Datenschutzvereinbarung
Wartung und Pflege von IT-Systemen

zwischen

Firma Kund:in, Name Kund:in, Anschrift Kund:in, PLZ/Ort Kund:in

- Auftraggeber:in -

und

Steve Rückwardt, TAS LEX-Partner.Net, An der Heerstraße 14, 06217 Merseburg

- Auftragnehmer –

Präambel

Zwischen den Parteien besteht ein Vertragsverhältnis über die Wartung und Pflege von IT-Systemen.

Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Bestimmungen des Art. 28 der Datenschutz-Grundverordnung (DSGVO) zwischen den Parteien getroffen.

1. Allgemeines

(1) Der Auftragnehmer führt im Auftrag der Auftraggeber:in Wartungs- und/oder Pflegearbeiten an IT-Systemen der Auftraggeber:in durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können.

2. Dauer und Beendigung des Auftrags

(1) Der Auftragnehmer führt für die Auftraggeber:in Leistungen (Wartung und/oder Pflege von IT-Systemen) durch. Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis („Hauptvertrag“), das entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (zum Beispiel BGB) basiert. Diese Vereinbarung beginnt ab Unterzeichnung durch beide Parteien und gilt für die Dauer des jeweiligen Hauptvertrages.

(2) Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

3. Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst auch folgende Arbeiten und/oder Leistungen:

- Anlegen von Benutzer:innen auf Server- oder Applikationsebene
- Einrichtung/Einräumung, Änderung und/oder Löschung von Benutzer:innenberechtigungen
- Eingabe, Änderung oder Löschung von Datenbankfeldern
- Fernwartung von IT-Systemen

Der Auftrag kann auch die Verarbeitung folgender Arten von personenbezogenen Daten beinhalten:

- Name und Kontaktdaten von Nutzer:innen der IT-Systeme
- ggf. weitere Daten von Betroffenen, die im jeweiligen IT-System der Auftraggeber:in gespeichert sind

Kreis der von der Datenverarbeitung Betroffenen:

- Beschäftigte der Auftraggeber:in
- Kund:innen der Auftraggeber:in
- Dritte

4. Rechte und Pflichten der Auftraggeber:in

(1) Der Auftragnehmer wird personenbezogene Daten für die Auftraggeber:in ausschließlich nach den vertraglichen Vereinbarungen und/oder den Weisungen der Auftraggeber:in verarbeiten. Die Auftraggeber:in hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Wartung und Pflege von IT-Systemen gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (zum Beispiel E-Mail) erfolgen. Mündlich erteilte Weisungen werden umgehend von Auftraggeber:in in Textform bestätigt.

(2) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen der Auftraggeber:in beim Auftragnehmer entstehen, bleiben unberührt.

(3) Die Auftraggeber:in informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch den Auftragnehmer feststellt.

(4) Der Auftragnehmer wird die Auftraggeber:in informieren, sofern er durch europäisches oder deutsches Recht verpflichtet ist, personenbezogene Daten im Rahmen dieses Auftrags zu verarbeiten. Der Auftragnehmer wird der Auftraggeber:in diese rechtlichen Anforderungen vor der Verarbeitung mitteilen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Zusammenhang mit den Wartungs-/Pflegearbeiten im Auftrag verarbeitet, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(2) Der Auftragnehmer wird die Auftraggeber:in unverzüglich darüber informieren, wenn eine von Auftraggeber:in erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch die Auftraggeber:in bestätigt oder geändert wird.

(3) Der Auftragnehmer ist verpflichtet, der Auftraggeber:in jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen der Auftraggeber:in unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(4) Dem Auftragnehmer ist bekannt, dass für die Auftraggeber:in eine Meldepflicht nach Art. 33, 34 DSGVO im Falle einer Datenschutzverletzung bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird der Auftraggeber:in bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird der Auftraggeber:in insbesondere und unverzüglich über unbefugte Zugriffe auf personenbezogene Daten, die im Auftrag der Auftraggeber:in verarbeitet werden, informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

(5) Der Auftragnehmer wird seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen.

(6) Der Auftragnehmer unterstützt die Auftraggeber:in bei der Einhaltung der in Art. 33-36 DSGVO genannten Pflichten, soweit die Auftraggeber:in insoweit auf die Unterstützung des Auftragnehmers angewiesen ist.

6. Kontrollbefugnisse

(1) Dier Auftraggeber:in hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen der Auftraggeber:in durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist der Auftraggeber:in gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle im Sinne des Absatzes 1 erforderlich ist.

(3) Die Auftraggeber:in kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Die Auftraggeber:in wird dabei Sorge dafür tragen,

dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden könnten.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber der Auftraggeber:in im Sinne des Art. 58 DSGVO in Verbindung mit § 40 BDSG, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an die Auftraggeber:in zu erteilen.

7. Fernwartung

(1) Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, der Auftraggeber:in eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann zum Beispiel durch Einsatz einer Technologie erfolgen, die der Auftraggeber:in ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(2) Für den Fall, dass die Auftraggeber:in einer Berufsgeheimnispflicht im Sinne des § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung im Sinne des § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

(3) Wenn die Auftraggeber:in bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

8. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmer:innen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung der Auftraggeber:in zulässig.

(2) Der Auftragnehmer hat die Unterauftragnehmer:in sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese/r die zwischen Auftraggeber:in und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass die Unterauftragnehmer:in die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber:in zu übermitteln. Der Auftragnehmer ist verpflichtet, sich von Unterauftragnehmer:in bestätigen zu lassen, dass diese/r eine/n betrieblichen Datenschutzbeauftragte/n benannt hat, sofern dies nach Art. 37 DSGVO in Verbindung mit § 38 BDSG erforderlich ist.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen der Auftraggeber:in auch gegenüber den Unterauftragnehmer:in gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(4) Die Verpflichtung der Unterauftragnehmer:in muss den Anforderungen von Art. 28 Abs. 4 DSGVO entsprechen.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 6 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

9. Vertraulichkeit

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie der Auftraggeber:in obliegen. Dies gilt insbesondere in den Fällen, in denen die Auftraggeber:in zur Einhaltung der Schweigepflicht aus § 203 StGB verpflichtet ist. Die Auftraggeber:in ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter:innen mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese zur Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet hat, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

10. Wahrung von Betroffenenrechten

(1) Die Auftraggeber:in ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Der Auftragnehmer unterstützt die Auftraggeber:in mit geeigneten technischen und organisatorischen Maßnahmen dabei, der Pflicht der Auftraggeber:in zur Beantwortung von Anfragen von Betroffenen nach den Art. 12-23 DSGVO nachzukommen, soweit der Auftraggeber:in insoweit auf die Unterstützung des Auftragnehmers angewiesen ist.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber der Auftraggeber:in zur Einhaltung der nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen.

(2) Für den Fall, dass der Auftragnehmer die Wartung und Pflege von IT-Systemen für die Auftraggeber:in auch außerhalb der Geschäftsräume der Auftraggeber:in durchführt (zum Beispiel im Falle der Fernwartung), sind vom Auftragnehmer zwingend die in der **ANLAGE** zu diesem Vertrag genannten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten einzuhalten.

12. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die

im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeber:in auszuhändigen bzw. zu löschen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

(2) Die Auftraggeber:in hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle muss mit angemessener Frist durch die Auftraggeber:in angekündigt werden.

13. Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____,	_____	Merseburg,	_____
Ort	Datum	Ort	Datum

_____	_____
- Auftraggeber -	- Auftragnehmer –

Unterzeichnung erfolgt digital mit qualifizierter Signatur – Versand erfolgt nach Anfrage

Anlage:
Technische und organisatorische
Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

1. Vertraulichkeit (Artikel 32 Abs. 1 lit. b DSGVO)

„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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; […]“

- **Zutrittskontrolle**

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Sicherheitsschlösser und -schlüssel
- Manuelles Schließsystem
- Schlüsselregelung (Schlüsselausgabe etc.)
- Videoüberwachung der Zugänge
- Bewegungsmelder
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal

- **Zugangskontrolle**

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

- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Zuordnung von Benutzerrechten
- Einsatz von zentraler Smartphone-Administrations-Software
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Anti-Viren-Software
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern

- Verschlüsselung von Smartphone-Inhalten
- Verschlüsselung von Datenträgern in Laptops / Notebooks

- **Zugriffskontrolle**

Maßnahmen, die 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.

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern
- Protokollierung der Vernichtung

- **Trennungskontrolle**

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

- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

- **Pseudonymisierung**

- Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Pseudonymes Arbeiten in Datenbanken

2. Integrität (Artikel 32 Abs. 1 lit. b DSGVO)

„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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko

angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; […]"

- **Weitergabekontrolle**

Maßnahmen, die 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.

- Verschlüsselte Verbindungen
- E-Mail-Verschlüsselung (Transportverschlüsselung)
- Beim physischen Transport: sichere Transportbehälter/-verpackungen

- **Eingabekontrolle**

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

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

3. Verfügbarkeit und Belastbarkeit (Artikel 32 Abs. 1 lit. b DSGVO)

„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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; […]"

- **Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Schutzsteckdosenleisten
- Feuer- und Rauchmeldeanlagen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Abs. 1 lit. d DSGVO; Artikel 25 Abs. 1 DSGVO)

„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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […] d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung; […]“

- **Auftragskontrolle**

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

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer
- Sicherstellung der Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertragsstrafen bei Verstößen