

## **Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO**

als Anlage zum Rahmenvertrag über den Bezug von Microsoft-Software vom **[Datum]**

- nachfolgend „Leistungsvereinbarung“ –

zwischen dem

Klinikum und Seniorenzentrum Itzehoe  
Zweckverband des Kreises Steinburg und der Stadt Itzehoe, Robert-Koch-Str. 2, 25524 Itzehoe

(nachfolgend "**Auftraggeberin**" genannt)

und dem

**Auftragnehmer**

**Straße**

**PLZ ORT**

(nachfolgend "**Auftragnehmer**" genannt)

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

### **Präambel**

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis gemäß Art. 28 Datenschutzgrundverordnung (DS-GVO) eingegangen. Um die Rechte und Pflichten aus dem Auftragsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

---

## § 1

### Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeitende des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die die Auftraggeberin gemäß Art. 4 Nr. 7 DS-GVO Verantwortliche ist

## § 2

### Gegenstand und Dauer des Auftrags

- (1) Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: (anzupassen, z.B.)
  - a) ...
  - b) ...
  - c) ...
- (2) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung oder sofern die Leistungsvereinbarung keine Dauer vorsieht zur einmaligen Ausführung.
- (3) Die Auftraggeberin kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags vorliegt, der Auftragnehmer eine Weisung der Auftraggeberin nicht ausführt oder der Auftragnehmer Kontrollrechte der Auftraggeberin vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

## § 3

### Konkretisierung des Auftragsinhalts

- (1) Art und Zweck der vorgesehenen Verarbeitung von Daten (Art. 4 Nr. 2 DS-GVO) sind in der Leistungsvereinbarung niedergelegt.

- 
- (2) Folgenden Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragnehmer (Art. 4 Nr. 1 DS-GVO): (jeweils anzupassen, z.B.)
- a) Name, Adresse
  - b) Geburtsdatum
  - c) Personalnummer
  - d) ...
- (3) Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst: **[Aufzählung oder Beschreibung der betroffenen Personenkategorien, z.B. Beschäftigte etc.]**.
- (4) 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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss, Binding Corporate Rules oder Standardvertragsklauseln) **[Anmerkung: Ggf. konkretisieren]**. Die nachträgliche Verlagerung ins EU-Ausland bedarf der vorherigen Zustimmung der Auftraggeberin.

## § 4

### Verantwortlichkeit und Weisungsbefugnis

- (1) Die Auftraggeberin ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Sie kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen. Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.
- (2) Der Auftragnehmer darf Daten ausschließlich im Rahmen der Weisungen der Auftraggeberin erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang

---

des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung der Auftraggeberin. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von der Auftraggeberin danach in der Regel schriftlich oder in einem dokumentierten elektronischen Format durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

- (3) Der Auftragnehmer hat die Auftraggeberin unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bei der Auftraggeberin bestätigt oder geändert wird.
- (4) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch die Auftraggeberin erteilen.
- (5) Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen der Auftraggeberin nicht erstellt. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggeberin berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.
- (6) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung der Auftraggeberin unmittelbar durch den Auftragnehmer sicherzustellen.
- (7) Der Auftragnehmer stellt der Auftraggeberin auf deren Wunsch Informationen zur Aufnahme in das von ihr zu führende Verzeichnis zur Verfügung.
- (8) Soweit die Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Mitarbeitenden des Auftragnehmers) verarbeitet werden, sind auch in diesem Fall die Maßnahmen nach Art. 32 DS-GVO sicherzustellen.

---

## § 5

### **Beachtung zwingender gesetzlicher Pflichten durch den Auftragnehmer**

- (1) Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragnehmer die nachfolgenden gesetzlichen Pflichten.
- (2) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten der Auftraggeberin befassten Mitarbeitenden die Vertraulichkeit der Daten gemäß Art 28 Abs. 3, 29, 32 DSGVO wahren und diese entsprechend auf das Datengeheimnis verpflichtet und in die für sie relevanten Bestimmungen zum Datenschutz eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.
- (3) Sofern der Auftragnehmer verpflichtet ist nach den anwendbaren Vorschriften einen Datenschutzbeauftragten zu bestellen, wird er die Kontaktdaten des Datenschutzbeauftragten der Auftraggeberin zum Zwecke der direkten Kontaktaufnahme mitteilen.
- (4) Der Auftragnehmer informiert die Auftraggeberin unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde wegen Verletzungen gegen datenschutzrechtliche Bestimmungen bei dem Auftragnehmer ermittelt.

## § 6

### **Technisch-organisatorische Maßnahmen und deren Kontrolle**

- (1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Er ist Gegenstand dieser Vereinbarung.
- (2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
- (3) Der Auftragnehmer wird der Auftraggeberin auf Anforderung die zur Wahrung ihrer Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung der Auftraggeberin vor

---

Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich die Auftraggeberin von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer der Auftraggeberin auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

- (4) Die Auftraggeberin kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen.

## **§ 7**

### **Mitteilung bei Verstößen durch den Auftragnehmer**

- (1) Der Auftragnehmer unterstützt die Auftraggeberin bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen.
- (2) Zu den Pflichten, bei denen der Auftragnehmer die Auftraggeberin unterstützt gehören u.a.
- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
  - b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an die Auftraggeberin zu melden;

- 
- c) die Verpflichtung, die Auftraggeberin im Rahmen ihrer Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
  - d) die Unterstützung der Auftraggeberin für deren Datenschutz-Folgenabschätzung sowie
  - e) die Unterstützung der Auftraggeberin im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

## **§ 8**

### **Löschung und Rückgabe von Daten**

- (1) Überlassene Datenträger und Datensätze verbleiben im Eigentum der Auftraggeberin. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten der Auftraggeberin beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändungen oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer die Auftraggeberin unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist ausgeschlossen.
- (2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch die Auftraggeberin, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung der Auftraggeberin datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist der Auftraggeberin auf Anforderung vorzulegen.
- (3) Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende der Auftraggeberin übergeben.

---

## § 9

### **Subunternehmer**

- (1) Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit vorheriger ausdrücklicher schriftlicher Genehmigung der Auftraggeberin vergeben werden. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen der Auftraggeberin und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden und die Verantwortlichkeiten klar abgrenzt sind. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).
- (3) Der Auftraggeberin sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist die Auftraggeberin berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.
- (4) Der Auftragnehmer haftet gegenüber der Auftraggeberin dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.



---

## § 10

### Nebenleistungen

Die §§ 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

## § 11

### Datenschutzkontrolle

Der Auftragnehmer verpflichtet sich, dem/ der behördlichen Datenschutzbeauftragten der Auftraggeberin zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

## § 12

### Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (2) Der Anhang „Technisch-organisatorische Maßnahmen“ ist Bestandteil dieser Vereinbarung.

---

Datum, Ort

---

Unterschrift (Auftraggeberin)

---

Name, Vorname, Funktion

---

Datum, Ort

---

Unterschrift (Auftragnehmer)

---

Name, Vorname, Funktion

---

## Anhang „Technisch-organisatorische Maßnahmen“

zur Vereinbarung zur Auftragsverarbeitung vom **[Datum]** zwischen

### Auftraggeberin und Auftragnehmer

§ 6 der Vereinbarung zur Auftragsvereinbarung verweist zur Konkretisierung der technisch-organisatorischen Datenschutzmaßnahmen auf diesen Anhang.

#### § 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind im Rahmen der Auftragsverarbeitung gesetzlich verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

#### § 2 Innerbetriebliche Organisation des Auftragnehmers

Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

#### § 3 Konkretisierung der Einzelmaßnahmen

Im Einzelnen werden folgende Maßnahmen bestimmt (Art. 32 DS-GVO):

Nr.	Maßnahme	Umsetzung der Maßnahme
Vertraulichkeit der Daten		
1.	Zutrittskontrolle  Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	<b>[Ergänzen, z.B. Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Schlüsselvergabe, Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Türsicherung]</b>

2.	<p>Zugangskontrolle</p> <p>Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.</p>	<p>[Ergänzen, z.B. Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: Kennwortverfahren, Automatische Sperrung, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern)]</p>
3.	<p>Zugriffskontrolle</p> <p>Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsbeziehung 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.</p>	<p>[Ergänzen, z.B. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren] (Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung)</p>
4.	<p>Trennungskontrolle</p> <p>Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.</p>	<p>[Ergänzen, z.B. Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten, Mandantenfähigkeit, Funktionstrennung zwischen Produktion/ Test]</p>
5.	<p>Pseudonymisierung</p> <p>Es ist zu gewährleisten, dass die Verarbeitung personenbezogener</p>	<p>[Ergänzen, ob und in welchem Umfang die Pseudonymisierung als Mittel der Vertraulichkeit eingesetzt wird]</p>

	Daten in einer Weise erfolgt, die das Risiko minimieren. Hierzu gehört die Pseudonymisierung von Daten.	
Integrität der Daten		
6.	<p>Weitergabekontrolle</p> <p>Es ist 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 Datenübertragung vorgesehen ist.</p>	<p>[Ergänzung, z.B. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur]</p>
7.	<p>Eingabekontrolle</p> <p>Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.</p>	<p>[Ergänzen, z.B. Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Protokollauswertungssysteme]</p>
Verfügbarkeit und Belastbarkeit		
8.	<p>Verfügbarkeitskontrolle</p> <p>Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige</p>	<p>[Ergänzen, z.B. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung](Beispiel: Backup-</p>

	Zerstörung oder Verlust geschützt sind.	Verfahren, Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung, Firewall, Notfallplan)
9.	<p>Rasche Wiederherstellbarkeit</p> <p>Es ist zu gewährleisten, dass die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt wird.</p>	[Ergänzen welche Maßnahmen zur raschen Wiederherstellbarkeit getroffen wurden. U.A. Hochverfügbare Backups, etc.]
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung		
10.	<p>Auftragskontrolle</p> <p>Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeberin verarbeitet werden können.</p>	[Ergänzen]Abgrenzung der Kompetenz zwischen Auftraggeberin und Auftragnehmer (Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Auftragnehmers, Kontrolle der Vertragsausführung)
11.	<p>Datenschutz-Management</p> <p>Es ist zu gewährleisten, dass durch ein Datenschutz-Management die Überprüfung gewährleistet ist.</p>	[Ergänzen welche Maßnahmen im Bereich des Datenschutzmanagements getroffen wurden]
12.	Incident-Response-Management.	[Ergänzen, welche Maßnahmen getroffen wurden, um bei Datenschutzverletzungen die Auftraggeberin und ggf. die Aufsichtsbehörden zu informieren. (Data Breach Notification)]

---

Datum, Ort

---

Unterschrift (Auftraggeberin)

---

Name, Vorname, Funktion

---

Datum, Ort

---

Unterschrift (Auftragnehmer)

---

Name, Vorname, Funktion