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 14 Tage nach Rechnungsstellung 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:

10.1.1 SAP haftet bei Vorsatz in voller Höhe, bei grober Fahrlässigkeit und bei Fehlen einer Beschaffenheit, für die SAP eine Garantie übernommen hat, nur in Höhe des vorhersehbaren Schadens, der durch die verletzte Pflicht oder die Garantie verhindert werden sollte;

10.1.2 in anderen Fällen: nur bei Verletzung einer wesentlichen Pflicht (Kardinalpflicht) und bis zu den im folgenden Unterabsatz genannten Haftungsgrenzen. Die Verletzung einer Kardinalpflicht im Sinne dieses Abschnitts 10.1.2 liegt vor bei Verletzung einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages erst ermöglicht oder deren Verletzung die Erreichung des Vertragszwecks gefährdet und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf.

Die Haftung ist in den Fällen von Abschnitt 10.1.2 beschränkt auf EUR 200.000,- pro Schadensfall, insgesamt auf höchstens EUR 500.000,- aus der Order Form.

10.2 Der Einwand des Mitverschuldens bleibt offen. Die Haftungsbegrenzungen gemäß Abschnitt 10.1 gelten nicht bei der Haftung für Personenschäden und bei der Haftung nach dem Produkthaftungsgesetz.

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 wiedersprechen. 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-Folgenab-schätzung.
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.