JULIAN AKICH
RECHTSANWALT

Arbeitspapier zur

Prüfung der TOMs

der PM Digital Solutions GmbH

Erstellt: 07.07.2020

Bearbeiter: JA	JULIAN AKICH RECHTSANWALT	**Gegenstand:** TOMs
Datum: 06.07.20		**Einstufung:** vertraulich

I. Auftrag

Die Mandantschaft ist eine neu gegründete GmbH mit Sitz in Karlsruhe. Gegenstand der Unternehmung ist das Digitalisieren von Handakten im Kundenauftrag. Die Mandantschaft tritt gegenüber ihren Kunden als Auftragsdatenverarbeiter auf. Der Unterzeichner ist der neu bestellte Datenschutzbeauftragte – nachfolgend DSB genannt – des Unternehmens. Im Rahmen eines Sonderauftrages ist er damit befasst, ein dem Risiko entsprechendes Datenschutzkonzept zu erstellen, der Geschäftsführung bei der Implementierung des Datenschutzkonzeptes zu helfen und die TOMs zu prüfen.

Nachfolgend werden die technischen und organisatorischen Maßnahmen der Unternehmung bewertet.

II. Bewertung

Die PM Digital Solutions GmbH ist ein neu gegründetes Unternehmen. Zum Zeitpunkt der Prüfung sind keine Mitarbeiter angestellt. Lediglich die beiden Geschäftsführer kommen mit den Kundendaten in Berührung. Die Geschäftsführer haben sich frühzeitig mit dem Thema Datenschutz beschäftigt. Beide gaben Auskunft über die vorhandenen und zukünftig noch zu implementierenden Maßnahmen.
Nach Ansicht des Unterzeichners sind die getroffenen technischen und organisatorischen Maßnahmen mit Blick auf das Risiko angemessen und sachgerecht. Die Prüfung der TOMs bliebt mit Blick auf das derzeit vorhandene Risiko ohne Beanstandung.

Es wird auf das Prüfungsprotokoll – **Anlage 1** – verwiesen.

Gez.

Dipl. iur. Julian Akich, LL.B.
Rechtsanwalt

Formular zur Prüfung der technischen und organisatorischen Maßnahmen

§ 1 Allgemeine Informationen

a) Geltungsbereich

Dieses Dokument ist Teil der Datenschutzdokumentation des Datenschutzmanagementsystems der PM Digital Solutions GmbH. Aufgrund der Vereinfachung der Darstellung wird im Folgenden für alle Rollen-, Stellen-, und Funktionsbezeichnungen die männliche Form, stellvertretend für die weibliche und männliche Schreibweise, verwendet.

Dieses Dokument gilt für die informationsverarbeitenden Systeme und Netzwerke, Dokumente und Informationen der gesamten Firma, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt (gespeichert) werden.

Diese Version des Dokumentes ersetzt alle früheren Versionen und Ausgaben. Sollten vertragliche oder gesetzliche Festlegungen dieses Dokument oder Teile hiervon berühren, haben diese in jedem Fall Vorrang. Die Aktualisierung und Weiterentwicklung dieses Dokumentes obliegt dem Datenschutzbeauftragten der [Firma]. Der Ausdruck dieses Dokumentes mit dem Vermerk „Original" stellt eine gelenkte Kopie dar und unterliegt dem Änderungsdienst.

Die nachfolgende Liste dient nur der erläuternden Darstellung gesetzlicher Anforderungen in Bezug auf den Datenschutz. Die Rechte und Pflichten der Parteien ergeben sich allein aus den vertraglichen Vereinbarungen und den gesetzlichen Bestimmungen zum Datenschutz. Insofern können aus dieser Liste keine Ansprüche abgeleitet werden. Technische Änderungen und/oder Änderungen in der Organisation, die keinen Einfluss auf die Erfüllung der gesetzlichen Anforderungen der DS-GVO in der jeweils aktuellen Fassung haben, bedürfen keiner gesonderten Information gegenüber dem Vertragspartner. Die angegebenen Punkte können je nach Vertrag/Leistungsschein variieren. Die Weitergabe an Dritte ist untersagt. Nur gültig für Vertragskunden.

b) Beschreibung des Aufbaus der Prüfliste

Die Fragen der Prüfliste sind mit folgenden Punkten überschrieben:

Nr.	laufende Nummerierung der jeweiligen Prüfabschnitte
Frage	datenschutzrelevante Fragestellung
Antwort	Beantwortung auf Basis aktueller Prozesse und Verfahren im Unternehmen Ankreuzantworten nach Stand der Technik
Anmerkung	Kommentar- oder Anmerkungsfeld für erklärende Hinweise zur Art der Umsetzung oder Notizen für den Datenschutzbeauftragten

c) Prüfung

Vor-/Nachname:	Rechtsanwalt Dipl. iur. Julian Akich, LL.B. Karlstraße 3-5 76133 Karlsruhe
Rolle:	Externer DSB
Prüfungsobjekt:	PM Digital Solutions GmbH

§ 2 Zutrittskontrolle

Nr.	*Frage*	*Antwort*
2.1	Wer ist für die Zutrittskontrolle beim Auftragsverarbeiter verantwortlich?	Geschäftsführer.
Zu 2.1.	**Die PM Digitial Solutions GmbH ist eine Unternehmung mit weniger als 5 Mitarbeiter. Verantwortlich für die Zutrittskontrolle sind die beiden Geschäftsführer Dominik Moritz und Daniel Paulus.**	
2.2	Wer legt die zu sichernden Objekte und Bereiche beim Auftragnehmer fest?	Geschäftsführer.
2.3	Werden die Zutrittsrechte dokumentiert?	Nein.
Zu 2.3.	**Es handelt sich um ein kleines Unternehmen mit weniger als 5 Mitarbeiter. Schon aufgrund der kleinen Organisation muss jeder Mitarbeiter zu jedem Bereich Zutritt haben. Die Dokumentation der Zutrittsrechte ist deshalb derzeit obsolet, wird aber erstellt, sobald es der Organisationsrahmen erforderlich macht.**	
2.4	Gibt es ein dokumentiertes Verfahren für die Vergabe/Entzug von Zutrittsrechten?	Nein.
Zu 2.4.	**Es wird auf die Einlassung zu 2.3. verwiesen.**	
2.5	Werden Anwesenheitsaufzeichnungen im Sicherheitsbereich geführt?	Ja.
2.6	Welche Personen, die nicht beim Auftragnehmer angestellt sind, verfügen über Zutrittsberechtigungen?	Vermieter hat einen Schlüssel, aber darf nicht unbegleitet zutreten.
2.7	Durch welche weiteren organisatorische/technische Maßnahmen wird die Zutrittskontrolle unterstützt?	Zutritt nur mit Sicherheitsschlüssel möglich.
2.8	Sind die Eingangstüren und Nebentüren gesichert, so dass ein Schutz vor unbemerktem Betreten/Verlassen der Gebäude besteht?	Ja.
2.9	Werden Externe in den Gebäuden beaufsichtigt?	Ja.
2.10	Werden Besucher zum Besuchten begleitet bzw. von ihm abgeholt?	Ja.
2.11	Werden Besucher erfasst?	Ja. Anhand einer Besucherliste.

Nr.	*Frage*	*Antwort*
2.12	Werden Fenster und nach außen gehende Türen verschlossen, wenn die Räume, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, nicht besetzt sind?	Ja.
2.13	Sind einstiegsgefährdete Fenster und Türen in Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, gegen Einbruch abgesichert?	Es wird ein Alarmsystem bis zum 01.08.2020 installiert.
2.14	Welche Personen dürfen die Serverräume und/oder das Rechenzentrum betreten?	Geschäftsführer und IT Techniker und Systemadministrator in Begleitung eines Geschäftsführers.
2.15	Sind die Serverräume bzw. das Rechenzentrum vor dem Zutritt unberechtigter Personen – insbesondere auch außerhalb der Geschäftszeiten – geschützt?	Serverräume: Ja. Rechenzentrum: Ja.
2.16	Durch welche Maßnahmen wird der Zutritt zu DV-, TK-Systemen für Unbefugte verwehrt?	Schlüsselregelung
2.17	Welche störenden Einflüsse existieren beim Auftragnehmer in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet?	Keine.
2.18	Werden schädigende Umgebungseinflüsse in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, bei der Installation und der Benutzung von IT-Komponenten beachtet?	Ja.

§ 3 Zugangskontrolle

Nr.	*Frage*	*Antwort*
3.1	Welche Maßnahmen schützen IT-Systeme vor unbefugter Nutzung?	Passwortvergabe, Protokollierung der Passwortnutzung.
3.2	Existieren für Mitarbeiter(innen) des Auftragnehmers, die Daten des Auftraggebers verarbeiten und/oder speichern bzw. Systeme betreuen, Hinweise über den Umgang mit administrativen Passwörtern?	Ja. Dokument: Version/Datum:
3.3	Verfügt jeder Berechtigte über ein eigenes, nur ihm bekanntes Passwort?	Ja.

Nr.	*Frage*	*Antwort*	
3.4	Gibt es Gruppenpasswörter, die von mehreren Nutzern eingesetzt werden?	Nein.	
3.5	In welchen Bereichen und zu welchem Zweck werden Gruppenpasswörter eingesetzt?	Bereich	Zweck
3.6	Wird dokumentiert, wann welcher Mitarbeiter das Gruppenpasswort benutzt hat?	Siehe 3.4.	
3.7	Gibt es eine Passwortrichtlinie, die die Struktur eines Passwortes, sowie die Änderungsintervalle und Nutzung beschreibt?	Ja. Dokument: Version/Datum:	
3.8	Sind Mitarbeiter des Auftragnehmers, die Daten des Auftraggebers verarbeiten/speichern aufgefordert komplexe Passwörter einzusetzen?	Ja.	
3.9	Wann werden Passwörter für IT-Systeme/Nutzer gewechselt?	Ca. alle 6 Monate.	
Zu 3.9.	**Ein Automatismus oder systemseitiges Ändern der Passwörter gibt es nicht. Die Mitarbeiter sind im Rahmen ihrer arbeitsrechtlichen Pflicht angehalten, ihr Passwort eigenverantwortlich alle 6 Monate zu ändern und damit die Vorgaben der Passwortrichtlinie zu beachten.**		
3.10	Welche Mindestlänge haben diese Passwörter?	Gemäß Passwortrichtlinie.	
3.11	Werden Passwörter für IT-Systeme/Nutzer nur verschlüsselt abgespeichert oder übertragen?	k.A.	
3.12	Gibt es für IT-Systeme/Nutzer eine Passwort-Historie, um zu vermeiden, dass alte Passwörter weiterverwendet werden?	Ja.	
3.13	Werden Administrationspasswörter für IT-Systeme gesichert aufbewahrt?	Ja.	
3.14	Werden Schlüssel für Kryptographie-Verfahren gesichert aufbewahrt?	Ja.	
3.15	Wie oft kann sich ein Benutzer an IT-Systemen vergeblich anmelden, bis der Zugriff automatisch gesperrt wird?	10 mal.	
3.16	Wie erfolgt im Falle der Sperrung eines Administrationszugangs die Entsperrung vorgenommen?	Undokumentiertes Verfahren.	
Zu 3.16	**In diesem Fall nimmt der Mitarbeiter Kontakt zu Systemadmin auf. Aufgrund der Größe des Unternehmens kann der Systemadmin den Kontaktierenden entsprechend identifizieren.**		

Nr.	*Frage*	*Antwort*
3.17	Sind die Passwörter der Mitarbeiter(innen) für IT-Systeme auch dem Administrator und/oder dem Management bekannt?	Nein.
3.18	Werden über alle Aktivitäten auf DV-Anlagen automatisch Protokolle erstellt?	Ja.
3.19	Von wem werden diese Protokolle hinsichtlich etwaiger Unregelmäßigkeiten ausgewertet und in welchen zeitlichen Abständen erfolgt dies?	Die Auswertung erfolgt manuell ohne festes Intervall.
3.20	Wie werden IT-Systeme gegen unbefugte Nutzung abgesichert?	Funktionelle Zuordnung einzelner Datenendgeräte, Protokollierung der Systemnutzung und Protokollauswertung.
3.21	Werden mobile PCs, die Daten des Auftraggebers verarbeiten bzw. speichern außerhalb der Bürozeiten unter Verschluss gehalten?	Ja.
3.22	Werden Räume, in denen IT-Systeme aufgestellt sind mit einem Zugangskontrollsystem ausgestattet?	Ja.
3.23	Wie findet die Identifizierung an IT-Systemen statt?	Benutzername und Kennwort.
3.24	Wie findet die Authentifizierung bei IT-Systemen statt?	Benutzername und Kennwort.
3.25	Wer genehmigt die Zugangsberechtigungen bei IT-Systemen?	Geschäftsführer.
3.26	Werden die Zugangsberechtigungen dokumentiert?	Ja.
3.27	Von wem werden die Einstellungen im BIOS-Setup vorgenommen?	IT-Administrator.
3.28	Ist der unbefugte Zugang zum BIOS-Setup möglich?	Nein.
3.29	Wird bei Arbeitsunterbrechungen ein passwortgeschützter Bildschirmschoner aktiviert?	Ja.
3.30	Sind die Daten auf mobilen IT-Systemen verschlüsselt?	Nein.

§ 4 Zugriffskontrolle

Nr.	*Frage*	*Antwort*
4.1	Wie werden Datenträger vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen geschützt?	es gibt einen Verantwortlichen für Datenträgerverwaltung, Bestandskontrolle, Verschlüsselung, kontrollierte Vernichtung
4.2	Wo werden Datenträger außerhalb der Arbeitszeiten aufbewahrt?	verschließbare Schränke

Nr.	*Frage*	*Antwort*
4.3	Wie wird die Datenträgerverwaltung durchgeführt?	
Zu 4.3	**Datenträger mit personenbezogenen Daten sind grundsätzlich nur im Ausnahmefall anzulegen:** **1. Eigene Daten des Auftragnehmers, bspw. Kunden und Rechnungsdaten. Archivierung zur Sicherstellung der steuerrechtlichen Pflichten,** **2. Daten des Auftragsgebers, allerdings zeitlich nur bis zum Upload oder zur Übergabe des physischen Speichermediums.** **Die Datenträgerverwaltung, welche sich auf sehr wenige Datenträger beschränkt, wird von den Geschäftsführern durchgeführt.**	
4.4	Wird durch eine Zugriffskontrolle sichergestellt, dass Mitarbeiter(innen) nur auf Programme und Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen („Need-to-know-Prinzip")?	Ja.
4.5	Durch welche Maßnahmen wird die Einschränkung der Zugriffsmöglichkeit der zur Benutzung eines IT-Systems Berechtigten auf ausschließlich die seiner Zugriffsberechtigung unterliegenden Daten gewährleistet?	Automatische Prüfung der Zugriffsberechtigung, Protokollierung der Zugriffsberechtigung, Protokollierung der Systemnutzung und Protokollauswertung.
4.6	Wie ist die differenzierte Zugriffsberechtigung aufgeteilt?	Dateien.
4.7	Wie sind die differenzierten Verarbeitungsmöglichkeiten aufgeteilt?	Lesen, Ändern, Löschen.
4.8	Sind die Daten auf mobilen IT-Systemen verschlüsselt?	Kein mobilen IT Systeme vorhanden.
4.9	Können Nutzer nur auf getestete und freigegebene Anwendungssoftware zugreifen?	Ja.
4.10	Auf wessen Veranlassung werden Zugriffsrechte für IT-Systeme vergeben?	Geschäftsleitung.
4.11	Wer genehmigt die Zugriffsberechtigungen auf Daten und Applikationen?	Geschäftsleitung.
4.12	Wer vergibt die Zugriffsberechtigungen im System?	IT-Administrator.
4.13	Werden Zugriffsrechte dokumentiert?	Ja.
4.14	Wie oft werden Zugriffsrechte überprüft?	Alle 12 Monate.
4.15	Sind die Wechseldatenträgerlaufwerke (z. B. DVD, USB-Sticks, ext. Festplatten) gegen unbefugte Benutzung gesichert?	Ja.

Nr.	*Frage*	*Antwort*
4.16	Gibt es ein Änderungsmanagement (Changemanagement)?	Nein.
Zu 4.16	**Aufgrund der marginalen Größe des Unternehmens ist ein Changemanagement derzeit obsolet.**	
4.17	Wer darf die genehmigte Konfigurationsänderung vornehmen?	IT-Administrator nur auf Geheiß der Geschäftsleitung.
4.18	Gibt es Sicherungsmaßnahmen gegen unbefugtes Kopieren von Daten auf lokale Rechner?	Ja.

§ 5 Weitergabekontrolle/Übermittlungskontrolle

Nr.	*Frage*	*Antwort*
5.1	Wird der Versand von Datenträgern durch Registrierung, Begleitzettel und/oder Lieferscheine kontrolliert?	Ja.
5.2	Besteht ein Verbot der Mitnahme von Behältnissen in Räume mit DV-Anlagen oder in Datenträgerarchive und ist das Mitbringen privater Datenträger untersagt?	Mitnahme: Ja. Mitbringen: Ja.
5.3	Werden stichprobenartige Kontrollen der Mitarbeiter (Taschenkontrolle o. ä.) durchgeführt?	Nein.
5.4	Wo befinden sich unbenutzte Datenträger?	Verschlossenes Behältnis.
5.5	Wie werden Datenträger vernichtet?	Zertifizierter Entsorger.
5.6	Wie werden Datenträger transportiert?	Ohne besonderer Maßnahme.
5.7	Wie werden Daten auf dem Übertragungsweg und beim Transport gegen das unbefugte Lesen, Kopieren, Verändern oder Entfernen geschützt?	Persönliche Übergabe oder Postversand, jedenfalls Datenverschlüsselung
5.8	Werden Empfangsbestätigungen, Lieferschein o. ä. verwendet?	Ja.
5.9	Werden zum Transport vorgesehene Daten mit sensitivem Inhalt (Art. 32 DS-GVO) verschlüsselt?	Ja.
5.10	Wird das Internet zur Weitergabe personenbezogener Daten genutzt?	Nein.
5.11	Welche Dienste werden dabei genutzt?	□ E-Mail □ WWW □ FTP □ elektronischer Geldverkehr

Nr.	*Frage*	*Antwort*
		□ Sonstige: _____
5.12	Welche Sicherungsmechanismen werden bei den unter 5.11 genannten Diensten eingesetzt?	□ alle Protokolle via VPN/IPsec gesichert □ E-Mail mit SMIME oder PGP □ WWW mit https oder SSL/TLS □ SFTP □ elektronischer Geldverkehr nach PCI DSS über ZDA (PKI) □ Sonstige: _____
5.13	Welche Sicherheitsmaßnahmen existieren?	Firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS)
5.14	Durch welche Maßnahmen kann überprüft und festgestellt werden, an welche Stellen Datenübermittlung durch Einrichtung zur Datenübertragung vorgesehen ist?	Dokumentation der vorgesehenen Abruf- und Übermittlungswege.
5.15	Sind IT-Systeme in einem verschlossenen Raum?	Ja.
5.16	Sind die Server-Konsolen gesperrt?	Ja.
5.17	Gibt es ein Berechtigungskonzept, in dem Netzwerkfreigaben und Zugriffsberechtigungen auf Ordner und Dateien für einzelne Benutzergruppen festgelegt sind?	Ja.
5.18	Wird das o. g. Konzept regelmäßig geprüft und aktualisiert?	Soweit erforderlich.
5.19	Werden bei Versetzung eines Mitarbeiters nicht mehr benötigte Zugangsberechtigungen entzogen?	Ja.
5.20	Werden bei Ausscheiden eines Mitarbeiters Zugänge zu IT-Systemen gesperrt?	Ja.
5.21	Welche Maßnahmen werden realisiert, wenn Rechner oder Datenträger von externen Dienstleistern mitgenommen werden müssen?	Ist nicht vorgesehen.
5.22	Werden externe Dienstleister schriftlich auf den Datenschutz verpflichtet?	Ja.
5.23	Wie werden geschäfts-/personenbezogene Daten bei Wartungs-/Reparaturarbeiten vor dem Zugriff durch externe Dienstleister geschützt?	Ja.
5.24	Werden externe Dienstleister bei ihren Aktivitäten beaufsichtigt?	Ja.

Nr.	*Frage*	*Antwort*
5.25	Werden Passwörter gewechselt, falls sie einem externen Dienstleister bekannt geworden sind?	Ja.
5.26	Werden die Möglichkeiten zur Fernwartung nur fallbezogen freigegeben?	Ja.
5.27	Wer genehmigt die Fernwartung	Geschäftsleitung.
5.28	Gibt es eine vertragliche Grundlage, die die Fernwartung regelt?	Nein.
Zu 5.28	**Aufgrund der Größe des Unternehmens nicht angezeigt.**	
5.29	Wer baut die Fernwartungsverbindung zwischen IT-Systemen und dem externen Dienstleister auf?	Netzwerkadministrator führt aus
5.30	Gibt es einen Freigabeprozess?	Ja, Freigabe ausschließlich von der Geschäftsleitung.
5.31	Gibt es bei der Fernwartung Schutzfunktionen gegen den Zugriff eines externen Dienstleisters auf Daten/Informationen der verantwortlichen Stelle?	Nein.

§ 6 Eingabekontrolle/Plausibilitätskontrolle

Nr.	*Frage*	*Antwort*
6.1	Durch welche Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind?	Protokollierung eingegebener Daten, Verarbeitungskontrolle (Transaktionskontrolle) der Anwendung
6.2	Gibt es einen Schadsoftwareschutz?	Ja.
6.3	In welchen Intervallen wird die Integrität der Partitionstabelle, des Bootsektors, des Hauptverzeichnisses und aller Programmdateien mit einem Prüfsummenprogramm und/oder einem Schadsoftwareschutz geprüft?	Bei jedem Rechnerstart.
6.4	Wie und wann erfolgt ein Update des Schadsoftwareschutzes?	Automatisch.
6.5	Werden sicherheitsrelevante Updates und Patches für Betriebssysteme und Anwendungsprogramme regelmäßig und zeitnah eingespielt?	Ja.
6.6	Werden Daten und Programme in unterschiedlichen Verzeichnissen abgespeichert?	Ja.

Nr.	*Frage*	*Antwort*
6.7	Werden Daten und Programme in unterschiedlichen Partitionen abgespeichert?	k.A.
6.8	Gibt es eine vollständige und aktuelle Netzwerkdokumentation?	Nein.
6.9	Wird die Integrität und Installation von erhaltenen Programmen überprüft?	Ja.
6.10	Werden erhaltene oder auszuliefernde Datenträger einem Schadsoftwarecheck unterzogen?	Nein.
6.11	Erfolgt bei Wiederverwendung bereits beschriebener Datenträger eine ausreichend starke Löschung der vorherigen Daten?	Ja.
6.12	Werden die durchgeführten Wartungs-, Fernwartungs- oder Reparaturarbeiten dokumentiert?	Ja.
6.13	Wird die Integrität von Datenträgern von externen Dienstleistern überprüft, bevor diese eingesetzt werden?	Keine externen Dienstleister vorhanden. Wenn vorhanden, dann Prüfung.
6.14	Wird vor größeren Wartungs-, Fernwartungs- oder Reparaturarbeiten eine komplette Sicherung der betroffenen Systeme erstellt?	Ja.
6.15	Wird der Fernwartungsvorgang dauerhaft überprüft oder aufgezeichnet?	Ja, durch Mitschnitt der Remotesession
6.16	Findet nach den durchgeführten Wartungs-, Fernwartungs- oder Reparaturarbeiten eine Integritätsprüfung statt?	Nein.

§ 7 Auftragskontrolle/Vertragskonformitätskontrolle

Nr.	*Frage*	*Antwort*
7.1	Durch welche Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind?	Protokollierung eingegebener Daten, Verarbeitungskontrolle (transaktionsbasiert)
7.2	Durch welche Maßnahmen wird gewährleistet, dass die Verarbeitung personenbezogener Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers erfolgt?	Schriftliche Weisung, Angebot und Auftragsbestätigung, Auftraggeber erhält alle Datenausgaben zur Kontrolle
7.3	Wie wird bei Änderungen im Verfahrensablauf/Programmänderungen durch den Auftragnehmer verfahren?	Keine Änderungen im Verfahrensablauf vorgesehen.

Nr.	*Frage*	*Antwort*
7.4	Wird der Auftraggeber über Programmabbrüche/Programmfehler informiert?	Nein.

§ 8 Verfügbarkeitskontrolle

Nr.	*Frage*	*Antwort*
8.1	Wie wird gewährleistet, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind?	Tägliches Backup.
8.2	Gibt es Notfall und Krisenmanagement (BCM)?	Nein.
8.3	Gibt es ein Backup-Rechenzentrum?	Nein.
Zu 8.3.	**Der Auftragnehmer digitalisiert analoge Handakten für den Auftraggeber. Die Handakten werden die Auftraggeber nach Abschluss der Digitalisierung zurückgegeben. Das Risiko eines Totalverlustes der Daten besteht nicht. Zumindest in analoger Form sind die Daten weiterhin vorhanden. Führt eine Systemstörung zu dem Verlust der Daten beim Auftragnehmer, wird der Auftragnehmer der Digitalisierungsprozess erneut durchführen.**	
8.4	Wer ist für die Sicherung der Daten zuständig?	Auftragnehmer.
8.5	Wie viele Generationen von Sicherungskopien existieren?	Eine.
8.6	In welchen Intervallen wird eine Datensicherung durchgeführt?	Täglich.
8.7	Wird eine regelmäßige Sicherung von datenverarbeitenden mobilen Endgeräten gewährleistet?	Ja.
Zu 8.7.	**Digitale Endgeräte werden unregelmäßig einem Backup unterzogen. Jeweils vor der Installation eines Updates wird ein Backup erstellt.**	
8.8	Wird das allgemeine Backup-Verfahren regelmäßig kontrolliert?	Ja.
8.9	Werden Sicherungsprotokolle erstellt und geprüft?	Ja.
8.10	Ist das Backup-Verfahren dokumentiert?	Ja.
8.11	Welche Backup-Methode wird angewendet?	Totalsicherung.
8.12	Wo werden Backup-Medien aufbewahrt?	Rechenzentrum.
8.13	Werden gesetzliche Aufbewahrungsfristen beachtet?	Ja.
8.14	Werden die gesetzlichen Vorgaben zur Löschung, Einschränkung und dem „Recht auf Vergessen werden“ eingehalten?	Ja.
8.15	Werden E-Mails, die die Geschäftsbeziehung mit dem Auftraggeber betreffen bzw. Daten enthalten, die für die Auftragsabwicklung notwendig sind, regelmäßig archiviert?	Ja.

Nr.	*Frage*	*Antwort*
8.16	Wie werden E-Mails archiviert?	Ja, automatisch.
8.17	Ist das Archivsystem zertifiziert?	Nein.
8.18	Welche störenden Einflüsse existieren beim Auftragnehmer in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet?	Nein.
8.19	Werden schädigende Umgebungseinflüsse in Räumen bzw. Gebäuden, in denen der Auftragnehmer Daten des Auftraggebers verarbeitet, bei der Installation und der Benutzung von IT-Komponenten beachtet?	Keine schädigenden Einflüsse vorhanden.
8.20	Gibt es eine Risikobewertung und einen Risikobehandlungsplan?	Nicht erforderlich.
8.21	Gibt es in den Serverräumen wasserführende Leitungen oder leichtbrennbare oder entzündliche Gegenstände?	Nein.
8.22	Sind in den Serverräumen Feuchtigkeits-, Rauch-, Wärmesensoren installiert?	Brandmelder.
8.23	Stehen in den Serverräumen entsprechend zugelassene Feuerlöscher /Löschanlagen zur Verfügung?	Ja.
8.24	Wie wird ein zuständiger Mitarbeiter bei einem Alarmsignal eines Sensors über den kritischen Zustand in den Serverräumen des Rechenzentrums informiert?	Alarmton.
8.25	Ist die Erreichbarkeit eines zuständigen Mitarbeiters im Katastrophenfall jederzeit gewährleistet?	Ja.
8.26	Gibt es Eskalationspläne?	Nein.
8.27	Sind die Serverräume vor Einbruch ausreichend geschützt?	Ja.
8.28	Sind die Serverräume entsprechend der technischen Spezifikation ausreichend klimatisiert?	Ja.
8.29	Stehen die Server in 19"-Racks?	Derzeit nicht.
8.30	Mit welcher Tür sind die Serverräume ausgestattet?	Normale Tür.
8.31	Werden verfahrensfremde Datenträger mit eindeutiger Zuordnung verwaltet?	Nein.
8.32	Besteht eine Archivordnung?	Nein.
8.33	Ist ein Archivverwalter bestellt?	Nein.
8.34	Existiert ein eigener Archivraum (Sicherungsbereich)?	Nein.
8.35	Besteht lediglich ein beschränkter Zugang zum Archivbereich?	ja/nein

Nr.	*Frage*	*Antwort*
8.36	Erfolgt die Ein- und Ausgabe von Datenträgern nur durch die Archivverwaltung?	ja/nein
8.37	Wird die Ein- und Ausgabe von Datenträgern revisionsfähig protokolliert?	ja/nein
8.38	Erfolgen regelmäßige Bestandskontrollen der Datenträger durch Soll-/Ist-Vergleich?	ja/nein
8.39	Ist das Mitnehmen von Taschen und Mänteln in die Sicherheitszonen (Archiv) untersagt?	ja/nein
8.40	Ist das Mitnehmen von Telefonen, Fotoapparaten und anderen elektronischen Geräten in Sicherheitszonen (Archiv) untersagt?	ja/nein
8.41	Wer ist für die Einhaltung von Wartungsintervallen, der Auswahl und Beauftragung von Wartungsunternehmen verantwortlich?	Geschäftsleitung.

§ 9 Datentrennungskontrolle/Mandantentrennungskontrolle

Nr.	*Frage*	*Antwort*
9.1	Wie wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?	Dateiseparierung.
9.2	Aus welchen Gründen ist eine Trennung nicht möglich/notwendig?	

§ 10 Prüfung der Betriebsorganisation und Rechenschaftspflicht

Nr.	*Frage*	*Antwort*
10.1	Durch welche Maßnahmen ist die innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird?	□ Datenschutzbeauftragter ist schriftlich bestellt □ Fachkundenachweise des Datenschutzbeauftragten liegen vor □ schriftliche Arbeitsanweisungen/Richtlinien/Merkblätter liegen vor □ Programme/Verfahren sind ordnungsgemäß dokumentiert □ Aufbewahrung/Archivierung aller maschinell erzeugten Protokolle ist geregelt □ Programmfreigabeverfahren ist eingerichtet □ Vier-Augen-Prinzip wird angewendet bei: - Einrichtung, Änderung oder Löschung von Mitarbeiterrollen - Änderung von TOMs _____

Nr.	*Frage*	*Antwort*

Gez.

Dipl. iur. Julian Akich, LL.B.

Dipl. iur. Julian Akich, LL.B.
RECHTSANWALT
* Bad Schönborn