AUFTRAGSVERARBEITUNGSVERTRAG

zwischen Kunde
als Verantwortlicher

- nachfolgend: Auftraggeber -

und GAPTEQ GmbH, Flintsbacher Straße 12, 83098 Brannenburg
als Auftragsverarbeiter

- nachfolgend: Auftragnehmer -

1. Gegenstand und Dauer des Vertrags

(1) Der Gegenstand des Vertrags ist in **Anlage 1** konkretisiert.

(2) Die Dauer und Kündbarkeit dieses Vertrages richten sich nach der Laufzeit und Kündbarkeit der jeweiligen Leistungsvereinbarung. Soweit die Leistungsvereinbarung auf unbestimmte Zeit geschlossen ist und nichts Abweichendes vereinbart ist, ist die jeweilige Leistungsvereinbarung nach Maßgabe der gesetzlichen Bestimmungen ordentlich kündbar. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

(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 Auftragsinhalts

(1) **Art und Zweck der vorgesehenen Verarbeitung von Daten**

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber werden in der **Anlage 1** konkretisiert.

(2) **Art der Daten**

Die Art der vom Auftraggeber verarbeiteten Daten werden in der **Anlage 1** konkretisiert.

(3) **Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen werden in **Anlage 1** konkretisiert.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gemäß Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung (**Anlage 2**). 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 Art. 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 – spätestens 12 Stunden nach Kenntniserlangung - an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 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.

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.

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

Der Auftraggeber stimmt der Beauftragung der in **Anlage 3** 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. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Genehmigung des Hauptauftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.“

(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 bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(6) Der Auftragsnehmer haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragnehmer seinen Pflichten gemäß dem mit dem Auftragnehmer geschlossenen Vertrag nachkommt. Der Auftragnehmer benachrichtigt den Auftraggeber, wenn der Unterauftragnehmer seine vertraglichen Pflichten nicht erfüllt.

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. In der **Anlage 3** werden die 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.

11. Haftung

a) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner nach Art. 82 DS-GVO.

b) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden.

c) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

d) Die Buchstaben b) und c) dieser Ziffer 11 gelten nicht, soweit der Schaden durch die konkrete Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

12. Anwendbares Recht, Gerichtsstand

a) Es findet deutsches Recht Anwendung.

b) Der Gerichtsstand befindet sich am Sitz des Auftragnehmers.

13. Schlussbestimmungen

a) Änderungen und Ergänzungen dieses Vertrags bedürfen einer gesonderten Vereinbarung in schriftlicher oder elektronischer Form sowie des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

b) Sollten einzelne Regelungen dieses Vertrags unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, die der wirtschaftlichen Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

Anlage 1 - Auftragsspezifische Konkretisierung

1. Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung ergibt sich aus der jeweiligen Leistungsvereinbarung und bezieht sich auf die Bereitstellung der jeweiligen Dienste, wie z.B. das Hosting der Cloud-Umgebung und die Bereitstellung des GAPTEQ-Portals.

2. Dauer der Verarbeitung

Bezüglich der Dauer wird auf Ziff. 1 Abs. 2 verwiesen.

3. Art der Verarbeitung

Die Art der Verarbeitung richtet sich nach der jeweiligen Leistungsvereinbarung und kann die Erhebung, Speicherung, Übermittlung, Nutzung, Löschung und sonstige Verarbeitung personenbezogener Daten umfassen, die der Auftragnehmer nach Weisung im Rahmen der Leistungserbringung für den Auftraggeber vornimmt.

4. Zweck der Verarbeitung

Zweck der Verarbeitung ist die Erfüllung der vertraglichen Pflichten des Auftragnehmers gegenüber dem Auftraggeber im Rahmen der Leistungserbringung, wie z.B. die Bereitstellung der GAPTEQ-Cloud-Instanz oder die Bereitstellung des GAPTEQ-Portals.

5. Art(en) der personenbezogenen Daten

- Name, Anschrift, E-Mail-Adresse, Telefonnummer und sonstige Kontaktdaten der Nutzer
- Anmeldedaten, Passwörter, Zugriffsrechte
- Nutzungsdaten, Verkehrsdaten, Protokolldaten und sonstige technische Daten, die bei der Nutzung des Portals und der sonstigen IT-Dienste des Auftragnehmers anfallen
- sonstige Daten, die der Auftraggeber im Rahmen der angebotenen Dienste des Auftragsnehmers zur Verfügung stellt

6. Kategorien betroffener Personen

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers

Anlage 2
Technische und organisatorische Maßnahmen

Allgemeines

Die GAPTEQ GmbH hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die GAPTEQ GmbH hat angemessene technische und organisatorische Maßnahmen etabliert, um den Zugang zu Orten zu beschränken, an denen personenbezogene Daten oder andere vertrauliche Informationen gespeichert aufbewahrt werden,

- Systeme, auf denen personenbezogene Daten oder andere vertrauliche Informationen gespeichert sind, gegen einen unbefugten Zugriff zu sichern,
- zu gewährleisten, dass nur autorisierte Personen Zugang haben,
- zu gewährleisten, dass Versuche eines unberechtigten Zugangs entdeckt und verhindert werden,
- jede Person, die Zugriff auf personenbezogene Daten oder andere vertraulichen Informationen nehmen möchte, eindeutig zu identifizieren,
- einen solchen Zugriff ausschließlich berechtigten Personen zu gestatten,
- zu verhindern, dass personenbezogene Daten oder andere vertrauliche Informationen unbefugt eingesehen, kopiert, verändert oder gelöscht werden können,
- Berechtigungsprofile einzurichten und zu konfigurieren, die sicherstellen, dass Mitarbeiter jeweils nur Zugriff auf solche personenbezogenen Daten und anderen vertraulichen Informationen bzw. zu solchen Ressourcen haben, die sie zur Erfüllung der ihnen jeweils zugewiesenen Pflichten zwingend benötigen
- feststellen zu können, ob personenbezogene Daten und andere vertrauliche Informationen im CRM System verändert oder gelöscht wurden,
- zu gewährleisten, dass personenbezogene Daten und andere vertrauliche Informationen nur gemäß GAPTEQ Sicherheitskonzept und sonstiger Vorgaben (z.B. anwendbare Gesetze, Kundenverträge, interne Richtlinien) erhoben, verarbeitet und genutzt werden,

- zu gewährleisten, dass personenbezogene Daten und andere vertrauliche Informationen, die für unterschiedliche Zwecke erhoben werden, getrennt verarbeitet werden können,
- zu gewährleisten, dass personenbezogene Daten und andere vertrauliche Informationen nach Möglichkeit pseudonymisiert oder verschlüsselt werden,
- zu gewährleisten, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten im Zusammenhang mit der Verarbeitung personenbezogener Daten und anderer vertraulicher Informationen auf Dauer sichergestellt werden,
- zu gewährleisten, dass die Verfügbarkeit personenbezogener Daten und anderer vertraulicher Informationen und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können,
- zu gewährleisten, dass alle Mitarbeiter, die Zugang zu personenbezogenen Daten oder anderen vertraulichen Informationen haben, ihrer Pflichten und der Konsequenzen ihrer Verletzung gewahr sind.

Darüber hinaus ergreift die GAPTEQ GmbH folgende angemessene, allgemeine Maßnahmen:

- Fachliche Fortbildungen/Onlinetrainings der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten
- Schulungen/Onlinetrainings und Unterweisungen für Mitarbeiter im Umgang mit der IT und zur Schärfung des IT-Sicherheitsbewusstseins
- Sicherheitshinweise werden allen Mitarbeitern in geeigneter Form bekannt gegeben und sind dauerhaft abrufbar
- Auswertung von Meldungen und Berichten zu ungewöhnlichen Vorkommnissen
- Untersuchung erkannter oder vermuteter Verstöße gegen sicherheitsrelevante Vorgaben
- Automatische Protokollierung der Systemnutzung unter Beachtung der daten-schutzrechtlichen Grenzen
- Regelmäßige und anlassbezogene Kontrolle der Funktionalität der IT, einschließlich unter dem Aspekt der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Verfügbarkeitskontrolle, Auftragskontrolle sowie der Trennungskontrolle
- Eskalations- und Meldewege bei sicherheitsrelevanten Vorkommnissen

- Verfügbarkeit der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten als Ansprechpartner bei allen Fragen zur IT-Nutzung und -sicherheit
- Schriftliche Verpflichtung aller, für die Erbringung der Dienstleistungen eingesetzten Beschäftigten auf die Wahrung der Vertraulichkeit gemäß Artikel 28, 29 und 32 DSGVO.

Maßnahmen in wichtigen Einzelbereichen sind in den folgenden Abschnitten zusammengefasst, wobei sich die Darstellung an den Vorgaben aus Art. 32 Abs. 1 der Datenschutzgrundverordnung orientiert.

1. Zugangskontrolle

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Ein unbefugter Zutritt zu den Gebäuden und Räumen ist durch verschiedene bauliche Maßnahmen, technische Einrichtungen und organisatorische Vorkehrungen erheblich erschwert:

- Türschlösser und elektrische Türschlösser (Zutrittstransponder)
- Sicherheitsschlösser: Haus- und Büro-Eingangstüren
- Schlüsselregelung und Quittierung der Schlüsselausgabe
- Gesicherte Aufbewahrung von Generalschlüsseln und Regelungen zur Generalschlüsselentnahme
- Biometrisches Authentifizierungssystem, teilweise per Fingerabdruck
- Verschließen von Türen und Fenstern außerhalb von Geschäftszeiten
- Klare Zuweisung der Berechtigungen (Zugang Gebäude, Büro)
- Gast-Prinzip: Der Zugang in Gebäude ist für Besucher nur über den mit Personal besetzten Empfang möglich, von dem aus Besucher durch einen internen Mitarbeiter abgeholt und durch das Gebäude geführt werden, d.h. Besucher können sich nicht frei und unkontrolliert im Gebäude bewegen
- Kein Serverraum und keine Server innerhalb der GAPTEQ Büroräume

2. Datenträger- und Speicherkontrolle, Benutzerkontrolle

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um zu verhindern, dass Datenträger von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Authentifizierung der Nutzer
    - Zur Anmeldung an jeglicher IT ist die Eingabe einer Benutzerkennung erforderlich, üblicherweise bestehend aus Nutzername und Passwort (Azure AD Verwendung zur zentralen Userverwaltung)
    - Default-Passwörter sind bei der ersten Nutzung zu ändern
    - Kennwortrichtlinie mit konkreten Vorgaben (Komplexitätsvorgabe für Passwörter)
    - Verbot von Gruppen-Passwörtern
    - Verbot der Weitergabe von Benutzerkennungen und Kennwörtern
    - Zwei-Faktor-Authentifizierung
    - Automatische Sperrung (z.B. Regelung zur automatischen Sperrung des Computers nach einer bestimmten Zeit der Inaktivität mit anschließendem erneutem Login)
    - Automatischer Standby-Betrieb der lokalen Rechner
    - Speicherung von Passwörtern in Hash-Format HMAC-SHA256
    - Verwendung von Salt-Verfahren 256
    - Umgehende Benachrichtigungspflicht gegenüber den IT-Verantwortlichen bei erkanntem oder vermutetem Passwortverlust oder sonstigen Anhaltspunkten für eine unbefugte Verwendung von Benutzerkennungen
    - Administratoren-Passwort ist nur festen Mitarbeitern der IT-Abteilung bekannt (Azure AD Multifaktorauthentifizierung und Azure AD Auditlogs)
- Einsatz von Firewalls, SPAM-Filtern und aktuellen Virenscannern (z.B. Microsoft Advance Thread Protection), einschließlich regelmäßiger Updates
- Verschlüsselung von Datenträgern (Bitlocker); Regelung zum Umgang mit mobilen Datenträgern
- Differenziertes Berechtigungskonzept:
    - Restriktive, zentrale Rechtevergabe nach dienstlichen Erfordernissen (Need-To-Know-Prinzip)
    - restriktive Rechtevergabe auch für zugehörige Dokumentation (Berechtigungskonzept Laufwerke, ERP, CRM, sonstige Systeme)

  - geregelter Prozess zur Rechtevergabe bei Neueintritt sowie zum Rechteentzug bei Aufgabenänderung/Austritt von Mitarbeitern
- Differenziertes Ordnerkonzept (alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können)
- Regelmäßige Reviews der vorhandenen Administrationskonten
- Umgehende Löschung bzw. Deaktivierung von Berechtigungen, die nicht oder nicht mehr benötigt werden
- Spezielle Sicherung des Zugangs der Administratoren
- Protokollierung von System-, Applikations- und Datenzugriffen (Azure AD Audit Logs und Sharepoint Zugriffshistorie)
- Sichere Löschung bzw. Vernichtung und Entsorgung von elektronischen Datenträgern und sonstige Unterlagen mit vertraulichen Informationen, die nicht weiter benötigt werden (Standard der Entsorgung: Peter-Gutmann-Algorithmus – 35-faches Überschreiben, Physikalische Zerstörung durch Shredder)

3. Zugriffskontrolle

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Einsatz von Firewalls, SPAM-Filtern und aktuellen Virenscannern (z.B. Microsoft Advance Thread Protection) einschließlich regelmäßiger Updates
- Differenzierte Berechtigungen und restriktive, zentrale Rechtevergabe nach dienstlichen Erfordernissen (Need-To-Know-Prinzip) und zugehörige Dokumentation. Vergabe von Berechtigungen nur nach Bestätigung des zuständigen Geschäftsführers.
- Differenziertes Ordnerkonzept (z.B. alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können)
- Umgehende Löschung bzw. Deaktivierung von Berechtigungen, die nicht oder nicht mehr benötigt werden
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken

- Systemseitige Autorisierung, d.h. Prüfung, ob der Nutzer zur Durchführung einer bestimmten Aktion berechtigt ist
- Spezielle Sicherung des Zugangs der Administratoren
- Protokollierung von System-, Applikations- und Datenzugriffen (Azure AD Audit Logs und Sharepoint Zugriffshistorie)
- Überwachung durch die IT-Verantwortlichen bei externer Wartung und Fernwartung
- Vorprüfung und Kontrolle externer Anbindungen an das interne Netz durch die IT-Verantwortlichen
- Richtlinien und Verpflichtungserklärungen für den Einsatz von Telearbeit

4. Übertragungs- und Transportkontrolle

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Daten-übertragung vorgesehen ist. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Verschlüsselung:
    - E-Mails Verschlüsselungstechnik bzw. -algorithmen durch AES (256 bit), Ipsec-Verfahren
    - Verschlüsselung von Datenträgern: Bitlocker
    - Verschlüsselung von Netzwerken: Transport Layer Security, TLS 1.2 -Verschlüsselung
    - Bereitstellung über verschlüsselte Verbindungen: sftp, ftps, https
- Tunnelverbindung, VPN (Azure VPN; IKEV2 AES256)
- Zentrales Mobile Device Management (Microsoft Endpoint Manager)
- Keine Benutzung von nicht freigegebener Hard-/ Software
- Zentrale Regelung zum E-Mail Versand; keine Weiterleitung von E-Mails an private E-Mail-Accounts von Mitarbeitern
- Vorsicht beim Umgang mit Backup-Bändern
- Vorgaben an Mitarbeiter bzgl. Ausdrucken von geheimen Unterlagen (Sicherstellung, dass kein anderer Zugriff auf Ausdrucke bekommt)

5. Eingabekontrolle

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob, von wem und zu welcher Zeit personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Zugangsregelungen und Benutzerberechtigungen
- Automatische Protokollierung der Systemnutzung unter Beachtung der daten-schutzrechtlichen Grenzen und der Aspekte der Eingabekontrolle; Überwachungs- und Protokollierungsmaßnahmen werden an den Stand der Technik und die Kritikalität der zu schützenden Daten angepasst und in dem damit verbundenen wirtschaftlichen Rahmen durchgeführt
- Die Eingabekontrolle in Datenbanksystemen erfolgt im Rahmen der mit den Datenbanksystemen gelieferten Standardverfahren

6. Wiederherstellbarkeit

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um sicherzustellen, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können bzw. zur Sicherung und Wiederherstellbarkeit des Datenbestandes. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Regelmäßige Datensicherung auf Sicherungsdatenträgern, einschließlich Spiegelung auf redundantes Speichersystem
- Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern durch Auslagerung (durch Cloudanbieter sichergestellt)
- Archivierung von Daten als Teil des Dokumentenmanagement-Prozesses (Backup mit 5 Jahren Aufbewahrungszeit)
- Überwachung der Speicherressourcen
- Funktions- und Recovery-Tests, einschließlich im Hinblick auf Risiko eines Datenverlusts
- Indizierung von Daten zur leichteren Auffindbarkeit als Teil des Dokumenten-management-Prozesses

7. Verfügbarkeitskontrolle

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dazu er-greift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Gebäude, Räume und IT sind in angemessenem Umfang gegen vorsätzliches oder fahrlässiges Verhalten oder höhere Gewalt herbeigeführte Störungen geschützt, unter anderem durch folgende Maßnahmen:
  - Brandschutzeinrichtungen (Feuerlöscher nahe der PC-Arbeitsräume, Rauchverbot)
- Vorkehrungen zur Sicherung und Wiederherstellbarkeit des Datenbestandes unter anderem durch folgende Maßnahmen:
  - Regelmäßige Datensicherung auf Sicherungsdatenträger, einschließlich Spiegelung auf redundantem Speichersystem
  - Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern durch Auslagerung (durch Cloudanbieter sichergestellt)
  - Archivierung von Daten als Teil des Dokumentenmanagement-Prozesses
  - Überwachung der Speicherressourcen
  - Funktions- und Recovery-Tests, einschließlich im Hinblick auf Risiko eines Datenverlusts
  - Indizierung von Daten zur leichteren Auffindbarkeit als Teil des Dokumenten-management-Prozesses
- Einsatz von Firewalls, SPAM Filtern und aktuellen Virenscannern (z.B. Microsoft Advance Thread Protection), einschließlich regelmäßiger Updates
- Urlaubs-, Krankheits- uns sonstige Vertretungsregelungen
- Vorbeugende Sperrung sicherheitskritischer Inhalte (z.B. bestimmte Dateitypen) und nicht vertrauenswürdiger Quellen (z.B. bestimmte Internetseiten)

8. Zuverlässigkeit und Datenintegrität

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um sicherzustellen, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Regelungen zur Sicherstellung der Verfügbarkeit und der Belastbarkeit

  - Speicherung personenbezogener und für eine weitere Verarbeitung vorgesehener Daten erfolgt auf einem System, welches vor hardwarebedingten Datenverlusten schützt (z.B. RAID); bei erhöhtem Schutzbedarf ggf Speicherung in redundanten Systemen
  - Eingesetzte Speichersysteme verfügen im Regelfall in Verbindung mit entsprechenden Softwarekomponenten über eine Technologie, die es erlaubt, definierte Datenstände bestimmter Zeitpunkte wiederherzustellen
  - Sicherung der Daten (Backup-Strategie wie z.B. online/offline; on-site/off-site) erfolgt in regelmäßigen Zyklen gemäß der geschlossenen vertraglichen Vereinbarung
- Rasche Wiederherstellbarkeit
  - Notfallplanung/Sicherheitskonzept in Verbindung mit Notfall- und Wiederanlaufplänen
  - Regelmäßiger und kontinuierlicher Prüf- und Verbesserungsprozess bzgl. des Sicherheitskonzeptes

9. Auftragskontrolle

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Kriterien für die Auswahl von externen Dienstleistern und Subunternehmern, insbesondere Berücksichtigung von Sicherheitsaspekten
- Formalisierung der Zusammenarbeit mit externen Dienstleistern und Subunternehmern, einschließlich interner Feedback- und Review-Prozesse
- Detaillierte schriftliche Festlegungen zu Auftragsverhältnissen
- Datenschutzkonforme Verträge mit Dienstleistern und Subunternehmern gemäß Art. 28 Abs. 3 DSGVO und dokumentierte TOMs der Dienstleister
- Schriftliche Verpflichtung aller, für die Erbringung der Dienstleistungen eingesetzten Dienstleister und Subunternehmer auf die Wahrung der Vertraulichkeit

10. Trennbarkeit

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dazu ergreift die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Physisch und/oder logisch getrennte Speicherung, Veränderung, Löschung und Übermittlung von Daten, die unterschiedlichen Zwecken dienen (Mandantenfähigkeit) durch Cloud-Architektur sichergestellt

11. Regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen

Die GAPTEQ GmbH ergreift angemessene Maßnahmen, um sicherzustellen, dass die Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen regelmäßig überprüft, bewertet und evaluiert wird. Dazu ergreift Die GAPTEQ GmbH unter anderem folgende Maßnahmen:

- Basis für den Datenschutz sind die zentralen, internen Datenschutz-Richtlinien von GAPTEQ, welche die Grundsätze zum Datenschutz, aber auch die Prozesse hinsichtlich Rechte der betroffenen Personen, Audits, Schulungen/Onlinetrainings und Bewusstseinsbildung beschreiben
- GAPTEQ stellt Vorgabedokumente, wie Formulare, Checklisten, Handbücher und Arbeitsanweisungen zur Verfügung, die in den HR- und weiteren Business-Prozessen verwendet werden; alle Mitarbeiter sind gemäß Art. 28,29, 32 DSGVO angewiesen, personenbezogene Daten nur auf Anweisung des Verantwortlichen zu verarbeiten
- Unterweisungen/Online Trainings für Mitarbeiter zur Aktualisierung des Datenschutzbewusstseins
- Regelmäßige Überprüfung und Anpassung der technischen und organisatorischen Maßnahmen zum Datenschutz gemäß Art: 32 DSGVO
- Leitungsebene wird regelmäßig über Status von Datenschutz und Informationssicherheit sowie mögliche Risiken und Konsequenzen aufgrund fehlender Maßnahmen informiert

Anlage 3 - Genehmigte Unterauftragsverhältnisse

Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
Microsoft Ireland Operations Limited	South County Business Park, One Microsoft Place, South County Business Park, Leopardstown Dublin 18, Ireland	Hosting	Angemessenheitsbeschluss durch Data Privacy Framework