbetrieb setzen wir verschiedene Betriebsteams ein um den Security- und Datenschutzanforderungen gerecht zu werden (Segregation of Duty).

Der Applikationsbetrieb der Verification Komponenten und des SAP „mobile Backend Application" erfolgt im Mischbetrieb sowohl aus Deutschland, als auch aus Ungarn und nicht aus Indien.

Die optionalen Leistungen des Services Application Service (ASE) aus Kapitel 2.1 Leistungsbeschreibung CNAO_CI/CD (Anlage 2), SpoC – Service Desk, Deployment neuer Versionen, Kapazitätsmanagement, Eskalationsmanagement, Aufsetzen agiler Prozesse und Bereitstellungsautomatisierung sind enthalten. Ebenso ist die Leistung DevOps Beratung (Consulting) aus Kapitel 4.2.4 Leistungsbeschreibung CNAO_CI/CD (Anlage 2) enthalten.

### 3.3.4 Mitwirkungspflichten des Kunden

Die Regelungen der Ziffer 2 (RACI Matrix) des Managed PaaS Leistungsscheins finden keine Anwendung.

### 3.3.5 Leistungsabgrenzungen und Mitwirkungsleistungen durch SAP

Die Verantwortung des Releaseprozesses (Bereitstellung Backlog + Releasedokumentation, Aussprechen von Freigaben, Q-Gate Definition, Rollback Szenarien) obliegt für die Verification Server Komponenten der Telekom und für die Backend for mobile Application Anwendung der SAP.

Für den Applikationsbetrieb ergeben sich mehrere Schnittstellen bzw. Übergabepunkte mit der SAP in den Bereichen Event Management, Incident Management, Change Management sowie Deployment. Diese werden im Folgenden genauer definiert.

Event Management

Das Cloud Application Operation Team der Telekom ist für das Erstellen und die Pflege von Monitoring Dashboards und Alerting zuständig. Um die notwendigen Metriken der Applikationen bzw. Services zu erhalten, ist die Unterstützung der SAP notwendig. Anhand dieser Metriken erstellt das Cloud Application Operation Team der Telekom entsprechende Monitoring Dashboards. Darüber hinaus ist die Definition von Schwellwerten von der SAP für die Erstellung von Alarmen/Events für die verschiedenen Applikationen/Services beizustellen.

Incident Management

Der Incident Workflow sieht den Service Desk der Telekom als zentrale Anlaufstelle für den Kunden zur Aufnahme von Incidents (1st Level Support). Der 2nd Level Support erfolgt

durch das jeweilige Cloud Application Operations Team der Telekom. Falls eine Lösung im 2nd Level Support nach Lösungsvorgabe der SAP nicht möglich ist, wird das Ticket an den 3rd Level Support der SAP übergeben. In diesem Fall endet mit der Übergabe an die SAP die Leistungserbringung des 2nd Levels. Für die Lösung von kritischen Fällen (Prio 1 und Prio 2) ist die Bereitstellung eines On-Call Services seitens der SAP notwendig. Der schematische Ablauf für Incidents ist in der folgenden Grafik dargestellt.

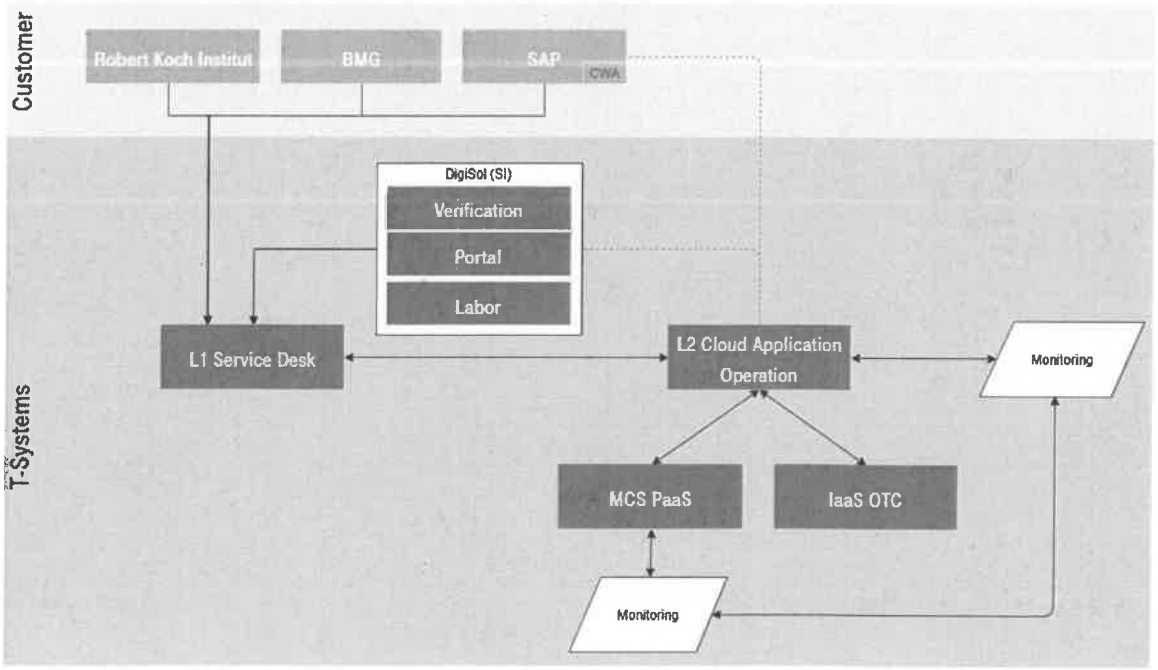



Abbildung 5: Schematischer Ablauf für die Bearbeitung von Incidents

## Change-Management

Deployments (funktionale Deployments und Hotfixes) behandeln wir als Standard Changes und werden nachfolgend beschrieben. Non-Standard Changes (bspw. Infrastruktur Changes, Changes an den CI/CD Tools bzw. an deren Version) sollten von SAP über den SDM eingereicht werden und werden vom SDM mit dem Kunden abgestimmt.

## Deployment

In der Entwicklungs- (Dev) und Testumgebung (Int) erhält die SAP die notwendigen Berechtigungen auf der Plattform und den benötigten Tools der Telekom. SAP trägt die Verantwortung für das Deployment von Anwendungscode in Dev und Int.

Der Übergabepunkt für das Deployment von Anwendungscode der SAP in der Pre-Produktion (WRU) und Produktionsumgebung (Prod) stellt die Magenta Trusted Registry der Telekom dar. Dort werden Container Images abgelegt. Folgende Voraussetzungen müssen für die dort abgelegten Images von SAP gelten:

- Die Images sind von SAP freigegeben und mit dem Kunden abgestimmt
- Das Cloud Application Operation (CAO) Team der Telekom erhält Zugriff auf vollständige Releasenotes
- SAP stellt die Dokumentation für ein Rollback Szenario zur Verfügung

Vor dem Deployment in der Prod Umgebung werden diverse Q-Gate Anforderungen vom CAO Team der Telekom geprüft (Releasenotes + Rollbackszenario vorhanden, Testergebnisse ohne Fehler, Monitoringanalyse ohne Auffälligkeiten). Ist eine der Q-Gate Überprüfungen vor dem Deployment auf Prod nicht erfüllt, wird der Change nicht

durchgeführt und zurückgegeben an das jeweilige Entwicklungs-Team der SAP. Der Prozess, sowohl für die interne Anwendungsentwicklung des DigiSol Teams der Telekom, also auch für die Zusammenarbeit mit SAP ist in dem folgenden Diagramm dargestellt.

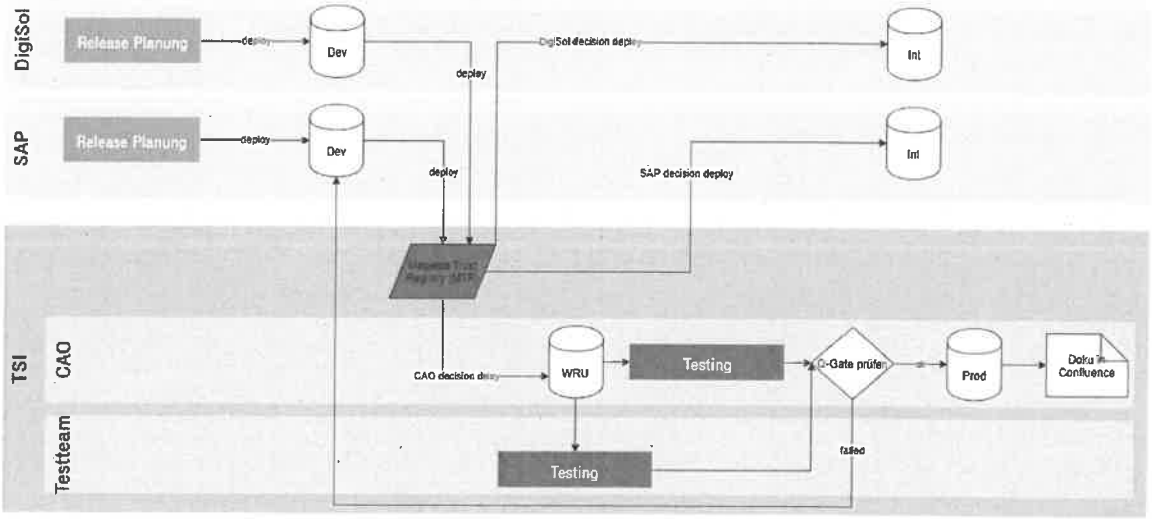



Abbildung 6: Deployment Prozess

| Mitwirkung / Beistellung | Dritter |
|---|---|
| Stellung des 3rd Level Supports, sowie auch Sicherstellung der Rufbereitschaft bei Incidents der Priorität 1 und 2 | SAP |
| Versionsupgrades der CI/CD Tools, sofern kundenspezifische Plugins installiert wurden, bedürfen der Unterstützung, um weiterhin die Kompatibilität zu gewährleisten. | SAP |
| Verantwortung des Test-Prozesses innerhalb von Entwicklungs- und Testumgebung. Sowie die Bereitstellung von Backlog und Releasedokumentation und Lieferung von vollständigen und verständlichen Releasenotes, um Fehlervorbeugung bei den Releases zu gewährleisten. | SAP |
| Scripte für das Deployment und für Rollback-Szenarien | SAP |
| Es obliegt der Verantwortung der SAP durch eine entsprechend angemessen robuste Applikationsarchitektur für eine dem Anwendungsbetrieb angemessene Verfügbarkeit seiner Applikationen Sorge zu tragen. | SAP |

## 3.4 IT-Sicherheit nach GOLIVE

Die Telekom liefert ein angemessen hohes IT-Sicherheitsniveau für alle Komponenten im Angebotsumfang. Alle angebotenen Leistungen genügen den marktüblichen „Security Best Practices", konkret den Technischen Sicherheitsrichtlinien der Telekom[3], die sowohl während der Entwicklung und Bereitstellung erbracht werden als auch während der anschließenden Betriebsphase in Form von Managed Services. Die Telekom ist vollumfänglich nach ISO 27001 zertifiziert. Die Maßnahmen zur IT Sicherheit werden in Phase nach GOLIVE nach Maßgabe der nachstehenden Bestimmungen weiterentwickelt.

Die Leistungen im Bereich IT-Sicherheit in der Betriebsphase gliedern sich in Einzelleistungen, die im Folgenden beschrieben werden.

Die Einzelleistungen der Abschnitte 2.4.1 Teilprojektleitung IT-Sicherheit, 2.4.2 IT-Sicherheitsberatung, 2.4.3 IT-Sicherheitskonzepte und 2.4.5 IT-Sicherheits-Review werden über den GOLIVE-Termin hinaus fortgeführt. Für die Leistungsbeschreibung wird auf die genannten Abschnitte verwiesen.

### 3.4.1 Managed Cyber Defense

Da ein Hauptziel der Anwendung die Wahrung der Anonymität der Nutzer ist, ist keine Übertragung von Logdaten mit personenbeziehbaren Daten der Nutzer (z. B. IP-Adressen) an das SIEM vorgesehen. Die Leistungen in den o. g. Abschnitten umfassen deshalb nicht die Verarbeitung und Analyse von personenbeziehbaren Daten der Nutzer, d. h. insbesondere keine Daten aus den mobilen Endgeräten und keine Anfragedaten von Nutzern an das Backend der Anwendung.

Die in Abschnitt 3.4.1.3 angebotene tiefere Analyse im Rahmen der Incident Response bezieht sich rein auf Daten und Systeme des Backend der Applikation. Die Leistungen umfassen keine Analysetätigkeiten von Endgeräten der Nutzer, insbesondere ist kein direkter Kontakt zu Nutzern vorgesehen.

#### 3.4.1.1 Security Operations Center inklusive SIEM

Um die IT-Sicherheit der Gesamtlösung in der Betriebsphase zu gewährleisten, überwacht die Telekom mittels einem Managed Cyber Defense Service wichtige Komponenten.

Der Service kombiniert automatisierte und manuelle Analysen von sicherheitsrelevanten Logs aus den IT-Systemen. Zusätzlich werden tagesaktuelle Threat Intelligence Informationen der Telekom genutzt, um die Qualität der Analysen zu steigern.

Die Managed Cyber Defense Services der Telekom ermöglichen:

- Angriffsversuche sowie ggf. erfolgreiche Kompromittierungen von Systemen und Identitäten zu erkennen und Gegenmaßnahmen einleiten zu können;
- durch qualifizierte Threat Intelligence Informationen (TI Feeds) eine signifikante Verringerung von False Positive Meldungen, so dass keine unnötigen Aufwände im Incident Response Prozess entstehen.

[3] https://www.telekom.com/resource/blob/314436/4ba45c4dd017c1652e61daddab7679a9/dl-technische-sicherheitsanforderungen-data.zip

### 3.4.1.2 Log-Verarbeitung und Alarm-Erzeugung

IT-Sicherheitsrelevante Logfiles werden zur Alarmierung von Auffälligkeiten oder zur Untersuchung von potentiellen Vorfällen an eine Security Information und Event Management-Lösung (SIEM) weitergeleitet. Hierzu wird das Magenta SIEM eingesetzt, eine Eigenentwicklung der Telekom. Unsere Lösung unterstützt eine Echtzeitalarmierung, eine Langzeitanalyse auf historischen Daten und auch eine vorfallbezogene Untersuchung.

Zur Echtzeitalarmierung und Langzeitanalyse werden Regelsätze im System konfiguriert. Diese Alarmierung ist auf Bedrohungsszenarien ausgerichtet, die auf die Plattform wirken und von eigenen Experten modelliert werden. Typische Alarmierungsszenarien sind beispielweise Versuche, Passworte durch simples Ausprobieren zu brechen oder aber auch der Abgleich von Logdaten gegen Indikationen, die bekanntermaßen auf maliziöse Aktivität hindeuten.

Damit eine Alarmierung unmittelbar erfolgt, wird ein Push-Verfahren eingesetzt. Logdaten werden direkt nach der Erzeugung auf dem Quellsystem an das SIEM weitergeleitet. Dies erfolgt über eine Transport Layer Security (TLS) gesicherte Verbindung und mittels der HTTP-Anfragemethode POST. Die TLS-Verbindung gewährleistet zum einen die Verschlüsselung der Verbindung und benutzt andererseits zusätzlich Client Zertifikate, so dass Sender und Empfänger jeweils authentisiert sind. Alle verwendeten kryptographischen Verfahren richten sich nach der technischen Richtlinie des BSI „BSI TR-02102-1 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ in der jeweils aktuellen Version.

Auf der SIEM-Plattform werden die Daten unmittelbar verarbeitet und eingelesen. In diesem ersten Schritt greift die Echtzeitarmierung nach konfigurierten Regelsätzen. Die Daten werden für sieben Tage gespeichert, um Analysen in die Vergangenheit über diesen Zeitraum vorzunehmen. Diese Analysen erfolgen mittels automatisierter Regeln oder incidentbezogen, wenn bspw. automatisierte Untersuchungen Anlass geben, weitergehende Analysen durchzuführen.

Die SIEM-Plattform ist hochverfügbar ausgelegt und wird sowohl fachlich als auch betrieblich in einem 24/7-Modell betrieben.

Die Detektionsszenarien (Anwendungsfälle) werden in der Projektphase nach Risiko-Abwägung sowie Verfügbarkeit entsprechender IT-Sicherheitslogs definiert und laufend optimiert. Dabei werden Informationsgehalt und Typisierung der Log-Quellen berücksichtigt, um eine effiziente Erkennung von IT-Sicherheitsvorfällen zu erreichen.

### 3.4.1.3 Security Monitoring und Incident Response

Im Rahmen des Managed Cyber Defense Service liefert die Telekom eine kontinuierliche Überwachung (24 x 7 Monitoring) der Alarmsysteme. Dieser Service wird von den Level 1- und Level 2-Analysten des Security Operations Center (SOC) der Telekom erbracht. Alarme werden in diesem Servicelevel rund um die Uhr analysiert, um mögliche Incidents zu erkennen. Die Klassifizierung und Lösung der Incidents erfolgt nach den festgelegten und risikopriorisierten Runbooks in der Aufbauphase.

Sollten die Analysen der SOC-Spezialisten Hinweise auf IT-Sicherheitsvorfälle geben, erfolgt im Rahmen von Incident Response Aktivitäten eine tiefere Analyse durch erfahrene Incident Responder der T-Systems. Diese Incident Responder übernehmen das Management des Incidents für die Telekom, legen die Remediation Strategy fest und decken Spezialthemen wie IT Forensik oder Malware Analyse ab. Nach Lösung des Incidents werden notwendige Sicherheitsmaßnahmen dokumentiert.

### 3.4.2 Penetration Testing (Fortführung)

Die Telekom unterzieht die App und die Backends („Verifikation Server", „Backend for mobile application", „Lab server" und „Portal server") einem regelmäßigem Penetrationstest. Dieser wird jährlich durchgeführt, und zwar gegen Ende eines jeden Betriebsjahres (d. h. bei 36 Monaten Laufzeit z. B. nach 9, 21 und 33 Monaten nach Inbetriebnahme).

Dabei wird der Schwerpunkt der regelmäßigen Penetrationstests jeweils festgelegt, z. B. wie folgt:

- Fokussierung auf eine Komponente, z. B. App und App-Backend. Dies ist vergleichbar mit dem initial durchgeführten Penetrationstest.
- Fokussierung auf geänderte/aktualisierte Komponenten.
- Erweiterung des Umfangs, z. B. auf Test- und Integrationssysteme, und/oder Systeme mit Schnittstellen („Test labs", „Health Authority"), und/oder Erweiterung der Prüfmethoden (z. B. Social Engineering).

Der Aufwand für den regelmäßigen jährlichen Penetrationstest wird auf eine feste, maximale Zahl von Personentagen im Jahr beschränkt. Sofern wichtige Anlässe – z.B. umfangreiche Änderungen – anstehen, wird der jährliche Test in zwei kleinere Tests aufgespalten, die zu unterschiedlichen Zeiten im Jahr stattfinden.

Telekom liefert den Ergebnisbericht für jeden regelmäßigen Test im PDF-Format.

### 3.4.3 Red Teaming

Im Gegensatz zum Penetration Testing gibt es beim sogenannten Red Teaming keine Einschränkung der untersuchten Komponenten und eingesetzten Methoden.

Red Teaming Übungen testen darüber hinaus die zur Anomalie- bzw. Angriffserkennung eingesetzten Sensoren und Alarmierungsverfahren.

Telekom führt einmal jährlich eine Red Teaming-Übung auf die von ihr betriebene IT-Infrastruktur durch.

### 3.4.4 IT-Sicherheitskonzept nach BSI-Standards 200-x

In Abstimmung mit dem RKI wird für den gesamten Informationsverbund unter Anwendung der ISO27001 oder alternativ des vom BSI empfohlenen Vorgehensmodells IT-Grundschutz 200-2 ein vollständiges und konsistentes Informationssicherheitskonzept erstellt. Als Dokumentationswerkzeug kann verinice eingesetzt werden.

Für die Erreichung dieses Ziels ergeben sich mehrere beratende Aufgabenpakete, die sich kanonisch aus der ISO27001 bzw. dem BSI-Vorgehensmodell ableiten: Festlegung des Geltungsbereichs, Modellierung, IT-Grundschutz-Checks, Risikoanalysen, Maßnahmenplanung sowie begleitende Beratung.

Das IT-Sicherheitskonzept wird anlassbezogen fortgeschrieben und einmal jährlich aktualisiert.

Die Vergütung für die Erstellung und Fortschreibung des Sicherheitskonzepts erfolgt nach Aufwand.

Sofern sich aus dem IT-Sicherheitskonzept nicht oder nur teilweise umgesetzte Anforderungen auf Seiten der Telekom ergeben, sind diese gesondert zu vergüten und es wird ein Change Request Verfahren eingeleitet.

### 3.4.5 IT-Sicherheitsbeauftragter IT-Grundschutz

Um einen reibungslosen IT-sicherheitstechnischen Ablauf zu gewährleisten, ist die Rolle eines vorhabenbezogenen IT-Sicherheitsbeauftragten während der Betriebsphase nach GOLIVE vorgesehen. Dieser sorgt für die Koordination, Steuerung sowie Kommunikation mit allen Beteiligten in allen relevanten IT-Sicherheitsbelangen.

Zu den Hauptaufgaben des IT-Sicherheitsbeauftragten gehören die Kundenkommunikation zur IT-Sicherheit und das kundenbezogene Berichtswesen zur IT-Sicherheit. Darüber hinaus gehören das Steuern und Überwachen eines konsistenten IT-Sicherheitsniveaus und der risikoorientierten Umsetzung von Maßnahmen zur IT-Sicherheit und Cyber Defence mit Bezug auf den Service dazu. Der IT-Sicherheitsbeauftragte unterstützt bei der Erstellung und Fortschreibung von servicebezogenen IT-Sicherheitsdokumentationen und -konzepten.

### 3.4.6 Annahmen und Rahmenbedingungen

Die im Abschnitt 3.4.1 beschriebenen und kalkulierten Tätigkeiten berücksichtigen keine Großstörungen durch Komponenten, auf welche die Telekom keinen Einfluss hat. Beispiel: Mehrere Millionen ungewöhnliche serverseitige Ereignisse durch fehlerhafte oder vorsätzlich manipulierte Software-Komponenten in Mobiltelefonen. Die Telekom reagiert auf Großstörungen gemäß „Best Effort". Die Aufwände seitens Telekom bei einer Großstörung werden separat und nach Aufwand berechnet.

### 3.4.7 Leistungsabgrenzung

Bezüglich IT-Sicherheitskonzept nach ISO 27001 oder BSI-Standards 200-x sind die folgenden Aufgaben nicht Bestandteil der angebotenen Leistung:

- Planung und Umsetzung von nicht oder nur teilweise umgesetzten Anforderungen aus dem IT-Sicherheitskonzept auf Seiten des Auftraggebers oder anderer Auftragnehmer
- Planung und/oder Durchführung von Zertifizierungen
- Maßnahmencontrolling/Koordinierung der Maßnahmenumsetzung, sofern sich die Maßnahmen nicht auf die Telekom beziehen.

### 3.4.8 Mitwirkungspflichten des Kunden

- Der Auftraggeber stellt Ansprechpartner bei sich selbst und bei weiteren Auftragnehmern wie SAP bzw. Meldewege zur Verfügung, damit die Telekom im Incident-Fall unmittelbar benachrichtigen und die notwendigen weiteren Schritte abstimmen kann.
- Bei Aufklärung von Sicherheitsvorfällen, die den Zugang zu Daten oder Systemen außerhalb des Zuständigkeitsbereichs der Telekom bedürfen, muss der Auftraggeber die in seinem Einflussbereich zur Aufklärung notwendigen Informationen in ausreichender Qualität zur Verfügung stellen.
- Identifizierung und Koordination der erforderlichen Ansprechpartner außerhalb der Telekom (d. h. seitens Auftraggeber und anderer Auftragnehmer)
- Bereitstellung von vorhandenen oder in der Entstehung befindlichen Dokumentationen außerhalb der Telekom sowie aller notwendigen Informationen, insofern zur Leistungserbringung notwendig Koordinierung erforderlicher

Besprechungen und Interviewtermine, insbesondere Bereitstellung der hierzu erforderlichen Fachexperten außerhalb der Telekom

- Für Penetrationstests als auch Red Team Einsätze ist eine Einverständniserklärung des Auftraggebers und ggf. weiterer Auftragnehmer und eine Festlegung der Rahmenbedingungen (auch „Rules of Engagement" genannt) erforderlich.

## 3.5 Netzwerk nach GOLIVE

Die Betriebstätigkeiten der Services der Phase vor GOLIVE werden fortgesetzt.

## 3.6 Hotline Services nach GOLIVE

Die Hotline Services vor dem GOLIVE werden unterschieden in:

Standardleistungen der Telekom:

- 0800 Freecall Leistungen der Telekom (als Zugangsmedium)
- IVR (Interactive Voice Response)

Sowie spezielle Supportleistungen:

- Technische Hotline
- Verifikations-Hotline

Für beide Hotlines wurde festgelegt, dass jeweils eine 0800 Freecall Nummer zum Einsatz kommen soll. Bei der technischen Hotline wird eine IVR zur Vorqualifizierung bzw. zum Schutz der technischen Hotline vorgeschaltet.

### 3.6.1 0800 Freecall Leistungen der Telekom

Die Telekom überlässt dem Kunden im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten den freecall 0800.

**A: Beistellung BMG**

Voraussetzung für die Inanspruchnahme von freecall 0800 ist die Beistellung des dem Kunden von der Bundesnetzagentur zugeteilten Rufnummer für den jeweils entsprechenden Dienst.

Voraussetzung für die Inanspruchnahme von Local Service Call ist ein Festnetz-Anschluss der Telekom auf Basis des Protokolls DSS1 oder ein IP-basierter Festnetz-Anschluss der Telekom. Hiervon sind bestimmte IP-Anschlüsse im Netz der Telekom ausgenommen. Der Festnetz-Anschluss und die Zuteilung der jeweiligen Rufnummer ist nicht Gegenstand dieses Vertrages.

**A.1: Verkehrsführungsprogramm**

Mittels des Verkehrsführungsprogramms bestimmen wir, aus welchen Einzugsbereichen, zu welchen Zeitfenster und zu welchen Zielen ankommende Verbindungen weitergeschaltet werden.

Das Verkehrsführungsprogramm hat für den Anrufer eine mittlere Verfügbarkeit von mindestens 99,9 % im Jahresdurchschnitt.

### A.2: Zeitfenster

Auswahl

- von Wochentag und Uhrzeit, zu denen die Anrufe zu den vom Kunden bestimmten Zielen weitergeleitet werden (periodische Zeitfenster) und
- von festgelegten Zeiträumen, zu denen die Anrufe zu den vom Kunden bestimmten Zielen weitergeleitet werden (temporäre Zeitfenster).

Ein temporäres Zeitfenster hat Vorrang vor einem periodischen Zeitfenster.

### A.3: Ziele

- Festnetz-Anschlüsse im In- und Ausland,
- Mobilfunk-Anschlüsse im In- und Ausland,
- nationale Teilnehmerrufnummern in Deutschland mit der Zugangskennzahl 032 (NTR 032),
- Zielansagen der Telekom,
- kundenindividuelle Ansagen,
- Servicenummern in Deutschland,
- Plattformen der Telekom,
- Satellitenfunkdienste oder
- Funkrufdienste.

Im Verkehrsführungsprogramm sind standardmäßig bis zu fünf Ziele einstellbar.

Das Ziel wird durch die Rufnummer (Landeskennzahl – soweit erforderlich –, Ortsnetzkennzahl bzw. Zugangskennzahl und Teilnehmerrufnummer) eindeutig gekennzeichnet. Die Mehrfachanwendung eines Ziels innerhalb eines Verkehrsführungsprogramms ist möglich. Zielansagen der Telekom, kundenindividuelle Ansagen sowie Warteschleifenansagen bei 0180call werden bei der Ermittlung der Anzahl der Ziele eines Verkehrsführungsprogramms nicht mitgezählt.

Die Telekom aktiviert mit der betriebsfähigen Bereitstellung des Verkehrsführungsprogramms zunächst nur das mit dem Kunden vereinbarte erste Ziel als Grundeinstellung.

### A.4: freecall 0800, 0180call und Local Service Call Verbindungen

Die Telekom schaltet die für eine freecall 0800 Call-Rufnummer ankommenden Anrufe zu den in einem Verkehrsführungsprogramm bestimmten Zielen weiter.

### B: Service

Die Telekom beseitigt unverzüglich Störungen ihrer technischen Einrichtungen im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten. Hierbei erbringt sie insbesondere folgende Serviceleistungen:

### B.1 Serviceannahme

Die Telekom nimmt täglich von 0.00 bis 24.00 Uhr Störungsmeldungen unter den Service-Telefonnummern entgegen.

### B.2 Servicebereitschaft

Die Servicebereitschaft ist werktags (montags bis freitags), soweit diese Tage keine gesetzlichen Feiertage sind, von 7.30 bis 20.00 Uhr.

**B.3 Reaktionszeit**

Die Telekom teilt auf Wunsch des Kunden während der Servicebereitschaft ein erstes Zwischenergebnis mit, wenn eine Rückrufnummer angegeben wurde. Diese Mitteilung erfolgt innerhalb von drei Stunden (Reaktionszeit) ab der Störungsmeldung.

Zeiten außerhalb der Servicebereitschaft werden auf die Reaktionszeit nicht angerechnet. Die Reaktion kann auch durch Antritt des Servicetechnikers vor Ort beim Kunden erfolgen.

**B.4 Rückmeldung**

Die Telekom informiert den Kunden nach Beendigung der Entstörung. Wird der Kunde beim erstmaligen Versuch nicht erreicht, gilt die Entstörungsfrist gemäß B.5 als eingehalten. Weitere Versuche zur Rückmeldung werden regelmäßig durchgeführt.

**B.5 Entstörungsfrist**

Die Telekom beseitigt während der unter den in B.2 genannten Zeiten der Servicebereitschaft die Störung innerhalb von 24 Stunden (Entstörungsfrist) nach dem Eingang der Störungsmeldung. Zeiten außerhalb der Servicebereitschaft werden auf die Entstörungsfrist nicht angerechnet.

Die Frist ist eingehalten, wenn die Störung innerhalb der Entstörungsfrist zumindest so weit beseitigt wird, dass die Leistung (ggf. übergangsweise mit Qualitätseinschränkungen) wieder genutzt werden kann und die Rückmeldung gemäß B.4 erfolgt.

Ferner ist die Frist auch eingehalten, wenn als Fehlerursache eine Störung im Netz anderer Netzbetreiber festgestellt wird. Störungen in Netzen anderer Netzbetreiber sind nicht Gegenstand dieses Vertrages.

### 3.6.2 IVR (Interactive Voice Response)

Die Technische Hotline wird mit einer Schutz-IVR versehen. Dies bedeutet, bei einem Anruf muss der Anrufende sich noch aktiv für „technische Fragen" entscheiden. Hierfür wird das Telekom-Produkt IVR Business zum Einsatz kommen.

**A: Servicebeschreibung**

Die Telekom ermöglicht im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten die Nutzung von Sprachdialogsystemen Interactive Voice Response Business (IVR Business).

Die ankommenden Anrufe werden zunächst zu dem IVR Business-System der Telekom weitergeschaltet.

Durch das IVR Business -System erhält der Anrufer entweder eine abschließende Ansage (Voice-File) oder die für die Service-Rufnummer ankommenden Anrufe erhalten eine Ansage und werden anschließend durch eine individuelle Verkehrsführung (Routingentscheidung) zu den Zielen – auch mit unterschiedlichen Standorten – weitergeschaltet.

Die individuelle Routingentscheidung erfolgt in Abhängigkeit von dem Dialog mit den Anrufern über das IVR Business-System der Telekom. Die Anrufer können eigenständig menügeführt durch das IVR Business-System mit festgelegten Kommandos, die im Mehrfrequenzwahlverfahren (DTMF) übermittelt werden oder mittels Spracherkennung Automatic Speech Regocniton (ASR), zu den vom Kunden in der Menüsteuerung festgelegten Zielen weitergeschaltet werden. Neben dem Erstziel werden noch jeweils drei Ersatzziele angeboten, wenn ein Ziel schon für eine andere Verbindung genutzt wird – Besetzt – oder die Verbindungen bei dem Ziel innerhalb eines von der Telekom festgelegten Zeitraumes nicht entgegengenommen wird – Kunde meldet sich nicht –.

Die Telekom schaltet die Service-Rufnummer auf das IVR Business-System und testet die Funktionalität. Das Verkehrsführungsprogramm der Service-Rufnummer kann als Defaultrouting bei Nichterreichen des IVR Business-System genutzt werden.

Die Telekom kann die Zugangsschnittstellen zu der IVR Business-Plattform aus technischen oder betrieblichen Gründen ändern. Die Nutzung der für den Zugang erforderlichen Verbindungen sowie die Nutzung des Internets sind nicht Gegenstand dieses Vertrages.

Parallel zur Nutzung des IVR Business-Systems sind die Leistungen Internet Manager plus, Customer Control, feste Durchwahl, Follow Me und CallGuard von freecall 0800, freecall International, freecall Universal, 0180call, Shared Cost International, Local Service Call oder Global Service Call nicht nutzbar.

**B: Einrichtung**

Unterstützung bei der Ersteinrichtung und Anpassung von IVR Business (z. B. Anlegen von Routingprofilen, Anlegen und Löschen von Modulen, Änderung der Routingziele, der Menüsteuerung, der Voice-Files, der Einzugsbereiche, der Zeitfenster, Setzen und Erhalt von Zählerpunkten, Einrichten von Voice Recording, Beratung bei Stimm- und Klangkonzept, Dialogdesign und Audioproduktion, Call-Flow Änderungen und/oder Durchführung eines Quality Check durch einen Operator der Telekom. Diese Leistung wird nach Aufwand abgerechnet.

Die Telekom stellt eine individuelle Ansage zur Verfügung, die im Störungsfall zur Informationsverbreitung bzw. als Hinweisansage auf Wunsch anlässlich einer Störungsmeldung aktiviert wird. Die Ansage wird montags bis freitags von 7.30 bis 20.00 Uhr, soweit diese Tage keine bundeseinheitlichen gesetzlichen Feiertage sind, innerhalb von maximal einer Stunde, in der übrigen Zeit innerhalb von maximal zwei Stunden aktiviert. Die Ansage bleibt bis zur Beendigung der Störung geschaltet. Die Gesamtlänge der individuellen Ansage beträgt höchstens 60 Sekunden.

**C: Service**

Die Telekom beseitigt im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten unverzüglich Störungen ihrer technischen Einrichtungen. Sie nimmt täglich von 0.00 bis 24.00 Uhr Störungsmeldungen unter den Service-Telefonnummern entgegen. Es gelten dabei folgende Parameter:

**C.1 Servicebereitschaft**

Die Servicebereitschaft ist täglich von 0.00 bis 24.00 Uhr.

**C.2 Reaktionszeit**

Die Telekom teilt innerhalb von 30 Minuten ab der Störungsmeldung ein erstes Zwischenergebnis mit, wenn eine Rückrufnummer angegeben wurde.

**C.3 Zwischenmeldung**

Die Telekom erteilt montags bis freitags von 7.30 bis 20.00 Uhr, soweit diese Tage keine bundeseinheitlichen gesetzlichen Feiertage sind, unter der vom Kunden angegebenen Rückrufnummer mindestens einmal je Stunde nach Ablauf der Reaktionszeit gemäß Ziffer C.2 eine Zwischenmeldung über den Bearbeitungsstand und den Ausblick auf weitere Maßnahmen. Die Zwischenmeldung erfolgt sofort bei Änderung des Bearbeitungsstandes. Außerhalb der Regelarbeitszeit erfolgen Zwischenmeldungen nach Vereinbarung zwischen Störungsmelder und Telekom.

### C.4 Entstörungsfrist / Rückmeldung

Die Telekom beseitigt die Störung innerhalb von vier Stunden nach Erhalt der Störungsmeldung. Die Frist ist eingehalten, wenn die Störung innerhalb der Entstörungsfrist zumindest so weit beseitigt wird, dass das IVR Business-System (ggf. übergangsweise mit Qualitätseinschränkungen) wieder genutzt werden kann. Ferner ist die Frist auch eingehalten, wenn als Fehlerursache eine Störung im Netz anderer Netzbetreiber festgestellt wird. Störungen in Netzen anderer Netzbetreiber sind nicht Gegenstand dieser Leistung.

Die Telekom informiert den Kunden nach Beendigung der Entstörung.

## 3.6.3 Die Leistungen des Supports im Überblick:

Nach dem Anruf über die 0800 Nummer verzweigen sich die Anrufe über die IVR. Dies wird im Wesentlichen wie folgt geschehen:

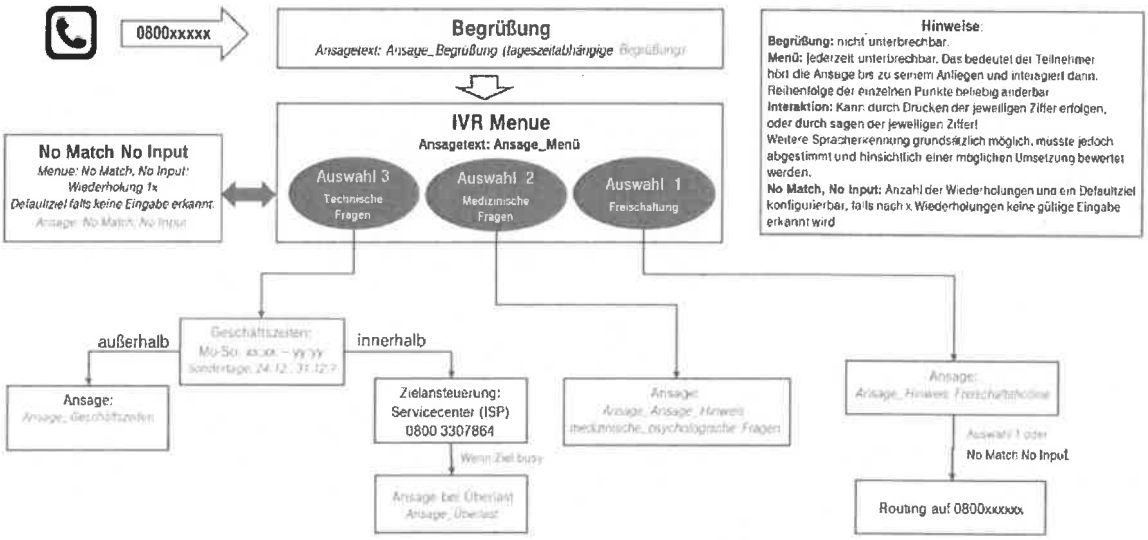



Abbildung 7: Design IVR technische Hotline

Die Support Services bis GOLIVE umfassen den Aufbau der in den nachfolgenden Gliederungspunkten beschriebenen Leistungs- und Servicemerkmalen. Nach dem GOLIVE werden dem Auftraggeber umfassende Auswertungen und Optimierungsvorschläge aus dem laufenden Betrieb unterbreitet (Beschreibungen folgen später)

### Technische Hotline

Technischer Support zur Installation und Nutzung der CoronaWarnApp auf Basis der Betriebssysteme iOS und Android sowie weiterführende Fragen zur APP. Fokus der Tätigkeit bildet die telefonische Unterstützung und Hilfestellung im Zusammenhang mit der Corona-App. Technisch komplexe Unterstützungsleistungen sind nicht vorgesehen.

Der technische Support beinhaltet die Unterstützung per Telefon:

- Hilfe, wenn der Bürger seine Accountdaten für die Nutzung des Playstore/ App Store nicht kennt (z.B. Passwort zurücksetzen oder Konto einrichten)
- Download + Installation der App aus dem Playstore/App Store
- Einstellungen in der App vornehmen
- Einstellungen am mobilen Endgerät vornehmen (Bluetooth, mobile Datennutzung…)

- Technischer Support beim Einlesen des QR-Codes über die CoronaWarnApp
- Probleme beim digitalen Verifikationsprozess

Die Leistungserbringung erfolgt nur im Zusammenhang mit der CoronaWarnApp.

Es werden keine medizinischen Fragen, Fragen zur allgemeinen Pandemie oder Fragen zum Datenschutz beantwortet. In diesen Fällen wird auf geeignete, vom Auftraggeber zur Verfügung gestellte, Dokumentationen (z.B. Webseiten) oder Hotlines verwiesen.

**Verifikations Hotline**

Es wird zum besseren Verständnis zwischen einem **„digitalen" Verifikationsprozess** und einem **„manuellen" Verifikationsprozess** unterschieden.

a. Der digitale Prozess beschreibt die Verifikation eines Testergebnisses innerhalb der Tracing-App.
b. Der manuelle Prozess beschreibt die Verifikation eines Testergebnisses durch ein Call-Center.

Die beschriebenen Prozesse basieren auf einem **„Ein-App-Verfahren"**, in dem die Benachrichtigung über den Infektionsstatus und das Contact-Tracing in einer App zusammengeführt sind. Bei Problemen innerhalb des „digitalen" Verifikationsprozesses" kommt die oben beschrieben Technische Hotline zum Einsatz. Die Verifikations-Hotline kommt erst dann zum Einsatz, wenn der „digitale" Verifikationsprozess fehlschlägt und der Nutzer die „manuelle" Verifikation starten möchte (der QR-Code liegt dem App Nutzer **nicht** vor und kann **nicht** gescanned werden).

Unter die Leistungen der Hotline fallen dann:

- Plausibilisierung mit dem Anrufer, ob tatsächlich ein positives Testergebnis vorliegt
- Erzeugung einer TAN über eine Backend-Schnittstelle
- Kommunikation der TAN an Anrufer

Die Leistungserbringung erfolgt nur im Zusammenhang mit der CoronaWarnApp.

Es werden keine medizinischen Fragen, Fragen zur allgemeinen Pandemie oder Fragen zum Datenschutz beantwortet.

### 3.6.4 Servicezeiten und SLA

Die **Technische Hotline** wird von Montag bis Samstag von 7.00 bis 22.00 Uhr zur Verfügung stehen, soweit diese Tage keine gesetzlichen Feiertage sind und umfasst zum Start 3000 Calls pro Tag, soweit diese Tage keine gesetzlichen Feiertage sind.

Die Leistungserbringung erfolgt i.d.R. umgehend beim Erstkontakt. Ist dies nicht möglich, meldet sich der Kunde nochmals (Verzicht auf Rückruf zur Vermeidung potenzieller Datenschutzprobleme). Bei Anrufen außerhalb dieser Zeiten wird für beide Hotlines jeweils mittels IVR (Interactive Voice Response) auf die Öffnungszeiten der Hotline verwiesen. Die Ansagen und Sprecher werden vom Auftraggeber freigegeben, die Telekom macht entsprechende Vorschläge.

Die **Verifikations-Hotline** wird in einem 7 x 24 Stunden Modus angeboten; dies umfasst auch Sonntage und gesetzliche Feiertage, bei 1000 Calls pro Tag.

Die Leistungserbringung erfolgt i.d.R. umgehend beim Erstkontakt. Ist dies nicht möglich, meldet sich der Kunde nochmals (Verzicht auf Rückruf zur Vermeidung potenzieller Datenschutzprobleme).

### 3.6.5 Voraussetzungen

Die Beratung der technischen Hotline erfolgt telefonisch. Ein Erfolg der Beratung wird durch den Auftragnehmer nicht geschuldet.

### 3.6.6 Abgrenzung der Leistungsanteile der Telekom

Es wird ausschließlich ein 1st Level Support für den Endnutzer erbracht.

### 3.6.7 Mitwirkungsleistungen und Beistellungen des Kunden

- Funktionen der APP (Warum braucht man diese APP, Was leistet diese AP? etc.)
- Fragen zur Nutzung der APP (Wozu? Was bring mir das oder anderen? Bin ich gesetzlich verpflichtet? etc.)
- Fragen zur technischen Anwendung (Wie kommuniziert die App? Spielt die Netzabdeckung eine Rolle? Etc.)
- Sonstige Fragen (z.B. Wo bekomme ich weitere Informationen?)
- Zeitnahe Bestellung der 0800 Nummern durch RKI (bis 13.05.2020)
- Abnahme Freigabe der IVR Ansagetexte
- Auswahl des entsprechenden Sprechers sowie der Wartemusik

Die Leistungserbringung erfolgt nur im Zusammenhang mit der Corona App.

### 3.6.8 Annahmen und Rahmenbedingungen

Die Barrierefreiheit der technischen Hotline und der Verifikations Hotline wird zum GOLIVE über eine vereinfachte Sprache umgesetzt. Darüberhinausgehende Maßnahmen werden im Rahmen des Change Request Verfahrens kostenpflichtig umgesetzt.

**Technische Hotline:**

Die maximale Call-Anzahl der Technischen Hotline zum Start der der CoronaWarnApp beträgt 3000 Calls pro Tag. Bei Überschreitung die Anzahl erfolgt ein Ansagetext „Rufen Sie bitte zu einem späteren Zeitpunkt wieder an).

Die vertraglich vereinbarten Callmengen zum Projektstart von 3000 pro Tag werden über die Laufzeit von 6 Monaten pauschal vom Auftraggeber vergütet. Zugrunde liegt dabei eine durchschnittliche Gesprächsdauer von 10 Minuten.

Ende des dritten Monats erfolgt ein Review und daraus folgend eine Anpassung der vertraglich vereinbarten Callmengen und der Gesprächsdauer anhand der durchschnittlichen Gesprächsdauer und Callmengen in den Monaten 1-3, gültig ab dem 7. Monat. Die neu vertraglich vereinbarten Callmengen werden zu 100% über die kommenden 4 Monate pauschal vom Auftraggeber vergütet. Das Review erfolgt regelmäßig alle drei Monate mit den daraus folgenden Anpassungen ab dem 5. Monat.

Die Mehrmengen, die aus einer angepassten Callmenge resultieren, werden entsprechend abgerechnet.

Sofern bei einem Review die Anzahl der Calls auf unter 200 Calls pro Tag angepasst werden müsste, bleibt es bei einer Vergütung von mindestens 200 Calls pro Tag.

Die Technische Hotline erbringt den Support für Smartphones in deutscher und englischer Sprache. Drei Monate nach GOLIVE wird die die diese Hotline auch in türkischer Sprache geliefert.

**Verifikations Hotline:**

Die maximale Call-Anzahl der Verifikations Hotline zum Start der der CoronaWarnApp beträgt 1000 Calls pro Tag. Die Verifikations Hotline zum Start der App erfolgt mit den Servicezeiten 7*24 Std. auch sonntags und an Feiertagen.

Eine Reduktion der Servicezeit oder Callmenge kann nur nach 6 Monaten mit einem Vorlauf von 3 Monaten reduziert werden. Die Verifikations Hotline erbringt den Support für Smartphones in deutscher, englischer und türkischer Sprache.

### 3.6.9 Mitwirkungsleistungen und Beistellungen des Kunden

Der Auftraggeber gibt bei Überlastsituationen eine der von der Telekom definierte Gegenmaßnahmen frei.

Der Auftraggeber stellt bei Fragen, die nicht die App betreffen, geeignete Verweise auf Webseiten oder Hotlines zur Verfügung.

Zusätzlich erfolgt die Beantwortung von weiterführenden Fragen auf Basis FAQ, wenn diese durch den Auftraggeber bereitgestellt werden, z.B.:

- Funktionen der CoronaWarnApp (Warum braucht man die CoronaWarnApp, Was leistet die CoronaWarnApp etc.)
- Fragen zur Nutzung der CoronaWarnApp (Wozu? Was bring mir das oder anderen? Bin ich gesetzlich verpflichtet? etc.)
- Fragen zur technischen Anwendung (Wie kommuniziert die CoronaWarnApp? Spielt die Netzabdeckung eine Rolle? etc.)
- Sonstige Fragen (z.B. Wo bekomme ich weitere Informationen?)
- Zeitnahe Bestellung der 0800 Nummern durch RKI (bis 13.06.2020)
- Freigabe der IVR Ansagetexte
- Auswahl des entsprechenden Sprechers sowie der Wartemusik

Die Leistungserbringung erfolgt nur im Zusammenhang mit der CoronaWarnApp.

## 3.6.10 Mitwirkungsleistungen und Beistellungen SAP

| Mitwirkung / Beistellung | Dritter |
|---|---|
| Kontinuierliche Zulieferung für die Bereitstellung von aktualisierten CoronaWarnApp Dokumentationen für die Erstellung von Hotline Frage-/ Antwort-Katalogen | SAP |
| Kontinuierliche Zulieferung für die Bereitstellung von aktualisierten FAQs | SAP |

# 4 PROJEKTMANAGEMENT

Der Umfang des Projektes Corona Warn App erfordert ein ganzheitliches Projektmanagement. Dies erfolgt unter Einbeziehung von Komponenten aus dem Agilen Projektmanagement ebenso wie aus der herkömmlichen Vorgehensweise nach dem Wasserfallmodell.

Im Projektmanagement sind folgende Bausteine enthalten

- Planung inkl. Leistungen nach GoLive
- Durchführung
- Test und GoLive
- Qualitätsmanagement

Das Projektmanagement erfolgt unter Fokussierung auf Time, Budget und Quality und wird durch erfahrene und i.d.R. zertifizierte Projektleiter (PMI, Agile-Scrum) erbracht.

Wir gehen für die Governance des Projektes von bundesweit zentralen Ansprechpartnern für die auf Seiten des BMG bei der Durchführung des Projekts aus.

In das Projektmanagement fallen außerdem Unterstützungsleistungen aus den Bereichen Proximity Measurement, Scoping, Kommunikation, Public Affaires, Architektur sowie externe Unterstützung durch BCG.

Des Weiteren sind folgende Leistungselemente als Teil des Projektmanagement aufgeführt.

## 4.1 Leistungsbeschreibung der BCG

Im Folgenden stellen wir unser geplantes Vorgehen je Unterstützungsbedarf (4 Module) dar:

a) Unterstützung beim Controlling des projektübergreifenden Prozessfortschritts und des Fortschritts innerhalb der einzelnen Arbeitspakete
   - Laufende Analyse des Kritischen Pfads und Herausarbeiten von Abhängigkeiten zwischen den Arbeitspaketen
   - Tracking der Aktivitäten und Meilensteine der einzelnen Arbeitspakete inkl. Follow-Up bei den Verantwortlichen
   - Erstellung und Verwaltung von Briefingunterlagen (zentrales Dashboard) für die Projektsteuerung

b) Begleitung der Gremienarbeit und thematische Aufbereitung
   - Organisation sowie ggf. Moderation von Gremiensitzungen und Regelabstimmungen im Projekt
   - Thematische Begleitung und schriftliche und grafische Aufbereitung komplexer Projektzusammenhänge als Basis übergreifender Abstimmung, interner Entscheidungsfindung und externer Kommunikation (z.B. Aufbereitung der technischen und organisatorischen Prozesse der Laboranbindung, Darstellung von User Stories für Nutzer*innen, RKI/Gesundheitsämter etc.)

c) Internes und externes Stakeholder-Management
   - Begleitung der Projektübergabe vom bisherigen Projektteam an T-Systems und SAP und Sicherstellung der reibungslosen Fortführung weiterhin erforderlicher Projektelemente (insb. Anbindung der Labore, Weiterentwicklung Bluetooth-Proximitätsmessung)

- Organisation und Begleitung von Abstimmungsprozessen mit relevanten internen und externen Stakeholdern (insb. BMG, RKI, Fraunhofer-Gesellschaften, BSI, BfDI, KVD)
- Unterstützung bei externer Kommunikationsstrategie und der Organisation der Kommunikation mit der interessierten Fachöffentlichkeit

d) Flexible Unterstützung bei der Adressierung kritischer Probleme im Projektverlauf

- Flexible koordinative und wenn nötig operative Unterstützung in kritischen Projektthemen
- Aktuelle Themen für mögliche Unterstützung sind hier aus unserer Sicht insbesondere:
  - Unterstützung bei der organisatorischen Anbindung der Labore und dem Aufbau des Callcenters sowie Koordination der diesbezüglichen Abstimmungen mit BMG, RKI und KVD
  - Unterstützung der Erarbeitung der Kommunikationsstrategie (Positionierung zu Apple/Google; Erläuterung Möglichkeiten und Grenzen des dezentralen Modells, Planung Launch-Kampagne)
  - Begleitung des Open Source Managements und der Interaktion mit der Open-Source-Community
  - Unterstützung bei der Planung und Koordination von Feldtests zum Test der App unter möglichst realen Bedingungen und einer großen Zahl an Testgeräten und Testpersonen

## 4.2 Service Delivery Management

Das Service Delivery Management der Telekom verantwortet die Leistungsbeziehungen zum BMG. Dabei gehört zu den zentralen Zielen insbesondere

- die beiderseitige Vertragsbeziehung erfolgreich zu gestalten
- projektimmanente und projektübergreifende Themen zu begleiten und als Ansprechpartner zu agieren
- Teilnahme an Steering Boards, Regelkommunikation u.Ä.

## 4.3 Open Source Software Management

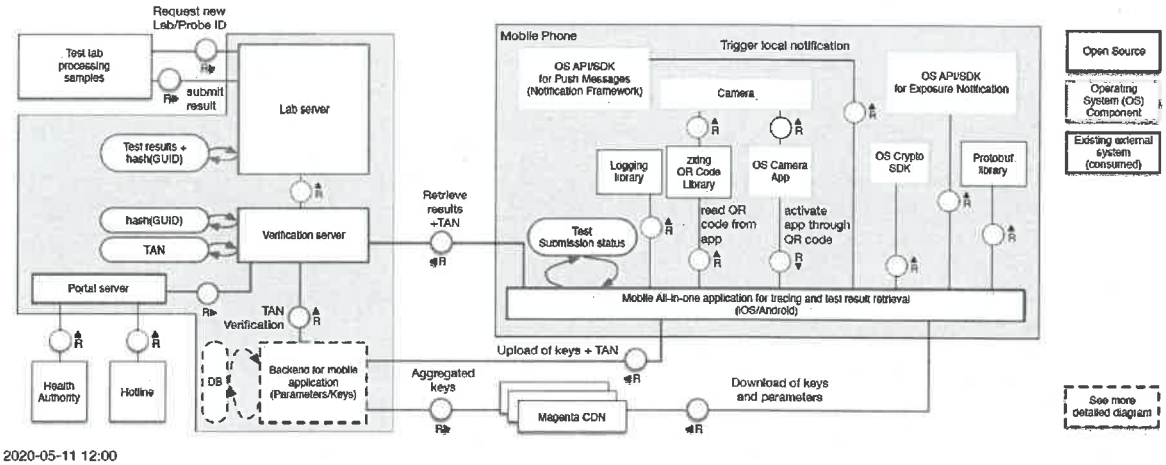
Die Telekom stellt die im Rahmen dieses Angebots erstellte Software sowie begleitende Architektur- und Fachdokumente unter Einhaltung der Apache 2.0 Open-Source-Lizenzregularien sowie der Gepflogenheiten der Open-Source-Community über die gemeinsam mit SAP administrierte GitHub Organisation „corona-warn-app“ öffentlich zur Verfügung.

Ziel ist die Sicherstellung einer größtmöglichen Transparenz gegenüber der interessierten Öffentlichkeit, sowie die Beteiligung der Open-Source-Community in Form von Reviews und Pull Requests (z.B. Korrektur- oder Verbesserungsvorschläge).

Die Telekom unterstützt die Sicherstellung der Open Source Compliance und Prozesse für ihre eigene Leistungsbestandteile wie folgt:

- Konzeption und Umsetzung des Veröffentlichungsprozesses unter der Apache 2.0 Lizenz
- Analyse der genutzten Komponenten und ihrer Lizenzen (Bill of Materials)
- Sicherstellung der Compliance mit den Lizenzen von verwendeten Open Source Bibliotheken
- Unterstützung der Entwicklungsteams zur Einhaltung der Open-Source Regeln und Lizenzen
- Administration der GitHub Organisation und Repositories
- Erstellung und Veröffentlichung von Compliance-Artefakten wie Lizenztexten, Copyrightinformationen und weiteren Lizenzelementen
- Erstellung von Templates für Copyright Headers für Sourcecode-Files
- Erstellung von Contribution-Guidelines für das Open-Source-Projekt und die betreffenden Repositories
- Management der sich beteiligenden Open-Source-Community (Community-Management)
- Erstellung von begleitenden Kommunikationsdokumenten und -formaten (z.B. öffentliche Website mit Basisinformationen zum Open-Source-Projekt, Project Landing Page, FAQs)
- Unterstützung der Community-Manager in allen Fragen der Open-Source-bezogenen Kommunikation
- Abstimmung mit allen relevanten Workstreams des Programms

In Abbildung 8: Open-Source-Anteile sind die derzeit geplanten Open-Source-Anteile (blau) am Gesamtsystem dargestellt:




Stand: 2020-05-11 12:00

Abbildung 8: Open-Source-Anteile

## 4.4 Proximity Measurement

Leistungen bis GOLIVE:

Unterstützung durch Beratung zur Entwicklung der App:

- Spezifikation der ExposureNotification-API
- technische Diskussionen mit dem Entwicklungsteam
- Diskussionen mit Apple/Google Entwicklern zur Spec der Schnittstelle
- Erarbeiten von Spezifikations-Dokumenten

Test und Bewertung der Google/Apple API anhand von Realtests

- Definition von bis zu 5 relevanten Testszenarien z.B. ÖPNV, Restaurant, Wartesituation, Versammlung/Meeting, öffentliche Bereiche
- Definition von Haltepositionen
- Testplanung mit Ablaufplan für Gruppen bis 10 Personen
- Konfiguration Endgeräte, Referenzsystem, Testsoftware etc.
- Mehrere ganztägige Tests mit 10 Testpersonen in der LINK Testhalle in Nürnberg
- Nachbereitung, Aufbereitung der Messwerte
- Auswertung, Ableitung der Performanz, Abgleich zwischen berechneten Risk-Scores und Referenzwerten

Leistungen nach GOLIVE:

Validierungstests der fertigen App

- Validierung der fertigen App gemäß festgelegter Test-Szenarien

Betreuung des Roll-Outs und Support für Planung weiterer Generationen

- technische Unterstützung beim Roll-Out
- Beratung bei etwaigen technischen Problemen
- Support von technischen Diskussionen mit Apple / Google für etwaige Verbesserungen der Schnittstelle
- Unterstützung an der Schnittstelle zur Risk-Score Berechnung

# 5 DATENSCHUTZ

Die Telekom ist nicht „Verantwortlicher" gemäß Artikel 4 Ziffer 7 Datenschutz-Grundverordnung (DSGVO).

Unterstützungsleistungen der Telekom zum Datenschutz werden im Leistungsverzeichnis unter dem Abschnitt Projektmanagement aufgeführt.

## 5.1 Datenschutzrechtliche Unterstützungsleistung

- Die Telekom unterstützt das BMG im Umgang mit datenschutzrechtlichen Fragestellungen. Insbesondere bei der Kommunikation und Abstimmung mit dem Datenschutzbeauftragten des BMG / RKI sowie mit dem BfDI und bei
- der Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen bzw. der Analyse hinsichtlich der Wirksamkeit getroffener Maßnahmen

## 5.2 Datenschutzkonzeption

Die Telekom unterstützt den Auftraggeber bei der datenschutzkonformen Ausgestaltung der Corona Warn App. Die Auftragnehmerin wird auf Basis der Informationen, die sie seitens der App-Entwickler sowie weiterer Beteiligter erhält, diese Datenschutzkonzepte für ihren Leistungsanteil erstellen. Sie wird zudem bei der Erstellung von Berechtigungskonzepten unterstützen.

Das Datenschutzkonzept umfasst folgende Inhalte:

- Die Verantwortlichkeiten
- Die zu verarbeitenden personenbezogenen Daten (Datenarten, Datenfeldkatalog, Datenkategorien)
- Personenbezogene Auswertungen (sofern einschlägig)
- Schnittstellenbeschreibungen (Import / Export)
- Den Verwendungszweck
- Die Rechtsgrundlagen
- Ein Löschkonzept
- Die Beschreibung der Anonymisierung / Pseudonymisierung personenbezogener Daten

## 5.3 Datenschutzfolgenabschätzung (DSFA)

Die Telekom arbeitet den „Verantwortlichen" bei der Vorbereitung und Durchführung der Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten gemäß Artikel 35 DSGVO (Datenschutzfolgenabschätzung) zu. Grundlage sind die der Telekom vom Verantwortlichen bereitgestellten Informationen.

Die Unterstützungsleistungen im Rahmen der Datenschutzfolgenabschätzung (DSFA) umfassen insbesondere:

- Die Vorbereitung inklusive
  - Festlegung von Rollen innerhalb des DSFA-Teams (Moderation, Protokollführung, Prüfung)
  - Definition und Dokumentation von Aufgabe und Umfang der DSFA
  - Festlegung Kontext des DSFA-Prozesses (Risikobewertung, -behandlung und -akzeptanz )
  - Festlegung der Empfänger des DSFA-Berichts
- Durchführung der DSFA inklusive
  - Beschreibung und Bewertung der Verarbeitungsvorgänge/ Prozessschritte
  - Risikobewertung gemäß Artikel 35 DSGVO
  - Beschreibung der Bedrohungsszenarien
  - Risikobewertung (Risikoidentifikation und -analyse) (brutto)
  - Risikobehandlung (Festlegung geeigneter technischer und organisatorischer Maßnahmen) ggf. erneute Risikobewertung (netto)

## 5.4 Leistungsabgrenzung

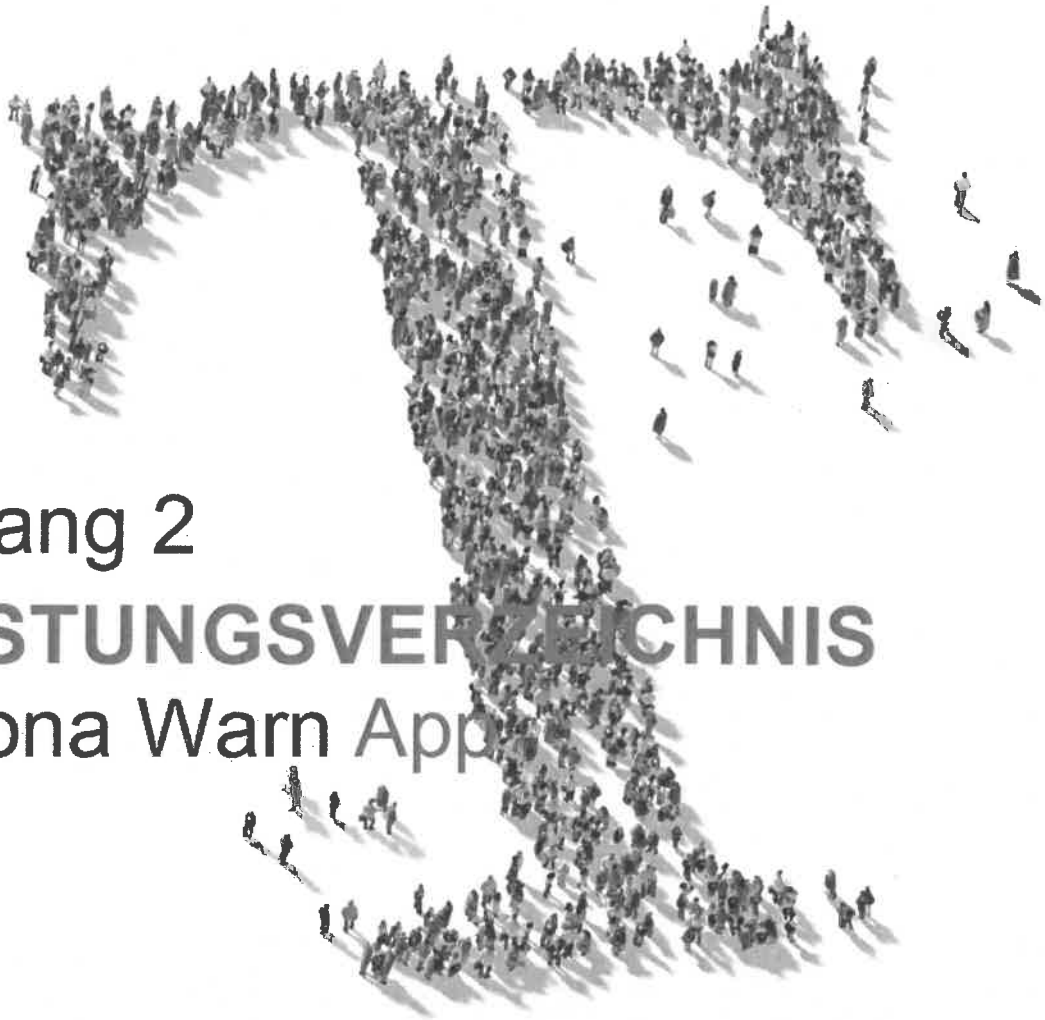
SAP liefert die Datenschutz-Teilkonzepte für "Mobile all-in-one Application for Tracing and Test result retrieval" und das "Backend for mobile application"; Telekom liefert das übergeordnete Datenschutz-Rahmenkonzept und die Datenschutz -Teilkonzepte für "Verification, Portal Server, Labor Server" und "Hotline".

# 6 LEISTUNGEN IM ZUSAMMENHANG MIT EINER EUROPÄISCHEN INTEROPERABILITÄT

Die folgende Übersicht gibt die Eckpunkte der Leistungen wieder. Diese werden im Zusammenhang mit der Konzeption sowohl vor als auch nach GOLIVE erbracht.

- Teilnahme als Experte am European eHealth-Netzwerk bis zur finalen Erstellung der „Interoperability specifications for cross-border transmission chains between approved apps" (inkl. Kommentierung).
- Beratungsleistungen zur Bereitstellung von technischen Schnittstellen zum jeweiligen nationalen dezentralen Tracing-System, so dass die grenzüberschreitende Kopplung der Tracing-Systeme funktioniert. Hinweis: Technische Interoperabilität zwischen Systemen mit unterschiedlicher Grundarchitektur (dezentral vs. zentral) kann nicht garantiert werden.
- Initiale Erläuterung der in DE verfolgten Architektur und (sobald vorliegend) der technischen Schnittstelle im jeweiligen europäischen Zielland gegenüber vom Auftraggeber zu benennenden Ansprechpartnern (Zielländer wurde vom Auftraggeber vorab definiert: Frankreich, Österreich, Schweiz)

Die Implementierung im jeweiligen europäischen Zielland wird nicht begleitet.



# Anhang 2
# LEISTUNGSVERZEICHNIS
# Corona Warn App

**Empfänger**
Bundesministerium für Gesundheit

von T-Systems International GmbH

**Angebotsnummer:** 1000820722
**Angebotsdatum:** 05.06.2020

T · · Systems ·

# Informationen zum Angebot

| | |
|---|---|
| An | Bundesministerium für Gesundheit<br>Friedrichstraße 108, 10117 Berlin |
| Über | Leistungsinformation Corona Warn App |
| Von | T-Systems International GmbH<br>BA Public & Healthcare<br>Hahnstr.43<br>60528 Frankfurt am Main |

| **Ansprechpartner** | |
|---|---|
| Kontakt | [redacted] |
| Telefon | [redacted] |
| Fax | [redacted] |
| E-Mail | [redacted] |

| | |
|---|---|
| **Angebotsnummer** | 1000820722 |
| **Angebotsdatum** | 05.06.2020 |

# Inhaltsverzeichnis

# 1 KOMMERZIELLES ANGEBOT

Telekom und SAP haben ihre jeweils in separaten Verträgen angebotenen Leistungen abgegrenzt. Die in diesem Dokument beschriebenen kommerziellen Regelungen basieren auf den Grundannahmen (Ziffer 1.4 der Leistungsbeschreibung).

[redacted]

## 1.1 Leistungsumfang und Change Request

Basis für das Leistungsverzeichnis ist Anhang 1 (Leistungsbeschreibung Corona-Warn-App) zum Vertrag über IT- Leistungen im Projekt Corona-Warn-App. Mit dem kommerziellen Angebot sind folgende in der Leistungsinformation aufgeführten Leistungen abgegolten:

a) Bis zum GOLIVE Termin gilt das in Kapitel 2 beschriebene Preismodell.

b) Nach GOLIVE Termin gilt das in Kapitel 3 beschriebene Preismodell.

geht davon aus, dass das Entwicklungsteam insbesondere für die weiteren Releases zwei Wochen über GOLIVE hinaus zur Verfügung steht. Je Release muss eine im Vorfeld abgestimmte Mobilisierung des Entwicklungsteams erfolgen. Eine weitere Beauftragung muss mit einem abzustimmenden Vorlauf erfolgen. Die Beauftragung erfolgt über das CR-Verfahren. Sofern seitens Auftraggebers eine Budgetabgrenzung zwischen BMG und RKI notwendig wird, ist dies in diesem Zusammenhang mitzuteilen.

## 1.2 Leistungszeitraum

Der Leistungszeitraum umfasst zwei Phasen:

a) Die Phase **bis zum GOLIVE** Termin (App-Launch plus eine Woche, derzeit 22.06.2020)

b) Die Phase **nach dem GOLIVE** Termin.

# 2 PREISMODELL BIS ZUM GOLIVE

Für den in Kapitel 1.2 definierten Leistungszeitraum wird der Kunde bei der Entwicklung und Markteinführung in dem in Kapitel 1.1 beschriebenen Leistungsumfang unterstützt. Die Kalkulationen beruhen dabei auf einer Aufwandsschätzung sowie den aktuellen Marktpreisen der Telekom bzw. den Angeboten Dritter [redacted]

Die folgenden Leistungselemente werden in Anhang 1 (Leistungsinformation Corona-Warn-App) beschrieben und dimensioniert. Die Abrechnung erfolgt [redacted] grundsätzlich nach Aufwand auf Basis der Rate Card (Kapitel 4). Leistungen, die als fester Bestandteil abgerechnet werden (fixer Anteil), sind in der untenstehenden Tabelle als einmalig gekennzeichnet. Darüber hinaus gehende Leistungen und Mengen werden über das Change-Request-Verfahren gemäß Abstimmungsvereinbarung über IT- Leistungen im Projekt Corona-Warn-App beauftragt. Alle genannten Mengen und einmalige Preise sind Schätzungen und können sich noch verändern.

Für den Fall, dass sich der GOLIVE Termin verschiebt bzw. nach GOLIVE Termin weitere Aufwände entstehen, um den in Anhang 1 (Leistungsinformation Corona-Warn-App) zum Vertrag über IT- Leistungen im Projekt Corona-Warn-App genannten Leistungsumfang auszufüllen oder der Leistungsumfang sich ändert, werden diese Tätigkeiten für den fixen Anteil über CR und für den variablen Anteil weiterhin über Rate Card gemäß Abschnitt 4 abgerechnet.

| 2.1 Verification | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| Development Verifikation Komponenten | RateCard | Senior Consultant Manager | [redacted] | [redacted] | 52 500,00 |
| Development Verifikation Komponenten | RateCard | Consultant Manager | | | 297 000,00 |
| Development Verifikation Komponenten | RateCard | IT Development Manager | | | 240 500,00 |
| Development Verifikation Komponenten | RateCard | IT Development Graduate | | | 28 600,00 |
| Integration Labore und Krankenhäuser | RateCard | Labore / Krankenhäuser | | | 1.264 200,00 |

| 2 2 Testing | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| Testing Service | RateCard | Project Management Senior | [redacted] | [redacted] | 56 000,00 |
| Testing Service | RateCard | IT Development Senior | | | 323.700,00 |
| Testing Service | RateCard | IT Development Senior | | | 27 000,00 |
| Test Equipment | einmalig | Stück | | | 7.142,86 |
| Mobile Device Cloud | einmalig | Stück | | | 14 285,71 |

| 2 3 Systems Operations and Hosting | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| System Operations and Hosting Komponenten | RateCard | Project Management Executive | [redacted] | [redacted] | 144 872,00 |
| System Operations and Hosting Komponenten | RateCard | Consultant Senior | | | 366 660,00 |
| System Operations and Hosting Komponenten | RateCard | IT Services Operations Manager | | | 38.400,00 |
| System Operations and Hosting Komponenten | RateCard | IT Development Assistant | | | 30.456,00 |
| System Operations and Hosting Komponenten | RateCard | IT Development Senior | | | 185 544,00 |
| one time set up | einmalig | Stück | | | 3 385,63 |
| OTC RDS (2 Monate) | monatlich | Stück | | | 6.799,47 |
| 2 months MCS PaaS Cluster (4 Umgebungen) | monatlich | Stück | | | 77.193,91 |

| 2.4 IT-Sicherheit | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| IT-Sicherheit Komponenten | RateCard | Consultant Senior | [redacted] | [redacted] | 50.400,00 |
| IT-Sicherheit Komponenten | RateCard | Consultant Manager | | | 216 000,00 |
| IT-Sicherheit Komponenten | RateCard | Consultant Manager | | | 120 000,00 |
| Penetration Testing | RateCard | Consultant Manager | | | 24 000,00 |

| 2 5 Netzwerk | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| Netzwerk Konfiguration und Integration | RateCard | IT Development Manager | [redacted] | [redacted] | 14 560,00 |

| 2 6 Hotline | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| Freecall 0800 /IVR | einmalig | Stück | [redacted] | [redacted] | 5 946,32 |
| Verification Hotline | einmalig | Stück | | | 15.789,47 |
| Technische Hotline | einmalig | Stück | | | 36 842,11 |
| Consulting Hotline | RateCard | Consultant Senior | | | 45 978,95 |

| 2.7 Projektmanagement | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| Project lead | RateCard | Consultant Executive | [redacted] | [redacted] | 323.730,00 |
| Project lead | RateCard | Project Management Manager | | | 70 875,00 |
| Project lead | RateCard | Project Management Senior | | | 200 800,00 |
| Project lead | einmalig | Stück | | | 955 863,16 |
| Scoping | RateCard | Project Management Senior | | | 30 000,00 |
| Scoping | RateCard | Project Management Executive | | | 78 000,00 |
| Scoping | RateCard | Consultant Senior | | | 189 000,00 |
| Proximity measure | RateCard | Project Management Senior | | | 136 000,00 |
| Communication | einmalig | Stück | | | 71.428,57 |
| Public Affaires | RateCard | Project Management Senior | | | 44 800,00 |
| Public Affaires | RateCard | Project Management Executive | | | 32 240,00 |
| Architecture | RateCard | IT Development Senior | | | 60.480,00 |
| Development | RateCard | IT Development Graduate | | | 13 200,00 |
| Development | RateCard | IT Development Manager | | | 159 900,00 |
| Development | RateCard | Consultant Manager | | | 81 000,00 |
| Data Privacy | RateCard | Project Management Senior | | | 192 000,00 |
| Data Privacy | RateCard | Project Management Manager | | | 270 000,00 |
| Data Privacy | RateCard | Consultant Senior | | | 3.150,00 |
| Proximity / Testing | RateCard | Consultant Senior | | | 42 000,00 |
| Open Source | RateCard | Consultant Senior | | | 100 800,00 |

| 2 8 Interoperabilität | Abrechnungs-methode | Einheit | Menge 2020 | Einzelpreis 2020 [EUR] | Total 2020 [EUR] |
|---|---|---|---|---|---|
| PAN EU - Unterstützung | RateCard | Project Management Executive | [redacted] | [redacted] | 187 200,00 |
| PAN EU - Unterstützung | RateCard | IT Development Senior | | | 57 600,00 |

# 3 PREISMODELL NACH GOLIVE

Für den in Kapitel 1.2 definierten Leistungszeitraum erbringt der Auftragnehmer die Leistung gemäß Anhang 1 (Leistungsbeschreibung Corona-Warn-App). Die Abrechnung erfolgt grundsätzlich nach Aufwand auf Basis der Rate Card (Kapitel 4). Zudem gibt es Leistungen, die auf monatlicher Basis und nach Stück abgerechnet werden. Diese sind in der untenstehenden Tabelle entsprechend gekennzeichnet. Darüber hinaus gehende Leistungen werden über das Change-Request-Verfahren gemäß Abstimmungsvereinbarung über IT- Leistungen im Projekt Corona-Warn-App beauftragt. Alle genannten Mengen und einmalige Preise sind Schätzungen und können sich noch verändern.

[redacted]

Für Änderungen, die sich aus der Umsetzung des Konzeptes aus IT-Grundschutz ergeben, schätzt die Telekom auf Basis bisheriger Erfahrungswerte für das Jahr 2021 einen Betrag in Höhe [redacted]

Für die Leistungen aus dem Leistungsbereich 3.5 werden monatlich mindestens 1,5 TB vom Kunden abgenommen, darüberhinausgehende Mengen werden in 100 GB Schritten abgerechnet und vergütet. [redacted]

Für die Leistungen aus dem Leistungsbereich 3.6 werden monatlich bis einschließlich Ende 2020 für die technische Hotline 3000 Calls pro Tag und die Verifikationshotline 1000 Calls pro Tag vom Kunden vergütet. Nach den ersten drei Monaten findet das in der Leistungsbeschreibung beschriebene Verfahren Anwendung. [redacted]

Die Leistungen aus dem Leistungsbereich 3.7 setzen sich aus dem Servicemanagement und Projektmanagement zusammen. [redacted] Leistungen des Servicemanagement werden mit 10% der jeweiligen monatlichen Vergütung der Leistungsbereiche 3.1 bis 3.6 vergütet.

Leistungen aus dem Leistungsbereich 3.8 werden auf RateCard-Basis vergütet. [redacted]

| Nach GOLIVE | | | | | | | Anzahl Monate | 6 | 12 | 12 | 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 3.1 Verification | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
| Verifikationskomponenten Betrieb | RateCard laufend | Consultant Manager | | | | | | 64.800,00 | 128.400,00 | 128.400,00 | 64.800,00 |
| Verifikationskomponenten Betrieb | RateCard laufend | IT Development Manager | | | | | | 69.680,00 | 139.360,00 | 139.360,00 | 69.680,00 |
| Betrieb der Gatewaykomponenten + Zentralkomponente GUID Erste lung | monatlich | für alle Labore | | | | | | 6.000,00 | 12.000,00 | 12.000,00 | 6.000,00 |
| Betrieb der Labor-Integration | monatlich | pro Labor/Stück | | | | | | 77.220,00 | 154.440,00 | 154.440,00 | 77.220,00 |
| 3rd Level Support | RateCard laufend | Consultant Manager | | | | | | 86.400,00 | 166.800,00 | 163.200,00 | 80.400,00 |
| 3rd Level Support | RateCard laufend | IT Development Manager | | | | | | 107.120,00 | 208.000,00 | 204.880,00 | 102.960,00 |

| 3.2 Testing | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Testing Service | RateCard laufend | IT Development Manager | | | | | | 72.800,00 | 145.600,00 | 145.600,00 | 72.800,00 |

| 3.3 System Operations und Hosting | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Managed PaaS | monatlich | Stück | | | | | | 247.816,08 | 495.632,16 | 495.632,16 | 247.816,08 |
| OTC -RDS | monatlich | Stück | | | | | | 21.828,42 | 43.656,84 | 43.656,84 | 21.828,42 |
| Erweiterung CI/CD | RateCard laufend | Project Management Executive | | | | | | 197.600,00 | 380.640,00 | 374.400,00 | 187.200,00 |
| Application Operation Verifikation Komponenten Basis | monatlich | Stück | | | | | | 726.436,68 | 1.452.873,36 | 1.452.873,36 | 726.436,68 |
| Application Operation Verifikation Development Koordination | RateCard einmalig | IT Development Senior | | | | | | 10.080,00 | - | - | - |
| Application Operation Verifikation Development Setup DevOps | RateCard einmalig | Project Management Executive | | | | | | 29.120,00 | - | - | - |
| Application Operation SAP Koordination | RateCard einmalig | IT Development Senior | | | | | | 10.080,00 | - | - | - |
| Application Operation SAP DevOps | RateCard einmalig | Project Management Executive | | | | | | 29.120,00 | - | - | - |
| Application Service pro Anwendung (Komplexität Hoch, Kritikalität 1) | monatlich | Stück | | | | | | 349.169,70 | 698.339,40 | 698.339,40 | 349.169,70 |

| 3.4 IT-Sicherheit | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Teilprojektleitung IT-Sicherheit | RateCard einmalig | Consultant Senior | | | | | | 45.360,00 | - | - | - |
| IT-Sicherheits-Review | RateCard einmalig | Consultant Senior | | | | | | 5.040,00 | - | - | - |
| IT-Sicherheitsberatung | RateCard einmalig | Consultant Manager | | | | | | 116.400,00 | - | - | - |
| IT-Sicherheitskonzepte | RateCard einmalig | Consultant Manager | | | | | | 116.400,00 | - | - | - |
| Managed Cyber Defense | monatlich | Stück | | | | | | 426.846,18 | 853.692,36 | 853.692,36 | 426.846,18 |
| Penetration Testing | RateCard laufend | Consultant Manager | | | | | | 24.000,00 | 24.000,00 | 24.000,00 | 24.000,00 |
| Managed Cyber Defense Setup | einmalig | Stück | | | | | | 195.425,00 | - | - | - |
| Red Teaming | RateCard laufend | Consultant Senior | | | | | | 33.600,00 | 33.600,00 | 33.600,00 | - |
| IT-Sicherheitskonzept nach BSI Standards 200-x | RateCard einmalig | Consultant Manager | | | | | | 370.800,00 | - | - | - |
| IT-Sicherheitsbeauftragter IT-Grundschutz | RateCard laufend | Consultant Senior | | | | | | 100.800,00 | 201.600,00 | 201.600,00 | 100.800,00 |
| DDoS Protection - erste 6 Monate | monatlich | Stück | | | | | | 53.750,04 | - | - | - |
| DDoS Protection ADDP - nach 6 Monaten | monatlich | Stück | | | | | | - | 81.831,36 | 81.831,36 | 40.915,68 |

| 3.5 Netzwerk | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| CDN Basis (enthält bis zu 1,5TB Datenvolumen) | monatlich | Stück | | | | | | 199.292,04 | 398.584,08 | 398.584,08 | 199.292,04 |
| CDN Kapazität | monatlich | pro 100GB | | | | | | - | - | - | - |

| 3.6 Hotline | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0800 für techn. Hotline - Bereitstellungsgebühr | monatlich | Stück | | | | | | 239,40 | 478,80 | 478,80 | 239,40 |
| 0800 für techn. Hotline | monatlich | Minuten Festnetz | | | | | | 5.400,00 | 10.800,00 | 10.800,00 | 5.400,00 |
| 0800 für techn. Hotline | monatlich | Minuten Mobilfunk | | | | | | 364.500,00 | 729.000,00 | 729.000,00 | 364.500,00 |
| 0800 für Verifikation Hotline - Bereitstellungsgebühr | monatlich | Stück | | | | | | 239,40 | 478,80 | 478,80 | 239,40 |
| 0800 für Verifikation Hotline | monatlich | Minuten Festnetz | | | | | | 1.800,00 | 3.600,00 | 3.600,00 | 1.800,00 |
| 0800 für Verifikation Hotline | monatlich | Minuten Mobilfunk | | | | | | 121.500,00 | 243.000,00 | 243.000,00 | 121.500,00 |
| IVR - Bereitstellungsgebühr | monatlich | Stück | | | | | | 3.539,28 | 7.078,56 | 7.078,56 | 3.539,28 |
| IVR | monatlich | Minuten | | | | | | 90.000,00 | 180.000,00 | 180.000,00 | 90.000,00 |
| IVR - CR für Ansagen etc. | ebruf | Pro angefangene halbe Stunde | | | | | | - | - | - | - |
| Technische Hotline - 6 Monate - 3000 calls | monatlich | Stück | | | | | | 7.425.734,40 | - | - | - |
| Technische Hotline - ab Monat 6 - bis zu 100 calls | monatlich | Stück | | | | | | - | 990.097,92 | 990.097,92 | 495.048,96 |
| | | | | | | | Anzahl Monate | 6 | 5 | 0 | 0 |
| Verifikations Hotline - 1000 calls | monatlich | Stück | | | | | | 665.445,90 | 554.538,25 | - | - |
| | | | | | | | Anzahl Monate | 0 | 7 | 12 | 6 |
| Verifikations Hotline ab 06/2021 - bis 150 calls - geänderte Servicezeiten | monatlich | Stück | | | | | | - | 512.572,06 | 878.694,96 | 439.347,48 |

| 3.7 Projektmanagement | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Projektmanagement Lead | RateCard laufend | IT Development Senior | | | | | | 44.640,00 | 90.720,00 | 90.720,00 | 44.640,00 |
| Projektmanagement MMS Beratung | einmalig | Stück | | | | | | 56.653,04 | - | - | - |
| Projektmanagement Data Privacy | RateCard laufend | Project Management Senior | | | | | | 40.000,00 | 80.000,00 | 80.000,00 | 40.000,00 |
| Proximity Measurement | RateCard laufend | Project Management Senior | | | | | | 120.000,00 | | | |
| Service Delivery Management / Service Management | monatlich | 10% Betriebskosten | | | | | | 356.712,55 | 666.521,03 | 667.749,79 | 333.192,65 |

| 3.8 Interoperabilität | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PAN EU - Unterstützung | RateCard einmalig | IT Development Senior | | | | | | 259.200,00 | - | - | - |

| 3.7 Anteil Open Source | Abrechnungs-methode | Einheit | Menge 2020 | Menge 2021 | Menge 2022 | Menge 2023 | Einzelpreis [EUR] | Total 2020 [EUR] | Total 2021 [EUR] | Total 2022 [EUR] | Total 2023 [EUR] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Open Source Management | RateCard einmalig | Consultant Manager | | | | | | 60.000,00 | - | - | - |
| Open Source Management | RateCard einmalig | Consultant Senior | | | | | | 16.800,00 | - | - | - |

Rate Card

## 3.1 Kategorien und Tagessatz

Die angegebenen Tagessätze beruhen auf Marktpreisen der Telekom bzw. den Angeboten Dritter. Es gilt entsprechend §7.3 a) des Vertrages über IT-Leistungen im Projekt Corona-Warn-App. Bei Bedarf werden die Kategorien erweitert.

| Kategorie | Tagessatz |
|---|---|
| IT Development Assistant | [redacted] |
| IT Development Graduate | [redacted] |
| IT Development Manager | [redacted] |
| IT Development Senior | [redacted] |
| Consultant Assistant | [redacted] |
| Consultant Graduate | [redacted] |
| Consultant Manager | [redacted] |
| Consultant Senior | [redacted] |
| Consultant Executive | [redacted] |
| Project Management Assistant | [redacted] |
| Project Management Graduate | [redacted] |
| Project Management Manager | [redacted] |
| Project Management Senior | [redacted] |
| Project Management Executive | [redacted] |
| IT Services Operations Skill Level 4 | [redacted] |
| Reisezeiten pro Stunde | [redacted] |

## 3.2 Skill-Ausprägung

| Consultant | 2 - Graduate | 3 - Manager | 4 - Senior | 5 - Executive |
|---|---|---|---|---|
| **Berufs-erfahrung** | 1-2 Jahre | 2-5 Jahre | 6-8 Jahre | >8 Jahre |
| **Beschrei-bung** | Unterstützung bei der Erstellung von Anforderungs- und Lösungskonzepten<br>Anwendung agiler Projektmethoden<br>Unterstützung bei Angebotslegung<br>Effektive und effiziente Beratung als fest integriertes Projekt-Teammitglied | Analysen des Ist-Zustandes und Konzeption des Soll-Zustandes<br>Begleitung/Unterstützung des Managements<br>Beratungstätigkeiten in Entwicklung und Implementierung neuer Systemlösungen sowie neuer Themengebiete, Kundenspezifische Lösungsfindung und Optimierung | Rolle als Teil- oder Projektleiter übernehmen<br>Lösungen für komplexe/innovative Fragestellungen finden<br>Eigenverantwortliche PM-Aufgabe: Planung, fachliches Controlling und Berichtswesen, Risiko- und Qualitätsmanagement<br>Beratungsleistung und Konzepterstellung hinsichtlich geeigneter Methoden und Vorgehensweisen | Selbstständige Beratungsleistung bei der Entwicklung und Umsetzung der Geschäftsstrategie<br><br>Entwicklung von Problemlösungsstrategien und Methoden zur Zielerreichung<br>Konfliktmanagement und Marktanalysen beherrschen und durchführen<br><br>Vertragsverhandlungen und Abschlüsse begleiten |

| IT Development | 1 - Assistant | 2 - Graduate | 3 - Manager | 4 - Senior |
|---|---|---|---|---|
| **Berufs-erfahrung** | <1 Jahr | 1-2 Jahre | 2-5 Jahre | 6-8 Jahre |
| **Beschrei-bung** | Mitarbeit in großen Software-Entwicklungsteams, Unterstützen bei Dokumentation, Programmierung und Testingphasen anhand gegebener Spezifikationen | Eigenverantwortliche Planung, Analyse und Entwicklung von Software-Komponenten mit einem Umfang von maximal drei Monaten und anhand gegebener Spezifikationen | Analyse, Bewertung der Erfordernisse, um Software und Applikationen zu entwickeln und umzusetzen<br>Sicherstellung von Testingphasen und Funktionstests<br>Technische Dokumentation erstellen | Gesamtverantwortliche Entwicklung von komplexeren Softwarekomponenten mit Spezifikationserstellung<br>Arbeiten in unterschiedlichen Phasen des SW-Projektes<br>Kommunikations- und Projektmanagement-Fähigkeiten sicher beherrschen einsetzen |

| Projektmanagement | 1 - Assistant | 2 - Graduate | 3 - Manager | 4 – Senior | 5 - Executive |
|---|---|---|---|---|---|
| **Berufs-erfahrung** | <1 Jahr | 1-2 Jahre | 2-5 Jahre | 6-8 Jahre | >8 Jahre |
| **Beschreibung** | Projektoffice, Support für den PM, Administrative Assistenztätigkeiten<br><br>Konkrete Aufgabenstellung aller Beteiligten im Blick behalten Koordination von Projekten und Ressourcen | Management kleiner Projekte oder Teilprojekte Entlastung des Projektleiters Schnittstelle zwischen Projektleiter und Team Effektivität- und Effizienzsteigerung überwachen | Management mittlerer Projekte Zuständig für Planung, Umsetzung, Abnahme und Nachbereitung von Projekten Führen und Organisieren des Projektteams | Management großer Projekte Das „große Ganze" im Auge behalten Budgetführung | Management großer und komplexer Projekte Gesamtprojektleitung Verantwortung der Team-zusammen-setzung Weisungs-befugnis im Konfliktfall Formelle Autorität Budgetverantwortung |

# Vertrag über die Verarbeitung personenbezogener Daten

- nachfolgend „AV-Vertrag" genannt -

zwischen

**der Bundesrepublik Deutschland,**
**vertreten durch das Bundesministerium für Gesundheit,**
**vertreten durch das Robert Koch-Institut**
**Nordufer 20**
**13353 Berlin**

- nachfolgend „Verantwortlicher" genannt –

und

**T-Systems International GmbH**
**Hahnstraße 43**
**60528 Frankfurt am Main**

- nachfolgend „Auftragsverarbeiter" genannt -

- gemeinsam nachfolgend einzeln oder gemeinsam auch „Parteien" genannt -

## § 1 Begriffsbestimmungen

Im Sinne dieses AV-Vertrags bezeichnet der Ausdruck

(a) „**Auftragsverarbeiter**" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
„Auftragsverarbeiter" ist die im Vorstehenden als „Auftragsverarbeiter" bezeichnete Vertragspartei.

(b) **„Dritter"** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

(c) „**Hauptvertrag**" den in § 2 näher gekennzeichneten Dienstleistungs- oder Kooperationsvertrag.

(d) **„Landes- und Unternehmensspezifische Bedingungen" („LUB")** in **Annex 1** die spezifischen Bedingungen des Verantwortlichen, die sich aus den verbindlichen Rechtsvorschriften des jeweiligen Mitgliedstaats ergeben oder auf örtliche Datenschutzvorgaben zurückzuführen sind. Sie enthalten Abweichungen vom oder Ergänzungen zum Hauptteil dieses AV-Vertrags;

(e) „**Verantwortlicher**" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
„Verantwortlicher" ist die im Vorstehenden als „Verantwortlichen" bezeichnete Vertragspartei, die hier in diesem AV-Vertrag allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(f) **„Verarbeitung"** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

(g) „**personenbezogene Daten**" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(h) „**weiterer Auftragsverarbeiter oder Unterauftragsverarbeiter**" den Vertragspartner des Auftragsverarbeiters, der von diesem mit der Durchführung bestimmter Verarbeitungsaktivitäten für den Verantwortlichen beauftragt wird;

(i) „**Sub-Unterauftragsverarbeiter**" den Vereinbarungspartner des weiteren Auftragsverarbeiters oder Unterauftragsverarbeiters, der von Letzterem mit der Durchführung bestimmter Verarbeitungsaktivitäten im Regelungsbereich dieses AV-Vertrags beauftragt wird.

## § 2 Gegenstand des Vertrags, Rechtsgrundlage

(1) **[Rechtsgrundlage]** Die Rechtsgrundlagen dieser Vereinbarung sind in Annex 1 aufgeführt. Ihr liegen die Bestimmungen der EU-Datenschutzgrundverordnung (EU DSGVO) ab deren Geltungsdatum sowie die im **Annex 1** näher bezeichneten jeweiligen „Landes- und Unternehmensspezifischen Bedingungen" (nachstehend „LUB" genannt) zugrunde. Bei Widersprüchen zwischen dem Hauptteil dieses AV-Vertrags und den LUB sind letztere maßgebend.

(2) **[Gegenstand des Vertrags]** Gegenstand des Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen in dessen Auftrag und nach dessen Weisung im Zusammenhang mit IT-Leistungen für den Betrieb der Corona Warn App der Bundesrepublik Deutschland in Ergänzung des Vertrags über IT- Leistungen im Projekt Corona Warn App der Parteien (nachstehend „Hauptvertrag" genannt").

(3) **[Konkretisierung der Verarbeitung]** Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen in Verbindung mit **Annex 2**. Der Verantwortliche gewährt dem Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen wie in **Annex 2** beschrieben.

(4) **[Wartung, Prüfung]** Erbringt der Auftragsverarbeiter für den Verantwortlichen Leistungen im Bereich Wartung / Fernwartung / IT-Fehleranalyse, bei denen ein Zugriff auf personenbezogene Daten des Verantwortlichen zwar nicht bezweckt ist, aber nicht ausgeschlossen werden kann, gilt diese Vereinbarung entsprechend. Etwaige diesbezügliche Detaillierungen der Verarbeitung legen die Vertragsparteien in **Annex 2** fest.

## § 3 Rechte und Pflichten des Verantwortlichen

(1) **[Zulässigkeit der Datenverarbeitung]** Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche verantwortlich. Der Verantwortliche wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

(2) **[Weisungen]** Der Auftragsverarbeiter wird personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Alle Weisungen werden schriftlich oder per E-Mail erteilt. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die geltenden rechtlichen Bestimmungen verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung einer solchen Weisung solange auszusetzen, bis diese durch den Aufraggeber bestätigt oder geändert wird.

(3) **[Vergütung Unterstützungsleistungen]** Soweit nicht ausdrücklich anders vereinbart (insbesondere in Anhang 1 Leistungsbeschreibung), werden Unterstützungsleistungen des Auftragsverarbeiters nach § 3 (5), (6) und § 4 (4), (5) (7), (8, dort Satz 2), (9), (10, dort Satz 2), (11) dieser Vereinbarung gesondert auf Basis von Anhang 2 Leistungsverzeichnis vergütet.

(4) **[Nachweis durch den Auftragsverarbeiter]** Dem Auftragsverarbeiter steht es frei, die hinreichende Umsetzung der Pflichten aus diesem ADV-Vertrag, insbesondere der technisch-organisatorischen Maßnahmen (§ 5) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch folgende Nachweise zu belegen:

- die Einhaltung genehmigter Verhaltensregeln;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit;
- Eigenerklärung des Auftragsverarbeiters.

(5) **[Überprüfungen, Inspektionen]** Der Verantwortliche kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in diesem ADV-Vertrag niedergelegten Pflichten durch die Einholung von Auskünften und Abfrage der unter § 3 Abs. 4 angeführten Nachweise beim Auftragsverarbeiter in Hinblick auf die ihn betreffende Verarbeitung kontrollieren. Der Verantwortliche wird vorrangig prüfen, ob die in Satz 1 dieses Absatzes eingeräumte Möglichkeit der Überprüfung ausreicht. Der Verantwortliche kann darüber hinaus auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz vor Ort kontrollieren. Der Verantwortliche kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Vom Verantwortlichen mit der Kontrolle betraute Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Die vom Verantwortlichen mit der Kontrolle betrauten Personen oder Dritte werden dem Auftragsverarbeiter in angemessener Form vorangekündigt und in die Lage versetzt, ihre Legitimation zur Durchführung der Kontrollen nachzuweisen. Dritte im Sinne dieses Absatzes dürfen keine Vertreter von Wettbewerbern des Auftragsverarbeiters sein. Der Verantwortliche wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen.

(6) **[Unterstützung durch den Verantwortlichen]** Der Verantwortliche wird in Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten unverzüglich und vollständig informieren. Der Verantwortliche wird in Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei der Prüfung möglicher Verstöße und bei Abwehr von Ansprüchen Betroffener oder Dritten sowie bei der Abwehr von Sanktionen durch Aufsichtsbehörden zeitnah und umfänglich unterstützen.

## § 4 Rechte und Pflichten des Auftragsverarbeiters

(1) **[Datenverarbeitung]** Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich im Rahmen des getroffenen Vertrags und nach Weisung des Verantwortlichen entsprechend der Regelung des § 3 Abs. 2. Der Auftragsverarbeiter verwendet die personenbezogenen Daten für keine anderen Zwecke und wird die ihm überlassenen personenbezogenen Daten nicht an unberechtigte Dritte weitergeben. Kopien und Duplikate werden ohne vorherige Einwilligung des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung.

Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen befassten Mitarbeiter und andere für den Auftragsverarbeiter tätigen Personen diese personenbezogenen Daten nur auf Grundlage der Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Der Auftragsverarbeiter wird durch den Verantwortlichen ermächtigt, im Rahmen des 3rd Level Supports, der als Beistellleistung durch die SAP erbracht und in einer separaten Leistungsvereinbarung zwischen dem Verantwortlichen und SAP beauftragt wird, das dem Verantwortlichen gegenüber der SAP bestehende datenschutzrechtliche oder in dieser separaten Leistungsvereinbarung vertraglich vereinbarte Weisungsrecht auszuüben und Weisungen zu erteilen. Datenschutzrechtliche oder in der separaten Leistungsvereinbarung vertraglich vereinbarte Informationspflichten der SAP gegenüber dem Verantwortlichen, insbesondere wenn SAP der der Auffassung ist, dass eine Weisung gegen die geltenden rechtlichen Bestimmungen verstößt, werden zunächst gegenüber dem Auftragsverarbeiter adressiert. Kann der Auftragsverarbeiter dem Einwand nicht selbst innerhalb von 14 Tagen Abhilfe schaffen, informiert der Auftragsverarbeiter den Verantwortlichen. Der Verantwortliche ist dabei über alle wesentlichen Schritte zu informieren und muss dem Abruf kostenpflichtiger Leistungen von SAP im Voraus zustimmen, sofern der Verantwortliche oder SAP den Auftragsverarbeiter auf die Kostenpflicht hinweisen.
Der Verantwortliche wird SAP entsprechend anweisen und dies in der separaten Leistungsvereinbarung vertraglich sicherstellen.

(2) **[Datenschutzbeauftragter]** Der Auftragsverarbeiter gewährleistet, einen unabhängigen, fachkundigen und zuverlässigen Datenschutzbeauftragten zu bestellen, sofern dies von dem anwendbaren Recht der Europäischen Union oder des Mitgliedsstaates, dem der Auftragsverarbeiter unterliegt, gefordert wird.

(3) **[Räumliche Beschränkungen; Vollmacht]** Den Ort der Datenverarbeitung legen die Parteien in **Annex 2** vor der Datenverarbeitung fest. Änderungen des Orts der Datenverarbeitung werden die Parteien bei Bedarf unter Beachtung der in dieser Vereinbarung festgelegten Form vereinbaren.

Eine Datenverarbeitung in sogenannten Drittländern (d. h. Ländern, die keine Mitgliedstaaten der Europäischen Union sind und über kein angemessenes Datenschutzniveau verfügen), wird unter Berücksichtigung der einschlägigen geltenden rechtlichen Bestimmungen der Europäischen Union vorgenommen.

Etwaige Einschränkungen bei der Wahl der Gestaltungsmöglichkeiten der Datenübermittlung nach Maßgabe der einschlägigen geltenden rechtlichen Bestimmungen werden die Parteien in **Annex 2** festlegen. Der Verantwortliche wird die Wahl der Gestaltung der Datenübermittlung durch den Auftragsverarbeiter nicht unbillig einschränken und im erforderlichen Umfang mitwirken.

Der Auftragsverarbeiter bzw. seine genehmigten Unterauftragsverarbeiter (§ 7) werden bei einer nach Annex 2 zugelassenen Verwendung der EU-Standardvertragsklauseln diese im Namen und im Auftrag des Verantwortlichen abschließen. Die entsprechende Vertretungsvollmacht hierfür wird hiermit durch den Verantwortlichen erteilt.

(4) **[Unterstützung bei Pflichten des Verantwortlichen]** Der Auftragsverarbeiter wird – im vertraglich vereinbarten Umfang unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen - den Verantwortlichen bei der Einhaltung seiner ihm nach den geltenden rechtlichen Bestimmungen obliegenden Pflichten unterstützen.

(5) **[Unterstützung bei Überprüfung und Auskunftsbegehren]** Ist der Verantwortliche gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von personenbezogenen Daten zu geben, so wird der Auftragsverarbeiter den Verantwortlichen darin unterstützen, diese Auskünfte zu erteilen, sofern diese Auskünfte die Datenverarbeitung gemäß diesem ADV-Vertrag betreffen.

Der Auftragsverarbeiter wird den Verantwortlichen –soweit rechtlich zulässig- über an ihn als Auftragsverarbeiter gerichtete Mitteilungen der Aufsichtsbehörden (z. B. Anfragen, Benachrichtigung über Maßnahmen oder Auflagen) in Verbindung mit der Verarbeitung von personenbezogenen Daten nach diesem ADV-Vertrag informieren. Soweit rechtlich zulässig wird der Auftragsverarbeiter Auskünfte an Dritte, auch an Aufsichtsbehörden, nur nach schriftlicher Zustimmung durch und in Abstimmung mit dem Verantwortlichen erteilen.

(6) **[Meldung von Zwischenfällen]** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

(7) **[Nachweis und Dokumentation]** Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung.

(8) **[Verzeichnis von im Auftrag durchgeführten Tätigkeiten der Verarbeitung]** Der Auftragsverarbeiter führt nach Maßgabe der einschlägigen geltenden rechtlichen Bestimmungen, denen der Auftragsverarbeiter unterliegt, ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung. Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage und stellt dem Verantwortlichen die für die Führung seines Verzeichnisses von Verarbeitungstätigkeiten notwendigen Angaben zur Verfügung, soweit diese Angaben im vertraglich umschriebenen Verantwortungs- und Leistungsbereich als Auftragsverarbeiter liegen und der Verantwortliche keinen anderen Zugang zu diesen Informationen hat.

(9) **[Datenschutz-Folgenabschätzung]** Falls der Verantwortliche eine Datenschutzfolgenabschätzung durchführt und/oder eine Konsultation der Aufsichtsbehörde nach einer Datenschutzfolgenabschätzung beabsichtigt, wird der Auftragsverarbeiter den Verantwortlichen hierbei angemessen unterstützen. Hierzu werden sich die Vertragsparteien bei Bedarf über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragsverarbeiters abstimmen.

(10) **[Ausübung von Betroffenenrechten]** Abhängig von der Art der Verarbeitung wird der Auftragsverarbeiter den Verantwortlichen bei dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nach Art. 12-22 DSGVO nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Bei Bedarf werden sich die Vertragsparteien über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragsverarbeiters abstimmen.

Soweit sich ein Betroffener zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, leitet der Auftragsverarbeiter die Anfragen des Betroffenen zeitnah an den Verantwortlichen weiter.

(11) **[Übergabe von Speichermedien]** Soweit sich Speichermedien im Besitz des Verantwortlichen befinden, wird der Verantwortliche vor einer etwaig vorgesehenen Übergabe (z.B. zur Prüfung oder Abwicklung von Gewährleistungsansprüchen) an den

Auftragsverarbeiter oder dessen Unter-Auftragsverarbeiter alle personenbezogenen Daten –soweit nicht anders vereinbart- löschen.

(12) **[Abschluss der vertraglichen Arbeiten]** Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien, mit Ausnahme der aufgrund gesetzlicher Verpflichtung des Auftragsverarbeiters weiter vorzuhaltenden personenbezogenen Daten, werden –soweit nicht im Hauptvertrag und dessen Anlagen und Anhänge bereits geregelt und soweit nicht anders vereinbart- an den Verantwortlichen zurückgegeben oder auf Kosten des Verantwortlichen vernichtet bzw. gelöscht. Gleiches gilt für Test- und Ausschussmaterial.

(13) **[Rückgabe oder Löschung von personenbezogenen Daten]** Sofern die Vertragsparteien eine ausdrückliche Vereinbarung zur Rückgabe und Löschung von personenbezogenen Daten bzw. Datenträgern getroffen haben, geht diese Vereinbarung den Regelungen in diesem Absatz vor.

Soweit die Vertragsparteien keine ausdrückliche Vereinbarung zur Rückgabe von personenbezogenen Daten bzw. Datenträgern des Verantwortlichen getroffen haben kann der Auftragsverarbeiter personenbezogene Daten bzw. Datenträger des Verantwortlichen auf Kosten des Verantwortlichen zurückgeben. Wenn der Verantwortliche seiner Rücknahmepflicht nicht nachkommt, steht es dem Auftragsverarbeiter frei, die personenbezogenen Daten bzw. Datenträger auf Kosten des Verantwortlichen zu löschen/vernichten.

Der Verantwortliche kann während des Bestehens des Vertragsverhältnisses oder mit Vertragsende schriftlich die personenbezogenen Daten, die nicht gemäß § 4 Abs. (12) vernichtet bzw. gelöscht sind, auf seine Kosten heraus verlangen und dem Auftragsverarbeiter einen Zeitpunkt (längstens bis Vertragsende) für die Herausgabe nennen. Die Vertragsparteien werden sich nach Herausgabeverlangen auf die weiteren Modalitäten der Herausgabe (wie z.B. Format) verständigen. Das Herausgabeverlangen muss dem Auftragsverarbeiter einen Monat vor dem vom Verantwortlichen benannten Zeitpunkt bzw. ein Monat vor Vertragsende zugegangen sein.

## § 5 Technische und organisatorische Sicherheitsmaßnahmen

(1) **[Technisch organisatorische Maßnahmen]** Der Verantwortliche und der Auftragsverarbeiter werden geeignete technische und organisatorische Maßnahmen treffen, um ein, dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die derzeit als geeignet angesehenen Maßnahmen des Auftragsverarbeiters sind in **Annex 3** und des spezifisch erstellten Anhangs (Technisch-Organisatorische Maßnahmen) beschrieben. Der Verantwortliche hat die technischen und organisatorischen Maßnahmen im Zusammenhang mit etwaigen weiteren Maßnahmen in Hinblick auf ein angemessenes Schutzniveau bewertet. Diese Maßnahmen werden wie in **Annex 3** beschrieben, als geeignete Maßnahmen vereinbart. Etwaige Weiterentwicklungen erfolgen nach Maßgabe von § 5 Abs. 2.

(2) **[Weiterentwicklung]** Die technischen und organisatorischen Maßnahmen können im Laufe des Vertragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

Die Sicherheit der Verarbeitung und die Angemessenheit des Schutzniveaus wird der Verantwortliche regelmäßig prüfen und dem Auftragsverarbeiter etwaigen Anpassungsbedarf unverzüglich mitteilen. Der Verantwortliche wird dem Auftragsverarbeiter hierzu alle erforderlichen Informationen zur Verfügung stellen. Der Auftragsverarbeiter seinerseits kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen der EU DSGVO und den LUB erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Der Verantwortliche ersetzt dem Auftragsverarbeiter, soweit nicht ausdrücklich anderweitig vereinbart, den durch die Anpassung der Schutzmaßnahmen an den technischen Fortschritt entstehenden Mehraufwand.

(3) **[Überprüfung und Nachweis]** Für die Überprüfungs- und Nachweismöglichkeiten gelten § 3 Abs. 4 und § 3 Abs. 5.

## § 6 Vertraulichkeit

(1) **[Vertraulichkeit]** Der Auftragsverarbeiter wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit wahren. Er wird die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten, soweit diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Vereinbarungen im Hauptvertrag zur Wahrung der Vertraulichkeit und zum Schutz von nicht personenbezogenen Daten bleiben unberührt. Soweit im Hauptvertrag hierzu keine Vereinbarung getroffen wurden, verpflichten sich beide Parteien, alle nicht allgemein offenkundigen Informationen aus dem Bereich der anderen Partei, die ihnen durch die Geschäftsbeziehung bekannt werden, geheim zu halten und nicht für eigene Zwecke außerhalb dieses Vertrages oder Zwecke Dritter zu verwenden.

(2) **[Pflichten beteiligter Personen]** Der Auftragsverarbeiter wird Personen, die Zugang zu personenbezogenen Daten haben, mit den für sie maßgeblichen Datenschutzvorgaben und Weisungen dieser Vereinbarung im Voraus vertraut machen.

(3) **[Geheimnisschutz]** Im Rahmen des Auftrages werden auch ggf. Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen. Der Auftragsverarbeiter verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Der Verantwortliche weist den Auftragsverarbeiter darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1. StGB strafbar machen. Der Auftragsverarbeiter wird seine Beschäftigten und andere für den Auftragsverarbeiter tätige Personen allgemein oder spezifisch zur Geheimhaltung verpflichten.

## § 7 Unterauftragsverarbeiter

(1) **[Befugnis]** Der Auftragsverarbeiter darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einsetzen.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Aufträge zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung erteilt und die keine Auftragsverarbeitungsleistung für den Verantwortlichen beinhalten.

(2) **[Gesonderte Genehmigung]** Für die in **Annex 4** aufgeführten Unterauftragsverarbeiter sowie die in **Annex 5** aufgeführten Sub-Unterauftragsverarbeiter und die dort genannten Aufgabenbereiche gilt die Genehmigung des Verantwortlichen als erteilt.

(3) **[Allgemeine schriftliche Genehmigung]** Der Verantwortliche erteilt hiermit dem Auftragsverarbeiter die allgemeine Genehmigung für den künftigen Einsatz weiterer Auftragsverarbeiter (Unterauftrags- und Sub-Unterauftragsverarbeiter).

(4) **[Information bei Änderungen]** Der Auftragsverarbeiter informiert den Verantwortlichen schriftlich oder per E-Mail, über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter), wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen binnen 14 Tagen nach Zugang der Information beim

Verantwortlichen Einspruch zu erheben. Die Vertragsparteien werden sich bei Bedarf über Art und Weise, hinzutretender oder alternativer Möglichkeiten der Information über den künftigen Einsatz oder Änderungen beim Einsatz weiterer Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter verständigen. Dies kann z.B. die Vorhaltung und den Abruf einer Listung der Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einschließen. Der Verantwortliche wird die Genehmigung zur Einbindung weiterer Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter nicht ohne wichtigen Grund verweigern.

(5) **[Kündigungsrecht des Auftragsverarbeiter]** Dem Auftragsverarbeiter steht ein außerordentliches Kündigungsrecht des Hauptvertrages nach Maßgabe des Hauptvertrages – oder für den Fall, dass ein solches Kündigungsrecht im Hauptvertrag nicht eingeräumt wurde, ein außerordentliches Kündigungsrecht von 4 Wochen zum Monatsende - zu, wenn nach Auffassung des Auftragsverarbeiters der Verantwortliche die Einbindung des Unterauftragsverarbeiters und/oder Sub-Unterauftragsverarbeiters ohne wichtigen Grund verweigert oder dem Auftragsverarbeiter eine Leistungserbringung ohne den abgelehnten Unterauftragsverarbeiter und/oder Sub-Unterauftragsverarbeiters nicht möglich ist.

(6) **[Auswahl, Back-to-Back-Vereinbarung]** Der Auftragsverarbeiter wird Unterauftragsverarbeiter auswählen, die hinreichende Garantien dafür bieten, dass die vereinbarten geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der einschlägigen geltenden rechtlichen Bestimmungen erfolgt. Der Auftragsverarbeiter wird mit Unterauftragsverarbeitern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen diesem Vertrag inhaltlich entsprechen. Der Auftragsverarbeiter wird mit dem Unterauftragsverarbeiter die technischen und organisatorischen Maßnahmen festlegen und die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen regelmäßig kontrollieren.

(7) **[Sub-Unterauftragsverarbeiter]** Die Beauftragung von Sub-Unterauftragsverarbeitern durch den Auftragsverarbeiter ist nach Maßgabe der § 7 Abs. (1) bis Abs. (6) zulässig.

(8) **[Verhältnis zum Hauptvertrag]** § 1 Abs. (7) des Hauptvertrages bleibt unberührt und gilt neben diesem § 7.

## § 8 Vertragsdauer; Kündigung

Diese Vereinbarung gilt für die Dauer der tatsächlichen Leistungserbringung durch den Auftragsverarbeiter. Dies gilt unabhängig von der Laufzeit etwaiger anderer Verträge

(insbesondere des Hauptvertrags), die die Parteien ebenfalls bzgl. der Erbringung der vereinbarten Leistungen abgeschlossen haben.

## § 9 Ansprechpartner

(1) Ansprechpartner beim Auftragsverarbeiter ist:

Ansprechpartner: [redacted]
Telefon: [redacted]
E-Mail: [redacted]

(2) Datenschutzbeauftragter des Auftragsverarbeiters ist:

Datenschutzbeauftragter: Dr. Claus D. Ulmer
Global Data Privacy Officer
Telefon: +49 228 181-82007
E-Mail: claus.ulmer@telekom.de

(3) Ansprechpartner des Verantwortlichen ist:

Ansprechpartner: Jörg Lekschas
Funktion: Datenschutzbeauftragter
Telefon: +49 30 18754 3594
E-Mail: Datenschutz@rki.de

(4) Datenschutzbeauftragter des Verantwortlichen ist:

Ansprechpartner: Jörg Lekschas
Funktion: Datenschutzbeauftragter
Telefon: +49 30 18754 3594
E-Mail: Datenschutz@rki.de

## § 10 Haftung und Freistellung

(1) **[Verantwortungsbereich des Verantwortlichen]** Der Verantwortliche gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Pflichten bei der Verarbeitung personenbezogener Daten.

(2) **[Haftung]** Die Haftungsregelung des Hauptvertrages gilt für diese Vereinbarung zur Auftragsverarbeitung, soweit nicht eine Haftungsbeschränkung nach Maßgabe der jeweils einschlägigen geltenden rechtlichen Bestimmungen zugunsten des Auftragsverarbeiters greift.

## § 11 Sonstiges

(1) **[Gültigkeit des Vertrags]** Von der Ungültigkeit einer Bestimmung dieses ADV-Vertrags bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

(2) **[Änderungen des Vertrags]** Sämtliche Änderungen dieses ADV-Vertrags sowie Nebenabreden bedürfen der Schriftform (einschließlich in elektronischer Form). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

(3) **[Geschäftsbedingungen]** Es besteht zwischen den Parteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen" des Verantwortlichen auf diesem ADV-Vertrag keine Anwendung finden.

(4) **[Gerichtsstand]** Der alleinige Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem ADV-Vertrag ist in **Annex 2** festgelegt. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

(5) **[Geltendes Recht]** Es gelten die Regelungen in § 2 (1) und Annex 1.

(6) **[Vorrangregelung]** Bei Widersprüchen zwischen den Bestimmungen dieses Vertrags und Bestimmungen sonstiger Vereinbarungen, insbesondere des Hauptvertrags, sind die Bestimmungen dieses ADV-Vertrags maßgebend. Im Übrigen bleiben die Bestimmungen des Hauptvertrags unberührt und gelten für diesen ADV-Vertrag entsprechend.

**Annexe:**

Nachstehende Annexe sind feste Bestandteile dieser Vereinbarung:

Annex 1: Landes- und Unternehmensspezifische Bedingungen (LUB)
Annex 2: Einzelheiten der Datenverarbeitung
Annex 3: Technische und organisatorische Sicherheitsmaßnahmen
Annex 4: Genehmigte Unterauftragsverarbeiter
Annex 5: Genehmigte Sub-Unterauftragsverarbeiter
Annex 6: Anlage technische und organisatorische Maßnahmen

| Verantwortlicher: | Auftragsverarbeiter: |
| --- | --- |
| _____ | _____ |
| Ort, Datum _____ | Ort, Datum _____ |
| Name: | Name: |
| _____ | _____ |
| Unterschrift: | Unterschrift: |
| _____ | _____ |
| Name: | Name: |
| _____ | _____ |
| Unterschrift: | Unterschrift: |
| _____ | _____ |

## Annex 1

## Landes- und Unternehmensspezifische Bedingungen („LUB")

1. Landesspezifische Bestimmungen für Auftragsverarbeiter mit Sitz in Deutschland:

**[Geltung EU-Datenschutzgrundverordnung]** Es gilt die europäischen Datenschutz-Grundverordnung [Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO] sowie das Bundesdatenschutzgesetz (BDSG).

a) **[Hinzutretende spezifische Bestimmungen]** Hinzutretend vereinbaren die Vertragsparteien folgende spezifische Bedingungen

-keine-

## Annex 2

## Einzelheiten der Datenverarbeitung

1. **Kategorien von Verarbeitungen, zu verarbeitende** personenbezogene **Daten/betroffene** personenbezogene **Daten; Art des Zugriffs:**

a. Angaben zu „Kategorien von Verarbeitungen"

- Cloud Speicherdienst
- App-Betrieb: „Application Operation" Service
- CDN
- Infrastruktur (Serverbetrieb)
- Call-Center (Hotline)

Einzelheiten sind in dem Dokument „Datenschutzkonzept der Corona Warn App der Bundesrepublik Deutschland" unter Ziffer IV. 3. Gesamt-Architektur (Beschreibung der Komponenten; vertiefend in Einzel-Konzepten) beschrieben.

b. Kategorien betroffener Personen:

- App-Nutzer
- Mitarbeiter Gesundheitsamt (manuelles Authentifizierungsverfahren)
- Mitarbeiter Hotline (manuelles Authentifizierungsverfahren)

Einzelheiten sind in dem Dokument „Datenschutzkonzept der Corona Warn App der Bundesrepublik Deutschland" unter Ziffer IV. 1. Rollenbeschreibung (who is who) beschrieben.

c. Betroffene personenbezogene Daten:

- Temporary Exposure Key (TEK); Rotating Proximity Identifiers (RPI).
- GUID, Registration-ID, Testergebnis und TAN / teleTAN
- Manuelles Authentifizierungsdaten (Name, Telefonnummer)

Einzelheiten sind in dem Dokument „Datenschutzkonzept der Corona Warn App der Bundesrepublik Deutschland" unter Ziffer V. 1. Wesentliche personenbezogene Daten beschrieben.

d. Besondere Kategorien von personenbezogenen Daten (z.B. Art. 9 DSGVO (müssen *hier detailliert angegeben werden).*

Gesundheitsdaten (Temporary Exposure Key (TEK); Rotating Proximity Identifiers (RPI); GUID, Registration-ID, TAN/TeleTAN in Verbindung mit Testergebnis)

e. Zugriff auf personenbezogene Daten

Der Auftragsverarbeiter betreibt für den Verantwortlichen die Corona Warn App der Bundesrepublik Deutschland.

In diesem Zusammenhang verarbeitet der Auftragsverarbeiter die über die App erzeugten Daten sowie die über die Schnittstelle zu den Laboren (Lab-Server), den Portal-Server sowie das CDN erzeugten Daten bzw. kann ein Zugriff darauf nicht ausgeschlossen werden.

## 2. Leistungen, Verarbeitungszweck:

Der Auftragsverarbeiter erbringt die folgenden Leistungen – Einzelheiten sind in Anhang 1 (Leistungsbeschreibung Corona Warn App) des Hauptvertrages sowie in dem Dokument „Datenschutzkonzept der Corona Warn App der Bundesrepublik Deutschland" unter Ziffer IV. 3. Gesamt-Architektur (Beschreibung der Komponenten; vertiefend in Einzel-Konzepten) dokumentiert.

**(1) Corona Warn App (CWA)**
Die Corona Warn App ist eine eigens entwickelte mobile Applikation, die die zentrale Komponente zur Nutzer-Interaktion darstellt. Als native Applikation sowohl für iOS als auch für Android nutzt sie Systemkomponenten als auch zusätzliche Bibliotheken um die näheren Kontakte zu ermitteln.
Der Auftragsverarbeiter erbringt Applikationsbetrieb der Leistungsklasse **„Application Service"** für die Verifikation Komponenten und die Mobile Backend Komponente von SAP.

**(2) Corona-Warn-App Server**
Der Corona-Warn-App Server dient als Backend der Corona-Warn-App und hat als Kernaufgabe die Verwaltung bzw. Verteilung von Kontaktdaten von infizierten Personen (diagnosis keys). Die Corona-Warn-App ist eine Individualapplikation, welche in Java entwickelt wurde. Sie läuft in Containern in kubernetes Clustern der OTC (Open Telekom Cloud).
Der Auftragsverarbeiter erbringt Applikationsbetrieb der Leistungsklasse **„Application Service"** für die Verifikation Komponenten und die Mobile Backend Komponente von SAP.

**(3) Storage Service**

Für die Speicherung der Keys der infizierten Personen wird ein eigenes Storage Service genutzt. Dieses wird vom Corona-Warn-App Server bespielt und vom Content Delivery Network als zentrale Datenverteilungsquelle genutzt. Er läuft in Containern in kubernetes Clustern der OTC (Open Telekom Cloud).
Der Auftragsverarbeiter erbringt Applikationsbetrieb der Leistungsklasse **„Application Service"** für die Verifikation Komponenten und die Mobile Backend Komponente von SAP.

**(4) Content Delivery Network**
Das Content Deliver Network der Deutschen Telekom dient zur Bereitstellung von Kontaktdaten der infizierten Personen (diagnosis keys). Durch cache-Mechanismen wird der Ressourcenaufwand reduziert. Das Storage Service des Content Delivery Network dient als Quelle der Auslieferung von Daten an die Corona-Warn-Apps welche aktiv die Daten anfragen. Es wird keine Push-Benachrichtigung an die Mobilgeräte ausgesandt.

**(5) Verification Server**
Der Verification Server dient als zentrale Komponente zur Verifikation von Daten. Er generiert und speichert alle gültigen Registration Tokens, die zum Abrufen von Testergebnissen mittels QR-Code, notwendig sind. Ebenso stellt er Prüf-Dienste zur Verfügung, welche vom Corona-Warn-App Server genutzt werden, um sicherzustellen, dass nur infizierte Personen ihre Kontaktdaten (diagnosis keys) hochladen können. Die Komponente ist eine Individualapplikation, welche in Java entwickelt wurde. Sie läuft in Containern in kubernetes Clustern der OTC (Open Telekom Cloud).

**(6) Laboratory Information System (LIS)**
Das Laboratory Information System (LIS) dient als Verwaltung der Testergebnisse. Es speichert die relevanten Testergebnisse und stellt die Verknüpfung zu den GUIDs her, welche per QR-Code gescannt wurden. Nur Informationen zu Tests, bei denen der QR-Code gescannt wurde, werden hier gespeichert. Das LIS dient als reines Datenspeicherungssystem. Die Labor Clients bespielen diesen und der Verification Server ruft die entsprechenden Ergebnisse ab. Die Komponente ist eine Individualapplikation, welche in Java entwickelt wurde. Sie läuft in Containern in kubernetes Clustern der OTC (Open Telekom Cloud).

**(7) Portal Server**
Der Portal Server dient als zentrale Generierungsmöglichkeit für teleTANs. Dieser wird sowohl vom Gesundheitsamt als auch von der Hotline genutzt. Die zentrale Funktionalität ist die Generierung von teleTANs und deren Ablage am Verification-Server. Damit ist sichergestellt, dass auch Personen, welche bei der Testabgabe keinen QR-Code gescannt haben, ebenso im Falle einer Infektion ihre Kontaktdaten (diagnosis keys) hochladen können. Die Komponente ist eine Individualapplikation, welche in Java entwickelt wurde. Sie läuft in Containern in kubernetes Clustern der OTC (Open Telekom Cloud).

**(8) Hotline**
- Technische Hotline: Technischer Support „FAQ-Hotline" – es werden keine personenbezogenen Daten verarbeitet.
- Freischalthotline (manueller Prozess): Sollte bei einem durchgeführten Test kein QR-Code hinterlegt worden sein, so besteht die Möglichkeit mittels teleTAN dennoch die Kontaktdaten einer infizierten Person zu übermitteln. Die Hotline vergibt nach erfolgter Verifikation eine teleTAN.

**(9) Support-Services**
Der Auftragsverarbeiter erbringt für den Betrieb den 1st und 2nd Level Support. Der 3rd Level Support wird von der SAP als Beistell-Leistung erbrach (Ziffer 3.3.5 der Leistungsinformation Anhang 1 des Hauptvertrages).

## 3. Verarbeitungsort:

Die Verarbeitung der Daten findet in Deutschland, den Niederlanden und Ungarn statt. Einzelheiten sind in Annex 4 und 5 dokumentiert.

## 4. (Anforderungen an die Auftragsverarbeitung in Drittländer)

Die Auftragsverarbeitung in (Standort, (Drittland-)Land) soll, soweit dies durch den Verantwortlichen genehmigt ist, auf folgender Grundlage vorgenommen werden

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (z.B. Art. 45 Abs. 3 DSGVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (z.B. Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (z.B. Art. 46 Abs. 2 lit. c und d DSGVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (z.B. Art 46 Abs. 2 lit. e i.V.m. 40 DSGVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (z.B. Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: ..... (z.B. Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DSGVO)

## 5. Gerichtsstand:

Bonn

## Annex 3

## Technische und organisatorische Sicherheitsmaßnahmen

Für die beauftragte Erhebung und / oder Verarbeitung von personenbezogenen Daten werden folgende Maßnahmen vereinbart:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
    a. Zutrittskontrolle
    Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
    b. Zugangskontrolle
    Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
    c. Zugriffskontrolle
    Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
    d. Trennungskontrolle
    Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)
    a. Weitergabekontrolle
    Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
    b. Eingabekontrolle
    Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
    a. Verfügbarkeitskontrolle
    Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
    b. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
    a. Datenschutz-Management;
    b. Incident-Response-Management;
    c. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
    d. Auftragskontrolle
       Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Detaillierte Einzelheiten zu den technischen und organisatorischen Maßnahmen gem. Art. 28 Abs.3 lit c) i.V.m. Art. 32 DSGVO sind in dem Dokument „Datenschutzkonzept der Corona Warn App der Bundesrepublik Deutschland" unter Ziffer VI. Designentscheidungen an Hand des Datenflusses sowie in der „Anlage technische und organisatorische Maßnahmen" (**Annex 6**) beschrieben.

## Annex 4

## Genehmigte Unterauftragsverarbeiter

## Angaben zu Unterauftragsverarbeitern / Leistungen / Verarbeitungsorte

### Gesonderte Genehmigung

Der Auftragsverarbeiter beabsichtigt, die folgenden Unterauftragsverarbeiter für die folgenden Leistungen / an den folgenden Verarbeitungsorten einzusetzen:

Deutsche Telekom Regional Solutions & Products GmbH
53113 Bonn, Friedrich-Ebert-Allee 71 -77
Services: 1st & 1,5 Level Support für OTC
Verarbeitungsort: Deutschland

IT Services Hungary
H-1097 Budapest, Toth Kalman u 2/B
Services: Operation, 1st and 2nd Level Support für OTC
Verarbeitungsort: Ungarn

Deutsche Telekom IT GmbH
53227 Bonn, Landgrabenweg 151
Service: User support MyWorkplace für OTC
Verarbeitungsort: Deutschland

Axivas Deutschland GmbH
68723 Schwetzingen, Carl-Benz-Straße 9-11
Services: Service Desk für OTC
Verarbeitungsort: Deutschland

Deutsche Telekom Individual Solutions & Products GmbH
53113 Bonn, Friedrich-Ebert-Allee 70
Services: DC Hardware disposal and replace für OTC
Verarbeitungsort: Deutschland, Niederlande

Axivas Deutschland GmbH
46047 Oberhausen, Zum Aquarium 6a
Services: Call-center Leistung für Hotline
Verarbeitungsort: Deutschland

Deutsche Telekom Technik GmbH
53227 Bonn, Landgrabenweg 151
Services: CDN
Verarbeitungsort: Deutschland

## Annex 5

## Genehmigte Sub-Unterauftragsverarbeiter

## Angaben zu Sub-Unterauftragsverarbeiter / Leistungen / Verarbeitungsorte

### Gesonderte Genehmigung

Die folgenden Sub-Unterauftragsverarbeiter dürfen für die folgenden Leistungen / an den folgenden Verarbeitungsorten eingesetzt werden:

GULP Solutions Services GmbH & Co.KG
50667 Köln, Breite Straße 137-139
Service: Servicedesk für OTC
Verarbeitungsort: Deutschland, Magdeburg
Eingesetzt von Deutsche Telekom Individual Solutions & Products GmbH

3 W Phone GmbH (100 Prozent Tochter der Axivas)
06108 Halle (Saale), Leipziger Straße 85a
Services: Call-center Leistung für Hotline
Verarbeitungsort: Deutschland
Eingesetzt von Axivas Deutschland GmbH

## Annex 6

## Anlage technische und organisatorische Maßnahmen

# Anhang 1: Technisch-Organisatorische Maßnahmen

(Version 1.0 - STAND: 05.06.2020)

## 1 Inhalt

### 1.1.1 Dokumentation und Konzeption

1001 **Dokumentation**

**Es müssen die folgenden Konzepte bereitgestellt werden:**

**Datenschutzkonzepte für**

- **Rahmendokument**
- **CWA Mobile Client**
- **CWA Backend**
- **Verifikation und Testergebnisse Backend**
- **Hotline**

**Berechtigungskonzepte für Komponenten**

- **CWA-Server**
- **Testresult-Server**
- **Portal Server**
- **Verification Server**
- **CDN**

**Die Erfüllung der Anforderung 1001 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1002 **Dokumentation**

**Für die Server (CWA Server, Testresult Server, Portal Server, Verification Server und CDN) müssen außerdem**

- **Betriebskonzepte**
- **Architekturdokumentation**

**bereitgestellt werden.**

**Die Erfüllung der Anforderung 1002 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1003 **Dokumentation**

**Es muss ein Verzeichnis der Verarbeitungstätigkeiten bereitgestellt werden**

**Die Erfüllung der Anforderung 1003 wird für diesen Vertrag verpflichtend vereinbart.** ☒

## 1.2 Spezielle Technisch-Organisatorische Maßnahmen

### 1.2.1 Pseudonymisierung

**Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zur Zuordenbarkeit erforderlichen zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, so dass der Verantwortliche/der Dienstleister keinen Zugriff auf diese Informationen hat.**

#### 1.2.1.1 Technische Maßnahmen

1004 **Pseudonymisierung**

**Zur Pseudonymisierung müssen die Zuordnungsdaten in getrennten und abgesicherten Systemen aufbewahrt werden, auf welche die pseudonymen Daten verarbeitende Personen keinen Zugriff haben.**

**Die Erfüllung der Anforderung 1004 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1005 **Pseudonymisierung**

**Die notwendigen zur Pseudonymisierung aufbewahrten Zuordnungsdaten müssen verschlüsselt abgelegt werden. Personen, die pseudonymen Daten verarbeiten, dürfen keinen Zugriff auf die Schlüssel haben.**

**Die Erfüllung der Anforderung 1005 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1006 **Pseudonymisierung**

**Die Pseudonymisierung muss immer im jeweiligen Quellsystem erfolgen.**

**Die Erfüllung der Anforderung 1006 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1007 **Pseudonymisierung**

**Der Quellcode der Erzeugungsfunktion muss einsehbar sein.**

**Die Erfüllung der Anforderung 1007 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1008 **Pseudonymisierung**

**Eine Prüfung auf Inplausibilitäten und Dopplungen im Vorfeld einer Pseudonymisierung erfolgt grundsätzlich automatisiert.**

**Die Erfüllung der Anforderung 1008 wird für diesen Vertrag verpflichtend vereinbart. ☒**

#### 1.2.1.2 Organisatorische Maßnahmen

1009 **Pseudonymisierung**

**Es werden alle Daten frühestmöglich pseudonymisiert verarbeitet.**

**Die Erfüllung der Anforderung 1009 wird für diesen Vertrag verpflichtend vereinbart. ☒**

1010 **Getrennte Verarbeitung**

**Die Server werden von getrennten Teams betrieben, um Re-Identifikationsattacken durch Administratoren zu erschweren. Um sicherzustellen, dass kein Missbrauch der Administrationsrechte stattfindet werden die Logs in regelmäßigen Abständen geprüft und ausgewertet.**

**Die Erfüllung der Anforderung 1010 wird für diesen Vertrag verpflichtend vereinbart. ☒**

### 1.2.2 Verschlüsselung

#### 1.2.2.1 Technische Maßnahmen

1011 **Datenminimierung**

**Auf den Servern gespeicherte personenbezogene Daten (Pseudonyme) müssen verhasht werden. Gesundheitsdaten (Diagnoseschlüssel und TAN) müssen verschlüsselt gespeichert werden.**

**Die Erfüllung der Anforderung 1011 wird für diesen Vertrag verpflichtend vereinbart. ☒**

1012 **Datenminimierung**

**Für den Datenaustausch zwischen der CWA und den Servern und die Speicherung personenbezogener Daten (Pseudonyme) werden dem aktuellen Stand der Technik entsprechende kryptographische Verfahren eingesetzt. Hierfür werden folgende Techniken eingesetzt**

**Die Erfüllung der Anforderung 1012 wird für diesen Vertrag verpflichtend vereinbart. ☒**

### 1.2.2.2 Organisatorische Maßnahmen

1013 Datenminimierung

**Bei dem Einsatz von Verschlüsselung wird sichergestellt, dass**

- **die Erzeugung des Schlüssels bzw. Schlüsselmaterials ein sicherer Prozess ist**
- **Salt (soweit eingesetzt) und/oder der Schlüssel bzw. das Schlüsselmaterial derart erzeugt werden, dass diese weder vorhersagbar sind noch erraten werden können**
- **der Erzeugung des Schlüssels bzw. Schlüsselmaterials eine qualitativ hochwertige Zufallszahlenquelle zugrunde liegt**
- **die Vertraulichkeit des Schlüssels bzw. des Schlüsselmaterials während des vollständigen Lebenszyklus der verarbeiteten personenbezogenen Daten gewährleistet ist**
- **der Zugriff auf den Salt und/oder den Schlüssel bzw. das Schlüsselmaterial auf ein absolutes Minimum vertrauenswürdiger Anwender beschränkt ist und geheim gehalten wird**

**Es liegt ein Konzept zum Schlüsselmanagement vor und dieses enthält Informationen sowohl zum Schlüsseltausch als auch zur Feststellung von Vorgehensweisen bei Kompromittierung.**

**Die Erfüllung der Anforderung 1013 wird für diesen Vertrag verpflichtend vereinbart.** ☒

## 1.2.3 Datenminimierung

### 1.2.3.1 Technische Maßnahmen

1014 Datenminimierung

**Es werden nur die für die Erreichung des Zwecks der CWA erforderlichen Daten verarbeitet. Es werden nur die Diagnoseschlüssel der letzten 2 Wochen auf das CWA Backend geladen.**

**Die Erfüllung der Anforderung 1014 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1015 Datenminimierung

**Die Server müssen mit großer Sorgfalt konfiguriert werden, so dass keine unnötigen Daten erhoben werden (es werden keine Kennungen in die Serverprotokolle aufgenommen). Anfragen der CWA an die Server geben keine unnötigen Informationen über den Benutzer preis. Es werden keine Standortdaten verarbeitet, auch nicht, um die Interoperabilität mit Mitgliedsstaaten zu ermöglichen.**

**Die Erfüllung der Anforderung 1015 wird für diesen Vertrag verpflichtend vereinbart.** ☒

### 1.2.3.2 Organisatorische Maßnahmen

## 1.2.4 Vertraulichkeit

### 1.2.4.1 Zutrittskontrolle

**Mit dem Begriff „Zutritt" ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT- Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netzverkabelungen befinden und verlegt sind, gehören hierzu. Die Datenverarbeitung erfolgt in Rechenzentren der OpenTelekomCloud (OTC).**

#### 1.2.4.1.1 Technische Maßnahmen

1016 Festlegung von Sicherheitsbereichen

**Der Schutzbedarf eines Gebäudes bzw. Raumes ist festzustellen anhand der darin befindlichen DV-Anlagen sowie ggf. sonstiger Unterlagen auf denen personenbezogene Daten verarbeitet bzw. gespeichert werden.**

**Die Erfüllung der Anforderung 1016 wird für diesen Vertrag verpflichtend vereinbart: ☒**

1017 Realisierung eines wirksamen Zutrittsschutzes

**Sicherheitsbereiche sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete technische (z.B. Spezialverglasung, Einbruchmeldesystem, Drehkreuz mit Chipkarte, Vereinzelungsanlage, Schließanlage) Maßnahmen abgesichert werden.**

**Es erfolgen folgende Zutrittskontrolle für den Zutritt zu den Servern:**

- **Sicherheitstür(en)**
- **Transponderkarte**
- **Schlüssel / Manuelles Schließsystem**
- **Schließsystem mit Codesperre**
- **Einbruchmeldeanlage**
- **Brandmeldeanlage**
- **Videoüberwachung**
- **Elektronische Signatur**

**Der Zutritt zum Rechenzentrum ist wie folgt gesichert:**

- **Alarmanlagen**
- **Vergitterte Fenster/Sicherheitsfenster, -schlösser, -türen mit einer definierten Widerstandsklasse**
- **Bewegungsmelder**
- **Durchbrechschutz gegen Fahrzeuge**

Zudem befinden sich die Server in abschließbaren Serverschränken. Gelagerte Notebooks befinden sich unter Verschluss in gesicherten Räumen. Die Aufbewahrung von Datensicherungen (z. B. Bänder, CDs) erfolgt in zutrittsgeschützten Safes oder Räumen.

Die Erfüllung der Anforderung 1017 wird für diesen Vertrag verpflichtend vereinbart. ☒

1018 Festlegung zutrittsberechtigter Personen

Die Voraussetzungen sowie der Kreis der allgemein zutrittsberechtigten Personen müssen festgelegt und die Zutrittsberechtigungen zu sicherheitsrelevanten Bereichen, auf das notwendige Minimum beschränkt werden ("Prinzip der minimalen Berechtigung"). Der Zutritt ist bei fehlender Berechtigung zu verwehren. Zutrittsmittel zu Gebäuden bzw. Räumlichkeiten sind grundsätzlich personengebunden zu vergeben und dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür zu sensibilisieren.

Die Erfüllung der Anforderung 1018 wird für diesen Vertrag verpflichtend vereinbart. ☒

1019 Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus

Ein Prozess zur Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. zum Entzug von Zutrittsrechten (einschl. Schlüssel-, Sichtausweise, Transponder, Chipkartenverwaltung etc.) ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Sperren von Zutrittsberechtigungen sind zu beschreiben. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zutrittsmittel und -rechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr erforderlichen Räumlichkeiten unverzüglich zu entziehen. Sämtliche mit Sicherheitsaufgaben betraute Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.

Die Erfüllung der Anforderung 1019 wird für diesen Vertrag verpflichtend vereinbart. ☒

1020 Begleitung von Besuchern und Fremdpersonal

Es existieren schriftlich fixierte Regelungen zum Zutritt für Firmenfremde, wie Gäste oder Lieferanten. Diese Regelungen beinhalten minimal die Anforderung, dass Firmenfremde Ihren berechtigten Aufenthalt innerhalb der Gebäude jederzeit nachweisen können, z.B. mittels Gästeausweis, Besucherausweis, oder Lieferantenausweis. Namen und Herkunft (Firmenzugehörigkeit, Geschäftsadresse oder Privatadresse) der Personen sind zu protokollieren. Die stichprobenartige Prüfung des berechtigten Aufenthaltes innerhalb der Gebäude ist obligatorisch. Besteht ein erhöhter Schutzbedarf, sind nicht autorisierte Personen zu begleiten bzw. während ihrer Tätigkeit zu beaufsichtigen.

Die Erfüllung der Anforderung 1020 wird für diesen Vertrag verpflichtend vereinbart. ☒

#### 1.2.4.1.2 Organisatorische Maßnahmen

1021 Realisierung eines wirksamen Zutrittsschutzes

Sicherheitsbereiche sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete organisatorische (z.B. Pförtner) Maßnahmen abgesichert werden. Hierzu existiert ein Zutrittskontrollsystem, in welchem die zutrittsberechtigten Mitarbeiter festgelegt sind. Es bestehen Regelungen für den Zutritt von Fremdpersonal, Reinigungspersonal und Besucher. Die Begleitung von Gästen im Gebäude ist in einer Richtlinie geregelt. Differenzierte Sicherheitsbereiche/-zonen (z. B. für Server, Großrechner, Archiv) sind festgelegt. Auch die Datenträger sind Bestandteil des Zutrittsschutzkonzepts und es liegt eine Anweisung zur Ausgabe von Schlüsseln vor. Es erfolgen folgende Zutrittskontrolle für den Zutritt zum Betriebsgelände/Gebäude:

- Empfang/Rezeption/Pförtner
- Besucherbuch/Protokoll der Besucher
- Verschließen von Türen und Fenstern, sobald Personal nicht im Raum
- Mitarbeiterausweise
- Besucherausweise
- Werkschutz/Wachpersonal

Die Erfüllung der Anforderung 1021 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.4.2 Zugangskontrolle

Maßnahmen zur Zugangskontrolle dienen der Verhinderung der unbefugten Nutzung von Anlagen/Systemen, mit welchen (personenbezogene) Daten verarbeitet werden. Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV- Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden.

#### 1.2.4.2.1 Technische Maßnahmen

1022 Zugangsschutz (Authentifizierung)

Der Zugang zu DV-Anlagen, auf denen Daten verarbeitet werden, darf erst nach Identifikation und erfolgreicher Authentifizierung (z.B. durch Benutzername und Passwort oder Chipkarte/ PIN) der befugten Personen durch dem Stand der Technik entsprechende Sicherheitsmaßnahmen möglich sein. Der Zugang ist bei fehlender Berechtigung entsprechend zu verwehren.

Die Erfüllung der Anforderung 1022 wird für diesen Vertrag verpflichtend vereinbart. ☒

1023 Starke Authentisierung bei hohem bis höchstem Schutzniveau

Eine starke Authentisierung erfolgt immer auf Basis mehrerer (mindestens zweier) Merkmale wie z.B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer eigenen Eigenschaft. Dies sind beispielsweise:

- Chipkarte mit Zertifikaten und PIN
- OneTimePassworte (OTP Generator, SMS TAN, ChipTAN) und Nutzerpasswort

Im Rahmen der Zwei-Faktor-Authentifizierung werden als die zwei Faktoren verwandt:

- Hardware Token (Smart Card)
- PKI / zertifikatsbasierte Anmeldung
- Geräte-Identifikation
- Virtuelle Smartcards

Die Erfüllung der Anforderung 1023 wird für diesen Vertrag verpflichtend vereinbart. ☒

1024 Nutzung der Datenübertragung durch Dritte

Die Nutzung von IT-Systemen mithilfe von Einrichtungen der Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert oder zumindest nachvollziehbar gemacht:

- Standleitung
- Teilnehmerkennung
- Ausweisleser
- Protokollierung der Systemnutzung und Protokollauswertung
- Sonstige: gleiche Sicherungen wie bei Zwei-Faktor-Authentifizierung

Die Erfüllung der Anforderung 1024 wird für diesen Vertrag verpflichtend vereinbart. ☒

1025 Protokollierung des Zugangs

Über alle Aktivitäten in den IT-Systemen werden automatisch Protokolle erstellt. Alle erfolgreichen und abgewiesenen Zugangsversuche müssen protokolliert (verwendete Kennung, Rechner, IP-Adresse) und für mindestens 30 Tage revisionssicher archiviert werden. Zur Missbrauchserkennung sind regelmäßig stichprobenartige Auswertungen vorzunehmen.

Die Erfüllung der Anforderung 1025 wird für diesen Vertrag verpflichtend vereinbart. ☒

1026 Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk

Das Authentisierungsgeheimnis (z.B. Benutzerkennung und Passwort) darf nie ungeschützt über das Netzwerk übertragen werden.

Die Erfüllung der Anforderung 1026 wird für diesen Vertrag verpflichtend vereinbart. ☒

1027 Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen

Nach wiederholter fehlerhafter Authentisierung muss der Zugang gesperrt werden. Ein Prozess zur Rücksetzung bzw. Entsperrung von gesperrten Zugangskennungen ist einzurichten, zu beschreiben und anzuwenden. Benutzerkennungen, welche über einen längeren Zeitraum nicht genutzt werden, müssen automatisch gesperrt bzw. auf inaktiv gesetzt werden.

Die Erfüllung der Anforderung 1027 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.4.2.2 Organisatorische Maßnahmen

1028 **Einfache Authentisierung (per Benutzername/Passwort) bei niedrigem bis mittlerem Schutzniveau**

Es gibt eine Richtlinie zur Vergabe und Nutzung von Passwörtern. Jeder Berechtigte verfügt über ein eigenes nur ihm bekanntes Passwort. Passworte müssen angemessenen Mindestregeln entsprechen wie z.B. einer minimalen Passwortlänge und Komplexität. Passworte müssen in regelmäßigen Abständen geändert werden. Erstpassworte müssen umgehend geändert werden. Die Umsetzung der Anforderungen an Passwortlänge, Passwortkomplexität und Gültigkeit ist soweit möglich durch technische Einstellungen sicherzustellen.

- Ein Passwort besteht aus mindestens 8 Zeichen.
- Das Passwort setzt sich aus einem Zeichenmix zusammen. Die verfügbaren Zeichen werden in vier Kategorien unterteilt:
  - Kleine Buchstaben z.B. abcdefgh...
  - Große Buchstaben z.B. ABCDEFGH...
  - Ziffern z.B. 123456...
  - Sonderzeichen z.B. !"§$%...
  - Der Zeichenmix muss aus mindestens drei der oben genannten Kategorien bestehen.
- Für das Passwort dürfen keine leicht zu erratenden Begriffe und keine Trivialpasswörter verwendet werden.
- Ein Passwort ist in regelmäßigen Abständen, mindestens jedoch jährlich zu ändern
- Bei Änderung darf nicht eines der letzten 4 verwendeten Passworte wieder verwendet werden
- Das Passwort darf bei der Eingabe nicht im Klartext auf dem Bildschirm sichtbar wird.
- Das Erstpasswort muss auf sicherem Wege zum Nutzer kommen und/oder dieser mindestens sofort nach erstmaliger Anmeldung aufgefordert werden, dieses zu ändern

Passwörter werden ausschließlich verschlüsselt gespeichert.

Die Erfüllung der Anforderung 1028 wird für diesen Vertrag verpflichtend vereinbart. ☒

1029 **Festlegung befugter Personen**

Für die Server existiert eine Benutzerverwaltung, in welcher Benutzern Authentifizierungsmöglichkeiten zugewiesen werden. Der Kreis der Personen, die befugt Zugang zu DV-Anlagen auf oder mit denen Daten verarbeitet und/oder gespeichert werden (können), ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum zu beschränken. Zugänge für temporär beschäftigte Personen (Berater, Praktikanten, Auszubildende) müssen individuell vergeben werden. Wieder verwendbare Kennungen (z.B. Berater1, Praktikant1, etc.) dürfen nicht vergeben werden.

Die Erfüllung der Anforderung 1029 wird für diesen Vertrag verpflichtend vereinbart. ☒

1030 Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen ist einzurichten, zu beschreiben und zwingend anzuwenden. Dieser beinhaltet mindestens einen Beantragungs- und Genehmigungsprozess sowie den Prozess zur Rücknahme von Authentifizierungsmedien und Zugangsberechtigungen.

Die Vergabe von Zugangsberechtigungen darf immer nur für diejenigen DV- Anlagen(-typen) erfolgen, zu welchen der Zugang im Rahmen der Aufgabenwahrnehmung notwendig ist ("Prinzip der minimalen Berechtigung"). Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu DV-Anlagen sind grundsätzlich personengebunden zu vergeben und an ein persönliches Credential (z.B. Passwort, Token, Chipkarte) zu knüpfen (Benutzerkennung). Authentifizierungsmedien und/oder Benutzerkennung/Passwort-Kombination dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür zu sensibilisieren.

Regelungen und Verfahren zum Sperren und datenschutzgerechten Löschen von Zugangskennungen müssen beschrieben werden. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Authentifizierungsmedien und Zugangsberechtigungen zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV-Anlagen, unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration).

Die Erfüllung der Anforderung 1030 wird für diesen Vertrag verpflichtend vereinbart. ☒

1031 Persönliche Zuordnung von Authentifizierungsmedien und Zugangskennungen

Authentifizierungsmedien sowie Zugangskennungen für den Zugang zu Anlagen und Systemen des Auftraggebers sind grundsätzlich personengebunden und an ein persönliches Passwort geknüpft (Benutzerkennung). Authentifizierungsmedien und/oder Zugangskennung/Passwort-Kombination dürfen nicht an Dritte weitergegeben werden.

Die Erfüllung der Anforderung 1031 wird für diesen Vertrag verpflichtend vereinbart. ☒

1032 Verhaltensweise

Der Mitarbeiter oder Erfüllungsgehilfe des Auftragnehmers/Dienstleisters ist verpflichtet, die Regelungen und Vorgaben der technischen und organisatorischen Zugangskontrolle zu befolgen und stellt zudem sicher, dass nicht durch falsches Verhalten Unberechtigten der Zugang zu DV-Anlagen des Auftraggebers ermöglicht wird.

Die Erfüllung der Anforderung 1032 wird für diesen Vertrag verpflichtend vereinbart. ☒

1033 Sicherheitsmanagement

Neue Schwachstellen in den IT-Systemen werden nach Bekanntwerden gemeldet, analysiert und ggf. behoben, um das Eindringen seitens unbefugter Dritter in die IT-Systeme zu verhindern. Es gibt definierte und erprobte/wirksame Verfahren im Fall eines (erfolgten) externen Angriffs auf relevante Daten und Systeme im Rahmen der OTC. Für die CWA existiert ein Life-Cyclemanagement. IT-Systeme

werden auf die Wirksamkeit (Effektivität) eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter mindestens jährlich durch Penetrationstests getestet.

Die Erfüllung der Anforderung 1033 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.4.3 Zugriffskontrolle

Die Anforderungen der Zugriffskontrolle sind darauf ausgerichtet, dass nur durch Berechtigte auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass die Daten nicht durch Unbefugte manipuliert oder gelesen werden können.

#### 1.2.4.3.1 Technische Maßnahmen

1034 Zugriffskontrolle technische Maßnahmen

Zur Sicherstellung der Zugriffskontrolle werden eine oder mehrere der folgenden technischen Maßnahmen ergriffen:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
  - Type Enforcement (TE)
  - Multi-Level Security (MLS)
- Role Based Access Control (RBAC)
- Attribute-based access control (ABAC)
- Context-Based Access Control (CBAC)
- Media Access Control

Zudem liegt eine eindeutige Zuordnung zwischen jedem Datenträger (Laufwerk etc.) und Berechtigten vor (insb. bei Gruppenlaufwerken).

Die Erfüllung der Anforderung 1034 wird für diesen Vertrag verpflichtend vereinbart. ☒

1035 Protokollierung und Auswertung der Programm- und Dateibenutzung

Die Programm- und Dateibenutzung wird protokolliert und stichprobenartig ausgewertet. Für den Fall, dass sog. „Superuser" Accounts eingesetzt werden, erfolgt ein Monitoring sowie eine regelmäßige Kontrolle von Aktivitäten, die mithilfe dieser Benutzerkonten durchgeführt werden.

Die Erfüllung der Anforderung 1035 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.4.3.2 Organisatorische Maßnahmen

1036 Erstellen eines Berechtigungskonzepts

Ein Berechtigungskonzept (Benutzer- und Administrationsberechtigungen) gewährleistet, dass der Zugriff auf Daten des Systems nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung gemäß interner Aufgabenverteilung und Funktionstrennung des Benutzers erforderlich ist. Es wird verbindlich geregelt, wie Berechtigungen beantragt, freigegeben, umgesetzt und wieder entzogen werden. Dazu werden die folgenden Maßnahmen ergriffen:

- Für jedes eingesetzte (Datenbank-)system sind im Berechtigungssystem die Rechte an Datenbanktransaktionen festgehalten.
- Im Rahmen dieses Berechtigungsmanagements ist manipulationssicher nachweisbar, wer wann welche Berechtigungen innehatte.
- Es bestehen differenzierte Berechtigungen (z. B. für Lesen, Löschen, Ändern).
- Es bestehen differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem.
- Es besteht eine funktionelle/personelle Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (techn.).
- Es existiert eine Benutzerverwaltung, über die Berechtigungen verwaltet werden.
- Es liegt ein Konzept der Laufwerksnutzung und -zuordnung vor.
- Die Wiederherstellung von Daten aus Backups ist in einem verbindlichen Verfahren geregelt (wer darf wann auf wessen Anforderung Backup-Daten einspielen?).

Die Erfüllung der Anforderung 1036 wird für diesen Vertrag verpflichtend vereinbart. ☒

1037 Umsetzung von Zugriffsbeschränkungen

Mit jeder Zugangsberechtigung muss eine Zugriffsberechtigung verknüpft sein, beispielsweise durch die Verknüpfung mit einer oder mehrere im Berechtigungskonzept definierten Rollen. Jeder Zugangsberechtigte darf nur mit den Anwendungen und innerhalb dieser Anwendungen nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind.

Soweit Datenbestände mehrerer Auftraggeber in einer Datenbank gespeichert oder mit einer Datenverarbeitungsanlage verarbeitet werden, sind logische Zugriffseinschränkungen vorzusehen, die ausschließlich auf die Datenverarbeitung für den jeweiligen Auftraggeber ausgerichtet sind (Mandantenfähigkeit). Zudem ist die Datenverarbeitung selbst soweit einzuschränken, dass ausschließlich die minimal erforderlichen Funktionen für die Verarbeitung der personenbezogenen Daten verwendet werden können.

Es werden in den Datenverarbeitungsanlagen eindeutige Merkmale eingebaut, die es der zugreifenden Person ermöglicht, zu erkennen, dass es sich um eine authentische Datenverarbeitungsanlage handelt. Zudem muss sich auch der Zugriffsberechtigte gegenüber der Datenverarbeitungsanlage anhand von nachprüfbaren eindeutigen Merkmalen identifizieren und authentisieren lassen, z.B. mittels Ausweislesern an den Terminals.

Die Erfüllung der Anforderung 1037 wird für diesen Vertrag verpflichtend vereinbart. ☒

1038 **Vergabe minimaler Berechtigungen**

Der Umfang der Berechtigungen, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung notwendige Minimum zu beschränken. Soweit bestimmte Funktionen ohne Verlust der Qualität der Datenverarbeitung zeitlich beschränkbar sind, sind Zugriffe auf die personenbezogenen Daten und Berechtigungen zeitlich zu begrenzen.

Die Erfüllung der Anforderung 1038 wird für diesen Vertrag verpflichtend vereinbart. ☒

1039 **Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen**

Ein Prozess zur Beantragung, Genehmigung, Vergabe und Rücknahme von Zugriffsberechtigungen und deren Prüfung ist einzurichten, zu beschreiben und zwingend anzuwenden. Regelungen und Verfahren zum Erteilen/Entziehen von Berechtigungen bzw. der Zuweisung von Benutzerrollen sind zu beschreiben. Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Berechtigungen sind an eine persönliche Benutzerkennung und an einen Account zu knüpfen. Dies schließt den Einsatz von mehreren Personen genutzten Gruppenkennungen/-passwörtern aus.

Bei der Vergabe der Berechtigungen bzw. Zuweisung von Benutzerrollen dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-know-Prinzip"). Dabei ist sicherzustellen, dass die im System abgebildete Funktionstrennung nicht durch kumulierte Berechtigungen aufgehoben wird.

Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, sind sämtliche Zugriffsrechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr benötigten DV- Anlagen und Speicherbereichen unverzüglich zu entziehen. Hierbei ist sicherzustellen, dass alle beteiligten Stellen über den Weggang bzw. Funktionsänderungen von Mitarbeitern informiert sind (insb. IT-/Berechtigungsadministration). Die Dokumentationen sind 3 Monate aufzubewahren.

Die Erfüllung der Anforderung 1039 wird für diesen Vertrag verpflichtend vereinbart. ☒

1040 **Trennung zwischen Test- und Produktionsumgebung**

Es erfolgt bei einer evtl. Programmentwicklung eine Funktionstrennung zwischen Test- und Produktionsumgebung.

Die Erfüllung der Anforderung 1040 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.4.4 Weitergabekontrolle

Hierbei handelt es sich um Maßnahmen, die verhindern, dass Daten unbefugt weitergegeben werden. Insbesondere soll verhindert werden, dass Daten bei einer elektronischen Übertragung bzw. Transport nicht unbefugt verarbeitet werden können.

#### 1.2.4.4.1 Technische Maßnahmen

1041 Legitimationsprüfung

Es erfolgt eine Legitimationsprüfung der Berechtigten.

Die Erfüllung der Anforderung 1041 wird für diesen Vertrag verpflichtend vereinbart. ☒

1042 Versendungsarten

Folgende Versendungsarten stehen für die Versendung personenbezogener Daten zur Verfügung:

- Datenverschlüsselung
- SSH
- VPN (Verschlüsselung)
- Sicheres Web-Formular / -Portal
- Gesicherte/Verschlüsselte Datenleitung

Die Erfüllung der Anforderung 1042 wird für diesen Vertrag verpflichtend vereinbart. ☒

1043 Ausschluss Datenträgertransport

Der Datenträgertransport ist ausgeschlossen.

Die Erfüllung der Anforderung 1043 wird für diesen Vertrag verpflichtend vereinbart. ☒

#### 1.2.4.4.2 Organisatorische Maßnahmen

1044 Festlegung empfangs-/weitergabeberechtigter Instanzen/Personen

Es ist gemeinsam mit dem Auftraggeber festzulegen welche Stellen/Personen an wen, welche Daten übermitteln dürfen und auf welchem Übertragungsweg dies geschehen soll.

Die Erfüllung der Anforderung 1044 wird für diesen Vertrag verpflichtend vereinbart. ☒

1045 Rechtmäßigkeit der Weitergabe ins Ausland

Die Erhebung, bzw. die Verarbeitung von Daten im Ausland ist grundsätzlich nur mit vorheriger Genehmigung des Auftraggebers möglich.

Die Erfüllung der Anforderung 1045 wird für diesen Vertrag verpflichtend vereinbart. ☒

1046 Übertragung zu externen Systemen

Werden personenbezogene Daten zu externen Systemen übertragen, ist eine Verschlüsselung zwingend erforderlich.

Die Erfüllung der Anforderung 1046 wird für diesen Vertrag verpflichtend vereinbart. ☒

1047 Implementation von Sicherheitsgateways an den Netzübergabepunkten

Die IT-/NT-Systeme, auf denen personenbezogene Daten verarbeitet werden, sind durch dem aktuellen Stand der Technik entsprechende Maßnahmen (i.d.R. Firewalls) vor unerwünschten Zugriffen oder Datenströme sowohl aus dem eigenen wie auch aus anderen Netzen zu schützen. Unabhängig davon, ob es sich um Netzwerk-/Hardware-Firewalls oder ergänzend dazu um hostbasierte Firewalls handelt, müssen diese dauerhaft aktiviert sein. Jedwede Deaktivierung oder Umgehung der Funktionen durch den Anwender muss dabei wirksam ausgeschlossen werden. Das Regelwerk muss so aufgesetzt werden, dass alle Kommunikationsbeziehungen außer den notwendigen automatisch geblockt werden.

Die Erfüllung der Anforderung 1047 wird für diesen Vertrag verpflichtend vereinbart. ☒

1048 Härtung der Backendsysteme

Die Backendsysteme müssen nach dem Stand der Technik gehärtet werden, damit sich ein Angreifer nicht aufgrund von Schwachstellen unbefugt Zugriff auf die Systeme und Daten verschaffen kann.

Die Erfüllung der Anforderung 1048 wird für diesen Vertrag verpflichtend vereinbart. ☒

1049 Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder

Alle Schnittstellen zu anderen IV-Verfahren sind zu dokumentieren. Diese Dokumentation muss mindestens die folgenden Informationen beinhalten:

- alle personenbezogenen Datenfelder
- Richtung der Übermittlung (Import/ Export)
- der jeweilige Verwendungszweck für die Übermittlung
- das IV-Verfahren/ die Schnittstelle, an das die Daten exportiert werden
- Art der Authentisierung der Schnittstelle
- Schutz der Übertragung (z.B. Verschlüsselung)

Insbesondere sind auch Import- und Exportschnittstellen aus bzw. in Dateien zu beschreiben, und wie deren Verwendung technisch oder organisatorisch geschützt wird. Auch Datenmigrationen sind entsprechend als Schnittstelle zu beschreiben.

Die Erfüllung der Anforderung 1049 wird für diesen Vertrag verpflichtend vereinbart. ☒

1050 Gesicherte Speicherung auf mobilen Datenträgern

Die Speicherung auf mobilen Datenträgern ist aufgrund des hohen Verlustrisikos zu vermeiden. Sollte eine Speicherung dennoch unumgänglich sein, so ist die Nutzung zu regeln und die Verschlüsselung der Daten auf dem Medium muss technisch sichergestellt sein. Nicht mehr benötigte Daten sind umgehend datenschutzgerecht zu löschen.

Die verwendete Hardware ist zudem gegen Verlust/Diebstahl zu schützen.

Die Erfüllung der Anforderung 1050 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1051 Einführung eines Prozesses zur Datenträgerverwaltungen

Es muss eine qualifizierte Datenträgerverwaltung existieren. Die Verwaltung der Datenträger muss dokumentieren, wie viele Datenträger mit personenbezogenen Daten für welche Aufgaben und Verarbeitungen erstellt wurden und wo diese bis zur Vernichtung gelagert werden. Über den Bestand der Datenträger ist regelmäßig eine Bestandskontrolle durchzuführen. Eine Lagerung der erstellten Datenträger in einem kontrollierten Sicherheitsbereich ist bei personenbezogenen Daten obligatorisch. Darüber hinaus wird die Anfertigung von Kopien von Datenträgern dokumentiert und für einen Zeitraum von 3 Monaten ab Beendigung des Auftrages oder der Tätigkeit aufbewahrt.

Die Erfüllung der Anforderung 1051 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1052 Prozess zur Sammlung und Entsorgung

Ein Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern und Informationsträgern in Papierform ist einzurichten und zu beschreiben. Dabei werden Regelungen und Verfahren zur sicheren Sammlung und internen Weitergabe sowie zu Lagerung, Transport und Vernichtung unter Berücksichtigung medientypischer Eigenarten in einer Organisationsrichtlinie/Verfahrensanweisung beschrieben. Das datenschutzgerechte Vernichten bzw. Löschen ist arbeitsplatz- und zeitnah durchzuführen, um ein Zwischenlagern der Datenträger weitgehend zu vermeiden. Dadurch wird auch der Personenkreis, der mit den Datenträgern umgeht, eingeschränkt und die Sicherheit erhöht. Alternative Entsorgungswege sind organisatorisch auszuschließen. Die Mitarbeiter sind hierfür regelmäßig zu sensibilisieren.

Die Erfüllung der Anforderung 1052 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1053 Einführung datenschutzgerechter Lösch- und Zerstörungsverfahren

Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor deren internen Wiederverwendung (z.B. Wechsel des Hauptnutzers) oder Weitergabe an externe Stellen datenschutzgerecht gelöscht werden. Die Formatierung ist als sicheres Löschverfahren ungeeignet. Es müssen andere sichere Lösch-/ Zerstörungsverfahren gewählt werden, die eine Rekonstruktion der Daten nur mit hohem Aufwand erlauben.

Die Erfüllung der Anforderung 1053 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1054 Führung von Löschprotokollen

Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit personenbezogenen Daten ist zu protokollieren. Die Protokolle sind mindestens 12 Monate revisionssicher zu archivieren.

Die Erfüllung der Anforderung 1054 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1055 Weitergabe von Datenträgern

Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor der Weitergabe an externe Stellen stets datenschutzgerecht gelöscht werden.

Die Erfüllung der Anforderung 1055 wird für diesen Vertrag verpflichtend vereinbart. ☒

1056 **Verbot der Vervielfältigung**

**Jegliche Art der Vervielfältigung (elektronisch und/oder analog) von Daten, Datenträgern oder Unterlagen des Auftraggebers ist unzulässig, sofern dies nicht explizit Bestandteil der Auftragsausführung ist. In diesem Fall dürfen Kopien ausschließlich für die vom Auftraggeber festgelegten Zwecke sowie in dem hierfür erforderlichen Umfang angefertigt werden. Als Vervielfältigen gilt auch der elektronische Versand z.B. via E-Mail.**

**Die Erfüllung der Anforderung 1056 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1057 **Wechseldatenträger**

**Sowohl das Einbinden externer (Wechsel-)datenträger (USB, Speicherkarten, CD/DVD etc.) in DV-Anlagen des Auftraggebers als auch das Kopieren von Daten des Auftraggebers auf externe (Wechsel-)datenträger ist untersagt, sofern dies nicht explizit Bestandteil der Auftragsausführung ist und durch den Leiter der zuständigen Stelle des Auftraggebers genehmigt wurde.**

**Die Erfüllung der Anforderung 1057 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1058 **Festlegung empfangs-/weitergabeberechtigter Instanzen/Personen**

Die Server verbinden sich nicht mit Profilen sozialer Medien.

Die Erfüllung der Anforderung 1058 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.4.5 Trennungskontrolle

Hierbei handelt es sich um Maßnahmen, welche gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische oder physikalische Trennung der Daten erreicht werden.

#### 1.2.4.5.1 Technische Maßnahmen

1059 **Sparsamkeit bei der Datenerhebung**

Es dürfen nur solche Daten erhoben, gespeichert oder verarbeitet werden, die unmittelbar dem eigentlichen Zweck dienen, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses zwingend notwendig sind. Dieser Zweck darf sich in keinem nachgelagerten Schritt der Verarbeitung, auch nicht nach einer Übermittlung ändern.

Die Erfüllung der Anforderung 1059 wird für diesen Vertrag verpflichtend vereinbart. ☒

1060 **Getrennte Verarbeitung**

Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung (Speicherung, Veränderung, Löschung und Übertragung etc.) und/oder Lagerung von Daten und/oder Datenträgern mit unterschiedlichen Vertragszwecken sind zu dokumentieren und anzuwenden.

Die Erfüllung der Anforderung 1060 wird für diesen Vertrag verpflichtend vereinbart. ☒

1061 Getrennte Verarbeitung

Die Testergebnisse werden nicht auf dem Verification Server, sondern nur auf dem Testresult Server gespeichert. Die Daten werden auf dem Verification Server, Testresult Server und Portal Server getrennt voneinander verarbeitet.

Die Erfüllung der Anforderung 1061 wird für diesen Vertrag verpflichtend vereinbart. ☒

1062 Getrennte Verarbeitung

OTC Infrastruktur sowie der Verification Server, Testresult Server und der CWA-Server, sowie die zugeordneten Datenbankinstanzen werden von unterschiedlichen Betriebsteams und in verschiedenen Cloud Subscriptions betrieben.

Die Erfüllung der Anforderung 1062 wird für diesen Vertrag verpflichtend vereinbart. ☒

1063 Getrennte Verarbeitung

Es existiert eine Trennung zwischen Test- und Produktivdaten.

Die Erfüllung der Anforderung 1063 wird für diesen Vertrag verpflichtend vereinbart. ☒

#### 1.2.4.5.2 Organisatorische Maßnahmen

1064 Getrennte Verarbeitung

Die Daten verschiedener Mandanten werden von unterschiedlichen Mitarbeitern beim Auftragnehmer verarbeitet, so dass die Gefahr der Weitergabe von personenbezogenen Daten unterbunden wird.

Die Erfüllung der Anforderung 1064 wird für diesen Vertrag verpflichtend vereinbart. ☒

1065 Getrennte Verarbeitung

Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung der Daten anderer Mandanten Rechnung trägt.

Die Erfüllung der Anforderung 1065 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.5 Integrität

#### 1.2.5.1 Eingabekontrolle

Diese Maßnahmen sollen dafür sorgen, dass man nachträglich feststellen kann, ob und wenn ja von wem personenbezogene Daten in informationstechnischen Systemen eingegeben, verändert oder entfernt worden sind.

#### 1.2.5.1.1 Technische Maßnahmen

1066 Protokollierung Administratorentätigkeiten

Es erfolgt eine Protokollierung der Administratorentätigkeiten insbesondere von Anlegen von Benutzern, sowie des Änderns von Benutzerrechten.

Die Erfüllung der Anforderung 1066 wird für diesen Vertrag verpflichtend vereinbart. ☒

#### 1.2.5.1.2 Organisatorische Maßnahmen

1067 Übersicht IT-Systeme

Es existiert eine Übersicht, welche IT-Systeme die Erfassung personenbezogener Daten ermöglichen.

Die Erfüllung der Anforderung 1067 wird für diesen Vertrag verpflichtend vereinbart. ☒

1068 Benutzerberechtigungen

Es sind Benutzerberechtigungen festgelegt und diese sind wie folgt differenziert:

- Lesen
- Ändern
- Löschen

Die Erfüllung der Anforderung 1068 wird für diesen Vertrag verpflichtend vereinbart. ☒

1069 Löschkonzept

Es existiert ein Löschkonzept. In welchem festgelegt ist, wer welche Daten zu welchen Zeitpunkten auf welche Weise löschen darf bzw. muss.

Die Erfüllung der Anforderung 1069 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.5.2 Auftragskontrolle

Hierunter fallen Maßnahmen, welche gewährleisten, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden.

**Organisatorische Maßnahmen**

1070 Auswahl des Auftragsverarbeiters

Auftragsverarbeiter werden ausschließlich nach einer Überprüfung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. Es werden nur Auftragsverarbeiter ausgewählt, die einen qualifizierten Datenschutzbeauftragten benannt haben und bei denen der Datenschutzbeauftragte über angemessene Ressourcen zur Wahrnehmung seiner Aufgabe verfügt.

Die Erfüllung der Anforderung 1070 wird für diesen Vertrag verpflichtend vereinbart. ☒

1071 Auftragsverarbeitungsvertrag

Es existiert ein Vertrag zur Auftragsverarbeitung, der den Anforderungen der DSGVO genügt.

Die Erfüllung der Anforderung 1071 wird für diesen Vertrag verpflichtend vereinbart. ☒

1072 Geheimhaltungsverpflichtungen

Im Vertrag zur Auftragsverarbeitung wird jeder Auftragsverarbeiter vertraglich verpflichtet, dass die Geheimhaltungsverpflichtungen auch an die Auftragsverarbeiter weitergegeben werden.

Die Erfüllung der Anforderung 1072 wird für diesen Vertrag verpflichtend vereinbart. ☒

1073 Verzeichnis der Verarbeitungstätigkeiten

Es wurde vereinbart, dass der Auftragsverarbeiter ein Verzeichnis der Auftrags-Verarbeitungstätigkeiten führt.

Die Erfüllung der Anforderung 1073 wird für diesen Vertrag verpflichtend vereinbart. ☒

1074 Aufgabenteilung

Die Aufgabenteilung zwischen Auftraggeber und Auftragnehmer einerseits, sowie Auftragnehmer und Subunternehmer anderseits, sind vor Aufnahme der Tätigkeit schriftlich festzulegen, soweit sich dies nicht bereits aus den abgeschlossenen Verträgen ergibt.

Die Erfüllung der Anforderung 1074 wird für diesen Vertrag verpflichtend vereinbart. ☒

1075 Weisungen

Die weisungsbefugten Personen auf Seite des Auftraggebers sind benannt und beim Auftragnehmer bekannt. Die zur Entgegennahme und Ausführung von Weisungen des Auftraggebers beim Auftragnehmer befugten Personen sind benannt. Alle Weisungen des Auftraggebers an den Auftragnehmer erfolgen schriftlich.

Die Erfüllung der Anforderung 1075 wird für diesen Vertrag verpflichtend vereinbart. ☒

1076 Regelungen/Beschränkungen der Auftragsausführung

Es dürfen nur die Arbeiten durchgeführt werden, die in der zu erstellenden Leistungsbeschreibung enthalten sind. Alle darüber hinaus gehenden Arbeitsschritte müssen vorher dezidiert mit der zuständigen Stelle auf Seiten des Auftraggebers abgesprochen und schriftlich freigegeben werden. Der Auftragnehmer stimmt den terminlichen Ablauf der Auftragsausführung vorab mit dem Auftraggeber ab.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. Der Auftragnehmer wird

diese unverzüglich beheben. Die meldepflichtigen Vorfälle sind spezifiziert und sowohl den eigenen Beschäftigten als auch allen vom Auftragnehmer eingesetzten Personen bekannt, inkl. Mitarbeitern von ggf. existierenden Unterauftragnehmern.

Die Erfüllung der Anforderung 1076 wird für diesen Vertrag verpflichtend vereinbart. ☒

1077 Unterauftragnehmer

Soweit der Auftraggeber einem Einsatz von Unterauftragnehmern (Subunternehmer/Dienstleister - siehe Begriffsbestimmung) zugestimmt hat, sind die Unterauftragnehmer sorgfältig auszuwählen, Art und Umfang der zu erbringenden Leistungen im Rahmen eines datenschutzrechtlichen Unterauftragsverhältnisses zu regeln und die Ausführung der Tätigkeiten und Leistungen im Sinne der vertraglichen Regelungen mit dem Auftraggeber zu überprüfen. Die Ergebnisse dieser Überprüfungen sind schriftlich zu dokumentieren und dem Auftragnehmer auf Verlangen vorzulegen. Die unmittelbaren Kontrollrechte des Auftraggebers bleiben hiervon unberührt.

Wenn der Auftragnehmer einen Unterauftragnehmer zur Erfüllung der Auftragsverarbeitung einsetzt, ist gewährleistet, dass mit Unterauftragnehmern Auftragsverarbeitungsverträge abgeschlossen werden und die Verträge des Auftragnehmers mit dem Unterauftragnehmern die Anforderungen des Auftraggebers an den Auftragnehmer widerspiegeln. Mit Unterauftragnehmern werden Datenschutzvereinbarungen abgeschlossen, die Geheimhaltungsvereinbarungen enthalten, die auch für den Auftragnehmer gelten.

Die Erfüllung der Anforderung 1077 wird für diesen Vertrag verpflichtend vereinbart. ☒

1078 Dokumentation

Es existiert eine Dokumentation, welche die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung erforderlichen Arbeitsschritte gewährleistet.

Die Erfüllung der Anforderung 1078 wird für diesen Vertrag verpflichtend vereinbart. ☒

1079 Übergabe bei Beendigung des Auftragsverhältnisses

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Daten, Unterlagen und Betriebsmittel erfolgen.

Die Erfüllung der Anforderung 1079 wird für diesen Vertrag verpflichtend vereinbart. ☒

1080 Konfigurationsänderungen

Konfigurationsänderungen an Anlagen oder Systemen des Auftraggebers sind unzulässig, wenn dies nicht explizit schriftlich als Bestandteil des Auftrags vereinbart wurde. In diesem Fall ist dies vorab mit der verantwortlichen Stelle abzustimmen und durch eine geeignete Dokumentation die Nachvollziehbarkeit der durchgeführten Änderungen zu gewährleisten.

Die Erfüllung der Anforderung 1080 wird für diesen Vertrag verpflichtend vereinbart. ☒

1081 **Audits**

**Bei den Auftragsverarbeitern erfolgen jährlich Audits. Es werden automatisch Nachweise bzgl. der Sicherheit der Verarbeitung (Art. 32 DS-GVO) bei Dienstleistern angefordert.**

**Die Erfüllung der Anforderung 1081 wird für diesen Vertrag verpflichtend vereinbart. ☒**

### 1.2.6 Verfügbarkeit

**Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten gegen zufällige Zerstörung oder zufälligen Verlust geschützt sind.**

#### 1.2.6.1 Technische Maßnahmen

1082 **Sicherung der Serverräume**

**Folgende Maßnahmen werden zur Sicherung der Serverräume ergriffen:**

- **Es existiert ein Brandschutz, insbesondere Feuer- und Rauchmeldeanlagen.**
- **Im Serverraum ist ein Feuerlöscher verfügbar.**
- **Der Serverraum ist klimatisiert.**
- **Im Serverraum erfolgt eine Überwachung von Temperatur und Feuchtigkeit.**
- **Jeder Server ist mit einer unterbrechungsfreien Stromversorgung (USV) verbunden.**
- **Es werden Hardware-RAID-Systeme eingesetzt.**
- **Im Serverraum sind Schutzsteckdosenleisten im Einsatz.**
- **Es existiert eine Alarmanlage, welche ein unbefugtes Eindringen in den Serverraum meldet.**

**Die Erfüllung der Anforderung 1082 wird für diesen Vertrag verpflichtend vereinbart. ☒**

1083 **Datenschutztresor**

**Es ist ein Datenschutztresor (entsprechend S60DIS, S120DIS oder anderer geeigneter Normen mit Quelldichtung etc.) vorhanden.**

**Die Erfüllung der Anforderung 1083 wird für diesen Vertrag verpflichtend vereinbart. ☒**

1084 **Vernichtung Datenträger**

**Alte oder unbrauchbare Datenträger werden datenschutzrechtlich ordnungsgemäß vernichtet.**

**Die Erfüllung der Anforderung 1084 wird für diesen Vertrag verpflichtend vereinbart. ☒**

### 1.2.6.2 Organisatorische Maßnahmen

1085 **Backup-Konzept**

**Es existiert ein angemessenes Backup- und Recovery-Konzept. Um die Verfügbarkeit der Daten auch im Notfall sicherzustellen, müssen die Daten regelmäßig gesichert werden. Zu diesem Zweck muss ein Backup-Konzept erstellt werden, dass einen befugten Mitarbeiter in die Lage versetzt, sämtliche Mittel für die Wiederherstellung der Daten so zu nutzen, dass die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung stehen. Hier wird unter anderem geregelt, dass Backups regelmäßig auf Datenvollständigkeit kontrolliert werden, regelmäßig überprüft wird, ob eine Rekonstruktion der gesicherten Daten tatsächlich möglich ist, welche Daten für welchen Zeitraum gesichert werden müssen, die anschließende Löschung der Daten, das „Haltbarkeitsdatum" der Sicherungsbänder und die katastrophensichere Aufbewahrung der Datenträger.**

**Die Erfüllung der Anforderung 1085 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1086 **Notfallplan**

**Es existiert ein Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (BCM-Konzept). Der Auftraggeber ist über jede Störung (z.B. vorsätzlicher Angriff intern/extern) und Außerbetriebnahme der Datenverarbeitung schnellstmöglich zu informieren. Liegen Anzeichen für eine Störung vor, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Notfallplan zu erstellen, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen, insb. auch auf Seite des Auftraggebers, über den Vorfall zu unterrichten sind.**

**Die Erfüllung der Anforderung 1086 wird für diesen Vertrag verpflichtend vereinbart.** ☒

1087 **Notfallhandbuch**

**Es existiert ein Notfallhandbuch mit Notfallplänen, Darstellung der Notfallorganisation – klare Regelung der Verantwortlichkeiten im Notfall.**

**Die Erfüllung der Anforderung 1087 wird für diesen Vertrag verpflichtend vereinbart.** ☒

### 1.2.7 Authentizität

1088 **Vortäuschen falscher Infektionsereignisse**

**Um Vortäuschen falscher Infektionsereignisse zu begegnen, wird von der Anwendung unmittelbar nach dem Scannen des QR-Codes der QR-Code auf dem Verifikationsserver gegen eine Registration Token eingetauscht und der QR-Code auf dem Server als verbraucht gekennzeichnet.**

**Die Erfüllung der Anforderung 1088 wird für diesen Vertrag verpflichtend vereinbart.** ☒

### 1.2.8 Resilienz/ Belastbarkeit/ Ausfallsicherheit/Wiederherstellbarkeit

**Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten bei Verlust oder Zerstörung schnell wiederhergestellt werden können.**

#### 1.2.8.1 Technische Maßnahmen

1089 **Netzwerk-Monitoring**

**Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet.**

**Die Erfüllung der Anforderung 1089 wird für diesen Vertrag verpflichtend vereinbart. ☒**

1090 **Server- und Client-Absicherung**

**Es gibt eine unterbrechungsfreie Stromversorgung. Es werden Hardware-RAID-Systeme eingesetzt. Es gibt Reserve-Clients (PC, Laptop, Tablet, Smartphone, ...), so dass bei einem Ausfall der Client ausgetauscht und die Arbeit schnellstmöglich wieder aufgenommen werden kann. Folgende Sicherheitssysteme schützen zudem Soft- und/oder Hardware vor Angriffen:**

- **Virenscanner**
- **Firewalls**
- **Spamfilter**
- **Verschlüsselungsprogramme**
- **Intrusion-Detection-System**
- **Intrusion-Prevention-System**

**Die Erfüllung der Anforderung 1090 wird für diesen Vertrag verpflichtend vereinbart. ☒**

#### 1.2.8.2 Organisatorische Maßnahmen

1091 **Ansprechpartner**

**Es wurde festgelegt, welche Person bei welcher Störung oder welchem Ausfall zu benachrichtigen ist.**

**Die Erfüllung der Anforderung 1091 wird für diesen Vertrag verpflichtend vereinbart. ☒**

### 1.2.9 Intervenierbarkeit

1092 Betroffenenrechte

**Durch die verarbeiteten Daten können die Benutzer nicht identifiziert werden. Daher können Ersuchen nach Art. 15 bis 20 DSGVO nicht beantwortet werden. Die Bereitstellung von Informationen, die die Identifizierung der Benutzer ermöglichen würde, findet nicht statt. Dies würde dem Ziel zuwiderlaufen, den Gesamtprozess so datensparsam wie möglich durchzuführen. Die Art. 15 bis 20 DSGVO sind daher nicht anwendbar (Art. 11 Abs.2 DSGVO).**

**Die Erfüllung der Anforderung 1092 wird für diesen Vertrag verpflichtend vereinbart. ☒**

1093 Betroffenenrechte

**Eine Überprüfung der automatisierten Entscheidungsfindung (Überprüfung der Empfehlungen im Kontaktfall) nach Art. 22 Abs. 3 DSGVO ist nicht notwendig, da durch die CWA und die angebundene IT-Infrastruktur keine rechtsverbindlichen Entscheidungen getroffen werden, sondern nur Empfehlungen ausgesprochen werden.**

**Die Erfüllung der Anforderung 1093 wird für diesen Vertrag verpflichtend vereinbart. ☒**

### 1.2.10 Transparenz

1094 Transparenz

**Durch die folgenden Maßnahmen wird eine größtmögliche Transparenz hergestellt:**

- **App und alle Komponenten sind quelloffen und auf Github dokumentiert**
- **öffentliche Diskussion unter anderem auf Github mit der technikinteressierten Öffentlichkeit und Beteiligung von Nichtregierungsorganisationen (NGO)**
- **Einbindung des in gesamten Entwicklungsprozess BfDI**
- **Datenschutzhinweise**
- **Erstellung des Verzeichnisses der Verarbeitungstätigkeiten für Auftragsverarbeiter**
- **Datenschutzkonzepte für alle Komponenten**
- **Datenschutzfolgenabschätzung**

**Die Erfüllung der Anforderung 1094 wird für diesen Vertrag verpflichtend vereinbart. ☒**

### 1.2.11 Zweckbindung / Nichtverkettung

### 1.2.11.1 Technische Maßnahmen

1095 **Keine zentrale Entität**

Das Vertrauen in die Server ist begrenzt. Die CWA wird auf der Grundlage einer Technologie mit einem dezentralisierten Ansatz entwickelt. Als Grundlage dienen die Protokolle DP-3T (Decentralized Privacy-Preserving Proximity Tracing) und TCN sowie die Spezifikationen für Privacy-Preserving Contact Tracing von Apple und Google. Die Begegnungsdaten der Benutzer verbleiben lokal auf dem Gerät und werden nicht geteilt.

Die Erfüllung der Anforderung 1095 wird für diesen Vertrag verpflichtend vereinbart. ☒

1096 **Kontrolle der Verarbeitungen**

Die Verwaltung des zentralen Servers folgt klar definierten Governance-Regeln und schließt alle erforderlichen Maßnahmen zur Gewährleistung seiner Sicherheit ein. Der Standort des zentralen Servers ist in Deutschland, so dass eine wirksame Aufsicht durch die zuständige Aufsichtsbehörde gewährleistet ist.

Die Erfüllung der Anforderung 1096 wird für diesen Vertrag verpflichtend vereinbart. ☒

1097 **Begegnungsdaten nur lokal**

Die Begegnungsdaten mit einer infizierten Person (exposures) verbleiben lokal auf dem Gerät und werden nicht geteilt (dezentrale Lösung). Auch Berechnungen, ob es durch den Kontakt zu einer infizierten Person zu einer Ansteckung gekommen sein kann, werden nur lokal auf dem Gerät durchgeführt.

Die Erfüllung der Anforderung 1097 wird für diesen Vertrag verpflichtend vereinbart. ☒

1098 **Löschung**

Alle personenbezogenen Daten werden sobald sie nicht mehr benötigt werden gelöscht.

Die Erfüllung der Anforderung 1098 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.2.11.2 Organisatorische Maßnahmen

1099 **Minimale Datenverarbeitung**

Es werden nur solche Daten verarbeitet, die unmittelbar dem eigentlichen Zweck dienen und die zur Erfüllung der Aufgabe oder Durchführung des Prozesses notwendig sind.

Die Erfüllung der Anforderung 1099 wird für diesen Vertrag verpflichtend vereinbart. ☒

1100 Auftragsverarbeitungsverträge

**Durch die Auftragsverarbeitungsverträge wird sichergestellt, dass auch die eingesetzten Vertragspartner die datenschutzrechtlichen Bestimmungen beachten.**

**Die Erfüllung der Anforderung 1100 wird für diesen Vertrag verpflichtend vereinbart. ☒**

## 1.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

### 1.3.1 Datenschutzmanagement

#### 1.3.1.1 Technische Maßnahmen

1101 Datenschutzmanagement

**Folgende Maßnahmen werden spezifisch ergriffen, um ein ordnungsgemäßes Datenschutzmanagement zu gewährleisten:**

- **Datenschutzmanagement-IT-System im Einsatz**
- **Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Beschäftigte und Externe nach Bedarf / Berechtigung**
  - **Intranet**
  - **Wiki**
  - **Github**

**Die Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird mindestens jährlich durchgeführt, sowie bei entsprechenden Anhaltspunkten auch in kürzeren Zyklen nach Bedarf.**

**Die Erfüllung der Anforderung 1101 wird für diesen Vertrag verpflichtend vereinbart. ☒**

#### 1.3.1.2 Organisatorische Maßnahmen

1102 Datenschutzmanagement

**Der Auftraggeber kommt seinen gesetzlichen Rechenschaftspflichten nach (Nachweis über Einhaltung datenschutzrechtlicher Vorgaben). Er hat einen internen Datenschutzbeauftragten benannt. Die Beschäftigten werden regelmäßig geschult und auf die Vertraulichkeit/Geheimhaltung verpflichtet, sowie bei Bedarf nach § 203 StGB.**

**Die Erfüllung der Anforderung 1102 wird für diesen Vertrag verpflichtend vereinbart. ☒**

1103 Privacy by Design und Privacy by Default

Datenschutz durch Technikgestaltung („Privacy by Design") und Datenschutz durch datenschutzfreundliche Voreinstellungen („Privacy by Default") werden bei allen Verarbeitungsprozessen umgesetzt.

Die Erfüllung der Anforderung 1103 wird für diesen Vertrag verpflichtend vereinbart. ☒

1104 Datenschutz-Folgenabschätzung

Bei Bedarf werden Datenschutz-Folgenabschätzungen durchgeführt.

Die Erfüllung der Anforderung 1104 wird für diesen Vertrag verpflichtend vereinbart. ☒

1105 Betroffenenrechte

Die Betroffenenrechte werden gewährleistet. Entsprechende Prozesse sind etabliert.

Die Erfüllung der Anforderung 1105 wird für diesen Vertrag verpflichtend vereinbart. ☒

1106 Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten wird ständig auf dem aktuellsten Stand gehalten.

Die Erfüllung der Anforderung 1106 wird für diesen Vertrag verpflichtend vereinbart. ☒

1107 Datenschutzvorfälle

Datenschutzvorfälle werden dokumentiert (Art. 33, 34 DSGVO).

Die Erfüllung der Anforderung 1107 wird für diesen Vertrag verpflichtend vereinbart. ☒

### 1.3.2 Organisationskontrolle

1108 Umsetzung von Schulungsmaßnahmen

Alle Personen, die mit personenbezogenen Daten umgehen oder sonst an der Auftragsdurchführung beteiligt sind (z.B. sofern vereinbart Wartungsunternehmen, Datenvernichter) sind nachweislich zu folgenden Themenkomplexen zu unterweisen:

- Grundsätze des Datenschutzes, einschließlich den technisch- organisatorischen Maßnahmen
- Pflicht zur Wahrung des Datengeheimnisses und Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse einschließlich Vorgängen des Auftraggebers
- Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Datenträgern und sonstigen Unterlagen
- Fernmeldegeheimnis (Verpflichtung nach §88 TKG)
- soweit erforderlich spezielle weitere Verschwiegenheitspflichten
- soweit erforderlich spezielle Hinweise, die sich aus der vertraglichen Vereinbarung und dem vorliegenden Katalog der Mindestvorgaben ergeben können.

Die Unterweisung hat durch geeignete und dem Auftrag angemessene Maßnahmen zu erfolgen und ist mindestens alle zwei Jahre, bei Bedarf (z.B. Änderung der Auftragsumstände oder gesetzlicher Bestimmungen) jedoch auch in kürzeren Abständen, zu wiederholen.

Die Erfüllung der Anforderung 1108 wird für diesen Vertrag verpflichtend vereinbart. ☒

1109 Funktionstrennung und -zuordnung

Im nächsten Schritt ist die Funktionstrennung festzulegen, zu dokumentieren und zu begründen, d.h. welche Funktionen nicht miteinander vereinbar sind, also nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür ergeben sich aus den Aufgaben selbst, den Anforderungen dieser Vereinbarung (insb. dem Katalog der Mindestvorgaben sowie ergänzender Standards) und aus gesetzlichen Bestimmungen. Grundsätzlich sind dabei operative Funktionen nicht mit kontrollierenden Funktionen vereinbar. Nach der Festlegung der einzuhaltenden Funktionstrennung erfolgt Zuordnung der Funktionen zu Personen.

Die Erfüllung der Anforderung 1109 wird für diesen Vertrag verpflichtend vereinbart. ☒

1110 Interne Audits

Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen müssen protokolliert (Benutzerkennung, Transaktionsdetails) werden.

Durch interne Auditierung beim Auftragnehmer wird sichergestellt, dass die Protokolle der Zugriffe auf die personenbezogenen Daten regelmäßig, spätestens jedoch alle zwei Monate, ausgewertet werden. Unregelmäßigkeiten werden dokumentiert, dem Auftraggeber unverzüglich schriftlich mitgeteilt und für einen Zeitraum von 3 Monaten ab Beendigung des Auftrages oder der Tätigkeit aufbewahrt.

Die Erfüllung der Anforderung 1110 wird für diesen Vertrag verpflichtend vereinbart. ☒

**Anhang 5 - Muster Leistungsnachweis**

**Corona Warn App - Leistungsnachweis Telekom - Mai 2020**

| Tätigkeit | Datum | Name Mitarbeiter/in | Beschreibung | Leistungsart / Rate Card | Stunden |
|---|---|---|---|---|---|
| 01 Projektmanagement | | | | | |
| | 04.05.2020 | Peter Müller | Projektssteuerung Corona Warn App | Projektmanagement 4 | 8 |
| | 04.05.2020 | Klaus Meier | Projektssteuerung Corona Warn App | Projektmanagement 5 | 8 |
| Projektmanagement Gesamt | | | | | 16 |
| 02 Entwicklung | 04.05.2020 | Klaus Klein | Entwicklung Verifikation | Entwickler 2 | 6 |
| | 04.05.2020 | Herta Meier | Entwicklung Verifikation | Entwickler 3 | 8 |
| | 05.05.2020 | Fritz Müller | Entwicklung Verifikation | Entwickler 3 | 9 |
| Entwicklung Gesamt | | | | | 23 |
| 03 ... | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Gesamt | | | | | |
| 04 ... | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Mai 2020 Gesamt | | | | | 39 |

# Leistungsschein

# Managed PaaS

28.05.2020

Managed PaaS

Red Hat Openshift Container Platform (OCP) 4.x

# Leistungsschein

# INHALT

# 1 LEISTUNGSBESCHREIBUNG

Der Auftragnehmer (Telekom) stellt dem Auftraggeber (Bundesministerium für Gesundheit (BMG)) für die Dauer des Vertrages eine Managed „Platform as a Service" (PaaS) zur Verfügung. Alle hierzu notwendigen Infrastrukturkomponenten und Softwarelizenzen (Red Hat Enterprise Linux und Red Hat OpenShift Container Platform) werden seitens des Auftragnehmers bereitgestellt.

Managed PaaS beinhaltet virtuelle Infrastruktur und virtuelle Netzwerkkomponenten und erlaubt das Erzeugen, das Management, sowie die Orchestrierung von Docker Containern.

Übergabepunkt für alle Leistungen ist der Übergabepunkt der Managed PaaS in das Internet, bzw. in das Netzwerk des Auftraggebers (z. B. VPN, MPLS).

## 1.1 Infrastrukturleistungen

Jede Plattform wird in einem dedizierten virtuellen Rechenzentrum (VPC = Virtual Private Cloud) betrieben.

Die Infrastrukturleistungen umfassen:

- Betrieb in einem Tier 3+ Rechenzentrum der T-Systems oder auf der Infrastruktur des im Preisblatt (siehe Anlagen) genannten Cloud-Providers.
- Volatiler Speicherplatz („Ephemeral")
- Anbindung der Plattform an den Übergabepunkt
- Netzwerk-Virtualisierung
- Virtuelle Netz- und Sicherheitsleistungen

Die Managed PaaS Plattformen werden in hochverfügbaren T-Systems Rechenzentren der Kategorie Tier 3+ betrieben oder auf der Infrastruktur eines Cloud-Provider (z.B. AWS). Die zugrundeliegende Plattform wird im Preisblatt (siehe Anlagen) festgelegt.

### 1.1.1 Domain und Zertifikate

Die Standard Domain für neue Plattformen lautet „aotp[xxx].mcs-paas.io" und eine Standard Route sieht wie folgt aus: http://[application]-[project].aotp[xxx].mcs-paas.io/.

Der Auftraggeber hat die Möglichkeit, Wildcard-Zertifikate für eine eigene Domain zu beschaffen und diese dann vom Auftragnehmer im Rahmen eines Change Requests entsprechend installieren zu lassen.

## 1.2 Plattformleistungen

Managed PaaS umfasst die gemanagten Dienste des Kernsystems mit den folgenden Leistungen:

- Dediziertes RH OCP Cluster (PaaS Instanz) in aktueller Version
- OpenShift-Web-Konsole (Self-Service Portal)
- Command-Line-Client (OC Client)
- Durch OpenShift (Red Hat) bereitgestellte Images
- Überwachung der Plattformverfügbarkeit
- Metrics Stack

Es gilt folgende Einschränkung:
Container die intern den User „root" voraussetzen oder mit erweiterten Rechten („Privileged Mode") laufen müssen, können ausschließlich durch das Betriebsteam des Auftragnehmers betrieben werden. Ein direkter Zugriff des Auftraggebers auf die virtuellen Maschinen der Plattform ist in jedem Fall ausgeschlossen bzw. verboten.

Folgende Leistungen können zusätzlich kostenpflichtig beauftragt werden:

- Unterstützung beim Aufbau eines automatisierten Build-Prozesses (CI/CD Pipeline)
- Erweitertes Reporting (unter vorherige Prüfung der technischen und kapazitären Machbarkeit)

### 1.2.1 Services der Open Telekom Cloud

Zusätzlich zur Infrastruktur für die Managed PaaS Plattform, besteht die Möglichkeit die folgenden Services der Open Telekom Cloud zu beziehen.

#### 1.2.1.1 Relational Database Service

Der Service ermöglicht dem Kunden die Nutzung einer relationalen Online-Datenbank. Dazu stehen operative Tools zur automatischen Bereitstellung, Wartung, Überwachung,Sicherung und Wiederherstellung der Datenbank zur Verfügung. Die Point-in-time-Recovery-Funktion ermöglicht die Datenbankwiderherstellung der letzten 35 Tage.Jede Datenbankversion steht als synchrone Primary/Standby.Zur Auswahl stehen folgende Datenbanken Versionen: PostgreSQL Version 9.5.x, 9.6.x, 10.x und 11.x (jeweils in der Community Version)

Die Nutzung des Relational Database Service erfolgt auf dem vorkonfektionierten Flavor 2 vCPU 8 GB RAM mit 50GB Ultra-High I/O Storage in der Entwicklungs-, Test, und Pre-Produktionsumgebung und 100GB Ultra-High I/O Storage in der Produktionsumgebung.

#### 1.2.1.2 Web Application Firewall

Die Web Application Firewall überwacht, filtert und blockiert auf HTTP und HTTPS basierenden Netzwerkverkehr zu einem Webserver. Dazu stehen Optionen zur Verwaltung, Konfiguration, Überwachung sowie zur Konfiguration verschiedener Schutzklassen und der Protokollierung der Aktivitäten zur Verfügung.

## 1.3 Abrechnungsmodell

Managed PaaS Plattformen werden grundsätzlich auf 3 Verfügbarkeitszonen verteilt mit einer Verfügbarkeit von 99.9% pro Jahr angeboten. Daraus ergibt sich eine minimale Grundausstattung von

- ✓ 3 x Master Server
- ✓ 3 x Infrastruktur Nodes
- ✓ 3 x Worker Nodes
- ✓ 3 x „Elasticsearch" Nodes (sofern EFK/EFG Stacks gewählt wurde)

Die Grundausstattung kann je nach konkretem Ressourcenbedarf erweitert werden.

Die Komponenten für das Monitoring (Prometheus/Grafana) gehören zur Grundausstattung und sind im monatlichen Grundpreis bereits enthalten.

Wird der EFK bzw. EFG Stack gebucht, werden zu einem monatlichen Grundpreis zusätzliche Server benötigt.

Über die Mindestabnahme hinaus, können per Change Request oder durch automatisches Skalieren der Plattform (siehe Kapitel Automatisches Skalieren) temporär weitere Worker Node Server („Worker") hinzukommen. Diese werden stündlich abgerechnet. .

## 1.4 Committed Edition

Als Basis dient die Committed Edition, welche gestaffelt nach der Höhe der monatlichen Mindestabnahme reduzierte Serverpreise bietet.

Aus dem Entgelt für die Plattformleistungen wird ein Gesamtbudget über die feste Laufzeit errechnet. Der Auftraggeber zahlt einen festen, monatlichen Abschlag auf das Gesamtbudget unabhängig von der tatsächlich verbrauchten Workload.

Wenn der Auftraggeber mehr als die vereinbarte Mindestabnahme verbraucht, wird die zusätzlich verbrauchte Workload stundengenau mit der nächsten Monatsrechnung zu dem für die gewählte Rabattstaffel festgelegten Serverpreis nachverrechnet. Bei Unterschreitung der gebuchten Abnahmemenge wird der Betrag in Rechnung gestellt, der sich auf Basis der gebuchten Abnahmemenge errechnet

Sofern auf Wunsch des Auftraggebers ein Wechsel der Worker Node Typen (MachineSet) durchgeführt werden soll, so werden die für den Zeitraum der Umstellung doppelt benötigte Ressourcen in Rechnung gestellt. Dabei ist zu beachten, dass das neue MachineSet mindestens die gleichen Ressourcen in Bezug auf CPU und RAM zur Verfügung stellt.

## 1.5 Automatisches Skalieren

Werden Ressourcen über die vereinbarte Mindestabnahme hinaus angefordert, skaliert die Plattform automatisch bis zu einer vom Auftraggeber festgelegten Maximalgröße. Der Serverpreis ändert sich hierdurch auch beim Erreichen der nächsten Rabattstaffelgrenze nicht. Es findet keine automatische Vertragsanpassung statt. Die Maximalgröße kann oberhalb der Mindestabnahmegröße jederzeit durch einen Change Request erhöht oder reduziert werden. Die Abrechnung der zusätzlichen Ressourcen erfolgt stundengenau.

Wird die von der Plattform angebotene Leistung über einen längeren Zeitraum zu einem erheblichen Teil nicht abgerufen, wird die maximale Plattformleistung automatisch und ohne Ankündigung reduziert. Dabei kommt es in der Regel dazu, dass Container innerhalb der Plattform verschoben, sprich evakuiert und neu deployed werden. Eine ggf. konfigurierte Deployment-Strategie vom Typ „Rolling" greift bei diesem Vorgang nicht. Hierdurch ggf. verursachte Einschränkungen der Verfügbarkeit der vom Auftraggeber betriebenen Applikationen gehen nicht zu Lasten der zugesicherten Plattformverfügbarkeit. Es obliegt der Verantwortung des Auftraggebers durch eine entsprechend robuste Applikationsarchitektur die Verfügbarkeit seiner Applikationen sicherzustellen.

Die durch den Hersteller definierten Limits bezüglich Autoscaling können unter folgendem Link eingesehen werden (hier z.B. für Version OCP 4.2):

https://docs.openshift.com/container-platform/4.2/machine_management/applying-autoscaling.html#cluster-autoscaler-about_applying-autoscaling

## 1.6 Desaster Recovery, Backup und Wiederherstellung

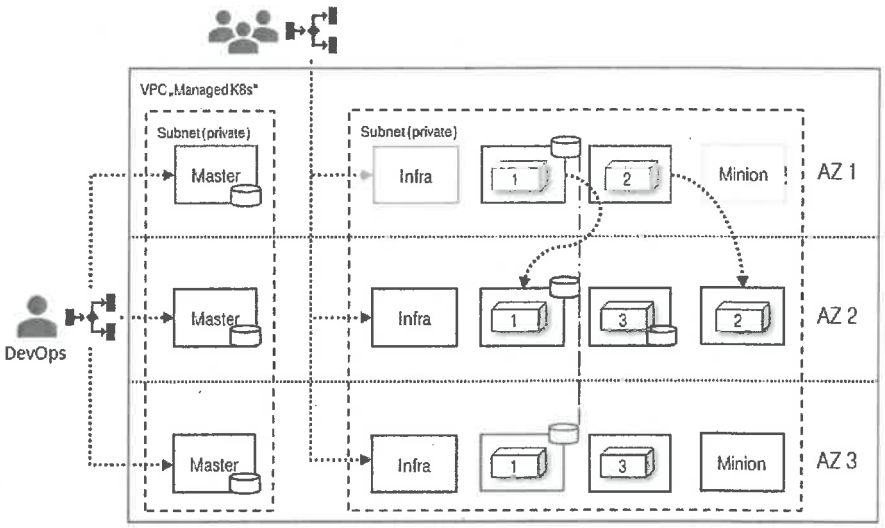
### 1.6.1 K-Fall Sicherheit

Managed PaaS Plattformen werden standardmäßig nicht K-Fall sicher, also nicht vollständig redundant in zwei voneinander unabhängigen Rechenzentren bereitgestellt. Diese Architektur kann auf Wunsch zusätzlich angeboten werden.

### 1.6.2 Hochverfügbarkeit

Managed PaaS Plattformen werden standardmäßig über die für die IaaS Plattform nutzbaren Verfügbarkeitszonen (AZ) verteilt, sofern das genutzte Rechenzentrum bzw. der gewählte Cloud Service Provider über drei Verfügbarkeitszonen verfügt.

Die Nutzung von drei Verfügbarkeitszonen kann bei entsprechender Applikationsarchitektur die Verfügbarkeit der Applikationen noch weiter erhöhen.




Voraussetzung für diese Architektur ist ein dritter Infra Node und die konsequente Nutzung von verteiltem Storage für Anwendungsdaten auf Persistenten Volumes. Zusätzlich müssen genügend Worker-Nodes (mindestens 3) und genügend Ressourcen (CPU, RAM) vorhanden sein, damit Pods, die durch den Verlust einer Verfügbarkeitszone verloren gegangen sind (siehe 1 und 2), durch den Self-Healing Mechanismus der Plattform automatisch in den verbliebenen Verfügbarkeitszonen re-deployed werden können. Für eine Zero-Downtime Architektur müssen sämtliche kritischen Pods in unterschiedlichen Verfügbarkeitszonen redundant deployed werden (siehe 1 und 3).

### 1.6.3 Desaster Recovery

Es wird standardmäßig kein vollständiges Backup der Managed PaaS Plattformen für ein Desaster Recovery angelegt. Das betrifft insbesondere die Konfiguration und den Zustand der Plattformen, die Konfiguration der vom Auftraggeber angelegten Projekte, die verwendeten und selbst erstellten Docker Images und die Nutzdaten auf den vom Auftraggeber

eingerichteten virtuellen Festplatten (Persistent Volumes). Sofern dies durch den Auftraggeber gewünscht wird, kann dies optional angeboten werden.

### 1.6.4 Backup/Wiederherstellung

Es wird standardmäßig kein Backup der Nutzdaten oder Anwendungsdaten auf den vom Auftraggeber eingerichteten virtuellen Festplatten (Persistent Volumes) angelegt.

Ein Backup von Anwendungsdaten kann hinzugebucht werden. In diesem Fall werden Daten auf den vom Auftraggeber eingerichteten virtuellen Festplatten (PV = Persistent Volume) täglich für 7 Tage gesichert. Eine Anpassung der Backup Policy ist per Change Request möglich.

Für Plattformen auf der OTC wird als Backupsystem der Volume Backup Service (VBS) genutzt.

Eine Wiederherstellung von Daten kann per Change Request in Abstimmung mit dem Support Team des Auftragnehmers während des überwachten Betriebes (AOT) innerhalb von 4 Stunden eingeleitet werden. Die Laufzeit der Rücksicherung der Daten steht u.a. in Abhängigkeit zu der Datenmenge.

Achtung: für Datenbankanwendungen hat der Auftragnehmer vor dem Sicherungslauf einen Datenexport (Dump) auf dem verwendeten PV zu erstellen. Bei der Wiederherstellung einer Sicherung bekommt der Auftraggeber den Dump aus der letzten Sicherung zurück, sodass der er die Datenbank durch Einspielen des Dumps wiederherstellen kann

## 1.7 Betriebszeiten

Die überwachte Betriebszeit (AOT = Attended Operation Time) ist der Zeitraum, in dem der technische Support erreichbar ist und eine Störung der Systemverfügbarkeit beheben kann. Der Auftraggeber kann zwischen folgenden Optionen wählen:

- AOT OFFICE TIME (CE[S]T)
- AOT FULL TIME (7x24, Rufbereitschaft außerhalb der OFFICE TIME)

Die OFFICE TIME umfasst jeweils die Zeit von 8:00 Uhr bis 18:00 Uhr (CE[S]T) außer an Wochenenden und bundeseinheitlichen Feiertagen.

## 1.8 Wartungsarbeiten, Change Requests

Wartungsarbeiten an Managed PaaS Plattformen und Change Requests werden grundsätzlich innerhalb des Standard-Wartungsfensters durchgeführt. Standard-Wartungsfenster finden Montag bis Donnerstag von 14:00 -16:00 Uhr, ausgenommen gesetzliche Feiertage (Zeitangaben in CE[S]T) statt. Arbeiten außerhalb des Standard-Wartungsfensters können kostenpflichtig gesondert beauftragt werden.

| Wartungsfenster | Aufschlag |
|---|---|
| Werktags 08:00 Uhr bis 18:00 Uhr | 0% |
| Werktags 06:00 Uhr bis 08:00 Uhr | 25% |
| Werktags 18:00 Uhr bis 20:00 Uhr | 25% |
| Werktags 20:00 Uhr bis 06:00 Uhr | 50% |
| Samstags | 50% |

| Wartungsfenster | Aufschlag |
|---|---|
| Sonn- und Feiertage | 100 % |

Arbeiten an Managed PaaS Plattformen, die potentiell zu Beeinträchtigungen der Verfügbarkeit führen können, werden grundsätzlich vom Auftragnehmer mindestens drei Werktage vor Beginn der Wartungsarbeiten angekündigt. Beeinträchtigung der Verfügbarkeit während angekündigter Wartungsarbeiten fließen nicht als ungeplante Ausfallzeiten mit in die Berechnung der Verfügbarkeit ein.

### 1.8.1 Sicherheitsrelevante Patches

Der Auftragnehmer installiert zeitnah, verfügbare sicherheitsrelevante Patches und Hotfixes. Patches und Hotfixes werden dabei gemäß CVSS Score Logik priorisiert und gemäß folgender Methodik eingespielt:

| Priorität / Kritikalität | Update Zyklus |
|---|---|
| Low | Update gemeinsam mit Release Rollout (OCP) |
| Important | Quartals Update |
| Critical | Update innerhalb zwei Wochen |

### 1.8.2 Software Updates und Upgrades

Der Auftragnehmer installiert nach eigenem Ermessen und nach eingehender Prüfung neue Versionen der vom Auftragnehmer eingesetzten Software.

Die Installation der Updates erfolgt in den vordefinierten Wartungsfenstern. Hierbei wird die Plattform seitens des Auftraggebers innerhalb der durch den Hersteller vorgegebenen supporteten Versionen und durch den Auftragnehmer freigegebenen Versionen gepatcht.

Wird durch den Auftraggeber eine ältere Version benötigt, für die vom Hersteller kein Support mehr geleistet wird, gehen Störungen nicht zu Lasten des Auftragnehmers.

Major Upgrades (z.B. OCP 4.x auf OCP 5.x) sind nicht Bestandteil des automatischen Upgrades und werden separat angeboten.

### 1.8.3 Change Requests

Der Auftraggeber kann Change und Service Requests beauftragen. Hierzu kann der Auftraggeber eine E-Mail an die bei Auftragserteilung bekanntgegebene Funktionsmailbox (FMB) mit dem Betreff „CHANGE: MSC PAAS/[customername][platformname]/[request]" senden. Im Text der E-Mail muss der Ansprechpartner mit Name, E-Mail-Adresse und Telefonnummer und eine möglichst genaue Beschreibung des Auftrags (in Englisch) enthalten sein. Auf welche Weise und mit welchen „Commands" der Auftrag ausgeführt wird, obliegt der Verantwortung des Auftragnehmers.

## 1.9 Service Desk

Der Service-Desk ist per E-Mail erreichbar und nimmt Change Requests und Incident Tickets des Auftraggebers auf. Der Auftraggeber erhält zu diesem Zweck vorbereitete Textvorlagen.

Die Service-Desk-Leistungen werden standardmäßig in deutscher Sprache erbracht. Alle Zeitangaben beziehen sich auf die mitteleuropäische Zeit (CE[S]T). Direkte Rückmeldungen aus dem Operating-Team des Auftragnehmers können in Deutsch oder Englisch sein.

### 1.9.1 Incident-Bearbeitung

Der Auftraggeber wird in Abhängigkeit der Kritikalität des Tickets über den aktuellen Stand der Bearbeitung informiert.

Die Analyse im Rahmen der Incident-Bearbeitung kann ergeben, dass die festgestellte Störung (Meldung eines Incident oder Monitoring) durch Mitarbeiter oder Applikationen des Auftraggebers verursacht wurde bzw. es sich um einen Fehler in der Programmierung der Applikation des Auftraggebers handelt. In diesem Fall werden dem Auftraggeber die Kosten für die Analyse in Rechnung gestellt und das Incident Ticket in ein Problem Ticket überführt. Die weitere Unterstützung des Auftraggebers bei der Behebung der Störung wird dann in Absprache und ggf. kostenpflichtig durchgeführt.

## 1.10 Service Delivery Management

Der Service Delivery Manager ist für die Einhaltung der in diesem Leistungsschein beschriebenen Services verantwortlich.

### 1.10.1 Funktionsmailbox

Durch den Auftraggeber kann das Service Delivery Management über die SDM Funktionsmailbox erreicht werden, sofern Änderungswünsche (Change Requests) seitens des Auftraggebers bestehen.

### 1.10.2 Named Contact

Sofern durch den Auftraggeber als zusätzlicher Service gewünscht, kann ein dedizierter Service Delivery Manager (Named Contact) die Kundenkommunikation übernehmen. Dieser dedizierte Service Delivery Manger kann folgende Leistungsinhalte erbringen:

- Service- und Betriebsmanagement (Betriebsverantwortung als zentral steuernde Instanz, SPOC)
- Regelmäßige Service Review Meetings / Vor-Ort-Termine
- Tiefgehende Kenntnisse der Kundenlösung
- Eskalationsmanagement (Eskalationsinstanz)
- Continual Service Improvement: Qualitätssicherung und Verbesserung (PDCA Zyklus)
- Steuerung von Rechten und Pflichten, Koordination von kundenindividuellen Wartungsfenstern
- Erstellung von Serviceberichten (SLA Reporting im Rahmen des Service Level Management, Incidentübersicht, Problemberichte, Changeübersicht)

Die gewünschten Tätigkeiten sind nur Bestandteil des Vertrages, sofern sie im Preisblatt aufgeführt sind.

# 2 LEISTUNGSUMFANG (RACI MATRIX)

Zur Veranschaulichung der Verantwortlichkeiten dient die folgende RACI Matrix zur Beantwortung der folgenden Fragen:

- Wer ist zuständig für die eigentliche Durchführung (Responsible)
- Wer ist rechenschaftspflichtig, im Sinne von „genehmigen", „billigen" oder „unterschreiben" (Accountable):
- Wer ist nicht direkt an der Umsetzung beteiligt, aber hat relevante Informationen für die Umsetzung (Consulted)
- Wer ist zu informieren über den Verlauf bzw. das Ergebnis der Tätigkeit (Informed)

| Aktivität | Auftragnehmer | Auftraggeber |
|---|---|---|
| Bereitstellung des Managed PaaS Portals | A/R | |
| Bereitstellung des OC Clients | A/R | C |
| Bereitstellung SSL Zertifikate / Wildcard Zertifikate. | I | A/R |
| Deployment von Middleware und Datenbanken | - | A/R |
| Bereitstellung von Rechenleistung zum Deployment von Middleware- und Datenbankprodukten | A/R | I |
| Bereitstellung von Datenbank und Middleware Lizenzen. Das Lizenzmodell muss für die Anwendung in der Cloud geeignet sein. | - | A/R |
| **PaaS Plattform Maintenance** | | |
| Bereitstellung von plattformspezifischer Wartung, einschließlich der Installation relevanter und vereinbarter Service Packs, Patches und Software-Wartungsversionen | A/R | C |
| Durchführung von Wartungsarbeiten zur Aktualisierung der Plattform | A/R | C |
| Test von plattformbezogenen Software Updates, Service Packs und Patches | A/R | - |
| Planen der plattformbezogenen Wartungen | A/R | I |
| **Benutzerverwaltung** | | |
| Benutzerverwaltung (technische Benutzer, max. 5 je Plattform) auf Middleware-Ebene (Benutzer, Gruppen) | A/R | |
| Verwaltung von Applikationsbenutzern | | A/R |
| Verwaltung und Management der Benutzerrollen und -profile der Softwarehersteller | A/R | |
| **Einrichtung** | | |
| Bestellung von PaaS Ressourcen zur Bereitstellung von Workloads | C | A/R |
| Bekanntgabe der externen IP Adresse der Plattform für die Bestellung einer kundenindividuellen Domain bei einem Domain Provider. | A/R | I |
| Bereitstellung von kundenindividuellen Domains | C | A/R |
| Bereitstellen einer Standarddomain, sofern durch Auftraggeber keine kundenindividuelle beigestellt wird | A/R | I |
| **Verwaltungsarbeiten** | | |
| Erfassung und Verwaltung von Fehlerlisten, Analyse der Fehlerlisten | A/R | |
| Umsetzung der vereinbarten Sicherheitsrichtlinien | A/R | |

| | | |
|---|---|---|
| **Incident Management** | | |
| Bereitstellung von Fehlerlisten zur Analyse auf Anfrage (im Falle eines plattformbezogenen Fehlers) | A/R | I |
| Management von Plattformvorfällen inklusive Dokumentation im Ticketing-System des Auftragnehmers | A/R | |
| **Problem Management** | | |
| Nachverfolgung der bearbeiteten Problemberichte im Standard-Ticketing-System des Auftragnehmers inkl. Root-Cause Analyse | A/R | I |
| **Patch Management** | | |
| Installation von sicherheitsrelevanten Patches und Hotfixes auf Plattform-Ebene | A/R | I |
| Informieren bei geänderten Softwareversionen des Softwareanbieters | A/R | I |
| **Monitoring** | | |
| Definition und Konfiguration der Systemüberwachung der Plattformkomponenten | A/R | - |
| Einrichten von Monitoring-Anforderungen | A/R | - |
| Monitoring der Plattform (tool-gesteuert) | A/R | - |
| Überwachung und Analyse der Plattform ermöglichen | A/R | I |
| Grundlegende Überwachung des Zustands der Plattform auf Betriebssystemebene (CPU-Last, freier Arbeitsspeicher, Netzwerkerreichbarkeit, Erreichbarkeit des Dateisystems und Nutzungsrate, z.B. Pods pro Node) | A/R | |
| Applikations-Monitoring | C | A/R |
| **Logging** | | |
| Systemlogs speichern (Plattform und Containerlogs) | A/R | |
| Bereitstellen von Logfiles im Fehlerfall (auf Anfrage) | A/R | I |
| Applikationslogging | - | A/R |
| Bereitstellung der Plattformnutzung auf Projektebene zur Weiterverarbeitung | A/R | I |
| **Backup Plattformkonfiguration** | | |
| Sicherung der kompletten Plattformkonfiguration inkl. der Docker Images zur schnellen Wiederherstellung der Plattform nach einem Totalausfall. Anwendungsdaten müssen vom Auftraggeber separat gesichert werden. | A/R | |
| **Backup Anwendungsdaten** | | |
| Erzeugen von wiederherstellbaren Snapshots bzw. Dumps laufender Anwendungen und Durchführung von dateibasierten Backups der Nutzdaten. | C | A/R |
| Backup Zeitplan definieren | C | A/R |
| Definition von Aufbewahrungszeiten | C | A/R |
| Durchführung von Middleware und Datenbankbackups inkl.: | C | A/R |
| - Logfiles | C | A/R |
| - Monitoring der Funktionalität inkl. Restore | C | A/R |
| Backup and Recovery von PaaS containers | C | A/R |
| Durchführung von Restores auf Kundenwunsch | C | A/R |

| Reporting | | |
|---|---|---|
| Standardreporting bestehend aus:<br>• SLA-Reporting | A/R | I |
| Projektbezogene Auslastungsstatistik auf Basis der verbrauchten PCU-Stunden und nutzungsabhängiger Verbräuche (z.B. Storage) | A/R | I |

# 3 SERVICELEVEL

## 3.1 Fehlerklassen

| | Definition | Beispiel |
|---|---|---|
| Priorität 1 (kritisch) | Geschäftsunterbrechung mit größeren, insbesondere größeren kommerziellen Auswirkungen:<br>Der Service ist vollständig unterbrochen. | Eine Störung verursacht einen Totalausfall. der Plattform. Die auf der Plattform betriebenen Applikationen sind nicht mehr erreichbar. |
| Priorität 2 (schwer) | Ausfälle oder Teilausfälle mit Einfluss auf das Geschäft des Auftraggebers oder mit Prozessbehinderungen.<br>Ein wesentliches Funktionsmerkmal ist ausgefallen oder ist wesentlich eingeschränkt und eine möglichst zügige Neutralisation ist erforderlich. | Eine Störung verursacht die Nichterreichbarkeit einzelner Microservices oder neue Anwendungen können nicht ausgerollt werden.<br>Eine schwerwiegende Bedienungseinschränkung liegt vor, z.B. können sich ganze Betriebsteams nicht mehr anmelden. |
| Priorität 3 (leicht) | Moderate oder geringfügige Auswirkung oder Beeinträchtigung bei der Nutzung:<br>IT-Problem, sonstiger Dienst oder sonstiges Funktionsmerkmal ist beeinträchtigt. Wesentliche Merkmale stehen weiterhin zur Verfügung. Störung ohne Verfügbarkeitseinschränkung. | Eine Störung verursacht eine geringe Betriebseinschränkung.<br>„Kosmetischer Fehler" ohne Einfluss auf die Funktionalität. Layout und/oder Designfehler. |

## 3.2 Reaktions- und Wiederherstellungszeiten

Zeitraum von der Meldung des Fehlers bis zur ersten Reaktion und bis zur Wiederherstellung.

| | Kritisch | Schwer | Leicht |
|---|---|---|---|
| Erste Reaktion* | ≤ 15 Minuten (Einmeldung per Telefon)<br>≤ 1 Stunde (Einmeldung per E-Mail) | ≤ 4 Stunden | ≤ nächster Arbeitstag |
| Wiederherstellung* | ≤ 4 Stunden (Prod System) | ≤nächster Arbeitstag | ≤ 3 Arbeitstage |

* innerhalb der gewählten AOT

## 3.3 Plattformauslastung

Seitens des Auftraggebers besteht eine Mitwirkungspflicht, absehbare Mehranforderungen an die Plattform aufzuzeigen, die über das vorher definierte Auslastungsprofil der Plattform hinausgehen.

# Leistungsbeschreibung & zusätzliche Bedingungen
# [CLOUD NATIVE APPLICATION OPERATION]

**Stand:** 28.05.2020

# Inhalt

# 1 EINLEITUNG

Das Cloud Application Operation von T-Systems bietet zwei Serviceprodukte um einen stabilen Cloud Betrieb von Applikationen und den CI/CD Tools sicherzustellen. Diese können getrennt voneinander oder als ergänzende Leistungen gemeinsam beauftragt werden.

Standardmäßig wird der Service 24*7 angeboten und je nach Bedarf aus Indien, Ungarn oder Deutschland erbracht. Grundsätzlich steht ein technischer Ansprechpartner aus Deutschland zur Koordination zur Verfügung.

Dieser Leistungsschein definiert die gemeinsamen Bedingungen für die Leistungen der beiden Servicemodelle: Cloud native Application Operation und CI/CD Service.

## 1.1 Cloud native Application Operation (CNAO)

Es wird ein agiler und zuverlässiger Applikationsbetrieb speziell für Cloud nativ entwickelte Applikationen angeboten. Von der proaktiven Überwachung (24*7), über das Troubleshooting, das Schnittstellenmangement als auch weiteren Services wie Nutzermanagement, Reporting und tiefgehenden Deep-Analysis, werden drei Servicepakete angeboten:

- Application Live Check (ALC)
- Application Support (ASU)
- Application Service (ASE)

Diese werden in Kapitel 2.1 detailliert erläutert.

## 1.2 CI/CD Service

Ob als Service Erweiterung zu dem genannten Cloud nativen Applikationsbetrieb, oder als alleinstehehender Service wird der CI/CD Service angeboten.

Im Rahmen dieses Leistungspaketes ermöglichen wir Ihnen durch die Einführung und Umsetzung unseres CI/CD-Toolchain Services eine automatisierte Entwicklungs-, Integrations-, Test- und Produktionsumgebung. Dazu wird die CI/CD Toolchain konfiguriert mit den dazugehörigen automatisierten Tools in der Cloud.

Eine detaillierte Leistungsbeschreibung befindet sich in Kapitel 4.3.1

# 2 CNAO - LEISTUNGSÜBERSICHT

Das Cloud native Application Operation (CNAO) des AN ermöglicht die proaktive Überwachung und Verwaltung der Anwendungen des Auftraggebers gemäß dieser Leistungsbeschreibung. Dabei teilt sich das Application Operation in drei Leistungsklassen auf:

- Application Live Check (ALC)
- Application Support (ASU)
- Application Service (ASE)

Innerhalb der Leistungsklassen wird Application Operation entsprechend der Kritikalität und der Komplexität einer Anwendung angeboten.

Bei der proaktiven Überwachung und Verwaltung von Applikationen – oder Services des Auftraggebers sind die überwachten Metriken dabei stets abhängig von der Applikation und werden vom Auftraggeber definiert, bzw. ergeben sich zumeist aus den Applikations- oder Produktbestandteilen.

Neben dem klassischen Monitoring und Management-Reporting erlaubt das Application Operation auch – sofern technisch möglich und sinnvoll – eine Echtzeitansicht- und Übersicht über den Zustand und die Verfügbarkeit der Applikation sowie ihrer Komponenten. Im Service ebenfalls enthalten ist die Lösung von definierten Störfällen.

Dieser Leistungsschein definiert die gemeinsamen Bedingungen für die Leistungen des Cloud native Application Operation.

## 2.1 Servicepakete und Leistungsübersicht CNAO

Cloud native Application Operation wird in den Varianten „Application Live-Check" (ALC), „Application Support" (ASU) und „Application Service" (ASE) angeboten.

| | | ALC | ASU | ASE |
|---|---|---|---|---|
| | STANDORT DER SERVICE-ERBRINGUNG | INDIEN | INDIEN / UNGARN | INDIEN / UNGARN / GERMANY |
| | OPTIONEN FÜR DIE ERREICHBARKEIT | 24*7 | 24*7 | 24*7 |
| **Monitoring / Logging** | Monitoring basierend auf vorhandenen Tools/Dashboards | X | X | X |
| | Monitoring/Überprüfung von Interfaces | | X | X |
| | Betrieb mittels vorhandener Runbooks | X | X | X |
| | Erstellung und Pflege von Runbooks | (X) | X | X |
| | Proaktives Monitoring und Parameterchecks | | | X |
| | Definition von Leistungsparametern (KPI) und Beratung | | | X |
| | System Logging (OS, Middleware, DB) und Monitoring | | X | X |
| | Semantisches Monitoring (Funktionale Tests) | | | X |
| **Fehler-behebung** | SpoC – Service Desk | | (X) | (X) |
| | Neustart von Services | X (entsprechend Runbook) | X | X |
| | Neustart / Administration von Datenbanken | | X | X |
| | Backup / Restore | | (X) nur Plattform & Container | X inkl. Applikations daten & Datenbanken |
| | Koordination von Drittdienstleistern | | X | X |
| | Verwendung eines Ticket-Tools | | X | X |
| | Root Cause Analysen (Ursachenforschung) | | (X) | X |
| | Pflege einer Fehler-/ Wissensdatenbank | | X | X |
| **Release (DevOps)** | Monitoring von Abnahmeprozessen (Q-Gates) | | | X |
| | Deployment neuer Versionen | | | (X) |
| | Durchführen von Rollbacks neuer Versionen | | | X |
| **Zusatz-leistungen** | Reporting | X (App Verfügbarkeit) | X (zusätzliche Reporting der KPIs) | X (zusätzlich Reporting der KPIs) |
| | Benutzerverwaltung (Systemnutzer, Logfiles, ...) | | (X) | X |
| | Kapazitätsmanagement | | | (X) |
| | Eskalationsmanagement | | (X) | (X) |
| | Servicemanagement | | (X) | X |
| | Aufsetzen agiler Prozesse | | (X) | (X) |
| | Qualitätsmanagement und kontinuierliche Verbesserung | | (X) | X |
| | DevOps Beratung | | (X) | X |
| | Bereitstellungsautomatisierung | | (X) | (X) |

**X – enthaltene Leistung**
**(X) – optionale Leistung**

## 2.2 Leistungsklassen Application Operation

Durch die Leistungsklasse einer Applikation / eines Services wird die Komplexität definiert. Hierfür sind im Wesentlichen die Bestandteile und Schnittstellen ausschlaggebend.

| | SIMPLE | MEDIUM | COMPLEX |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Anzahl Einzelkomponenten | 1 - 5 | 6 – 10 | > 10 |
| Anzahl Schnittstellen | 1 - 2 | 2 – 5 | > 5 |
| Anzahl 3rd Party | 1 - 2 | 3 – 5 | > 5 |

## 2.3 Kritikalität Application Operation

Durch die Kritikalität der Anwendung / des Services wird festgelegt, wie hochverfügbar eine Applikation sein muss.

Hierbei wird gemeinsam mit dem Autraggeber eine Bewertung hinsichtlich der Kritikalität vorgenommen:

- Nutzungsgrad
- Wirkungsgrad
- Ausfallkritikalität
- Anzahl Schnittstellen
- Häufigkeit von Releases

Es wird eine Einstufung in die Kritikalitäten vorgenommen:

| | EINORDNUNG |
|---|---|
| Kritikalität 1 – HOCH KRITISCH | Die Applikation / der Service muss permanent zur Verfügung stehen. Ein Ausfall hat eine direkte Auswirkung auf die Kunden oder die Geschäftsprozesse des Auftraggebers |
| Kritikalität 2 – MITTEL KRITISCH | Die Applikation / der Service darf kurzzeitig nicht zur Verfügung stehen. Ein Ausfall hat keine direkte Auswirkung auf die Kunden oder die Geschäftsprozesse des Auftraggebers |
| Kritikalität 3 – WENIGER KRITISCH | Die Applikation / der Service kann über einen längeren Zeitraum nicht zur Verfügung stehen. Ein Ausfall hat keine direkte Auswirkung auf die Kunden oder die Geschäftsprozesse des Auftraggebers oder kann durch andere Maßnahmen ausgeglichen werden. |

Sofern eine Applikation / ein Service der Kritikalitätsstufe 2 oder 3 zugeordnet wird, können für diese Applikation / diesen Service keine Prio 1 Tickets beim Service Desk eröffnet werden.

## 2.4 Leistungen des Auftragnehmers

Nachfolgend werden die Leistungen für die Servicepakete Application Live Check, Application Support und Application Service ausführlich beschrieben. Die Serviceleistungen für den Auftragnehmer wird in Absprache mit dem Auftraggeber im Servicehandbuch definiert und festgehalten.

# 3 BEREITSTELLUNG

Eine gute Planung sowie die erfolgreiche Umsetzung innerhalb einer Transitionphase ist die grundlegende Voraussetzung für den reibungslosen Ablauf in unserem agilen Betrieb von Cloud Applikationen und dem CI/CD Service.

Generell ist der Umfang der Transition Leistung durch den AN davon abhängig, ob der Auftraggeber die Plattform und Tools dem Auftragnehmer zur Verfügung stellt für die Erbringung des Betriebs, oder der Auftraggeber die Tools vom Auftraggeber einsetzt.

Wird die Umgebung sowie die Tools vom Auftraggeber bereitgestellt, ist sicherzustellen dass dem Operationsteam alle benötigten Zugänge und Zugriffe ermöglicht werden. Der Auftraggeber ist verantwortlich für die Verfügbarkeit.

Wird die Umgebung von dem Auftragnehmer bereitgestellt so leistet der AN einen Managed Service für den Auftraggeber.

Während der Transitionphase unterstützt der AN den AG mit drei unterschiedlichen Verfahren basierend auf Best Practices von Industrie und des AN.

Jede zu überwachende Applikation wird zuerst in den Betrieb übernommen. Im Rahmen der Transitionphase wird der Betrieb vorbereitet. Hierzu wird nach SCRUM eine entsprechende Planung und Umsetzung erfolgen. Hierzu gehören die Dokumentation, die technische Realisierung im Betrieb, Schulungen des Operationsteams, Aufsetzen der Betriebsprozesse und durchlaufen der Testphase.


- **Application Live Check**
    - Der Auftraggeber stellt dem Auftragnehmer die für die Applikation notwendigen Runbooks zur Verfügung. Diese werden durch den Auftragnehmer getestet und in den Betriebsprozess übernommen.
    - Der Auftraggeber stellt dem Auftragnehmer alle notwendigen Ansprechpartner und Kontaktinformationen zur Verfügung.
- **Application Support und Application Service**
    - Hierbei wird durch den Auftragnehmer, in enger Zusammenarbeit mit dem Auftraggeber, das für den Applikationsbetrieb und die Applikationsüberwachung notwendige Wissen gesammelt und festgehalten. Diese Wissenssammlung umfasst unter anderem, aber nicht ausschließlich:
        - Knowledge Base
        - Runbooks für definierte Applikations- und Fehlerzustände

- Responsibility Matrix

# 4 BETRIEB

## 4.1 Betriebszeiten

Die überwachte Betriebszeit (AOT = Attended Operation Time) ist der Zeitraum, in dem der technische Support erreichbar ist und eine Störung der Systemverfügbarkeit beheben kann. Der Auftraggeber kann zwischen folgenden Optionen wählen:

- AOT OFFICE TIME (CE[S]T)
- AOT FULL TIME (7x24, Rufbereitschaft außerhalb der OFFICE TIME)

Die OFFICE TIME umfasst jeweils die Zeit von 8:00 Uhr bis 18:00 Uhr (CE[S]T) außer an Wochenenden und bundeseinheitlichen Feiertagen.

- Prio 1 und 2 Tickets werden 24*7 bearbeitet
- Prio 3 Tickets innerhalb der AOT

## 4.2 Betriebsleistungen CNAO

### 4.2.1 Monitoring / Logging

Der „Application Service" ermöglicht eine proaktive Überwachung und Verwaltung von Auftraggeberapplikationen. Die überwachten Metriken sind dabei stets abhängig von der Applikation und werden vom Auftraggeber definiert, bzw. ergeben sich zumeist aus den Applikations- oder Produktbestandteilen.

Neben dem klassischen Monitoring und Management-Reporting erlaubt der „Application Service" – eine Echtzeitansicht - und Übersicht über den Zustand und die Verfügbarkeit der Applikation sowie ihrer Komponenten.

Das Application Operation besteht dabei aus folgenden Kernkomponenten:

- **Überwachung** – Die Überwachung der definierten Applikationsendpunkte und Schnittstellen.
  - **Application Live Check**
    - Definition und Überwachung von Alarmen für spezifische Funktionen und Schnittstellen
    - Überwachung der Plattform im Rahmen der durch den Auftraggeber vorgegebenen Überwachungsmetriken, im Besonderen die Events auf Infrastrukturebene und die Events auf Anwendungsebene
  - **Application Support**
    - Alle Leistungen des Application Live Check
    - Definition der KPIs gemeinsam mit dem Auftraggeber. Durchführung eines fachlichen Monitorings auf Anwendungsebene im Sinne von Alarmierung bei Unter- oder Überschreiten von Schwellwerten.
    - Bei Feststellung eines Events, die Filterung nach Klassifikationen und die Einleitung definierter Maßnahmen.

- Die Verknüpfung von Events zu den jeweiligen Services, damit eine Prioritätenbewertung (d.h. Auswirkung und Dringlichkeit) erfolgen kann.
- Das Erkennen und Berücksichtigen von Wechselbeziehungen zu Events und die anschließende Einleitung entsprechender Reaktionen.

- **Application Service**
  - Alle Leistungen des Application Support
  - Periodische Health Checks der Applikationen während der AOT
  - Manuelles semantisches Monitoring zur Überwachung der Funktionalität, die sich über mehrere Microservices erstrecken während der AOT. (Bsp. Anmelden am System)
  - Pro-aktives Monitoring während der AOT, Untersuchung von wiederkehrendem oder auffälligem Verhalten im Monitoring – sowie die Erzeugung von Tickets zu Auffälligkeiten, die auf best effort Basis gelöst werden oder weitergeleitet werden
  - Überprüfung der systemrelevanten der applikationsrelevanten Logdateien für die Identifikation von Problemen während des Betriebs und Detailanalyse von Incidents
  - Prüfen der Logdaten der Anwendungen, mit besonderem Blick auf Kapazitätsengpässe, unautorisierte Zugriffe und Aufarbeitung von Incidents

### 4.2.2 Fehlerbehebung (Troubleshooting)

Behandeln von Störungen im Betriebsablauf die entweder über den Service Desk durch berechtigte Benutzer oder technisches Personal gemeldet werden, oder die durch Monitoring Tools im Rahmen des Event Managements automatisiert erkannt und berichtet werden. Incidents können Unregelmäßigkeiten sein, oder Ausfälle, Störungen, Defekte und Programmfehler, sowie Störungen, die durch Deployments auftreten.

Das primäre Ziel ist die schnellstmögliche Wiederherstellung des gestörten IT Services. Der Auftragnehmer unterstützt den Auftraggeber bei der Definition eines Prozesses für die Eskalation von Incidents.

- **Entstörung** – für definierte Störfälle können im Onboarding Entstörvorgänge definiert werden. Beim Erkennen eines Störfalles werden diese abgearbeitet und (sofern technisch möglich) auf Erfolg überprüft. Schlägt dieser fehl oder wird ein nicht beschriebener Störfall erkannt/gemeldet, so erfolgt eine Eskalation über definierte Wege und Kontaktpunkte.

  - **Application Live Check:**

    Ausführen der im Runbook definiert Anweisungen. Sofern hierdurch die Störung nicht behoben werden kann, erfolgt eine Information des durch den Auftraggeber definierten 3rd Level Supports

    Es obliegt dem Auftraggeber, die Runbooks entsprechend der Weiterentwicklung der Applikation anzupassen und dem Auftragnehmer diese über den Change Request Prozess zur Verfügung zu stellen.

  - **Application Support**
    - Entstören des Fehlers entsprechend der mit dem Auftraggeber definiert Runbooks

- Beheben von anwendungsspezifischen technischen Issues und Bugs, die ohne die fachliche Zuarbeit des Auftraggebers behoben werden können, bspw. Restarts von Services und Datenbanken
- Koordination von Drittanbietern beim Bug Fixing im Einflussbereich der Anwendung, ebenso das Routing und die Überwachung von Incident – Tickets zu diesen Issues

- **Application Service**
  - Alle Leistungen des Application Support
  - Durchführen von selbständigen Tests, mit denen das Wiederaufleben von defekten Services trainiert wird. Die betroffenen Services sind vor Vertragsabschluss vom Auftraggeber mitzuteilen
  - Im Rahmen fehlgeschlagener Deployments das Anstoßen bzw. selbst durchführen eines Backups/Restores.
  - Bereitstellen und Pflegen der Werkzeuge, Prozesse, Qualifikationen und Regeln für eine effektive und effiziente Bearbeitung von Incidents
  - Erfassung und Qualifizierung eingehender Störungen; die Priorisierung wird aus dem 1st/1.5 Level Support übernommen und nur angepasst, sofern diese nicht der SLA Vereinbarung entspricht. Telekom behält sich das Recht vor Anpassungen an der Servicekritikalität vorzunehmen sollte es den im Leistungsschein vorhandenen Beschreibungen nicht entsprechen..
  - Eskalation von ungelösten Incidents gemäß den vom AG genehmigten Verfahren als auch die hohe Priorisierung der Incidents, die große Auswirkungen haben
  - Falls eine Lösung im 2nd Level Support nicht möglich ist, wird das Ticket gem. Eskalationsmatrix an den 3rd Level Support übergeben. Hiermit endet die SLA-Berechnung.
  - Incident Überwachung und funktionale Eskalation, so dass bei zu langen Lösungszeiten rechtzeitig Maßnahmen eingeleitet werden können
  - Incident Abschluss und Review, um sicherzustellen, dass der Incident tatsächlich gelöst worden ist und dass alle Informationen zur Beschreibung des Lösungsweges in ausreichendem Detail dokumentiert sind. Zusätzlich sollen Erkenntnisse aus der Lösung des Incidents für die Lösung künftiger Incidents nutzbar gemacht werden (Wissensdatenbank)
  - Bereitstellen von Informationen für das Problem Management, über wiederkehrende Störungen, Störungsmuster, Trends und Anwendbarkeit bereitgestellter Lösungen und Workarounds
  - Incidents zu verhindern bzw. die Auswirkungen von Incidents zu minimieren, die nicht verhindert werden können
  - Ermittlung der Ursache (Root Cause) von Incidents, die einem Problem zuzuordnen sind und Veranlassung von geeigneten Maßnahmen zur Verbesserung oder Korrektur der Situation
  - kontinuierliche Trendanalyse bezüglich der Anzahl und Art der Probleme, um Bereiche für Verbesserungsmaßnahmen zu identifizieren

### 4.2.3 Release (DevOps) – Standard Change „Deployment"

Im Rahmen des Leistungspaketes Application Service können vom Auftraggeber Leistungen im Bereich Releasemanagement hinzugebucht werden. Der Auftraggeber verantwortet den Releaseprozess (Bereitstellung Backlog + Releasedokumentation, Aussprechen von Freigaben) und liefert vollständige und verständliche Releasenotes um Fehlervorbeugung bei den Releases zu gewährleisten.

Hierbei werden durch den Auftragnehmer vom Auftraggeber initiierte Deployments und Hotfixes (Changes) ausschließlich an Werktagen (Montag bis Freitag) in der Zeit zwischen 8:00 Uhr und 18:00 Uhr (CET) bearbeitet - ausgenommen an bundeseinheitlichen Feiertagen.

Die Anzahl der Deployments ist auf ein Deployment pro Werktag begrenzt. Sofern weitere Deployments gewünscht werden, können diese über das Change Request Verfahren beauftragt werden.

- **Deployment** – Der Auftragnehmer wird das Deployment, mit Hilfe der zur Verfügung gestellten Scripte ausführen. Dabei werden die allgemeinen Prozess- und Qualitätsvorgaben Anwendung finden.
- Q-Gate Defintion durch Auftragnehmer / Q-Gate Freigabe erfolgt durch den Auftraggeber
- Der Auftraggeber stellt pro Deployment Rollback Szenarien dar und sicher, die von dem Applikationsbetrieb bei Bedarf ausgeführt werden
- Der Auftraggeber stellt die notwendige technische Infrastruktur (Systemzugänge), sowie Informationen und Ansprechpartner bereit, die zur Erfüllung des Auftrags erforderlich sind.

### 4.2.4 Add-on Services

- **Usermanagement**

  Neue Mitarbeiter des Auftraggebers werden eingerichtet und mit den notwendigen Rollen und Rechten ausgestattet, im Rahmen des vom Auftraggeber zur Verfügung gestellten Authentifizierungskonzepts. Ebenso werden neue Mitarbeiter, die den Betrieb unterstützen, im Onboarding aufgenommen.
  - Onboarding von Entwicklern (Dev) und Ops-Mitarbeitern
  - Offboarding von Entwicklern (Dev) und Ops-Mitarbeitern – wie im Authentifizierungskonzept des Auftraggebers beschrieben
  - Gruppenzugehörigkeit und Rechteverwaltung – Betreuung des vom Auftraggeber definierten Berechtigungsprozess gemeinsam mit den Fachverantwortlichen des Auftrageber. Im Rahmen einer regelmäßigen Pflege werden Gruppenzugehörigkeiten mit den Fachverantwortlichen abgeglichen.

- **Reporting**
  - Erstellung von regelmäßigen Reports zu den Services und in Absprache mit dem Auftraggeber in geeigneter Form übermitteln
  - Regelmäßiges Service Review Meeting zwischen Service Delivery Manager und Auftraggeber

- **Service Management**
  - Zur-Verfügung-Stellung der vereinbarten Service Level und der nachgelagerten Funktionalitäten
  - Der Auftragnehmer wird die definierten Service Level einhalten und permanent überwachen. Monitore werden im Rahmen ihrer Kommunikations- und Koordinierungsaufgaben die zur Verfügung gestellten Monitore überwachen und bei Schwellwertüberschreitung, die prozessual beschriebenen Alarmierungen durchführen.

- **Eskalationmanagement**

  **Optional auf Anfrage**

  - Manager vom Dienst (Eskalationsmanager in den Randzeiten)
    - Koordinationsverantwortung von Störungen mit Priorität 1 & 2
    - koordiniert alle Beteiligten, die zur Lösung der Störung benötigt werden, bis zum Abschluss
    - Einsatzzeiten sind individuell abzustimmen (Wochentags, Wochenende und Feiertage)
    - Reaktionszeit innerhalb der Rufbereitschaft beträgt in der Regel 0,5 Stunden

- **Quality Management**
  - Der AN wird einen kontinuierlichen Verbesserungsprozess zur Verfügung stellen, der die erbrachte Serviceleistung, im Rahmen periodischer Service Review Meetings, messbar macht.
  - Der Auftraggeber unterstützt dabei die Monitore weiter zu optimieren und zu ergänzen.

- **DevOps Beratung (Consulting)**
  - Kontinuirliche Verbesserung des Monitorings und Pflege der Bestands Monitoring Tools in Abstimmung mit dem Auftraggeber
  - Pflege von dem eingesetzten betriebsnotwendingen Tools nach onboarding im Support

  **Optional auf Anfrage:**

  - Erweiterung und Verbesserung des Monitorings durch den Einsatz neuer Monitoringtools in Abstimmung mit dem AG
  - Vorschläge zur Ergänzung von Metriken innerhalb der Applikationen für die Optimierung der Monitore durch den AG
  - Umfangreichere Veränderungen an dem Betriebskonzept werden zwischen Auftraggeber und Auftragnehmer abgestimmt und gegebenenfalls zusätzlich beauftragt.

- **Bereitstellungsautomatisierung (Deployment Automation)**

  **Optional auf Anfrage**

  - Reduktion der notwendigen manuellen Schritte für die Durchführung eines Deployments
  - Optimierung des Deploymentprozess für eine größtmögliche Automatisierung in Abstimmung mit den Prozessen des AG

## 4.3 Betriebsleistung CI/CD Service

Mit dem CI/CD Service wird ein Toolservice für die container-basierte Software-Entwicklung angeboten. Der AG übernimmt hierbei die Verantwortung für den CI/CD Prozess.

| | |
|---|---|
| **CI/CD by customer (AG)** | Der AG stellt das Tool- und Berechtigungskonzept und nutzt den reinen Betriebsservice für seine CI/CD Tools, die in seiner Umgebung laufen oder laufen werden. |

Folgende Tools werden standardmäßig im Rahmen des CI/CD Services vom AG betrieben:

| DevOps Tools | Funktion |
|---|---|
| Nexus, Sonarqube, Gitlab, GitlabRunner oder Jenkins | Continous Integration / Continous Delivery |
| Prometheus, Grafana | Monitoring / Logging |

Hinweis: Auf Anfrage und gegen Aufpreis können andere Tools vom Auftragnehmer beigestellt werden. Weiter muss das Konzept und der Zugriff im Rahmen eines Berechtigungskonzepts vom AG beigestellt werden.

- Die genaue Zielarchitektur wird vom AG mit Unterstützung des AN in einem Architekturkonzept konkret beschrieben.
- Der Auftraggeber stellt die notwendige technische Infrastruktur (Systemzugänge), sowie Informationen und Ansprechpartner bereit, die zur Erfüllung des Auftrags erforderlich sind.

### 4.3.1 CI/CD Leistungsbeschreibung

Durch den Ansatz der managed Tools wird sichergestellt, dass der AG seinen "Continous Integration" und "Continous Delivery" Prozess über alle seine Stages erfolgreich ausführen kann.
Im Rahmen eines managed agilen CI/CD Toolchain Betriebs stellen wir die Überwachung via Monitoringtools sicher. Im Störungsfall stellen wir eine schnelle Wiederherstellung der Toolchain sicher.

Folgende Leistungen werden angeboten:

| Aufgaben | CI/CD Service |
|---|---|
| Überwachung der CI/CD Container | X |
| Back-up & Wiederherstellung der TSI Tools | X |
| Back-up & Wiederherstellung von Inhalten | X |
| Patchmanagement der TSI Tools | X |
| Plugin-Support für TSI Tools | X |
| Service Desk | X |

X = Standardleistung

#### 4.3.1.1 CI/CD Back-up

Es wird regelmäßig ein Back-up der Server- und TSI Toolumgebung durchgeführt, um diese bei Bedarf wiederherstellen zu können. Dabei kann es zu kurzen Unterbrechungen oder Beeinträchtigungen der Applikationen kommen.

Es wird standardmäßig ein tägliches Backup der Nutzdaten bzw. Anwendungsdaten auf der bereitgestellten Umgebung angelegt.

Eine Wiederherstellung von Daten kann per Change Request in Abstimmung mit dem Support Team des Auftragnehmers während des überwachten Betriebes (AOT) innerhalb von 4 Stunden eingeleitet werden. Die Laufzeit der Rücksicherung der Daten steht u.a. in Abhängigkeit zu der Datenmenge.

#### 4.3.1.2 Software Updates and Upgrades CI/CD Tools

Der Auftragnehmer installiert neue Versionen (Minor Updates) der Software nach eigenem Ermessen und nach gründlicher Prüfung. Die Updates werden in den vordefinierten Wartungsfenstern installiert.

Wenn der AG eine ältere Version benötigt, für die der Hersteller keinen Support mehr bietet, trägt der Auftragnehmer bei Störungen keine Verantwortung über den reibungslosen Betrieb der CI/CD Tools.

#### 4.3.1.3 Plugin Support für die CI/CD Tools

Die CI/CD Tools werden nur mit den Plugins installiert, welche für den Betrieb notwendig sind. Weitere Plugins welche für spezielle Anforderungen des AG notwendig sind, können in Abstimmung zwischen AN und AG als optionale Leistung installiert werden.

Der AN stellt sicher, dass notwendige Versionsupgrades der Tools (Sicherheitspatches) vorrangig installiert werden. Der AN versucht sicher zu stellen, dass bei diesen Versionsupgrades auch weiterhin die zusätzlich installierten Plugins lauffähig sind. Dabei werden kritische/notwendige Updates für einen reibungslosen Betrieb Vorrang haben.

## 4.4 Service Qualität

### 4.4.1 Verfügbarkeit CNAO

Für die Services Application Live Check und Application Support wird seitens des Auftragnehmers keine Verfügbarkeit zugesagt, da das Leistungsspektrum des Services in der Ausführung vordefinierte Tätigkeiten besteht.

Im Rahmen des Application Service erhält der Auftraggeber Verfügbarkeitszusagen. Diese werden jedoch erst nach einem zwischen Auftraggeber und Auftragnehmer festzulegenden Testzeitraum für Applikationen / Services gültig, damit die Stabilität einer Anwendung / eines Service und die zugehörigen Runbooks getestet werden können.

Sollte sich während der Betriebszeit herausstellen, das die Verfügbarkeit einer Applikation / eines Services aufgrund mangelnder Betriebsstabilität nicht eingehalten werden kann, behält sich der Auftragnehmer vor, den Service einzustellen, bis durch den Auftraggeber die Applikation / der Service mit einer hinreichende Betriebsstabilität bereitgestellt wird. Dies gilt für alle drei Services (ALC, ASU und ASE).

Die definierte Verfügbarkeit für Applikationen im Applikation Service beträgt:

| Verfügbarkeit: | Rahmenbedingungen: |
|---|---|
| 99,5% / Monat | Vollständig redundant ausgelegte Applikation/Service. |
| 98,5% / Monat | Die Applikation / der Service oder Teile davon sind nicht redundant ausgelegt. |

$$\text{Durchschnittliche Verfügbarkeit} = \frac{365 \text{ Tage} * 24 \text{ Stunden} - \text{Ausfallzeit in Stunden}}{365 \text{ Tage} * 24 \text{ Stunden}}$$

Als Kriterium dienen die Ergebnisse des Monitorings am Leistungsübergabepunkt. Der Übergabepunkt muss zwischen dem AG und AN defineirt werden.

Der Auftragnehmer teilt dem AG monatlich die erreichte Verfügbarkeit mit.

Excused Events: Ausfallzeiten auf Grund eines der nachfolgenden Ereignisse bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt:

- Ausfälle aufgrund von Wartungsarbeiten
- Ausfälle aufgrund von Störungen auf Infrastrukturebene (AG-seitig oder Zulieferanten)
- Störungen, Ausfälle und Probleme, die auf den Kunden, seine Mitarbeiter oder Vertreter zurückzuführen sind, insbesondere Ausfälle auf Grund einer Überschreitung der zur Verfügung gestellten Kapazitäten
- Angriffe Dritter, z.B. durch (D)DoS Attacken, Hacking, Spamming

- Gefährdung oder Störung für Leistungen Dritter

### 4.4.2 Verfügbarkeit CI/CD

Die Verfügbarkeit des CI/CD Services beträgt 99,0% je Kalendermonat am Leistungsübergabepunkt und wird wie folgt berechnet:

$$\text{Durchschnittliche Verfügbarkeit} = \frac{365 \text{ Tage} * 24 \text{ Stunden} - \text{Ausfallzeit in Stunden}}{365 \text{ Tage} * 24 \text{ Stunden}}$$

Als Kriterium dienen die Ergebnisse des Monitorings am Leistungsübergabepunkt. Übergabepunkt für alle Leistungen ist der Übergabepunkt der CI/CD Tools an den AG.

Die Telekom teilt dem Kunden monatlich die erreichte Verfügbarkeit mit.

Excused Events: Ausfallzeiten auf Grund eines der nachfolgenden Ereignisse bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt:

- Ausfälle aufgrund von Wartungsarbeiten
- Störungen, Ausfälle und Probleme, die auf den Kunden, seine Mitarbeiter oder Vertreter zurückzuführen sind, insbesondere Ausfälle auf Grund einer Überschreitung der zur Verfügung gestellten Kapazitäten
- Angriffe Dritter, z.B. durch (D)DoS Attacken, Hacking, Spamming
- Gefährdung oder Störung für Leistungen Dritter

Der AN ist berechtigt, die Leistung für den AG ohne vorherige Benachrichtigung, bis zur Behebung einer Gefährdung oder Störung für Leistungen Dritter oder die Infrastruktur, zu deaktivieren.

### 4.4.3 Wartung/Wartungsfenster

Es werden regelmäßig Wartungsarbeiten durchgeführt. Sollte es zu Unterbrechungen kommen, wird der AG vorab informieren. Der AN ist hierbei bestrebt, Beeinträchtigungen durch Wartungsarbeiten möglichst gering zu halten. Wartungsarbeiten gelten nicht als Ausfallzeiten und bleiben daher bei der Berechnung der Verfügbarkeit unberücksichtigt. Im Falle von Notfall-Wartungsarbeiten erfolgt eine Information der Kunden ggf. nachträglich.

Standard-Wartungsfenster finden Montag bis Donnerstag von 14:00 -16:00 Uhr, ausgenommen gesetzliche Feiertage (Zeitangaben in CE[S]T) statt. Arbeiten außerhalb des Standard-Wartungsfensters können kostenpflichtig gesondert beauftragt werden.

| Wartungsfenster | Aufschlag |
|---|---|
| Werktags 08:00 Uhr bis 18:00 Uhr | 0% |
| Werktags 06:00 Uhr bis 18:00 Uhr | 25% |
| Werktags 18:00 Uhr bis 20:00 Uhr | 25% |
| Werktags 18:00 Uhr bis 06:00 Uhr | 50% |
| Samstags | 50% |
| Sonn- und Feiertage | 100 % |

Arbeiten an den CI/CD Tools, die potentiell zu Beeinträchtigungen der Verfügbarkeit führen können, werden grundsätzlich vom Auftragnehmer mindestens drei Werktage vor Beginn der Wartungsarbeiten angekündigt.

Beeinträchtigung der Verfügbarkeit während angekündigter Wartungsarbeiten fließen nicht als ungeplante Ausfallzeiten mit in die Berechnung der Verfügbarkeit ein.

### 4.4.4 Servicelevel

Für bestimmte Leistungen des AN werden zwischen den Parteien Service Level vereinbart, für die zu erreichende Sollwerte in Form qualitativer wie quantitativer Zielgrößen festgelegt und in absoluten Werten, Prozentwerten oder Zeitangaben dokumentiert wurden (Service Level Agreement, kurz „SLA"). Diese Service Level sind von der AN im Rahmen der vertragsgegenständlichen Leistungserbringung einzuhalten. Der AN hat die Einhaltung der vereinbarten Service Level mittels der zwischen den Vertragsparteien vereinbarten Messverfahren nachzuweisen.

Für die Sicherstellung des CNAO „Application Services" gilt folgendes:

- Die Verfügbarkeit der Hauptservices (Core, Backend und Skills) werden gemessen und in den Service Review Meetings besprochen, sowie Optimierungsbedarfe abgeleitet.
- Schnellstmögliche Analyse, Wiederherstellung und Weitergabe an Dritte
- Stetige Anforderungen zur verbesserten Stabilität der Systeme in Richtung Entwicklung

### 4.4.5 Fehlerklassen / Prioritäten

| PRIORITÄT | DEFINITION | BESCHREIBUNG UND BEISPIELE |
|---|---|---|
| PRIO 1 | – Ausfall der Plattform oder Ausfall von kritischen Services mit gravierenden Auswirkungen (Entwicklung und Produktion)<br>– Eine hohe Useranzahl ist von dem Ausfall betroffen (Ausfall gegenüber Endkunde/User) | – Eine Störung sorgt für einen Totalausfall eines Webshops und in Folge dessen für Verluste.<br>– Die Entwicklungsplattform ist komplett ausgefallen |
| PRIO 2 | – Teilausfall der Plattform oder Teilausfall von Services mit Einfluss auf das Auftraggebergeschäft<br>– Hauptfunktionen sind bedeutend eingeschränkt<br>– Schnellstmögliche Wiederherstellung ist erforderlich<br>– Wenige User sind betroffen | – Eine Störung sorgt für einen Teilausfall eines Rechnerverbundes oder einer Nicht-Verfügbarkeit eines (einzelnen) Mikroservices / einer Webapplikation, dadurch kommt es zu wesentlichen operativen Einschränkungen bspw. Funktionseinschränkungen |
| PRIO 3 | – Hauptfunktionen bleiben verfügbar<br>– Randfunktionen sind unterbrochen<br>– Der Vorfall ist ohne Verfügbarkeitseinschränkungen<br>– Sehr wenige bis keine User sind betroffen | – IT Probleme oder andere Services / Funktionen die zu Unterbrechungen im Hintergrund führen, oder zu unwesentlichen Unterbrechungen<br>– Bspw. kosmetische Fehler (Design / Layout) |

### 4.4.6 Service Level Agreements (Reaktions- und Bearbeitungszeiten)

Zeitraum von der Meldung des Fehlers bis zur ersten Reaktion und bis zur Wiederherstellung.

| | Kritisch | Schwer | Leicht |
|---|---|---|---|
| Erste Reaktion* | ≤ 15 Minuten (Einmeldung per Telefon)<br>≤ 30 Minuten (Einmeldung per Alert)<br>≤ 1 Stunde (Einmeldung per E-Mail) | ≤ 4 Stunden | ≤ nächster Arbeitstag |
| Bearbeitungzeit* | ≤ 4 Stunden (Prod System) | ≤nächster Arbeitstag | ≤ 3 Arbeitstage |

* innerhalb der gewählten AOT

**Definition:**

- **Reaktionszeit:**
  - Start: Eingang eines Service-Events
  - Ende: Eröffnung eines Tickets
- **Bearbeitungszeit / Wiederherstellungszeit:**
  - Innerhalb der Servicezeit kann der 2nd Level
    - einen Vorgang selbst lösen oder
    - tritt mit benannten Dritten in Kontakt.
  - Start: Ticket trifft in der Assignmentgroup des 2nd Level ein
  - Ende: Ticket wird geschlossen oder an Dritte übergeben

# 5 GLOSSAR

| **Abkürzung** | **Beschreibung** |
|---|---|
| AG | Auftraggeber |
| ALC | Application Live Check |
| AN | Auftragnehmer |
| AOT | Attended Operation Time |
| ASE | Application Service |
| ASU | Application Support |
| CI/CD | Continuous Integration/ Continuous Delivery |
| CNAO | Cloud Native Application Operation |
| KPI | Key Performance Indicator |