

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO
ggf. Ergänzung zu bestehenden Wartungs- & Pflegevertrag / IT nach Maß/
Fernwartungsvertrag

zwischen

im Folgenden Auftraggeber bzw. „Name des Kunden“ genannt, und

Pro-fekt e.K. | Dr.-Knauer-Str. 6 | 96242 Sonnefeld

im Folgenden Auftragnehmer / Auftragsverarbeiter oder Pro-fekt genannt.

Verantwortlich nach Art. 24 DSGVO Art. 37 DSGVO= Frau Yvonne Engelhardt YvEn@Pro-fekt.de

[Stand: Mai 2017]

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der erteilten Auftragserteilung dem bestehenden Pflege- Wartungsvertrag und der Fernwartungsvereinbarung sowie aus etwaigen Einzelweisungen auf die hier verwiesen wird.

(2) Dauer

Die Dauer dieses Auftrags Lieferdaten(Laufzeit) entspricht der Laufzeit des Hauptvertrags. Eine Kündigung kann nur schriftlich erfolgen.

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 sind konkret beschrieben unter 1 genannten Auftrages, dem bestehenden Pflege- Wartungsvertrag und der Fernwartungsvereinbarung

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

- unregelmäßigen, regelmäßigen Inanspruchnahme von Dienstleistungen zur Hard- und Soft-Ware des Auftraggebers, sowie der Unterstützung durch den Auftragnehmer zur Sicherstellung der Betriebsfähigkeit der EDV-Anlage auch mittels Fernwartung
- Betriebswirtschaftliche Organisation: Bedarfs- Anforderungsanalysen, hochwertige Beratungsleistungen und IT-Dienstleistungen Optimierung von Betriebs- Produktionsabläufen
- GSD Software: Projektplanung: Einführung, Umsetzung, Erweiterungen Sicherheitskonzepte: Planung, Erprobung Durchführung und die Überprüfung, Backuplösung inkl. Notfallplan Individual Programmierung: C, C++, .NET, Java, PHP, Webprogrammierung
- Office: Visual Basic – Makro, Linux/Unix: Shell Script Programmierung Datenbanken: Konzept, Planung, Umsetzung, Erweiterung, ERM, Modellierung

- Mediengestaltung: CI, Imageberatung, Logoerstellung, Satz, Layout, SEO Optimierung
- Systemadministration: Server Wartung / Betreuung – Windows, Linux, Unix, Virtualisierung, System Überwachung, Hardware Reparaturen, Firewall / Tunnel, Netzwerk Betreuung, Datenbank Wartung und Sicherung, Cloud
- Mediengestaltung: Bildmodifikation, Druckdaten, Webdesign, Daten aus digitaler Vorlage einpflegen
- GSD Software: Formulare, Serien-Dokumente, Vorlagensystem
- 1st Level Support – Hilfestellung zur einfachen Problembehebung: Bedienhilfe zu Software und Hardware

Der Auftragnehmer erhebt, verarbeitet und nutzt personenbezogene Daten. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 – 50 EU-DSGVO erfüllt sind.

(2) Art der Daten

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

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Passwort, Zugangsdaten
- Lieferdaten
- Supportdaten
- Zeiterfassungsdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Hersteller
- Handelsvertreter
- Ansprechpartner
- Verbraucher

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers 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 Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Frau Yvonne Engelhardt YvEn@Pro-fekt.de benannt.

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 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.

Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag 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.

Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

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.

Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

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 z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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 sowie Kontrollmaßnahmen zu ergreifen.

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

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

WORTMANN nAG
Bredenhop 20
32609 Hüllhorst

Webhosting Franken
Inh.: Holger Häring
Bonalinostasse 1
96110 Scheßlitz / Bayern

domainfactory GmbH
Oskar-Messter-Str. 33
85737 Ismaning
Deutschland

ESET Deutschland GmbH
Spitzweidenweg 32
07743 Jena

GSD Gesellschaft für Software, Entwicklung und Datentechnik mbH
Ludwigsstädter Straße 95+97
96342 Stockheim-Neukenroth

Liste der zugelassenen Subunternehmer GSD

GSD Software Polska Sp. z o.o.
Wydawnicza 1/3
92-333 Łódź

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen

Magellan Netzwerke GmbH
Max-Reichpietsch-Straße 2
51147 Köln

Actian Germany GmbH
Halenreihe 42
22359 Hamburg Germany

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399, USA

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(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.

(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.

7. 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 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 solcher Maßnahmen, die nicht nur den konkreten 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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber 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. Hierzu gehören u.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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(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 einem seiner benannten Ansprechpartner bestätigt oder geändert wird.

Liste der Ansprechpartner

Gemäß der AVDD benennt der Auftraggeber Ansprechpartner und wird diesbezügliche Änderungen dem Vertragspartner unverzüglich schriftlich mitteilen.

Abteilung / Funktion	Name	Telefon	E-Mail

Erklärung: Die oben genannten Ansprechpartner sind die aktuell einzigen des Auftraggebers. Ältere Ansprechpartner-Listen verlieren hiermit Ihre Gültigkeit.

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 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.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort, Datum

Name, Funktion

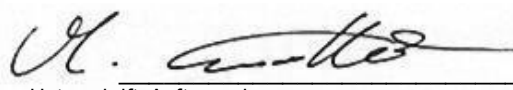
Unterschrift, Auftraggeber

Burgkunstadt 23.05.2018

Ort, Datum

Marco Engelhardt Geschäftsleitung

Name, Funktion



Unterschrift, Auftragnehmer

1 Zutrittskontrolle

Maßnahmen:

- Zutritt zu Datenverarbeitungsanlagen durch Türsicherung
- Schlüsselvergabe an berechtigte Mitarbeiter wird protokolliert
- Gebäude Zu- und Ausgänge durch Videoüberwachung (außerhalb der Betriebszeiten) gesichert
- Fremdpersonal, u. a. Lieferanten und IT-Service wird durch Pro-fekt Mitarbeiter beaufsichtigt
- Biometrische Zugangssperren (Fingerabdruck auf Laptop)
- Chipkarten- / Transponder-Schließsystem
- Manuelles Schließsystem
- Videoüberwachung der Zugänge

2 Zugangskontrolle

Maßnahmen:

- Userkennung durch sicheres Passwort (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des
- Kennworts gemäß Arbeitsrichtlinie
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Firewall
- Protokollierung von Benutzern und Rechten (Sicherheitsrichtlinie über Domäne)
- Regelung zur E-Mail- und Internetnutzung gemäß Arbeitsrichtlinie
- Gehäuseverriegelungen bei Servern
- Authentifikation mit biometrischen Verfahren (z. B. Fingerabdruck)
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Hardware Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren-Software

3 Zugriffskontrolle

Maßnahmen:

- Berechtigungsprofil, nach DOCUframe-Gruppen differenziert nach Lese- und Schreibberechtigung dokumentiert
- sowie Vertretungsregelung (Group-Policies + DOCUframe Gruppenzugehörigkeit)
- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Physische, nicht wiederherstellbare Löschung von Datenträgern vor Wiederverwendung = kein Einsatz gemäß
- Einsatz von Aktenvernichtern
- Verwaltung der Rechte durch Systemadministrator
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern

4 Weitergabekontrolle

Maßnahmen:

- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- Bei Datenträgertransporten, Verschlüsselung der Daten durch Passwort
- Übergabeprotokoll bzw. Ein-Ausgangsprotokoll für Datenträger
- Schutz der Schnittstellen von PCs, USB-Sticks gemäß Arbeitsrichtlinie
- Löschung, Vernichtung von Datenträger gem. Arbeitsrichtlinie
- Bei Fernwartung entsprechend der Fernwartungsvereinbarung, den Kundenvorgaben und Home-Office-Betrieb wird der Zugriff auf Kundendaten via VPN gesichert
- Beim physischen Transport: sichere Transportbehälter / -verpackungen

5 Eingabekontrolle

Maßnahmen:

- Protokoll der Einwahlvorgänge in Kundensysteme
- Die Eingabe der Daten wird datenfeldbezogen, datensatzbezogen und dateibezogen protokolliert
- Protokollierung der Eingabe, Änderung und Löschung von Daten im DOCUframe
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6 Auftragskontrolle

Maßnahmen:

- Eindeutige Vertragsgestaltung zur Durchführung des Kundenauftrages
- Formalisierte Auftragserteilung (Auftragsformular)
- Kontrolle der Auftragsausführung mit DOCUframe Projekt
- Auswahl des Subunternehmers unter Sorgfalts Gesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Frau Yvonne Engelhardt benannt
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrages (Löschkonzept)

7 Verfügbarkeitskontrolle

Maßnahmen:

- Backup-Verfahren gemäß Pro-fekt Sicherheitsrichtlinie
- Spiegeln von Festplatten, z.B. RAID-Verfahren, regelmäßige Sicherungskopien, getrennte Aufbewahrung
- Virenschutz / Firewall
- Notfallplan
- Sicherung des Serverraumes durch unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung von Datensicherung an einem sicheren ausgelagerten Ort
- Schutzsteckdosen in Serverräumen
- Serverräume nicht unter sanitären Anlagen

8 Trennungskontrolle

Maßnahmen:

- "Interne Mandantenfähigkeit" auf Anwendungsebene
- Funktionstrennung zwischen Produktions- & Testsystem
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Festlegung von Datenbankrechten (Berechtigungskonzept)