LANDRATSAMT REUTLINGEN
Den 08.10.2018

KT-Drucksache Nr. IX-0569

für den Verwaltungsausschuss
-nichtöffentlich-

für den Kreistag
-öffentlich-

Externes Scannen der Personalakten der Beamten und Beschäftigten des Landkreises

Beschlussvorschlag:

Die Personalakten der Beamten und Beschäftigten des Landkreises werden an einen externen Dienstleister zur Verscannung übermittelt.

Aufwand/Finanzielle Auswirkungen:

Gesamtaufwand/ Gesamtinvestition:	17.000,00 EUR	Anteil Landkreis:	17.000,00 EUR
Teilhaushalt: 1 Produktgruppe: 11.20		zur Verfügung stehende HH-Mittel:	80.000,00 EUR

Sachdarstellung/Begründung:

I. Kurzfassung

Im Zuge der Einführung eines Dokumentenmanagementsystems (DMS), zunächst im Hauptamt als Pilotbereich, soll auch die elektronische Personalakte als Fachverfahren implementiert werden.

Hierfür soll der Bestand der Personalakten aller Bediensteten an einen externen Dienstleister weitergegeben und von diesem innerhalb eines vorgegebenen Zeitrahmens verscannt werden.

II. Ausführliche Sachdarstellung

1. Einführung eines DMS beim Hauptamt

Beim Hauptamt wird im Herbst 2018 als Pilotamt das DMS enaio der Firma Optimal Systems eingeführt. Dieses DMS ist in Baden-Württemberg bei 32 von 35 Landkreisen im Einsatz und wird auch von ITEOS betreut und vertrieben.

Sowohl der Abschluss entsprechender Dienstleistungs- und Betreuungsverträge wie auch die Verscannung von ca. 20 Aktenmetern laufender Sachakten wurden bzw. werden zuständigkeitshalber von der Verwaltung veranlasst.

2. Rechtliche Grundlage

Gemäß § 85 a Landesbeamtengesetz Baden-Württemberg ist die Verarbeitung von Personalaktendaten der Beamten zulässig,

- soweit sie erforderlich ist zur Verrichtung technischer Hilfstätigkeiten; hierunter fällt auch die Verscannung der Daten
- wenn der Landkreis die Einhaltung der beamten- und datenschutzrechtlichen Vorschriften regelmäßig kontrolliert.

Die Auftragserteilung bedarf der vorherigen Zustimmung des Kreistags.

3. Vergabe

Es wurden mehrere Angebote eingeholt. Vorgesehen ist die Vergabe an eines der folgenden Unternehmen:

- BruderhausDiakonie, Reutlingen bzw. Villingen-Schwenningen
- Scamitec-Esslingen Dr. Kienlin GmbH, Esslingen am Neckar
- Dokumenten- und Datenservice Wandel GmbH, Filderstadt
- Keller GmbH, Ditzingen

Mit ITEOS wird derzeit noch der finale Zeitplan zur Einrichtung notwendiger Schnittstellen ausgelotet, daher konnte noch mit keinem der in Frage kommenden Unternehmen abschließend verhandelt bzw. ein Vertrag geschlossen werden.

Die getroffenen technischen und organisatorischen Maßnahmen sowie die ergänzenden Festlegungen nach Artikel 28 der Verordnung (EU) 2016/679 ergeben sich beispielhaft aus den Anlagen.

Die beim Auftragsverarbeiter mit der Datenverarbeitung beauftragten Beschäftigten werden besonders auf den Schutz der Personalaktendaten verpflichtet.

bruderhaus DIAKONIE
Stiftung Gustav Werner und Haus am Berg

Datenschutz- und Datensicherheitskonzept

BruderhausDiakonie – Werkstätten Digitalisierung

Stand Juni 2018

Inhalt

1. Ziel des Datenschutzkonzeptes

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der Auftragsverarbeitung genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

2. Vorbemerkung

Die Digitalisierung der BruderhausDiakonie übernimmt das Einscannen von Belegen, Zeichnungen oder Büchern für Ihre Auftraggeber nach Kundenvorgaben. Die Datenerhebung, -verarbeitung und –nutzung erfolgt im Kundenauftrag.

Eine detaillierte Beschreibung des Leistungsumfangs ist zwischen den Auftraggebern und der BruderhausDiakonie-Werkstätten – Digitalisierung - vertraglich geregelt.

Um diese Aufgaben ausführen zu können, werden im Betrieb Daten von unterschiedlicher Datenschutzrechtlicher Relevanz verarbeitet.

In diesem Dokument werden die von der BruderhausDiakonie-Werkstätten – Digitalisierung - getroffenen datenschutzrechtlichen Maßnahmen festgelegt wie:

- Beachtung von Rechtsvorschriften, Richtlinien und sonstige Arbeitsanweisungen zur Datensicherheit und zur Ordnungsmäßigkeit der Datenverarbeitung.
- Schutz der vertraulichen Daten aller Beteiligten,
- Gewährleistung der Integrität und Verfügbarkeit der Daten und der Informationssysteme,
- Gewährleistung der Vollständigkeit und Authentizität der Daten,
- Sicherstellung der Kontinuität der Arbeitsabläufe,
- Transparente und nachvollziehbare Gestaltung der Datenverarbeitungsprozesse,
- Verpflichtung der für die BruderhausDiakonie-Werkstätten – Digitalisierung - tätigen Mitarbeiter sowie Vertragspartner zum Schutz anvertrauter Daten.

Zusätzlich dazu werden hier auch die datenschutztechnisch getroffenen Maßnahmen und Regelungen im Betrieb BruderhausDiakonie-Werkstätten – Digitalisierung - unter folgenden Gesichtspunkten betrachtet:

- Wie ist der Datenschutz organisiert?
- Welche Verschlüsselungstechnologien werden genutzt?
- Wie erfolgt der Zugriff auf die Daten und die Authentifizierung des Anwenders?
- Wie häufig erfolgt die Datensicherung?
- Welche Maßnahmen greifen im Falle eines Serverausfalls?
- Wie ist die Sicherheit des Datentransfers organisiert?

3. Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

Die BruderhausDiakonie-Werkstätten – Digitalisierung - eingeschlossen ihrer Mitarbeiter und Subunternehmer, verpflichten sich zur Einhaltung von datenschutzrechtlichen Vorschriften. Die betroffenen Personen wurden darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind in
Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein;
- es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

4. Rollen und Verantwortlichkeiten

Verantwortlicher im Sinne des Datenschutzgesetzes ist die

BruderhausDiakonie
Stiftung Gustav Werner und Haus am Berg
Ringelbachstraße 211
72762 Reutlingen
Telefon 07121 278-0
Telefax 07121 278-300
Internetadresse (URL): http://www.bruderhausdiakonie.de

Der Vorstand der BruderhausDiakonie
besteht aus folgenden Personen:

Lothar Bauer (Vorsitzender des Vorstandes),
Andreas Lingk (Kaufmännischer Vorstand),
Günter Braun (Fachlicher Vorstand).

Datenschutzbeauftragte:

Thomas Althammer
c/o Althammer & Kill GmbH & Co. KG
Buchenhain 15
30938 Burgwedel
Telefon +49 5139 973949-0
Telefax +49 5139 973949-9
E-Mail kontakt-dsb(at)althammer-kill.de

Koodination der Datenschutzaufgaben:

Andreas Bauer
Werkstattleiter
Sven Saur
Produktionsleiter
Am Heilbrunnen 100
72766 Reutlingen
Tel. 07121-14495-0
Email: Andreas.Bauer@bruderhausdiakonie.de

5. Verpflichtung zur kontinuierlichen Verbesserung eines Datenschutzmanagementssystems

Regelmäßige Schulungen einmal pro Jahr sind für die Mitarbeiter verpflichtend. Die Einhaltung des Datenschutzkonzeptes wird einmal jährlich überprüft. Das Ergebnis des Audits wird In einem Soll-Ist-Vergleich protokolliert.

6. Datenschutzrechtliche Rahmenbedingungen

Das Erheben und Verarbeiten personenbezogener Daten in der Europäischen Datenschutz-Grundverordnung (EU DS-GVO) und im für die BruderhausDiakonie geltenden Datenschutzgesetz der Ev. Kirche (DSG-EKD 2018) geregelt. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (so genannter Betroffener).

Generell gilt, dass Personenbezogene Daten nur verarbeitet werden dürfen, wenn gesetzliche Vorschriften dies erfordern oder der Betroffene ausdrücklich eingewilligt hat. Die Einwilligung ist nur wirksam, wenn der Nutzer über die Tragweite des Verfahrens informiert wurde, das heißt welche Daten zu welchem Zweck in welcher Form gespeichert und verarbeitet werden und die Einwilligung nicht in anderen Erklärungen versteckt worden ist.

Die Art und Weise der Speicherung seiner Daten muss für den Betroffenen nachvollziehbar sein.
Die DSGVO legt außerdem fest, dass die Datenverarbeitung nur noch rechtmäßig ist zur Wahrung berechtigter Interessen des Verantwortlichen, sofern nicht Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen.

Die von der BruderhausDiakonie-Werkstätten – Digitalisierung - eingescannten, verarbeiteten und gespeicherten Daten sind von unterschiedlicher datenschutzrechtlicher Relevanz (Artikel 9 DS-GVO).

Die ordnungsgemäße und datenschutzgerechte Verarbeitung der Daten findet vorwiegend als Auftragsdatenverarbeitung im Rahmen vertraglicher Vereinbarungen statt. Die Digitalisierung der Bruderhausdiakonie ist hier Auftragnehmer nach §11 DSG-EKD 2018 und Artikel 5 DS-GVO. Danach ist grundsätzlich der Auftraggeber für die Einhaltung des Datenschutzrechtes außerhalb der Räume der BruderhausDiakonie – Werkstätten, Am Heilbrunnen 100 in Reutlingen für die Einhaltung des Datenschutzrechtes verantwortlich.

Der Auftragnehmer verpflichtet sich, die Verarbeitung der ihm übergebenen personenbezogenen Daten ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers durchzuführen
(§ 11 DSG-EKD und Artikel 5 DS-GVO). Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen das Bundesdatenschutzgesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
.
Die BruderhausDiakonie – Digitalisierung speichert und verarbeitet die folgende Daten:

Betroffenengruppen:

Die Betroffenengruppen ergeben sich daraus, welche Dokumente für den Auftraggeber eingescannt werden.
Kunden und Mitarbeiter gehören aber immer zu den betroffenen Personengruppen.

Datenkategorien:

Die Datenkategorien ergeben sich aus dem zu digitalisierenden Scannmaterial.
Bei Kunden und Mitarbeiter sind es
Name, Kontakt- und Auftragsdaten (Kunden),
Arbeitsfortschritts- und Arbeits- und Fehlzeiten (Mitarbeiter).

Daten können zur Erfüllung gesetzlicher Verpflichtungen oder der reibungslosen Abwicklung von Aufträgen weitergegeben werden an

BruderhausDiakonie – Büroservice, Reutlingen – Zur Arbeitsvorbereitung
Intego gGmbH, Villingen-Schwenningen – zur Auftragsabwicklung

Alle Daten liegen auf dem Server und sind mit den entsprechenden Schutzmaßnahmen gesichert. (Siehe technische und organisatorische Maßnahmen nach Artikel 25 DSGVO)

7. Allgemeiner Schutzbedarf

Der allgemeine Schutzbedarf der auftragsbezogenen Daten ist entsprechend der Vorgaben des Auftraggebers von unterschiedlicher Relevanz .
Besondere Aufmerksamkeit erfordern bei BruderhausDiakonie - Digitalisierung die Daten, die den gesetzlichen Vorgaben entsprechend in der Personalverwaltung verarbeitet und entsprechend den Bestimmungen an Behörden und Sozialversicherungsträger weitergegeben werden müssen. Hier ist der Schutzbedarf als „hoch“ anzusehen. Entsprechende Vorkehrung zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit sind getroffen

Als geeignete Maßnahmen sind hier Virenschutz und ein Firewall-System anzusehen, die Weitergabe erfolgt nur in verschlüsselter Form über gesicherte Leitungen. Der Zugang zu Systemen und Dateien ist passwortgeschützt und durch die Vergabe von Berechtigungen so geregelt, dass niemand Zugriff auf sensible Daten hat, der nicht unmittelbar zu seinem Aufgabengebiet gehören
Eine Weitergabe erfolgt nur über verschlüsselte und gesicherte Leitungen.
Eine Pseudonymisierung ist mit der Verwendung von Kunden- und Personalnummern gewährleistet.
Virenschutz und Firewall sind vorhanden
Daten werden passwortgeschützt über verschlüsselte Leitungen weitergegeben.

8. Technische und organisatorische Maßnahmen nach DSGVO

Die technischen und organisatorischen Maßnahmen werden wie im Artikel 32 Abs. 1 DSGVO gefordert entsprechend dem Stand der Technik im angemessenen Verhältnis zum angestrebten Schutzzweck von der BruderhausDiakonie - Digitalisierung umgesetzt. Alle anfallenden Verfahren werden dokumentiert und regelmäßig überprüft.

Im Folgenden werden die unter datenschutzrechtlichen Gesichtspunkten relevanten Maßnahmen vorgestellt, die grundsätzlich bei BruderhausDiakonie - Digitalisierung berücksichtigt werden.

8.1. Pseudonymisierung

Kunden- und Auftragsnummern gewährleisten die Pseudonymisierung der personenbezogenen Daten.

8.2. Verschlüsselung

Datenübertragungen finden über gesicherte und verschlüsselte Leitungen per SFTP und VPN statt. Ein Netz-Passwort ist vorhanden. Der Passwortschutz ist auf dem Server eingerichtet.

8.3. Gewährleistung der Vertraulichkeit

Der Serverraum befindet sich in einem verschlossenen Serverschrank im verschlossenen Serverraum. Zugang haben lediglich die Administratoren und deren Vorgesetze.

Beim Verlassen des Serverraums wird die Tür abgeschlossen, um den Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen für Unbefugte zu verhindern.
Der Zugang zu den Räumlichkeiten der Digitalisierung ist nur für autorisierte Personen möglich. Berechtigt sind alle Mitarbeiter der Digitalisierung, deren Berechtigungen hierzu nachprüfbar dokumentiert sind.
Der Bereich, in dem die Kundenaufträge bearbeitet werden, ist räumlich von der Publikumszone getrennt und mit einer per Fingerscan bzw. Code-Karten gesicherten Tür verschlossen.
Besucher werden an der Pforte in Empfang genommen. Von da werden sie zum Bereich Digitalisierung begleitet.
Jeder Kunde, Besucher und Mitarbeiter unterschreibt eine Datenschutzerklärung, bevor er die Bearbeitungszone betritt.
Sobald die Datenträger vom Kunden zum Löschen freigegeben sind, werden sie mit einer speziellen Software zur Datenlöschung 35 x überschrieben.
Rechner werden automatisch gesperrt, sobald sie nicht benutzt werden. Einblick in die Daten ist dann nur mit Passwort möglich.
Nicht mehr benötigte Betriebsmittel wie Datenträger werden so entsorgt, dass ein Rekonstruieren der Inhalte nicht mehr möglich ist. CDs werden geschreddert, Papierdokumente von der Firma Leins datenschutzkonform professionell entsorgt.
Der elektronische Zugang zu Systemen der BruderhausDiakonie-Werkstätten – Digitalisierung - via Netzwerk ist nach heutigen technischen Standards gesichert.
Zugangsdaten zu Serversystemen sind nur der Administratorin der Digitalisierung oder Ihren Vertretern bekannt.
Die Rechner werden automatisch gesperrt, sobald sie nicht benutzt werden, so dass keine betriebsfremden Personen zufällig Einblick in die betrieblichen Daten erlangen können.
Räume, Container und Schränke, in denen Daten unter Verschluss gehalten werden, werden direkt nach Benutzung wieder verschlossen. Die Besitzer der Schlüssel sind in einer Schlüsselkartei erfasst.

8.4. Gewährleistung der Integrität

Datenträger werden sachgerecht und vor unbefugtem Zugriff geschützt aufbewahrt.
Von Dritten erhaltene Datenträger werden auf Computer-Viren überprüft.
Die Belege werden in verschlossenen Gitterboxen angeliefert.
Im Wareneingang der Digitalisierung wird jeder Vorgang erfasst und mit einem Laufzettel ausgestattet. Jeder Vorgang hat seine eigene Box.
Der Laufzettel bleibt bei der Box bis zum letzten Arbeitsgang.

Die Daten werden nach Kundenwunsch unterschiedlich verarbeitet.
Der Ablauf des Verfahrens wird in Absprache mit dem Kunden festgelegt.
Alle Aufträge werden entsprechend der vergebenen Rechte getrennt voneinander verarbeitet und gespeichert.

8.5. Gewährleistung der Verfügbarkeit

Über Systemeinrichtungen und Verfahren gewährleistet die Digitalisierung der BruderhausDiakonie – Werkstätten, dass auftrags- sowie personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Die Datensicherungen finden 4 x täglich als Volumen-Schattenkopie statt und 1 x täglich komplettes Backup auf externe Festplatte.
Die Sicherheitskopien werden sowohl auf dem Server als auch auf Datenträgern im Tresor aufbewahrt. Auf diese Weise wird zufälliger Datenverlust verhindert. Eine USV-Anlage schützt die IT-Anlage außerdem vor Datenverlust.

8.6. Gewährleistung der Belastbarkeit der Systeme

Alle IT- und Scann**-** Systeme werden in einem regelmäßigen turnusmäßige Rhythmus auf Funktion und Belastbarkeit überprüft

8.7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die tägliche Datensicherung wird zeitgesteuert nach Vorgabe des Vertragspartners durchgeführt. Die Daten werden auf physikalisch getrennten Speichermedien vorgehalten.

8.8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Regelmäßige Schulungen finden statt.
Interne Verhaltensregeln sind vereinbart.
Ein umfassendes Datenschutz- und Notfallvorsorgekonzept ist vorhanden.

Die Einhaltung des Datenschutzes wird regelmäßig einmal jährlich von den Datenschutzmitarbeitern der Firma ms computer GmbH geprüft.
Ein Verzeichnis über die Verarbeitungstätigkeiten wird geführt und regelmäßig aktualisiert.

Dieses Verzeichnis enthält folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

9. Geschäftsgegenstand

Die Digitalisierung der Bruderhausdiakonie übernimmt das Einscannen von Belegen, Zeichnungen oder Büchern für Ihre Auftraggeber nach Kundenvorgaben. Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausübung der oben angegebenen Zwecke.

Digitalisierte Belege, Zeichnungen, Bücher und Originalbelege werden anschließend an den Eigentümer zurückgegeben oder datenschutzkonform durch die Fa. Leins vernichtet.

Die Auftragsabwicklung gliedert sich wie folgt:

- Die Belege werden in verschlossenen Gitterboxen angeliefert werden.
- Im Wareneingang des Scanbereichs wird jeder Vorgang erfasst und mit einem Laufzettel ausgestattet. Jeder Vorgang hat seine eigene Box. Kundendaten werden durch Laufnummer ersetzt und sind nicht zuordenbar
- Der Laufzettel bleibt bei der Box bis zum letzten Arbeitsgang.
- Die Daten werden nach Kundenwunsch unterschiedlich verarbeitet.
- Der Ablauf des Verfahrens wird in Absprache mit dem Kunden festgelegt.

10. Standorte und organisatorische Gliederung

Verwaltungsabteilungen und die Abteilungen für Einkauf, Marketing, Vertrieb, Personalverwaltung sind außerhalb der Betriebsräume der BruderhausDiakonie-Werkstätten – Digitalisierung - in einem anderen Gebäude untergebracht.
Die BruderhausDiakonie-Werkstätten – Digitalisierung - ist räumlich und IT-technisch von der übrigen Infrastruktur der BruderhausDiakonie – Werkstätten getrennt.
Für das Digitalisieren der Kundenbelege wird Informationstechnik eingesetzt.

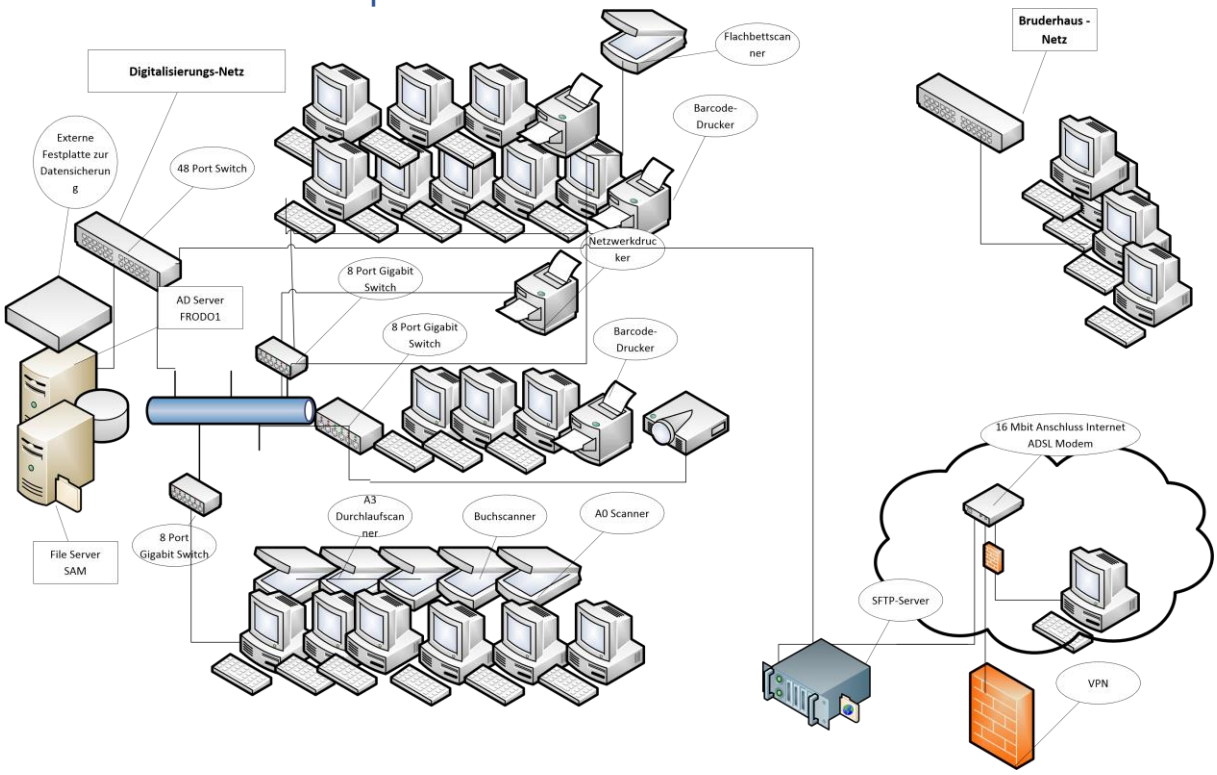
Der Stand der Informationssicherheit in diesem Bereich wird ständig geprüft. Sollten die vorhandenen Sicherheitsvorkehrungen dem Schutzbedarf der Geschäftsprozesse und Anforderungen nicht mehr entsprechen, werden sofort Gegenmaßnahmen eingeleitet, die den dadurch gegebenen Gefährdungen entgegenwirken.

Räumliche Gegebenheiten
Die Produktionsstätte Am Heilbrunnen besteht aus einem Raum. Hier wird das Scanmaterial nach Aufträgen und Auftraggeber getrennt in abgeschlossenen Kästen verarbeitet. Aufträge, die noch nicht abgearbeitet werden, lagern in abgeschlossen Boxen im Lager.
Die Räumlichkeiten der Digitalisierung haben zwei Türen. Der Zugang ist nur durch eine mit Fingerabdruck-Scanner gesicherte Tür möglich. Eine Tür dient lediglich als Fluchttür und ist nur von innen zu öffnen. Zwei weitere Türen, die nur von innen zu öffnen sind, gehen in den Innenhof. Betriebsfremde Personen haben keinen Zugang zu diesem Innenhof.
Der Serverraum ist ein ca. 6 qm großer, abgeschlossener Raum ohne Fenster und ist mit einer Klimaanlage ausgestattet.

11. Netze und IT-Systeme

Die BruderhausDiakonie-Werkstätten – Digitalisierung - betreibt ein internes Netz auf der Basis von Ethernet TCP/IP und Microsoft Windows-Betriebssystemen. Es läuft unabhängig von dem Netz der BruderhausDiakonie und wird auch direkt von der BruderhausDiakonie-Werkstätten – Digitalisierung - aus administriert.
Der Server ist mit 18 Arbeitsplatzrechnern verbunden. Die Daten werden zentral auf dem Server gespeichert, die Software läuft auf den Arbeitsplatzrechnern.
Auf 3 Rechnern wird mit Office 2010 gearbeitet, 9 Arbeitsplätze haben folgende Software installiert: DPU Scan, NextImage, Cocpac, P-touch, Mozilla Firefox, Acrobat Reader, Irfan View, Secure Earser, Foxit Reader, Nero Express, Paint.net, Gimp2, Time Design, Canon Scan, abbyy-finereader und TrendMicro.
Das Netzwerk hat keine Verbindung nach außen. Mails können lediglich auf dem Internetfähigen Rechner der IT-Leiterin empfangen werden. Hier ist eine Antivirensoftware von TrendMicro zum Schutz installiert. Auch Sticks und andere angelieferte Datenträger werden hier auf Viren geprüft, bevor sie verwendet werden.

Der aktuelle Netzwerkplan:



Beschreibung:
Die Netzwerkadressen aller Komponenten werden per DHCP automatisch vergeben und verwaltet.
IP-Adressen werden dynamisch vergeben. Nur Server und Drucker haben feste IP-Adressen.
Passwörter zur Anmeldung im Netzwerk werden alle 6 Wochen am Server zurückgesetzt und müssen erneuert werden.
Die Rechte werden zentral durch die Systemadministratorin nach Gruppenrichtlinien vergeben. Gastzugänge gibt es nicht.

12. Leitlinie zur Informationssicherheit und Sicherheitskonzept

12.1 Geltungsbereich des Sicherheitskonzepts

Die Leitung der BruderhausDiakonie-Werkstätten – Digitalisierung - verabschiedet mit dieser Leitlinie die folgenden für alle Abteilungen und Mitarbeiter verbindlichen Grundsätze zur Informationssicherheit im Unternehmen.

Stellenwert von Informationen, Informationstechnik und deren Sicherheit für den Bereich der BruderhausDiakonie-Werkstätten – Digitalisierung

Der Erfolg der BruderhausDiakonie-Werkstätten – Digitalisierung ist abhängig von aktuellen und korrekten Informationen. Diese werden ausschließlich elektronisch verarbeitet, gespeichert und übermittelt. In allen Geschäftsprozessen kommt hier deshalb der Informationstechnik ein hoher Stellenwert zu.

Die folgenden Beispiele veranschaulichen die Bedeutung von Informationssicherheit:

- Die Belege, die in der BruderhausDiakonie-Werkstätten – Digitalisierung - im Kundenauftrag eingescannt werden, beinhalten Daten von unterschiedlichem Schutzbedarf. Unter anderem werden auch Personaldaten digitalisiert. Zum Schutz dieser Informationen sind wir im Interesse der Betroffenen und aus gesetzlichen Gründen verpflichtet.
- An vielen Stellen des Unternehmens werden vertrauliche Informationen von Kunden und Geschäftspartnern vorrätig gehalten. Ein Missbrauch dieser Informationen kann das Ansehen und damit auch den geschäftlichen Erfolg der BruderhausDiakonie-Werkstätten – Digitalisierung - nachhaltig beschädigen und ist daher zu verhindern.
- Die Wettbewerbsposition der BruderhausDiakonie-Werkstätten – Digitalisierung - der Bruderhausdiakonie beruht unter anderem auch auf der Datensicherheit, die den Kunden gewährleistet werden kann.

Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzung dafür, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen zu gewährleisten. Aufgrund unserer Verantwortung für die Informationssicherheit haben wir einen Sicherheitsprozess in Gang gesetzt. Dazu gehört die Entwicklung und Umsetzung dieser Leitlinie und eines Sicherheitskonzepts. Die Einhaltung der Leitlinie sowie Aktualität und Angemessenheit des Sicherheitskonzepts werden regelmäßig überprüft.

12.2. Ziele der Informationssicherheit und Kernelemente unserer Sicherheitsstrategie

Die Informationstechnik dient unserem Unternehmen im Wesentlichen zur Abwicklung unserer Auftragsverarbeitung.
Ein Ausfall wichtiger IT-Systeme ist bis zu einem Tag überbrückbar, darüber hinaus wären Beeinträchtigungen der Auftragsabwicklung riskant.

In Abwägung der Gefährdungen, der Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln sind uns die folgenden Aspekte zur Informationssicherheit besonders wichtig:

1. Geschäftsprozesse, Anwendungen und Informationstechnik müssen sorgfältig durchdacht werden und einfach zu steuern bleiben. Komplexe Strukturen, die zu unnötigen Risiken führen, sind zu vermeiden.
2. Informationssicherheit erfordert nicht nur organisatorische und technische Maßnahmen, sondern auch, dass sich alle Mitarbeiter der möglichen Gefährdungen bewusst sind und sich sicherheitsgerecht verhalten. Dazu sollen regelmäßige Fortbildungsmaßnahmen zur Informationssicherheit beitragen.
3. Die Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen sind zu schützen. Auch im Umgang mit elektronischen Dokumenten und Informationen sind Geheimhaltungsanweisungen strikt zu befolgen.
4. Die für das Unternehmen relevanten Gesetze und Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen müssen eingehalten werden.
5. Ziel ist, die Sicherheit der Informationstechnik (gleichwertig neben Leistungsfähigkeit und Funktionalität) im Unternehmen aufrechtzuerhalten, so dass die Geschäftsinformationen bei Bedarf verfügbar sind. Ausfälle der IT haben Beeinträchtigungen des Unternehmens zur Folge. Lang andauernde Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag führen, sind nicht tolerierbar.
6. Durch Sicherheitsmängel im Umgang mit IT verursachte Ersatzansprüche, Schadensregulierungen und Image-Schäden müssen verhindert werden.
7. Gebäude und Räumlichkeiten des Unternehmens werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu den IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Informationen durch ein restriktives Berechtigungskonzept geschützt.
8. Es ist darauf zu achten, dass bei Investitionen die Belange der Informationssicherheit angemessen berücksichtigt sind.

9. Die Übergänge zu externen Kommunikationsnetzen sind besonders zu schützen. Dies betrifft auch Fernwartungszugänge. Solche Eingänge in das Netz der BruderhausDiakonie-Werkstätten – Digitalisierung - dürfen nur abgestimmt geöffnet werden. Zugriffe und durchgeführte Aktionen sind zu protokollieren.
10. Die Informationstechnik in der BruderhausDiakonie-Werkstätten – Digitalisierung - wird direkt individuell von hier administriert, unabhängig von der zentralen IT-Abteilung der BruderhausDiakonie.
11. Die BruderhausDiakonie-Werkstätten – Digitalisierung - muss in der Lage sein, rasch auf Krisen reagieren zu können. Der Bereich setzt daher ein umfassendes Notfall-Management ein, es dient da dazu um auch bei gravierenden Unterbrechungen seine wesentlichen Geschäftsprozesse so schnell wie möglich wieder aufnehmen zu können.
12. Bei der Entwicklung von Konzepten und der Einführung von Maßnahmen zur Informationssicherheit orientieren wir uns an allgemein anerkannten Standards, zum Beispiel der IT-Grundschutz-Vorgehensweise und den Empfehlungen des BSI-Standards 100-4 zum Notfall-Management

12.3. Organisationsstruktur für Informationssicherheit

- Damit Informationssicherheit in unserem Bereich dauerhaft den erforderlichen Stellenwert besitzt, koordiniert die Verantwortliche für den Bereich Digitalisierung alle Arbeiten zur Informationssicherheit. Der Inhaber dieser Aufgabe ist in dieser Funktion unmittelbar der Leitung der BruderhausDiakonie-Werkstätten – Digitalisierung - unterstellt und ist verpflichtet, ihr regelmäßig über den Stand, Probleme und aktuelle Vorhaben zur Informationssicherheit zu berichten.
  Die Verantwortlichen der Abteilung Digitalisierung sind frühzeitig bei allen Investitionsentscheidungen und Projekten beteiligt, die die Belange der Informationssicherheit berühren.
- Die externe Datenschutzbeauftragte ist hier in beratender Funktion tätig.
  Zu den Aufgaben dieser Arbeitsgruppe gehört es, Konzepte zur Informationssicherheit weiter zu entwickeln und diesbezügliche Entscheidungen vorzubereiten.
- Für die geschäftlich relevanten Informationen ist Frau Ponath-Schütz benannt. Sie ist verantwortlich für die Einschätzung der geschäftlichen Bedeutung (der Information, Technik), für die sichere Nutzung und Kontrolle, inklusive der Einhaltung von Sicherheitsgrundsätzen, Standards und Richtlinien. Der „Eigentümer“ definiert die erforderliche Zugänglichkeit (der Information, Technik) sowie Art und Umfang der Autorisierung. Er ist für die Verwaltung der zustehenden Zugriffsrechte der Benutzer verantwortlich und gegenüber der Leitung in Rechenschaftspflicht.
- Jeder Mitarbeiter soll im Rahmen seines Umgangs mit Informationen und Informationstechnik (als Benutzer, Berater, Geschäftspartner) die erforderliche

Integrität und Vertraulichkeit von Informationen sowie Verbindlichkeit und Beweisbarkeit von Geschäftskommunikation gewährleisten und die Richtlinien des Unternehmens einhalten. Unterstützt durch sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten Sicherheitsvorfälle von innen und außen vermeiden. Erkannte Fehler sind dem Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

12.4. Verstöße und Sanktionen

Jeder Beschäftigte im Bereich der BruderhausDiakonie-Werkstätten – Digitalisierung - ist zu einem sorgfältigen Umgang mit den Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen verpflichtet. Beabsichtigte oder grob fahrlässige Verletzungen der Informationssicherheit, zum Beispiel

- Der Missbrauch von Daten, der finanziellen Verlust verursachen kann.
- Der unberechtigte Zugriff auf Informationen oder ihre Änderung und unbefugte Übermittlung,
- die illegale Nutzung von Informationen aus dem Unternehmen oder
- die Gefährdung der Informationssicherheit anderer Unternehmen oder Institutionen,

können disziplinarische Folgen bis hin zur Kündigung des Arbeitsverhältnisses, gegebenenfalls auch straf- und zivilrechtliche Konsequenzen haben. Bei finanziellem Schaden können Haftungsansprüche und Regressforderungen geltend gemacht werden.

Anlagen

Anlage 1: Vorlage Verfahrensbeschreibung

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Hauptniederlassung: ☐ ja ☐ nein

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel

Name, Vorname

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Bezeichnung der Verarbeitungstätigkeit	Anlage
Datum der Anlegung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	
Bezeichnung der Verarbeitungstätigkeit	

Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien	☐ ☐ ☐ Sonstige : Besondere Arten personenbezogener Daten: ☐

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden	☐ intern Abteilung/ Funktion
	☐ extern Empfängerkategorie
Datenübermittlung Nennung der konkreten Datenempfänger Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	☐Datenübermittlung findet nicht statt und ist auch nicht geplant ☐Datenübermittlung findet wie folgt statt: ☐Drittland, Name: ☐internationale Organisation, Bezeichnung: Empfängerkategorie Dokumentation geeigneter Garantien

Fristen für die Löschung der verschiedenen Datenkategorien	

Technische und organisatorische Maßnahmen (TOM) gemäß Artikel 32 Abs.1 DSGVO Bemerkungen*: siehe TOM-Beschreibung*

……	……	.....
Verantwortlicher	Datum	Unterschrift

Anlage 2: Vorlage Datenträgerprotokoll

Datenträgerprotokoll

Datenträgerbestand		Verwendet seit	Weitergabe		gelöscht	vernichtet
Bezeichnung	Inhalt	Datum	Datum	An Kunde	Datum	Datum

Anlage 4: Muster Verpflichtungserklärung Einhaltung datenschutzrechtlicher Anforderungen Mitarbeiter

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO) für Mitarbeiter

Frau/Herr

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

_____

Ort, Datum

_____ _____

Unterschrift des Verpflichteten Unterschrift des Verantwortlichen

Anlage zur Vereinbarung nach Art. 28 DSGVO:

Technisch-organisatorische Maßnahmen

Der Auftragnehmer weist durch entsprechende Dokumentation seine getroffenen technischen und organisatorischen Maßnahmen zur Datenschutzorganisation und IT-Sicherheit nach:

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

I.1 Zutrittskontrolle

Unter der Zutrittskontrolle werden die Maßnahmen verstanden, die implementiert sind, um Unbefugten den physischen Zutritt zu Datenverarbeitungssystemen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Die Zutrittskontrolle wird gewährleistet durch:

- **Besucher werden an der Pforte in Empfang genommen. Von da werden sie zum Bereich Digitalisierung begleitet. Jeder Kunde, Besucher und Mitarbeiter unterschreibt eine Datenschutzerklärung, bevor er die Bearbeitungszone betritt.**
- **Die Räume des Auftragnehmers befinden sich Am Heilbrunnen 100, 72766 Reutlingen siehe § 2 (1) der Leistungsvereinbarung („Scanraum“). Die Türen der Produktionsräume sind mit Sicherheitsschlössern und einer biometrischen Zugangskontrolle versehen. Türen und Fenster sind außerhalb der Betriebszeiten fest verschlossen.**
- **Die Schlüssel zum Scanraum, in denen die Auftragsdokumente aufbewahrt, verarbeitet oder ggf. vernichtet werden, befinden sich in der ausschließlichen Obhut der zuständigen Mitarbeitenden des Auftragnehmers. Dritte haben zu den Räumlichkeiten keinen Zutritt. Die Vergabe von Schlüsseln an die zuständigen Mitarbeitenden ist schriftlich geregelt.**
- **Der Zugang zu den Räumlichkeiten mit den Systemen ist nur für autorisierte Personen möglich. Berechtigt sind alle Mitarbeiter des Scan-Service, deren Berechtigungen hierzu nachprüfbar dokumentiert sind.**
- **Der Serverschrank befindet sich in einem geschlossenen Serverraum. Zugang haben lediglich die Administratoren. Beim Verlassen des Serverraums wird die Tür abgeschlossen, um den Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen für Unbefugte zu verhindern.**
- **Der Bereich, in dem die Kundenaufträge bearbeitet werden, ist räumlich von der Publikumszone getrennt und mit einer per Fingerscan bzw. Code-Karten gesicherten Tür verschlossen.**

Initials _____

I.2 Zugangskontrolle

Unter der Zugangskontrolle werden die Maßnahmen verstanden, die implementiert sind, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können, etwa durch. Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzer-stammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung. Die Zugangskontrolle wird gewährleistet durch:

- **Der elektronische Zugang zu Systemen des Scan-Service via Netzwerk ist nach heutigen technischen Standards gesichert. Zugangsdaten zu Serversystemen sind nur Administratoren der Digitalisierung oder Ihren Vertretern bekannt.**
- **Die Rechner werden automatisch gesperrt, sobald sie nicht benutzt werden, so dass keine betriebsfremden Personen zufällig Einblick in die betrieblichen Daten erlangen können.**
- **Die Passwörter werden alle 6 Wochen geändert, müssen 8-stellig sein und Groß- und Kleinbuchstaben sowie entweder Zahlen oder Sonderzeichen enthalten.**
- **Räume, Container und Schränke, in denen Daten unter Verschluss gehalten werden, werden direkt nach Benutzung wieder verschlossen. Die Besitzer der Schlüssel sind in einer Schlüsselkartei erfasst.**

I.3. Zugriffskontrolle

Die Zugriffskontrolle umfasst die Maßnahmen, die implementiert sind, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle wird gewährleistet durch:

- **Datenübertragungen finden über gesicherte und verschlüsselte Leitungen per SFTP und VPN statt. Ein Netz-Passwort ist vorhanden. Der Passwortschutz ist auf dem Server eingerichtet.**
- **Sobald die Datenträger vom Kunden zum Löschen freigegeben sind, werden sie mit einer speziellen Software zur Datenlösung 35x überschrieben.**
- **Rechner werden automatisch gesperrt, sobald sie nicht benutzt werden. Einblick in die Daten ist dann nur mit Passwort möglich.**
- **Nicht mehr benötigte Betriebsmittel wie Datenträger werden so entsorgt, dass ein Rekonstruieren der Inhalte nicht mehr möglich ist. CD´s werden geschreddert, Papierdokumente von der Firma Leins professionell entsorgt.**
- **Die Verwendung von elektronischen Speichermedien ist nicht möglich, da die Laufwerke hierfür gesperrt sind.**

I.4. Trennungskontrolle

Das Trennungsgebot verlangt die Implementierung von Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Die folgenden Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken sind implementiert. Die Trennungskontrolle wird gewährleistet durch:

- **Interne Mandantenfähigkeit / Zweckbindung**
- **Funktionstrennung /Produktion / Test)**

I.5 Pseudonymisierung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO). Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- **Kunden- und Auftragsnummern gewährleisten die Pseudonymisierung der personenbezogenen Daten.**

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

II.1. Weitergabekontrolle

Unter der Weitergabekontrolle werden die Maßnahmen verstanden, die implementiert sind, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports und ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dabei insbesondere folgende Aspekte der Weitergabe personenbezogener Daten zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle. Die Weitergabekontrolle wird gewährleistet durch:

- **Die Weitergabe der Daten erfolgt über einen sftp-Server. Das interne Netzwerk des Scan-Service hat keinerlei Verbindung nach außen.**
- **Alle Aufträge werden nach Kundenwunsch entsprechend der vergebenen Rechte getrennt voneinander verarbeitet und gespeichert.**
- **Datenträger werden sachgerecht und vor unbefugtem Zugriff geschützt aufbewahrt.**
- **Von Dritten erhaltene Datenträger werden auf Computer-Viren überprüft.**
- **Die Belege werden in verschlossenen Gitterboxen angeliefert. Im Wareneingang des Scanbereichs wird jeder Vorgang erfasst und mit einem Laufzettel ausgestattet. Jeder Vorgang hat seine eigene Box in der ein Laufzettel bis zum letzten Arbeitsgang enthalten ist.**

II.2. Eingabekontrolle

Unter der Eingabekontrolle werden die Maßnahmen verstanden, die implementiert sind, damit nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird gewährleistet durch:

- **Da jeder Mitarbeiter sich mit seinem persönlichen Passwort einloggt, ist gewährleistet, dass auch nachträglich festgestellt werden kann, wann und von wem personenbezogene Daten erfasst, verändert oder entfernt worden sind. Die Dokumentation erfolgt zum Kundendatensatz und ist durch den Auftraggeber nicht manipulierbar.**

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

III.1. Verfügbarkeitskontrolle

Unter der Verfügbarkeitskontrolle werden die Maßnahmen verstanden, die implementiert sind, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Die Verfügbarkeitskontrolle wird gewährleistet durch:

- **Über Systemeinrichtungen und Verfahren gewährleistet der Scan-Service der BruderhausDiakonie – Werkstätten, dass auftrags- sowie personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.**
- **Die Datensicherungen finden 4 x täglich als Volumen-Schattenkopie statt und 1x täglich ein komplettes Backup auf eine externe Festplatte. Die Sicherheitskopien werden sowohl auf dem Server als auch auf Datenträgern im Tresor aufbewahrt. Auf diese Weise wird zufälliger Datenschutz verhindert. Eine USV-Anlage schützt die IT-Anlage außerdem vor Datenverlust.**

III.2 Rasche Wiederherstellbarkeit

Die tägliche Datensicherung je Mandant wird zeitgesteuert nach Vorgabe des Vertragspartners durchgeführt. Die Daten werden auf physikalisch getrennten Speichermedien vorgehalten.

- **Alle IT- und Scannsysteme werden in einem regelmäßigen Rhythmus auf Funktion und Belastbarkeit überprüft. Die tägliche Datensicherung wird zeitgesteuert durchgeführt.**

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

IV.1 Auftragskontrolle

Unter der Auftragskontrolle werden die Maßnahmen verstanden, die implementiert sind, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des AG verarbeitet werden können. Die weisungsgemäße Auftragsdatenverarbeitung wird gewährleistet durch:

- **Auf Basis der Datenschutzerklärung zur Auftragsdatenverarbeitung wird gewährleistet, dass die Verarbeitung von personenbezogenen Daten durch die BruderhausDiakonie – Werkstätten, Scan-Service, nur entsprechend der Weisungen des Vertragspartners durchgeführt wird.**

IV.2 Datenschutz-Management

siehe Datenschutz-Konzept (Anlage)

IV.3 Incident-Response-Management/ Notfall-Management

siehe Datenschutz-Konzept (Anlage): 10. Leitlinie zur Informationssicherheit und Sicherheitskonzept

Initials _____

SCAMITEC-ESSLINGEN
DR. KIENLIN GMBH

SCANNEN MIKROVERFILMEN
INFORMATIONSTECHNOLOGIEN

SCAMITEC-ESSLINGEN
DR. KIENLIN GmbH
Limburgstraße 35
73 734 Esslingen
TEL: 0711 / 35 36 35
FAX: 0711 / 35 35 12
www.scamitec.de
HRB 213744

Landratsamt Reutlingen
- Hauptamt -

z.Hd. Herrn Kehrer
Bismarckstr. 47

72764 Reutlingen

Ihre Zeichen	Ihre Nachricht vom	Unsere Zeichen	Datum
Hr. Kehrer	Mail 19.09 .2018	LK -Ed KU/ LRA_RT_DSGVO.doc	20. September 2018
Tel.: 07121 - 480- 0 /1214	Fax -1800	Lars.Kienlin@scamitec.de	
M.Kehrer@Kreis-Reutlingen.de			

DSGVO (TOM)

Sehr geehrter Herr Kehrer,

wie von Ihnen gewünscht, teilen wir Ihnen unsere technischen und organisatorischen Maßnahmen (TOM) für die sichere Verarbeitung personenbezogener Daten mit:

DATENSCHUTZKONZEPT

- Alle Mitarbeiter sind schriftlich zur Geheimhaltung (BDSG/DSGVO) verpflichtet.
- Zutritt zu unseren Geschäftsräumen ist nur autorisierten Personen gestattet. Wir haben keinen Publikumsverkehr.
- Aktentransporte werden datenschutzkonform durch eigenes Personal in eigenen geschlossenen Fahrzeugen durchgeführt.
- Wir setzen LINUX-Server ein, die über einen Lancom-Router mit dem Internet verbunden und durch Firewalls abgeschirmt sind. Wir verwenden kein WLAN (Funknetz).
- Der Datenserver verwendet ein RAID-5 zur sicheren Datenspeicherung.
- Alle Scandaten werden grundsätzlich an den Scansystemen im ersten Schritt lokal gespeichert, wobei dies je nach Weiterverarbeitung redundant erfolgt.
- Zur Weiterverarbeitung und Qualitätskontrolle werden die Daten auf den Server kopiert, wo sie je nach Verarbeitung in mehreren Versionen abgespeichert werden.
- Relevante Zwischenversionen werden zusätzlich lokal an Datenerfassungs- oder Kontrollarbeitsplätzen gespeichert.
- Fertig bearbeitete und an Kunden übergebene Daten werden auf einem NAS und externen HDs gespeichert.
- Datenübertragung erfolgt nur per SFTP oder verschlüsselte Datenträger.
- Alle Speicherschritte und Orte werden nach einem definierten Schema durchgeführt und parallel dokumentiert.
- Datenlöschungen werden nach kundenspezifisch oder gesetzlich vorgeschriebenen vordefinierten Zeiträumen durchgeführt und dokumentiert.

Wir hoffen, Ihnen hiermit ausführliche Informationen geben zu können.

Als Referenzen für die Verarbeitung von personenbezogene Akten können wir Ihnen z.B. das Personalamt der Stadt Esslingen, das Robert-Bosch-Krankenhaus oder die SWSG (Siedlungs- und Wohnungsbau Stuttgart GmbH) nennen.

Falls Sie weitergehende Fragen haben, können Sie uns gerne kontaktieren, damit wir diese direkt klären können.

Mit freundlichen Grüßen

SCAMITEC-ESSLINGEN
DR. KIENLIN GMBH

Lars Kienlin
Geschäftsführer

Anlage: Erklärung über die Einhaltung der Datenschutzgrundverordnung

DATENSCH.DOC

DATENSCHUTZ

Erklärung über die Einhaltung der Datenschutzgrundverordnung (DSGVO)
bei der Einscannung und Mikroverfilmung durch
SCAMITEC-ESSLINGEN
DR. KIENLIN GMBH

1. SCAMITEC-ESSLINGEN hat einen Datenschutzbeauftragten bestellt.

2. Alle bei SCAMITEC-ESSLINGEN beschäftigten Personen sind schriftlich zur Geheimhaltung verpflichtet worden.

3. SCAMITEC-ESSLINGEN hat alle technischen und organisatorischen Maßnahmen getroffen, damit zu scannendes und zu verfilmendes Material und Daten während des Transports und des Verbleibs im Unternehmen vor dem Zugriff unbefugter Personen gesichert sind.

4. Unbefugten ist der Zugang zu den Datenverarbeitungsanlagen und den Mikrofilm-, bzw. Scan-Abteilungen verwehrt.

5. Die unbefugte Kenntnisnahme, Veränderung oder Vernichtung von Daten wird verhindert.

6. Bei SCAMITEC-ESSLINGEN werden von den bei der Be- und Verarbeitung beteiligten Personen Auftragsprotokolle geführt, wodurch eine durchgängige Überprüfung ermöglicht wird.

7. Es ist sichergestellt, daß keine weiteren als die in Auftrag gegebenen Originale oder Kopien erstellt werden.

8. Daten und Unterlagen werden bei SCAMITEC-ESSLINGEN ausschließlich an die vom Auftraggeber benannten Personen übermittelt.

9. SCAMITEC-ESSLINGEN vernichtet Probeverfilmungen, Testfilme, fehlerhafte Filme grundsätzlich mit einer speziellen Mikrofilmvernichter, fehlerhafte Rückvergrößerungen mit einem Aktenvernichter. Scan-Dateien werden unwiederbringlich gelöscht.

10. Das vom Auftraggeber schriftlich zur Vernichtung freigegebene Material wird durch SCAMITEC-ESSLINGEN nach DSGVO vernichtet.

SCAMITEC-ESSLINGEN
DR. KIENLIN GMBH