Inhaltsverzeichnis

Inhalt

1 Dokumenteninformationen 2
1.1 Auftraggeber 2
1.2 Dienstleister 2
2 Einführung 2
2.1 Risikoklassifizierung 3
2.2 Gegenstand der Dienstleistung 3
3 Technische und organisatorische Maßnahmen 4
3.1 Allgemeine Fragen 4
3.2 Vertraulichkeit (Geheimhaltung) 5
3.2.1 Zutrittskontrolle 5
3.2.2 Zugangskontrolle 5
3.2.3 Zugriffskontrolle 6
3.2.4 Trennungskontrolle 7
3.2.5 Pseudonymisierung 7
3.2.6 Verschlüsselung 8
3.3 Integrität (Korrektheit und Unverfälschbarkeit) 8
3.3.1 Eingabekontrolle 8
3.3.2 Weitergabekontrolle 9
3.4 Verfügbarkeit, Belastbarkeit und schnelle Wiederherstellbarkeit 10
3.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 11
3.5.1 Datenschutzfreundliche Technikgestaltung (Art. 25 Abs. 1) 11
3.5.2 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2) 11
3.5.3 Auftragskontrolle 12
3.5.4 Datenschutz-Managementsystem 13
4 Schlusserklärung 14

1 Dokumenteninformationen

1.1 Auftraggeber

AUFTRAGGEBER	
Name auftraggebende Gesellschaft:	
Ansprechpartner Auftraggeber:	
eMail-Adresse Auftraggeber:	
Telefon-Nr. Auftraggeber:	
Betroffene Verfahren aus Verfahrensverzeichnis:	

Es handelt sich bei dieser Prüfung um eine

☒ Erstkontrolle
☐ Folgekontrolle
Letzte Kontrolle war am: _____

Das Auftragsverhältnis darf erst nach Prüfung des vollständig ausgefüllten Dokumentes und Freigabe begonnen werden.

Es wird empfohlen, dass Dokument während der gesamten Dauer des Verfahrens aufzubewahren.

1.2 Dienstleister

DIENSTLEISTER bzw. AUFTRAGNEHMER	
Name Auftragnehmer:	
Ansprechpartner Auftragnehmer:	
Funktion des Ansprechpartners:	
eMail-Adresse Auftragnehmer:	
Telefon-Nr. Auftragnehmer:	
Ausfülldatum:	

2 Einführung

Das vorliegende Dokument ist im Rahmen des Datenschutzmanagementsystems ein Teil der Datenschutzdokumentation des Auftraggebers. Die europäische Datenschutzgrundverordnung (DSGVO) schreibt im Artikel (Art.) 28 vor, dass ein Auftragsverarbeiter sowohl vor der Verarbeitung von personenbezogenen Daten als auch anschließend regelmäßig zu kontrollieren ist. Eine Prüfung vor Ort beim Dienstleister und ein fester zeitlicher Abstand ist nicht geregelt. Allerdings hat die verantwortliche Stelle eine risikoorientierte Prüfungsplanung umzusetzen. Verantwortlicher für die

Planung, Durchführung und Dokumentation der Prüfung ist die Stelle, die die wesentlichen Entscheidungen über Art, Umfang, Zweck und Mittel der Datenverarbeitung trifft.

Der zukünftige Dienstleister hat vor Vertragsunterzeichnung die vom Auftrag betroffenen und konkreten TOMs auszufüllen.

2.1 Risikoklassifizierung

Es sind gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen zu treffen, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Es wird folgende **Risikoklassifizierung** vorgenommen:

	Gering: Es werden keine besonderen personenbezogenen Daten gemäß Artikel 9 DSGVO[1] verarbeitet. ➢ Keine zusätzliche Vor-Ort-Prüfung erforderlich ➢ Wiederholungsprüfung nach spätestens 5 Jahren
✓	**Mittel:** Es werden besondere personenbezogenen Daten gemäß Artikel 9 DSGVO[1] verarbeitet, aber nicht als wesentlicher Teil des Kerngeschäfts oder in der beauftragten Dienstleistung. ➢ Vor-Ort-Prüfung nur in Ausnahmefällen erforderlich ➢ Wiederholungsprüfung nach spätestens 3 Jahren
	Hoch: Es werden besondere personenbezogenen Daten gemäß Artikel 9 DSGVO[1] im Kerngeschäft oder in der beauftragten Dienstleistung verarbeitet. In diese Risikoklassifizierung fallen auch Bankdaten und Daten von Berufsgeheimnisträgern. ➢ Eine Vor-Ort-Prüfung ist grundsätzlich erforderlich ➢ Wiederholungsprüfung nach spätestens 2 Jahren ➢ Vermutlich Datenschutzfolgenabschätzung erforderlich, bei der der Auftragsverarbeiter den Auftraggeber unterstützt.

[1] Besondere personenbezogene Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben oder genetische bzw. biometrische Daten.

Die Risikoklassifizierung kann ggf. durch weitere externe Aspekte, wie z.B. mögliche Reputationsrisiken bzw. öffentliche Diskussionen über den Dienstleister, beeinflusst werden.

Bei der Risikoklassifizierung wurde von folgenden zu schützenden **Personengruppen (Betroffene)** vom Auftraggeber ausgegangen:

☐ Interessenten bzw. Kunden als natürliche Personen
☒ Interessenten bzw. Kunden als juristische Personen
☐ Beschäftigte, Bewerber
☐ Kinder, die jünger als 16 Jahre sind
☐ Patienten
☐ Mieter
☐ _____

2.2 Gegenstand der Dienstleistung

☐ Es findet eine Software-Entwicklung für den Auftraggeber statt.
☐ Es ist ein Fernzugriff bzw. eine Fernwartung möglich.
☐ Es wird eine EDV-Anwendung betrieben.
Wenn ja, welche Programme bzw. Module/Funktionen? _____
☐ Es werden Geschäfts- oder Administrationsprozesse durchgeführt.
☐ Lettershop
☐ Mailingaktion
☐

☒**Beschreibung der Dienstleistung bzw. Datenflüsse:**
(Bitte alle Datenflüsse im Rahmen des Auftrages inkl. zu externen Partnern bzw. Schnittstellen beschreiben. Hierbei bitte auch die Schutzmaßnahmen, wie z.B. Verschlüsselung und Authentifizierung, skizzieren.)

3 Technische und organisatorische Maßnahmen

Wichtig: Die nachfolgenden Fragen bzw. Maßnahmen beziehen Sie auf die Systeme, Anwendungen, Räumlichkeiten bzw. Prozesse, die für die Verarbeitung der Aufraggeber-Daten benutzt werden.

3.1 Allgemeine Fragen

(j = ja, n = nein, nr = nicht relevant)

Allgemeine Fragen zum Auftragsverarbeiter	j	n	nr	Bemerkung
Erfolgt Datenverarbeitung/-Speicherung im internen Rechenzentrum?				
Erfolgt Datenverarbeitung/-Speicherung im externen Rechenzentrum? Bitte Gesellschaft und Land nennen.				
Erfolgt Datenverarbeitung/-Speicherung in den Geschäftsräumen?				
Erfolgt Datenverarbeitung/-Speicherung auf mobilen Endgeräten? (Notebook, Laptop, Tablet, Smartphone usw.)				
Erfolgt Datenverarbeitung/-Speicherung an Heimarbeitsplätzen?				
Erfolgt Datenverarbeitung/-Speicherung ggf. an anderen Orten?				
Gibt es eine Zertifizierung z.B. nach ISO2700x, BSI-Grundschutz, PCI-DSS, ISO 27018 (Cloud Services)?				

Gibt es eine Ausrichtung z.B. nach ISO2700x, BSI-Grundschutz, PCI-DSS, ISO 27018 (Cloud Services)?				
Erfolgte eine Prüfung bzgl. Datenschutz/Informationssicherheit durch einen Externen (Wirtschaftsprüfer, Unternehmensberatung, Revision usw.)?				

3.2 Vertraulichkeit (Geheimhaltung)

3.2.1 Zutrittskontrolle

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

(j = ja, n = nein, nr = nicht relevant)

Zutrittskontrolle	j	n	nr	Bemerkung
Wer ist für die Zutrittskontrolle verantwortlich?				
Liegen Zertifikate oder Prüfberichte bzgl. der physischen Sicherheit der betroffenen Räume vor? (z.B. VDS 2333)				
Abgestufte Sicherheitsbereiche				
Gebäude außerhalb Bürozeiten abgeschlossen				
Verschlossene Büros				
PCs, Notebooks in gesicherten Räumen				
Gesicherte Fenster				
Alarmanlage				
Manuelles Schließsystem der Türen				
Sicherheitsschlösser				
Berechtigungsausweise (z.B. Chipkarten, Transpondersystem)				
Biometrische Zutrittssperre				
Klingelanlage mit Kamera				
Videoüberwachung der Eingänge				
Absicherung evtl. Gebäudeschächte				
Eigener Serverraum oder Technikraum verschlossen				
Eigener Serverraum/Technikraum gegen Zutritt gesichert				
Schlüsselregelung / Liste				
Empfang, Rezeption, Pförtner				
Besucherbuch mit Protokollierung				
Mitarbeiter- / Besucher-Ausweise				
Richtlinie zur Begleitung von Besuchern				
Wachpersonal sorgfältig ausgewählt				
Reinigungsdienst sorgfältig ausgewählt				
Datenträger unter Verschluss				

Ergänzende Beschreibung bzgl. der **Zutrittskontrolle**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.2.2 Zugangskontrolle

Maßnahmen, die verhindern das Datenverarbeitungs-Systeme (Hardware, Betriebssystem, Software-Anwendung) von Unbefugten genutzt werden können.

(j = ja, n = nein, nr = nicht relevant)

Zugangskontrolle	j	n	nr	Bemerkung
Personifizierte Nutzer im Netzwerk				
Personifizierte Nutzer in zentraler Kunden-Software				
Login mit Benutzername + Passwort				
Techn. Passwort-Prüfung 3 aus 4 (Groß-/Kleinschreibung, Buchstaben, Zahlen, Sonderzeichen)				
Inhaltliche Prüfung der Passwort-Komplexität				
Anti-Viren-Software Server				
Anti-Viren-Software Clients				
Firewall				
Intrusion Detection-System (Angriffserkennungssystem)				
VPN bei Remote-Zugriffen				
BIOS-Passwort				
Sperrung externer Schnittstellen (USB)				
Automatische Desktopsperre				
Dokumentation der Zugangsberechtigungen				
Erfolgt ein Fernzugriff?				
Fernzugriff via VPN				
Fernzugriff: Authentifizierung via Hardware-/Software-Token				
Fernzugriff: Authentifizierung on Demand (auf Anforderung)				
Fernzugriff wird protokolliert				
WLAN für Netzwerkzugang im Einsatz				
Allgemeine Datenschutz-/Datensicherheit Richtlinie				
Passwort-Richtlinie vorhanden				
Vorgabe manuelle Desktopsperre				
Vorgabe beim Verlassen des Arbeitsplatzes keine vertraulichen Informationen, Papiere, Wechselmedien liegen zu lassen.				
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern				
Prozess zur Rechtevergabe bei Abteilungswechsel von Mitarbeitern				
Prozess zur Rechtevergabe bei Austritt von Mitarbeitern				
Minimale Anzahl Netzwerk-Administratoren				

Ergänzende Beschreibung bzgl. der **Zugangskontrolle**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.2.3 Zugriffskontrolle

Maßnahmen die verhindern, dass unerlaubte Tätigkeiten innerhalb von IT-Systemen durchgeführt werden. Es handelt sich z.B. um Lesen, Kopieren, Verändern, und Entfernen von Daten außerhalb eingeräumter Berechtigungen.

(j = ja, n = nein, nr = nicht relevant)

Zugriffskontrolle	j	n	nr	Bemerkung
Trennung von Berechtigungsbewilligung und Berechtigungsvergabe				
Aktenshredder Partikelschnitt				
Externe Aktenvernichtung				
Physische Datenträgerlöschung				
Protokollierung von Zugriffen (Eingaben, Änderung, Löschung von Daten)				
Bestehen differenzierte Berechtigungen für Daten, Anwendungen bzw. (z.B. für lesen, ändern)				
Berechtigungskonzept (need-to-know-Prinzip)				
Konzept zur Laufwerksnutzung				
Minimale Anzahl Administratoren für die Anwendung				
Regelmäßige Überprüfung von Berechtigungen der Benutzer und Administratoren				
Auswertung von Logfiles bzw. Protokollen				

Ergänzende Beschreibung bzgl. der **Zugriffskontrolle**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.2.4 Trennungskontrolle

Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobenen Daten auch getrennt verarbeitet werden.

(j = ja, n = nein, nr = nicht relevant)

Trennungskontrolle	j	n	nr	Bemerkung
Physische Trennung der Systeme, Datenbanken. (Eigenes System oder eigene Datenbank je Auftraggeber)				
Physische Trennung Datenträger				
Mandantenfähigkeit innerhalb der Anwendungen				
Getrennte Datensicherung je Auftraggeber				
Berechtigungskonzept ermöglicht getrennte DV der Mandanten/Kunden				
Trennung von Produktiv- und Testumgebung				
Werden Testdaten aus Originaldaten gewonnen und anonymisiert?				
Trennung durch unterschiedliche Mitarbeiter				

Ergänzende Beschreibung bzgl. der **Trennungskontrolle**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.2.5 Pseudonymisierung

Maßnahmen, damit Personen nur mit zusätzlichen Informationen identifiziert werden können. Unterstützt den Grundsatz der **Datenminimierung** und privacy bei default, senkt die Risiken.

(j = ja, n = nein, nr = nicht relevant)

Pseudonymisierung	j	n	nr	Bemerkung
Frühestmögliche Pseudonymisierung im Verarbeitungsprozess				
Pseudonymisierung durch Löschung bestimmter Daten				
Pseudonymisierung durch Aggregierung der Daten				
Pseudonym-Zuordnung durch Betroffenen (z.B. frei gewählte Nutzer-ID)				
Pseudonym-Zuordnung durch den Auftraggeber				
Pseudonym-Zuordnung durch Auftragnehmer				
Pseudonym-Zuordnung durch Dritten (z.B. Zertifizierungsstelle, Treuhänder)				
Trennung der Zuordnungsdaten und getrennte Aufbewahrung				
Interne Anweisung vor Datenweitergabe Daten zu pseudonymisieren/anonymisieren				

Ergänzende Beschreibung bzgl. der **Pseudonymisierung**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.2.6 Verschlüsselung

Maßnahmen zum Schutz von Daten gegen unbefugte Kenntnisnahme oder absichtliche Manipulation

(j = ja, n = nein, nr = nicht relevant)

Verschlüsselung	j	n	nr	Bemerkung
Verschlüsselung von Notebooks, PCs				
Datenträgerverschlüsselung (z.B. USB-Stick)				
Smartphone-Verschlüsselung				
Verschlüsselung sonstiger Speichermedien (z.B. Kamera)				
Verschlüsselung der Kunden-Datenbanken				
Verschlüsselung von Mail-Inhalten				
Verschlüsselung von Mail-Anhängen				
Verschlüsselter Internet-Auftritt				

Arbeitsanweisung zur manuellen Verschlüsselung				

Ergänzende Beschreibung bzgl. der **Verschlüsselung**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.3 Integrität (Korrektheit und Unverfälschbarkeit)

3.3.1 Eingabekontrolle

Maßnahmen, um die Dateneingabe, -Veränderung und Entfernung nachzuweisen.

(j = ja, n = nein, nr = nicht relevant)

Eingabekontrolle	j	n	nr	Bemerkung
Werden Daten des Auftraggebers erfasst oder geändert?				
Klare Zuständigkeiten für Datenlöschung				
Vertragliche Beschränkung auf bestimmte Mitarbeiter				
Differenzierte Benutzerberechtigungen (Lesen, ändern, löschen)				
Technische Protokollierung wer und wann in den Anwendungen Daten erfasst bzw. verändert hat?				
Technische Protokollierung der Administratorentätigkeit				
Automatisierte Kontrolle der Protokolle				
Manuelle Kontrolle der Protokolle				
Archivierung von Anforderungen zur Passwortrücksetzung				
Archivierung von Anforderungen zur Berechtigungsvergabe				
Qualifizierte elektronische Signatur (entspricht grundsätzlich einer handgeschriebenen Unterschrift) möglich				
Übersicht, welche Programme Datenänderungen durchführen können				
Aufbewahrung von Papierformularen, von denen Daten in IT-Systemen übernommen werden				

Ergänzende Beschreibung bzgl. der **Eingabekontrolle**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.3.2 Weitergabekontrolle

Maßnahmen, um die elektronischen Übertragungen und den Datentransport zu sichern.

(j = ja, n = nein, nr = nicht relevant)

Weitergabekontrolle	j	n	nr	Bemerkung
Sind zwischen Auftraggeber und Auftragnehmer Übertragungswege schriftlich vereinbart?				
Verschlüsselter Datenträgertransport				
Mail-Transportverschlüsselung (z.B. TLS)				
Mail-Inhaltverschlüsselung (z.B. PGP)				
Mail-Anhangverschlüsselung (z.B. ZIP)				
Verschlüsselte VPN-Verbindung				
Standleitung				
Arbeitsanweisung zum Verschlüsseln				
Dokumentation der Datenempfänger mit Dauer der Überlassung bzw. der Löschfristen				
Sorgfältige Auswahl von Transportpersonal				
Gesicherter Eingang für An- und Ab-Lieferungen von mobilen Datenträgern				
Werden Datenträger, die vom Auftraggeber stammen bzw. für diesen genutzt werden, besonders gekennzeichnet?				
Vollständigkeitsprüfung bzw. Richtigkeitsprüfung				
Persönliche Übergabe mit Protokoll				
Verbot des Einsatzes privater Speichermedien				
Regelung zur Vernichtung von Speichermedien und Daten				
Vernichtungsregelung den Mitarbeitern bekannt				
Entsorgungscontainer vorhanden				
Werden Löschprotokolle geführt?				

Ergänzende Beschreibung bzgl. der **Weitergabekontrolle**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.4 Verfügbarkeit, Belastbarkeit und schnelle Wiederherstellbarkeit

Maßnahmen, um die Daten gegen Verlust und Zerstörung zu schützen.

(j = ja, n = nein, nr = nicht relevant)

Verfügbarkeit	j	n	nr	Bemerkung
Vertragliche Regelungen für die Aufbewahrungsdauer von Daten vorhanden?				
Durchführung von Datensicherungen				
Gewährleistung der techn. Lesbarkeit der Backup-Medien für Zukunft				
Feuer- und Rauchmeldeanalage				
CO2-Feuerlöscher Serverraum bzw. Technikraum				
Serverraum klimatisiert				
Unterbrechungsfreie Stromversorgung (USV)				
Einsatz von Schutzprogrammen (Virenscanner, Firewall, Spamfilter u.a.) mit regelmäßiger Aktualisierung				
Intrusion Detection- bzw. - Prevention System				

Ausweich-Rechenzentrum				
Datenspiegelung				
Backup- /Recoverykonzept				
Server-Raum im getrennten Brandabschnitt				
Daten-Wiederherstellung wird regelmäßig getestet				
Aufbewahrung der Datensicherungen außerhalb des Serverraums				
Keine sanitären Anschlüsse im Serverraum				
Schwachstellenanalyse durchgeführt (Wasser, Feuer, Gelände, Gebäude, Rechnernetz)				
Notfallplan bzw. Notfallverfahren mit regelmäßigem Praxistest				
Penetrationstest bei webbasierten Anwendungen				

Ergänzende Beschreibung bzgl. der **Verfügbarkeit**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

3.5.1 Datenschutzfreundliche Technikgestaltung (Art. 25 Abs. 1)

Maßnahmen, die sicherstellen, dass ein Produkt, Dienst, System bzw. EDV-Anwendung zum frühestmöglichen Zeitpunkt datenschutzkonform entwickelt wird. Die wesentlichen Maßnahmen ergeben sich aus Art. 5 DSGVO.

(j = ja, n = nein, nr = nicht relevant)

Datenschutzfreundliche Technikgestaltung	j	n	nr	Bemerkung
Rechtmäßigkeit: Technische Schnittstellen werden nur freigegeben, wenn datenschutzrechtlich zulässig				
Transparenz: Alle Funktionen und Verarbeitungen sind bekannt				
Datenminimierung durch Pseudonymisierung				
Datenminimierung durch Anonymisierung				
Richtigkeit: Daten können berichtigt bzw. gelöscht werden				
Speicherbegrenzung: Löschkonzept ist technisch implementiert				
Alle Daten können durch eine automatisierte Löschroutine gelöscht werden				
Datenübertragbarkeit (Art. 20): Können alle Daten einer einzelnen betroffenen Person zur Verfügung gestellt werden?				
Findet eine automatisierte Einzelfallentscheidung statt, die eine rechtliche Wirkung für den Betroffenen hat?				

Ergänzende Beschreibung bzgl. der **datenschutzfreundlichen Technikgestaltung**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.5.2 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2)

Maßnahmen, die sicherstellen, dass ein Produkt, Dienst, System bzw. EDV-Anwendung für den Nutzer ohne weitere Aktivitäten beim ersten Einschalten bzw. Aufruf datenschutzfreundliche Einstellungen bzw. Komponenten aufweist.

(j = ja, n = nein, nr = nicht relevant)

Datenschutzfreundliche Voreinstellung	j	n	nr	Bemerkung
Es werden nicht mehr Daten verarbeitet als für den Zweck erforderlich ist.				
Daten werden nur so lange gespeichert wie für Zweck erforderlich.				
Erstellung eines Persönlichkeitsprofils				
Keine Zugriffsmöglichkeit durch Dritte				
Transparente und nachvollziehbare Verarbeitung				

Ergänzende Beschreibung bzgl. der **datenschutzfreundlichen Voreinstellung**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

3.5.3 Auftragskontrolle

Maßnahmen, die sicherstellen, dass Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

(j = ja, n = nein, nr = nicht relevant)

Auftragskontrolle	j	n	nr	Bemerkung
Eindeutige Vertragsgestaltung gem. Art. 28 DSGVO				
Hat der Auftraggeber umfassende vertragliche Weisungsrechte?				
Ist geregelt wer Weisungen beim Dienstleister entgegen nehmen darf?				
Kontrollrechte des Auftraggebers vorhanden				
Vor Ort-Kontrolle des Auftraggebers vorhanden				
Sorgfältige Auswahl von Sub-Dienstleistern				
Datenverarbeitung ausschließlich in einem Land des europäischen Wirtschaftsraumes				
Wird für die Dienstleistung eine Cloud-Lösung eingesetzt?				
Befinden sich die Server des Cloud-Anbieters innerhalb des europäischen Wirtschaftsraums?				

Werden die Daten in der Cloud verschlüsselt übertragen und/oder in der Cloud gespeichert?				
Werden die Anforderungen des Auftraggebers bei der Cloud-Lösung eingehalten?				
Sicherstellung der ordnungsgemäßen Datenvernichtung bzw. Daten-Rückgabe nach Auftragsabschluss?				

Ergänzende Beschreibung bzgl. der **Auftragskontrolle**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

Liste der für die konkrete Beauftragung erforderlichen Sub-Dienstleister:

Name und Anschrift des Sub-Dienstleisters	Land	Gegenstand der Dienstleistung	Welche datenschutzrechtliche Vereinbarung (z.B. Auftrags-verarbeitung, EU-Standard-klauseln, Privacy Shield)?

3.5.4 Datenschutz-Managementsystem

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der technischen und organisatorischen Maßnahmen.

(j = ja, n = nein, nr = nicht relevant)

Datenschutz-Managementsystem	j	n	nr	Bemerkung
Ist dokumentiert, wie der Schutz der Betroffenen gewährleistet wird? (z.B: Berichtigung, Löschung, Sperrung, Auskunft der Daten)				
Zentrale Dokumentation der Verarbeitungstätigkeiten vorhanden				
Verzeichnis von Verarbeitungstätigkeiten wird mind. jährlich geprüft bzw. aktualisiert				
Datenschutzfolgenabschätzung nach Art. 35 werden durchgeführt				
Durchführung von Penetrationstests				
Sicherheitskonzept vorhanden				
Incident-/Ticket-System				
Notfallübungen werden durchgeführt und Optimierungsmaßnahmen ergriffen				
Hat jeder Mitarbeiter Arbeitsanweisung/Richtlinie bzgl. Datenschutz und Informationssicherheit erhalten?				

Schriftlich benannter Datenschutzbeauftragter nach Art. 38 und 39 vorhanden				
Datenschutzverantwortung ist festgelegt				
Mitarbeiter auf Datengeheimnis verpflichtet				
Mitarbeiter werden regelmäßig geschult/sensibilisiert				
Jährliche Überprüfung der technischen und organisatorischen Maßnahmen (TOMs)				
Dokumentierte Vorgehensweise für evtl. Datenschutzverletzungen, Sicherheitsvorfälle, Störungen, Ausfälle				
Einbindung eines Datenschutzbeauftragten und Security-Spezialisten				

Ergänzende Beschreibung bzgl. des **Datenschutz-Managementsystems**. Vor allem bei o.a. Punkten, die mit nein oder nicht relevant beantwortet wurden.

4 Schlusserklärung

Als verantwortliche Person vom Dienstleister bzgl. der TOMs bestätige ich die Richtigkeit aller vorstehenden Angaben.

Ort _____ Datum _____

Name des Unterzeichners in Blockbuchstaben _____

Unterschrift _____