Vertrag zur Auftragsverarbeitung personenbezogener Daten gemäß Art. 28 DSGVO[1]

AV-Vertrag
für
Projekt- und Wartungstätigkeiten mit Zugang auf IT-Systeme des Kunden

Zwischen dem/der

.....
- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

apollon GmbH+Co.KG

Maximilianstraße 104

75172 Pforzheim

.....
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Vertrags

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

- Projektarbeiten (z.B. Customizing, Entwicklung, Inbetriebnahme), wobei Umfang und Inhalt in der zugrundeliegenden Leistungsvereinbarung (z.B. Entwicklungsauftrag) geregelt sind;

und/oder

[1] basierend auf dem Muster des GDD e.V. Stand Juni 2021, siehe https://www.gdd.de/aktuelles/start-seite/ueberarbeitetes-muster-zur-auftragsverarbeitung-gem-art-28-ds-gvo

- ggf. Support-/Wartungsarbeiten (je nach Regelungen in der zugrundeliegenden Leistungsvereinbarung)

per Remote-Zugriff auf Test- und Entwicklungssysteme des Auftraggebers, in Abstimmung mit dem Auftraggeber auch auf operative Systeme, wobei die Aufgaben durch gesonderte Leistungsvereinbarungen beauftragt werden und der Auftragnehmer im Rahmen dieser Aufgaben in Kontakt mit personenbezogenen Daten kommen kann, die auf den dortigen Systemen vom Auftraggeber gespeichert sind oder vom Auftraggeber dem Auftragnehmer z.B. in Form von Log-Files- oder sonstigen Datenbankauszügen zur Durchführung der Aufgaben überlassen werden.

(2) Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 3 Monaten zum Monatsende gekündigt werden, wobei eine Kündigung dessen Geltung für noch laufende/noch nicht abgeschlossene Leistungsvereinbarungen unberührt lässt. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas Anderes.

2. Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Zur Durchführung von Projekt- und Support-/Wartungsarbeiten erhält der Auftragnehmer einen Remote-Zugriff auf Systeme des Auftraggebers, wobei der Auftragnehmer bei Durchführung dieser Aufgaben in Kontakt mit personenbezogenen Daten kommen kann, die auf den dortigen Systemen vom Auftraggeber gespeichert sind oder vom Auftraggeber dem Auftragnehmer z.B. in Form von Log-Files- oder sonstigen Datenbankauszügen zur Durchführung der Aufgaben überlassen werden. Eine Bearbeitung personenbezogener Daten findet nur im Ausnahmefall statt, z.B. Einrichten von Administrations- und Zugriffsrechten für Mitarbeiter des Auftraggebers.

(2) Art der Daten

Von der in Ziff.2 (1) vorgesehenen Datenverarbeitung können – je nachdem welche Tätigkeiten der Auftraggeber beauftragt und in welchem Umfang er einen Zugang auf seine IT-Systeme ermöglicht - folgende Datenkategorien betroffen sein: Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorien, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Kunden, Beschäftigte, Lieferanten/Dienstleister, Ansprechpartner.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung (Anlage 1). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.

4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass

der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

☒ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

☒ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage 2 werden die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

☒ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Unterschriften

Auftraggeber	**apollon GmbH Co. KG**
Erster Unterzeichner	*Erster Unterzeichner*
_____ Ort, Datum	_____ Ort, Datum
_____ Name	_____ Name
_____ Titel	_____ Titel
_____ Unterschrift	_____ Unterschrift
Zweiter Unterzeichner	*Zweiter Unterzeichner*
_____ Ort, Datum	_____ Ort, Datum
_____ Name	_____ Name
_____ Titel	_____ Titel
_____ Unterschrift	_____ Unterschrift

Anlage 1 - Technisch-organisatorische Maßnahmen

Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 DSGVO) der apollon GmbH+Co. KG unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen, wobei apollon die Muttergesellschaft Meyle+Müller GmbH+Co. KG als Erfüllungsgehilfen einsetzen darf.

Ansprechpartner für den Datenschutz

Fragen zum Datenschutz bei apollon und zu den aufgelisteten Datenschutzmaßnahmen beantwortet Ihnen:

Georg Schütz

Datenschutzbeauftragter

Dekra Assurance Services GmbH

georg.schuetz.partner@dekra.com

(1) Zutrittskontrolle

- Unbefugten wird der Zutritt zum von apollon eingesetzten Rechenzentrum durch folgende Maßnahmen verwehrt:
- Der Serverraum wird videoüberwacht; Speicherung der Videodaten als MPEG-Dateien.
- Zugang zum Serverraum über einen wiederum durch Codeschlüssel geschützten Bereich.
- Sicherheitsbereichstüren sind durch ein elektronisches Zutrittskontrollsystem geschützt. Dieses basiert auf berührungslosen passiven Identkarten (Legic).
- Besucher für diese Bereiche werden begleitet.
- Der Serverraum ist baulich gesichert, fensterlos und besitzt festes Mauerwerk.
- Es existiert eine Alarmanlage, die alle Zutrittsmöglichkeiten zum Gebäude einschließt. Im Alarmfall wird der Sicherheitsdienst automatisch informiert.

(2) Zugangskontrolle

Durch folgende Maßnahmen wird verhindert, dass DV-Systeme von Unbefugten genutzt werden können:

- Systemanwender authentifizieren sich durch Benutzerkennung und Passwort.
- Individuelle Berechtigungen werden durch die Einrichtung persönlicher Benutzerkonten gesteuert. Einwahlversuche werden protokolliert. Benutzerkonten werden nach 5 Fehlversuchen gesperrt.
- Folgende Vorgaben werden für die Passwörter gemacht: Mindestens 10 Zeichen, Groß-, Kleinschreibung, Zahlen bzw. Sonderzeichen.
- Aktuelle Firewall ist installiert.

(3) Zugriffskontrolle

- Die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen haben ausschließlich auf die zu ihrer Zugriffsberechtigung unterliegenden Daten Zugriff.
- Personenbezogene Daten können bei der Verarbeitung und Nutzung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Dieses wird durch programmtechnische Vorgaben einerseits und durch vertragliche Vorgaben im Arbeitsvertrag gewährleistet. Zugriffe werden protokolliert.

(4) Weitergabekontrolle

- Personenbezogene Daten können bei der elektronischen Übertragung bzw. während des Transports oder der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.
- Es kann überprüft und festgestellt werden, an welche Stellen eine Übermittlung personenbezogener Daten eine Datenübertragung vorgesehen ist.
- Im Bereich der Verarbeitung personenbezogener Daten werden entsprechende Protokolle geführt.
- Verschlüsselung der Daten auf der gesamten Datenverbindungsstrecke zwischen Kunde und apollon.
- Die Entsorgung von Papierunterlagen geschieht durch Benutzung von Reißwölfen bzw. eines dafür beauftragten Entsorgungsunternehmens.

(5) Eingabekontrolle

Die Möglichkeit, nachträglich zu überprüfen, von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, ist gegeben durch:

- die organisatorische Festlegung von Zuständigkeiten und Zugriffssteuerung
- Protokolle der Datenerfassung.

(6) Auftragskontrolle

Die Unter-Auftragnehmer werden gemäß Art. 28 DSGVO sowie unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO ausgewählt. Das betrifft unter anderem folgende Maßnahmen:

- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers
- die Mitteilungspflicht bei Verstößen des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags etc.

(7) Verfügbarkeitskontrolle

Personenbezogenen Daten sind gegen zufällige Zerstörung oder Verlust geschützt, siehe auch Punkt 2. Dies wird zudem durch folgende Maßnahmen gewährleistet:

- Regelmäßige Datensicherung, an den Arbeitstagen inkrementell, am Wochenende vollständig.
- Server mit Kundendaten werden 1x täglich inkrementell gesichert
- Regelmäßige Prüfung der Wiederherstellbarkeit, Protokollierung nach jeder Sicherung.
- Backupmedien werden in Lampertz-Safes gelagert.

(8) Trennungskontrolle

Zu unterschiedlichen Zwecken erhobene Daten können getrennt verarbeitet werden. Dies gewährleistet apollon durch:

- Verarbeitung auf getrennten Servern, Services werden getrennt.
- Die Daten werden in unterschiedlichen Systemen verarbeitet.
- Unterschiedliche Mandanten auf Basis von Kunden- bzw. Mandantennummern

(9) Pseudonymisierung

Sofern die jeweiligen eingesetzten Produkte dies unterstützen, werden pseudonymisierende Maßnahmen bei allen Produkten umgesetzt. Da diese Vorgaben herstellerabhängig sind (Datenbank unterstützt Pseudonymisierungs-Hashs nicht), wird bei Nicht-Vorhandensein jener, mittels bereits aufgeführter Maßnahmen versucht, den maximalen Schutz zu gewährleisten (Passwortstärke etc.)

(10) Verschlüsselung

Jegliche angebotenen Webdienste werden via Wildcard-Zertifikat vom Herausgeber „Go Daddy“ geschützt. Dieser Schutz beinhaltet die Verwendung des gängigen TLS-Verschlüsselungsverfahren. „Go Daddy“ ist ein anerkannter und vertrauenswürdiger Zertifikatsaussteller.

Weitere Dienste werden ebenfalls via TLS verschlüsselt (u.a. HTTPS, SFTP). Der Schutz innerhalb der Windows-Domäne wird durch die domäneneigene Stammzertifizierungsstelle gewährleistet und automatisiert via Stammzertifikat ausgerollt.

Die Verschlüsselung der Kunden-VPN-Verbindungen wird individuell mit den jeweiligen Administratoren bzw. Ansprechpartnern ausgehandelt und anschließend dokumentiert. Hierbei kommt der Verschlüsselungsalgorithmus nach Stand der Technik zum Einsatz.

(11) Privacy by Default

Die zur Verfügung gestellten Endgeräte werden über ein Softwarepaketierungsprodukt vorinstalliert. Hierbei werden vorgefertigte, auf den Datenschutz abgestimmte, Images verwendet, die den Austausch der personenbezogenen Inhalte gemäß gängiger Vorgaben der jeweiligen Hersteller reglementiert.

Mobile Endgeräte werden von der ausgebenden Stelle mit entsprechenden Reglementierungen ausgegeben.

(12) Privacy by Design

Soweit gemäß der mit dem Auftraggeber geschlossenen Leistungsvereinbarung apollon-eigene Softwareprodukte wie z.B. Online Media Net- und Online Mobile Services-Produkten von apollon bereitgestellt bzw. eingesetzt werden, wird schon bei den Release-Candidates darauf geachtet, dass gespeicherte personenbezogenen Daten per Hash pseudonymisiert werden. Loginname + Passwort werden als verkryptete Inhalte in Datenbanken abgelegt, und sind nur als diese von der verwendeten Algorithmik verwendbar.

(13) Technische Sicherheit

(13.1) Online-Daten

Soweit gemäß der mit dem Auftraggeber geschlossenen Leistungsvereinbarung apollon-eigene Softwareprodukte wie z.B. Online Media Net- und Online Mobile Services-Produkten von apollon bereitgestellt bzw. eingesetzt werden, wird diese Software auf mehreren virtuellen Servern basierend auf einer Server Virtualisierungs-Lösung im Cluster betrieben und durch Hochverfügbarkeit (HA) und Lastverteilung (DRS) Funktionen ergänzt. Alle DTP- und Bild-Daten werden auf zentralen Fileservern vorgehalten. Die Systeme sind mit allen gängigen Redundanzkomponenten aufgebaut. Die Daten werden in einem hochverfügbaren Speichernetzwerk (SAN) gespeichert. Eingesetzte Datenbanken werden auf einem Datenbank-Cluster betrieben.

(13.2) Backup von Daten

Einmal pro Woche, am Wochenende, wird durch eine spezielle Software ein Voll-Backup des gesamten Online-Datenbestandes durchgeführt; d. h. alle Daten werden komplett auf ein anderes Speichersystem gesichert. Zudem erfolgt täglich eine inkrementelle Sicherung der Online-Datenbestände [inkrementell => nur die am Tage veränderten Daten werden gesichert; veränderte Daten sind z. B. auch neu auf den Fileserver aufgespielte Daten, aber auch z. B. Bilddaten, die durch Farbretusche verändert wurden]. Beide Backup-Vorgänge laufen vollautomatisch ab. Die Sicherungszielsysteme werden im zweiten Serverraum (in einem anderen Brandabschnitt) betrieben.

(13.3) Backup von OMN-Systemen

Einmal pro Woche, am Wochenende, wird durch eine spezielle Software ein Voll-Backup der virtualisierten OMN-Server durchgeführt; d.h. alle Daten werden komplett auf ein anderes Speichersystem gesichert. Zudem erfolgt täglich eine inkrementelle Sicherung der virtualisierten Systeme. Beide Backup-Vorgänge laufen vollautomatisch ab. Die Sicherungszielsysteme werden im zweiten Serverraum (in einem anderen Brandabschnitt) betrieben.

(13.4) Stromversorgung

Mittels Unterbrechungsfreier Strom-Versorgung (USV) wird gewährleistet, dass im Falle eines Stromausfalls die Stromversorgung im von apollon eingesetzten konzerneigenen Rechenzentrum solange aufrechterhalten wird, bis das Gesamt-System automatisch und kontrolliert heruntergefahren wurde (von der USV-Anlage gesteuert). Dadurch ist sichergestellt, dass weder Datenbestände noch Hardwareteile zerstört werden.

Das von apollon eingesetzte konzerneigene Rechenzentrum verfügt zusätzlich über eine eigene Notstromversorgung. Das System besteht aus einem Diesel-Notstromaggregat und versorgt o. g. USV-Systeme innerhalb weniger Sekunden mit selbsterzeugter Energie. Der Treibstoffvorrat ermöglicht einen Notstrombetrieb von 24 Stunden.

(13.5) Internetanbindung und Firewall

Derzeit ist eine Sonicwall Super Massive - Firewall zum Schutz vor unbefugten Zugriffen aus dem Internet im Einsatz. Als Sicherheits-Puffer zwischen LAN und Internet ist eine sog. »DMZ« geschaltet. Die Firewall ist als Aktiv-Passiv-Cluster konstruiert. Wenn ein System ausfällt übernimmt das andere die Arbeit.

Ebenso ist die Anbindung an das Internet redundant, zwei 1 GBit-Leitungen von zwei Providern mit unterschiedlicher Hauszuführung werden als Autonomes System betrieben. Bei Ausfall einer Verbindung werden die ein- und ausgehende Datenpakete über den anderen Provider gelenkt.

(13.6) Virenschutz

Sämtliche Arbeitsplatz Rechner auf Windows- und Mac OS-Basis sind mit Antiviren-Software ausgestattet, die regelmäßig und automatisiert aktualisiert wird (servergesteuert). Zudem sind die E-Mail- und HTTP-Gateway-Server mit entsprechenden Antiviren-Lösungen ausgestattet.

Jedes Netzwerkpaket wird über die Firewall direkt am Gateway per DPI (Deep Paket Inspection) auf Viren geprüft, sowohl interner als auch externer Traffic.

(13.7) Zugangs- und Einbruchschutz

Wichtige Ein- und Durchgänge sind durch elektronische Schlösser gesichert; dies geschieht mittels einer computergesteuerten Schließanlage (insbesondere Eingang zum Serverraum). Diese regelt den Zugang durch Einsatz individuell für jeden Zugangsberechtigten programmierbarer Codeschlüssel (Zugang, Tag, Uhrzeit bzw. Zeitfenster, Protokollierung).

Das gesamte Gebäude wird in der Nacht (am Wochenende auch tagsüber) von einem Wachdienst kontrolliert. Dabei werden evtl. geöffnete Fenster und unverschlossene Stockwerks- bzw. Bereichstüren abgeschlossen. Außerdem werden u.U. noch eingeschaltete elektronische Geräte – falls nicht besonders vereinbart – ausgeschaltet. Das Erdgeschoß ist durch eine Einbruchmeldeanlage gesichert. Im Falle eines Einbruchs wir ein Alarm ausgelöst.

(13.8) Brandschutz

Die betrieblichen Räumlichkeiten sind mit einer Brandmeldeanlage ausgestattet. In allen Räumen sind Brandmelder installiert, im Falle eines Brandes wird automatisch die Feuerwehr alarmiert. Zusätzlich ist das von apollon eingesetzte Rechenzentrum mit einem Rauch-Ansaug-System, Minimalrauchfühlern und einer automatischen Gaslöschanlage ausgestattet.

Anlage 2 - Genehmigte Unterauftragsverhältnisse

Firma Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland*
Meyle+Müller GmbH + Co. KG	Maximilianstraße 104 75172 Pforzheim	(1) Betreiben von Teilen der IT-Infrastruktur, auf der der Auftragnehmer seine Leistungen erbringt; (2) administrative und arbeitsteilige Tätigkeiten als Muttergesellschaft	Keine Datenübermittlung in Drittländer

* An dieser Stelle kommen insbesondere die Standarddatenschutzklauseln der Kommission gem. Art. 46 Abs. 2 lit. c DS-GVO in der Variante „Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter“ (Modul 3) in Betracht.

Anlage 3 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Weisungsempfänger des Auftragnehmers:

Name: Norbert Weckerle

E-Mail: nweckerle@apollon.de

Telefon: 0162 26 26 199

Name: Tobias Marks

E-Mail: tmarks@apollon.de

Telefon: 0162 26 26 109

Weisungsberechtigte des Auftraggebers:

Name: _____

E-Mail: _____

Telefon: _____

Name: _____

E-Mail: _____

Telefon: _____