DocuSign Envelope ID: 46C267BD-AF3E-4C26-9F0C-BE4660600327

Order Form Nr. [redacted]
(„Order Form")

zwischen	**SAP Deutschland SE & Co. KG** Hasso-Plattner-Ring 7 69190 Walldorf (nachfolgend „SAP")
und	**Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit** Friedrichstraße 108 10117 Berlin (nachfolgend „BMG" oder „Auftraggeber")
Projekt-beschreibung	Entwicklung einer Corona Warn App
Datum	[redacted]
Anlagen	1. Scope Dokument 2. Servicebeschreibung für Innovative Business Solutions Development Services on Cloud 3. Servicebeschreibung für Innovative Business Solutions Development Support Services on Cloud 4. Allgemeine Geschäftsbedingungen für SAP Services der SAP Deutschland SE & Co. KG („AGB für Services") mit Ausnahme deren Anlage „Vereinbarung über die Datenverarbeitung für SAP Pflege und Professional Services Version 05-2018" („DPA"), anstelle derer die Anlage „Vereinbarung zur Auftragsverarbeitung" gilt 5. Muster Leistungsnachweis Erstellungsvertrag 6. Beschreibung Service Elements

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.

Ein vielversprechender Ansatz hierbei ist die Identifikation und Dokumentation relevanter Kontakte mittels Smartphone/ Bluetooth LE. Die Deutsche Telekom AG über Ihre Tochter T-Systems International GmbH ("Telekom") und SAP haben sich jeweils als Auftragnehmer bereiterklärt, die bisherigen Forschungsergebnisse in ein die vertraglich vereinbarten fachlichen Anforderungen sowie vertraglich vereinbarten 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 im Rahmen der vereinbarten Pflegeleistungen und ggf. auf Basis separater Beauftragungen mit weiteren gebotenen Nachentwicklungen auf Basis fachlicher Anforderungen voranzutreiben.

Vor diesem Hintergrund schließen SAP und der Auftraggeber diese Order Form als eine Vereinbarung für Leistungen, die den Allgemeinen Geschäftsbedingungen für SAP Services der SAP Deutschland SE & Co. KG („AGB für Services") einschließlich deren Anlage „Vereinbarung über die Datenverarbeitung für SAP Pflege und Professional Services Version 05-2018" („DPA") und den sonstigen Anlagen unterliegen. Übergeordnet zu dieser Order Form haben der Auftraggeber und der Telekom einen Vertrag über IT-Leistungen im Projekt Corona Warn App und die Parteien mit der Telekom eine dreiseitige Abstimmungsvereinbarung geschlossen ("Abstimmungsvereinbarung").

Inhalt

1. SAP Services

Die im Rahmen dieser Order Form gegenüber dem Auftraggeber zu erbringenden Leistungen setzen sich aus den Leistungen zusammen, die im vorliegenden Dokument, dem Scope Dokument und in den Servicebeschreibungen angegeben sind.

„Servicebeschreibung" bezeichnet die spezifischen Beschreibungen der Leistung(en), die dem Auftraggeber gemäß der vorliegenden Order Form erbracht werden, als Anlagen 3 und 4 beigefügt sind, als Teil dieser Order Form gelten und den Umfang der zu erbringenden Leistungen sowie weitere Einzelheiten detaillierter beschreiben.

„Scope Dokument" bezeichnet das Dokument, das dieser Order Form als Anlage 2 beigefügt ist, als Teil dieser Order Form gilt und den Umfang der zu erbringenden Leistungen sowie weitere Einzelheiten detaillierter beschreibt.

Die folgende Tabelle enthält eine Zusammenfassung der geltenden Servicebeschreibungen und Scope Dokumente für die im Rahmen dieser Order Form zu erbringenden Leistungen:

Servicebeschreibung	Scope Dokumente
Servicebeschreibung für Innovative Business Solutions Development Services on Cloud* (Anlage 3)	Scope-Dokument für Innovative Business Solutions Development Services on Cloud (Anlage 2)*
Servicebeschreibung für Innovative Business Solutions Development Support Services on Cloud (Anlage 4)	---

* "Innovative Business Solutions Development Services on Cloud" werden nachfolgend auch als "Development Services on Cloud" bezeichnet.

2. Vergütung und Zahlungsbedingungen

Zahlungen sind 30 Tage nach Zugang einer prüffähigen Rechnung fällig. Es wird kein Skonto gewährt. Der Rechnung sind bei Vergütung nach Aufwand von SAP unterschriebene Nachweise über die Leistungen und die ggf. weiteren geltend gemachten Kosten entsprechend Anlage 5 - Leistungsnachweis Erstellungsvertrag - beizufügen.

2.1 Nach Aufwand berechnete Leistungen

Der geschätzte Gesamtaufwand beträgt [redacted] Daraus ergibt sich eine geschätzte Vergütung in Höhe von 9.531.687,00 Euro (in Worten: Euro Neun Millionen Fünfhunderteinunddreißig Tausend Sechshundertsiebenundachtzig).

Service Element*	Tagessatz für Leistungen (in Euro)**	Geschätzte Anzahl an Tagen
High Value Design Services	[redacted]	
Special Development Services	[redacted]	
Project Management Services	[redacted]	

* Die Service Elements sind in Anlage 6 beschrieben.

** Bei den vertragsgegenständlichen Innovative Business Solutions Development Services on Cloud handelt es sich um marktgängige Entwicklungsleistungen. Bei den die Vergütungsgrundlage für diese Leistungen bildenden Tagessätzen, zu deren einheitlicher Anwendung SAP schon aufgrund allgemein anerkannter Rechnungslegungsgrundsätze verpflichtet ist, handelt es sich um Marktpreise im Sinne von § 4 Abs. 1 VO PR 30/53, hilfsweise um feste Sätze im Sinne von § 7 Abs. 2 VO PR 30/53.

Grundlage für diese Schätzung sind die der SAP vom Auftraggeber bereitgestellten Informationen und die Einschätzung des Projektumfangs durch SAP anhand der Informationen des Auftraggebers. Die geschätzte Vergütung, die Zeitpläne und der Umfang können Änderungen unterliegen, der gesamte tatsächliche Umfang der erbrachten Leistungen wird nach Zeit und Aufwand in Rechnung gestellt. Die Abrechnung nach Aufwand erfolgt nach Abnahme der Features auf der Grundlage einer in der Rechnung enthaltenen Aufstellung der Tätigkeiten. SAP informiert den Auftraggeber wöchentlich über den jeweils angefallenen Aufwand (Gesamtbetrag und Leistungsnachweise gemäß Muster in Anlage 5).

[redacted]

Ein Tagessatz bezieht sich auf acht (8) Arbeitsstunden (übliche Geschäftszeiten: Montag bis Freitag, 8:00 bis 17:00 Uhr). Mehrarbeit ist auf Stundenbasis zu vergüten.
Generell berechnet SAP für Einsätze an Wochenenden und Feiertagen (gesetzliche Feiertage sowie der 24. und 31. Dezember) sowie für Nachteinsätze (22:00 bis 6:00 Uhr) den 1,5-fachen Arbeitsstundensatz. SAP wird dem Auftraggeber Einsätze am Wochenende und an Feiertagen sowie Nachteinsätze für Leistungen, [redacted] erbracht werden sollen, im Voraus anzeigen; der Auftraggeber kann dem Einsatz aus berechtigtem Grund widersprechen. In diesem Fall sind die diesbezüglichen Nachteile (insb. Zeitverzögerung) vom Auftraggeber zu tragen.

Die vorstehend vereinbarte Vergütung nach Aufwand ist das Entgelt für den Zeitaufwand, Materialkosten, Reisekosten und sonstige Aufwendungen von SAP im Zusammenhang mit der

Leistungserbringung, die damit vollständig abgegolten sind. Vom Auftraggeber zu vertretende Wartezeiten von SAP werden wie Arbeitszeiten vergütet. SAP muss sich jedoch anrechnen lassen, was er durch die Nichterbringung seiner Leistung erspart oder durch anderweitige Verwendung seiner Dienste erwirbt oder zu erwerben böswillig unterlässt.

[redacted]

Leistungszeitraum

Die Leistungen mit Ausnahme der Innovative Business Solutions Development Support Services on Cloud werden ab dem [redacted] bis zur Abnahme der Features erbracht. Die Innovative Business Solutions Development Support Services on Cloud werden ab Abnahme der Features erbracht.

2.2 Vereinbarung eines Kontingents zur Umsetzung von zusätzlichen, bei Vertragsschluss nicht vereinbarten Anforderungen

SAP stellt dem Auftraggeber bis zum 31.05.2021 ein Kontingent an Innovative Business Solutions Development Services on Cloud gemäß nachfolgender Tabelle zur Verfügung, das für Leistungen, die nicht bereits gem. Abschnitt 2.1 und 2.2 dieser Order Form geleistet werden, einschlägig. Darunter fallen können bspw. erweiterte Funktionalitäten anhand neuer Bedarfslagen beim BMG, Umsetzung von Vorschlägen aus der Open Source-Community oder ähnliches. Der Auftraggeber ist nicht verpflichtet, die Leistungen aus dem Kontingent abzurufen.

Service Element	Tagessatz für Leistungen (in Euro)	Kontingent / Tage
High Value Design Services	[redacted]	
Special Development Services	[redacted]	
Project Management Services	[redacted]	

Eine Erhöhung des Kontingents oder Umverteilung der einzelnen Service Elemente kann, abweichend vom Change Request Verfahren (gem. Abstimmungsvereinbarung), nur einvernehmlich erfolgen. Der zuvor genannte Umfang an Services steht dem Auftraggeber im Rahmen des o.g. Zeitraums zur zur Verfügung. Die Konkretisierung des zu liefernden Scopes der Leistungen, sowie die Vereinbarung des konkreten Leistungszeitraums erfolgt über eine einvernehmliche Regelung entsprechend im Rahmen des Change Request Verfahrens gem. Abstimmungsvereinbarung.

2.3 Innovative Business Solutions Development Support Services on Cloud

Die Innovative Business Solutions Development Support Services on Cloud werden für die im Scope Dokument genannten Innovative Business Solutions Development Services on Cloud erbracht.

Die Jahresvergütung für Innovative Business Solutions Development Support Services on Cloud beträgt vorbehaltlich etwaiger Erhöhungen gemäß nachstehender Regelungen [redacted]% der für die Innovative Business Solutions Development Services on Cloud vereinbarten Vergütung, Projektsupport „Large Enterprise", die bis zur zur Abnahme der Features angefallen ist.

[redacted]

Bei den Innovative Business Solutions Development Support Services on Cloud sowie den Innovative Business Solutions Development Support Services on Cloud 24/7 On-Call Service handelt es sich um marktgängige Leistungen, für welche der vorstehende Prozentsatz als Marktpreis im Sinne von § 4 Abs. 1 VO PR 30/53 vereinbart wird.

Daher beträgt die jährliche Vergütung für Innovative Business Solutions Development Support Services on Cloud (inkl. 24/7 On-Call Service) auf Basis der geschätzten Vergütung (wie oben dargestellt, maßgeblich ist die tatsächliche endgültige Vergütung für die Innovative Business Solutions Development Services on Cloud):
1.906.716,00 EUR (in Worten: Euro Eine Million Neunhundertsechs TausendSiebenhundertsechzehn).

Soweit die vereinbarte Vergütung für die Innovative Business Solutions Development Services on Cloud, z.B. durch einen Änderungsantrag geändert wird, wird auch die Jahresvergütung für Innovative Business Solutions Development Support Services on Cloud und die Anzahl der Tage für die Durchführung von Verbesserungen, gemäß Kapitel 3.2.5 der Servicebeschreibung für Innovative Business Solutions Development Support Services on Cloud entsprechend angepasst.

[redacted]

Jede Vergütung wird jährlich mit Wirkung zum 1. Januar eines Kalenderjahres in Rechnung gestellt. Jede Vergütung, die vor dem 1. Januar fällig ist (vorliegend die Vergütung für die Innovative Business Solutions Development Support Services on Cloud für das laufende Kalenderjahr 2020), wird anteilig für das laufende Kalenderjahr in Rechnung gestellt.

[redacted]

„Lokale Geschäftszeit" bezeichnet die regulären Arbeitszeiten (Wochentage von Montag bis Freitag: 8:00 bis 17:00 Uhr MEZ) mit Ausnahme der gesetzlichen Feiertage in Walldorf (Baden-Württemberg), Deutschland, und des 24. und 31. Dezembers.

3. Änderungsmanagement (Change-Requests)

Für Veränderungen, die sich im Rahmen des Projektverlaufes ergeben, haben sich die Parteien in der Abstimmungsvereinbarung auf einen gemeinsamen Prozess mit der Telekom verständigt.

Ergeben sich im Rahmen des Projektverlaufes notwendige Veränderungen, die aus Sicht des Auftraggebers oder der SAP den Leistungsumfang, den Leistungsinhalt, Methoden oder Termine betreffen, sind diese auf Basis von schriftlich vereinbarten Änderungen bzw. Ergänzungen zu vereinbaren. Alle identifizierten Änderungen werden im Rahmen des Change Request-Verfahrens gemäß Abstimmungsvereinbarung dokumentiert und verfolgt.

4. Ort der Leistungserbringung / "EU Access"

Die Innovative Business Solutions Development Services on Cloud werden entsprechend Abschnitt 3.4. des Scope-Dokumentes erbracht.

Soweit SAP im Zusammenhang mit den Leistungen unter dieser Order Form Zugriff auf Echtdaten der Corona Warn App erhält, insbesondere im Zusammenhang mit Zugriffen auf das Produktivsystem oder Testsysteme, in denen Echtdaten verarbeitet werden, wird SAP gewährleisten, dass solche Zugriffe ausschließlich von Lokationen innerhalb des Europäischen Wirtschaftsraums oder der Schweiz erfolgen. SAP wird Echtdaten – auch soweit sie nur zu Testzwecken zur Verfügung gestellt werden – ausschließlich im Gebiet des Europäischen Wirtschaftsraums oder der Schweiz speichern.

5. Laufzeit der Order Form oder der Services

Die Laufzeit dieser Order Form endet mit Abschluss oder Beendigung aller von dieser Order Form abgedeckten Leistungen („Laufzeit"). Zur Klarstellung wird darauf hingewiesen, dass die Beendigung eines bestimmten Service keine Beendigung eines anderen im Rahmen der Order Form beauftragten Service nach sich zieht.

6. Besondere Bedingungen

6.1 Besondere Regelungen zu den AGB für Services

[redacted]

6.2 Zustimmung zur Veröffentlichung der Vertragseckdaten im Amtsblatt

SAP stimmt einer Veröffentlichung der Vertragseckdaten inklusive der vereinbarten Vergütung in einem Amtsblatt zu.

6.3 Sicherheitsprüfung

[redacted]

6.4 Einbindung Dritter in die Leistungserbringung

SAP darf zur Erbringung von Leistungen, die qualitativ oder quantitativ für die Werkleistungen wesentlich sind, Subunternehmer (vergaberechtlich Unterauftragnehmer genannt) nur einsetzen oder eingesetzte Subunternehmer nur auswechseln, wenn der Auftraggeber dem ausdrücklich zumindest in Textform zustimmt. Er wird unverzüglich zustimmen, wenn sich unter Berücksichtigung des neuen Subunternehmers anstelle des alten Subunternehmers keine andere Zuschlagsentscheidung ergeben hätte. Die Zustimmung gilt als erteilt, wenn der Auftraggeber dem Einsatz oder Austausch eines Subunternehmers nicht innerhalb einer Frist von 30 Tagen nach schriftlicher Mitteilung durch SAP widerspricht; Die Einarbeitung des neuen Subunternehmers erfolgt auf Kosten von SAP. Für nachfolgend genannten Sub-Prozessoren bzw. – soweit diese Eigenschaft gegeben - Subunternehmer gilt die Zustimmung des Auftraggebers als erteilt:

Projektleistungen:

- **Gesund Zusammen GmbH**, mit Sitz in Urbanstr. 1, 10967 Berlin, Deutschland
- **Insight Culture**, mit Sitz in Große Friedberger Str. 33-35, 60313 Frankfurt, Deutschland
- **Edelman GmbH**, mit Sitz in Niddastraße 91, 60329 Frankfurt, Deutschland
- **schöne neue kinder GmbH**, mit Sitz in Nymphenburger Straße 86, 80636 München, Deutschland
- **RA Schick** mit Sitz in Friedrich-Kahl-Str. 12, 60489 Frankfurt, Germany

Innovative Business Solutions Development Support Services on Cloud:

- **SAP România SRL**, Clădirea A1/LA, et. 2, Strada Tipografilor 11-15, București 013714, Rumänien
- **SAP Bulgaria Ltd.**, 136A, Tzar Boris III Blvd. 1618 Sofia, Bulgarien
- **SAP Ireland Limited**, Parkmore Business Park East, Brockagh, Parkmore, Galway, Co. Galway, Irland

Die vorstehende Regelung gilt auch für "Berater" im Sinne von Ziffer 1.3 der AGB für Services, sofern es sich nicht um Organe oder Angestellte von SAP oder eines der vorstehend genannten oder mit Zustimmung des Auftraggebers eingebunden Subunternehmers handelt.

6.5 Übertragung auf das Robert Koch-Institut

Der Auftraggeber wird zu Beginn des Projekts Corona Warn App vom Bundesministerium für Gesundheit vertreten. Der Auftraggeber kann die Durchführung der Order Form (im Sinne von Projektarbeit) jederzeit auf das RKI übertragen. Dies umfasst insbesondere auch die Wahrnehmung der Aufgaben nach der Abstimmungsvereinbarung und die Vertretung in den in Anlage 3 der Abstimmungsvereinbarung genannten Gremien.

SAP unterstützt die Übertragung der Durchführung der Order Form auf das RKI und wird insbesondere bestehende Dokumentation an das RKI übergeben und Vertreter des RKI in die Dokumentation einweisen sowie weitere Unterstützungsleistungen in angemessenem Umfang erbringen.

Der Auftraggeber kann verlangen, dass mit Übertragung der Durchführung der Order Form die Abrechnung von Leistungen von SAP mit dem Auftraggeber auf einen vom Auftraggeber benannten Stichtag abzugrenzen und für die Zeiträume vor und nach dem Stichtag gesondert abzurechnen ist.

6.6 Schutzrechte Dritter

[redacted]

[redacted]

6.8 Kündigung nach § 648 BGB

Der Auftraggeber hat bis zur Abnahme der Features das Recht, diese Order Form insgesamt gemäß § 648 BGB zu kündigen. Soweit nichts anderes vereinbart ist, hat SAP im Falle der Kündigung aufgrund dieser Regelung die gesetzlichen Rechte, ist jedoch verpflichtet, auf der Basis der durch die Kündigung ersparten Aufwendungen die von ihm beanspruchte Vergütung darzulegen. Der bis zur Kündigung erstellte Entwicklungsstand der Features und der Dokumentation ist auf Verlangen des Auftraggebers gem. Abschnitt 9.2 zu veröffentlichen. Des Weiteren ist SAP verpflichtet darzulegen, welche Leistungsteile SAP als fertig gestellt bzw. begonnen ansieht bzw. welche SAP bereits von Dritten erworben hat. SAP unterstützt den Auftraggeber auf dessen Wunsch gegen angemessene Vergütung in angemessener Weise so, dass der Auftraggeber oder ein Dritter die nach dieser Order Form vereinbarte Werkleistung fertig stellen kann, sofern dies für SAP nicht unzumutbar ist. Diese Unterstützungsleistung gilt als „Füllauftrag" im Sinne von § 648 BGB, soweit dies für SAP nicht unzumutbar ist.

6.9 Sonstiges

Sofern bereits zu einem früheren Zeitpunkt Vereinbarungen zum gleichen Leistungsgegenstand erstellt wurden, verlieren diese hiermit ihre Gültigkeit. Diese Order Form enthält abschließend alle Vereinbarungen der Vertragspartner über den Vertragsgegenstand. Schriftliche oder mündliche Nebenabreden zur vorliegenden Order Form sind nicht getroffen bzw. werden durch die Order Form gegenstandslos. Sollten bereits vor Unterzeichnung der Order Form Leistungen erbracht werden bzw. erbracht worden sein, so gelten hierfür die vorstehend genannten Konditionen. Dies gilt insbesondere für die Regelungen zur Vergütung.

Sollten einzelne Bestimmungen dieser Order Form unwirksam oder undurchführbar sein, berührt dies die Wirksamkeit der Order Form im Übrigen nicht. Die Vertragspartner sind in einem solchen Fall verpflichtet, eine unwirksame Bestimmung durch diejenige wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen am nächsten kommt.

Eigenschaften der Leistungen, technische Daten, Spezifikationen und Leistungsangaben in dieser Order Form oder ihren Anlagen sowie sonstigen vertragsrelevanten Dokumenten oder Beschreibungen dienen allein der Leistungsbeschreibung. Sie sind nicht als Garantie oder zugesicherte Eigenschaft zu verstehen.

Falls und soweit in Leistungsbeschreibungen „Garantien", „Gewährleistungen", „Zusicherungen", „zugesicherte Eigenschaften", „einstehen für" oder „Sicherstellungen" und von den vorgenannten Begriffen abgeleitete Begriffe vereinbart werden, stellen diese keine Garantie im Sinne des Gesetzes (insbesondere § 276 BGB) und keine zugesicherte Eigenschaft dar.
Die Vereinbarung von Eigenschaften oder sonstige Beschreibungen der Leistungsfähigkeit einer Leistung sowie die Verwendung der oben genannten Begriffe gelten nur dann und insoweit als Garantie im Rechtssinne, wie diese ausdrücklich und schriftlich in einer gesonderten Garantieurkunde zu diesem Vertrag als Garantie bezeichnet werden.

7. Nutzungsrechte, Verbreitungsrecht

[redacted]

7.2 Externe Dienstleister / Betrieb der Features

Der Auftraggeber darf Dritten Zugriff auf die Features, die Dokumentation und andere SAP-Materialien zum Zwecke der Bereitstellung von Anlagen-, Implementierungs-, System-, Anwendungsverwaltungs- oder Disaster-Recovery-Services sowie zur Weiterentwicklung und Pflege der Features für den Auftraggeber gewähren.

7.3 Verbreitungsrecht

SAP räumt dem Auftraggeber darüber hinaus das nicht-ausschließliche, einfache, weltweite, nicht-übertragbare Recht ein, die Features [redacted] Endnutzern zum Download und zur Nutzung zugänglich zu machen. [redacted]

Die Einhaltung der jeweils einschlägigen Regelungen [redacted] liegt in der Verantwortung des Auftraggebers und er gewährleistet wirkt darauf hin, dass das Robert Koch

Institut diese Regelungen einhält (SAP bleibt jedoch dafür verantwortlich, bei der Erstellung der Features die jeweils einschlägigen Regelungen zu beachten und die Features so zu erstellen, dass diese entsprechend dieser Ziffer 7.3 verbreitet werden können). [redacted]

7.4 Innovative Business Solutions Development Support Services on Cloud

Diese Ziffer 7 gilt – vorbehaltlich Abschnitt 8.3 dieser Order Form - für Arbeitsergebnisse, insbesondere Änderungen oder Erweiterung der Features oder der Dokumentation, entsprechend, die von SAP im Rahmen der Innovative Business Solutions Development Support Services on Cloud oder sonst im Zusammenhang mit dieser Order Form erstellt werden.

8. Rechte an geistigem Eigentum; Open Source

[redacted]

8.2 Open Source

SAP verpflichtet sich, den Source Code der Features einschließlich zugehöriger Dokumentation nach Maßgabe des folgenden auf GitHub unter der Apache 2.0 Lizenz zu veröffentlichen, um jeweils ein Code-Review durch die Open Source Community zu ermöglichen. Dabei stellt SAP die im Rahmen dieses Angebots erstellten Features sowie begleitende Architektur- und Fachdokumente unter Einhaltung der Apache 2.0 Open-Source-Lizenzregularien sowie der Best-Practices der Open-Source-Community über die gemeinsam mit der Telekom administrierte GitHub Organisation „Corona Warn App" zur Verfügung. Zusätzlich wird, gemeinsam durch SAP und der Telekom, eine GitHub Landing Page für das Projekt erstellt und eine öffentliche Website mit Basisinformationen zu dem Open Source Projekt und dessen Ansatz. Ziel ist die Herstellung von Transparenz gegenüber der interessierten Öffentlichkeit, sowie die Beteiligung der Open-Source-Community in Form von Reviews und Pull Requests (z.B. Korrektur- oder Verbesserungsvorschläge). [redacted] Der Umfang der veröffentlichten Dokumentation ist mit dem Auftraggeber jeweils vor Veröffentlichung abzustimmen.

8.3 Pull Requests

SAP nimmt Pull Requests nach Maßgabe der Contribution-Guidelines für das Open Source Projekt und die betreffenden Repositories entgegen. Wenn und soweit ein Pull Request Code enthält, der in den Source Code der Features übernommen wird, erfolgt die Einräumung der Nutzungsrechte gem. Ziffer 7.1. Abs. 2 unter den Bedingungen der Apache-2.0.

Der Auftraggeber beurteilt, ob der Pull Request in den Sourcecode der Features übernommen werden oder dort umgesetzt werden soll. Wenn und soweit die Übernahme oder Umsetzung des Pull Request eine Änderung gem. Abschnitt 3 (CR-Verfahren) erforderlich macht, findet Abschnitt 3 entsprechende Anwendung, wobei der Auftraggeber innerhalb einer der Anfrage angemessenen Frist mitteilen wird, ob er der Änderung zustimmt. Die Parteien sind sich einig, dass Pull Requests, die durch reine Fehlerbehebungen oder Bug Fixes umgesetzt werden können, nicht der Zustimmung des Auftragnehmers bedürfen.

8.4 Innovative Business Solutions Development Support Services on Cloud

Diese Ziffer 9 gilt für Arbeitsergebnisse, insbesondere Änderungen oder Erweiterung der Features oder der Dokumentation, entsprechend, die von SAP im Rahmen der Innovative Business Solutions Development Support Services on Cloud erstellt werden.

9. Sonstiges

9.1 Zusammenarbeit der Parteien / Ausschluss von Arbeitnehmerüberlassung und Scheinselbstständigkeit

SAP wird durch organisatorische Maßnahmen gewährleisten, dass die im Rahmen der Leistungserbringung eingesetzten Mitarbeiter ausschließlich deren Direktionsrecht und Disziplinargewalt unterstehen. Es erfolgt keine Eingliederung des zur Leistungserbringung eingesetzten Mitarbeiters der SAP in die Organisation des Auftraggebers oder in die Organisation eines anderen Projektbeteiligten. SAP bestimmt grundsätzlich Ort und Zeit der Leistung selbst. Jedoch sind zeitliche, räumliche und fachliche Anforderungen zu beachten, soweit sie sich aus den jeweiligen Verträgen ergeben oder in zwischen den Parteien abgestimmten Termin- oder Leistungsplänen enthalten oder zur Erreichung des Zwecks der Beauftragung erforderlich sind. Für die zur Erbringung der Leistungen notwendigen Arbeitsmittel ist SAP selbst verantwortlich, soweit nicht anders vereinbart.

[redacted]

-

Dem Auftraggeber ist es gestattet, vertrauliche Informationen, die er auf Grund der oben genannten Prüfungen erhält, solchen Prüfern zugänglich zu machen, die einen gesetzlichen Prüfauftrag wahrnehmen.

10. Rangfolge

Im Falle von Widersprüchen oder Abweichungen zwischen Bestimmungen der Dokumente gilt folgende Rangfolge:

1. Abstimmungsvereinbarung
2. Order Form
3. Scope Dokument (Anlage 1)
4. Spezifikation (Anhang 1 zum Scope Dokument)
5. Servicebeschreibung für Innovative Business Solutions Development Services on Cloud (Anlage 2)
6. Servicebeschreibung für Innovative Business Solutions Development Support Services on Cloud (Anlage 3)
7. Allgemeine Geschäftsbedingungen für SAP Services der SAP Deutschland SE & Co. KG („AGB für Services") mit Ausnahme deren Anlage „Vereinbarung über die Datenverarbeitung für SAP Pflege und Professional Services Version 05-2018" („DPA"), anstelle derer die Anlage „Vereinbarung zur Auftragsverarbeitung" gilt (Anlage 4)

Angenommen von:

SAP Deutschland SE & Co. KG (SAP)

DocuSigned by:

Name: ppa. Kirstin Graichen

Titel: [redacted]

Datum: [redacted]

DocuSigned by:

Name: ppa. Gabriele Spiess

Titel: [redacted]

Datum: [redacted]

Angenommen von:

Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit (Auftraggeber)

i.V.

Name:

Titel: St

Datum: 11.06.2020

Anlage 1

zu Order Form Nr. 49003196

Scope Dokument für Innovative Business Solutions Development Services on Cloud

Scope Dokument zur Order Form Nr. 49003196

Die SAP-Servicebeschreibung für Innovative Business Solutions Development Services on Cloud GERMAN v.2-2020 (nachfolgend: „Servicebeschreibung") ist integraler Bestandteil dieses Scope-Dokuments. Dieses Scope-Dokument ist Teil der Anlage 1 zur Order Form.

Inhalt

1. Projekt Scope

1.1 Methodology Lifecycle

1.1.1 SAP erbringt die Innovative Business Solutions Development Services on Cloud („Development Services on Cloud") gemäß der SAP Innovative Business Solutions Methodology Waterfall Lifecycle.

1.1.2 Die für die Entwicklung der Features maßgeblichen Spezifikationen sind in Anhang 1 dokumentiert (**"Spezifikation"**).

1.1.3 Die Allgemeinen Anforderungen gemäß Abstimmungsvereinbarung und die Spezifikation stellen – vorbehaltlich etwaiger über das Change Request-Verfahren vereinbarter Änderungen - die einzige rechtlich bindende Beschreibung der Features dar.

1.1.4 SAP bietet dem Auftraggeber an, bereits entwickelte Features zu demonstrieren, damit der Auftraggeber sein Feedback dazu abgeben kann („Präsentationen" oder „Show & Tell Sessions"). Die Projektmanager vereinbaren die Anzahl, den Umfang sowie die Zeitpläne für derartige Präsentationen.

1.1.5 Bis zur Abnahme aller Projektleistungen können beide Parteien schriftlich Änderungen an den Custom Development Services gemäß dem Change-Request-Verfahren anfordern.

1.1.6 SAP stellt die Features in der nicht produktiven Umgebung der Open Telekom Cloud (OTC), welche der Auftraggeber im Rahmen seiner Beistellleistungen bei der Telekom beschafft, des Auftraggebers bereit.

1.1.7 Der Abnahmeprozess ist in der Abstimmungsvereinbarung geregelt.

1.2 Entwicklungsumgebung und Cloud-Laufzeitumgebung (Base Cloud Services)

Der Auftraggeber hat die Entscheidung getroffen, dass die Features unter Zuhilfenahme der Entwicklungsumgebung der „Open Telekom Cloud, kurz: „OTC" entwickelt, gebaut (built) und verteilt (deployed) werden sowie von ihm dort ausgeführt werden. Der Auftraggeber ist für die Beschaffung und Verfügbarkeit der Entwicklungsumgebung und Cloud-Laufzeitumgebung verantwortlich, in der die Features entwickelt, gebaut, verteilt und ausgeführt werden sollen, sowie ggf. für zusätzliche Services/Tools, die für die Entwicklung, den Bau, die Verteilung und die Ausführung der Features erforderlich sind. Jegliche Änderungen an der betreffenden Entwicklungsumgebung und Cloud-Laufzeitumgebung unterliegen dem Change-Request-Verfahren.

Base Cloud Services und Base Cloud Support Services sind keine Voraussetzungen für die Leistungen im Zusammenhang mit diesem Scope Dokument; anderweitige Bestimmungen in den Servicebeschreibungen finden keine Anwendung.

Entwicklungsumgebung und Cloud-Laufzeitumgebung
Open Telekom Cloud (OTC)

1.3 Sprachen

Die vereinbarte Kommunikationssprache für das Projekt ist Deutsch. Die Projektdokumentation (wie z. B. Besprechungsprotokolle, Statusberichte usw.) wird in Deutsch zur Verfügung gestellt.

Die Spezifikation wird in Deutsch zur Verfügung gestellt.

Die Features werden in Deutsch zur Verfügung gestellt. Kommentare im Code werden nicht übersetzt.

1.4 Dokumentation der Lösung

SAP ist zur Dokumentation der Features verpflichtet und erstellt eine funktionale und technische SAP-Lösungsdokumentation, die dem Auftraggeber zusammen mit den Features bereitgestellt wird. Die Lösungsdokumentation wird gemäß Abstimmungsvereinbarung erstellt.

Die Dokumentation muss es dem für die Nutzung und Administration einzusetzenden Personal des Auftraggebers bzw. der Telekom ermöglichen, die Features ordnungsgemäß zu nutzen, sofern das Personal eine objektiv ausreichende Vorbildung und Ausbildung aufweist.

Die Lösungsdokumentation kann als Teil der Features und/oder in einem oder mehreren einzelnen Dokumenten bereitgestellt werden. Lösungsdokumentation, die nicht Teil der Features ist, wird im PDF-Format bzw. auf dem SAP Help Portal in Download-fähiger Form bereitgestellt. Die Lösungsdokumentation wird entsprechend den Regelungen in der Abstimmungsvereinbarung zur Verfügung stehen.

SAP dokumentiert die im Rahmen der Mängelhaftung und im Rahmen der Innovative Business Solutions Development Support Services on Cloud durchgeführten Maßnahmen.

SAP wird alle Anpassungen und Änderungen, die aufgrund von Maßnahmen im Rahmen der Mängelhaftung oder im Rahmen der Innovative Business Solutions Development Support Services on Cloud an den Dokumentationen erforderlich werden, in diese einarbeiten, soweit nichts anderes vereinbart ist. Soweit eine Einarbeitung SAP rechtlich nicht möglich ist, wird er eine entsprechende Ergänzung der Dokumentation zur Verfügung stellen.

An für den Auftraggeber erstellten Dokumentationen (einschließlich aller Aktualisierungen und Einarbeitungen) räumt SAP diesem die Rechte entsprechend der Order Form ein. Soweit Teile der Dokumentation der Open Source-Lizenz "Apache 2.0" unterliegen, räumt SAP dem Auftraggeber die Rechte gemäß dieser Open Source-Lizenz ein.

SAP teilt dem Auftraggeber auf dessen Anforderung in angemessener Frist, unabhängig davon spätestens jedoch bis zur Erklärung der Abnahme mit, welche für die Bearbeitung und Umgestaltung der Features notwendigen Werkzeuge SAP bei deren Erstellung verwendet bzw. entwickelt hat. SAP wird die Features so entwickeln, dass für deren Bearbeitung und Umgestaltung lediglich allgemein am Markt verfügbare Werkzeuge erforderlich sind.

1.5 Dokumentation in SAP Solution Manager

Nutzt der Auftraggeber SAP Solution Manager für die Dokumentation der Development Services on Cloud, wird der Inhalt vom Auftraggeber erstellt und gepflegt.

2. Projektzeitplan und Meilensteine

Das Projekt hat eine Laufzeit vom 24.04.2020 bis voraussichtlich 19.06.2020.

3. Projektorganisation

3.1 Rollen

Funktion	Teammitglied des Auftraggebers*	SAP-Teammitglied*
Projektmanager	zu bestimmen bei Projektbeginn	Martin Georg Fassunge

*Oder Mitarbeiter mit vergleichbaren Qualifikationen

3.2 Verantwortlichkeiten

Im Folgenden werden die wichtigsten Projektaktivitäten aufgeführt. Der Auftraggeber und SAP sind für die Ausführung ihrer jeweiligen Projektaktivitäten verantwortlich.

SAP ist für die folgenden Aufgaben verantwortlich:

- Erstellen und Aktualisieren des Projektplans in Zusammenarbeit mit dem Auftraggeber
- Organisieren von Workshops zur detaillierteren Ausarbeitung der Geschäfts- und Softwareanforderungen
- Erstellung der Spezifikation und Übermitteln an den Auftraggeber
- Organisieren der Prüfung von Dokumenten, wenn und soweit zwischen den Parteien vereinbart
- Entwickeln der Features und Erstellen der Lösungsdokumentation
- Mitteilung von Ort und Zeit des Integrationstests an den Auftraggeber mit angemessenem Vorlauf
- Durchführen des Integrationstests und Übermittlung der Ergebnisse (Testspezifikationen und Protokoll)
- Bereitstellung der Features zur Abnahme und Unterstützen des Abnahmetests gemäß Abstimmungsvereinbarung
- Bereitstellen der Features und der Lösungsdokumentation für den Auftraggeber
- SAP übernimmt im Aufttrag des Auftraggebers die folgenden Mitwirkungspflichten gegenüber dem Betreiber des Auftraggebers (derzeit T-Systems):
  - Teilnahme an der von T-Systems initiierten Abstimmung in Bezug auf die Definition der Überwachungsmetriken, KPIs, Definition der Runbooks spätestens 5 Tage vor Go-Live
  - Unterstützung des Cloud Application Operation Teams der Telekom beim Erstellen und der Pflege von Monitoring Dashboards und Alerting, was die notwendigen Metriken der Applikationen bzw. Services anbelangt. In diesem Zusammenhang definiert SAP Schwellwerte für die Erstellung von Alarmen/Events für die verschiedenen Applikationen/Services
  - Unterstützung der T-Systems in den Bereichen Change-Management und Deployment entsprechend der Anlage 2 zur Abstimmungsvereinbarung
  - Stellung des 3rd Level Supports, sowie Rufbereitschaft bei Incidents der Priorität 1 und 2 entsprechend der Anlage 2 zur Abstimmungsvereinbarung
  - Unterstützung bei Versionsupgrades der CI/CD Tools, sofern kundenspezifische Plugins installiert wurden
  - Verantwortung des Test-Prozesses bezogen auf die von SAP geschuldeten Leistungen innerhalb von Entwicklungs- und Testumgebung, sowie Bereitstellung von Backlog und Releasedokumentation, Lieferung von vollständigen und verständlichen Releasenotes
  - Lieferung der Scripte für das Deployment und für Rollback-Szenarien
  - Zur Verfügstellen einer angemessen robusten Applikationsarchitektur, um für eine dem Anwendungsbetrieb angemessene Verfügbarkeit der Features Sorge zu tragen
  - Bereithalten von Ansprechpartnern bzw. Meldewegen, damit die Telekom im Incident-Fall unmittelbar

benachrichtigen und die notwendigen weiteren Schritte abstimmen kann

- Lieferung der Datenschutz-Teilkonzepte für [redacted]
- Zulieferung zu CoronaWarnApp Dokumentationen für die Erstellung von Frage-/Antwort-Katalogen
- Zulieferung für die Bereitstellung von FAQs

- Leitung des Workstreams Open Source (OSS WS), was die folgenden Aufgaben umfasst:
  - Leitung und Koordination des OSS WS
  - Konzeption und Umsetzung der Veröffentlichungsprozesse
  - Überwachung der Einhaltung der Apache 2.0 Lizenzbedingungen
  - Lizenz-Analyse der genutzten Komponenten (Bill of Materials)
  - Unterstützung der Entwicklungsteams bgzl. Einhaltung der Open-Source Best-Pratices und Lizenzen
  - Administration der GitHub Organisation und der zugehörigen Repositories
  - Erstellung und Veröffentlichung von Compliance-Artefakten wie Lizenztexten und Notice-Files
  - Erstellung von Templates für Copyright Headers der Sourcecode-Dateien
  - 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 (z.B. Project Landing Page, FAQs)
  - Abstimmung mit allen relevanten Workstreams des Gesamtprogramms
- Verteilung der Features in die nicht produktive Cloud-Umgebung des Auftraggebers.

Der Auftraggeber ist insbesondere für die folgenden Aufgaben verantwortlich:

- Vor dem Projektstart:
  - Bereitstellen und Zugänglichmachen der Entwicklungsumgebung und Cloud- Laufzeitumgebung.
  - Bereitstellen und Zugänglichmachen der Cloud-Laufzeitumgebung für die Verteilung.
  - Benennen geeigneter Mitglieder für das Projektteam des Auftraggebers, die aktiv am Projekt mitwirken
- Teilnahme an Workshops zur detaillierteren Ausarbeitung der Geschäfts- und Softwareanforderungen, einschließlich Geschäftsprozessbeschreibungen
- Überprüfung und Bestätigung der Spezifikation
- Planung und Ausführung des Abnahmetests gemäß dem in der Abstimmungsvereinbarung vereinbarten Abnahmetestverfahren
- Abnahme der Features
- Teilnahme an Teammeetings und Telefonkonferenzen von SAP und dem Auftraggeber

Die Mitarbeit des Auftraggebers ist in allen Phasen des Projekts erforderlich und umfasst u. a. die oben aufgeführten Aufgaben. Der Auftraggeber identifiziert gegenüber SAP bestimmte Mitarbeiter als Ansprechpartner für technische Fragestellungen und als Teilnehmer beim Abnahmetest des Auftraggebers und gewährleistet, dass sie bei Bedarf für die Arbeit am Projekt zur Verfügung stehen. Der Auftraggeber gewährleistet, dass alle Mitarbeiter, die er für das Entwicklungsprojekt abstellt, kompetent und für die Ausführung ihrer Aufgaben hinreichend qualifiziert sind.
Sofern eine Mitwirkung des Auftraggebers nicht in zwischen den Parteien abgestimmten Zeitplänen festgehalten ist, hat SAP den Auftraggeber so rechtzeitig auf die zu erbringende Mitwirkung hinzuweisen, dass die vereinbarte Leistungserbringung nicht gefährdet wird. Sofern eine Mitwirkung des Auftraggebers nach Auffassung von SAP nicht oder nicht rechtzeitig oder nicht ordnungsgemäß erfolgt und diese für den Projekterfolg wesentlich ist, wird SAP den Auftraggeber hierauf hinweisen.

3.3 Mitwirkung des Auftraggebers

Der Auftraggeber erbringt die in diesem Scope Dokument und den Servicebeschreibungen aufgeführten Mitwirkungsleistungen und Beistellungsleistungen. Er wird SAP die erforderlichen Informationen und Unterlagen aus seiner Sphäre zur Verfügung stellen. Der Auftraggeber wird den Mitarbeitern von SAP Zugang zu seinen Räumlichkeiten und der dort vorhandenen informationstechnischen Infrastruktur gewähren, soweit dies zur Erbringung der Leistung erforderlich ist und die vertraglich vereinbarten persönlichen Voraussetzungen (z.B. Sicherheitsüberprüfungen nach Sicherheitsüberprüfungsgesetz - SÜG) erfüllt sind. Kommt der Auftraggeber seinen Mitwirkungsleistungen trotz Aufforderung durch SAP nicht, nicht rechtzeitig oder unvollständig nach, kann SAP ein Angebot unterbreiten, diese Leistungen selbst anstelle des Auftraggebers zu erbringen. Sonstige Ansprüche von SAP bleiben unberührt.

Verlangt SAP eine über die geschuldete Mitwirkung des Auftraggebers hinausgehende Leistung des Auftraggebers, kann der Auftraggeber es übernehmen, diese anstelle von SAP als eigene Mitwirkung zu erbringen; die für die Leistung zu zahlende Vergütung reduziert sich entsprechend. SAP ist jedoch verpflichtet, diesen Beitrag des Auftraggebers zu prüfen, ggf. zu korrigieren und in seine Leistungen zu integrieren. Die vertraglichen und gesetzlichen Ansprüche des Auftraggebers bleiben unberührt.

Der Auftraggeber hat Störungen bzw. Mängel unter Angabe der ihm bekannten und für deren Erkennung zweckdienlichen Informationen zu melden. Der Auftraggeber wird die Störungsmeldung in der Regel auf einem

zwischen den Parteien abzustimmenden Störungsmeldeweg vornehmen. Auf Nachfrage von SAP hat er im Rahmen des Zumutbaren bestimmte, in seine Sphäre fallende Maßnahmen zu treffen, die eine Feststellung und Analyse der Störung bzw. des Mangels ermöglichen, z.B. notwendige, mit zumutbarem Aufwand von ihm beschaffbare einzelne technische Informationen aus seiner Sphäre bereit zu stellen.

Der Auftraggeber wird SAP über von ihm veranlasste Änderungen an den Beistellungen informieren, sofern sich diese auf die vertraglichen Leistungen von SAP auswirken. Bei vereinbarten Pflegeleistungen wird der Auftraggeber SAP rechtzeitig über nicht von SAP vorgenommene oder initiierte Änderungen an den Features informieren, sofern sich diese auf die Erbringung der vertraglichen Leistungen von SAP auswirken. Diese Pflicht gilt unabhängig davon, ob der Auftraggeber zu einer solchen Änderung berechtigt ist. SAP wird den Auftraggeber über ihr bekannte nachteilige Auswirkungen dieser Änderungen unverzüglich unterrichten. Jeder Vertragspartner kann verlangen, dass der Vertrag entsprechend der Änderungen angepasst wird.

Die ordnungsgemäße Datensicherung der Produktivumgebung obliegt dem Auftraggeber.

[redacted]

Darüber hinaus liegt es in der Verantwortung des Auftraggebers für den ordnungsgemäßen Betrieb der Features über T-Systems nachfolgend genannte Infrastruktur bereit zu stellen, jeweils in 2 Lokationen und 3 Availibility Zones:

- Openshift
- High availability Postgress Datenbank
- Objectstore
- CDN
- Hashicorp Vault

Zudem wird der Auftraggeber dafür Sorge tragen, dass die Features inkl. der Nutzer der Features das Recht haben, auf die Webservices des Verification Servers, des Object Stores und das Content Delivery Network von T-Systems zuzugreifen.

3.4 Ort der Serviceerbringung und Remote-Zugriff

Die Development Services on Cloud werden am Standort von SAP erbracht.

Bestimmte Arbeiten, wie z. B. Projektmanagement, Workshops, Konzepterstellung und Testunterstützung, können in den Räumlichkeiten des Auftraggebers in Berlin oder an einem anderen zwischen den Parteien vereinbarten Ort stattfinden.

3.5 Projektsteuerung

Die Projektsteuerung ist in der Abstimmungsvereinbarung geregelt.

3.6 Projektleistungen

In der folgenden Tabelle sind die SAP-Projektleistungen aufgeführt. Projektleistungen sind „Arbeitsergebnisse", die einer Abnahme zugänglich sind.

Projektleistung	Beschreibung der Projektleistung	Abnahmekriterien
Spezifikation	Vgl. Servicebeschreibung	Vgl. 4.2
Features	Vgl. Servicebeschreibung	Vgl. 4.3
Dokumentation der Lösung	Vgl. 1.3	k. A.

4. Abnahme, Abnahmetests und Bestätigung

4.1 Allgemeines

4.1.1 SAP verlangt vom Auftraggeber eine schriftliche Abnahmeerklärung für alle Projektleistungen, die einer Abnahme zugänglich sind. Der Auftraggeber muss solche Projektleistungen ohne Verzögerung abnehmen. SAP kann dem Auftraggeber ein Abnahmeprotokoll zur Verfügung stellen.

4.1.2 [redacted]

4.1.3 Der Auftraggeber darf die Abnahme von Projektleistungen nicht aus unwesentlichen Gründen unbillig verweigern, verzögern oder ablehnen.

4.2 Abnahme der Features

4.2.1 Die Abnahme der Features ist in der Abstimmungsvereinbarung geregelt.

4.2.2 Die Abnahme hat förmlich zu erfolgen. Der Abnahme steht es aber gleich, wenn der Auftraggeber die Features nicht innerhalb einer ihm von SAP bestimmten angemessenen Frist abnimmt, obwohl er dazu verpflichtet ist.

5. Ergänzende Regelungen für Mängel

[redacted]

- Verbesserung der Features (Continuous Improvement – CI)
- 24/7 On-call-Service

[redacted]

6.1.1. Im Rahmen der Meldungsbearbeitung wird für jede Störung ein Incident über das SAP Ticketing System (BCP) in der Sprache Englisch angelegt. In der Meldungsbearbeitung werden sowohl Mängel der Features im CWA Backend, als auch in der eigentlichen App auf iOS und Android berücksichtigt. Die Meldungen werden entsprechend kategorisiert und priorisiert. Nach Analyse und Reproduktion des Fehlers durch entsprechende Experten wird eine Lösung, bzw. ein Workaround ermittelt und zur Verfügung gestellt. Details zum Meldungsbearbeitungsprozess inkl. Zusammenspiel Incident und Deployment sind im Abschnitt „3.2.4 Incident Handling" der Anlage „Supportkonzept" beschrieben.

[redacted]

6.1.3. Im Rahmen der Conflict Resolution wird durch SAP regelmäßig geprüft, ob es ein Update der Betriebssystem iOS oder Android einschließlich der von den Features verwendeten iOS- oder Android-API gibt. Ferner wird laufend überwacht werden, ob es Sicherheitsmeldungen, z.B. von CERT-Bund, zu Komponenten der Features gibt, auf die reagiert werden muss. Ferner wird überwacht, dass alle in den Features verwendeten Komponenten (auch die in kompilierter Form eingebundenen Komponenten) stets auf dem aktuellen Patch- bzw. Update-Stand sind. SAP untersucht dann entsprechend den Impact und das Risiko und plant eine entsprechende Migration. Nach Absprache mit den Verantwortlichen erfolgt danach die Realisierung und das Ergebnis wird dem Auftraggeber zur Abnahme vorgelegt. Zur Klarstellung: diese Leistungen setzen vorhandene und aktuelle Schnittstellen seitens Apple und Google voraus. Darüber hinaus werden im Rahmen der Conflict Resolution auch Bugfixes zur Verfügung gestellt und Stabilisierungsmaßnahmen der Features vorgenommen. [redacted]

6.1.4. Beim Community Management werden durch die SAP Community Manager folgende Aktivitäten durchgeführt:

- Gemeldete Code Issues der Community (Github) aus den einzelnen Streams aufgreifen und Entwicklern der SAP zum Review weitergeben
- Von Community (Github) bereitgestellte Bugfixes entgegennehmen und zum Review&Aufnahme in die bestehenden Features weitergeben
- Feature Requests / Optimierungen aufgreifen und mit Product Ownern/Entwicklern der SAP besprechen und ggf. den Change Request Verfahren (6.1.2) anstoßen
- Feedback der Community (Github) einarbeiten und moderieren
- Feedback der Appstores konsolidieren und mit SAP-Entwicklungsteams teilen
- Roadmap Kommunikation mit Community (Github)
- Moderation Community (Github)

6.1.5. Beim Prozess der Verbesserung der Features (Continuous Improvement – CI) geht es darum Verbesserungen der von SAP im Rahmen der jeweiligen Development Services on Cloud ausgelieferten Features zu ermöglichen. Diese werden üblicherweise im Rahmen des Change Request Verfahren oder Community Management-Prozesses identifiziert. SAP analysiert die Anforderungen und informiert den Auftraggeber innerhalb eines angemessenen Zeitraums darüber, ob die Verbesserung der Features, unter Berücksichtigung der noch verbliebenen Tage für Verbesserungen, realisiert werden können. SAP unterbreitet dem Auftraggeber einen Lösungsvorschlag und eine Aufwandsschätzung (nachfolgend als „Realisierungsangebot" bezeichnet) für die Anpassung der Features. Nachdem der Auftraggeber das Realisierungsangebot akzeptiert hat, nimmt SAP die Verbesserung der Features vor und dokumentiert die hierfür notwendigen Verbesserungstage.

[redacted]

Weitere Details zu den Development Support Services on Cloud sind in Anlage 2 zur Abstimmungsvereinbarung geregelt.

[redacted]

[redacted]

6.3 Mängelhaftung bei Pflegeleistungen

Sind die Pflegeleistungen mangelhaft erbracht, gelten die Regelungen zu Mängeln entsprechend. An Stelle des Rücktritts tritt das Recht auf Kündigung der Development Support Services on Cloud.

6.4 Dokumentation der Pflegeleistungen

SAP dokumentiert die durchgeführten Pflegeleistungen in angemessener Art und Weise, soweit nichts anderes vereinbart ist.

[redacted]

Zu Absatz 6 des Abschnitts 4.2 der SAP-Servicebeschreibung Innovative Business Solutions Development Support Services on Cloud vereinbaren die Parteien, dass dieser nur vorbehaltlich der Bestimmungen zum Datenschutz und zur Datensicherheit gilt; Einschränkungen, die sich aufgrund der Features selbst ergeben, sind von SAP hinzunehmen.

[redacted]

7. Change-Request-Verfahren

Das Change-Request-Verfahren ist in der Abstimmungsvereinbarung geregelt. Ziffer 4 der AGB für Services findet keine Anwendung.

8. Annahmen und Ausschlüsse

Die folgenden Annahmen und Ausschlüsse gelten zusätzlich zu jenen, die im Abschnitt Annahmen und Ausschlüsse der Servicebeschreibung aufgeführt sind. Abweichend hiervon kann SAP nicht einseitig weitere Annahmen oder Ausschlüsse aufnehmen.

Alle Aspekte oder Services, die nicht in diesem Scope-Dokument als im Projektumfang der Development Services on Cloud enthalten definiert sind, gelten als nicht im Projektumfang inbegriffen. Dazu zählen insbesondere die folgenden Ausschlüsse:

- Projektleistungen, die nicht explizit im Scope-Dokument angegeben sind
- Analyse von Ist-Geschäftsprozessen
- Inhalte für und Durchführung von Schulungen, die nicht explizit im Scope-Dokument angegeben sind
- Die zu entwickelnde Anwendung basiert auf dem Exposure Notification Framework, das von Apple und Google zur Verfügung gestellt wird. Für den Betrieb der App ist die Verfügbarkeit dieses Exposure Notification Frameworks zwingend erforderlich.

Anhang 1
Spezifikation

Spezifikation

Corona-Warn-App

Dokumentenversion: 1.1 – Endgültige Version
Datum: 5. Juni 2020

Vertraulich

THE BEST RUN SAP

Historie

Version	Datum	Kommentar
1.0	3. Juni 2020	Initiale Version
1.1	5. Juni 2020	Kapitel 3 Projektumfang: Update auf Basis des zugrundeliegenden GitHub-Dokuments *Scoping Dokument* Kapitel 4 Architektur: Referenz auf das GitHub-Dokument *Solution Architecture*

Inhalt

Abbildungsverzeichnis

1 Informationen zum Dokument

Diese Spezifikation ist die Grundlage für die Entwicklungen, die durch SAP vorgenommen werden. Sie beschreibt den Leistungsumfang, der durch SAP im Rahmen des Projektes bereitgestellt wird.

1.1 Glossar

Das Glossar zur Corona-Warn-App ist öffentlich auf GitHub einsehbar:
https://github.com/corona-warn-app/cwa-documentation/blob/master/glossary.md

2 Geschäftlicher Kontext

Hinweis

Dieses Kapitel stellt allgemeine Hintergrundinformationen zur Verfügung. Konkrete Anforderungen an die Software sind in Kapitel 3 Projektumfang spezifiziert.

2.1 Einleitung

Ziel der Corona-Warn-App ist es, SARS-CoV-2-Infektionsketten schnellstmöglich zu erkennen und zu durchbrechen. Personen sollen zuverlässig und schnell über Begegnungen mit anderen infizierten Personen und damit mögliche Übertragungen des Virus informiert werden, damit sie sich freiwillig isolieren können, um damit zu einer Eindämmung der SARS-CoV-2-Pandemie beizutragen.

Dieses Dokument beschreibt die funktionalen Anforderungen an die Gestaltung der App aus einer fachlichen und prozessualen Sicht. Die Beschreibung ist in der aktuellen Version inhaltlich auf das erste Release begrenzt und eine initiale Version.

In der Gesamtplanung ist die Veröffentlichung weiterer Dokumente aus der Entwicklung vorgesehen, um frühzeitig Rückmeldungen zu erhalten und gegebenenfalls aufzunehmen. Nachfolgend werden zunächst das Release-Architektur-Dokument sowie der Backend-Source-Code alpha verfügbar gemacht.

Die Definition und Gliederung der Anforderungen folgen einer personenzentrierten Methodik. Dabei erfolgt die Gestaltung des gesamten Prozessablaufs aus Sicht derjenigen, welche die App nutzen, bzw. der im Prozess eingebundenen Stakeholder. Das Ziel ist es, die Bedürfnisse aller genannten Beteiligten so abzubilden, dass eine hohe Akzeptanz erreicht wird und die jeweiligen Funktionen intuitiv bedienbar sind.

Anhand einer User Journey (Nutzungsreise) sind die Interaktionspunkte und das Erlebnis während der Nutzung aufgezeigt. Die daraus entstehenden Anforderungen werden sogenannten Epics (Beschreibung einer Anforderung auf einer hohen Abstraktionsebene) zugeordnet. Die Epics beschreiben die einzelnen Kontakt-Ereignisse sowie übergreifende Funktionalitäten im gesamten Prozess, die für die Nutzung und Akzeptanz der App erforderlich sind. Aus den Epics heraus werden die detaillierten Anforderungen in Form sogenannter User Stories (eine in Alltagssprache formulierte Software-Anforderung) abgeleitet. Die einzelnen Anforderungen werden so strukturiert in den Entwicklungsprozess gebracht.

2.2 User Journey

2.2.1 Beschreibung der Nutzungsprofile (Stakeholder)

Folgende wesentliche Nutzungsprofile bzw. Stakeholder sind in die User Journey bzw. in den Gesamtprozess eingebunden und in ihrer Rolle beschrieben:

App-Bedienung

Alle Personen, welche die App benutzen: Werden über mögliche Begegnungen mit infizierten Personen informiert, verifizieren eigene Testergebnisse bzw. warnen dann alle Personen, denen sie begegnet sind, freiwillig und pseudonym.

Hotlines

Unterstützen Personen bei der Bedienung der App in der Beantwortung von Fragestellungen zur Nutzung der App, zur Technik sowie zum Datenschutz und geben auf Nachfrage verhaltensbezogene Informationen sowie weitere Informationsmöglichkeiten im Kontakt- bzw. Infektionsfall weiter. Unterstützen bei Verifikation und Freischaltung von Testergebnissen in der App für infizierte Personen und können diesen die Kontaktaufnahme mit dem zuständigen Gesundheitsamt empfehlen.

Robert Koch-Institut (RKI)

Stellt epidemiologische Informationen und Handlungsempfehlungen für die Bedienung der App zur Verfügung (Content). Bestimmt die Parameter für die Messung der Kontakte (im Rahmen der technischen Möglichkeiten durch die API).

2.2.2 User Journey

Die Nutzung der App wird aufgrund von nacheinander stattfindenden Kontakt-Ereignissen und Interaktionen von Personen in verschiedene Phasen eingeteilt. Zu jeder Phase sind den Personen Motivationen oder Anforderungen zugeordnet, die ihre Erwartungen an die Funktionsweise erfüllen und intuitiv durch den Prozess leiten.

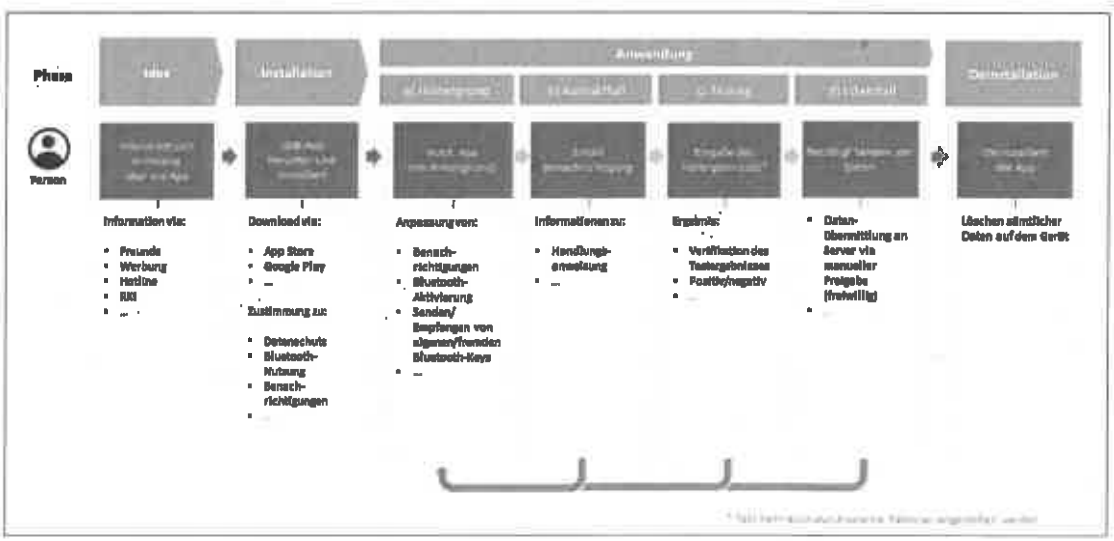


Abbildung 1: User Journey

Phase Idee

In dieser Phase entscheidet eine Person, sich über die App zu informieren. Das kann über unterschiedliche Quellen erfolgen. In dieser Phase haben die Personen ggf. verschiedene Fragestellungen zur Nutzung der App (Anwendung, Datenschutz, Barrierefreiheit etc.). Diese sollen bereits vor dem Download beantwortet werden können (Hotline, Informationen auf Internetseiten des RKI und des BMG, App Store/Google Play Store).

Phase Installation

Eine Person entscheidet sich zum Download der App (App Store/Google Play Store) und wird nach der technischen Installation beim erstmaligen Öffnen der App durch eine Einführung begleitet. In der Einführungsphase erhält die Person eine Übersicht über die Funktionsweise, Nutzungsbedingungen und Datenschutzbestimmungen sowie erforderliche Einwilligungen, Einstellungen und Benachrichtigungen.

Phase Anwendung

Die Phase der Anwendung ist in vier weitere Bereiche unterteilt, in welchen die Person unterschiedliche Bedürfnisse hat.

1. **Hintergrund**
   Im Ruhezustand (Idle Mode) des Mobiltelefons läuft die Anwendung im Hintergrund und speichert für die Person automatisiert und verschlüsselt die in der Nähe befindlichen Pseudo-IDs anderer Personen anhand definierter Parameter über Entfernung und Dauer des Kontaktes. In regelmäßigen Abständen holt sich die App vom Server eine Liste der Pseudo-IDs der sich freiwillig infiziert gemeldeten Personen und vergleicht diese mit den gespeicherten Pseudo-IDs im Gerät, um einen möglichen Kontakt zu ermitteln.
2. **Kontaktfall**
   Im festgestellten Kontaktfall zu infizierten Personen erhält die Person jeweils eine Benachrichtigung und verhaltensbezogene Empfehlungen. Hier kann zum Beispiel die Kontaktaufnahme mit ärztlichem Fachpersonal, mit dem zuständigen Gesundheitsamt und/oder die freiwillige häusliche Isolation empfohlen werden.
3. **Testing**
   Im Fall eines durchgeführten Tests auf eine SARS-CoV-2-Infektion kann die Person über die App den digitalen Testinformationsprozess starten und damit über das ermittelte Testergebnis benachrichtigt werden.
4. **Infektfall**
   Im Fall eines positiven SARS-CoV-2-Befunds kann eine Person freiwillig die in der App gespeicherten eigenen pseudonymen Warn-IDs veröffentlichen, damit andere Personen, die die App nutzen, auf ihrem eigenen Smartphone abgleichen können, ob sie mit der infizierten Person in Kontakt standen.

Phase Deinstallation

Eine Person kann die App jederzeit deinstallieren. Alle in der App gespeicherten Daten werden vollständig gelöscht.

3 Projektumfang

3.1 Abgrenzung der Leistungen der Parteien

3.1.1 Übersicht zur Leistungsabgrenzung

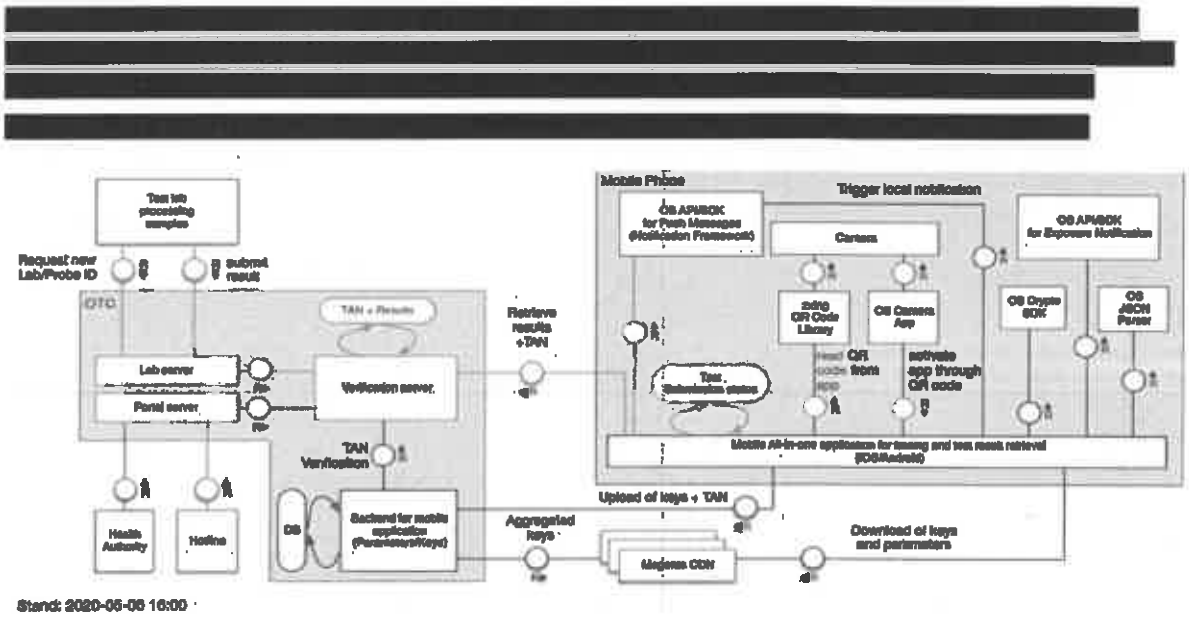


Abbildung 2: Leistungsbereiche der Industriepartner

3.1.2 Aufgaben und Leistungsumfang der SAP

Die Leistungen der SAP umfassen:

- Design und Entwicklung der Corona-Warn-App (IOS und Android); basierend auf einem neuen SDK, das von Apple und Google zur Verfügung gestellt wird und als Exposure Notification Framework bezeichnet wird,
- Entwicklung des Backends zur Entgegennahme von Upload-Anfragen der Clients (Tracing Server); Übergabe von Konfigurationsparametern an die mobilen Anwendungen und Zusammenfassung der Diagnoseschlüssel in Blöcke,
- Publizieren der wesentlichen Projektbestandteile als Open Source auf GitHub.

3.1.3 Aufgaben und Leistungsumfang der T-Systems

Die Leistungen der T-Systems ergeben sich aus T-Systems-Vertrag. Diese umfassen insbesondere:

- Die Entwicklung und den Betrieb des Verifikationsservers, des Lab Servers sowie des Portal Servers innerhalb des Prozesses zur Verifizierung / Falsifizierung einer gemeldeten Infektion,
- Betrieb des Backends zur Entgegennahme von Upload-Anfragen der Client (Tracing Server),
- Bereitstellung einer Managed „Platform as a Service" (PaaS),
- Hotline Service.

3.2 Abgrenzung zum Scoping Document auf GitHub

Die nachfolgenden Kapitel entsprechen wortgenau dem deutschen Scoping Document der Corona-Warn-App (Stand: 05.06.2020), welches öffentlich auf GitHub einsehbar ist:

https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/scoping_document.de.md

3.3 Übersicht der Epics

Die Funktionen der App sind in Prozessphasen der Nutzung (mit direktem Bezug zur User Journey) und übergreifende Unterstützungsprozesse unterteilt. Eine Übersicht der Epics ist nachfolgend dargestellt:

3.3.1 Prozessphasen der Nutzung

#	Epic	Beschreibung
1	Anbahnung und Installation (Onboarding-Prozess)	Sämtliche Prozesse, die insbesondere bei erstmaliger Nutzung der App erfolgen (z.B. Zustimmung Datenschutz, Sprachauswahl)
2	Informationen und Instruktionen zur Nutzung der Applikation	Hilfestellungen zur Nutzung der App (z.B. Anwendungshandbuch, Tutorial) sowie Informationen zum Impressum der App
3	Nutzung im Regelprozess	Funktionen der App im "Idle mode" (z.B. Aktivierung/Deaktivierung, Anpassung von Einstellungen, Überwachung von App-Aktivität)
4	Kontaktfall (Begegnung mit infizierter Person)	Funktionen rund um Kontaktpunkte (z.B. Benachrichtigungen, Handlungsempfehlungen).
5	Covid-19-Testergebnismeldung	Funktionen im Zusammenhang mit der Testergebnismeldung
6	Auslösung einer Warnung	Prozess zur Auslösung einer Warnung im Falle eines positiven Testergebnisses

3.3.2 Supportprozesse

#	Epic	Beschreibung
7	Parametrisierung	Parameter der Kontaktpunktdefinition
8	Technische Unterstützung	Support-Prozesse (z.B. Hotlines)
9	Barrierefreiheit	Apps von Trägern öffentlicher Gewalt müssen dem Behindertengleichstellungsgesetz (BGG) nach barrierefrei sein (§ 12). Apps sollen von allen Menschen mit Behinderungen bedient werden können.
10	Content-Management	Zur Anpassung und Aktualisierung von Inhalten in der App (Texte, Links, Hotlines etc.)

3.4 Übersicht der User Stories

Die Anforderungen an die Corona-Warn-App, die den fachlichen Umfang der Anwendung definieren, sind nachfolgend in der üblichen Form aus Sicht der nutzenden Personen formuliert, sofern nicht anders angegeben:

„Als <Stakeholder> möchte ich <Handlung durchführen>, um <gewünschtes Ergebnis zu erzielen>."

Die zugehörigen Akzeptanzkriterien ergänzen die Spezifikation der Anforderungen, indem sie Bedingungen definieren, die die Software erfüllen muss, um die Bedürfnisse der nutzenden Personen zu befriedigen.

3.4.1 Anbahnung und Installation (Onboarding-Prozess)

# User Story ID	User Story	Akzeptanzkriterien
E01.01	Als Person, die die App nutzt, möchte ich beim erstmaligen Start der App eine Einleitung zur Funktionsweise der App erhalten (App-Motivation).	1. Einführung in die Funktionsweise der App wird bei erstmaligem Start der Applikation angezeigt. 2. Einführung in die Funktionsweise der App wird bei weiteren Startvorgängen nicht angezeigt. 3. Die erklärenden Inhalte sind in den jeweiligen Funktionsbereichen zur Nutzung vorhanden.

E01.02	Bei der Nutzung der App möchte ich beim erstmaligen Start der App über die Nutzungsbedingungen und Datenschutzbestimmungen (Data Protection Screen) informiert werden und meine Zustimmung geben, um über den Umgang mit meinen Daten innerhalb der Anwendung aufgeklärt zu sein.	1. Mit Nutzung der App akzeptiert die Person die Nutzungsbedingungen und Datenschutzbestimmungen. 2. Die Nutzungsbedingungen sind innerhalb der App einsehbar. 3. Die Abfrage erfolgt nur bei der erstmaligen Nutzung.
E01.03	Als Person, die die App nutzt, möchte ich bei der erstmaligen Nutzung der App gefragt werden, ob ich der Erstellung pseudonymer IDs und deren Aussendung an Geräte in meiner Nähe durch die App zustimme, damit ich über die Funktionsweise der App informiert bin.	1. Eine Bestätigung der Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe durch die App ist Voraussetzung für die Nutzung der entsprechenden Funktionalitäten zur Risiko-Ermittlung. 2. Nach der erstmaligen Nutzung erfolgt die Abfrage nicht.
E01.04	Bei der erstmaligen Nutzung der App möchte ich gefragt werden, ob die App auf die Bluetooth-Funktion des Smartphones zugreifen darf, damit ich die mobiltelefonseitige Nutzung der App kontrollieren kann.	1. Diese User Story ist gleichbedeutend mit E01.03. Die Berechtigung zur Nutzung der Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe beinhaltet die Nutzung von Bluetooth Low Energy (BLE) bereits. 2. Die Einstellungen für die generellen Bluetooth-Funktionalitäten sind nur in den Systemeinstellungen möglich.

E01.05	Bei der erstmaligen Nutzung der App möchte ich gefragt werden, ob die App mir Benachrichtigungen schicken darf, damit in verschiedenen Situationen Push-Notifications ausgegeben werden können.	1. Eine Abfrage zu den Benachrichtigungseinstellungen der App findet vor der erstmaligen Nutzung statt. Es können damit lokale Benachrichtigungen erhalten werden. Echte Push-Notifications von externen Servern werden nicht unterstützt (APNs/GCM). 2. Nach der erstmaligen Nutzung erfolgt die Abfrage nicht.
E01.06	Als Person, die die App nutzt, möchte ich bei der erstmaligen Nutzung der App meine Sprache angezeigt bekommen, damit die Nutzung der App für mich verständlich ist.	1. Erkennung der eingestellten Systemsprache wird durchgeführt. 2. Wenn die erkannte Systemsprache nicht im Content hinterlegt ist, wird im Default Englisch ausgewählt. 3. In der ersten Version der App ist Mehrsprachigkeit vorgesehen.
E01.07	Als Person, die die App nutzt, möchte ich bereits während des Onboardings Hilfen und Einstellungen zur Barrierefreiheit bekommen, um die App nutzen zu können.	1. Die Barrierefreiheit wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems genutzt.

3.4.2 Informationen und Instruktionen zur Nutzung der App

# User Story ID	User Story	Akzeptanzkriterien
E02.01	Als Person, die die App nutzt, möchte ich Zugriff auf eine FAQ-Liste haben, um mir bei Fragen zur App selbst weiterhelfen zu können.	1. Es wird entweder ein Link auf eine Internetseite mit FAQs zur Verfügung gestellt, oder die Internetseite integriert innerhalb der App dargestellt.
E02.02	Als Person, die die App nutzt, möchte ich Zugriff auf eine Anleitung haben, um die App und ihre Funktionen zu verstehen.	1. Eine entsprechende Erläuterung der verschiedenen Funktionalitäten der App wird bereitgestellt.
E02.03	Als Person, die die App nutzt, möchte ich Zugriff auf ein Erklärvideo haben, um die App und ihre Funktionen zu verstehen.	1. Videos werden nicht in der App eingebettet, können aber beispielsweise über die FAQs zur Verfügung gestellt werden.
E02.04	Als Person, die die App nutzt, möchte ich das Impressum der App einsehen können, um zu sehen, wer für die Entwicklung und Inhalte der App verantwortlich ist.	1. Es gibt ein Untermenü "Impressum" 2. Das Impressum beinhaltet die üblichen Angaben zur Impressumspflicht.
E02.05	Als Person, die die App nutzt, möchte ich Nutzungsbedingungen und Datenschutzinformationen jederzeit einsehen können.	1. Die App bietet einfachen Zugriff auf Nutzungsbedingungen und Datenschutzinformationen.

E02.06	Bei der Nutzung der App möchte ich die verschiedenen Hotlines zu technischen, datenschutzbezogenen, gesundheitsbezogenen und psychologischen Fragestellungen sowie zur Verifikation eines Testergebnisses angezeigt bekommen, damit ich weitere Informationen oder Antworten auf Fragen erhalte.	1. Die App bietet einen Zugriff auf eine technische Hotline und eine Hotline zur Erlangung einer Telefon-TAN. 2. Die zeitliche Erreichbarkeit der Hotlines (z.B. 24/7) wird angezeigt. 3. Telefonnummern können direkt aus der App gewählt werden.

3.4.3 Nutzung im Regelprozess

# User Story ID	User Story	Akzeptanzkriterien
E03.01	Als Person, die die App nutzt, möchte ich die App aktivieren und deaktivieren können, um die Funktion ein- und auszuschalten.	1. Die Funktionalität zur Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe kann ein- und ausgeschaltet werden. 2. Die Konsequenzen des Ein-/Ausschaltens werden erklärt.

E03.02	Als Person, die die App nutzt, möchte ich die App in den Auslieferungszustand zurücksetzen können, damit ich sie neu konfigurieren kann.	1. Die App kann über eine Einstellung in den Auslieferungszustand zurückgesetzt werden. Die gespeicherten Traces müssen über die Systemeinstellungen gelöscht werden.
E03.03	Bei der Nutzung der App möchte ich die Applikationseinstellungen (Zugriffsrechte, z.B. Benachrichtigungen) in einem Menü anpassen können, um Funktion und Zugriffe der App verwalten zu können.	1. Ein Menü zu App-Einstellungen kann durch die nutzende Person aufgerufen werden. 2. Die Benachrichtigungen können ein- und ausgeschaltet werden. 3. Der Zugriff auf die Funktionalität zur Erstellung pseudonymer IDs und deren Aussendung an Geräte in der Nähe kann ein- und ausgeschaltet werden. 4. Vor der Deaktivierung der Zugriffsrechte erhalte ich Informationen darüber, welche Funktionen der App dadurch nicht mehr (vollumfänglich) funktionieren.

3.4.4 Kontaktfall (Begegnung mit infizierter Person)

# User Story ID	User Story	Akzeptanzkriterien
E04.01	Bei der Nutzung der App möchte ich informiert werden, wenn eine Person, zu der ich Kontakt hatte, sich als infiziert gemeldet hat. Damit kann ich geeignete Maßnahmen treffen, um die Verbreitung des Virus zu stoppen.	1. In Abhängigkeit der Benachrichtigungseinstellung schickt die App eine Benachrichtigung an die nutzende Person. 2. Bei einer Änderung der Risikoeinschätzung für die nutzende Person informiert die Benachrichtigung die nutzende Person über Neuigkeiten in der App. Die tatsächlich geänderte Risikoeinschätzung wird erst innerhalb der App angezeigt.
E04.02	Als Person, die die App nutzt, möchte ich im Kontaktfall Handlungsanweisungen durch die App bekommen, um mein Verhalten an die Empfehlungen des RKI anzupasse	1. Die Benachrichtigung führt die nutzende Person zur App. Handlungsempfehlungen des RKI sind in der App statisch hinterlegt.

3.4.5 Covid-19-Testergebnismeldung

# User Story ID	User Story	Akzeptanzkriterien
E05.01	Als RKI möchte ich, dass ausschließlich positiv getestete Personen einmalig eine Warnung auslösen können, um Missbrauch zu vermeiden.	1. Nur positive Tests können eine Warnung auslösen. Der Verifikationsserver und die Hotline zum Telefon-TAN Verfahren stellen dies sicher. 2. Für jeden Test kann nur einmal eine Warnung ausgelöst werden.
E05.02	Bei der Nutzung der App möchte ich im Falle eines positiven Testergebnisses Informationen über die Erkrankung und nötige nächste Schritte bekommen, um mein Verhalten an die Handlungsempfehlungen des RKI anpassen zu können.	1. Eine Benachrichtigung informiert lediglich über Neuigkeiten in der App. Das Testergebnis selbst kann nur in der App eingesehen werden. 2. In der App wird ein Infotext mit definiertem Inhalt angezeigt (z.B. Informationen zum Ausgang des Testergebnisses, Informationen über erforderliche Maßnahmen, eine Hotline-Nummer).

3.4.6 Auslösen einer Warnung

# User Story ID	User Story	Akzeptanzkriterien
E06.01	Als Person, die die App nutzt, möchte ich einen vom medizinischen Fachpersonal oder Test-Center ausgehändigten QR-Code scannen können; damit mir später das Testergebnis in der Corona-Warn-App zur Verfügung gestellt werden kann.	1. Ein auf dem Flyer des medizinischen Fachpersonals oder Test-Centers vorhandener QR-Code kann mit der Warn-App gescannt werden. 2. Erklärungstext wird angezeigt.
E06.02	Als Person, die die App nutzt, möchte ich innerhalb der Corona-Warn-App informiert werden, sobald ein Testergebnis verfügbar ist.	1. Eine Benachrichtigung informiert lediglich über Neuigkeiten in der App. Das Testergebnis selbst kann nur in der App eingesehen werden. 2. Die Benachrichtigung enthält explizit nicht das Ergebnis positiv oder negativ.
E06.03	Bei der Nutzung der App möchte ich, dass bei Vorliegen meines positiven Testergebnisses nach meiner Zustimmung die pseudonymisierten IDs, auf deren Basis ich an den vergangenen Tagen für andere Personen sichtbar war, an den Warn-Server übermittelt werden, damit Kontaktpersonen durch ihre Apps gewarnt werden können.	1. IDs können pseudonymisiert an den Warn-Server übermittelt werden. 2. Die Übermittlung ist nur möglich, sofern zuvor eine Verifikation erfolgreich durchgeführt wurde. Der Verifikationsserver und die Hotline zum Telefon-TAN Verfahren stellen dies sicher. 3. Die Übermittlung ist nur möglich, sofern die Person vorher zugestimmt hat.

# User Story ID	User Story	Akzeptanzkriterien
E06.04	Bei der Nutzung der App möchte ich neben dem digitalen auch einen manuellen Prozess, z.B. über ein Call-Center nutzen können, damit auch ohne einen vorhandenen QR-Code die pseudonymisierten IDs, unter denen ich in den vergangenen Tagen für andere Personen sichtbar war, an den Warn-Server übermittelt werden, so dass Kontaktpersonen durch ihre Apps gewarnt werden können.	1. Die zuständige Stelle kann eine TAN generieren und diese der Person mitteilen. (Generiert wird die TAN von einem Server, nicht durch das Call-Center selbst.)
E06.05	Als Person, die die App nutzt, möchte ich die Möglichkeit zur Eingabe einer TAN innerhalb der App haben, damit ich die mir telefonisch mitgeteilte TAN zur Zuordnung meines Testergebnisses zu der von mir genutzten Instanz der App nutzen kann.	1. Die Eingabe einer TAN innerhalb der App ist möglich. 2. Es wird überprüft und zurückgemeldet, ob die eingegebene TAN korrekt war (zu prüfen, ob technisch möglich).

E06.06	Bei der Nutzung der App möchte ich, dass ich nach der Verifikation der TAN meine pseudonymen IDs freiwillig teilen und etwaige Kontaktpersonen warnen kann.	1. IDs können pseudonymisiert an den Warn-Server übermittelt werden. 2. Die Übermittlung ist nur möglich, sofern zuvor eine Verifikation erfolgreich durchgeführt wurde. Der Verifikationsserver und die Hotline zum Telefon-TAN Verfahren stellen dies sicher. 3. Die Übermittlung ist nur möglich, sofern die Person vorher zugestimmt hat.

3.4.7 Parametrisierung

# User Story ID	User Story	Akzeptanzkriterien
E07.01	Als RKI möchte ich die Parameter zur Risiko-Score-Bestimmung (im Rahmen der technischen Möglichkeiten durch die API) einstellen können, um stets den aktuellen Forschungsergebnissen zur Virusübertragung Rechnung zu tragen.	1. In Abhängigkeit von der bereitgestellten API können Schwellenwerte konfiguriert werden. 2. Die App bezieht dynamische Konfigurationen des RKI, die die Berechnung der Risiko-Einstufung beeinflussen können.

3.4.8 Technische Unterstützung

# User Story ID	User Story	Akzeptanzkriterien
E08.01	Als Person, die die App nutzt, möchte ich eine Hotline kontaktieren können, um technische Probleme mit der App zu lösen	1. Die Telefonnummer der technischen Hotline ist in der App hinterlegt.

3.4.9 Barrierefreiheit

# User Story ID	User Story	Akzeptanzkriterien
E09.01	Als Person, die die App nutzt, möchte ich eine Sprachausgabe nutzen können, um die App (z.B. bei fehlendem oder eingeschränktem Sehvermögen) nutzen zu können.	1. Die Barrierefreiheit bzgl. Sprachausgabe wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.
E09.02	Als Person, die die App nutzt, möchte ich gute Kontraste, veränderbare Schriftgrößen und eine gut lesbare Schriftart haben, um die Texte der App gut lesen zu können.	1. Die Barrierefreiheit bzgl. Kontraste und Schrift wird im Rahmen der Möglichkeiten der Version des jeweils hinterlegten Betriebssystems verfügbar gemacht.
E09.03	Als Person, die die App nutzt, möchte ich, dass mir die Inhalte in einfacher Sprache zur Verfügung gestellt werden, damit ich leicht verstehe, wie ich die App nutzen kann und warum ich es tun sollte.	1. Die Texte und Sprachen werden vom Auftraggeber definiert.

3.4.10 Content Management

# User Story ID	User Story	Akzeptanzkriterien
E10.01	Als RKI möchte ich die Inhalte der App zentral verwalten, um Aktualisierungen von Texten, Links, Hotlines etc. einmalig für alle Stellen in der App durchführen zu können.	1. Das Content-Management erfolgt auf Grundlage der Anforderungen des RKI 2. Der Content wird auf statische und dynamische Inhalte entsprechend der technischen Machbarkeit differenziert 3. Aktualisierungen erfolgen in der ersten Version über ein App-Update.

4 Architektur

Gemäß der unter https://github.com/corona-warn-app/cwa-documentation veröffentlichten Dokumentation in der bis zur Abnahme / Go-Live-Freigabe nach Abstimmungsvereinbarung jeweils aktuellen Fassung. Bei Widersprüchen zwischen verschiedenen Sprachversionen desselben Dokuments geht die englischsprachige Fassung vor.

www.sap.com/contactsap

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. See www.sap.com/copyright for additional trademark information and notices.

THE BEST RUN SAP

DocuSign Envelope ID: 46C267BD-AF3E-4C26-9F0C-BE4660600327

Anlage 2

zu Order Form Nr. 49003196

Servicebeschreibung für Innovative Business Solutions Development Services on Cloud

SAP-Servicebeschreibung
Innovative Business Solutions Development Services on Cloud

SAP erbringt Innovative Business Solutions Development Services on Cloud („Development Services on Cloud"), um unter Verwendung der Entwicklungsumgebung und Cloud-Laufzeitumgebung des Auftraggebers auf der Grundlage einer gemeinsam vereinbarten Lösungsbeschreibung individuelle, auftraggeberspezifische Funktionen zu entwerfen und zu entwickeln, wie in der jeweiligen Order Form und im entsprechenden Scope-Dokument genauer dargelegt.

Dieses Dokument enthält Definitionen und Inhalte, die für derartige Development Services on Cloud gelten.

1. Definitionen

1. **„Abnahme"** bezeichnet die Abnahme einer Projektleistung in Form einer schriftlichen Einverständniserklärung, die über ein Abnahmeprotokoll erfolgt.
2. **„Abnahmeprotokoll"** bezeichnet ein Dokument, in dem die Abnahme erklärt wird.
3. **„Abnahmetest"** bezeichnet einen Test der Features, der vom Auftraggeber zwecks Abnahme der Features durchgeführt wird.
4. **„Add-on"** bezeichnet jede Entwicklung, die neue und unabhängige Funktionen hinzufügt, die vorhandenen SAP-Funktionen jedoch nicht verändert und SAP-Schnittstellen oder anderen SAP-Code nutzt, mit deren Hilfe andere Softwareprodukte mit den Features kommunizieren oder diese aufrufen können.
5. **„Verbundenes Unternehmen"** bezeichnet jede rechtliche Einheit innerhalb des Vertragsgebiets, an der der Auftraggeber mehr als fünfzig Prozent (50 %) der Aktien oder Stimmrechte hält. Eine solche rechtliche Einheit wird nur so lange als Verbundenes Unternehmen betrachtet, wie dieser Anteil gehalten wird.
6. **„Base Cloud Services"** bezeichnet die SAP Cloud Services („SAP Base Cloud Services") und/oder Nicht-SAP-Cloud-Services („Nicht-SAP-Base-Cloud-Services"), die im Scope-Dokument für die entsprechenden Development Services on Cloud beschrieben werden, auf denen die Entwicklung, Verteilung und Nutzung der Features beruhen. Base Cloud Services werden nicht im Rahmen einer Order Form für Development Services on Cloud lizenziert oder bezogen und müssen separat erworben werden.
7. **„Geschäftspartner"** bezeichnet eine rechtliche Einheit oder einen Rechtsträger, die bzw. der im Zusammenhang mit den internen Geschäftsvorfällen des Auftraggebers Zugriff auf die Features benötigt, z. B. Kunden, Distributoren und/oder Lieferanten des Auftraggebers.
8. **„Geschäftsanforderungen"** bezeichnet die geschäftlichen Ziele des Auftraggebers und deren Bezug zum Scope der Development Services on Cloud.
9. **„Bestätigung"** bezeichnet eine Einverständniserklärung per E-Mail.
10. **„Cloud Service"** bezeichnet jeden eigenständigen On-Demand-Service.
11. **„Entwicklungsumgebung und Cloud-Laufzeitumgebung"** bezeichnet die Infrastruktur, Plattform und Anwendungsservices, die vom Auftraggeber bereitgestellt werden; dies umfasst auch die Base Cloud Services. Die Umgebung besteht aus folgenden Teilen:

    11.1 **„Entwicklungsumgebung"** bezeichnet die auftraggeberspezifische Umgebung für die Entwicklung, den Bau und die Verteilung der Features, wie im jeweiligen Scope-Dokument beschrieben.

    11.2 **„Cloud-Laufzeitumgebung"** bezeichnet die auftraggeberspezifische Umgebung für die Ausführung der Features, wie im jeweiligen Scope-Dokument beschrieben. Diese besteht aus:

        11.2.1 **„Nicht produktive Cloud-Umgebung"**, in der die Features getestet werden.

        11.2.2 **„Cloud-Produktivumgebung"**, die für den normalen Geschäftsbetrieb eingesetzt wird und in der die Daten des Auftraggebers erfasst werden.
12. **„Innovative Business Solutions Development Services on Cloud"/„Development Services on Cloud"** bezeichnet Services, auf die sich die Parteien im Rahmen der entsprechenden Order Form geeinigt haben und die im jeweiligen Scope-Dokument ausgeführt sind.
13. **„Rechte an geistigem Eigentum"** bezeichnet Patente jeder Art, Designrechte, Gebrauchsmuster oder andere gleichartige Erfindungsrechte, Urheberrechte, Halbleiterschutzrechte, Rechte an Geschäftsgeheimnissen, Geheimhaltungsrechte, Marken, Handelsnamen und Dienstleistungsmarken sowie alle anderen Rechte an immateriellem Eigentum, einschließlich diesbezüglicher Anmeldungen und Eintragungen in irgendeinem Land, die sich aus gesetzlichen Regelungen, dem Gewohnheitsrecht oder Verträgen

ergeben, unabhängig davon, ob diese vollständig formalisiert vorliegen und bereits bestehen oder erst in Zukunft beantragt, ausgegeben oder erworben werden.

14. **„Features"** bezeichnet SAP-Software-Funktionen, die als Bestandteil der jeweiligen Development Services on Cloud entwickelt und ausgeliefert werden.

15. **„Übersichtsarchitektur"** bezeichnet die geplante Architektur der Lösung auf einer grob granularen Ebene.

16. **„Modifikation"** bezeichnet (i) eine Änderung an dem/den ausgelieferten Quellcode/Metadaten oder (ii) jede Entwicklung, bei der es sich nicht um den ausgelieferten Quellcode oder Metadaten handelt, die die vorhandenen Funktionen der Features anpasst, erweitert oder ändert, einschließlich der, jedoch nicht beschränkt auf die Erstellung von neuen Anwendungsprogrammierschnittstellen (APIs), alternativen Benutzungsoberflächen oder die Erweiterung der SAP-Datenstrukturen oder (iii) jede anderweitige Änderung der Features (außer Add-ons), die die Verwendung oder Einbindung von SAP-Materialien einschließt (wie unten definiert).

17. **„Product-Backlog"** bezeichnet die Software-Anforderungen des Auftraggebers, die als Features von SAP realisiert werden sollen. Das Product-Backlog ist in Product-Backlog-Positionen aufgeschlüsselt und bildet zusammen mit dem Vision & Scope Document die Lösungsbeschreibung. Die abgenommene Version des Vision & Scope Document und die finale Version des Product-Backlogs enthalten die einzige rechtlich bindende Beschreibung der Features. Diese bilden die Grundlage für den Abnahmetest der Features.

18. **„Product-Backlog-Position"** umfasst die von SAP gemäß den Software-Anforderungen des Auftraggebers zu entwickelnden Features mit ihrer entsprechenden funktionalen Beschreibung und den Abnahmekriterien sowie die vereinbarten Prioritäten jeder Product-Backlog-Position und den Bearbeitungsstand der bereitzustellenden Features. Die Product-Backlog-Positionen sind im Product-Backlog enthalten.

19. **„SAP Innovative Business Solutions Methodology Scrum Lifecycle"** bezeichnet eine iterative und inkrementelle Projektmanagementmethode, bei der die Software-Anforderungen des Auftraggebers im Rahmen von Sprints nach und nach in Features umgesetzt werden.

20. **„SAP-Materialien"** bezeichnet jegliche Software, Programme, Werkzeuge, Systeme, Daten oder andere Materialien, die SAP dem Auftraggeber im Vorfeld oder im Zuge der Erfüllung der jeweiligen Order Form zur Verfügung stellt, einschließlich Features und Dokumentationen sowie jeglicher Informationen, Materialien oder Feedback, die der Auftraggeber SAP bezüglich der Features und Dokumentationen bereitstellt.

21. **„Software-Anforderungen"** bezeichnet die Benutzeranforderungen sowie die funktionalen und nicht-funktionalen Anforderungen des Auftraggebers.

22. **„Quellcode"** bezeichnet den Programmcode der Features in von Menschen lesbarer Form.

23. **„Sprint"** bezeichnet einen festgelegten Zeitraum, in dem bestimmte Arbeiten durchgeführt und zur Prüfung fertiggestellt werden.

24. **„Vertragsgebiet"** umfasst alle Staaten der Welt mit Ausnahme solcher, die gemäß den US-Exportgesetzen verboten sind und den gesetzlichen Bestimmungen der jeweiligen Order Form unterliegen.

25. **„Drittanbieter-Software"** bezeichnet (i) alle Softwareprodukte und sämtliche Inhalte, für die der Auftraggeber Nutzungsrechte erworben hat (wie in der zugehörigen Order Form angegeben), alle jeweils so, wie sie von anderen Unternehmen als SAP, SAP SE und/oder deren verbundenen Unternehmen entwickelt und an den Auftraggeber gemäß der zugehörigen Order Form ausgeliefert wurden; (ii) alle neuen Releases, Updates und Versionen dieser Softwareprodukte, die gemäß der Support- oder Gewährleistungsverpflichtung von SAP zur Verfügung gestellt werden und (iii) alle vollständigen oder partiellen Kopien der vorstehenden Produkte.

26. **„Nutzungsbedingungen"** bezeichnet in Bezug auf die in einer Order Form angegebenen Features das bei Unterzeichnung der jeweiligen Order Form gültige Dokument zu den SAP-Software-Nutzungsrechten („Nutzungsbedingungen"), zu finden unter http://www.sap.com/company/legal/index.epx, das einen Bestandteil der Order Form darstellt. Derartige Dokumente zu den SAP-Software-Nutzungsrechten sind durch Referenz Bestandteil der Order Form. SAP empfiehlt dem Auftraggeber, Kopien der geltenden Dokumente zu den SAP-Software-Nutzungsrechten für die eigenen Unterlagen anzufertigen.

27. **„Vision & Scope Document"** enthält die Geschäftsanforderungen des Auftraggebers und die Übersichtsarchitektur. Ferner bildet das Vision & Scope Document zusammen mit dem Product-Backlog die Lösungsbeschreibung. Die abgenommene Version des Vision & Scope Document und die finale Version des Product-Backlogs enthalten die einzige rechtlich bindende Beschreibung der Features. Diese bilden die Grundlage für den Abnahmetest der Features.

2 SAP Innovative Business Solutions Methodology

SAP erbringt Development Services on Cloud unter Anwendung der im Scope-Dokument beschriebenen Innovative Business Solutions Development Methodology Scrum Lifecycle.

3 Rollen und Projektsteuerung

Die Rollen und die Projektsteuerung sind im Scope-Dokument definiert.

4 Mitwirkungspflichten des Auftraggebers

Die allgemeinen Mitwirkungspflichten des Auftraggebers sind im Folgenden aufgeführt. Weitere Einzelheiten zu den spezifischen Mitwirkungspflichten des Auftraggebers und von SAP sind im Scope-Dokument enthalten. Der Auftraggeber hat folgende Pflichten:

1. Sicherstellen, dass der Auftraggeber über sämtliche Nutzungsrechte verfügt, einschließlich der Nutzungsrechte von Drittanbietern, die SAP zur Erbringung der Development Services on Cloud benötigt.
2. Ernennen eines Projektmanagers und/oder eines Programmmanagers, der für SAP als zentraler Ansprechpartner beim Auftraggeber fungiert.
3. Unterstützung durch die Unternehmensleitung des Auftraggebers, deren Vertreter rechtzeitig und regelmäßig zur Verfügung stehen, um den Fortschritt zu überwachen und als Entscheidungsträger für Grundsatzentscheidungen und bei der Behebung von Problemen zu fungieren.
4. Verwalten der externen Dienstleister des Auftraggebers.
5. Bereitstellung sachkundiger Ressourcen mit Entscheidungsbefugnis, die als Mitglieder des Teams für die Arbeit am Projekt des Auftraggebers zur Verfügung stehen.
6. Bereitstellen einer geeigneten Arbeitsumgebung, von Systemzugang, von Zugang zum Internet und von Telekommunikationsservices für die SAP-Mitarbeiter, die in den Räumlichkeiten des Auftraggebers eingesetzt werden. Keiner der SAP-Mitarbeiter verfügt über ein Büro in den Geschäftsräumen des Auftraggebers mit Schlüsseln, die die ausschließliche Nutzung des betreffenden Büros durch SAP ermöglichen. Es wird empfohlen, dem SAP-Team einen geschützten Ort zur Verfügung zu stellen.
7. Gewährleistung des Zugangs zu den Räumlichkeiten des Auftraggebers für SAP, soweit dies für die Erbringung der Development Services on Cloud erforderlich ist, einschließlich der Bereitstellung aller notwendigen Identifikationsmaterialien (Besucherausweise, Zugangskarten usw.).
8. Weitergabe der Namen und Kontaktdaten aller dem Projekt zugewiesenen Schlüsselressourcen, sowohl eigene Mitarbeiter als auch Mitarbeiter von Dritten, an SAP.
9. Sicherstellen, dass jegliche für die Development Services on Cloud erforderliche Hardware vor dem Start des Projekts abgesichert wird.
10. Bereitstellung der Entwicklungsumgebung und Cloud-Laufzeitumgebung und Systemlandschaft, einschließlich aller erforderlichen Tools für die Entwicklung, den Bau, die Verteilung und die Ausführung der Features mit den notwendigen Berechtigungen für den Vor-Ort- und Remote-Zugriff auf diese Systeme für SAP. Alternativ, wenn die Features nicht in der Entwicklungsumgebung des Auftraggebers entwickelt werden, nur Bereitstellung der Cloud-Laufzeitumgebung für die Ausführung der Features mit den notwendigen Berechtigungen für den Vor-Ort- und Remote-Zugriff auf diese Systeme für SAP.
11. Bereitstellung einer konsistenten, stabilen und schnellen Verbindung zwischen SAP und der Entwicklungsumgebung und Cloud-Laufzeitumgebung des Auftraggebers zu den benötigten Zeiten. Alternativ, wenn die Features nicht in der Entwicklungsumgebung des Auftraggebers entwickelt werden, nur Bereitstellung einer konsistenten, stabilen und schnellen Verbindung zwischen SAP und der Cloud-Laufzeitumgebung des Auftraggebers zu den benötigten Zeiten.
12. Gestatten der Nutzung von SAP-Laptops und -Mobilgeräten im Netzwerk des Auftraggebers und einer Verbindung zum SAP-Netzwerk über SAP-VPN-Protokolle (VPN: Virtual Private Network); andernfalls stellt der Auftraggeber PCs und/oder Laptops mit der Microsoft Office Suite und E-Mail-Funktion für das SAP-Team bereit. Vom Auftraggeber bereitgestellte Laptops und/oder PCs müssen mit aktueller Virenschutzsoftware ausgestattet sein. Alternativ, wenn die Features nicht in der Entwicklungsumgebung des Auftraggebers entwickelt werden, nur Bereitstellung einer Systemverbindung für Verteilungszwecke.
13. Bereitstellung eines zuständigen Ansprechpartners für SAP zur Erläuterung relevanter Nutzungsrechte und Systeme sowie Nicht-SAP-Cloud-Services von Drittanbietern.
14. Sicherstellen, dass das Projekt des Auftraggebers im Einklang mit den maßgeblichen gesetzlichen und behördlichen Vorschriften steht.

Der Auftraggeber erkennt an und stimmt zu, dass die Möglichkeit zur Erbringung der in der entsprechenden Order Form angegebenen Development Services on Cloud durch SAP von Beiträgen abhängig ist, die der Auftraggeber zu erbringen hat.

Sollte SAP feststellen, dass eine wesentliche erforderliche Reaktion oder Maßnahme des Auftraggebers sich so weit verzögert, dass der Zeitplan für die Lieferung der Projektleistungen dadurch beeinträchtigt oder wegen der Verzögerung nach vernünftigem Ermessen nicht eingehalten werden kann, informiert SAP den Auftraggeber darüber unverzüglich in schriftlicher Form. Der Auftraggeber hat daraufhin: (i) unverzüglich zu reagieren; (ii) die erforderliche Maßnahme auszuführen; oder (iii) eine Aussetzung der betreffenden Development Services on Cloud zu beantragen, wobei der Auftraggeber jedoch sämtliche Mehrkosten infolge der Aussetzung basierend auf den zum jeweiligen Zeitpunkt gültigen SAP-Preisen bzw. -Sätzen zu tragen hat.
In Bezug auf eine von SAP gegebene Mitteilung gemäß diesem Abschnitt verpflichtet sich der Auftraggeber, innerhalb von fünf (5) Werktagen nach Erhalt der Mitteilung von SAP in schriftlicher Form darauf zu antworten. Antwortet der Auftraggeber nicht innerhalb von fünf (5) Werktagen, so wird der Gesamtprojektzeitplan mindestens um den mit der Verzögerung durch den Auftraggeber zusammenhängenden Zeitraum verlängert.

5 Annahmen und Ausschlüsse

A. Die Annahmen der Servicebeschreibung sind im Folgenden aufgeführt. SAP kann weitere Annahmen in die jeweilige Order Form oder in das Scope-Dokument aufnehmen.

1. Die mit den Development Services on Cloud betrauten Mitarbeiter unterstehen der Weisung von SAP und werden an SAP-Standorten eingesetzt. Reisen von SAP-Mitarbeitern müssen zwischen den Parteien je nach Bedarf vereinbart werden.
2. Die gesamte Begleitdokumentation wird mit Rechnern bzw. Laptops mit Microsoft-Office-Anwendungen (Microsoft Word, Microsoft Excel, Microsoft Project, Microsoft Visio und Microsoft PowerPoint), Adobe Reader und sonstigen Hilfsprogrammen für die Dokumentation ausgearbeitet, auf die sich SAP und der Auftraggeber gemeinsam einigen.

B. Die Ausschlüsse der Servicebeschreibung sind im Folgenden aufgeführt. SAP kann weitere Ausschlüsse in die jeweilige Order Form oder in das Scope-Dokument aufnehmen.

1. Entwicklungen, die nicht im vorliegenden Scope-Dokument aufgeführt sind.

DocuSign Envelope ID: 46C267BD-AF3E-4C26-9F0C-BE4660600327

Anlage 3

zu Order Form Nr. 49003196

Servicebeschreibung für Innovative Business Solutions Development Support Services on Cloud

SAP-Servicebeschreibung

Innovative Business Solutions Development Support Services on Cloud

SAP bietet Innovative Business Solutions Development Support Services on Cloud („Development Support Services on Cloud") für Features an, die von SAP im Rahmen der Erbringung von Innovative Business Solutions Development Services on Cloud („Development Services on Cloud") gemäß einer Order Form entwickelt und ausgeliefert wurden.

Begriffe, die in diesem Dokument nicht definiert sind, sind in der Servicebeschreibung für Innovative Business Solutions Development Services on Cloud und/oder in den jeweiligen Allgemeinen Geschäftsbedingungen definiert.

1 DEFINITIONEN

1. **„Base Support Services"** bezeichnet die Support Services, die für die Base Cloud Services zwischen dem Auftraggeber und SAP und/oder dem Auftraggeber und dem Anbieter von Nicht-SAP-Base-Cloud-Services erbracht werden.
2. **„Customer Communication Point"** (Kontaktstelle beim Auftraggeber) bezeichnet diejenigen Mitarbeiter des Auftraggebers, die berechtigt sind, Development Support Services on Cloud anzufordern. Der Auftraggeber benennt mindestens zwei (2) und maximal fünf (5) qualifizierte englischsprachige Ansprechpartner, die berechtigt sind, im Rahmen dieser Servicebeschreibung Development Support Services on Cloud anzufordern und setzt SAP darüber in schriftlicher Form in Kenntnis.

2 SERVICEANSATZ

Für Development Support Services on Cloud sind zwei Supportmodelle verfügbar: „Full Edition" und „Large Enterprise". Large Enterprise Development Support Services on Cloud sind ausschließlich für Auftraggeber verfügbar, die für ihre SAP-Systemlandschaft eine Vereinbarung über SAP Product Support for Large Enterprises geschlossen haben. Für alle anderen Auftraggeber werden nur Full Edition Development Support Services on Cloud angeboten.

Die Kombination aus den zugrunde liegenden Base Cloud Services und dem SAP-Supportmodell des Auftraggebers bestimmt den spezifischen Scope der Development Support Services on Cloud für die Features gemäß der nachfolgenden Tabelle. Einzelheiten zu den Services sind in Abschnitt 3.2 ausgeführt.

Base Cloud Services	**SAP Base Cloud Services und/oder Nicht-SAP-Base-Cloud-Services**		**SAP Commerce Cloud**	
Supportmodell für Development Support Services on Cloud	**Full Edition**	**Large Enterprise**	**Full Edition**	**Large Enterprise**
Service				
Meldungsbearbeitung (siehe Beschreibung in Abschnitt 3.2.1)	X	X	X	X
Conflict Resolution Service für Aktualisierungen von SAP Base Cloud Services (siehe Beschreibung in Abschnitt 3.2.2)	X	X		
Conflict Resolution Service für Aktualisierungen von Nicht-SAP-Base-Cloud-Services (siehe Beschreibung in Abschnitt 3.2.3)	X	X		
Conflict Resolution Service für Aktualisierungen von SAP Commerce Cloud (siehe Beschreibung in Abschnitt 3.2.4)			X	X
Verbesserung der Features (siehe Beschreibung in Abschnitt 3.2.5)	X	X	X	X

Development Support Services on Cloud Delivery Management (siehe Beschreibung in Abschnitt 3.2.6)	X		X	

3 DEVELOPMENT SUPPORT SERVICES ON CLOUD

3.1 Allgemeine Bestimmungen

3.1.1 Sämtliche Development Support Services on Cloud werden ausschließlich für Features erbracht. Sonstige SAP-Software, Base Cloud Services, SAP Cloud Services, Nicht-SAP-Software, Nicht-SAP-Cloud-Services sowie Drittanbieter-Software, die vom Auftraggeber lizenziert und/oder erworben werden, sind ausdrücklich von den im Rahmen dieser Servicebeschreibung bereitgestellten Development Support Services on Cloud ausgenommen.

3.1.2 Development Support Services on Cloud werden ausschließlich für die neueste Version der Features erbracht. Der Auftraggeber muss gewährleisten, dass alle Development Support Services on Cloud (Code-Korrekturen, Patches usw.), die SAP im Rahmen dieser Servicebeschreibung bereitstellt, ordnungsgemäß und zeitnah auf die Features angewendet werden.

3.1.3 Die in dieser Servicebeschreibung beschriebenen Development Support Services on Cloud werden für diejenige nicht produktive Cloud-Umgebung des Auftraggebers bereitgestellt, über die dem Auftraggeber auch die Features bereitgestellt wurden. Aus begründetem Anlass und unter Berücksichtigung aller weiteren Voraussetzungen in Bezug auf Development Support Services on Cloud kann der Auftraggeber anfragen und SAP kann zustimmen, dass SAP die Development Support Services on Cloud in einer anderen nicht produktiven Cloud-Umgebung als der oben genannten erbringt.

Wenn der Auftraggeber die Entwicklungsumgebung und die Cloud-Laufzeitumgebung bereitstellt, trägt er die alleinige Verantwortung für die Anwendung der erbrachten Development Support Services on Cloud in seiner Cloud-Produktivumgebung.

Wenn der Auftraggeber nur die Cloud-Laufzeitumgebung bereitstellt, wendet SAP die Development Support Services on Cloud in der nicht produktiven Cloud-Umgebung des Auftraggebers an. Der Auftraggeber kann anfragen und SAP kann zustimmen, dass SAP die Development Support Services on Cloud in der Cloud-Produktivumgebung des Auftraggebers erbringt.

3.1.4 Development Support Services on Cloud werden nur während der in der entsprechenden Order Form festgelegten lokalen Geschäftszeiten und ausschließlich über den Customer Communication Point erbracht.

3.2 Scope der Development Support Services on Cloud

SAP bietet folgende Development Support Services on Cloud für die mit den entsprechenden Development Services on Cloud ausgelieferten Features:

3.2.1 Meldungsbearbeitung („Meldungsbearbeitung")

SAP unterstützt den Auftraggeber im Falle der Meldung von Störungen durch Bereitstellen von Informationen zur Fehlerbehebung, Fehlervermeidung oder Fehlerumgehung. Das primäre Medium hierfür ist die von SAP bereitgestellte Support-Infrastruktur. Der Auftraggeber kann jederzeit Support-Meldungen aufgeben. Die mit dem Problemlösungsprozess befassten Personen können den Status der Support-Meldung jederzeit abrufen.

SAP stellt Folgendes bereit:

1. Bearbeitung von Support-Meldungen bei Problemen im Zusammenhang mit den Features
2. Code-Korrekturen oder Patches (z. B. veränderte Programme, in denen die genannte Störung nicht reproduziert wird) oder Behelfslösungen oder Aktionspläne

3.2.2 Conflict Resolution Service für Aktualisierungen von SAP Base Cloud Services

Sind die Fehlfunktionen in den betreffenden Features auf Aktualisierungen der SAP Base Cloud Services zurückzuführen, untersucht SAP mögliche Kompatibilitätskonflikte zwischen den Features und nachfolgenden Aktualisierungen der SAP Base Cloud Services und stellt Möglichkeiten und/oder Lösungen zur Behebung oder Vermeidung jeglicher Kompatibilitätsprobleme bereit.

3.2.3 Conflict Resolution Service für Aktualisierungen von Nicht-SAP-Base-Cloud-Services

1. Sind die Fehlfunktionen in den betreffenden Features auf Aktualisierungen der Nicht-SAP-Base-Cloud-Services zurückzuführen, untersucht SAP mögliche Kompatibilitätskonflikte zwischen den Features und nachfolgenden Aktualisierungen der Nicht-SAP-Base-Cloud-Services. Sofern dies technisch machbar ist,

legt SAP eine Schätzung in Bezug auf den für die Bereitstellung von Möglichkeiten und/oder Lösungen zur Behebung oder Vermeidung jeglicher Kompatibilitätsprobleme erforderlichen Aufwand vor.

2. Falls (i) der Aufwand durch die verbleibende Anzahl der für die Verbesserung der Features verfügbaren Tage im laufenden Kalenderjahr abgedeckt werden kann und (ii) der Auftraggeber der Nutzung der verbleibenden Anzahl der für die Verbesserung von Features verfügbaren Tage zustimmt, stellt SAP Möglichkeiten und/oder Lösungen zur Behebung oder Vermeidung von Kompatibilitätsproblemen bereit.

   Falls (i) der Aufwand die verbleibende Anzahl der für die Verbesserung der Features verfügbaren Tage im laufenden Kalenderjahr überschreitet und (ii) der Auftraggeber bei Aktualisierungen der Nicht-SAP-Base-Cloud-Services Support für die Features bei SAP anfordert und (iii) SAP der Erbringung derartiger Services zustimmt, schließen der Auftraggeber und SAP eine zusätzliche Vereinbarung ab.

3.2.4 Conflict Resolution Service für Aktualisierungen von SAP Commerce Cloud

1. Um eine langfristige Kompatibilität der Features mit SAP Commerce Cloud zu gewährleisten, kann der Auftraggeber von SAP verlangen, (i) mögliche Konflikte zwischen den Features und nachfolgenden Aktualisierungen für SAP Commerce Cloud zu untersuchen und (ii) Möglichkeiten und/oder Lösungen zur Behebung oder Vermeidung von Kompatibilitätskonflikten bereitzustellen.

2. Um den Conflict Resolution Service anzufordern, setzt der Auftraggeber SAP hiervon acht (8) Wochen im Voraus schriftlich in Kenntnis.

3. Der Auftraggeber stellt einen englischsprachigen Projektmanager zur Verfügung, der als Ansprechpartner für SAP beim Auftraggeber dient.

4. Vor dem Conflict Resolution Service stellt der Auftraggeber sicher, dass die entsprechende Aktualisierung des SAP Commerce Cloud Service auf die nicht produktive Cloud-Umgebung angewendet wurde, in der der Conflict Resolution Service ausgeführt werden soll.

5. Klarstellend wird darauf hingewiesen, dass der Auftraggeber dafür verantwortlich ist, SAP Commerce Cloud ordnungsgemäß zu aktualisieren.

3.2.5 Verbesserung der Features („Verbesserung der Features")

1. Die Verbesserung der Features soll dem Auftraggeber, der Development Support Services on Cloud bezieht, dabei helfen, Verbesserungen der von SAP im Rahmen der jeweiligen Development Services on Cloud ausgelieferten Features zu ermöglichen. Der Auftraggeber muss SAP ein Anforderungsdokument übermitteln, in dem die Anforderungen bezüglich der Verbesserung der Features deutlich dargelegt sind. Nach Erhalt des Antrags analysiert SAP die Anforderungen und informiert den Auftraggeber innerhalb eines angemessenen Zeitraums darüber, ob die Verbesserung der Features unter Berücksichtigung der unten dargelegten Beschränkungen vorgenommen werden kann. Ist die Verbesserung der Features machbar, unterbreitet SAP dem Auftraggeber einen Lösungsvorschlag und eine Aufwandsschätzung (nachfolgend als „Realisierungsangebot" bezeichnet) für die Anpassung der Features. Der Auftraggeber informiert SAP schriftlich innerhalb von zehn (10) Werktagen über die Annahme oder die Ablehnung des Realisierungsangebots. Nachdem der Auftraggeber das Realisierungsangebot akzeptiert hat, nimmt SAP die Verbesserung der Features vor. Nach Abschluss der Verbesserung informiert SAP den Auftraggeber über die Bereitschaft der entsprechenden Features sowie über den Gesamtaufwand, der wie im Folgenden beschrieben für die Verbesserung der Features vom Kontingent abgezogen wird. Die Verbesserung der Features gilt nach der Auslieferung der verbesserten Features als akzeptiert.

2. Der Auftraggeber ist berechtigt, die in der entsprechenden Order Form angegebene maximale Anzahl an Tagen für die Verbesserung(en) der Features aufzuwenden. Die maximale Anzahl an Tagen entspricht [redacted] der jährlichen Vergütung für die Development Support Services on Cloud [redacted] Diese Gesamtanzahl an Tagen muss jeweils im laufenden Kalenderjahr genutzt werden; eine Übertragung in das Kalenderjahr davor oder danach, zwischen verschiedenen Order Forms über Development Support Services on Cloud oder über das Ende der Laufzeit (einschließlich Verlängerungslaufzeiten) der Development Support Services on Cloud hinaus ist nicht möglich. Für nicht genutzte Tage darf der Auftraggeber keine Ansprüche geltend machen; dies gilt insbesondere für Erstattungsansprüche. Zur Klarstellung: Wenn die Development Support Services on Cloud im Laufe eines Kalenderjahres beginnen, wird die Anzahl der Tage für die Verbesserung von Features für das betreffende Kalenderjahr anteilig berechnet.

3. Vor Beginn jeglicher Aktivitäten vereinbart SAP mit dem Auftraggeber den Zeitrahmen für die Analyse eines Antrags und die Vorlage eines Realisierungsangebots. Das Realisierungsangebot beinhaltet einen vorläufigen Zeitplan für die Durchführung der Verbesserung von Features, in dem die Ressourcenverfügbarkeit sowie bestehende Auslieferungsverpflichtungen berücksichtigt werden. Nach Annahme des

Realisierungsangebots durch den Auftraggeber beginnt SAP mit den Aktivitäten und nimmt zeitnah die Verbesserung der Features vor.

4. Der Auftraggeber nimmt die folgenden Einschränkungen zur Kenntnis und akzeptiert, dass SAP einen vom Auftraggeber eingereichten Antrag ablehnen kann, wenn:

   (i) der Antrag sich nicht auf die ausgelieferten Features bezieht; oder

   (ii) der Antrag aus technischen oder sonstigen Beschränkungen nicht umgesetzt werden kann; oder

   (iii) der Antrag die verbleibende Anzahl der für die Verbesserung der Features verfügbaren Tage im laufenden Kalenderjahr überschreitet; oder

   (iv) der Antrag die angemessene Auslieferungskapazität des internen SAP-Supportteams für den verbleibenden Zeitraum im laufenden Kalenderjahr überschreitet.

5. Zur Klarstellung wird darauf hingewiesen, dass SAP und der Auftraggeber für Anträge, deren Scope über das für Verbesserungen von Features in diesem Dokument vereinbarte Maß hinausgeht, eine gesonderte Vereinbarung treffen können.

3.2.6 Development Support Services on Cloud Delivery Management

SAP benennt einen Development Support Services on Cloud Delivery Manager („Delivery Manager"). Der Delivery Manager übernimmt die folgenden Aufgaben:

1. Funktion als zentraler Ansprechpartner für den Auftraggeber in Verbindung mit den Development Support Services on Cloud sowie Planung von Aktivitäten im Zusammenhang mit den Development Support Services on Cloud
2. Einrichtung und Verwaltung der Meldungskomponente beim Auftraggeber und der zugehörigen Meldungswarteschlange(n)
3. Leitung des internen SAP-Supportteams, das für die Erbringung von Development Support Services on Cloud im Rahmen der Order Form abgestellt wurde
4. Bereitstellung regelmäßiger Statusberichte zu Themen in Bezug auf Development Support Services on Cloud (z. B. Berichte über Support-Meldungen des Auftraggebers; Bereitstellung eines Statusberichts zu den Development Support Services on Cloud)
5. Besprechung der Auswirkungen zukünftiger Implementierungsstrategien der Roadmap des Auftraggebers auf die im Rahmen der jeweiligen Development Services on Cloud entwickelten Features
6. Besprechung mit dem Auftraggeber, wie mit Meldungen zu verfahren ist, die im Hinblick auf die im Rahmen der jeweiligen Development Services on Cloud entwickelten Features nicht als Mangel eingestuft werden können

3.3 Global Support Backbone

Das Global Support Backbone dient als SAP-Wissensdatenbank und Extranet zum Wissensaustausch, über das SAP ausschließlich für Auftraggeber und Partner Inhalte und Services bereitstellt. Zum Global Support Backbone gehört auch das SAP Support Portal unter https://support.sap.com.

4 VORAUSSETZUNGEN

4.1 Voraussetzung für die Erbringung von Development Support Services on Cloud ist, dass Base Support Services für die Base Cloud Services erbracht werden.

4.2 Um gemäß diesem Dokument Development Support Services on Cloud zu beziehen, muss der Auftraggeber folgende Voraussetzungen erfüllen:

1. Er entrichtet kontinuierlich alle Vergütungen gemäß den jeweiligen Development Support Services on Cloud.
2. Darüber hinaus erfüllt der Auftraggeber die Verpflichtungen aus der vorliegenden Servicebeschreibung sowie die sich aus der entsprechenden Order Form für Development Support Services on Cloud und aus den Base Support Services ergebenden Verpflichtungen.
3. Der Auftraggeber stellt sicher, dass er über sämtliche Nutzungsrechte verfügt, einschließlich der Nutzungsrechte von Drittanbietern, die SAP zur Erbringung der Development Support Services on Cloud benötigt.

4. Er stellt sicher, dass die Base Cloud Services und jegliche erforderlichen zusätzlichen Services/Tools verfügbar sind, um die Development Support Services on Cloud für die Features bereitzustellen.
5. Er verwaltet die externen Dienstleister des Auftraggebers.
6. Er stellt Remote-Zugriff über ein von SAP definiertes technisches Standardverfahren bereit, erhält diesen aufrecht und räumt SAP alle notwendigen Berechtigungen ein, insbesondere für die Problemanalyse im Rahmen der Meldungsbearbeitung. Der Auftraggeber gewährt den Remote-Zugriff ohne Einschränkungen hinsichtlich der Nationalität der SAP-Mitarbeiter, die die Meldungen bearbeiten, oder des Landes, in dem sie sich befinden. Der Auftraggeber ist sich bewusst, dass nicht gewährter uneingeschränkter Zugriff Verzögerungen in Bezug auf die Meldungsbearbeitung sowie die Bereitstellung von Korrekturen nach sich ziehen kann und SAP gegebenenfalls nicht in der Lage ist, effizient Unterstützung zu leisten.
7. Alle Support-Meldungen werden mit der von SAP für die entsprechenden Features definierten Meldungskomponente über die zum jeweiligen Zeitpunkt aktuelle SAP-Infrastruktur an SAP übermittelt, die SAP dem Auftraggeber von Zeit zu Zeit zur Verfügung stellt. Der Auftraggeber wird bei Erhalt der Features schriftlich über die Meldungskomponente informiert. Ordnet der Auftraggeber eine Support-Meldung zu den Features nicht der richtigen Meldungskomponente zu, kann dies die Reaktionszeit verlängern.
8. Support-Meldungen sind auf Englisch zu verfassen.
9. In der Meldung beschreibt der Auftraggeber, wie der Fehler auftritt, und ggf. ist eine Demonstration erforderlich. Der Auftraggeber unterstützt SAP bei der Analyse des Fehlers und der Erbringung der Development Support Services on Cloud. Zu diesem Zweck stellt der Auftraggeber, falls erforderlich, eigene Mitarbeiter ab.
10. Bereitstellung eines zuständigen Ansprechpartners für SAP zur Erläuterung relevanter Drittanbieter-Software und -systeme sowie Nicht-SAP-Cloud Services.
11. Der Auftraggeber stellt SAP alle Dokumente zu Änderungen und Erweiterungen zur Verfügung, die durch oder für den Auftraggeber in der Entwicklungsumgebung und der Cloud-Laufzeitumgebung erstellt wurden und die der Analyse des Fehlers dienlich sein könnten. Des Weiteren hält der Auftraggeber geeignete und aktuelle Dokumentationen zu diesen Änderungen und Erweiterungen vor und macht sie SAP bei Bedarf zugänglich.
12. Development Support Services on Cloud werden nicht für vom Auftraggeber vorgenommene Änderungen und Erweiterungen bereitgestellt. SAP erbringt keine Development Support Services on Cloud für von derartigen Änderungen betroffene Features.
13. Der Auftraggeber verpflichtet sich, SAP ggf. unverzüglich über alle Änderungen an der Entwicklungsumgebung und der Cloud-Laufzeitumgebung zu informieren und SAP alle übrigen Informationen, die für die Nutzung der Features relevant sind, zukommen zu lassen.

5 LAUFZEIT UND KÜNDIGUNG

5.1 Development Support Services on Cloud beginnen mit der letzten Abnahme der im Rahmen der jeweiligen Development Services on Cloud ausgelieferten Features und werden bis zum Ende des folgenden Kalenderjahres erbracht („Anfangslaufzeit"). Nach der Anfangslaufzeit verlängern sich die Development Support Services on Cloud zu Beginn jedes Kalenderjahres um ein (1) weiteres Jahr (jeweils eine „Verlängerungslaufzeit").

5.2 Development Support Services on Cloud werden stets für den gesamten Scope der im Rahmen der jeweiligen Development Services on Cloud von SAP ausgelieferten Features erbracht; der Auftraggeber hat stets dafür zu sorgen, dass die jeweiligen Development Services on Cloud vollständig von den Development Support Services on Cloud abgedeckt werden (insbesondere alle Features und alle Teillieferungen), oder er muss die Development Support Services on Cloud insgesamt kündigen. Eine Teilkündigung ist nicht zulässig.

5.3 Development Support Services on Cloud können von beiden Parteien schriftlich mit einer Frist von drei (3) Monaten zum Ende der Anfangslaufzeit und der jeweiligen Verlängerungslaufzeit gekündigt werden. Ungeachtet dessen ist SAP berechtigt, die Development Support Services on Cloud einen (1) Monat nach schriftlicher Mitteilung an den Auftraggeber, dass dieser die Vergütung für die Development Support Services on Cloud gemäß der entsprechenden Order Form nicht entrichtet hat, zu kündigen.

5.4 Im Falle der Kündigung der Development Support Services on Cloud kann der Auftraggeber, der nur die Cloud-Laufzeitumgebung bereitstellt, zum Zeitpunkt des Inkrafttretens der Kündigung anfragen, dass SAP ihm die neueste Version des Quellcodes zur Verfügung stellt.

DocuSign Envelope ID: 46C267BD-AF3E-4C26-9F0C-BE4660600327

Anlage 4

zu Order Form Nr. 49003196

Allgemeine Geschäftsbedingungen für SAP Services der SAP Deutschland SE & Co. KG („AGB für Services") mit Ausnahme deren Anlage „Vereinbarung über die Datenverarbeitung für SAP Pflege und Professional Services Version 05-2018" („DPA"), anstelle derer die Anlage „Vereinbarung zur Auftragsverarbeitung" gilt

SAP SERVICES

Allgemeine Geschäftsbedingungen

SAP Deutschland SE & Co KG

("AGB für Services")

GELTUNG DER VERTRAGSBEDINGUNGEN

In allen Vertragsbeziehungen, in denen die SAP Deutschland SE & Co. KG (nachfolgend „SAP" genannt) für andere Unternehmen, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliche Sondervermögen (nachfolgend "Auftraggeber" genannt) Leistungen erbringt – außer bei Überlassung und Pflege von Standardsoftware und/oder bei Zugänglichmachung von SAP Cloud Services – gelten ausschließlich die vorliegenden Allgemeinen Geschäftsbedingungen und die Regeln der SAP-Services Deutschland Preis- und Konditionenliste („PKL Services").

Für die Überlassung und Pflege von Standardsoftware und/oder die Zugänglichmachung von SAP Cloud Services gelten die Vereinbarungen des Softwarevertrages i.S.v. Abschnitt 1.8 abschließend.

Entgegenstehende bzw. ergänzende Bedingungen – insbesondere Allgemeine Geschäftsbedingungen des Auftraggebers – werden nicht Vertragsinhalt, auch wenn die SAP einen Vertrag (Order Form) durchführt, ohne solchen Bedingungen ausdrücklich zu widersprechen. Sofern, insbesondere aufgrund technischer Gegebenheiten bei dem Auftraggeber der jeweiligen Annahme zum SAP-Angebot (z. B. in Bestellungen) jeweils die Einkaufsbedingungen oder ähnliche Klauselwerke des Auftraggebers beigefügt werden, entfalten diese Bedingungen keinerlei Gültigkeit, auch wenn sie in der Annahme zum Angebot selbst nicht ausdrücklich ausgeschlossen werden.

1. DEFINITIONEN

1.1 „Arbeitsergebnisse" bezeichnet sämtliche Ergebnisse der Serviceleistungen der SAP unter einer jeweiligen Order Form.

1.2 „Auftraggeberdaten" bezeichnet alle vom Auftraggeber in von SAP bereitgestellten Systemen erfassten Inhalte, Materialien, Daten und Informationen, einschliesslich Auftraggeber-spezifischer Informationen (wie z. B. Berichte), die der Auftraggeber unter Verwendung derbereitgestellten Systeme erstellt hat. Darunter fallen insbesondere nicht von SAP und/oder ihren Erfüllungsgehilfen unter einer Order Form erstellte Arbeitsergebnisse und/oder Services im Sinne dieser Bedingungen.

1.3 „Berater" bezeichnet SAP Mitarbeiter und Subunternehmer der SAP einschließlich Freie Mitarbeiter, die SAP nach eigenem Ermessen zur Erbringung und Abwicklung der vertraglichen Serviceseinsetzt.

1.4 „IP Rechte" (bzw. „Rechte am geistigen Eigentum") bezeichnet ohne Einschränkung alle Patente und sonstigen Rechte an Erfindungen, Urheberrechte, Marken, Geschmacksmuster und andere Schutzrechte und sämtliche damit im Zusammenhang stehende Verwertungs- und Nutzungsrechte.

1.5 „Order Form" bezeichnet die Vereinbarungen über die Erbringung der Services. Anstelle des Begriffs „Order Form" kann auch die Bezeichnung „Vertrag" treten.

1.6 „Services" sind sämtliche Leistungen, die SAP im Sinne von Abschnitt „Geltung der Vertragsbedingungen" Absatz 1 der Geltung dieser Allgemeinen Geschäftsbedingungen unterstellt, die in einer Order Form ggf. unter Bezugnahme auf die Documente „Service Description" und/oder „Scope Document" vereinbart wurden.

1.7 „SAP Software" bezeichnet (i) sämtliche Standard-Software-Produkte und die dazugehörige Dokumentation, die für oder von SAP oder ihren verbundenen Unternehmen entwickelt worden sind; (ii) sämtliche neuen Fassungen (insbesondere Releases, Updates, Patches, Korrekturen) dieser SAP Software, die dem Auftraggeber in Durchführung des Softwarevertrages zur Verfügung gestellt werden, und (iii) sämtliche vollständigen oder teilweisen Kopien hiervon.

1.8 „Softwarevertrag" bezeichnet die Vereinbarungen über die Überlassung und Pflege von Standard-Software bzw. über die Zugänglichmachung zu SAP Cloud Services zwischen SAP (oder einem mit SAP SE im Sinne der §§ 15 ff. AktG verbundenen Unternehmen oder einem autorisierten Partner der SAP) und Auftraggeber, unter denen der Auftraggeber das Recht gewährt bekommt, SAP Software oder SAP Cloud Services zu nutzen.

1.9 „Verbundene Unternehmen" bezeichnet Unternehmen, die im Sinne des § 15 AktG ff mit einem anderen Unternehmen verbunden sind.

1.10 „Vertrauliche Informationen" bezeichnet sämtliche Informationen, die SAP oder der Auftraggeber gegen unbeschränkte Weitergabe an Dritte schützen, oder die nach den Umständen der Weitergabe oder ihrem Inhalt nach als vertraulich anzusehen sind. Jedenfalls gelten folgende Informationen als Vertrauliche Informationen von SAP: sämtliche SAP Software, Programme, Werkzeuge, Daten oder andere Materialien, die SAP dem Auftraggeber vorvertraglich oder auf Grundlage der Order Form zur Verfügung stellt.

2. LEISTUNGSERBRINGUNG

2.1 Der Auftraggeber gibt die Aufgabenstellung vor. Auf dieser Grundlage wird die Aufgabenerfüllung gemeinsam geplant. Die SAP kann hierfür ggf. ein schriftliches Konzept unterbreiten. Weitergehende Einzelheiten ergeben sich aus der Order Form.

2.2 Die SAP entscheidet, welche Berater sie zur Erfüllung und Abwicklung der Order Form einsetzt und behält sich deren Austausch jederzeit vor. SAP steht für das Verschulden von Erfüllungsgehilfen wie für eigenes Verschulden ein. Die Services können nach Wahl der SAP in den Geschäftsräumen der SAP, beim Sitz des Auftraggebers oder Remote erbracht werden. Auch soweit Services beim Auftraggeber erbracht werden, ist dieser nicht gegenüber den von SAP eingesetzten Beratern weisungsbefugt. Die Berater werden nicht in den Betrieb des Auftraggebers eingegliedert. Der Auftraggeber kann nur dem Projektkoordinator der SAP Vorgaben machen, nicht unmittelbar den einzelnen Beratern.

2.3 Der Auftraggeber trägt das Risiko, ob die in Auftrag gegebenen Services seinen Wünschen und Bedürfnissen entsprechen. Über Zweifelsfragen hat er sich rechtzeitig durch Mitarbeiter der SAP oder durch fachkundige Dritte beraten zu lassen. Der Auftraggeber hat selbstständig zu prüfen, ob durch das zugrundeliegende Projekt zusätzlicher Lizensierungsbedarf erwächst. SAP weist ausdrücklich darauf hin, dass SAP dies nicht geprüft hat und diese Prüfung nicht Gegenstand der Order Form ist.

2.4 Über die Gespräche zur Präzisierung oder Veränderung vertraglicher Gegebenheiten, insbesondere des Vertragsgegenstandes kann die SAP Gesprächsnotizen fertigen. Der Auftraggeber wird die Notizen alsbald prüfen und die SAP über eventuell notwendige Änderungen und Ergänzungen unterrichten.

2.5 Von der SAP dem Auftraggeber vorvertraglich überlassene Gegenstände (z. B. Vorschläge, Testprogramme, Konzepte) sind geistiges Eigentum der SAP (vgl. Abschnitt 7). Sie dürfen nicht vervielfältigt und Dritten nicht zugänglich gemacht werden. Wenn keine Order Form zustande kommt, sind sie zurückzugeben oder zu löschen und dürfen nicht benutzt werden. Im Übrigen gelten auch für das vorvertragliche Schuldverhältnis die Regelungen dieser Allgemeinen Geschäftsbedingungen, insbesondere die Haftungsbegrenzungsklausel des Abschnitt 10.

Falls SAP über den Umfang der Order Form hinaus mit Einverständnis des Auftraggebers Leistungen erbringt, gelten für die erbrachten Leistungen die Regelungen und Konditionen der Order Form entsprechend.

2.6 Abnahme

2.6.1 Bei allen einer Abnahme zugänglichen Arbeitsergebnissen kann die SAP eine schriftliche Abnahmeerklärung vom Auftraggeber verlangen. Der Auftraggeber nimmt Arbeitsergebnisse unverzüglich nach Maßgabe dieses Abschnitts 2.6 ab. Dazu kann ein vom Auftraggeber zu unterzeichnendes Abnahmeprotokoll erstellt werden.

2.6.2 Hat eine Order Form mehrere, vom Auftraggeber voneinander unabhängig nutzbare Einzelwerke zum Gegenstand, so werden diese Einzelwerke getrennt abgenommen.

2.6.3 Werden in einer Order Form Teilwerke definiert, so kann die SAP Teilwerke zur Abnahme vorstellen. Bei späteren Abnahmen wird allein das Funktionieren des neuen Teilwerks und das korrekte Zusammenwirken der früher abgenommenen Teilwerke mit dem neuen Teilwerk geprüft.

2.6.4 Enthält die Order Form die Erstellung eines Konzeptes, insbesondere für die Ausprägung, Änderung oder Erweiterung von Standardsoftware, so kann die SAP für das Konzept eine getrennte Abnahme verlangen.

2.6.5 Der Auftraggeber hat innerhalb von 15 Arbeitstagen das Arbeitsergebnis zu prüfen und durch den Ansprechpartner schriftlich entweder die Abnahme zu erklären oder die festgestellten Mängel mit genauer Beschreibung und Angabe der Fehlersymptomatik mitzuteilen. Wenn er sich in dieser Frist nicht erklärt o-

der den Service ohne Rüge nutzt, gilt das Arbeitsergebnis als abgenommen. Unwesentliche Mängel berechtigen nicht zur Verweigerung der Abnahme. Der produktive Einsatz oder die produktive Inbetriebnahme von (Teil-) Arbeitsergebnissen durch den Auftraggeber gilt in jedem Falle als Abnahme der jeweiligen (Teil-) Arbeitsergebnissen.

2.6.6 Die SAP beseitigt die laut Abschnitt 2.6.5 gerügten Mängel in einer der Schwere des Mangels angemessenen Frist. Nach Mitteilung der Mängelbeseitigung prüft der Auftraggeber das Leistungsergebnis binnen fünf Arbeitstagen. Im Übrigen gilt Abschnitt 2.6.5 entsprechend.

3. MITWIRKUNG DES AUFTRAGGEBERS

3.1 Der Auftraggeber sorgt für die zur Erbringung der vertragsgegenständlichen Services erforderliche Arbeitsumgebung (nachfolgend: „IT-Systeme") ggf. entsprechend den Vorgaben der SAP. Es liegt in seinem Verantwortungsbereich, den ordnungsgemäßen Betrieb der notwendigen IT-Systeme erforderlichenfalls durch Wartungsverträge mit Dritten sicherzustellen. Der Auftraggeber beachtet insbesondere die Vorgaben der SAP.

3.2 Der Auftraggeber wirkt bei der Auftragserfüllung im erforderlichen Umfang unentgeltlich mit, indem er z. B. Mitarbeiter, IT-Systeme, Daten und Telekommunikationseinrichtungen zur Verfügung stellt. Er gewährt der SAP unmittelbar und mittels Datenfernübertragung Zugang zur Software und zu den IT-Systemen. Er beantwortet Fragen und prüft Ergebnisse. Soweit der Auftraggeber für die Leistungserbringung der SAP Materialien bereitstellt, stellt er sicher, dass diese frei von Rechten Dritter sind, die der Leistungserbringung durch SAP entgegenstehen könnten.

3.3 Der Auftraggeber benennt schriftlich einen Ansprechpartner für die SAP und eine Adresse und E-Mail-Adresse, unter der die Erreichbarkeit des Ansprechpartners sichergestellt ist. Der Ansprechpartner muss in der Lage sein, für den Auftraggeber die erforderlichen Entscheidungen zu treffen oder unverzüglich herbeizuführen. Der Ansprechpartner sorgt für eine gute Kooperation mit dem Ansprechpartner bei SAP. Die Mitarbeiter des Auftraggebers, deren Tätigkeit erforderlich ist, sind in angemessenem Umfang von anderen Tätigkeiten freizustellen.

3.4 Der Auftraggeber testet Arbeitsergebnisse gründlich auf Mangelfreiheit und auf Verwendbarkeit in der konkreten Situation, bevor er mit ihrer operativen Nutzung beginnt. Dies gilt auch für Services, die er im Rahmen der Nacherfüllung erhält.

3.5 Der Auftraggeber trifft angemessene Vorkehrungen für den Fall, dass die Arbeitsergebnisse mit Störungen behaftet sind (z. B. durch Datensicherung, Störungsdiagnose, regelmäßige Überprüfung der Ergebnisse). Mangels eines ausdrücklichen schriftlichen Hinweises im Einzelfall können die von SAP eingesetzten Berater immer davon ausgehen, dass alle Daten, mit denen sie in Berührung kommen können, gesichert sind.

3.6 Der Auftraggeber erbringt darüber hinaus alle zur Vertragsdurchführung notwendigen und erforderlichen Mitwirkungsleistungen. Ergänzende Regelungen enthält ggf. die Order Form.

3.7 Die Erbringung der Mitwirkungspflichten durch den Auftraggeber ist vertragliche Hauptpflicht und Voraussetzung für die ordnungsgemäße Leistung der SAP.

3.8 Der Auftraggeber trägt Nachteile und Mehrkosten aus einer Verletzung seiner Pflichten und stellt SAP in diesem Zusammenhang von Ansprüchen Dritter frei.

4. CHANGE REQUEST-VERFAHREN

4.1 Während der Laufzeit eines Projekts können die Ansprechpartner beider Vertragspartner (Abschnitt 3.3) jederzeit schriftlich Änderungen, insbesondere der vereinbarten Services, Methoden und Termine vorschlagen.

4.2 Im Falle eines Änderungsvorschlages durch den Auftraggeber wird die SAP innerhalb von zehn Arbeitstagen mitteilen, ob die Änderung möglich ist und welche Auswirkungen sie auf die Order Form hat, insbesondere unter Berücksichtigung des zeitlichen Verlaufs und der Vergütung. Der Auftraggeber hat sodann binnen fünf Arbeitstagen der SAP schriftlich mitzuteilen, ob er seinen Änderungsvorschlag zu diesen Bedingungen aufrechterhalten will oder ob er die Order Form zu den alten Bedingungen fortführen will. Wenn die Prüfung eines Änderungsvorschlages einen nicht unerheblichen Aufwand darstellt, kann die SAP den durch die Prüfung bedingten Aufwand separat in Rechnung stellen.

4.3 Im Falle eines Änderungsvorschlages durch die SAP wird der Auftraggeber innerhalb von zehn Arbeitstagen schriftlich mitteilen, ob er der Änderung zustimmt.

4.4 Solange kein Einvernehmen über die Änderung besteht, werden die Arbeiten nach der bestehenden Order Form fortgesetzt. Der Auftraggeber kann stattdessen verlangen, dass die Arbeiten ganz oder teilweise unterbrochen oder gemäß den Voraussetzungen des Abschnitts 12.1 endgültig abgebrochen werden.

Im Fall der Unterbrechung wird ab dem 1. Arbeitstag pro Tag und SAP-Mitarbeiter im Projekt, dessen Arbeit ruht, eine Vergütung in Höhe des vereinbarten Satzes, ansonsten gemäß den in der PKL Services vorgesehenen Tagessätzen fällig. Im Fall des endgültigen Abbruchs bestimmen sich die Rechtsfolgen nach der Vorschrift des § 648a BGB.

5. VERGÜTUNG, ZAHLUNG, STEUERN, VORBEHALT

5.1 Vergütung

5.1.1 Die Vergütung richtet sich mangels anderer schriftlicher Vereinbarung nach der jeweils gültigen PKL Services.

5.1.2 SAP ist berechtigt, Teilleistungen der Services in Rechnung zu stellen.

5.1.3 Die Abrechnung nach Aufwand erfolgt auf der Grundlage einer in der Rechnung enthaltenen Aufstellung der Tätigkeiten. Erhebt der Auftraggeber gegen die in der Aufstellung getroffenen Festlegungen nicht innerhalb von zwei Wochen schriftlich Widerspruch, so gelten diese als anerkannt.

5.1.4 SAP kann Abschlagszahlungen oder volle Vorauszahlungen fordern, wenn zum Auftraggeber noch keine Geschäftsverbindung besteht, wenn die Lieferung ins Ausland erfolgen soll oder der Auftraggeber seinen Sitz im Ausland hat oder wenn Gründe bestehen, an der pünktlichen Zahlung durch den Auftraggeber zu zweifeln.

5.1.5 Der Auftraggeber kann nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen aufrechnen und ein Zurückbehaltungsrecht nur auf unbestrittene oder rechtskräftig festgestellte Ansprüche stützen. Er kann seine Forderungen – unbeschadet der Regelung des § 354 a HGB – nicht an Dritte abtreten.

5.1.6 Die SAP behält sich das Eigentum und die Rechte (Abschnitt 7) an den Arbeitsergebnissen bis zum vollständigen Ausgleich ihrer Forderungen aus der Order Form vor. Der Auftraggeber hat die SAP bei Zugriff Dritter auf das Vorbehaltsgut sofort schriftlich zu benachrichtigen und den Dritten über die Rechte der SAP zu unterrichten.

5.2 Rechnungsstellung und Fälligkeit. Zahlungen sind [redacted] fällig. Skonto wird nicht gewährt. Mit Fälligkeit kann SAP Verzugszinsen in Höhe des jeweils gültigen gesetzlichen Verzugszinssatzes verlangen.

5.3 Steuern. Alle Preise verstehen sich zuzüglich der jeweils geltenden gesetzlichen Umsatzsteuer.

6. LAUFZEIT / KÜNDIGUNG.

6.1 Laufzeit der Order Form. Soweit in der jeweiligen Order Form nicht anders geregelt, tritt jede Order Form mit Datum ihrer Letztunterzeichnung in Kraft und läuft über die in der Order Form bestimmte Laufzeit.

6.2. Kündigung. Soweit dort nichts anderes vereinbart ist, kann eine Order Form nicht ordentlich gekündigt werden. Die Kündigung aus wichtigem Grund bleibt hiervon unberührt. Ein wichtiger Grund liegt insbesondere dann vor, wenn der Auftraggeber nach schriftlicher Mahnung der SAP nicht innerhalb von 30 Tagen eine fällige wesentliche Pflicht vertragsgemäß erbracht hat, insbesondere z.B. mit einer Zahlung unter der jeweiligen Order Form mehr als 30 Tage in Verzug geraten ist.

6.3 Wirkung der Kündigung. Bei Kündigung der jeweiligen Order Form sind sämtliche Vertraulichen Informationen der Parteien der jeweils offenlegenden Partei unverzüglich zurück zu gewähren oder auf Wunsch der jeweiligen offenlegenden Partei zu zerstören und die Zerstörung entsprechend nachzuweisen.

7. RECHTE

Alle Rechte an den Services – insbesondere das Urheberrecht, die Rechte an Erfindungen sowie technische Schutzrechte – stehen im Verhältnis zum Auftraggeber ausschließlich der SAP bzw. der SAP SE (der Muttergesellschaft von SAP) zu, auch soweit die Services durch Vorgaben oder Mitarbeit des Auftraggebers entstanden sind. Wenn nichts anderes schriftlich vereinbart ist, hat der Auftraggeber an den Services mit der vollständigen Zahlung der bis einschließlich zur Abnahme fälligen Teilbeträge ein einfaches Nutzungsrecht zu dem Zweck, seine internen Geschäftsvorfälle

und die von Verbundenen Unternehmen abzuwickeln, im gleichen Umfang und Dauer wie unter dem Softwarevertrag vereinbart.

Die Nutzung ausschließlich zu Testzwecken ist vor der Abnahme in erforderlichem Umfang gestattet. Der Auftraggeber ist berechtigt, notwendige Sicherungskopien der Arbeitsergebnisse zu erstellen. Jede Sicherungskopie ist als solche zu kennzeichnen und mit dem Urheberrechtsvermerk des Originaldatenträgers zu versehen.

8. VERTRAULICHKEIT, DATENSCHUTZ

8.1. Nutzung von Vertraulichen Informationen. Die Vertragspartner verpflichten sich, alle vor und im Rahmen der Vertragserfüllung erlangten Vertraulichen Informationen des jeweils anderen Vertragspartners zeitlich unbegrenzt vertraulich zu behandeln und nur im Rahmen der Vertragserfüllung und Vertragsabwicklung zu verwenden. Das Vervielfältigen Vertraulicher Informationen in beliebiger Form ist untersagt, es sei denn, es erfolgt im Rahmen der Vertragsabwicklung und in Erfüllung des Zwecks der jeweiligen Order Form. Vervielfältigungen Vertraulicher Informationen der jeweils anderen Partei müssen alle Hinweise und Vermerke zu ihrem vertraulichen oder geheimen Charakter enthalten, die im Original enthalten sind.

In Bezug auf die Vertraulichen Informationen der jeweils anderen Partei (a) unternimmt jede Partei alle Zumutbaren Schritte (gemäß Definition unten), um alle Vertraulichen Informationen vertraulich zu behandeln und (b) gewährt jede Partei nur solchen Personen Zugriff auf die Vertraulichen Informationen der anderen Partei, die den Zugriff zur Vertragserfüllung und Vertragsabwicklung benötigen. Im Sinne dieser Vereinbarung sind „Zumutbare Schritte" solche Schritte, die der Empfänger zum Schutz seiner eigenen vergleichbaren Vertraulichen Informationen unternimmt und die mindestens einer angemessenen Sorgfalt entsprechen; dies schließt seitens des Auftraggebers die sorgfältige Verwahrung und den Schutz der Vertraulichen Informationen gegen Missbrauch ein.

8.2 Ausnahmen. Der vorstehende Abschnitt 8.1. gilt nicht für Vertrauliche Informationen, die (a) vom Empfänger ohne Rückgriff auf die Vertraulichen Informationen der offenlegenden Partei unabhängig entwickelt oder rechtmäßig und ohne Pflicht zur Geheimhaltung von einem Dritten erworben wurden, der berechtigt ist, diese Vertraulichen Informationen bereitzustellen, (b) ohne Vertragsverletzung durch den Empfänger allgemein öffentlich zugänglich geworden sind, (c) dem Empfänger zum Zeitpunkt der Offenlegung ohne Einschränkungen bekannt waren oder (d) nach schriftlicher Zustimmung der offenlegenden Partei von den vorstehenden Regelungen freigestellt sind oder (e) der Empfänger rechtmässig von einem Dritten erhalten hat, der das Recht zur Offenlegung besitzt und die Informationen ohne Einschränkungen hinsichtlich der Verwendung oder Offenlegung bereitstellt.

8.3 Vertrauliche Vertragsinhalte; Öffentlichkeit. Der Auftraggeber behandelt die Regelungen der jeweiligen Order Form, insbesondere die darin enthaltenen Preise, vertraulich. Keine der Parteien verwendet den Namen der jeweils anderen Partei ohne deren vorherige schriftliche Zustimmung in öffentlichkeitswirksamen, Werbe- oder ähnlichen Aktivitäten. In Abweichung hierzu ist SAP jedoch befugt, den Namen des Auftraggebers in Referenzkundenlisten zu verwenden, sowie anhand der vertraglichen Inhalte Analysen (z. B. zur Bedarfsprognose) zu erstellen und – vorbehaltlich jeweils einvernehmlicher Vereinbarung – in anderen Marketingaktivitäten von SAP zu verwenden. Dies schließt die Überlassung an und Verwendung zur Bedarfsanalyse durch mit SAP Verbundene Unternehmen ein. Soweit dies die Überlassung und Verwendung von Kontaktdaten von Ansprechpartnern des Auftraggebers umfasst, wird der Auftraggeber ggf. erforderliche Einwilligungen einholen.

8.4 Datenschutz. Die abschließenden Regelungen zu datenschutzrechtlichen Verpflichtungen der Vertragspartner im Rahmen möglicher Auftragsdatenverarbeitung (insbesondere im Rahmen von Fehlersuche oder bei der Beseitigung von Mängeln im Rahmen der Order Form) ergeben sich aus der den vorliegenden AGB für Services beigefügten Anlage „Vereinbarung über die Datenverarbeitung für SAP Pflege und Professional Services".

9. SACH- UND RECHTSMÄNGEL, SONSTIGE LEISTUNGSSTÖRUNGEN

9.1 Für der gesetzlichen Sach- und Rechtsmängelhaftung unterliegende Leistungen leistet SAP nach Maßgabe von Abschnitt 9.1 bis Abschnitt 9.7 Gewähr dafür, dass die Leistung die ausdrücklich vereinbarten Beschaffenheitsmerkmale hat und dass dem Übergang der vereinbarten Befugnisse auf den Auftraggeber (Abschnitt 7) keine Rechte Dritter entgegenstehen. Soweit keine Beschaffenheit vereinbart ist, bezieht sich die Haftung darauf, dass sich die Leistung für die vertraglich vorausgesetzte, sonst gewöhnliche, Verwendung eignet und eine Beschaffenheit aufweist, die bei Services dieser Art üblich ist und die der Auftraggeber bei Services dieser Art erwarten kann.

9.2 Der Auftraggeber wird der SAP auftretende Mängel unverzüglich mit genauer Beschreibung des Problems und den für die Fehlerbeseitigung nützlichen Informationen schriftlich mitteilen. Hierzu hat der Auftraggeber die Arbeitsergebnisse unverzüglich nach Ablieferung durch SAP, soweit dies nach ordnungsmäßigem Geschäftsgang tunlich ist, zu untersuchen und, wenn sich ein Mangel zeigt, diesen unverzüglich gegenüber SAP anzuzeigen. Unterlässt der Auftraggeber die Anzeige, so gilt das Arbeitsergebnis als genehmigt, es sei denn, dass es sich um einen Mangel handelt, der bei der Untersuchung nicht erkennbar war. Zeigt sich später ein solcher Mangel, so muss die Anzeige unverzüglich nach der Entdeckung gemacht werden, anderenfalls gilt das Arbeitsergebnis auch in Ansehung dieses Mangels als genehmigt. Zur Erhaltung der Rechte des Auftraggebers genügt die rechtzeitige Absendung der Anzeige. Hat SAP den Mangel arglistig verschwiegen, so kann sich SAP auf die Regelungen der vorstehenden Sätze 2 bis 5 nicht berufen. Nur der Ansprechpartner (Abschnitt 3.3) ist zu Rügen im vorstehenden Sinne befugt.

9.3 SAP leistet bei nachgewiesenen Sachmängeln Gewähr durch Nacherfüllung in der Weise, dass SAP nach ihrer Wahl dem Auftraggeber einen neuen, mangelfreien Stand der Arbeitsergebnisse überlässt oder den Mangel beseitigt. Die Mangelbeseitigung kann auch darin bestehen, dass SAP dem Auftraggeber zumutbare Möglichkeiten aufzeigt, die Auswirkungen des Mangels zu vermeiden. Bei nachgewiesenen Rechtsmängeln leistet SAP Gewähr durch Nacherfüllung, indem sie dem Auftraggeber eine rechtlich einwandfreie Benutzungsmöglichkeit an den Arbeitsergebnissen oder nach ihrer Wahl an ausgetauschten oder geänderten gleichwertigen Arbeitsergebnissen verschafft. Der Auftraggeber muss einen neuen Stand der Arbeitsergebnisse übernehmen, wenn der vertragsgemäße Funktionsumfang erhalten bleibt und die Übernahme nicht unzumutbar ist. Die Dringlichkeit der Fehlerbehebung richtet sich nach dem Grad der Betriebsbehinderung. Die Regeln der vorliegenden Bedingungen, insbesondere § 3 gelten entsprechend.

9.4 Falls die Nacherfüllung nach Ablauf einer vom Auftraggeber zu setzenden angemessenen Nachfrist endgültig fehlschlägt, kann er vom Vertrag zurücktreten oder ein Dauerschuldverhältnis kündigen oder die Vergütung mindern. Die Voraussetzungen des Abschnitts 12.1 sind bei der Nachfristsetzung zu erfüllen. Schadensersatz oder Ersatz vergeblicher Aufwendungen wegen eines Mangels leistet SAP im Rahmen der in Abschnitt 10 festgelegten Grenzen. Andere Rechte wegen Sach- oder Rechtsmängel sind ausgeschlossen.

9.5 Die Verjährungsfrist für die Ansprüche gemäß den Abschnitten 9.1 bis 9.4 beträgt ein Jahr und beginnt mit der Abnahme des jeweiligen Arbeitsergebnisses. Dies gilt auch für Ansprüche aus Rücktritt und Minderung gemäß Abschnitt 9.4 Satz 1. Die Verkürzung der Verjährungsfrist gilt nicht bei Vorsatz oder grober Fahrlässigkeit seitens SAP, arglistigem Verschweigen des Mangels, Personenschäden oder Rechtsmängeln im Sinne des § 438 Abs. 1 Nr. 1 a BGB.

9.6 Für Mängel an Nachbesserungsleistungen, Umgehungen oder Neulieferungen im Wege der Nacherfüllung endet die Verjährung ebenfalls in dem in Abschnitt 9.5 bestimmten Zeitpunkt. Die Verjährungsfrist wird jedoch, wenn SAP im Einverständnis mit dem Auftraggeber das Vorhandensein eines Mangels prüft oder die Nacherfüllung erbringt, so lange gehemmt, bis SAP das Ergebnis ihrer Prüfung dem Auftraggeber mitteilt oder die Nacherfüllung für beendet erklärt oder die Nacherfüllung verweigert. Die Verjährung tritt frühestens drei Monate nach dem Ende der Hemmung ein.

9.7 Erbringt SAP Leistungen bei Fehlersuche oder -beseitigung, ohne hierzu verpflichtet zu sein, so kann SAP eine Vergütung gemäß Abschnitt 5.1 verlangen. Dies gilt insbesondere, wenn ein gemeldeter Sachmangel nicht nachweisbar ist oder SAP nicht zuzuordnen ist, oder wenn die SAP Software nicht in Übereinstimmung mit der Dokumentation genutzt wird. Zu vergüten ist insbesondere auch der Mehraufwand bei der Beseitigung von Mängeln, der bei SAP dadurch entsteht, dass der Auftraggeber seine Mitwirkungspflichten nicht ordnungsgemäß erfüllt, die SAP Software oder Arbeitsergebnisse unsachgemäß bedient oder von SAP empfohlene SAP-Services nicht in Anspruch genommen hat.

9.8 Wenn ein Dritter Ansprüche behauptet, die der Ausübung der vertraglich eingeräumten Nutzungsbefugnis entgegenstehen, so hat der Auftraggeber SAP unverzüglich schriftlich und umfassend zu unterrichten. Stellt der Auftraggeber die Nutzung der Arbeitsergebnisse aus Schadensminderungs- oder sonstigen wichtigen Gründen ein, ist er verpflichtet, den Dritten darauf hinzuweisen, dass mit der Nutzungseinstellung ein Anerkenntnis der behaupteten Schutzrechtsverletzung nicht verbunden ist. Er wird die gerichtliche Auseinandersetzung mit dem Dritten nur im Einvernehmen mit der SAP führen oder SAP zur Führung der Auseinandersetzung ermächtigen.

9.9 Erbringt SAP außerhalb des Bereichs der Sach- und Rechtsmängelhaftung Services nicht oder nicht ordnungsgemäß oder begeht SAP eine sonstige Pflichtverletzung, so hat der Auftraggeber dies gegenüber SAP stets schriftlich zu rügen und SAP eine Nachfrist einzuräumen, innerhalb derer SAP Gelegenheit zur ordnungsgemäßen Erfüllung der Services oder dazu gegeben wird, in sonstiger Weise Abhilfe zu schaffen. Es gilt Abschnitt 12.1. Für Schadensersatz oder Ersatz vergeblicher Aufwendungen gelten die in Abschnitt 10 festgelegten Grenzen.

10. HAFTUNG.

10.1 In allen Fällen vertraglicher und außervertraglicher Haftung leistet SAP Schadensersatz oder Ersatz vergeblicher Aufwendungen nur in dem nachfolgend bestimmten Umfang:

[redacted]

10.3 Für alle Ansprüche gegen SAP auf Schadensersatz oder Ersatz vergeblicher Aufwendungen bei vertraglicher und außervertraglicher Haftung gilt eine Verjährungsfrist von einem Jahr. Die Verjährungsfrist beginnt mit dem in § 199 Abs. 1 BGB bestimmten Zeitpunkt. Sie tritt spätestens mit Ablauf von 5 Jahren ab Entstehung des Anspruchs ein. Die Regelungen der Sätze 1 bis 3 dieses Absatzes gelten nicht für die Haftung bei Vorsatz oder grober Fahrlässigkeit oder bei Personenschäden oder nach dem Produkthaftungsgesetz. Die abweichende Verjährungsfrist für Ansprüche wegen Sach- und Rechtsmängeln (Abschnitte 9.5 und 9.6) bleibt von den Regelungen dieses Absatzes unberührt.

11. VERTRAGSÜBERTRAGUNG

Der Auftraggeber ist nicht berechtigt die jeweilige Order Form oder einzelne Rechte und Pflichten daraus auf einen Dritten zu übertragen.

12. SCHLUSSBESTIMMUNGEN

12.1 Die Zusammenarbeit erfordert ein hohes Maß an Vertrauen, Zusammenwirken und Einigungsbereitschaft. Durch Gesetz oder Vertrag vorgesehene Fristsetzungen des Auftraggebers müssen – außer in Eilfällen – mindestens zehn Arbeitstage betragen. Soll der fruchtlose Ablauf einer gesetzten Frist den Auftraggeber zur Lösung vom Vertrag (z. B. durch Rücktritt, Kündigung oder Schadensersatz statt der Leistung) oder zur Minderung der Vergütung berechtigen, so muss der Auftraggeber diese Konsequenzen des fruchtlosen Fristablaufs schriftlich zusammen mit der Fristsetzung androhen. SAP kann nach Ablauf einer gemäß Satz 2 gesetzten Frist verlangen, dass der Auftraggeber seine aus dem Fristablauf resultierenden Rechte binnen zwei Wochen nach Zugang der Aufforderung ausübt.

12.2 SAP kann Angebote von Auftraggebern innerhalb von vier Wochen annehmen. Angebote von SAP sind freibleibend, soweit schriftlich nichts anderes vereinbart ist. Im Zweifel sind das Angebot oder die Auftragsbestätigung seitens SAP für den Vertragsinhalt der Order Form maßgeblich.

12.3. Leistungszeit.

12.3.1. Termine sind unverbindlich, es sei denn, sie sind ausdrücklich und schriftlich als verbindlich vereinbart. Die Pflicht der SAP zur Realisierung beginnt erst mit der Abnahme des Konzeptes durch den Auftraggeber.

12.3.2. Wenn die SAP auf eine Mitwirkung oder Information des Auftraggebers wartet oder durch Streik, Aussperrung, behördliches Eingreifen oder andere unverschuldete Umstände in der Auftragsdurchführung behindert ist, gelten Liefer- und Leistungsfristen um die Dauer der Behinderung und um eine angemessene Anlaufzeit nach Ende der Behinderung als verlängert. Die SAP wird dem Auftraggeber die Behinderung mitteilen.

12.3.3. Arbeitstage sind die Wochentage von Montag bis Freitag (08:00 Uhr bis 17:00 Uhr MEZ), außer bundeseinheitliche Feiertagen und dem 24. und 31. Dezember.

12.4 Die Services der SAP, einschließlich davon betroffener SAP Software unterliegen den Ausfuhrkontrollgesetzen verschiedener Länder, insbesondere den Gesetzen der Vereinigten Staaten von Amerika und der Bundesrepublik Deutschland. Der Auftraggeber verpflichtet sich, die Services, nicht ohne vorherige schriftliche Zustimmung von SAP an eine Regierungsbehörde zur Prüfung einer eventuellen Nutzungsrechtseinräumung oder zu anderweitiger behördlicher Genehmigung zu übergeben und sie nicht in Länder oder an natürliche oder juristische Personen zu exportieren, für die gemäß den entsprechenden Ausfuhrgesetzen Exportverbote gelten. Ferner ist der Auftraggeber für die Einhaltung aller geltenden rechtlichen Vorschriften des Landes, in dem sich der Hauptsitz des Auftraggebers befindet, und anderer Länder in Bezug auf die Nutzung der SAP Software durch den Auftraggeber und seine Verbundenen Unternehmen verantwortlich.

12.5 Für alle vertraglichen und außervertraglichen Ansprüche gilt ausschließlich deutsches Recht ohne das UN-Kaufrecht. Das Kollisionsrecht findet keine Anwendung. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit der Order Form ist Karlsruhe, sofern der Auftraggeber Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist.

12.6 Vertragsänderungen und -ergänzungen sowie alle vertragsrelevanten Willenserklärungen und Erklärungen zur Ausübung von Gestaltungsrechten, insbesondere Kündigungen, Mahnungen oder Fristsetzungen bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis. Das Schriftformerfordernis kann auch durch Briefwechsel oder (abgesehen von Kündigungen) durch elektronisch übermittelte Unterschriften (Telefax, Übermittlung eingescannter Unterschriften via Email, oder andere durch oder im Auftrag von SAP bereitgestellte, vereinbarte elektronische Vertragsschlussverfahren, wie z. B. den SAP Store) eingehalten werden. § 127 Abs. 2 und 3 BGB finden jedoch im Übrigen keine Anwendung.

12.7 Services, die nicht von der ausdrücklichen Leistungsbeschreibung der jeweiligen Order Form erfasst sind, sind gesondert schriftlich zu vereinbaren. Mangels abweichender Vereinbarung gelten für diese Services die Allgemeinen Geschäftsbedingungen von SAP für SAP Services und die Vergütungspflicht nach Maßgabe der jeweils gültigen PKL Services.

ANLAGE „VEREINBARUNG ÜBER DIE DATENVERARBEITUNG FÜR SAP PFLEGE UND PROFESSIONAL SERVICES"

1. HINTERGRUND

1.1 Zweck und Anwendung. Dieses Dokument ("DPA") wird in die Vereinbarung einbezogen und ist Teil eines schriftlichen (auch in elektronischer Form geschlossenen) Vertrags zwischen SAP und dem Auftraggeber. Dieses DPA gilt für Personenbezogene Daten, die vom Auftraggeber und den Verantwortlichen im Zusammenhang mit der Erbringung von SAP Diensten zugänglich gemacht werden. Die SAP Dienste („SAP Dienste") werden in der jeweiligen Vereinbarung, die auf dieses DPA verweist bestimmt; hierbei kann sich um folgende Leistungen handeln:

(a) Pflege (auch: Support), wie im Software- und Pflegevertrag festgelegt; und/oder

(b) Professional Services, wie im Vertrag zwischen Auftraggeber und SAP beschrieben („Service Vertrag").

1.2 Struktur. Die Anhänge 1 und 2 sind Bestandteil dieses DPA. Sie legen den vereinbarten Gegenstand, die Art und den Zweck der Verarbeitung, die Art der Personenbezogenen Daten, die Kategorien der Betroffenen Personen und die anzuwendenden technischen und organisatorischen Maßnahmen fest.

1.3 GDPR / DSGVO. SAP und der Auftraggeber sind sich darüber einig, dass es in der Verantwortung jeder Partei liegt, die Anforderungen zu überprüfen und zu übernehmen, die durch die Datenschutz Grundverordnung 2016/679 ("DSGVO") an die Verantwortlichen und Auftragsverarbeiter gestellt werden, insbesondere in Bezug auf die Artikel 28 und 32 bis 36 der DSGVO, wenn und soweit sie auf die Personenbezogenen Daten des Auftraggebers/der Verantwortlichen anwendbar sind, die im Rahmen der Leistungserbringung verarbeitet werden. Zur Veranschaulichung sind in Anhang 3 die relevanten DSGVO-Anforderungen und die entsprechenden Abschnitte in diesem DPA aufgeführt.

1.4 Governance. SAP wird als Auftragsverarbeiter tätig. Der Auftraggeber und die Rechtspersonen, denen der Auftraggeber ermöglicht, Personenbezogene Daten in für SAP bei Erbringung der SAP Dienste zugängliche Systeme einzubringen, handeln als Verantwortliche im Rahmen des DPA. Der Auftraggeber ist einziger Kontaktpunkt und allein verantwortlich für die Einholung aller relevanten Genehmigungen, Zustimmungen und Einwilligungen für die Verarbeitung Personenbezogener Daten gemäß diesem DPA, sowie, soweit erforderlich, der Zustimmung der Verantwortlichen zum Einsatz von SAP als Auftragsverarbeiter. Soweit vom Auftraggeber Genehmigungen, Zustimmungen, Weisungen oder Einwilligungen erteilt werden, werden diese nicht nur im Namen des Auftraggebers, sondern auch im Namen anderer Verantwortlicher denen der Auftraggeber die Einbringung von Personenbezogenen Daten eröffnet hat, erteilt. Wenn SAP den Auftraggeber informiert oder ihm Meldungen übermittelt, gelten diese Informationen oder Meldungen als von denjenigen Verantwortlichen erhalten, denen der Auftraggeber die Einbringung der Personenbezogenen Daten ermöglicht hat. Es liegt in der Verantwortung des Auftraggebers, diese Informationen und Meldungen an die entsprechenden Verantwortlichen weiterzuleiten.

2. SICHERHEIT DER VERARBEITUNG

Angemessene Technische und Organisatorische Maßnahmen. SAP hat die in Anhang 2 aufgeführten technischen und organisatorischen Maßnahmen umgesetzt und wird diese anwenden. Der Auftraggeber hat diese Maßnahmen geprüft und erklärt sich damit einverstanden, dass hinsichtlich des vom Auftraggeber jeweils vereinbarten SAP Dienstes die Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, des Kontextes und der Zwecke der Verarbeitung Personenbezogener Daten angemessen sind. Anlage 2 findet nur insoweit Anwendung, als die SAP Dienste in SAP Räumlichkeiten oder aus SAP Räumlichkeiten heraus erbracht werden. Erbringt SAP die SAP Dienste in Räumlichkeiten des Auftraggebers und räumt der Auftraggeber SAP Zugang zu den Systemen und Daten des Auftraggebers ein, wird SAP die angemessenen administrativen, technischen und physischen Bedingungen des Auftraggebers einhalten, um diese Daten zu schützen und vor unbefugtem Zugriff zu bewahren. Im Zusammenhang mit jedem Zugriff auf das System und die Daten des Auftraggebers wird der Auftraggeber eigenverantwortlich dem SAP Personal Passwörter und Berechtigungen und für den Zugriff auf seine Systeme zuteilen, diese Passwörter und Berechtigungen widerrufen sowie die Zugriffsmöglichkeit beenden, sobald er dies für angemessen hält. Der Auftraggeber gewährt SAP keinen Zugang zu Systemen oder Informationen des Auftraggebers oder eines Dritter, es sei denn, dieser Zugang ist für die Erbringung der SAP Dienste unerlässlich. Der Auftraggeber darf keine Personenbezogenen Daten in nicht-produktiven Umgebungen speichern.

2.1 Änderungen. SAP wendet die in Anhang 2 beschriebenen technischen und organisatorischen Maßnahmen auf alle SAP-Kunden, die vergleichbare SAP Dienste beziehen gleichermaßen an. SAP kann die in Anhang 2 aufgeführten Maßnahmen jederzeit ohne Vorankündigung ändern, solange sie ein vergleichbares oder besseres Sicherheitsniveau aufrechterhält. Einzelne Maßnahmen können durch neue Maßnahmen ersetzt werden, die dem gleichen Zweck dienen, ohne das Sicherheitsniveau zum Schutz Personenbezogener Daten zu verringern.

3. SAP PFLICHTEN

3.1 Weisungen des Auftraggebers. SAP wird Personenbezogene Daten nur in Übereinstimmung mit den dokumentierten Weisungen des Auftraggebers verarbeiten. Die Vereinbarung (einschließlich dieses DPA) stellt eine solche dokumentierte Erst-Weisung dar. Der Auftraggeber kann während der Erbringung der SAP Dienste weitere Weisung geben. SAP unternimmt alle zumutbaren Anstrengungen, um allen anderen Weisungen des Auftraggebers zu folgen, soweit sie nach Datenschutzrecht erforderlich, technisch durchführbar und ohne Änderungen an der Erbringung der SAP Dienste möglich sind. Sollte eine der vorgenannten Ausnahmen zu treffen oder SAP anderweitig einer Weisung nicht nachkommen können oder der Meinung sein,

dass eine Weisung gegen das Datenschutzrecht verstößt, wird SAP den Auftraggeber unverzüglich benachrichtigen (E-Mail erlaubt).

3.2 **Verarbeitung auf Basis rechtlicher Erfordernisse.** SAP kann auch Personenbezogene Daten verarbeiten, sofern dies nach geltendem Recht erforderlich ist. In einem solchen Fall wird SAP den Auftraggeber vor der Verarbeitung über diese rechtlichen Anforderungen informieren, es sei denn, das betreffende Recht verbietet solche Informationen wegen eines wichtigen öffentlichen Interesses.

3.3 **Befugte Personen.** Zur Verarbeitung Personenbezogener Daten gewähren SAP und seine Unterauftragsverarbeiter nur befugten Personen Zugang, die sich zur Vertraulichkeit verpflichtet haben. SAP und seine Unterauftragsverarbeiter werden die Personen, die Zugang zu Personenbezogenen Daten haben, regelmäßig in Bezug auf die anwendbaren Datensicherheits- und Datenschutzmaßnahmen schulen.

3.4 **Kooperation.** Auf Wunsch des Auftraggebers wird SAP angemessen mit dem Auftraggeber und den Verantwortlichen zusammenarbeiten, um Anfragen von Betroffenen Personen oder Aufsichtsbehörden bezüglich der Verarbeitung Personenbezogener Daten durch SAP oder einer Verletzung Personenbezogener Daten zu bearbeiten. SAP wird den Auftraggeber so bald wie zumutbar möglich über jede Anfrage informieren, die SAP von einer Betroffenen Person im Zusammenhang mit der Verarbeitung des Schutz es Personenbezogener Daten erhalten hat, ohne selbst auf diese Anfrage ohne weitere Weisungen des Auftraggebers zu antworten. SAP wird gemäß den Weisungen des Auftraggebers und dem Datenschutzrecht Personenbezogene Daten, die sich im Besitz von SAP befinden (falls zutreffend) berichtigen oder löschen oder deren Verarbeitung einschränken.

3.5 **Meldung von Verletzungen des Schutzes Personenbezogener Daten.**
SAP wird dem Auftraggeber eine Verletzung des Schutzes Personenbezogener Daten unverzüglich nach Kenntniserlangung melden und ihm angemessene und SAP vorliegende Informationen zur Verfügung stellen, um ihn bei der Erfüllung seiner Verpflichtungen zur Meldung einer Verletzung des Schutzes Personenbezogener Daten gemäß den Anforderungen des Datenschutzrechts zu unterstützen. SAP kann diese Informationen in Abschnitten zur Verfügung stellen, je nachdem, zu welchem Zeitpunkt sie verfügbar werden. Eine solche Meldung ist kein Eingeständnis des Verschuldens oder der Haftung von SAP oder dahingehend auszulegen.

3.6 **Datenschutz-Folgenabschätzung.** Wenn der Auftraggeber (oder seine für die Verarbeitung Verantwortlichen) gemäß Datenschutzrecht verpflichtet sind, eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation mit einer Aufsichtsbehörde durchzuführen, stellt SAP auf Wunsch des Auftraggebers diejenigen Dokumente zur Verfügung, die für die SAP Dienste allgemein verfügbar sind (z.B. dieses DPA, die Vereinbarung, Auditberichte oder Zertifizierungen). Jede zusätzliche Unterstützung wird zwischen den Vertragsparteien einvernehmlich vereinbart.

4. DATEN LÖSCHUNG

Der Auftraggeber erteilt SAP hiermit die Weisung, die bei SAP verbliebenen Personenbezogenen Daten innerhalb einer angemessenen Zeit gemäß dem Datenschutz zu löschen (spätestens innerhalb von 6 Monaten) nachdem diese nicht mehr für die Vertragserfüllung benötigt werden, es sei denn, deren Aufbewahrung ist nach anwendbarem Recht erforderlich.

5. ZERTIFIZIERUNGEN UND AUDITS

5.1 **Auftraggeber Audit.** Der Auftraggeber oder ein von ihm beauftragter unabhängiger externer und für SAP zumutbarer Prüfer (unter Ausschluss von Prüfern, die entweder Wettbewerber der SAP sind, oder nicht angemessen qualifiziert oder unabhängig sind) können die Service und Support Center und die IT-Sicherheitspraktiken von SAP im Hinblick auf die von SAP verarbeiteten Personenbezogenen Daten prüfen, wenn:

(a) SAP keinen ausreichenden Nachweis über die Einhaltung der technischen und organisatorischen Maßnahmen. durch eine Zertifizierung über die Einhaltung von ISO 27001 oder anderer Standards (Umfang gemäß der Regelung im Zertifikat) erbracht hat. Die Zertifizierungen sind unter folgendem Link oder auf Anfrage erhältlich: https://www.sap.com/corporate/en/company/quality.html#certificates;oder

(b) Eine Verletzung des Schutzes Personenbezogener Daten vorliegt; oder

(c) eine Prüfung offiziell durch eine Aufsichtsbehörde des Auftraggebers verlangt wird; oder

(d) der Auftraggeber gemäß zwingendem Datenschutzrecht über ein direktes Auditrecht verfügt, und der Auftraggeber nur einmal binnen eines 12-Monatszeitraums auditiert, es sei den zwingendes Datenschutzrecht verlangt häufigere Audits.

5.2 **Audits anderer Verantwortlicher.** Jeder andere Verantwortliche darf die Service und Support Center und die IT-Sicherheitspraktiken von SAP, die für die von SAP verarbeiteten Personenbezogenen Daten relevant sind, nur dann gemäß Abschnitt 5.1 überprüfen, wenn einer der in Abschnitt 5.1 genannten Fälle auf den anderen Verantwortlichen zutrifft. Eine solche Prüfung muss durch den Auftraggeber gemäß Abschnitt 5.1 durchgeführt werden, es sei denn, die Prüfung muss von dem anderen Verantwortlichen selbst nach dem Datenschutzrecht durchgeführt werden. Wenn mehrere Verantwortliche, deren Personenbezogene Daten von SAP auf der Grundlage der Vereinbarung verarbeitet werden, ein Audit erfordern, wird der Auftraggeber alle angemessenen Mittel einsetzen, um die Audits zu kombinieren und Mehrfach-Audits zu vermeiden.

5.3 **Umfang des Audits.** Der Auftraggeber ist verpflichtet, Audits mindestens sechzig Tage im Voraus anzukündigen, es sei denn, dass zwingendes Datenschutzrecht oder eine zuständige Datenschutzbehörde eine kürzere Frist vorschreiben. Häufigkeit, Zeitraum und Umfang der Audits sind zwischen den Parteien vernünftig und nach Treu und Glauben einvernehmlich

zu vereinbaren. Auftraggeberaudits sind, soweit möglich, auf Fern-Audits beschränkt. Wenn ein Vor-Ort Audit rechtlich verpflichtend vorzunehmen ist, ist dieser auf maximal einen Werktag beschränkt. Über solche Einschränkungen hinaus werden die Parteien aktuelle Zertifizierungen oder andere Auditberichte verwenden, um wiederholte Audits zu vermeiden oder zu minimieren. Der Auftraggeber hat SAP die Ergebnisse eines jeden Audits zur Verfügung zu stellen.

5.4 **Auditkosten.** Der Auftraggeber trägt die Kosten von Audits, es sei denn, ein solches Audit deckt einen wesentlichen Verstoß von SAP gegen dieses DPA auf, in diesem Fall trägt SAP die eigenen Kosten des Audits. Falls sich aus einem Audit ergibt, dass SAP Ihren Verpflichtungen aus diesem DPA nicht nachgekommen ist, heilt SAP diesen Verstoß umgehend auf eigene Kosten.

6. UNTERAUFTRAGSVERARBEITER

6.1 **Zulässiger Einsatz.** SAP erhält hiermit eine vorherige allgemeine schriftliche Genehmigung, die Verarbeitung von Personenbezogenen Daten unter den nachfolgenden Voraussetzungen auf Unterauftragsverarbeiter zu übertragen:

(a) SAP oder SAP SE im Namen der SAP beauftragt Unterauftragsverarbeiter im Rahmen schriftlicher Verträge (einschließlich elektronischer Form), die mit den Bestimmungen dieses DPA in Bezug auf die Verarbeitung Personenbezogener Daten durch den Unterauftragnehmer übereinstimmen. SAP haftet für etwaige Verstöße durch den Unterauftragsverarbeiter gemäß den Bestimmungen der Vereinbarung;

(b) SAP wird die Sicherheits-, Datenschutz- und Vertraulichkeitspraktiken eines Unterauftragsverarbeiters vor dessen Auswahl bewerten, um festzustellen, dass er in der Lage ist, das in diesem DPA geforderte Schutzniveau für Personenbezogene Daten zu bieten;

(c) Für Pflege wird die bei Vertragsschluss gültige Liste der Unterauftragsverarbeiter der SAP von SAP veröffentlicht oder dem Auftraggeber auf Anfrage zur Verfügung gestellt, einschließlich des Namens, der Anschrift und der Rolle jedes Unterauftragsverarbeiters, den SAP zur Erbringung der SAP Dienste einsetzt.

(d) Für Professional Services wird SAP auf Anfrage des Kunden die Liste zur Verfügung stellen oder die Unterauftragsverarbeiter vor dem Beginn der jeweiligen Professional Services identifizieren.

6.2 **Neue Unterauftragsverarbeiter.** Der Einsatz von Unterauftragsverarbeitern erfolgt nach Ermessen der SAP unter der Voraussetzung, dass folgende Regelungen eingehalten werden:

(a) SAP informiert den Auftraggeber im Voraus über jegliche geplante Hinzufügungen oder Ersetzungen zu der Liste der Unterauftragsverarbeiter, einschließlich des Namens, der Anschrift und der Rolle des neuen Unterauftragsverarbeiters. Für Pflege erfolgt dies über ein Bekanntmachung auf dem SAP Support Portal oder über E-Mail (nachdem der Auftraggeber sich im SAP Portal entsprechend registriert hat). Für Professional Services über ein Bekanntmachung auf dem SAP Support Portal, E-Mail, oder über eine schriftliche Benachrichtigung.

(b) Der Auftraggeber kann solchen Änderungen gemäß Abschnitt 6.3 widersprechen.

6.3 **Widerspruch gegen neue Unterauftragsverarbeiter.**

(a) Für Pflege gilt: Sofern der Auftraggeber gemäß Datenschutzrecht einen berechtigten Grund hat, der Verarbeitung Personenbezogener Daten durch die neuen Unterauftragsverarbeiter zu widersprechen, kann er die Pflege durch schriftliche Erklärung gegenüber SAP kündigen, spätestens jedoch zum Ablauf von dreißig Tagen nach dem Datum der Information von SAP an den Auftraggeber über den neuen Unterauftragsverarbeiter. Kündigt der Auftraggeber nicht innerhalb dieser Frist von dreißig Tagen, so gilt der neue Unterauftragsverarbeiter als durch den Auftraggeber genehmigt.
Innerhalb der Dreißig-Tagesperiode ab dem Datum der Information von SAP an den Auftraggeber, in der der Auftraggeber über den neuen Unterauftragsverarbeiter informiert wird, kann der Auftraggeber verlangen, dass die Parteien in gutem Glauben zusammenkommen und eine Lösung des Widerspruchs besprechen. Diese Besprechungen verlängern die Kündigungsfrist nicht und berühren nicht das Recht von SAP, den/die neuen Unterauftragsverarbeiter nach Ablauf der Frist von dreißig Tagen in Dienst nehmen zu dürfen.

(b) Für Professional Services gilt: Sofern der Auftraggeber gemäß Datenschutzrecht einen berechtigten Grund hat, der Verarbeitung Personenbezogener Daten durch die neuen Unterauftragsverarbeiter zu widersprechen, kann er SAP innerhalb von fünf Werktagen nach der Information durch SAP gemäß Ziffer 6.2 schriftlich widersprechen. Widerspricht der Auftraggeber der Verwendung des Unterauftragsverarbeiters, kommen die Parteien in gutem Glauben zusammen, um eine Lösung zu besprechen. SAP kann sich entscheiden: (i) den Unterauftragsverarbeiter nicht zu verwenden oder (ii) die vom Auftraggeber in seinem Widerspruch geforderten Korrekturmaßnahmen zu ergreifen und den Unterauftragsverarbeiter zu verwenden. Wenn keine dieser Optionen vernünftigerweise möglich ist und der Auftraggeber weiterhin aus einem berechtigten Grund Einspruch erhebt, kann jede Partei die betreffenden Professional Services mit einer Frist von fünf Tagen schriftlich kündigen. Widerspricht der Auftraggeber nicht innerhalb von fünf Tagen nach Erhalt der Mitteilung, so gilt die Annahme des Unterauftragsverarbeiter als erfolgt. Bleibt der Widerspruch des Auftraggebers dreißig Tage nach seiner Erhebung ungelöst und hat SAP keine Kündigung erhalten, so gilt der Unterauftragsverarbeiter als akzeptiert.

(c) Jede Kündigung nach diesem Abschnitt 6.3 wird von beiden Parteien als unverschuldet betrachtet und unterliegt den Bestimmungen der Vereinbarung.

6.4 **Notfallaustausch.** SAP kann einen Unterauftragsverarbeiter ohne vorherige Mitteilung austauschen, wenn sich der Grund für den Austausch der zumutbaren Kontrolle von SAP entzieht und der umgehende Austausch aus Sicherheits- oder anderen

dringenden Gründen erforderlich ist. In diesem Fall informiert SAP den Auftraggeber über den neuen Unterauftragsverarbeiter unverzüglich nach seiner Ernennung. Abschnitt 6.3 gilt entsprechend.

7. INTERNATIONALE VERARBEITUNG

7.1 **Regeln für internationale Verarbeitung.** SAP ist berechtigt, die Verarbeitung von Personenbezogene Daten auch unter Einbeziehung von Unterauftragsverarbeitern im Sinne dieses DPA außerhalb des Landes, in dem sich der Auftraggeber befindet unter Einhaltung des Datenschutzrechts durchzuführen.

7.2 **Standardvertragsklauseln (Standarddatenschutzklauseln).** Sofern (i) Personenbezogene Daten eines EWR- oder schweizerischen Verantwortlichen in einem Land außerhalb des EWR, der Schweiz bzw. außerhalb eines Landes, einer Organisation oder eines Gebiets, das von der Europäischen Union als sicheres Land mit einem angemessenen Datenschutzniveau gemäß Art. 45 GDPR anerkannt ist, verarbeitet werden, oder (ii) Personenbezogene Daten eines anderen Verantwortlichen international verarbeitet werden und eine solche internationale Verarbeitung ein angemessenes Mittel nach dem anwendbaren Recht des Verantwortlichen erfordert, und das angemessene Mittel durch den Abschluss von Standardvertragsklauseln erfüllt werden kann, gilt:

- (a) SAP und der Auftraggeber vereinbaren die Geltung der Standardvertragsklauseln;
- (b) Der Auftraggeber vereinbart die Standardvertragsklauseln mit jedem relevanten Unterauftragsverarbeiter wie folgt: (i) Der Auftraggeber tritt als unabhängiger Inhaber von Rechten und Pflichten den Standardvertragsklauseln bei, die zwischen SAP oder SAP SE und dem Unterauftragsverarbeiter vereinbart wurden („Beitrittsmodell") oder (ii) der Unterauftragsverarbeiter (vertreten durch SAP) vereinbart die Standardvertragsklauseln mit dem Auftraggeber ("Vollmachtsmodell"). Das Vollmachtsmodell gilt, wenn und soweit SAP ausdrücklich über die Liste der Unterauftragsverarbeiter gemäß Abschnitt 6.1(c) oder Abschnitt 6.1.(d) oder über eine Mitteilung an den Auftraggeber erklärt hat, dass dieses Modell für einen Unterauftragsverarbeiter verfügbar ist; und/oder
- (c) Andere Verantwortliche, denen der Auftraggeber die Einbringung von Personenbezogenen Daten gemäß der Vereinbarung gestattet hat, können ebenfalls die Standardvertragsklauseln mit SAP und/oder den relevanten Unterauftragsverarbeitern in gleicher Weise wie der Auftraggeber gemäß den obigen Abschnitten 7.2 (a) und (b) vereinbaren. In diesen Fällen vereinbart der Auftraggeber die Standardvertragsklauseln im Namen der anderen Verantwortlichen.

7.3 **Bezug zwischen Standardvertragsklauseln und Vereinbarung.** Keine der Bestimmungen in der Vereinbarung darf bei widersprüchlichen Regelungen dahingehend ausgelegt werden, dass sie Vorrang vor einer Bestimmung der Standardvertragsklauseln hat. Zur Klarstellung: Wo dieses DPA Regelungen für Audit und Unterauftragsverarbeiter in den Abschnitten 5 und 6 näher beschreibt, gelten diese Regelungen auch in Bezug auf die Standardvertragsklauseln.

7.4 **Für die Standardvertragsklauseln geltendes Recht.** Die Standardvertragsklauseln unterliegen dem Recht des Landes, in dem der Verantwortliche seinen Sitz hat.

8. DOKUMENTATION; VERARBEITUNGSVERZEICHNIS

Jede Partei ist für die Einhaltung ihrer Dokumentationspflichten verantwortlich, insbesondere für die Führung von Verarbeitungsverzeichnissen, soweit dies nach dem Datenschutzrecht erforderlich ist. Jede Partei unterstützt die andere Partei in angemessener Weise bei der Erfüllung von deren Dokumentationspflichten, einschließlich der Bereitstellung der Informationen, die die andere Partei von ihr benötigt, in einer von der anderen Partei angeforderten angemessenen Form (z. B. durch die Verwendung eines elektronischen Systems), damit die andere Partei den Verpflichtungen im Zusammenhang mit der Führung von Verarbeitungsverzeichnissen nachkommen kann.

9. DEFINITIONEN

Hervorgehobene Begriffe, die hier nicht definiert werden, haben die ihnen in der Vereinbarung zugewiesene Bedeutung.

9.1 **"Auftragsverarbeiter"** bezeichnet eine natürliche oder juristische Person, öffentliche Behörde oder Agentur oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, sei es direkt als Auftragsverarbeiter eines Verantwortlichen oder indirekt als Unterauftragsverarbeiter eines Auftragsverarbeiters, der Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

9.2 **"Autorisierte Benutzer"** sind alle Personen, denen der Auftraggeber in Übereinstimmung mit einer SAP-Softwarelizenz den Zugang zur Nutzung der SAP-Dienste erteilt. Dies kann ein Mitarbeiter, Agent, externer Mitarbeiter oder Vertreter des (i) Auftraggebers, (ii) Verbundenen Unternehmen des Auftraggebers und/oder (iii) Geschäftspartnern des Auftraggebers und der Verbundenen Unternehmen des Auftraggebers (gemäß der Definition im Software- und Pflegevertrags) sein.

9.3 **"Betroffene Person"** bezeichnet eine identifizierte oder identifizierbare natürliche Person gemäß der Definition im Datenschutzrecht.

9.4 **"Datenschutzrecht"** bezeichnet die geltenden Rechtsvorschriften zum Schutz der Grundrechte und Freiheiten von Personen und deren Persönlichkeitsrecht in Bezug auf die Verarbeitung von Personenbezogenen Daten im Rahmen der Vereinbarung (und beinhaltet in Bezug auf die Beziehung zwischen den Parteien bezüglich der Verarbeitung Personenbezogener Daten

durch SAP im Auftrag des Auftraggebers, die DSGVO als Mindeststandard, unabhängig davon, ob die Personenbezogenen Daten der DSGVO unterliegen oder nicht.).

9.5 **"Personenbezogene Daten"** bezeichnet alle Informationen in Bezug auf eine Betroffene Person, die dem Schutz des Datenschutzrechts unterliegen. In diesem DPA sind darunter nur diejenigen personenbezogenen Daten zu verstehen, die SAP oder Ihren Unterauftragsverarbeitern bereitgestellt werden oder auf die SAP oder Ihre Unterauftragsverarbeiter zugreifen, um die SAP Dienste gemäß der Vereinbarung zu leisten.

9.6 **"Professional Services"** bedeutet Implementierungsleistungen, Beratungsleistungen und/oder Leistungen wie SAP Premium Engagement Support Services, Innovative Business Solutions Development Services, Innovative Business Solutions Development Support Services.

9.7 **"Standardvertragsklauseln"** (auch als „EU-Modellklauseln" bezeichnet) bezeichnet die Standardvertragsklauseln (Auftragsverarbeiter) bzw. jegliche nachfolgenden von der Europäischen Kommission veröffentlichten Versionen dieser Klauseln (die automatisch gelten). Die bei Vertragsschluss geltenden Standardvertragsklauseln sind hierzu als Anhang 4 beigefügt.

9.8 **"Unterauftragsverarbeiter"** bezeichnet Verbundene Unternehmen der SAP, die SAP SE, sowie Verbundene Unternehmen der SAP SE, sowie Dritte, die von SAP, der SAP SE oder den Verbundenen Unternehmen der SAP SE zur Erbringung der SAP Dienste eingesetzt werden, und die Personenbezogene Daten gemäß diesem DPA verarbeiten.

9.9 **"Verantwortlicher"** bezeichnet die natürliche oder juristische Person, öffentliche Behörde oder Agentur oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung Personenbezogener Daten bestimmt; für die Zwecke dieses DPA gilt der Verantwortliche im Verhältnis zu SAP, wenn der Auftraggeber als Auftragsverarbeiter für einen anderen Verantwortlichen handelt, als zusätzlicher und unabhängiger Verantwortlicher mit den entsprechenden Rechten und Pflichten eines Verantwortlichen gemäß diesem DPA.

9.10 **"Verletzung des Schutzes Personenbezogener Daten"** bezeichnet eine/n bestätigte/n (1) versehentliche oder widerrechtliche Vernichtung, Verlust, Veränderung, eine unbefugte Offenlegung von bzw. einen unbefugten Zugang Dritter zu Personenbezogenen Daten oder (2) einen vergleichbaren Vorfall mit Personenbezogenen Daten, bei denen der Verantwortliche in jedem Fall gemäß Datenschutzrecht zur Meldung an die zuständigen Datenschutzbehörden oder gegenüber den Betroffenen Personen verpflichtet ist.

Anhang 1 zum DPA und, falls anwendbar, zu den Standardvertragsklauseln

Datenexporteur
Der Datenexporteur ist der Auftraggeber, der einen Software-Pflegevertrag oder einen Service Vertrag mit SAP abgeschlossen hat, unter dem er die dort beschriebenen SAP Dienste in Anspruch nehmen kann. Räumt der Datenexporteur anderen Verantwortlichen die Möglichkeit ein, den SAP Service ebenfalls zu nutzen, sind diese anderen Verantwortlichen ebenfalls Datenexporteure.

Datenimporteur
SAP und ihre Unterauftragsverarbeiter stellen die SAP Dienste gemäß der mit dem Datenexporteur abgeschlossenen Vereinbarung bereit, die die folgenden SAP Dienste umfasst:

Unter einem Software- und Pflegevertrag: SAP und/oder ihre Unterauftragsverarbeiter bieten Unterstützung, wenn ein Auftraggeber ein Support-Ticket einreicht, weil die Software nicht verfügbar ist oder nicht wie erwartet funktioniert. Sie beantworten Telefonanrufe und führen einfache Störungsbehebung durch und bearbeiten Support-Tickets in einem Tracking-System.

Unter einem Services Vertrag: SAP und/oder ihre Unterauftragsverarbeiter erbringen Leistungen, die dem Einzelvertrag und dem jeweiligen Scope Dokument unterliegen.

Betroffene Personen
Sofern nicht anderweitig durch den Datenexporteur angegeben, lassen sich die übermittelten Personenbezogenen Daten in der Regel einer der folgenden Kategorien von Betroffenen Personen zuordnen: Mitarbeiter, Subunternehmer, Geschäftspartner oder sonstige Personen, deren Personenbezogene Daten dem Datenimporteur übertragen werden oder die Zugriffsmöglichkeit eingeräumt wird.

Datenkategorien
Die übermittelten Personenbezogenen Daten betreffen die folgenden Datenkategorien:
Der Auftraggeber bestimmt die Kategorien von Daten und/oder Datenfelder, die im Rahmen der SAP Dienste gemäß der jeweiligen Vereinbarung übertragen werden. Die übermittelten Personenbezogenen Daten lassen sich in der Regel einer der folgenden Datenkategorien zuordnen: Name, Telefonnummer, E-Mail-Adresse, Zeitzone, Anschrift, Systemzugriff/-nutzung/-Berechtigungsdaten, Name des Unternehmens, Vertragsdaten, Rechnungsdaten und anwendungsspezifische Daten, die von Autorisierten Nutzern übertragen werden, wie beispielsweise Finanzdaten wie Bankkontendaten sowie Kredit- oder Debitkartendaten.

Besondere Datenkategorien (falls zutreffend)
Die übermittelten Personenbezogenen Daten lassen sich den folgenden besonderen Datenkategorien zuordnen: wie in der Vereinbarung (inkl. der Einzelvereinbarung) dargelegt (sofern zutreffend).

Verarbeitungsvorgänge / Zwecke
Die übermittelten Personenbezogenen Daten werden den in der Vereinbarung beschrieben grundlegenden Verarbeitungsmaßnahmen unterzogen, die folgende Verarbeitungsmaßnahmen umfassen können:

- Verwendung von Personenbezogenen Daten, um die SAP Dienste zu erbringen
- Speicherung von Personenbezogenen Daten
- Rechnergestützte Verarbeitung von Personenbezogenen Daten zur Datenübertragung
- Ausführung von Anweisungen des Auftraggebers gemäß der Vereinbarung

Anhang 2 zum DPA und, falls anwendbar, zu den Standardvertragsklauseln -
Technische und organisatorische Maßnahmen

1. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

In den folgenden Abschnitten werden die aktuellen technischen und organisatorischen Maßnahmen der SAP definiert. SAP kann diese Maßnahmen jederzeit unangekündigt ändern, solange eine vergleichbare oder höhere Sicherheitsstufe aufrechterhalten wird. Einzelne Maßnahmen können durch neue Maßnahmen, die denselben Zweck erfüllen, ersetzt werden, ohne dass die Sicherheitsstufe beim Schutz Personenbezogener Daten verringert wird.

1.1 Zutrittskontrolle. Unbefugten wird der physische Zugang zu Einrichtungen, Gebäuden und Räumlichkeiten verwehrt, in denen sich Datenverarbeitungssysteme befinden, die Personenbezogene Daten verarbeiten oder nutzen.

Maßnahmen:

- SAP schützt Gebäude durch angemessene Maßnahmen basierend auf der SAP Security Policy.
- Im Allgemeinen sind Gebäude durch Zutrittskontrollsysteme (z. B. Zutritt per Chipkarte) gesichert.
- Als Mindestanforderung müssen die äußeren Zugänge eines Gebäudes mit einer zertifizierten Schließanlage ausgestattet sein, einschließlich einer modernen, aktiven Schlüsselverwaltung.
- Abhängig von der Sicherheitseinstufung werden Gebäude, einzelne Bereiche und das umliegende Gelände möglicherweise durch weitere Maßnahmen geschützt. Dazu gehören spezielle Zutrittsprofile, Videoüberwachung, Einbruchmeldeanlagen und biometrische Zutrittskontrollsysteme.
- Die Vergabe der Zutrittsrechte an die berechtigten Personen erfolgt auf individueller Basis gemäß den Maßnahmen zur System- und Datenzugriffskontrolle (siehe folgende Abschnitte 1.2 und 1.3). Dies gilt auch für den Zutritt von Besuchern. Gäste und Besucher in SAP-Gebäuden müssen sich namentlich an der Rezeption anmelden und von autorisiertem SAP-Personal begleitet werden.
- SAP-Personal und externes Personal müssen ihren Firmenausweis an allen SAP-Standorten tragen.

Zusätzliche Maßnahmen für Rechenzentren:

- Für alle Rechenzentren gelten strenge Sicherheitsmaßnahmen, die u. a. durch Wachpersonal, Überwachungskameras, Bewegungsmelder und Zugangskontrollmechanismen unterstützt werden, um Anlagen und Einrichtungen von Rechenzentren vor dem Zugriff Unbefugter zu schützen. Zu den Systemen und zur Infrastruktur der Rechenzentren haben ausschließlich autorisierte Personen Zugang. Um die ordnungsgemäße Funktion zu schützen, werden Sicherheitsgeräte (Bewegungssensoren, Kameras usw.) in regelmäßigen Abständen gewartet.
- SAP sowie alle von Dritten betriebenen Rechenzentren protokollieren die Namen und Uhrzeiten von befugten Personen, die die nicht öffentlichen Bereiche von SAP innerhalb der Rechenzentren betreten.

1.2 Systemzugriffskontrolle. Datenverarbeitungssysteme, die zur Erbringung der SAP Dienste genutzt werden, sind vor einer nicht autorisierten Nutzung zu schützen.

Maßnahmen:

- Die Gewährung des Zugriffs auf sensible Systeme, einschließlich der Systeme zur Speicherung und Verarbeitung Personenbezogener Daten, erfolgt über mehrere Berechtigungsstufen. Berechtigungen werden über definierte Prozesse gemäß der SAP Security Policy verwaltet.
- Alle Personen greifen mit einer eindeutigen Kennung (User-ID) auf die Systeme von SAP zu
- SAP hat Verfahren eingerichtet, so dass angeforderte Änderungen an Berechtigungen nur in Übereinstimmung mit der SAP Security Policy durchgeführt werden (beispielsweise werden keine Rechte ohne entsprechende Berechtigung erteilt). Wenn ein Mitarbeiter das Unternehmen verlässt, werden dessen Zugriffsrechte aufgehoben.
- SAP hat eine Kennwortrichtlinie festgelegt, die die Weitergabe von Kennwörtern untersagt, regelt, wie vorzugehen ist, wenn ein Kennwort offengelegt wird, und erfordert, dass Kennwörter regelmäßig geändert und vorgegebene Kennwörter geändert werden. Zur Authentifizierung werden personalisierte Benutzerkennungen (User-IDs) zugewiesen. Alle Kennwörter müssen bestimmte Mindestbedingungen erfüllen und werden in verschlüsselter Form gespeichert. Im Fall von Domänenkennwörtern erzwingt das System alle sechs Monate eine Änderung des Kennworts, das den Anforderungen an komplexe Kennwörter entsprechen muss. Jeder Computer verfügt über einen kennwortgeschützten Bildschirmschoner.
- Das Unternehmensnetzwerk ist durch Firewalls vor dem öffentlichen Netzwerk geschützt.
- SAP verwendet aktuelle Virenscanner an den Übergängen zum Firmennetz (für E-Mail-Konten), sowie auf allen Fileservern und auf allen Einzelplatzcomputern.
- Das Sicherheitspatch-Management gewährleistet die Anwendung entsprechender regelmäßiger Sicherheits-Updates. Der vollständige Zugriff auf das SAP-Firmennetzwerk und die kritische Infrastruktur ist durch eine strenge Authentifizierung geschützt.

1.3 Datenzugriffskontrolle. Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, erhalten nur Zugriff auf die Personenbezogenen Daten, für die sie Zugriffsrechte besitzen, und Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Maßnahmen:

- Im Rahmen der SAP Security Policy erfordern Personenbezogene Daten zumindest den gleichen Schutz wie „vertrauliche" Informationen im Sinne des SAP-Informationsklassifizierungsstandards.
- Der Zugriff auf Personenbezogene Daten wird nur bei entsprechender Notwendigkeit gewährt („Need-to-know"-Prinzip). Jeder Person wird der Zugriff nur auf diejenigen Informationen gewährt, die sie zur Erledigung ihrer Pflichten benötigt. SAP verwendet Berechtigungskonzepte, die die Zuweisungsprozesse und die zugewiesenen Rollen pro Account (User ID) dokumentieren. Alle Auftraggeberdaten werden gemäß der SAP Security Policy geschützt.
- Alle produktiven Server werden in den Rechenzentren oder in sicheren Serverräumen betrieben. Die Sicherheitsmaßnahmen zum Schutz der Anwendungen zur Verarbeitung Personenbezogener Daten werden in regelmäßigen Abständen geprüft. Zu diesem Zweck führt SAP interne und externe Sicherheitsüberprüfungen und Penetrationstests ihrer IT-Systeme durch.
- SAP erlaubt nicht die Installation eigener Software oder sonstiger Software, die nicht durch SAP genehmigter wurde.
- Durch einen entsprechenden SAP-Sicherheitsstandard wird geregelt, auf welche Weise Daten und Datenträger gelöscht oder vernichtet werden, wenn sie nicht mehr benötigt werden.

1.4 Datenübertragungskontrolle. Die Datenübertragungskontrolle gewährleistet, dass Personenbezogene Daten, außer soweit für die Erbringung der SAP Dienste gemäß der jeweiligen Vereinbarung notwendig, bei der Übertragung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Beim physischen Transport von Datenträgern werden bei SAP geeignete Maßnahmen getroffen, um die vereinbarten Service-Level zu gewährleisten (z. B. Verschlüsselung, mit Blei ausgekleidete Behälter).

Maßnahmen:

- Personenbezogene Daten sind bei der Übertragung über interne SAP-Netzwerke geschützt gemäß der SAP Security Policy geschützt.
- Im Hinblick auf die Übertragung der Daten zwischen SAP und ihren Auftraggebern werden die für die Übertragung erforderlichen Sicherheitsmaßnahmen zwischen den Parteien vereinbart und werden hiermit zum Bestandteil der Vereinbarung. Dies gilt sowohl für die physische als auch für die netzwerkbasierte Datenübertragung. In jedem Fall übernimmt der Auftraggeber die Verantwortung für die Datenübertragung, sobald sie außerhalb der von SAP kontrollierten Systeme erfolgt (z. B. Daten, die außerhalb der Firewall des SAP-Rechenzentrums übertragen werden).

1.5 Dateneingabekontrolle. Es wird die Möglichkeit geschaffen, im Nachhinein zu untersuchen und festzustellen, ob und von wem Personenbezogene Daten erfasst, modifiziert oder aus den Datenverarbeitungssystemen der SAP entfernt wurden.

Maßnahmen:

- SAP gestattet ausschließlich befugten Personen im Rahmen ihrer Pflichten, auf Personenbezogene Daten zuzugreifen.
- SAP hat für die SAP Dienste ein Protokollierungssystem für das Erfassen, Ändern und Löschen oder Sperren Personenbezogener Daten durch SAP oder ihre Unterauftragsverarbeiter im technisch möglichen Umfang implementiert.

1.6 Auftragskontrolle. Auftragskontrolle ist erforderlich um zu gewähren, das Personenbezogene Daten, die im Auftrag verarbeitet werden, ausschließlich in Übereinstimmung mit Weisungen des Auftraggebers verarbeitet.

Maßnahmen:

- SAP nutzt Kontrollen und Verfahren, um die Einhaltung der Verträge zwischen SAP und ihren Auftraggebern, Unterauftragsverarbeitern oder anderen Serviceanbietern zu überwachen.
- Im Rahmen der SAP Security Policy erfordern Personenbezogene Daten zumindest den gleichen Schutz wie „vertrauliche" Informationen im Sinne des SAP-Informationsklassifizierungsstandards.
- Sämtliche SAP-Mitarbeiter und Unterauftragsverarbeiter oder anderen Serviceanbieter werden vertraglich verpflichtet, die Geheimhaltungspflicht in Bezug auf alle sensiblen Informationen einschließlich Geschäftsgeheimnissen von Auftraggebern und Partnern der SAP einzuhalten.
- Bei der Pflege haben Auftraggeber jederzeit die Kontrolle über ihre Remote-Support-Verbindungen. SAP-Mitarbeiter können ohne Wissen und Zustimmung des Auftraggebers nicht auf ein Auftraggeber System zugreifen. Für Pflege bietet SAP ein spezielles, sicheres Support-Ticket an, in dem SAP einen speziellen, zugangskontrollierten und überwachten Sicherheitsbereich für die Übertragung von Zugangsdaten und Passwörtern zur Verfügung stellt. Die Auftraggeber haben jederzeit die Kontrolle über ihre Remote-Support-Verbindungen. SAPMitarbeiter können ohne Wissen und aktiver Beteiligung des Auftraggebers nicht auf ein On Premise System des Auftraggebers zugreifen.

1.7 Verfügbarkeitskontrolle. Personenbezogene Daten werden vor versehentlicher oder nicht autorisierter Vernichtung oder Verlust geschützt.

Maßnahmen:

- SAP verfügt über regelmäßige Backup-Prozesse zur Wiederherstellung der Verfügbarkeit geschäftskritischer Systeme bei Bedarf.

- SAP verwendet unterbrechungsfreie Stromversorgungen (USV, Batterien, Generatoren usw.), um die Stromversorgung für die Rechenzentren zu schützen.
- SAP hat Geschäftskontinuitätspläne für geschäftskritische Prozesse definiert.
- Notfallprozesse und -systeme werden regelmäßig getestet.

1.8 Trennungskontrolle. Personenbezogene Daten, die für unterschiedliche Zwecke erfasst werden, können getrennt verarbeitet werden.

Maßnahmen:

- SAP nutzt angemessene technischen Kontrollen, um jederzeit die Trennung von Auftraggeberdaten zu erreichen.
- Der Auftraggeber (einschließlich seiner von ihm freigegebenen Verantwortlichen) wird auf Basis einer sicheren Authentifizierung und Autorisierung ausschließlich Zugriff auf seine eigenen Daten gewährt.

  Wenn zur Bearbeitung eines Supportfalls des Auftraggebers Personenbezogene Daten dieses Auftraggebers benötigt werden, werden die Daten dieser Meldung zugeordnet und nur zur Bearbeitung dieser Meldung verwendet; für die Bearbeitung anderer Meldungen findet kein Zugriff auf diese Daten statt. Diese Daten werden in dedizierten Support-Systemen gespeichert.

1.9 Datenintegritätskontrolle. Personenbezogene Daten bleiben während der Verarbeitungsaktivitäten unversehrt, vollständig und aktuell.

Maßnahmen:

SAP hat zum Schutz vor unautorisierten Änderungen eine mehrere Schichten umfassende Sicherheitsstrategie umgesetzt. Insbesondere verwendet SAP die folgenden Mittel, um die obigen Abschnitte zu Kontrollen und Maßnahmen umzusetzen. Insbesondere:

- Firewalls
- Security Monitoring Center
- Antivirensoftware
- Erstellen von Sicherungskopien und Wiederherstellung
- Externe und interne Penetrationstests
- Regelmäßige Prüfung der Sicherheitsmaßnahmen durch externe Prüfer

Anhang 3 zum DPA

Ausschließlich zur Veranschaulichung benennt die folgende Tabelle die einschlägigen Artikel der DSGVO und die entsprechenden Regelungen des DPA.

Artikel der DSGVO	Abschnitt des DPA	Mit Klick auf den Link zum jeweiligen Abschnitt
28(1)	2 und Anhang 2	SICHERHEIT DER VERARBEITUNG und Anhang 2 Technische und organisatorische Maßnahmen
28(2), 28(3) (d) und 28 (4)	6	UNTERAUFTRAGSVERARBEITER
28 (3) Satz 1	1.1 und Anhang 1, 1.2	Zweck und Anwendung., Anhang 1, Struktur.
28(3) (a) und 29	3.1 und 3.2	Weisungen des Auftraggebers. , Verarbeitung auf Basis rechtlicher Erfordernisse.
28(3) (b)	3.3	Befugte Personen.
28(3) (c) und 32	2 und Anhang 2	SICHERHEIT DER VERARBEITUNG und Anhang 2 Technische und organisatorische Maßnahmen
28(3) (e)	3.4	Kooperation.
28(3) (f) and 32-36	2 und Anhang 2, 3.5, 3.6	SICHERHEIT DER VERARBEITUNG und Anhang 2 Technische und organisatorische Maßnahmen Meldung von Verletzungen des Schutzes Personenbezogener Daten., Datenschutz-Folgenabschätzung.
28(3) (g)	4	DATEN LÖSCHUNG
28(3) (h)	5	ZERTIFIZIERUNGEN UND AUDITS
28 (4)	6	UNTERAUFTRAGSVERARBEITER
30	8	DOKUMENTATION; VERARBEITUNGSVERZEICHNIS
46(2) c)	7.2 und Anhang 4	Standardvertragsklauseln und Anhang 4 Standardvertragsklauseln (Auftragsverarbeiter)

Anhang 4 zum DPA

Standardvertragsklauseln (Auftragsverarbeiter)[1]

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

[...]
(in den Klauseln nachfolgend als „Datenexporteur" bezeichnet)

Und

[...]
(in den Klauseln nachfolgend als „Datenimporteur" bezeichnet)

(die „Partei", wenn eine dieser Organisationen gemeint ist, die „Parteien", wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln"), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1);

b) der „Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter" ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht" bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen" sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2

Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3

Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person

[1] Gemäß dem Beschluss der Kommission vom 5. Februar 2010 (2010/87/EU)

die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs [2]

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7

Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11

Vergabe eines Unterauftrags

(1) **Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss [3]. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.**

(2) **Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.**

(3) **Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: ...**

(4) **Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.**

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) **Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.**

(2) **Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.**

---

[1] Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

[2] Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

[3] Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

Vereinbarung zur Auftragsverarbeitung

Als Anlage zur Order Form (Corona Warn App Projekt), hierin „Order Form", „Leistungsvereinbarung" oder „Einzelabruf" genannt wird zwischen dem

Robert Koch Institut (als Vertreter der Bundesrepublik Deutschland)

- nachfolgend „Verantwortlicher" oder „RKI"-

und

SAP Deutschland SE & Co. KG
Hasso-Plattner-Ring 7
69190 Walldorf

- nachfolgend „Auftragsverarbeiter" oder „SAP" -

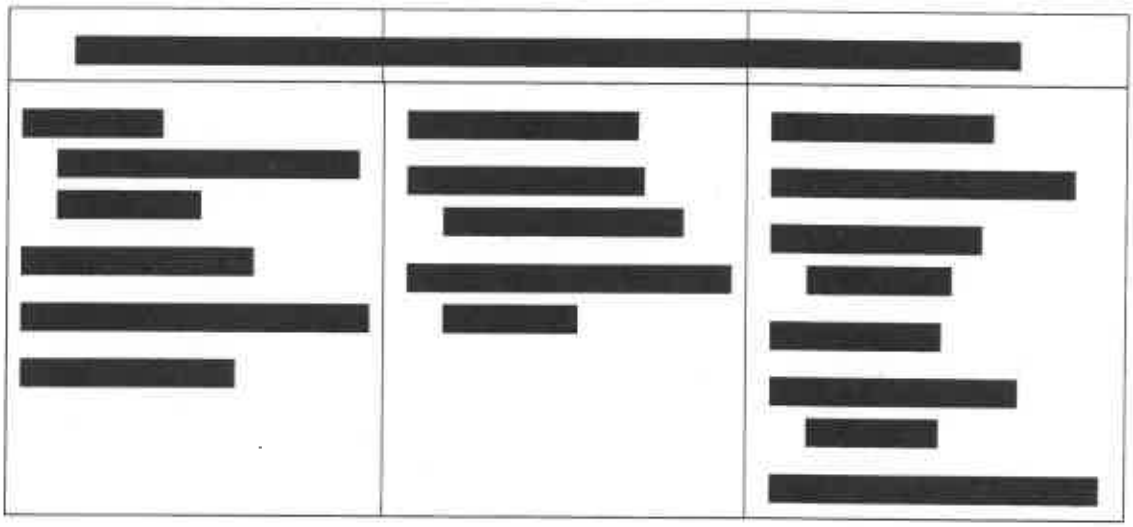
- beide nachfolgend gemeinsam „Vertragsparteien" -

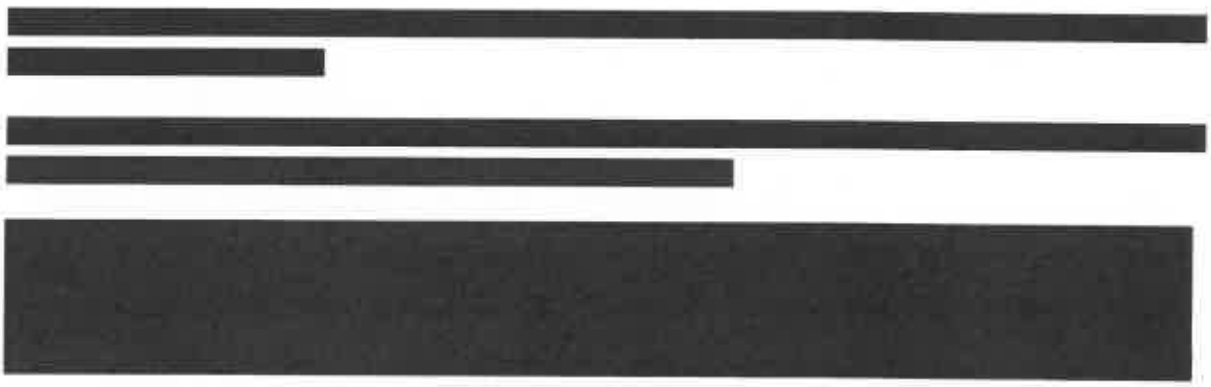
die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel

Die Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit („BMG") hat mit SAP einen Vertrag über Entwicklungs- und Pflegeleistungen im Projekt Corona Warn App sowie mit der T-Systems einen Vertrag über IT-Leistungen im Projekt Corona Warn App geschlossen. Das unter diesen Verträgen von SAP und T-Systems entwickelte und zum Betrieb bereitgestellte System zum Betrieb der Corona Warn App wird in der zwischen dem BMG sowie T-Systems und SAP geschlossenen Abstimmungsvereinbarung insgesamt als "Gesamtsystem" bezeichnet. Im Rahmen der Abstimmungsvereinbarung sind gemeinsame Regelungen und Prozesse sowie ein Rahmen für die übergreifende Zusammenarbeit im Projekt Corona Warn App vereinbart.





Die Vertragsparteien der Order Form (hierin: auch „Leistungsvereinbarung") gehen ein Auftragsverarbeitungsverhältnis ein. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der 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), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarungen sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung.

Die übermittelten personenbezogenen Daten werden den in der Vereinbarung beschrieben grundlegenden Verarbeitungsmaßnahmen unterzogen, die u.a. folgende Verarbeitungsmaßnahmen umfassen können:

- Verwendung von personenbezogenen Daten, um die in der Order Form beschriebenen Pflege-, Support- und Weiterentwicklungsleistungen für die Corona Warn App zu erbringen
- Ausführung von Anweisungen des Verantwortlichen gemäß der AVV

(2) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

Die Datenarten und –kategorien werden durch die vereinbarte Funktionalität der Features bestimmt und ergeben sich aus der Spezifikation als Anlage zur Order Form.

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen lässt sich, sofern in der jeweiligen Leistungsvereinbarung nicht anderweitig angegeben, einer der folgenden Kategorien von Betroffenen Personen zuordnen: Nutzer der Features..

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen jeweils verantwortlich. Der Verantwortliche kann, soweit dies auf Grund der Verarbeitung pseudonymisierter Daten möglich ist, jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich (in Text- oder Schriftform) zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften, sei technisch für ihn undurchführbar oder nicht ohne Änderungen an der Erbringung der vereinbarten Leistungen möglich. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt bzw. geändert wird.

[redacted] Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Die Parteien stellen sich auf Wunsch in angemessener Weise und Umfang Informationen zur Ermöglichung der Erfüllung der Verpflichtungen im Zusammenhang mit der Führung von Verarbeitungsverzeichnissen

zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) EU Access: [redacted] wird der Auftragsverarbeiter bei Zugriffen auf Systeme des Verantwortlichen nur solche Unterverarbeiter einzusetzen, die die Innovative Business Solutions Development Support Services on Cloud aus dem Gebiet des Europäischen Wirtschaftsraums und der Schweiz heraus erbringen.

(9) Der Auftragsverarbeiter sorgt dafür, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur entsprechend dieser Vereinbarung zur Auftragsverarbeitung verarbeiten. [redacted]

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit (Datengeheimnis) verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen [redacted] Der Auftragsverarbeiter und seine Unterauftragsverarbeiter werden die Personen, die Zugang zu personenbezogenen Daten haben, regelmäßig in Bezug auf die anwendbaren Datensicherheits- und Datenschutzmaßnahmen schulen.

[redacted]

(4) Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, die/der ihre/seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten der/des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

[redacted]

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

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

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

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken im Rahmen des § 10 von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

[redacted]

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen bei Verletzung des Schutzes personenbezogener Daten insbesondere bei Verstößen gegen gesetzliche Datenschutzbestimmungen, sofern diese jeweils Auswirkungen auf personenbezogene Daten des Verantwortlichen haben umgehend nach Kenntniserlangung. Er wird ihn bei der Erfüllung seiner Verpflichtungen zur Meldung einer Verletzung des Schutzes personenbezogener Daten gemäß den Anforderungen des Datenschutzrechts unterstützen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter unterstützt den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Der Verantwortliche erteilt dem Auftragsverarbeiter mit Abschluss dieser Vereinbarung zur Auftragsverarbeitung die widerrufliche Weisung, nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens 6 Monate nach Beendigung der Leistungsvereinbarung sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen und personenbezogene Daten beinhalten, datenschutzgerecht zu löschen. Gleiches gilt für Test- und Ausschussmaterial [redacted]

(3) Der Auftragsverarbeiter kann Dokumentationen (z.B. Support-Tickets), die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

Die nachfolgenden Regelungen gelten für den Fall, dass es sich um Dritte handelt, die vergaberechtlich als Unterauftragnehmer zu qualifizieren sind (also bei Übernahme von Leistungen, die qualitativ oder quantitativ für von SAP gemäß der Order Form geschuldete Werkleistungen wesentlich sind) ergänzend zu Abschnitt 7.4 der Order Form, in den übrigen Fällen (also soweit es sich beim jeweiligen Unterauftragsverarbeiter nicht um einen Unterauftragnehmer im vergaberechtlichen Sinn handelt) abschließend.

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen oder Unterauftragsverarbeiter) unter den nachfolgenden Voraussetzungen einsetzen:

(a) Der Auftragsverarbeiter oder die SAP SE im Namen des Auftragsverarbeiters beauftragt Unterauftragsverarbeiter im Rahmen schriftlicher Verträge, die mit den Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung in Bezug auf die Verarbeitung personenbezogener Daten durch den Unterauftragsverarbeiter übereinstimmen. Der Auftragsverarbeiter haftet für etwaige Verstöße durch den Unterauftragsverarbeiter gemäß den Bestimmungen des jeweiligen Einzelabrufs;

(b) Der Auftragsverarbeiter wird die Sicherheits-, Datenschutz- und Vertraulichkeitspraktiken eines Unterauftragsverarbeiters vor dessen Auswahl bewerten, um festzustellen, dass er in der Lage ist, das in dieser Vereinbarung zur Auftragsverarbeitung geforderte Schutzniveau für personenbezogene Daten zu bieten;

(c) Zum Zeitpunkt der Unterzeichnung dieses Vertrags sind für den Auftragsverarbeiter die nachfolgend bezeichneten Unterauftragsverarbeiter unter Umständen mit der Verarbeitung von personenbezogenen Daten beschäftigt. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden.

Innovative Business Solutions Development Support Services on Cloud:

- SAP România SRL, Clădirea A1/LA, et. 2, Strada Tipografilor 11-15, Bucureşti 013714, Rumänien
- SAP Bulgaria Ltd., 136A, Tzar Boris III Blvd. 1618 Sofia, Bulgarien
- SAP Ireland Limited, Parkmore Business Park East, Brockagh, Parkmore, Galway, Co. Galway, Irland

(2) Der Auftragsverarbeiter informiert den Verantwortlichen rechtzeitig entsprechend den Regelungen dieses Absatzes 2 über jegliche geplante Hinzufügungen oder Ersetzungen zu der Liste der Unterauftragsverarbeiter, einschließlich des Namens, der Anschrift und der Rolle des neuen Unterauftragsverarbeiters. Dies erfolgt über eine Bekanntmachung auf dem SAP Support Portal oder über E-Mail (nachdem der Verantwortliche sich im SAP Portal entsprechend registriert hat).

Der Verantwortliche ist berechtigt, der Verarbeitung personenbezogener Daten durch die neuen Unterauftragsverarbeiter zu widersprechen, wenn er einen berechtigten datenschutzrechtlichen Grund hat, spätestens jedoch zum Ablauf von dreißig Tagen nach dem Datum der Information des Auftragsverarbeiters an den Verantwortlichen über den neuen Unterauftragsverarbeiter. Widerspricht der Verantwortliche nicht innerhalb dieser Frist von dreißig Tagen, so gilt der neue Unterauftragsverarbeiter als durch den Verantwortlichen genehmigt.

Der Auftragsverarbeiter kann einen Unterauftragsverarbeiter ohne vorherige Mitteilung austauschen, wenn sich der Grund für den Austausch der zumutbaren Kontrolle des Auftragsverarbeiters entzieht und der umgehende Austausch aus Sicherheits- oder anderen dringenden Gründen zwingend erforderlich ist.

In diesem Fall informiert er den Verantwortlichen über den neuen Unterauftragsverarbeiter unverzüglich nach seiner Ernennung. § 8 Absatz 2 Unterabsatz 2 gilt entsprechend.

Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter dafür zu sorgen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

[redacted]

(4) Für Verschulden von Subunternehmen haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen gem. § 278 BGB für die Einhaltung der vertraglichen Pflichten.

§ 9 Internationale Verarbeitung

(1) Regeln für internationale Verarbeitung. Der Auftragsverarbeiter ist berechtigt, die Verarbeitung von personenbezogenen Daten unter Einbeziehung von Unterauftragsverarbeitern im Sinne dieser AVV außerhalb des Landes, in dem sich der Verantwortliche befindet unter Einhaltung des Datenschutzrechts durchzuführen.

(2) Standardvertragsklauseln (Standarddatenschutzklauseln). Sofern „EU Access" (vgl. § 3 Absatz 8) nicht einschlägig ist und personenbezogene Daten des Verantwortlichen in einem Land außerhalb des EWR, der Schweiz bzw. außerhalb eines Landes, einer Organisation oder eines Gebiets erfolgt, das von der Europäischen Union als sicheres Land mit einem angemessenen Datenschutzniveau gemäß Art. 45 GDPR anerkannt ist, verarbeitet werden, gilt:

(a) Der Auftragsverarbeiter und der Verantwortliche vereinbaren die Geltung der Standardvertragsklauseln;
(b) Der Verantwortliche vereinbart die Standardvertragsklauseln mit jedem relevanten Unterauftragsverarbeiter wie folgt: (i) Der Verantwortliche tritt als unabhängiger Inhaber von Rechten und Pflichten den Standardvertragsklauseln bei, die zwischen dem Auftragsverarbeiter oder SAP SE und dem Unterauftragsverarbeiter vereinbart wurden („Beitrittsmodell") oder (ii) der

Unterauftragsverarbeiter (vertreten durch den Auftragsverabeiter) vereinbart die Standardvertragsklauseln mit dem Verantwortlichen ("Vollmachtsmodell"). Das Vollmachtsmodell gilt, wenn und soweit der Auftragsverarbeiter ausdrücklich über die Liste der Unterauftragsverarbeiter gemäß § 8 Absatz 1 c oder über eine Mitteilung an den Vearntwortlichen erklärt hat, dass dieses Modell für einen Unterauftragsverarbeiter verfügbar ist; und/oder

(c) Andere Verantwortliche, denen der im Rubrum des jeweiligen Einzelabrufs genannte Verantwortliche die Einbringung von personenbezogenen Daten gemäß der AVV gestattet hat, können ebenfalls die Standardvertragsklauseln mit dem Auftragsverarbeiter und/oder den relevanten Unterauftragsverarbeitern in gleicher Weise wie der im Rubrum des jeweiligen Einzelabrufs genannte Verantwortliche gemäß den obigen Regelungen in § 9 Absatz 2 (a) und (b) vereinbaren. In diesen Fällen vereinbart der im Rubrum des jeweiligen Einzelabrufs genannte Verantwortliche die Standardvertragsklauseln im Namen der anderen Verantwortlichen.

(3) Bezug zwischen Standardvertragsklauseln und Vereinbarung. Keine der Bestimmungen in der Vereinbarung darf bei widersprüchlichen Regelungen dahingehend ausgelegt werden, dass sie Vorrang vor einer Bestimmung der Standardvertragsklauseln hat. Zur Klarstellung: Wo diese AVV Regelungen für Audit und Unterauftragsverarbeiter in den §§ 8 und 10 näher beschreibt, gelten diese Regelungen auch in Bezug auf die Standardvertragsklauseln.

(4) Für die Standardvertragsklauseln geltendes Recht. Die Standardvertragsklauseln unterliegen dem Recht des Landes, in dem der Verantwortliche seinen Sitz hat.

§ 10 Zertifizierungen und Audits, Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich dem Datenschutzbeauftragten des Verantwortlichen [redacted] Zugang und Informationen wie folgt zu gewähren:

(1) **Audit des im Rubrum des jeweiligen Einzelabrufs genannten Verantwortlichen.** Der im Rubrum des jeweiligen Einzelabrufs genannte Verantwortliche oder ein von ihm beauftragter unabhängiger Prüfer (Ausschluss von Prüfern, die entweder Wettbewerber des Auftragsverarbeiters sind, oder nicht angemessen qualifiziert oder unabhängig sind) können Überprüfungen beim Auftragsverarbeiter durchführen, indem sie die Service und Support Center und die IT-Sicherheitspraktiken des Auftragsverarbeiters im Hinblick auf die vom Auftragsverarbeiter verarbeiteten Personenbezogenen Daten prüfen.

[redacted]

Eine solche Vor-Ort-Prüfung durch den Verantwortlichen darf nur einmal binnen eines 12-Monatszeitraums erfolgen, es sei denn zwingendes Datenschutzrecht verlangt häufigere Audits oder es liegt ein begründeter Anlaß (z.B. eine Datenschutzverletzung) für ein häufigeres Audit vor.

(2) **Audits anderer Verantwortlicher.** Jeder andere Verantwortliche darf die Service und Support Center und die IT-Sicherheitspraktiken des Auftragsverarbeiters, die für die vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten relevant sind, ebenfalls gemäß § 10 Absatz 1 überprüfen. Eine solche Prüfung soll nach Möglichkeit durch den im Rubrum des jeweiligen Einzelabrufs genannte Verantwortlichen gem. § 10 Absatz 1 durchgeführt werden. Wenn mehrere Verantwortliche, deren personenbezogene Daten vom Auftragsverarbeiter auf der Grundlage der Vereinbarung verarbeitet werden, ein Audit erfordern, wird der im Rubrum des jeweiligen Einzelabrufs genannte Verantwortliche alle angemessenen Mittel einsetzen, um die Audits zu kombinieren und Mehrfach-Audits zu vermeiden.

(3) **Umfang des Audits.** Der im Rubrum des jeweiligen Einzelabrufs genannte Verantwortliche ist verpflichtet, Audits mindestens sechzig (60) Tage im Voraus anzukündigen, es sei denn, dass zwingendes Datenschutzrecht oder eine zuständige Datenschutzbehörde eine kürzere Frist vorschreiben oder ein begründeter Anlass für eine kürzere oder keine Frist besteht (z.B. eine Datenschutzverletzung). Die Parteien werden vorrangig aktuelle Zertifizierungen oder andere Auditberichte verwenden, um Erstaudits oder wiederholte Audits zu vermeiden oder zu minimieren.

(4) **Auditkosten.** [redacted]
Falls sich aus einem Audit ergibt, dass der Auftragsverarbeiter seinen vertraglichen oder gesetzlichen Verpflichtungen nicht nachgekommen ist, heilt er diesen Verstoß umgehend auf eigene Kosten.

(5) **Informationen.** Der Auftragsverarbeiter stellt dem Verantwortlichen entsprechend Art. 28 Abs. 3 lit h. Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung.

(6) [redacted]

§ 11 Schlussbestimmungen

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

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder

undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Datum, Ort	Datum, Ort
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang-Muster zur Vereinbarung der Auftragsverarbeitung - Technisch-organisatorische Maßnahmen („Anlage TOM")

1. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

In den folgenden Abschnitten werden die aktuellen technischen und organisatorischen Maßnahmen des Auftragsverarbeiters (hierin auch: „SAP") definiert.

[redacted]

a. **Zutrittskontrolle.** Unbefugten wird der physische Zugang zu Einrichtungen, Gebäuden und Räumlichkeiten verwehrt, in denen sich Datenverarbeitungssysteme befinden, die Personenbezogene Daten verarbeiten oder nutzen.

Maßnahmen:

- SAP schützt Gebäude durch angemessene Maßnahmen basierend auf der SAP Security Policy.
- Im Allgemeinen sind Gebäude durch Zutrittskontrollsysteme (z. B. Zutritt per Chipkarte) gesichert.

- Als Mindestanforderung müssen die äußeren Zugänge eines Gebäudes mit einer zertifizierten Schließanlage ausgestattet sein, einschließlich einer modernen, aktiven Schlüsselverwaltung.
- Abhängig von der Sicherheitseinstufung werden Gebäude, einzelne Bereiche und das umliegende Gelände möglicherweise durch weitere Maßnahmen geschützt. Dazu gehören spezielle

Zutrittsprofile, Videoüberwachung, Einbruchmeldeanlagen und biometrische Zutrittskontrollsysteme.

- Die Vergabe der Zutrittsrechte an die berechtigten Personen erfolgt auf individueller Basis gemäß den Maßnahmen zur System- und Datenzugriffskontrolle (siehe folgende Abschnitte 1.2 und 1.3). Dies gilt auch für den Zutritt von Besuchern. Gäste und Besucher in SAP-Gebäuden müssen sich namentlich an der Rezeption anmelden und von autorisiertem SAP-Personal begleitet werden.
- SAP-Personal und externes Personal müssen ihren Firmenausweis an allen SAP-Standorten tragen.

Zusätzliche Maßnahmen für Rechenzentren:

- Für alle Rechenzentren gelten strenge Sicherheitsmaßnahmen, die u. a. durch Wachpersonal, Überwachungskameras, Bewegungsmelder und Zugangskontrollmechanismen unterstützt werden, um Anlagen und Einrichtungen von Rechenzentren vor dem Zugriff Unbefugter zu schützen. Zu den Systemen und zur Infrastruktur der Rechenzentren haben ausschließlich autorisierte Personen Zugang. Um die ordnungsgemäße Funktion zu schützen, werden Sicherheitsgeräte (Bewegungssensoren, Kameras usw.) in regelmäßigen Abständen gewartet.
- SAP sowie alle von Dritten betriebenen Rechenzentren protokollieren die Namen und Uhrzeiten von befugten Personen, die die nicht öffentlichen Bereiche von SAP innerhalb der Rechenzentren betreten.

b. **Systemzugriffskontrolle.** Datenverarbeitungssysteme, die zur Erbringung der SAP Dienste genutzt werden, sind vor einer nicht autorisierten Nutzung zu schützen.

Maßnahmen:

- Die Gewährung des Zugriffs auf sensible Systeme, einschließlich der Systeme zur Speicherung und Verarbeitung Personenbezogener Daten, erfolgt über mehrere Berechtigungsstufen. Berechtigungen werden über definierte Prozesse gemäß der SAP Security Policy verwaltet.
- Alle Personen greifen mit einer eindeutigen Kennung (User-ID) auf die Systeme von SAP zu
- SAP hat Verfahren eingerichtet, so dass angeforderte Änderungen an Berechtigungen nur in Übereinstimmung mit der SAP Security Policy durchgeführt werden (beispielsweise werden keine Rechte ohne entsprechende Berechtigung erteilt). Wenn ein Mitarbeiter das Unternehmen verlässt, werden dessen Zugriffsrechte aufgehoben.
- SAP hat eine Kennwortrichtlinie festgelegt, die die Weitergabe von Kennwörtern untersagt, regelt, wie vorzugehen ist, wenn ein Kennwort offengelegt wird, und erfordert, dass Kennwörter regelmäßig geändert und vorgegebene Kennwörter geändert werden. Zur Authentifizierung werden personalisierte Benutzerkennungen (User-IDs) zugewiesen. Alle Kennwörter müssen bestimmte Mindestbedingungen erfüllen und werden in verschlüsselter Form gespeichert. Im Fall von Domänenkennwörtern erzwingt das System alle sechs Monate eine Änderung des Kennworts, das den Anforderungen an komplexe Kennwörter entsprechen muss. Jeder Computer verfügt über einen kennwortgeschützten Bildschirmschoner.
- Das Unternehmensnetzwerk ist durch Firewalls vor dem öffentlichen Netzwerk geschützt.
- SAP verwendet aktuelle Virenscanner an den Übergängen zum Firmennetz (für E-Mail-Konten), sowie auf allen Fileservern und auf allen Einzelplatzcomputern.
- Das Sicherheitspatch-Management gewährleistet die Anwendung entsprechender regelmäßiger Sicherheits-Updates. Der vollständige Zugriff auf das SAP-Firmennetzwerk und die kritische Infrastruktur ist durch eine strenge Authentifizierung geschützt.

c. **Datenzugriffskontrolle.** Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, erhalten nur Zugriff auf die Personenbezogenen Daten, für die sie Zugriffsrechte besitzen, und Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.
Maßnahmen:

- Im Rahmen der SAP Security Policy erfordern Personenbezogene Daten zumindest den gleichen Schutz wie „vertrauliche" Informationen im Sinne des SAP-Informationsklassifizierungsstandards.

- Der Zugriff auf Personenbezogene Daten wird nur bei entsprechender Notwendigkeit gewährt („Need-to-know"-Prinzip). Jeder Person wird der Zugriff nur auf diejenigen Informationen gewährt, die sie zur Erledigung ihrer Pflichten benötigt. SAP verwendet Berechtigungskonzepte, die die Zuweisungsprozesse und die zugewiesenen Rollen pro Account (User ID) dokumentieren. Alle Auftraggeberdaten werden gemäß der SAP Security Policy geschützt.
- Alle produktiven Server werden in den Rechenzentren oder in sicheren Serverräumen betrieben. Die Sicherheitsmaßnahmen zum Schutz der Anwendungen zur Verarbeitung Personenbezogener Daten werden in regelmäßigen Abständen geprüft. Zu diesem Zweck führt SAP interne und externe Sicherheitsüberprüfungen und Penetrationstests ihrer IT-Systeme durch.
- SAP erlaubt nicht die Installation eigener Software oder sonstiger Software, die nicht durch SAP genehmigter wurde.
- Durch einen entsprechenden SAP-Sicherheitsstandard wird geregelt, auf welche Weise Daten und Datenträger gelöscht oder vernichtet werden, wenn sie nicht mehr benötigt werden.

d. **Datenübertragungskontrolle.** Die Datenübertragungskontrolle gewährleistet, dass Personenbezogene Daten, außer soweit für die Erbringung der SAP Dienste gemäß der jeweiligen Vereinbarung notwendig, bei der Übertragung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Beim physischen Transport von Datenträgern werden bei SAP geeignete Maßnahmen getroffen, um die vereinbarten ServiceLevel zu gewährleisten (z. B. Verschlüsselung, mit Blei ausgekleidete Behälter).
Maßnahmen:

- Personenbezogene Daten sind bei der Übertragung über interne SAP-Netzwerke gemäß der SAP Security Policy geschützt.
- Im Hinblick auf die Übertragung der Daten zwischen SAP und ihren Auftraggebern werden die für die Übertragung erforderlichen Sicherheitsmaßnahmen zwischen den Parteien vereinbart und werden hiermit zum Bestandteil der Vereinbarung. Dies gilt sowohl für die physische als auch für die netzwerkbasierte Datenübertragung. In jedem Fall übernimmt der Auftraggeber die Verantwortung für die Datenübertragung, sobald sie außerhalb der von SAP kontrollierten Systeme erfolgt (z. B. Daten, die außerhalb der Firewall des SAP-Rechenzentrums übertragen werden).

e. **Dateneingabekontrolle.** Es wird die Möglichkeit geschaffen, im Nachhinein zu untersuchen und festzustellen, ob und von wem Personenbezogene Daten erfasst, modifiziert oder aus den Datenverarbeitungssystemen der SAP entfernt wurden.
Maßnahmen:

- SAP gestattet ausschließlich befugten Personen im Rahmen ihrer Pflichten, auf Personenbezogene Daten zuzugreifen.
- SAP hat für die SAP Dienste ein Protokollierungssystem für das Erfassen, Ändern und Löschen oder Sperren Personenbezogener Daten durch SAP oder ihre Unterauftragsverarbeiter im technisch möglichen Umfang implementiert.

f. **Auftragskontrolle.** Auftragskontrolle ist erforderlich um zu gewähren, das Personenbezogene Daten, die im Auftrag verarbeitet werden, ausschließlich in Übereinstimmung mit Weisungen des Auftraggebers verarbeitet.
Maßnahmen:

- SAP nutzt Kontrollen und Verfahren, um die Einhaltung der Verträge zwischen SAP und ihren Auftraggebern, Unterauftragsverarbeitern oder anderen Serviceanbietern zu überwachen.
- Im Rahmen der SAP Security Policy erfordern Personenbezogene Daten zumindest den gleichen Schutz wie „vertrauliche" Informationen im Sinne des SAP-Informationsklassifizierungsstandards.
- Sämtliche SAP-Mitarbeiter und Unterauftragsverarbeiter oder anderen Serviceanbieter werden vertraglich verpflichtet, die Geheimhaltungspflicht in Bezug auf alle sensiblen Informationen einschließlich Geschäftsgeheimnissen von Auftraggebern und Partnern der SAP einzuhalten.
- Bei der Pflege haben Auftraggeber jederzeit die Kontrolle über ihre Remote-Support-Verbindungen. SAP-Mitarbeiter können ohne Wissen und Zustimmung des Auftraggebers nicht auf ein Auftraggeber System zugreifen. Für Pflege bietet SAP ein spezielles, sicheres Support-Ticket an, in dem SAP einen speziellen, zugangskontrollierten und überwachten Sicherheitsbereich für die Übertragung von Zugangsdaten und Passwörtern zur Verfügung stellt. Die Auftraggeber haben jederzeit die Kontrolle über ihre Remote-Support-Verbindungen. SAP-Mitarbeiter können ohne Wissen und aktiver Beteiligung des Auftraggebers nicht auf ein On Premise System des Auftraggebers zugreifen.

g. **Verfügbarkeitskontrolle.** Personenbezogene Daten werden vor versehentlicher oder nicht autorisierter Vernichtung oder Verlust geschützt.
Maßnahmen:

- SAP verfügt über regelmäßige Backup-Prozesse zur Wiederherstellung der Verfügbarkeit geschäftskritischer Systeme bei Bedarf.
- SAP verwendet unterbrechungsfreie Stromversorgungen (USV, Batterien, Generatoren usw.), um die Stromversorgung für die Rechenzentren zu schützen.
- SAP hat Geschäftskontinuitätspläne für geschäftskritische Prozesse definiert.
- Notfallprozesse und -systeme werden regelmäßig getestet.

h. **Trennungskontrolle.** Personenbezogene Daten, die für unterschiedliche Zwecke erfasst werden, können getrennt verarbeitet werden.
Maßnahmen:

- SAP nutzt angemessene technischen Kontrollen, um jederzeit die Trennung von Auftraggeberdaten zu erreichen.
- Der Auftraggeber (einschließlich seiner von ihm freigegebenen Verantwortlichen) wird auf Basis einer sicheren Authentifizierung und Autorisierung ausschließlich Zugriff auf seine eigenen Daten gewährt.
- Wenn zur Bearbeitung eines Supportfalls des Auftraggebers Personenbezogene Daten dieses Auftraggebers benötigt werden, werden die Daten dieser Meldung zugeordnet und nur zur Bearbeitung dieser Meldung verwendet; für die Bearbeitung anderer Meldungen findet kein Zugriff auf diese Daten statt. Diese Daten werden in dedizierten Support-Systemen gespeichert.

I. **Datenintegritätskontrolle.** Personenbezogene Daten bleiben während der Verarbeitungsaktivitäten unversehrt, vollständig und aktuell.
Maßnahmen:

SAP hat zum Schutz vor unautorisierten Änderungen eine mehrere Schichten umfassende Sicherheitsstrategie umgesetzt.

Insbesondere verwendet SAP die folgenden Mittel, um die obigen Abschnitte zu Kontrollen und Maßnahmen umzusetzen. Insbesondere:

- Firewalls
- Security Monitoring Center
- Antivirensoftware
- Erstellen von Sicherungskopien und Wiederherstellung
- Externe und interne Penetrationstests

Regelmäßige Prüfung der Sicherheitsmaßnahmen durch externe Prüfer

Anhang 4 zur AVV
Standardvertragsklauseln (Auftragsverarbeiter)[1]

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

[...]
(in den Klauseln nachfolgend als „**Datenexporteur**" bezeichnet)

Und

[...]
(in den Klauseln nachfolgend als „**Datenimporteur**" bezeichnet)

(die „Partei", wenn eine dieser Organisationen gemeint ist, die „Parteien", wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln"), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1);

b) der „Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter" ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der

[1] Gemäß dem Beschluss der Kommission vom 5. Februar 2010 (2010/87/EU)

Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht" bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen" sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2

Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3

Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs [2]

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7

Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11

Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss [3]. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: ...

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

(1) Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

(2) Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche

(3) Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

DocuSign Envelope ID: 46C287BD-AF3E-4C26-9F0C-BE4660600327

Anlage 5

zu Order Form Nr. 49003196

Muster Leistungsnachweis Erstellungsvertrag

Anlage 5

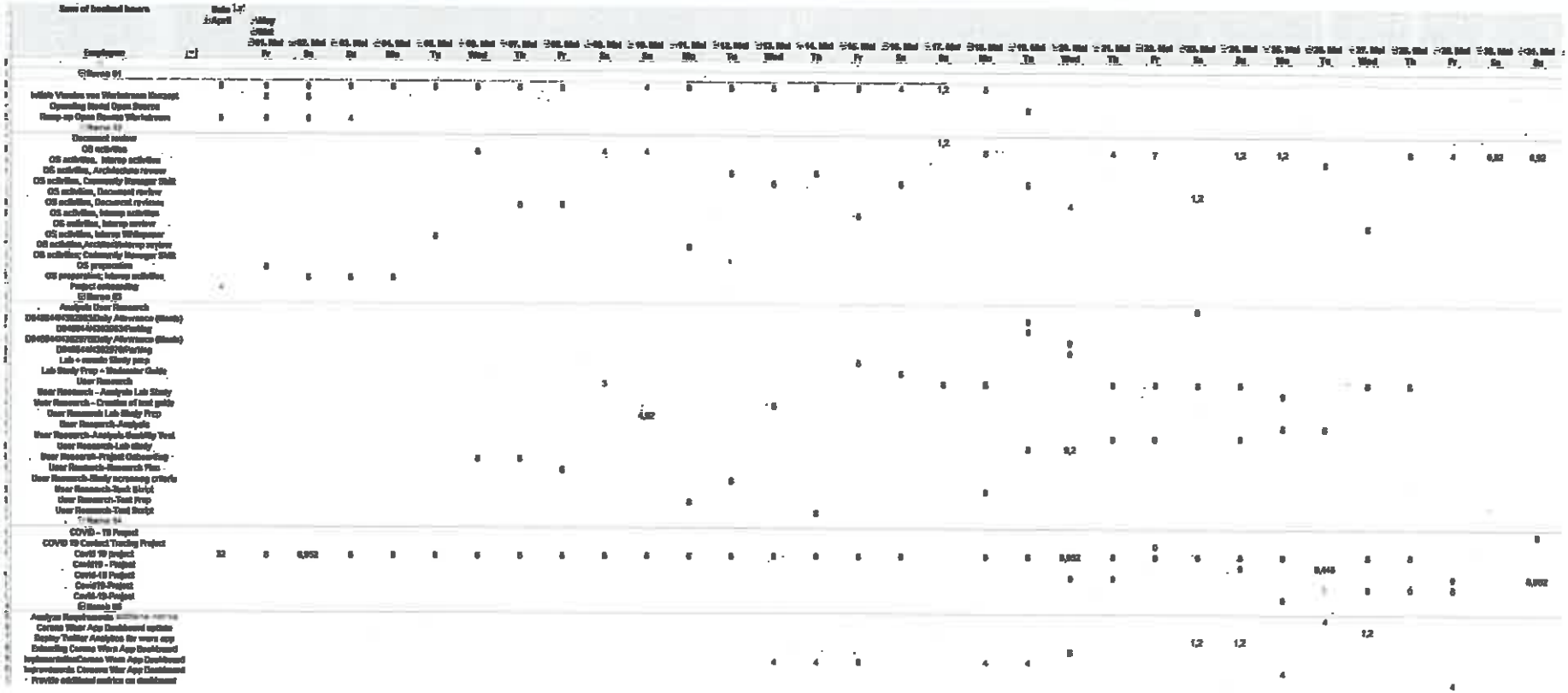
zu Order Form Nr. 49003196

Muster Leistungsnachweis Erstellungsvertrag

Ansicht 1:

Sum of booked hours	+Mai																																
	+18			+19							+20							+21								+22							+23
Name	01. Mai	02. Mai	03. Mai	04. Mai	05. Mai	06. Mai	07. Mai	08. Mai	09. Mai	10. Mai	11. Mai	12. Mai	13. Mai	14. Mai	15. Mai	16. Mai	17. Mai	18. Mai	19. Mai	20. Mai	21. Mai	22. Mai	23. Mai	24. Mai	25. Mai	26. Mai	27. Mai	28. Mai	29. Mai	30. Mai	31. Mai
Name 01	8,0	7,0	8,0	8,0	8,0	8,0	8,0	8,0	5,5	3,5	8,0	8,0	7,0	8,0	8,0	4,5		8,0	8,0	8,0	8,0	8,0	4,9		8,0						
Name 02	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0		8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0		6,0	8,0	8,0	8,0	8,0	8,0		
Name 03	8,0	8,0	8,0	4,0	8,0	8,0	4,0	8,0	8,0	4,9	8,0	8,0	8,0	8,0	3,0	3,0		3,0													
Name 04																															
Name 05														4,9					8,0	8,0	4,9	8,0	7,0	7,0	8,0						
Name 06																			8,0	8,0	4,9	1,2	3,0	3,0	3,0						
Name 07	8,0	8,0	4,0	8,0	8,0	8,0	8,0	8,0		4,0	8,0	8,0	8,0	8,0	8,0	4,0	1,2	8,0	8,0												
Name 08	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	4,0	4,0	8,0	8,0	8,0	8,0	8,0	8,0	1,2	8,0	6,0	4,0	4,0	7,0	1,2	1,2	1,2	8,0	6,0	8,0	4,0	0,9	8,9
Name 09																				8,0	8,0	8,0	4,9	3,0	4,9	4,9	4,9	8,0	8,0	3,0	
Name 10	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0														
Name 11																				8,0		8,0			8,0	8,0		8,0			
Name 12	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	7,0	8,0	8,0	8,0	8,0	8,0	8,0	0,9	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0
Name 13						8,0	8,0	8,0	3,0	4,9	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	9,2	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0			
Name 14	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0			0,0	0,0												
Name 15	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0		8,0	8,0	9,0	8,0	8,0	6,0	8,0	8,0	9,4	8,0	8,0	8,0		9,0
Name 16																			8,0	8,0			8,0								
Name 17		0,9		3,0	0,9	0,5	0,5	0,9			0,9	0,9	0,9	0,9	0,5			0,5	0,9												
Name 18												0,9	0,9	1,2	8,0			1,2	1,2	3,0		4,0			1,2	8,0	3,0	4,0	1,2		
Name 19													4,0	4,0	8,0			4,0	4,0	8,0			1,2	1,2	4,0	4,0	1,2		4,0		
Name 20																			1,2	4,0		4,0	8,0								
Name 21																		4,0	4,0	4,0	8,0	4,0									
Name 22				8,0		8,0					8,0		8,0					8,0							8,0						

Ansicht 2:



DocuSign Envelope ID: 46C267BD-AF3E-4C26-9F0C-BE4660800327

Anlage 6
zu Order Form Nr. 49003196
Beschreibung Service Elements

High Value Design Services

'High Value Design Services' für IDP erstellen typischerweise das Design für "Innovative Development Projects" (IDP). Dies kann sämtliche oder einzelne der folgenden Leistungen umfassen:

- Durchführung von "high level" Analysen und Dokumentation der aktuellen Prozessabläufe und Anforderungen des Kunden zum Zwecke der Unterstützung der Projektbewertung und zur Erarbeitung von Lösungsvorschlägen, einschließlich der zukünftig geplanten Prozessabläufe
- Identifizierung von Risiken der Anwendung und und Massnahmen zur Risikominderung, einschließlich der Entwicklung von Machbarkeitsstudien
- Erstellung von Lösungsvorschlägen und Spezifikationsdokumentation, einschließlich der entsprechenden Planung, Analyse und schriftlichen Erstellung (unter Einhaltung der IDP Entwicklungsmethodologie, des entsprechenden Dokumentationsstandards, weiterer Standards und Richtlinien und Information Design-Prozesse der SAP)
- Durchführung von Spezifikationsanalysen in Bezug auf die Vollständigkeit und Richtigkeit der Spezifikation
- Design User Experience
- Analyse der Projektdokumentation, Übersetzungs- sowie Überarbeitungsdienstleistungen um diese auf die gewünschten Qualitätsansprüche anzupassen
- Durchführung von Code Reviews zur Einhaltung der Produkt- und Sicherheitsstandards der SAP und der Anforderungen an das Design im Rahmen des Projekts und der Spezifikationsrichtlinien
- Analyse von Testvorgaben zur Bewertung der Einhaltung der in der Spezifikationsdokumentation festgelegten Anforderungen sowie von nicht funktionalen Anforderungen
- Analyse der Testdurchführung zur Qualitätssicherung
- Prüfung der Dokumentation, Rückverfolgbarkeitsanforderungen und Richtigkeit nach Maßgabe der Anforderungen des Projekts, einschließlich der nicht- funktionalen Anforderungen
- Prüfung der Vollständigkeit von Anwendungsstellen, einschließlich vom Kunden zur Verfügung gestellter Dokumente und Software-Paketen
- Durchführung von Qualitätsanalysen zur Einhaltung der Entwicklungs- und Qualitätssicherungsanforderungen

Special Development Services

'Specialized Development Services' erbringt typischerweise die fundamentalen Ausführungsleistungen für ein Projekt welches auf SAP Innovative Development Technologie basiert, wie z.B. S/4HANA, Internet of Things, oder SAP Fiori. Dies kann alle oder einzelne der folgenden Leistungen umfassen:

- Coding der Geschäftslogik nach Maßgabe der Programmiermodelle und Backend-Funktionen
- Entwicklung der Nutzer-Schnittstellen bestehend aus nicht standardisierten UI-Komponenten
- Qualitätsüberprüfungen zur Qualitätssicherung, einschließlich der Anwendung von automatisierten Tools, die Spezialkenntnisse erfordern

Project Management Services

Das Project Management für Innovative Development Projects umfasst typischerweise die Steuerung und Auslieferung eines Innovative Development Projects (IDP). Die Aufgaben der 'Project Management Services' für Innovative Development Projects umfassen SAP's spezifische Project Management-Verantwortlichkeiten in Bezug auf die IDP Leistungen und umfasst keine Aktivitäten des Kunden. Dies kann alle oder einzelne der folgenden Leistungen bzw. Verantwortlichkeiten umfassen:

- Erstellung des Projektplans und Klärung interner Beschränkungen und Abhängigkeiten innerhalb des Projekts
- Leitung und Verantwortung für die Projektplanung und die Überwachung der Auslieferung von Arbeitsergebnissen in Bezug auf eine erfolgreiche Projektdurchführung
- Unterstützung bei der Umsetzung genereller Zielsetzungen und Anforderungen des Kunden in konkrete Projektziele, in eine Erstellungsstrategie und in strategische Erstellungspläne
- Definieren, Erstellen und Aufrechterhalten des Modells für die Projektumsetzung über die gesamte Dauer des Projekts

- Erstellung von Projektstandards in Bezug auf die Projektmethodologie, die Dokumentation, Tools, Budgetplanung und Reporting, etc.
- Koordinierung von Aktivitäten im Projekt und von Projektteams in Übereinstimmung mit dem Projektplan
- Überwachung und Berichterstattung über den Fortschritt des Projekts anhand des Projektplans
- Steuerung von Änderungen im Rahmen des Projekts in Übereinstimmung mit dem Plan zum Änderungsmanagement zur Kontrolle der Anforderungen, der Qualität und des Zeitplans
- Steuerung und Eingreifen bei Problemen oder Risiken im Rahmen des Projekts und Koordinierung des Problem- und Risikomanagements innerhalb des Projekts
- Steuerung der Übergabe der Arbeitsergebnisse und des Abnahmeprozesses
- Eskalationslevel für die einzelnen Arbeitsgruppen und Teams innerhalb des Projekts
- Enge Zusammenarbeit mit den Auftraggebern, den Projektmanagern des Auftraggebers und dem Steering Committee des Projekts um Entscheidungen für den Projektfortschritt herbeizuführen
- Steuerung der Erwartungshaltung der Projektbeteiligten