Auftragsverarbeitung personenbezogener Daten nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

1 Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus ihrem vorliegenden letztdatierten gültigen Dienstleistungsvertrag, in ihren Einzelheiten beschriebenen Auftragsverarbeitung, ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

2 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

3 Gegenstand und Dauer der Verarbeitung

3.1 Gegenstand

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO.
Der Auftragnehmer übernimmt folgende Verarbeitungen:

a. **Mietberufsbekleidung:**
   Bei einer Anprobe werden Name, Vorname, Berufsgruppe, Berufsbekleidungsartikel, Anzahl, Größe sowie Seitenlänge (Hosen) erfasst und an das Service-Center übermittelt. Dort werden die Daten in die ERP-Datenbank eingegeben und im Anschluss von den Mitarbeitern der Einkleidung als Patch auf die Mietberufsbekleidung aufgebracht. Sie dienen im Einzelnen der richtigen Zuordnung der Kleidung je Mitarbeiter. Ein erneuter Zugriff auf die Daten erfolgt bei einem Austausch der Kleidung (Verschleiß, Beschädigung, Artikeltausch, Größentausch)

b. **Mietberufsbekleidung im Pool (automatische Ausgabesysteme)**
Der Auftraggeber stellt dem Auftragnehmer folgende Daten zur Verwaltung des Ausgabe-Automaten zur Verfügung: Name, Vorname, Berufsgruppe, ggfls. ID-Nummer, Chip-Karte, Berufsbekleidungsartikel, Größen sowie Seitenlänge (Hosen). Diese werden in der ERP-Datenbank und anschließend auf die Automaten-Datenbank übertragen und sind per Fernwartung für den Automaten-Hersteller sichtbar. Sobald sich ein Mitarbeiter über seine ID-Karte anmeldet, erhält er im Anschluss Berufsbekleidung ohne pb-Daten als Pool-Ware. Der Kredit-Vorgang wird verbucht.

c. **Bewohnerwäsche pro persona**
Der Auftraggeber stellt dem Auftragnehmer folgende Daten zur Verfügung: Name, Vorname, Wohnbereich, Einrichtung zur Verfügung. Diese Daten werden in der Bewohnerwäscheabteilung verarbeitet und auf die jeweiligen Wäschesäcke der Bewohner gepacht. Sie dienen zur richtigen Zuteilung/Erfassung der bewohnereigenen Wäsche und der späteren bewohnerbezogenen Auslieferung. Jedes Wäschestück wird bei Abgabe in die Wäscherei erfasst, sodass eine Beurteilung der Waschzyklen möglich ist.

d. **Debitoren- / Kreditoren-Daten**
Speicherung von Firmendaten, Kontaktpersonen, Bankverbindungen zur Abfrage, Bestellung, Rechnungsstellung

Die Verarbeitung beruht auf allen zwischen den Parteien bestehenden Dienstleistungsverträgen.

3.2 Dauer

Die Verarbeitung beginnt zum Vertragsbeginn der Zusammenarbeit und erfolgt auf unbestimmte Zeit bis zur Kündigung oder dem längst gültigen Vertrages.

4 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

4.1 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art:
Erfassen, Organisation, Ordnen, Speicherung, Auslesen, Abfragen,

Die Verarbeitung dient folgendem Zweck:
Bearbeitung und Zuteilung von Berufsbekleidung, Austausch/Neuausstattung von Berufsbekleidung, Verwaltung von Bekleidungskrediten bei automatischer Ausgabe, Bearbeitung und Zuteilung von Bewohnerbekleidung, Erfassung von Bearbeitungszyklen.

4.2 Art der Daten

Es werden folgende Daten verarbeitet:

- Name
- Vorname
- Berufsgruppe
- Art und Menge der Bekleidung
- Farbe, Größe ggfls. Seitenlänge (Hose)
- Kundenanschrift (Einrichtung z.B. Klinik, Senioreneinrichtung etc.)
- Bei bewohnereigener Wäsche zusätzlich Wohnbereich
- Lieferantendaten

4.2.1 Kategorien der betroffenen Personen

- Mitarbeiter des Auftragsgeber (Mietberufsbekleidung)
- Bewohner einer Senioreneinrichtung bei Teilnahme am proPersona-Systems (Bearbeitung von bewohnereigener Wäsche)
- Lieferanten und deren Ansprechpartner für Sitex

5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in

Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

6 Technische und organisatorische Maßnahmen

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden nicht ohne Wissen des Auftraggebers erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen sowie vorgeschriebene Back-ups, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Dem Auftraggeber steht das Recht zu, die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit zu überprüfen.

7 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

8 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(5) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(6) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

(7) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen.

(8) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

(9) Zurzeit sind die in Anlage 2 mit Namen und Anschrift bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(10) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des

Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

9 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung und die schriftliche Bestätigung der Betroffenen sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber hat dafür Sorge zu tragen, dass Mitarbeiter des Auftraggeber, welche Zugang zu pb-Daten über die Schnittstelle besitzen, über die Datenschutzrichtlinien informiert sind und bei Ausscheiden die Zugangsberechtigungen entzogen werden.

(5) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(6) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

10 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 72 Stunden ab Kenntnis des Auftragnehmers vom

relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

11 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

12 Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die Rückgabe bzw. Löschung/Anonymisierung auch bei Subunternehmern herbeizuführen.

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

13 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

14 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen. Dies gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

15 Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

Technische und organisatorische Maßnahmen zur Sicherstellung der Verarbeitung personenbezogener Daten nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

technische Maßnahmen:

1. ständige Speicherung auf gespiegelter Festplatte
2. tägliche Datensicherung auf Sicherungsband
3. Aufbewahrung der Sicherungsbänder/Generationen im feuerfesten Tresor
4. getrennte Gebäudebereiche zwischen Server und Sicherungstresor
5. Abo für Antivirenprogramm auf Server und Arbeitsplatzcomputern

organisatorische Maßnahmen:

1. Unterweisung und schriftliche Erklärung der betroffenen Mitarbeiter auf Datenschutz
2. Kennwortzuteilung für Windows
3. Kennwortgeschützte Ordnerfreigaben pro Berechtigungsgruppen
4. Kennwortgeschützte Softwarefreigaben
5. Kennwortgeschützte Modulfreigaben innerhalb der Branchensoftware
6. Nutzerregistrierung bei Anlagen und Änderungen von Daten/Eingaben
7. Gebäudezugang mittels Personalchip einschl. Berechtigungszeiten

1) Zutrittskontrolle
   a) Es kommt ein Schließsystem zum Einsatz, verwaltet durch IT-Abteilung und Personalabteilung
   b) Zugang zum Serverraum nur durch IT Mitarbeiter und Generalschlüssel
   c) Büroräume Nachts, Wochenende und an Feiertagen verschlossen
   d) Nachtwächter in der Zeit von 22.00 Uhr bis 07.00 Uhr
   e) Zugang zum Betriebsgelänge gesteuert über Chipkarten nach Mitarbeitergruppe und Zeitraum
   f) Live-Videoüberwachung und Speicherung der Videoaufnahmen für eine Woche
2) Zugangskontrolle
   a) Zugang zum IT-System nur über entsprechende Zugangsberechtigung. Beantragung durch Vorgesetzten oder Personalabteilung
   b) Remote Zugriffe erfolgen über eine verschlüsselte Verbindung
   c) Zugriff auf Server über Internet werden durch eine Firewall mit aktuellen Schutzmaßnahmen (IPS, IDS, usw.) abgesichert
   d) Es wird ein Spamfilter eingesetzt der regelmäßig und automatisch aktualisiert wird
   e) Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist
   f) Zugriff der Clients auf das Internet wird gefiltert um Schadsoftware und das aufrufen von illegale Webseiten zu verhindern
3) Zugriffskontrolle
   a) Berechtigungen für IT-Systeme und Applikationen werden durch Administrator eingerichtet
   b) Berechtigungen werden nur für die zur Erledigung der Arbeit benötigten Daten erteilt
   c) Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert
4) Weitergabekontrolle
   a) Soweit möglich werden Daten verschlüsselt an Empfänger übertragen
   b) Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist
5) Eingabekontrolle
   a) Eingabe, Änderung und Löschung von personenbezogenen Daten werden protokolliert

b) Mitarbeiter arbeiten mit eigenen Benutzeraccounts die nicht mit anderen Mitarbeitern geteilt werden dürfen, ausgenommen sind Produktionsarbeitsplätze

6) Auftragskontrolle
   a) Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union
7) Verfügbarkeitskontrolle
   a) Speicherung der Daten erfolgt auf redundanten Speichersystemen
   b) Serverhardware ist redundant ausgelegt
   c) IT-Syteme verfügen über eine unterbrechungsfreie Stromversorgung und eine Klimatisierung die beide in der Lage sind Störungen (z.B. Übertemperatur) zu melden
   d) Es ist eine Brandmeldeanlage installiert
   e) Feuerlöscher stehen für den Notfall bereit
   f) Untertägig werden Sicherungen von den wichtigsten System gemacht
   g) Täglich werden Sicherungen von allen System gemacht
   h) Sicherungen werden extern ausgelagert (Bankschließfach)
   i) Rücksicherungen werden unregelmäßig überprüft
   j) Ein Monitoring informiert bei Störungen
8) Trennungskontrolle
   a) Die eingesetzten IT-Systeme sind mandantenfähig
   b) Trennung von administrativen- und Standard-Benutzerkonten
   c) Es ist ein betrieblicher Datenschutzbeauftragter benannt