

# Auftragsverarbeitung gemäß Art. 28 DSGVO

## Vertrag

Zwischen dem/der

### Träger/Einrichtung

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

Vermeer Care GmbH  
Andreas-Gayk-Straße 15-17  
24103 Kiel

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

## I. Gegenstand und Dauer des Auftrags

### (1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Kaufvertrag auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

### (2) Dauer

Der Startzeitpunkt wurde für den \_\_\_\_\_ festgelegt.

Die Dauer dieses Auftrags 24 Monate ohne Geräte entspricht der Laufzeit der Leistungsvereinbarung.

(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.

(5) Während des gesamten **Testzeitraumes** kann der Auftraggeber vom Vertrag zurückzutreten.

## 2. Konkretisierung des Vertragsinhalts

### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten:

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Bereitstellung, Einrichtung und Support der Webanwendung und der App-Software,
- Pflege und Wartung der Web- und App-Software

### (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten/Adressdaten/Kontaktdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Gesundheitsdaten

### (3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Beschäftigte
- Sorgeberechtigte
- Kinder

## 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 setzen.

Die Verarbeitung von Daten, die diesem Vertrag unterliegen, ist in Privatwohnungen gestattet (Heim- und Telearbeit).

## 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.
- j) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32-36 DSGVO genannten Pflichten.
- k) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Als Datenschutzbeauftragter ist beim Auftragnehmer Maik Preißler, c/o Vater Solution GmbH, Boschstraße 5, 24118 Kiel, 0431 20084576 benannt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(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. Beauftragt der Auftragnehmer einen Unterauftragnehmer, muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragnehmer gemäß dieses Vertrages gelten.

Der Auftraggeber stimmt der Beauftragung der in Anlage 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.

(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 gestattet.

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.

## 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 VDS, 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, in einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. 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

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 und 4 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines oder mehrerer Verstöße gegen die DSGVO erleidet. Sind für einen solchen Schaden Auftraggeber und Auftragnehmer verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung für den Schaden entspricht.

(2) Der Auftragnehmer haftet dem Verantwortlichen gegenüber entsprechend auch für die Einhaltung datenschutzrechtlicher Vorgaben durch die Subunternehmer, die er zur Erfüllung seiner Aufgaben einsetzt. Das Verschulden von Subunternehmern ist dem Auftragnehmer wie eigenes Verschulden zuzurechnen.

(3) Der Auftragnehmer unterstützt den Auftraggeber mit Auskünften zu allen ihm zur Verfügung stehenden Informationen, wenn der Auftraggeber einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder anderen Ansprüchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist.

## 12. Gerichtsstand

(1) Gerichtsstand ist der Ort des Auftraggebers.

---

Ort, Datum, Unterschrift  
Auftraggeber

---

Ort, Datum, Unterschrift  
Vermeer Care GmbH

# Anlage 1 - Technisch-organisatorische Maßnahmen

Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers 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.

## 1. Organisatorische Maßnahmen

---

- Ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO liegt vor.
- Ein Datenschutz-Managementsystem ist vorhanden. Dieses wird regelmäßig aktualisiert und jährlich fortgeschrieben.
  - Es existiert ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen
  - Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
  - etc.
- Mitarbeiter wurden nachweislich über Datenschutzrecht und Datensicherheit geschult.
- Ein Datenschutz-Schulungskonzept liegt vor.
- Mitarbeiter sind nachweislich auf die Verschwiegenheit verpflichtet.
- Eine Datenschutz- und Datensicherheitsrichtlinie ist vorhanden.

## 2. Vertraulichkeit

---

a) *Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle*  
Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

- Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
- Alarmanlage
- Automatisches Zutrittskontrollsystem, Ausweisleser
- Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
- Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
- Sicherheitsschlösser
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem
- Werkschutz/Pförtner
- Empfang mit Anmeldung
- Sorgfältige Auswahl von Wachpersonal
- Sorgfältige Auswahl von Reinigungspersonal
- Lichtschranke/Bewegungsmelder
- Feuerfeste Türen
- Fenstervergitterung

**b) Zugangs- und Benutzerkontrolle**

*Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

- Benutzeridentifikation und Passwortverfahren implementiert
- Einsatz von VPN-Technologie
- Verschlüsselung von Smartphone-Inhalten
- Verschlüsselung von mobilen Datenträgern
- Es existiert eine zentrale Firewall
- Es erfolgt eine automatische Sperrung der Bildschirme mit Passwortschutz

**c) Zugriffskontrolle**

*Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

- Schriftliches Berechtigungskonzept vorhanden
- Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- Verwaltung der Rechte durch System-Administrator
- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Einsatz von Akten-/ Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- Verschlüsselung von Datenträgern
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Löschungskonzept für Daten
- Protokollierung der Vernichtung
- Es gibt Regeln für die Verwendung von mobilen Geräten

**d) Transport- und Übertragungskontrolle**

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

- Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- E-Mail-Verschlüsselung
- Protokollierung von Übermittlungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen  
Sicherung von Datenträgertransporten (verschießbarer Transportbehälter), auch für Papier

**e) Auftragskontrolle**

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

- Vorhandene Vereinbarungen zur Auftragsverarbeitung
- Kontrolle der Vertragsausführung
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

- Regelung zu Wartungen (speziell Fernwartung)

### 3. Integrität

---

#### a) *Eingabekontrolle/Verarbeitungskontrolle*

*Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

#### b) *Dokumentationskontrolle*

*Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.*

- Führung eines Verzeichnis der Verarbeitungstätigkeiten
- Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

### 4. Verfügbarkeitskontrolle

---

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wiederhergestellt werden können.*

- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsschutz
- Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Virenschutzsystem
- Spiegelung von Festplatten (z. B. RAID-Verfahren)
- Konzept für Katastrophenfall vorhanden

## 5. Trennungsgebot

---

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- Festlegung Technologie von Datenbankrechten
- Trennung von Daten verschiedener Auftraggeber

## 6. Wiederherstellbarkeit der Verfügbarkeit

---

*Maßnahmen, die gewährleisten, dass nach einem physischen oder technischen Zwischenfall die personenbezogenen Daten schnell wieder verfügbar sind.*

- Virtualisierung sichert schnelle Wiederherstellbarkeit der Systeme
- Aktivierte Snapshotfunktion gewährleistet zeitnahe Fallbacks
- Datensicherung mit vollständiger Recovery Funktion
- Backup2disc sichert schnelle Datenrücksicherung

## 7. Gewährleistung der Belastbarkeit der Systeme

---

*Maßnahmen, die gewährleisten, dass die Belastbarkeit der Systeme ausreichend sichergestellt ist.*

- Redundanz der Server & Backup Umgebung
- Monitoring der aktiven Systeme zeigt Belastung und Auslastung
- N+1 Redundanzen im Netzwerksegment sichert Verfügbarkeit bei Ausfall
- Redundante Datenanbindung
- Redundante Klimatisierung
- Datenspeicherung auf Storage mit RAID Systemen mindestens RAID 1
- Regelmäßige Soft- und Firmware-Updates auf IT-Systemen
- Regelmäßige Test-Rücksicherungen
- Serviceverträge mit Hard- und Softwareherstellern

## 8. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

---

- Dokumentiertes Prüfkonzept mit Datenschutzberichten
- Dokumentierte Prüfverfahren für Verarbeitungstätigkeiten
- Prozesse zur Anpassung bei negativem Prüfverlauf sind dokumentiert
- Prozesse zur Meldung neuer/veränderter Verarbeitungen sind dokumentiert

## 9. Incident-Response-Management

---

- Es existiert ein dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde).
- Es existiert eine dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen.
- Es existiert ein formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

## Anlage 2 - Genehmigte Unterauftragsverhältnisse

<b>Firma Unterauftragnehmer</b>	<b>Anschrift/Land</b>	<b>Leistung</b>	<b>Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland</b>
Vermeer Consulting GmbH	Andreas Gayk Straße 15-17 24103 Kiel	IT-Dienstleistungen	Eine Datenübermittlung in ein Drittland findet nicht statt.
Cloud Dienstleister	Germany West Central	Server in Frankfurt	Eine Datenübermittlung in ein Drittland findet nicht statt.