



Hochschule Neubrandenburg

University of Applied Sciences

Fachbereich Agrarwirtschaft und Lebensmittelwissenschaften

Die Datenschutz-Grundverordnung (DS-GVO) in der Sozialen Arbeit am Beispiel des Gartenhaus e.V.

Bachelor-Thesis

Studiengang Angewandte Betriebswirtschaftslehre

vorgelegt von

Nehls, Thomas

Urn:nbn:de:gbv:519-thesis2018.0415.1

Ort und Datum der Abgabe: Stralsund, den 16.07.2018

Betreuer: Prof. Dr. C. Fuchs und Prof. Dr. R. Northoff

Inhaltsverzeichnis

Abbildungsverzeichnis	III
Abkürzungsverzeichnis	IV
1 Einleitung	1
1.1 Problemstellung	2
1.2 Zielstellung	3
1.3 Vorgehensweise	4
2 Rechtliche Grundlagen	4
2.1 Historie zu DS-GVO und BDSG	4
2.2 Anwendungsbereich Art. 2 und 3 i. V. m. Art. 4 DSGVO	5
3 Material und Methoden	6
3.1 Grundsätze für personenbezogene Daten in der Sozialen Arbeit	6
3.2 Rechtsbeziehungen Leistungsberechtigter, -träger, -erbringer	8
3.3 Grundsätze für die Verarbeitung Art. 5 DS-GVO	10
3.4 Rechtmäßigkeit der Verarbeitung Art. 6,7 DS-GVO	11
4 Vorstellung „Gartenhaus“ Psychosozialer Träger e.V.	13
5 Datenverarbeitung, -speicherung und Datensicherheit	14
5.1 Rolle und Bedeutung des Datenschutzes	14
5.2 Ausgangssituation im Unternehmen	16
5.2.1 Risikobasiertes Denken DIN EN ISO 9001:2015	16
5.2.2 Der betriebliche Datenschutzbeauftragte	17
6 Herausforderungen durch die EU DS-GVO	19
6.1 Verarbeitung besonderer personenbezogener Daten Art. 9 DS-GVO	19
6.2 Verantwortung für die Verarbeitung Art. 24, 25 DS-GVO	20
6.3 Verzeichnis von Verarbeitungstätigkeiten Art. 30 DS-GVO	21
6.4 Sicherheit der Verarbeitung Art. 32 DS-GVO	22
6.4.1 Verschlüsselung/Pseudonymisierung Art. 32 Abs.1, lit. a	23
6.4.2 Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit	24
6.4.3 Wiederherstellbarkeit Art. 32 Abs.1 lit. c	29
6.4.4 Verfahren zur regelmäßigen Überprüfung Art. 32 Abs. 1 lit. d	29
6.5 Datenschutzfolgeabschätzung (DSFA) Art. 35. DS-GVO	30
6.5.1 Identifizierung von Risiken	31
6.5.2 Risikobeurteilung	33

6.6	Datenverarbeitung Klientendaten	34
6.6.1	Leistungsträger (ITP)	34
6.6.2	Datenverarbeitung durch den Leistungserbringer	36
6.6.3	Kontrollrechte des Leistungsträgers	39
6.6.4	Datenlöschung / Datenträgerentsorgung Klienten	40
6.7	Datenverarbeitung Mitarbeiterdaten.....	41
6.7.1	Abrechnungsrelevante Daten Mitarbeiter	42
6.7.2	Personalentwicklung / Mitarbeiterführung	44
6.7.3	Datenlöschung /Datenträgerentsorgung Mitarbeiter	46
6.7.4	Betriebsrat	47
6.8	Mitgliederverwaltung	48
6.9	Betroffenenrechte	48
6.9.1	Informationspflicht Art. 13 DS-GVO	49
6.9.2	Auskunftsrecht Art. 15 DS-GVO.....	49
6.9.3	Recht auf Berichtigung und Löschung Art. 16, 17 DS-GVO	51
6.9.4	Verletzungen des Datenschutzes Art. 33, 34 DS-GVO	52
6.9.5	Haftungsansprüche Betroffener	53
7	Diskussion und Empfehlung	54
8	Zusammenfassung	59
	Anhang.....	61
	A1 Datenschutzrechtliche Beurteilung von Verarbeitungstätigkeiten (DSFA)	
	A2 Verarbeitungsverzeichnisse	
	A3 technisch organisatorische Maßnahmen (TOM)	
	A4 Qualitätshandbuch	
	A5 Rechtliche Aufklärung zum Datenschutz (ITP/Bogen D)	
	Literaturverzeichnis	62

Abbildungsverzeichnis

Abb. 1	Rechtsbeziehungen im Leistungsfall SGB IX, XII	9
Abb. 2	Grundsätze der Verarbeitung Art. 5 DS-GVO	10
Abb. 3	Rechtmäßigkeit der Verarbeitung Art. 6 DS-GVO	12
Abb. 4	Einrichtungen des „Gartenhaus“ e.V.	14
Abb. 5	Maßnahmen zur Datenintegrität	27
Abb. 6	Bedrohungen im Geschäftsbetrieb	32
Abb. 7	Schadensszenario Datenpanne Klientendaten	34

Abkürzungsverzeichnis

AG	Arbeitsgemeinschaft
Art	Artikel
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnologie
BTHG	Bundesteilhabegesetz
DSFA	Datenschutzfolgeabschätzung
DS-GVO	Datenschutz-Grundverordnung
EU	Europäische Union
EQG	Einrichtungenqualitätsgesetz
ErwGr	Erwägungsgrund
GG	Grundgesetz
HLu	Hilfen zum Lebensunterhalt
IBRP	Integrierter Behandlungs-/ Rehabilitationsplan
IT	Informationstechnologie
ITP	Integrativer Teilhabepan
KdU	Kosten der Unterkunft
LRV	Landesrahmenvertrag
M-V	Mecklenburg-Vorpommern
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
QMH	Qualitätsmanagementhandbuch

1 Einleitung

„Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden Charta) sowie Artikel 16 Absatz 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“

(Erwägungsgrund 1 der Verordnung (EU) 2016/679)

Die zunehmende Digitalisierung persönlicher Daten sowie deren Vernetzung in anwendungsübergreifenden Systemen bieten dem interessierten Nutzer im Alltag viele Vorteile. Im Internet stehen enorme Mengen an Informationen zur Verfügung, zunehmend auch personifiziert, die jeder internetfähige Rechner oder jedes Smartphone permanent und überall abrufen kann. Mit einem Navigationssystem und der GPS-Ortung findet sich der Ortsunkundige auch in fremden Städten zurecht und beim Einkauf an der Supermarktkasse kann der Warenkorb bei Kartenzahlung bestimmten Kundenprofilen zugeordnet werden. Jeder Nutzer dieser technischen Errungenschaften hinterlässt dabei im Internet unsichtbare Spuren, seine personenbezogenen Daten.

„Daten über Menschen, über deren Eigenschaften und deren Verhalten werden heute gekauft und verkauft. Der Einzelne wird hierbei Objekt wirtschaftlicher Interessen im globalen Maßstab.“ (Wächter, 2017, S.6f)

Der Einsatz moderner Techniken in der Informationstechnologie schafft in einem erheblichen Umfang Gefährdungen für die Privatsphäre des Einzelnen. Durch die breite Verfügbarkeit digitaler Daten sowie deren Vernetzung zwischen verschiedenen Anwendern besteht eine immer größer werdende Gefahr von nichtautorisierten Verarbeitungsvorgängen. Die Verbraucherschützer sind alarmiert.

Der Art. 2 Abs. 1 GG umfasst zusammen mit Art. 1 Abs. 1 GG die freie Entfaltung der Persönlichkeit unter dem Schutz des Einzelnen vor einem Missbrauch seiner persönlichen Daten. Weitere umfangreiche Regelungen hierzu enthält national das Bundesdatenschutzgesetz (BDSG) und europaweit rechtsverbindlich ab 25.05.2018 auch die europäische Datenschutz-Grundverordnung (DS-GVO).

Diese gesetzlichen Regelungen sollen in ihrer Gesamtheit alle Betroffenen in die Lage versetzen, in einem hohen Maß über ihre persönlichen Daten zu bestimmen und sie vor nichtautorisierter Weitergabe und Verarbeitung schützen. Alle Bürger der EU sind nun im gleichen Maße in der Lage versetzt, jederzeit von jedem Datenverarbeiter, ganz gleich in welchem Land der EU er seinen Sitz hat, zu erfahren, was über ihn gespeichert ist und zu welchem Zweck.

Auch in der Branche Gesundheitsdienst und Wohlfahrtspflege werden personenbezogene Daten erhoben und verarbeitet. Damit können den Patienten und Klienten optimale Hilfe und Unterstützung bei ihren spezifischen Einschränkungen zu Teil werden. Um die großen Datenmengen an Gesundheitswerten erfassen und auswerten zu können und um den beteiligten Fachkräften einen Zugriff auf einheitliche Datenbanken des Patienten/Klienten zu ermöglichen, ist es auch hier notwendig geworden, das riesige Potential der digitalen Verarbeitung nutzbar zu machen.

1.1 Problemstellung

Nach mehr als zweijähriger Übergangszeit wurden die Neuregelungen der europäischen Datenschutz-Grundverordnung (DS-GVO) am 25.05.2018 in allen europäischen Mitgliedsstaaten rechtlich verbindlich. Die nationalen Gesetzgeber hatten die Aufgabe, die Forderungen der DS-GVO in nationales Recht (BDSG) umzusetzen. Nach der Übergangszeit sollten neben den Mitgliedsstaaten der EU auch die privatgewerblichen Anwender von Datenverarbeitungen in der Lage sein, sich entsprechend rechtlich zu orientieren und rechtskonform aufzustellen.

Haben sich die Unternehmen in Deutschland nun ausreichend darauf vorbereitet? Wie wirken sich die Regelungen der DS-GVO bspw. in Gesundheitsdienst und Wohlfahrtspflege aus? Müssen Aufbau- und Ablauforganisation von Helfersystemen, hier speziell im Beispielunternehmen (Anspruchsberechtigte nach SGB XII/6.Kap.) neu strukturiert werden? Welche qualitativen und quantitativen Veränderungen hinsichtlich Datenschutz und Datensicherheit sind notwendig, um den Anforderungen aus der Umsetzung des Bundesteilhabegesetzes (BTHG) unter Berücksichtigung der DS-GVO in der Sozialen Arbeit zu entsprechen?

„Die Bedeutung der Gewährleistung des Datenschutzes im Gesundheits- und Sozialwesen (GSW) erklärt sich aus dem Umstand, dass seine Verletzung in diesem Bereich unmittelbar die soziale Stellung und die physische und psychische Unversehrtheit des betroffenen Menschen bedrohen kann.“ (Bake et.al, 2004, S.6)

Welche zentrale Bedeutung in Bezug auf die Erhebung, Verarbeitung und Sicherheit personenbezogener (Klienten)Daten nimmt dabei in Mecklenburg-Vorpommern die Einführung des Integrierten Teilhabepfandes (ITP) ein?

1.2 Zielstellung

Ziel der Thesis ist eine Darstellung der besonderen Anforderungen an die Erhebung, Verarbeitung, Speicherung und Löschung personenbezogener Daten in der Sozialen Arbeit im Beispielunternehmen. In der sozialen Arbeit ist die Quantität und Qualität der benötigten Daten für die personenzentrierte Hilfe von entscheidender Bedeutung. Die öffentlichen und freien Träger von Gesundheitsdienst und Wohlfahrtspflege sind vertraglich verpflichtet, entsprechend ihrer Leistungs- und Prüfungsvereinbarung, § 75 Abs. 3 Nr. 1, 3 SGB XII i. V. m. Landesrahmenvertrag Mecklenburg-Vorpommern (LRV) gem. § 79 Abs. 1 SGB XII die vereinbarte Qualität in der Betreuung anzubieten und umzusetzen.

Mit einer Betrachtung des IST-Zustandes in den Bereichen Datenschutz und Datensicherheit im Beispielunternehmen soll im Vergleich mit den Soll-Werten aus der DS-GVO eine Analyse mit anschließender Auswertung erfolgen. Der Umgang mit personenbezogenen Daten erfordert verbindliche Handlungsleitlinien für die Beschäftigten im Rahmen von Datenschutz und Datensicherheit im Unternehmen. Die Darstellung der Geeignetheit der strukturellen Voraussetzungen (Aufbau- und Ablauforganisation) beim Gartenhaus e.V. unter Anwendung der Anforderungen aus DS-GVO und BDSG soll helfen, entsprechende Schwachstellen zu identifizieren, Verbesserungspotentiale zu erkennen und geeignete Maßnahmen zur Erfüllung der Konformität zu entwickeln.

Ziel dabei soll sein, die Notwendigkeit und Vielfalt der personenbezogenen Daten in der sozialen Arbeit in Übereinstimmung zu bringen mit dem Datenschutz im Interesse der dem Helfer anvertrauten Klienten.

1.3 Vorgehensweise

Nach der Darstellung der Anforderungen aus DS-GVO und BDSG (in seiner Fassung vom 30.06.2017) sowie deren Bewertung hinsichtlich der Relevanz im Beispielunternehmen sollen signifikante Untersuchungspunkte identifiziert werden. An diesen Punkten erfolgen Datenschutzfolgeabschätzungen (DSFA), die dann zur Ableitung konkreter Handlungsleitlinien im Beispielunternehmen dienen. In diesen Folgeabschätzungen werden datensensible Prozesse hinsichtlich der Eintrittswahrscheinlichkeit von Datenverlusten bzw. zu erwartender Schadenshöhen analysiert. Zu den relevanten Verfahren im Rahmen der Verarbeitung personenbezogener Daten werden Verzeichnisse erstellt. Diese dienen der Darstellung der Prozesse hinsichtlich der Verantwortlichkeiten bei der Verarbeitung der Daten.

Eine Betrachtung des für die Soziale Arbeit notwendigen Datenmaterials, ohne Nennung konkreter personenbezogener Daten, soll unter Beachtung der Einführung des Integrierten Teilhabeplanes (ITP) erfolgen. Eine Einordnung des ITP hinsichtlich seiner Funktion in der Sozialen Arbeit wird in Kap. 3.1 vorgenommen.

Weiterhin werden vorhandene technisch organisatorische Maßnahmen (TOM) hinsichtlich der Aktualität des technischen Standes, deren Effektivität und der Angemessenheit untersucht.

Ausgewählte systemrelevante Prozesse in der Betreuungsarbeit im Gartenhaus e.V. sollen analysiert und hinsichtlich des Eintretens möglicher Schäden sowie deren Auswirkungen (Eintrittswahrscheinlichkeit und Schadenshöhe) bewertet werden. Ziel der Untersuchungen soll die Ableitung geeigneter Maßnahmen im Unternehmen zur Verbesserung der Prozesse sein.

2 Rechtliche Grundlagen

2.1 Historie zu DS-GVO und BDSG

Die Verordnung (EU) 2016/679 mit dem Kurztitel „Datenschutz-Grundverordnung“ ist am 24.05.2016 (Abl. EU 04. Mai.2016 L 119 S. 1f) in Kraft getreten. Sie hob damit die Richtlinie 95/46/EG aus dem Jahr 1995 auf. Im Gegensatz zur vorherigen Richtlinie gilt die DS-GVO ab 25.05.2018, nach einer zweijährigen Überleitungsfrist, sofort mit Inkrafttreten zwingend in allen EU-Mitgliedsstaaten.

Der deutsche Gesetzgeber hat mit dem Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU) eine neue Fassung des Bundesdatenschutzgesetzes (BDSG) auf den Weg gebracht und zeitgleich mit der DS-GVO am 25.05.2018 in Kraft gesetzt. Damit gelten die beiden gesetzlichen Rahmenwerke uneingeschränkt für alle nationalen Anwender im Inland. Erweitert wurden die 99 Artikel der DS-GVO mit 173 Erwägungsgründen (ErwGr.) um der Erläuterung der Ziele und Zwecke der Verordnung mehr Raum geben zu können.

Ziele der Verordnung sollen neben dem Schutz personenbezogener Daten (Kap. 1, Art. 1 Abs. 2 DS-GVO) eine europaweite Harmonisierung des Datenschutzes für einen freien Verkehr personenbezogener Daten (Kap. 1 Art. 1 Abs. 3 DS-GVO) sein. Damit wurde ein Schutzniveau geschaffen, das in erster Linie natürlichen Personen dienen soll. Bei juristischen Personen findet die Verordnung nur Anwendung, wenn z.B. im rechtlichen Rahmen persönliche Daten von Gesellschaftern einer Unternehmung betrachtet werden sollen.

Das neue Bundesdatenschutzgesetz (BDSG-neu), beschlossen im deutschen Bundestag am 27.04.2017, ist in 3 Abteilungen gegliedert. Teil 1 enthält Regelungen für jede Datenverarbeitung, unabhängig von DS-GVO oder anderen Zwecken, Teil 2 bezieht sich ausschließlich auf die DS-GVO und Teil 3 stellt die Richtlinien für Polizei und Justiz dar. Im Nachfolgenden wird die Rechtsquelle „BDSG“ immer in der Fassung vom 30.06.2017 zitiert. Erfolgen Verweise auf die Vorgängerversion, sind gekennzeichnet mit BDSG aF.

2.2 Anwendungsbereich Art. 2 und 3 i. V. m. Art. 4 DS-GVO

Der *sächliche Anwendungsbereich* für das Beispielunternehmen bestimmt sich nach Art. 2 Abs. 1 1. Hs. DS-GVO durch „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten“. Die Definitionen der Begrifflichkeiten „personenbezogene Daten“ und „Verarbeitung“ regelt Art. 4 Nr. 1, 2 DS-GVO.

Danach sind „personenbezogene Daten“ Informationen zu direkt identifizierbaren Personen hinsichtlich bestimmter Merkmale. Diesen Sachverhalt im Beispielunternehmen stellen die Klienten mit ihren Diagnosen, Hilfeplänen und Entwicklungsberichten sowie die Mitarbeiter mit ihren Personalstammdaten, Abrechnungen und Bankverbindungen dar.

Mit dem Vorgang der „Verarbeitung“ (Art. 4 Nr. 2) ist das Erheben und Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten beschrieben. Alle die hier aufgeführten Vorgänge werden im Rahmen der sozialen Arbeit am Klienten sowie in der Mitarbeiterabrechnung relevant. Durch die Erstellung von zusätzlichen Klienten- und Mitarbeiterakten in Papierform ist auch der zweite Halbsatz des Art. 2 Abs. 1 DS-GVO bestimmend: „sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“. Keine Anwendung findet die DS-GVO gem. Art. 2 Abs. 2 lit. c bei rein privaten Datenverarbeitungen.

Der *räumliche Anwendungsbereich* wird durch Art. 3 Abs. 1 DS-GVO mit „Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union“ definiert. Dies trifft für das Beispielunternehmen sowohl für den Sitz der Unternehmung am Ort des Vereinsregister Stralsund, Bundesrepublik Deutschland, und gleichzeitig auch mit den Tätigkeitsbereichen innerhalb des Landkreises Vorpommern-Rügen zu.

3 Material und Methoden

3.1 Grundsätze für personenbezogene Daten in der Sozialen Arbeit

Zur Erläuterung soll zunächst der anspruchsberechtigte Personenkreis sowie deren Mitwirkungspflichten anhand nationaler Gesetzgebung dargestellt werden.

Im § 53 Abs. 1 SGB XII, wird der Leistungsberechtigte wie folgt beschrieben:

„Personen, die durch eine Behinderung im Sinne von § 2 Abs. 1 Satz 1 des Neunten Buches wesentlich in ihrer Fähigkeit, an der Gesellschaft teilzuhaben, eingeschränkt oder von einer solchen wesentlichen Behinderung bedroht sind, erhalten Leistungen der Eingliederungshilfe, wenn und solange nach der Besonderheit des Einzelfalles, insbesondere nach Art oder Schwere der Behinderung, Aussicht besteht, dass die Aufgabe der Eingliederungshilfe erfüllt werden kann. Personen mit einer anderen körperlichen, geistigen oder seelischen Behinderung können Leistungen der Eingliederungshilfe erhalten.“

Leistungen der Eingliederungshilfe nach dem Bundesteilhabegesetz können nur nach genauer Untersuchung der Lebensumstände bei sachkundiger Bewertung der Teilhabeeinschränkungen gewährt werden. Dazu ist eine Mitwirkung des Einzelnen, im Regelfall des Hilfesuchenden selbst oder seines gesetzlichen Betreuers, notwendig. Diese Mitwirkungspflicht für den Hilfesuchenden ergibt sich gegenüber dem zuständigen Leistungsträger aus den §§ 60 ff. SGB I. Danach hat der Hilfesuchende alle Tatsachen anzugeben, die für die Gewährung der Hilfen relevant sind. Welche Tatsachen dies im Einzelfall sind, kann der Hilfesuchende aber oftmals gar nicht einschätzen. Festgestellte Defizite müssen dann vom zuständigen Sachbearbeiter des Leistungsträgers oder aber vom Bezugsbetreuer beim Leistungsberechtigten durch eine gezielte und fachkundige Befragung ausgeglichen werden.

Um den regional zuständigen Leistungsträgern ein Instrument zur sachgerechten Datenerhebung an die Hand zu geben, wurde in Mecklenburg-Vorpommern auf Beschluss des Sozialministeriums zum 01.01.2018 der „Integrierte Teilhabeplan“ (ITP) eingeführt. Der ITP wurde vom Institut für personenzentrierte Hilfen GmbH, Fulda, entwickelt und soll ein Verfahren zur Feststellung von Hilfebedarfen bei Menschen mit Behinderungen auf Grundlage persönlicher Zielsetzung, Ressourcen und Beeinträchtigungen sein.

Er ersetzt den bislang gültigen Integrierten Behandlungs- und Rehabilitationsplan (IBRP). Die bisherige Verfahrensweise bis zum 31.12.2017 sah vor, dass regelmäßige Hilfeplankonferenzen mit Vertretern des Leistungsträgers, der Leistungserbringer sowie den jeweiligen Klienten, ggf. mit einer Vertrauensperson, durchgeführt werden. Der IBRP wurde dabei, wie jetzt auch der ITP, mit dem Klienten zusammen entwickelt und im Verlauf der Hilfe von den Leistungserbringern fortgeschrieben.

Der nun gültige ITP soll helfen, dem hilfesuchenden Menschen in seiner Lebenssituation, mit seinen individuellen Bedarfen eine passgenaue Hilfe anzubieten. Ein sachgerechter Einsatz des Erhebungsinstrumentes ITP soll dabei durch lizenzierte Moderatoren- und Anwenderschulungen bei Leistungsträgern und Leistungserbringern sichergestellt werden. Durch Schaffung passgenauer Hilfen erfolgt im Leistungssystem ein Paradigmenwechsel von einer ehemals einrichtungszentrierten hin zu einer personenzentrierten Hilfe.

Zusätzlich werden Daten zur materiellen Situation des Betroffenen erhoben. Dies ist erforderlich, um die leistungsgerechten Voraussetzungen gem. § 2 Abs. 1 SGB XII zu prüfen. Die Gesamtheit aller erhobenen Daten im ITP ermöglicht den Prozessbeteiligten ein sehr detailliertes Bild des einzelnen Klienten und verdeutlicht bei Offenbarung der Datenmenge und –tiefe gegenüber einem Dritten die Notwendigkeit eines funktionierenden Datenschutzes im Interesse des Betroffenen.

„Wenn der Klient im Hinblick auf die Dinge, die ihn belasten, ständige Unsicherheit mit sich herumträgt, was er nun riskieren kann preiszugeben und was nicht, behindert das die Arbeit in einem nicht unerheblichen Maße. Deshalb muss juristisch klar sein, unter welchen Voraussetzungen überhaupt preisgegebene Informationen verwendet werden dürfen.“(Mörsberger, 1985, S.34)

3.2 Rechtsbeziehungen Leistungsberechtigter, -träger, -erbringer

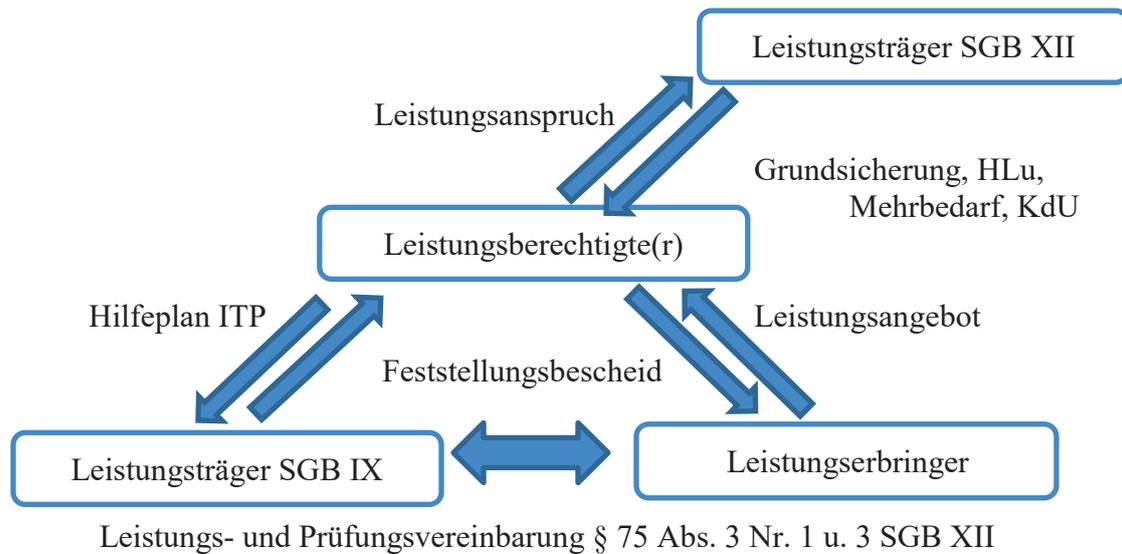
Zur Betrachtung der notwendigen Informationsströme für eine Leistungsgewährung im Rahmen eines Teilhabeplans sollen die Rechtsbeziehungen zwischen Leistungsträger, Leistungsberechtigtem und Leistungserbringer näher beschrieben werden. Im Zentrum der Betrachtung steht der Leistungsberechtigte mit seiner individuellen Lebenssituation, seinen Ansprüchen sowie seinen Ressourcen.

Aus Anlass eines Gesamtplanverfahrens (BTHG) werden die vom Leistungsträger erhobenen Teilbedarfe, unter Anwendung des ITP, auf einander abgestimmt und mit dem Leistungsberechtigten individuelle Teilhabeziele vereinbart. Das Gesamtplanverfahren stellt dabei den verwaltungstechnischen Prozess, beginnend mit der Bedarfserhebung, bis zur konkreten Bewilligung einer Hilfe dar.

„Dabei muss der nach dem Zuständigkeitsklärungsverfahren leistende Träger in Abstimmung mit den anderen Reha-Trägern und dem Leistungsberechtigten insb. die Beteiligten (auch die nach § 22 SGB IX), den festgestellten Bedarf, die Berücksichtigung des Wunsch- und Wahlrechts und die voraussichtlich erforderlichen Leistungen in einem Teilhabeplan schriftlich festhalten und diesen im Verlauf der Reha-Maßnahme ggf. fortschreiben.“ (von Boetticher, 2018, S.104)

In der nachfolgenden Abbildung sind in der Peripherie die Leistungsträger (SGB IX, SGB XII) und der Leistungserbringer (bspw. Gartenhaus e.V.) angeordnet, wobei der Leistungsträger die Hilfen auswählt und finanziert, der Leistungserbringer die personenzentrierte Hilfen gemäß Teilhabeplan anbietet.

Abb.1 Rechtsbeziehungen im Leistungsfall SGB IX, XII



Quelle: eigene Darstellung

Der Leistungsberechtigte kann seinen individuellen Bedarf in seiner konkreten Lebenssituation, z.B. Grundsicherung, beim Leistungsträger nach SGB IX und die Hilfen wegen seiner seelischen oder körperlichen Beeinträchtigung beim Leistungsträger gem. SGB XII beantragen.

Während die Leistungsträger das Regulieren von Geldleistungen im Leistungsfall selber vornehmen können, bedienen sie sich bei den Hilfen zur Wiedereingliederung über Leistungs- und Prüfungsvereinbarungen mit einem zugelassenen Leistungserbringer. Die Beantragung der Hilfen obliegt dem Hilfesuchenden alleine. Unterstützung kann ihm durch eine Bezugsbetreuung, wenn er schon im Hilfesystem angekommen ist, oder auch durch einen gesetzlich ernannten Betreuer gewährt werden.

Alle Prozessbeteiligten sollen in ihren Zuständigkeiten auf einen identischen Datenbestand des Leistungsberechtigten zugreifen können. Um dies zu ermöglichen müssen rechtliche und technische Rahmenbedingungen vorliegen und alle Beteiligten den sorgsamem Umgang mit den anvertrauten Daten praktizieren.

3.3 Grundsätze für die Verarbeitung Art. 5 DS-GVO

Bei der Verarbeitung personenbezogener Daten haben wegen der großen Bedeutung für den Betroffenen verbindliche Grundsätze zu gelten.

Abb.2 Grundsätze Art. 5 DS-GVO

a) Rechtmäßigkeit und Transparenz	Die zu verarbeitenden Daten sollen rechtmäßig erworben, nach Treu und Glauben verarbeitet, sowie transparent für die betroffene Person nachvollziehbar sein.
b) Zweckbindung	Die personenbezogenen Daten sollen „...für festgelegte eindeutige und legitime Zwecke erhoben werden...“. Die strenge Zweckbindung untersagt dem Verarbeiter eine andere als die vereinbarte Nutzung der Daten.
c) Angemessenheit	Die zu erhebenden Daten sollen dem Zweck der Verarbeitung angemessen sein. Es gilt das Prinzip der Datenminimierung, d.h. es sollen nur solche Daten in Quantität und Qualität erhoben werden, die auch notwendig sind, um den Zweck zu erfüllen.
d) Richtigkeit	Es sind nur solche Daten zu verarbeiten, für die sichergestellt ist, dass diese richtig und aktuell sind. Weiterhin sind Maßnahmen zu ergreifen um unrichtige Daten zu identifizieren, zu sperren, zu ändern oder zu löschen.
e) Speicherbegrenzung	Personenbezogene Daten sind nur so lange zu speichern, wie es die Zweckbindung erfordert. Eine längere Speicherdauer z.B. zur Archivierung oder Erstellung interner statistischer Auswertungen muss durch geeignete Maßnahmen abgesichert werden.
f) Datensicherheit	Personenbezogene Daten müssen in angemessener Weise „vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“ geschützt werden.

Diese Grundsätze beschreiben erforderliche Standards und bieten dem Verantwortlichen der Datenverarbeitung eine Orientierung bei der Anwendung der Norm.

Die Anwendbarkeit der Grundsätze sowie der Stand der Umsetzung im Beispielunternehmen wird in den nachfolgenden Kapiteln der Thesis jeweils getrennt nach Klienten-, Mitarbeiter- und Mitgliederdaten dargestellt.

Zusätzlich ist der Verantwortliche nach Art. 5 Abs. 2 DS-GVO „...für die Einhaltung der Grundsätze nach Absatz 1 verantwortlich und muss dessen Einhaltung nachweisen können (Rechenschaftspflicht).“ Dieser Nachweis gelingt durch Dokumentation interner und externer Audits im Rahmen des Qualitätsmanagements, durch regelmäßige Datenschutzfolgeabschätzungen sowie durch die laufenden Aufzeichnungen des Datenverarbeiters bzw. seines Datenschutzbeauftragten zum Stand der Umsetzung der technisch organisatorischen Maßnahmen.

3.4 Rechtmäßigkeit der Verarbeitung Art. 6, 7 DS-GVO

Die „Verarbeitung“ im Kontext der DS-GVO ist gem. Art. 4 Nr. 2 die Erhebung, die Erfassung, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung, der Abgleich oder die Verknüpfung, die Einschränkung bzw. das Löschen oder die Vernichtung. Für rechtmäßige Verarbeitung dieser Verarbeitungsvorgänge sind nun in der DS-GVO mit Art. 6 einige Grundsätze festgeschrieben worden.

„Mit dem Gebot der Rechtmäßigkeit wird dem Grunde nach noch einmal wiederholt, dass jede Datenverarbeitung entweder auf einer Einwilligung der betroffenen Person oder aber auf einer anderweitigen Rechtsgrundlage beruhen muss (vgl. Art. 6 Abs. 1 DS-GVO)“ (Tinnefeld et.al, 2017, S.237)

Für eine Rechtmäßigkeit in der Verarbeitungstätigkeit mit den Daten muss mindestens eine der nachfolgenden Voraussetzungen vorliegen.

Abb.3 Rechtmäßigkeit der Verarbeitung Art. 6 DS-GVO

a) Einwilligung	Der Betroffene hat seine Einwilligung gegeben, z.B. beim Leistungsträger mit Erstellung des ITP oder zusätzlich beim Leistungserbringer vor Ort
b) Verarbeitung für Erfüllung eines Vertrages oder auf Anfrage des Betroffenen vorvertraglich	Leistungs- und Prüfungsvereinbarung gem. § 75 Abs. 3 Nr. 1 und 3 SGB XII i. V. m. dem LRV M-V gem. § 79 Abs. 1 SGB XII
c) Erfüllung rechtlicher Verpflichtungen	Finanzbehörden gem. § 85 AO Sozialdaten gem. §§ 67 ff SGB X
d) Schutz lebenswichtiger Interessen des Betroffenen	kann in Krisensituationen bei Eigen- oder Fremdgefährdung zutreffend sein
e) Wahrnehmung einer Aufgabe im öffentlich rechtlichen Interesse	Vereinszweck gem. Satzung
f) im Eigeninteresse ohne Einschränkung der Interessen des Betroffenen	Vereinszwecks gem. Satzung Unternehmensfortführung

Quelle: eigene Darstellung

Die DS-GVO verbietet, wie das bisherige Datenschutzrecht auch, grundsätzlich die Verarbeitung personenbezogener Daten. Ausnahmetatbestände für eine Zulässigkeit sind demnach nur, wenn gesetzliche Normen dies erlauben oder aber die betroffene Person ihre Einwilligung erklärt hat.

Der großen Bedeutung bei der Abgabe einer Einwilligung durch den Betroffenen wird die DS-GVO mit einem eigenen Artikel (7) gerecht. Hier werden in den Absätzen 1 bis 4 die Bedingungen für die Rechtmäßigkeit formuliert, im Besonderen die Anforderungen an die Freiwilligkeit bei der Einwilligung.

Die Form der Einwilligung ist gesetzlich nicht vorgegeben, aber nach Art. 7 Absatz 1 DS-GVO und § 51 Absatz 1 BDSG, hat der Verarbeiter der Daten eine Nachweispflicht.

4 Vorstellung „Gartenhaus“ e.V.

Untersuchungsgegenstand dieser Thesis ist die Datenschutz-Grundverordnung am Beispiel des „Gartenhaus“ Psychosozialer Trägerverein Stralsund e.V.. Der Verein ist ein gemeinnütziger Träger, der in der Versorgungsregion Vorpommern-Rügen die Interessen psychisch kranker Erwachsener sowie deren Angehörigen vertritt.

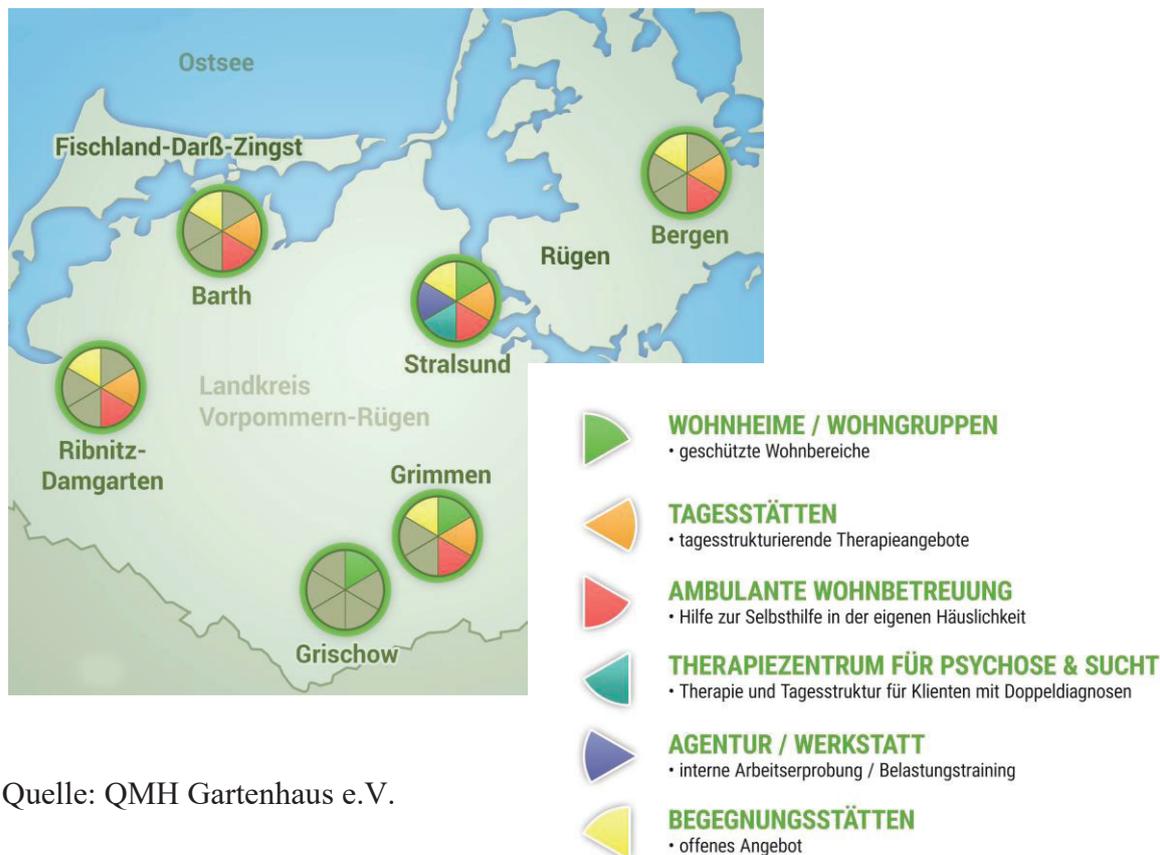
Die Empfehlungen der Psychiatrie-Enquete der Bundesrepublik Deutschland, welche Ende der siebziger Jahre mit einer Bestandsaufnahme der Unterbringung und Betreuung psychisch kranker Menschen begannen, führten zur Definition der bedarfsgerechten Versorgung dieses Personenkreises. Mit dem Einigungsvertrag vom 31.08.1990 und dem damit verbundenen Beitritt der ehemaligen DDR zur Bundesrepublik galt der Qualitätsstandard auch in den neuen Bundesländern. In der Folge wurde der Verein „Gartenhaus“ e.V. im November 1992 in Stralsund gegründet und rechtsbekundend beim Amtsgericht Stralsund unter der Vereinsregisternummer 249 eingetragen.

Aufgabe des „Gartenhaus“ e.V. ist es, den psychisch kranken Erwachsenen in und nach einer Krisensituation, ggf. nach Klinikaufhalten, mittels anerkannter und vereinbarter psychosozialer Hilfen eine Reintegration in den Alltag zu ermöglichen. Tagesstrukturierende Maßnahmen sollen helfen, dass der Klient eine größtmögliche Selbstbestimmtheit in seiner Wohnform finden kann. Bei schwer chronifizierten Langzeitklienten kann bereits das Vermeiden von Klinikaufhalten und die Alltagsstabilisierung Herausforderung genug sein.

Rechtsgrundlagen für die Tätigkeiten des Vereins stellen neben der Vereinssatzung der Landesrahmenvertrag für Mecklenburg-Vorpommern mit § 79 Abs. 1 SGB XII, Leistungs- und Prüfungsvereinbarungen für stationäre, teilstationäre und ambulante Einrichtungen sowie weitere spezifische Gesetze und Vorschriften zur Regelung der Unterbringungs- und Betreuungsleistungen dar.

Satzungsgemäß betreibt der „Gartenhaus“ e.V. Wohneinrichtungen, Tagesstätten, Kontakt- und Begegnungstätten, verschiedene Arbeits- und Beschäftigungsprojekte, das Ambulante Betreute Wohnen im Landkreis und der Hansestadt Stralsund, ein Therapiezentrum für Personen mit Doppeldiagnosen und verschiedene weitere Angebote in Kooperation mit anderen Institutionen im Rahmen der Versorgung psychisch kranker Erwachsener.

Abb.4 Einrichtungen des Gartenhaus e.V.



Quelle: QMH Gartenhaus e.V.

Der „Gartenhaus“ e.V. ist mit seinen Tätigkeitsfeldern „Betreuung und Pflege“ durch die TÜV Nord Cert GmbH zertifiziert. Damit finden jährlich externe Überwachungsaudits und alle 3 Jahre Rezertifizierungen im Unternehmen statt. In diesen Audits und zusätzlich durch jährliche interne Audits soll die Konformität des Qualitätsmanagementsystems, mit den gesetzlichen Grundlagen und der DIN ISO EN 9001:2015 überprüft werden. Festgestellte Abweichungen, z.B. im Datenschutz, sind zu protokollieren und durch geeignete und angemessene Maßnahmen abzustellen.

5 Datenverarbeitung, -speicherung und Datensicherheit

5.1 Rolle und Bedeutung des Datenschutzes

Datenschutz und Datensicherheit müssen sich ständig den technischen Entwicklungen und den damit verbundenen Anforderungen anpassen. Während sich die Möglichkeiten der Datensicherheit mit jeder technischen Innovation in der Informationstechnologie sofort verbessern lassen, können die Aufsichtsbehörden und Gesetzgeber häufig erst

nachträglich die unausgewogenen Positionen der beteiligten Parteien (Betroffene und Datenverarbeiter) ausgleichen. Deutlich flexibler in der Anpassung sind an dieser Stelle Vereinbarungen zu datenschutzrechtlichen Grundprinzipien in der Unternehmenskultur.

Ein Interessensausgleich zwischen den Akteuren im nationalen Gesundheits- und Sozialwesen scheint nach Auffassung des Autors zumindest im Rahmen des Datenschutzes in Deutschland bereits gut zu funktionieren.

„Im Gesundheits- und Sozialwesen steht im Vordergrund aller Aktionen der Patient – der kranke Mensch - den es zu heilen gilt; dabei ist dessen Recht auf informelle Selbstbestimmung verantwortungsbewusst und angemessen zu respektieren und zu verwirklichen.“ (Bake et al, 2004 , S. 7).

Datenschutz und Datensicherheit sind inhaltlich zwei unterschiedliche Themengebiete, die in Bezug auf die Verarbeitung personenbezogener Daten eng miteinander verbunden und grundsätzlich Bestandteil einer bestimmten Unternehmenskultur sein sollten. Ein darin verankerter Leitgedanke ist die Festlegung, dass Unternehmenswerte und Persönlichkeitsrechte in gleicher Weise zu schützen sind.

Die besondere Bedeutung des Datenschutzes in der EU wird erkennbar durch das generelle Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DS-GVO. Die europäische Norm lässt hier mit Absatz 2 lita. a bis j, 10 Ausnahmetatbestände zu, unter denen eine Verarbeitung trotzdem zulässig ist.

Desweiteren fördert die DS-GVO ausdrücklich Maßnahmen, welche die Ausarbeitung von Verhaltensregeln bei der Umsetzung der Verordnung, also auch beim Umgang mit den sensiblen Daten, fördern. Der Art. 40 DS-GVO benennt hier Anwendungsbeispiele zur Ausarbeitung von Verhaltensregeln zur Konkretisierung der Verordnung. Ziel dieser Empfehlungen soll eine weitere Präzisierung der unternehmensinternen Leitlinien zum Schutz sensiblen Daten und zur Stärkung der Persönlichkeitsrechte Betroffener sein.

Ein anderes Kriterium für die besondere Bedeutung des Datenschutzes in der EU wird durch das Kapitel VI der DS-GVO deutlich. Jedes Mitgliedsland der EU ist aufgefordert gem. Art. 51 DS-GVO, unabhängige nationale Aufsichtsbehörden zur „Überwachung der Anwendung dieser Verordnung“ zu installieren, „...damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird...“.

Dabei wird vom Datenverarbeiter verlangt (Art. 31 DS-GVO), mit den Aufsichtsbehörden bei der Erfüllung der Aufgaben zusammenzuarbeiten. Die nationale Verpflichtung hierzu ergibt sich aus § 40 Abs. 4 S.1 BDSG. Zuständige Aufsichtsbehörde für das Beispielunternehmen, „Gartenhaus“ e.V., ist der Landesbeauftragte für den Datenschutz in Mecklenburg-Vorpommern mit Sitz in der Landeshauptstadt Schwerin.

Die Aufgaben der Behörde sind in Art. 57 Abs. 1 DS-GVO geregelt und umfassen u.a. die Sensibilisierung, Beratung und Kontrolle der öffentlichen und nichtöffentlichen Stellen für einen ordnungsgemäßen Umgang mit personenbezogenen Daten zur Wahrung des Rechtes des Einzelnen auf informelle Selbstbestimmung. Weiterhin fungiert die Aufsichtsbehörde als Beschwerde- und Untersuchungsstelle bei Anzeigen von Betroffenen zum Datenschutz.

5.2 Ausgangssituation im Unternehmen

5.2.1 Risikobasiertes Denken DIN EN ISO 9001:2015

Im Januar 2017 hat sich der „Gartenhaus“ e.V. nach der Norm DIN EN ISO 9001:2015 neu zertifizieren lassen. Diese Norm fordert in Abschnitt 0.3.3 i. V. m. Abschnitt 4 ein Risikobasiertes Denken im Unternehmen. Belege für das verankerte Risikobewusstsein im Unternehmen lassen sich u. a. in den Festlegungen des QMH B1 bspw. zum Umgang mit Lieferanten (A2.8), im Umgang mit der Wartung von Dienstfahrzeugen und technischen Anlagen sowie einem jährlichen Versicherungsaudit finden.

„Die Erfüllung der Anforderung dieser Internationalen Norm verlangt von der Organisation, dass sie Maßnahmen plant und umsetzt, mit denen Risiken und Chancen behandelt werden. Die Behandlung von sowohl Risiken als auch Chancen bildet eine Grundlage für die Steigerung der Wirksamkeit des Qualitätsmanagementsystems, für das Erreichen verbesserter Ergebnisse und für das Vermeiden von negativen Auswirkungen.“ (Gräbig, 2016, S.73)

Abschnitte 6.1.1 und 6.1.2 der DIN EN ISO 9001:2015 verpflichten zu einer Planung von Maßnahmen mit dem Ziel der Verhinderung unerwünschter Auswirkungen. Diese eingeleiteten Maßnahmen sollen regelmäßig eine Bewertung hinsichtlich ihrer Wirksamkeit erfahren.

Das Beispielunternehmen entsprach den Forderungen des risikobasierten Denkens zum Zeitpunkt der Zertifizierung im Januar 2017 und damit auch schon in einigen Teilen den Forderungen der DS-GVO vor dem 25.05.2018. So waren bereits Festlegungen in verbindlichen Handlungsleitlinien zum Datenschutz, QMH B1 VA 4.2.4-2 (alt), sowie durch interne Auditierung der Schlüsselprozesse, auch hinsichtlich des Datenschutzes, ausgearbeitet und umgesetzt. Die Herangehensweise des risikobasierten Denkens hat bei der Bewertung des Datenschutzes im Unternehmen am Übergang zur DS-GVO zu einer reibungslosen und konfliktarmen Umsetzung der Maßnahmen und zur Erfüllung der neuen Anforderungen geführt.

5.2.2 Der betriebliche Datenschutzbeauftragte

Die Notwendigkeit der Bestellung eines Datenschutzbeauftragten im Beispielunternehmen ist aus Art. 37 Abs. 1, lits. b, c DS-GVO sowie aus dem BDSG mit § 38 Abs. 1, S. 1 abzuleiten. Danach ist ein Datenschutzbeauftragter zu bestimmen, wenn besondere personenbezogene Daten gem. Art. 9 DS-GVO von mehr als in der Regel 10 Mitarbeitern als Kerntätigkeit verarbeitet werden.

Von den aktuell 103 Mitarbeitern des Unternehmens arbeiten nahezu 100 % mit personenbezogenen Daten unserer Klienten. Das sind neben dem Betreuungsfachpersonal auch die Hilfskräfte in Hauswirtschaft und Fahrdienst, die Ansprechpartner in den Kontakt- und Begegnungsstätten des Vereins. Zusätzliche Hilfe bekommen die Mitarbeiter durch ehrenamtliche Kräfte und die Angehörigen im freiwilligen sozialen Jahr (FSJ). Alle Mitarbeiter unterzeichnen bei Beschäftigungsaufnahme eine verbindliche Verpflichtung zur Einhaltung datenschutzrechtlicher Anforderungen (A4.8).

Der gesetzlichen Anforderung zur Bestellung eines betrieblichen Datenschutzbeauftragten ist das Unternehmen mit der Ernennungsurkunde am 01.12.2017 nachgekommen. Der Datenschutzbeauftragte „...benötigt eine entsprechende fachliche Qualifikation und charakterliche Eigenschaften, die eine besondere Vertrauenswürdigkeit erwarten lassen. Zu seinen möglicherweise weiterhin zu übernehmenden Aufgaben darf er nicht im Interessenkonflikt stehen.“

(Bake et al, 2004, S.15)

Die entsprechende fachliche Eignung hat der interne Datenschutzbeauftragte durch seinen beruflichen Werdegang und durch einem Zertifikatslehrgang im Oktober .2017 bei der TÜV Akademie in Rostock erlangt.

Die Aufgaben des Datenschutzbeauftragten sowie seine Unabhängigkeit regeln allgemein die Art. 38 und 39 DS-GVO i. V. m. §§ 6, 7 und 3 Abs. 1 BDSG. Der betriebliche Datenschutzbeauftragte im Beispielunternehmen belegt eine Stabstelle (A4.0) und ist in der Wahrnehmung seiner Aufgaben und Pflichten durch die Geschäftsführung nicht beschränkt. Der Datenschutzbeauftragte hat neben seiner Beratungsfunktion für die Geschäftsleitung auch die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben im Unternehmen zu gewährleisten.

Weiterhin ist er nach Art. 39 Abs. 1 lit. b DS-GVO angehalten, an der „Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter“ mitzuwirken. Im Beispielunternehmen wurden regelmäßig Schulungen zur Thematik Datenschutz/Datensicherheit durch das IT-Unternehmen Gecko mbH, Rostock, durchgeführt. Am 08.05.2018 hat der betriebliche Datenschutzbeauftragte alle LeiterInnen der Organisationseinheiten mit den Neuerungen der DS-GVO vertraut gemacht. Für eine nachhaltige Sensibilisierung der Belegschaft ist für Oktober 2018 eine weitere interne Weiterbildung für das Betreuungspersonal vorgesehen.

Der betriebliche Datenschutzbeauftragte ist zusätzlich im Arbeitskreis für interne Datenschutzbeauftragte des Paritätischen Landesverbandes Mecklenburg-Vorpommern vernetzt. Dieser Arbeitskreis soll den internen Datenschutzbeauftragten der Mitgliedsorganisationen Hilfe und Unterstützung geben, damit sie in ihrer Beratungsfunktion für die jeweiligen freien Träger eine rechtskonforme Aufbau- und Ablauforganisation der Betreuungstätigkeit bewirken können.

Die Ablauforganisation zur Gewährleistung des Datenschutzes wird in einer internen Verfahrensweisung QMH B1 VA 4.2.4-4 geregelt.(A4.1)

Dort sind verbindliche Handlungsleitlinien festgeschrieben, die alle MitarbeiterInnen im Beispielunternehmen zu befolgen haben. Die Konformität von Verfahrensweisung und tatsächlicher Umsetzung wird in regelmäßigen internen und externen Audits in den Einrichtungen überprüft.

Damit wird die Anforderung aus Art. 5 Abs. 2 DS-GVO „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können“ erfüllt.

Besondere Herausforderungen nach DS-GVO sind nun die Erstellung von Verzeichnissen der Verarbeitungstätigkeiten und die Durchführung von Datenschutzfolgeabschätzungen zur Identifizierung von Risiken in der Datenverarbeitung. Darin einzubeziehen ist nach Art. 39 Abs. 1 lit. c, auf Anfrage auch der Datenschutzbeauftragte.

6 Herausforderungen durch die EU DS-GVO

6.1 Verarbeitung besonderer personenbezogener Daten Art. 9 DS-GVO

Eine wirksame und nachhaltige soziale Arbeit in der Gemeinschaft erfordert die Erhebung und Verarbeitung personenbezogener Daten. Dazu müssen zu Beginn der Teilhabeplanung die individuelle Beeinträchtigung Hilfesuchender festgestellt werden. Dies setzt die Kenntnis darüber und das Einverständnis des Betroffenen voraus. Nur durch die Mitwirkung des Betroffenen (Kap. 3.1) ist es dem zuständigen Leistungsträger möglich, eine wirksame personenzentrierte Hilfe anzubieten. Dabei ist immer auch der Grundsatz der Datensparsamkeit gem. Art. 5 Abs. 1 lit. c DS-GVO zu beachten. Die Wirksamkeit einer Hilfe kann dabei immer nur so hoch sein, wie die Qualität der vorliegenden Informationen über den Betroffenen hierzu.

Der Art. 9 DS-GVO regelt die Verarbeitung besonderer Kategorien personenbezogener Daten. So untersagt die DS-GVO in Abs. 1 z.B. die Verarbeitung von Daten u.a. zur rassischen oder ethnischen Herkunft, zur religiösen Weltanschauung, zu Gesundheitsdaten oder zum Sexualleben oder der sexuellen Orientierung. Zweifellos sind aber einige dieser Daten wichtig für ein objektives Bild über das Hilfesuchen des Betroffenen. Der Abs. 2 lit. a dieses Artikels definiert den Ausnahmetatbestand für eine Verarbeitung dieser Daten im Beispielunternehmen.

Danach gilt das Verbot nach Art.9 Abs. 1 DS-GVO nicht, wenn der Betroffene gemäß Abs. 2 lit. a ausdrücklich der Verarbeitung mit einer Zweckbindung eingewilligt hat. Nach Art. 7 Abs. 1 DS-GVO hat diese Einwilligung freiwillig zu erfolgen.

Seine Einwilligung hierzu gibt der Betroffene bereits beim Leistungsträger im Rahmen seines Teilhabegesprächs zur Erstellung des Integrierten Teilhabepplans (ITP). Mit dem Ergänzungsbogen zum ITP (A5_Rechtliche Aufklärung zum Datenschutz) gibt er sein Einverständnis auch zur Weitergabe der Daten an den jeweiligen Leistungserbringer. Eine Beurteilung seiner Einwilligungserklärung hinsichtlich der Qualität seiner Freiwilligkeit soll nach Art. 7 Abs. 4 DS-GVO immer unter Berücksichtigung der Notwendigkeit der Daten für die Erfüllung des Vertrages erfolgen.

In diesem Zusammenhang soll zusätzlich auf Art. 10 der DS-GVO hingewiesen werden. Danach ist es nur noch unter behördlicher Aufsicht gestattet, Register über strafrechtliche Verurteilungen von Betroffenen zu führen. Das Wissen um einzelne spezifische Straftaten der Betroffenen ist aber im Rahmen der Sozialen Arbeit unentbehrlich, auch um andere Klienten und Mitarbeiter zu schützen.

6.2 Verantwortung für die Verarbeitung Art. 24, 25 DS-GVO

Der Art. 24 Abs. 1, Satz 1 DS-GVO verpflichtet den Verantwortlichen der Datenverarbeitung, unter Würdigung von Eintrittswahrscheinlichkeiten und Schadenshöhen bei möglichen Datenpannen, zu geeigneten technischen und organisatorischen Maßnahmen. Zusätzlich hat der Verantwortliche diese Maßnahmen zu dokumentieren, um „...den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“

„Ein „Verantwortlicher“ ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Art. 4 Nr. 7 DS-GVO“ (Voigt/Von dem Bussche, 2017, S.21)

Die Verantwortung für die Datenverarbeitung trägt nach § 26 Abs. 1, 2 BGB im Beispielunternehmen vollumfänglich der gemeinnützige Verein, vertreten durch seinen Geschäftsführer und dem ehrenamtlichen Vorstand.

Um die geeigneten und angemessenen technischen Mittel und Maßnahmen ergreifen zu können, wie in Art. 25 DS-GVO i. V. m. § 64 Abs. 1 BDSG gefordert, hat das Unternehmen zwei überregional tätige IT- Spezialisten vertraglich binden können.

Die Gecko mbH zeichnet für den technisch organisatorischen Aufbau der Datenverarbeitung im Beispielunternehmen verantwortlich. In enger Zusammenarbeit werden in regelmäßigen Abständen die bereits installierten technischen Maßnahmen hinsichtlich ihrer Angemessenheit, Wirksamkeit und Zukunftsfähigkeit überprüft. Das aktuell technisch umgesetzte Sicherheitsniveau bei der Datenverarbeitung im Unternehmen lässt sich aus der Anlage 3 (TOM) dieser Thesis entnehmen.

Entsprechend Art. 25 Abs. 2 DS-GVO sind geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass nur die richtigen Daten im erforderlichen Umfang verarbeitet werden und kein Unberechtigter Zugriff darauf hat. Für die Windows-Oberflächen der Arbeitsplatzrechner zeichnet Gecko mbH als Administrator für die Vergabe der Zugriffsrechte verantwortlich. Die Moveo Software GmbH reglementiert die Zugriffe der Mitarbeiter auf die verschiedenen Datenbestände von Klienten im Dokumentationsprogramm „procare“.

6.3 Verzeichnis von Verarbeitungstätigkeiten Art. 30 DS-GVO

Die DS-GVO verpflichtet in Art. 30 Abs. 1 jeden Verantwortlichen und ggf. seinen Vertreter, über Verarbeitungstätigkeiten ein Verzeichnis zu führen. Das BDSG in seiner alten Fassung kannte bereits Verfahrensverzeichnisse für meldepflichtige automatisierte Verarbeitungen.

Das Führen dieser Verzeichnisse gehörte nach Härtung, 2016, S. 7, zu den „Kernaufgaben des betrieblichen Datenschutzbeauftragten“. (§ 4g Abs. 2 S. 1 i. V. m. § 4e S. 1 BDSG aF) So sollten bspw. Prozessbeschreibungen zu Kunden- und Mitarbeiterdatenbanken erstellt und laufend aktualisiert werden. Diese Prozessbeschreibungen gab es im Beispielunternehmen bereits vor der Rechtsverbindlichkeit der DS-GVO in den Verfahrensbeschreibungen des Qualitätshandbuchs, Abteilung B1.

Mit Art. 30 DS-GVO geht die Verantwortung vom betrieblichen Datenschutzbeauftragten nun auf den Verantwortlichen der Verarbeitung über. Die qualitativen Anforderungen an das Verzeichnis ergeben sich aus Abs. 1 lita a bis g.

Die Daten müssen hinsichtlich ihrer Qualität, ihrer Verarbeitung, der Zuständigkeiten sowie der technisch organisatorischen Maßnahmen zur Sicherung beschrieben werden.

Die Dokumentationspflicht ergibt sich aus Abs. 3 des Artikels, wonach ein schriftlicher Nachweis, hier ein Rechenschaftsbericht, zu führen ist. In der Anlage der Thesis, A2.1 bis A2.14, sind die Verarbeitungstätigkeiten des Beispielunternehmens für die jeweiligen Anwendungen dargestellt. Die Anzahl der notwendigen Verfahrensverzeichnisse eines Datenverarbeiters wird dabei maßgeblich von der inhaltlichen Komplexität der Prozesse bestimmt.

Der Art. 30 Abs. 5 DS-GVO befreit Unternehmen von dieser Regelung, wenn Sie weniger als 250 Personen beschäftigen. Das Beispielunternehmen entspricht mit der Belegschaft von derzeit 103 Mitarbeitern der Voraussetzung für eine Befreiung. Im zweiten Halbsatz des betreffenden Artikels sind wiederum die Ausnahmen vom Befreiungstatbestand festgelegt. Sollte die Verarbeitung der Daten Rechte und Freiheiten der Betroffenen gefährden, die Verarbeitung dieser Daten nicht nur gelegentlich erfolgen und es sich um Daten gem. Art. 9 DS-GVO handeln, so ist ein Verarbeitungsverzeichnis gem. DS-GVO anzufertigen. Der „Gartenhaus“ e.V. arbeitet in der Betreuung der Klienten permanent mit besonderen Kategorien personenbezogener Daten und ist somit aus diesen Gründen von der Erstellung der Verarbeitungsverzeichnisse nicht befreit.

In der alten Fassung des BDSG bestand nach § 4g Abs. 2 S. 2 die Verpflichtung des Datenschutzbeauftragten „Jedermann“ in die Tätigkeiten der Verarbeitungen Einsicht zu gewähren. Diese Verpflichtung kennt die DS-GVO und das BDSG in seiner aktuellen Fassung nicht mehr. Damit sind national die Bundesdatenschutzbeauftragte sowie die regional zuständige Datenaufsichtsbehörde, der Landesdatenschutzbeauftragte M-V berechtigt, Vorlage von Verzeichnissen der Datenverarbeitungstätigkeiten zu verlangen. Das Verarbeitungsverzeichnis erfüllt die Dokumentationspflichten nach Art. 24 Abs. 1 DS-GVO.

6.4 Sicherheit der Verarbeitung Art. 32 DS-GVO

Neben den Erlaubnistatbeständen für eine Verarbeitung und der Einhaltung der Verarbeitungsgrundsätze (Art. 5 DS-GVO) ist ein angemessenes Schutzniveau in der Datenverarbeitung durch geeignete technisch organisatorische Maßnahmen zu gewährleisten. Der risikoorientierte Ansatz der DS-GVO schlägt mit ErwGr. 78 beispielhaft folgende Maßnahmen vor:

6.4.1 Verschlüsselung/Pseudonymisierung Art. 32 Abs.1, lit. a

„Pseudonymisierung ist in der Praxis ein gebräuchliches Mittel, um die Möglichkeit zur Identifikation betroffener Personen anhand ihrer Daten zu vermeiden.“

(Voigt/von dem Bussche, 2017, S.18)

Dabei werden die Daten in einer Weise verändert, „...dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können,...“ (Art. 4 Nr. 5 DS-GVO)

In der Vergangenheit wurden für statistische Zwecke im Beispielunternehmen Klientendaten außerhalb der Betreuungsdokumentation mit einem separaten Erhebungsbogen „Basisdokumentation“ QMH B2 FM 8-5 erfasst, pseudonymisiert, entsprechend § 3 Abs. 6a BDSG aF, und ausgewertet. Die Ergebnisse der Auswertungen sollten dazu dienen, Aussagen hinsichtlich möglicher kausaler Zusammenhänge von Klientenherkunft, Bildung, individuellem Krankheitsbild und z.B. Reintegrationsrate der Klienten abzuleiten. Erforderliche Maßnahmen auf Grund der Ergebnisse wurden im Rahmen kontinuierlicher Verbesserungsprozesse in Betreuungsplanung und –realisation eingearbeitet. Dieses Verfahren wurde mit Rechtswirksamkeit der DS-GVO zum 25.05.2018 eingestellt.

Grundsätzlich wäre eine Pseudonymisierung der personenbezogenen Daten auf Grund der Zweckbindung einer laufenden Kostenbewilligung/Feststellungsbescheid bei einem Leistungserbringer nicht zielführend. Die Quantität und Qualität der erhobenen Daten im ITP zur Sicherstellung personenzentrierter Hilfen lässt immer Rückschlüsse auf die einzelne betreffende Person zu. Eine Erfolgskontrolle würde seitens des zuständigen Leistungsträgers im Rahmen der Heimaufsicht gem. § 15 i. V .m. § 13 HeimG unmöglich werden, da die Prüfung grundsätzlich an der Person des Leistungsberechtigten zu erfolgen hat und ggfls. Nachfragen der Aufsichtsbehörde an den Hilfeempfänger hinsichtlich seiner eigenen Wahrnehmung im Teilhabeverfahren zu stellen sind.

Eine Verschlüsselung (Chiffrieren) definiert das BSI in seinem Glossar als „...einen Klartext in Abhängigkeit von einer Zusatzinformation, die „Schlüssel“ genannt wird, in einem zugehörigen Geheimtext (Chifftrat), der für diejenigen, die den Schlüssel nicht haben, nicht entzifferbar sein soll.“

Verschlüsselt werden die personenbezogenen Daten, wie auch alle anderen Daten im Beispielunternehmen, bei Erstellung einer Sicherungskopie zur Wiederherstellbarkeit nach Art. 32 Abs. 1 lit. c DS-GVO. Auf den Arbeitsplatzrechnern der verschiedenen Einrichtungen erfolgt derzeit noch keine Verschlüsselung in der Zwischenablage.

6.4.2 Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit

In Art. 32 Abs. 1 lit. b DS-GVO wird die Fähigkeit gefordert, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit „...auf Dauer sicherzustellen...“. Damit sind eingeleitete Maßnahmen zur Datensicherheit auf ihre Zukunftsfähigkeit zu prüfen. Die technisch organisatorischen Maßnahmen für Datenschutz und Datensicherheit stellen keine statischen Systembetrachtungen dar, sondern erfordern eine laufende Anpassung an die sich ändernden Anforderungen. Jährliche Revisionen sind die Maßnahmen zur Prüfung auf deren Konformität.

Vertraulichkeit im Umgang mit den personenbezogenen Daten sollen Zugangskontrollen gem. § 64 Abs. 3 Satz 1, Nr.1. zusammen mit Zugriffskontrollen gem. § 64 Abs. 3 Satz. 1 Nr. 5 BDSG sicherstellen. Alle betreuenden Einrichtungen, einschließlich der Geschäftsstelle, Abteilung Rechnungslegung, halten die hochsensiblen Daten in Aktenschränken und elektronischen Dokumentationssystemen unter Verschluss. Die protokollierte Schlüsselnachweise in den Einrichtungen ermöglichen es, jederzeit zu bestimmen, welcher Personenkreis sich in welchen sensiblen Räumen aufhalten darf und somit Zugang zu den Dokumentationssystemen hat. Für den Serverraum in der Geschäftsstelle ist wegen der Sensibilität eine besondere Zutrittskontrolle zu prüfen. Hier kann ggf. ein Besucherprotokoll geführt werden, auch um Fremdpersonen der Wartungsfirmen nachträglich noch eindeutig identifizieren zu können.

Die Zugriffskontrolle erfolgt im Beispielunternehmen durch Authentifizierung der jeweiligen Person am System. Dies ist nach Tsolkas/Schmidt, S. 130, die älteste und gebräuchlichste Form in der Informationstechnologie. Dabei wird die Eingabe einer UserID und eines Passwortes erforderlich. Während die UserID meist unternehmensintern bei den Mitarbeitern allgemein bekannt ist, stellt das Passwort eine höchst private Information dar. Nur in der korrekten Kombination von UserID und Passwort wird die vorher im System hinterlegte Zugriffsberechtigung aktiviert.

Alle Mitarbeiter des betreuenden Fachpersonals haben eine eigene UserID und auch ein individuelles Passwort. Zur Erhöhung der Datensicherheit und zur Verbesserung der Zugriffskontrolle sollte die Passwortvergabe einem noch näher zu bestimmenden Bedingungsnetzwerk unterworfen werden. Zudem ist die Vergabe von Passwörtern von einem permanenten in einen temporären Status zu verändern.

Die Passwortqualität ist hinsichtlich der Passwortlänge, Ablaufdatum, Zeichenverwendung und Passworthistorie zu optimieren. Inhaltliche Hilfestellung hierzu bieten neben dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) auch das Landesamt für Datenschutz M-V auf seiner Internetseite mit der Orientierungshilfe „Empfehlungen zur Passwortgestaltung und zum Sicherheitsmanagement“.

Integrität wird im Glossar des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) bezeichnet mit der „...Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen“. Dort heißt es weiter „Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurde.“ Um eine Datenintegrität sicherzustellen, muss gewährleistet werden, dass nur berechtigte Personen Zugriff auf bestimmte Datensysteme haben.

Diese Berechtigungssteuerung geht in ihrer Herangehensweise von zwei Standpunkten aus: „Es wird festgelegt, WER WO Berechtigungen besitzt. Damit ergeben sich zwei Seiten: Die Seite des „WER“ bezieht sich auf die Identitäten, die Seite des „WO“ dagegen auf die Ressourcen.“(Tsolkas/Schmidt, 2017, S.83)

Nach Tsolkas und Schmidt werden die Identitäten anhand der Eigenschaften, Funktionen und Tätigkeiten sowie Zugehörigkeiten, in definierten Rollen, bestimmt. Die Identitäten im Unternehmen sind die Mitarbeiter mit den jeweiligen individuellen beruflichen und persönlichen Eigenschaften. In ihrer Funktion und Tätigkeit lassen sich Betreuungsfach- und -hilfspersonal unterscheiden. Die Zugehörigkeit ist gekennzeichnet durch den gewöhnlichen Arbeitsort im Unternehmen, also durch die jeweiligen Einrichtungen mit dem entsprechenden Klientendaten.

Durch die Etablierung einer rollenbasierten Berechtigungssteuerung, wie in Tsolkas und Schmidt auf S. 90f beschrieben, erfolgt die Rechtevergabe nicht an einer Identität sondern an einer vorher definierten Rolle. Diese Berechtigungsvergabe an die jeweiligen Mitarbeiter erfolgt zentral durch die „technische Rolle“ des Administrators.

„Das Gestaltungselement der technischen Rolle wird benutzt, um den Funktionsumfang in einer IT-Anwendung festzulegen, den eine Identität wahrnehmen kann, wenn sie diese technische Rolle besitzt.“(Tsolkas/Schmidt, 2017, S. 93)

Das IT-Unternehmen, Gecko mbH, vergibt in Abstimmung mit der SachbearbeiterIn der Rechnungslegung im Unternehmen diese Berechtigungen. Die Ressourcen hingegen sind die Objekte, also Klienten/Mitarbeiter mit ihren personenbezogenen Daten, die den Identitäten, in Abhängigkeit vom Arbeitsort, zur Verfügung gestellt werden. Für den „Gartenhaus“ e.V. lässt sich das interne Berechtigungskonzept in Kurzform wie folgt darstellen.

Klientenbereich:

- a) jeder Mitarbeiter des Betreuungsfachpersonals kann auf die Daten der Klienten zugreifen, die ihm im Rahmen seiner beruflichen Tätigkeit am Arbeitsort über eine aktuelle Kostenbewilligung anvertraut sind. Er kann sie lesen, verändern und auch löschen.
- b) jeder Mitarbeiter als Hilfskraft in Betreuung und Hauswirtschaft kann nur die Daten der Klienten lesen, die ihm von der Einrichtungsleitung einzeln und direkt anvertraut wurden. Dabei ist die Relevanz der Daten für den einen Sachverhalt zu prüfen. Die Hilfskraft hat keine Änderungs-, Sperr- oder Löschungsbefugnis.
- c) die SachbearbeiterIn Rechnungslegung hat auf die abrechnungsrelevanten Daten Lese- und Sperrzugriff, jedoch keine Änderungskompetenz.

Mitarbeiterbereich

- a) nur die SachbearbeiterIn „Personalbuchhaltung“ hat auf die digitalen personalbezogenen Daten sowie den Personalakten der Mitarbeiter Zugriff. Sie arbeitet im Bedarfsfall und auf Anfrage der Geschäftsführung Datenmaterial zu.
- b) die EinrichtungsleiterInnen können im Einzelfall und auf Anfrage zur Personalentwicklung einzelne Daten in der Personalbuchhaltung anfragen.

In Anlehnung an die Kategorisierung der Zugriffskontrollen nach Tsoikas und Schmidt, S. 164f, ist für das Beispielunternehmen primär eine identitätsbezogene Zugriffskontrolle festzustellen. Es folgt keine Klassifizierung der Daten in Sicherheitsstufen, wie es eine ressourcenorientierte Zugriffskontrolle vorsieht.

Folgende weitere Maßnahmen hat der Verantwortliche im Beispielunternehmen nach einer Risikobewertung gem. BDSG ergriffen:

Abb. 5 Maßnahmen zur Datenintegrität

Datenträgerkontrolle § 64 Abs. 3, S. 1, Nr. 2 BDSG
<ul style="list-style-type: none"> - Lagerung von Papierakten unter Doppelverschluss - Doppelanmeldung je Mitarbeiter in Windows und procure
Speicherkontrolle § 64 Abs. 3, S. 1, Nr. 3 BDSG
<ul style="list-style-type: none"> - Doppelanmeldung je Mitarbeiter in Windows und procure
Benutzerkontrolle § 64 Abs. 3, S. 1, Nr. 4 BDSG
<ul style="list-style-type: none"> - Ausschluss einer automatische Datenweitergabe an Dritte - Eingeschränkter Datenexport mittels externer Datenträger
Zugriffskontrolle § 64 Abs. 3, S. 1, Nr. 5 BDSG
<ul style="list-style-type: none"> - Berechtigungsmanagement je Einrichtung und Berufsbild
Datenintegrität § 64 Abs. 3, S. 1, Nr. 11 BDSG
<ul style="list-style-type: none"> - Monitoring der Serversysteme durch Gecko mbH - Regelmäßige Schulungen der internen Mitarbeiter - Wartungsvertrag für IT-Systeme mit der Gecko mbH

Ein weiterer Aspekt bei der Sicherstellung von Datenintegrität ist die Internetnutzung am Arbeitsplatz. Durch die Notwendigkeit eines Aktualisierungsmanagement zur Gewährleistung der Belastbarkeit und der Verfügbarkeit der Systeme ist an allen Arbeitsplatzrechnern eine automatische Verbindung zum Internet vorinstalliert. Dieser Zugang baut bei Vorlage wichtiger up-dates eine Verbindung zum Software-Hersteller auf und aktualisiert außerhalb der Geschäftszeiten entsprechende Programme. Damit sind eine Kontinuität in der Belastbarkeit und die Aktualisierung wichtiger Virens Scanner in der Anwendersoftware gewährleistet.

Die Risiken einer Internetnutzung am Arbeitsplatz sind dabei vielfältig.

So können z.B. „...nicht gewollte oder sogar illegale Inhalte in das Unternehmensnetzwerk eindringen...“ und ungewollt „...internetete Informationen das Unternehmensnetzwerk verlassen.“ (Tsolkas/Schmidt, 2017, S.320)

Eine umfassende Auswertung der Zugriffe und Kontrolle der Inhalte durch den Arbeitgeber ist dabei wegen des Vertrauenstatbestandes zwischen Arbeitgeber und Arbeitnehmer unzulässig. Ein anderer Aspekt bei der Verwendung des Internets am Arbeitsplatz ist die Gestattung der privaten Nutzung durch die Beschäftigten. Nach Auffassung des Gesetzgebers, wird der Arbeitgeber damit zum Telekommunikations- bzw. Telemedienanbieter für den Beschäftigten. (§ 88 Abs. 2 S.1 Telekommunikationsgesetz i. V. m. § 11 Abs. 1 Nr.1 Telemediengesetz)

Eine *Verfügbarkeitskontrolle* gem. § 64 Abs. 3, S. 1, Nr. 13 BDSG soll sicherstellen, dass die personenbezogenen Daten gegen Zerstörung, Vandalismus und Verlust geschützt sind. Dies wird durch den Verschluss der Arbeitsplatzrechner und Aktensysteme, durch eine Notstromversorgung in der Serverlandschaft und durch eine installierte Klimaanlage im Serverraum der Geschäftsstelle gewährleistet. Um einen Totalverlust zu verhindern, werden die Daten der Arbeitsplatzrechner zum Teil bereits doppelt gesichert, d.h. vor Ort auf einem externen Datenträger und zusätzlich auf der Datensicherung direkt am Server, einer externen Festplatte (Qnap). Dieses Sicherheitsmerkmal muss zwingend auf allen einzelnen Arbeitsplatzrechner der Einrichtungen umgesetzt werden. Die externen Festplatten werden räumlich getrennt in feuerfesten und verschlossenen Schränken aufbewahrt.

Zur ständigen Überprüfung der *Belastbarkeit* werden die Rechnerlandschaften der Einrichtungen und der Geschäftsstelle durch ein Monitoring der Gecko mbH überwacht. Der § 64 Abs. 3 S. 1, Nr. 10 BDSG verlangt vom Verantwortlichen die Zuverlässigkeit, dass „...alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),...“. Meldungen hierzu werden zentral von der Gecko mbH ausgewertet und zeitnah, bereits im Falle des möglichen Auftretens, an den Verwaltungsleiter des Gartenhaus e.V. weitergegeben. Hier werden entsprechend der zeitlichen und inhaltlichen Priorität zusammen mit den Technikern der Gecko mbH und den betroffenen Einrichtungen Lösungsmöglichkeiten eruiert und deren Umsetzung vereinbart.

Zur Erhöhung der Belastbarkeit sei an dieser Stelle, wie bereits bei der Verfügbarkeitskontrolle, nochmal auf das Vorhandensein einer Klimaanlage und einer Notstromversorgung im Serverraum der Geschäftsstelle hingewiesen

6.4.3 Wiederherstellbarkeit Art. 32 Abs. 1 lit. c

Die DS-GVO und der § 64 Abs. 3, S. 1, Nr. 9 BDSG fordern eine „rasche“ Wiederherstellbarkeit der eingesetzten Systeme bei einem „physischen oder technischen Zwischenfall“.

Dazu werden mindestens einmal jährlich im Rahmen von IT-Wartungsarbeiten in den Einrichtungen und auch am Server in der Geschäftsstelle, Rücksicherungen von den installierten Back-up-Systemen vorgenommen. Dabei prüft das Wartungsunternehmen, Gecko mbH, die Wiederherstellbarkeit von Datenbeständen und ggfls. das Auftreten von Abweichungen (quantitative Datenmengenkontrolle) vom Soll-Datenbestand. Die installierte Notstromversorgung der Serverlandschaft garantiert auch hier die Einhaltung der Wiederherstellbarkeit nach Art. 32 Abs. 1 lit. c DS-GVO.

6.4.4 Verfahren zur regelmäßigen Überprüfung Art. 32 Abs. 1 lit. d

Der „Gartenhaus“ e.V. ist ein seit 2007 zertifiziertes Unternehmen; seit 2017 nach DIN ISO 9001:2015, Zertifikat-Register-Nr. 44 100 077645. Die TÜV Nord Cert GmbH führt als zugelassener Zertifizierer einmal jährlich ein Überwachungs- bzw. bei Laufzeitende, nach jeweils 3 Jahren, ein Rezertifizierungsaudit durch.

Die Normanforderung DIN EN ISO 9.2 (Internes Audit) verlangt u.a. von der Organisation die Planung, Durchführung und Auswertung von internen Audits. Im Rahmen dieser Audits vor Ort werden die vorhandenen technisch organisatorischen Maßnahmen zur Einhaltung von Datenschutz und Datensicherheit in den Einrichtungen hinsichtlich der Konformität zur DS-GVO und dem BDSG überprüft. Festgestellte Abweichungen und Verbesserungspotentiale werden im Auditbericht QMH B2 FM 8-3 protokolliert.

Zur Feststellung der Angemessenheit der technischen Maßnahmen und zum Stand der möglichen Technik für Datenschutz und Datensicherheit finden jährlich Sachinhaltgespräche zwischen der Verwaltungsleitung und der Gecko mbH Stralsund, zuletzt am 27.04.2018, statt.

In Auswertung der Ergebnisse aus dem Monitoring wird im Rahmen dieser Veranstaltungen von den IT-Spezialisten der jeweils aktuelle Stand der IT-Technik vorgestellt und Empfehlungen für deren Einsatz in den Einrichtungen des Unternehmens ausgesprochen.

Ziel beider Parteien dabei ist es, unter Beachtung, „...der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen...“ den Stand der Technik für „... ein angemessenes Schutzniveau zu gewährleisten...“ (Art. 32 Abs. 1 DS-GVO)

6.5 Datenschutzfolgeabschätzung (DSFA) Art. 35. DS-GVO

Erwägungsgründe (ErwGr.) 83, 84 i. V. m. Art. 35 Abs. 1 DS-GVO verpflichten den Verantwortlichen der Datenverarbeitung (Abs. 3 lits. a, b, c) unter bestimmten Voraussetzungen zur Durchführung von Datenschutzfolgeabschätzungen (DSFA). Dabei hat er dem Umfang, der besonderen Umstände und dem Zweck der Datenverarbeitung Rechnung zu tragen.

Der Art. 35 Abs. 3 lits. a, b DS-GVO i. V. m. § 67 BDSG fordert im Beispielunternehmen die Erstellung von Datenschutz-Folgeabschätzungen, wenn:

a) eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, „...die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten...“;

b) eine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogener Daten gemäß Artikel 9 Absatz 1 ...“ stattfindet.

Ziele der DSFA sind das Identifizieren von Risiken bei der Verarbeitung personenbezogener Daten sowie deren Einschätzung hinsichtlich Eintrittswahrscheinlichkeit und möglicher Schadenshöhen. Hier wird explizit das Risiko personenbezogener Daten Betroffener betrachtet und nicht Unternehmensrisiken.

Die Datenschutzfolgeabschätzungen für die identifizierten und bewerteten Risiken im Beispielunternehmen sind in der Anlage 1 dieser Thesis aufgeführt.

Im Ergebnis hat der Verantwortliche festgestellt, dass im Beispielunternehmen Risiken in der Verarbeitung von personenbezogenen Daten für Klienten (A1.2) und Mitarbeiter (A1.3) sowie bei der Entsorgung des gesamten Datenmaterials (A1.1) bestehen. Für die DSFA der Video-Anlage im Therapiezentrum (A1.4) kann auf Grund der Nichtaufzeichnung von Bildern die Unbedenklich erklärt werden.

Eine vorherige Konsultation bei der Erstellung der DSFA mit der Aufsichtsbehörde nach Art. 36 Absatz 1 DS-GVO erschien, nach Rücksprache mit dem betrieblichen Datenschutzbeauftragten nicht notwendig, da der Datenverantwortliche bereits Maßnahmen zur Eindämmung des Risikos eingeleitet hat.

Diese Maßnahmen wurden hinsichtlich ihres Umfangs als angemessen bewertet. Der Stand der eingesetzten technischen Mittel hierbei ist nach Feststellung der Gecko mbH aktuell.

Zusätzlich haben die bereits erstellten DSFA regelmäßigen Revisionen zu unterliegen, hauptsächlich dann, wenn gem. Art. 35 Absatz 11 DS-GVO „...hinsichtlich des mit dem Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind“. In diesem Zusammenhang sei auf die regelmäßigen Prüfungsvorgänge im Rahmen der Wartung der IT-Anlage (Kap. 6.4.4) hingewiesen.

6.5.1 Identifizierung von Risiken

„Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheit der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.“ (ErwGr. 76 DS-GVO)

Weitere Hinweise zur Katalogisierung von Risiken finden sich in ErwGr. 75 der DS-GVO. Danach sind eine mögliche Diskriminierung, Identitätsdiebstahl und –betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit in einem Berufsgeheimnis sowie andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile Risiken, die bei Verletzung des Datenschutzes im Beispielunternehmen für die Klienten auftreten können. Dabei ist es nach ErwGr. 83 unerheblich, ob die Handlungen die zu den Risiken führen, absichtlich, unabsichtlich und unrechtmäßig waren.

Für das zu betrachtende Unternehmen sind folgende Szenarien möglich.

Abb. 5 Bedrohungen im Geschäftsbetrieb

Vernichtung personenbezogener Daten	-(un)beabsichtigtes Löschen von Daten in Dokumentationssystemen z.B. Word-Dateien in Sozialberichten
Verlust personenbezogener Daten	-Einbruchdiebstahl in einer Einrichtung und Entwendung von PC-Technik, Kommunikationstechnik - Download von Schadsoftware
Veränderung personenbezogener Daten	-(un)beabsichtigtes Ändern von Daten in Datenbeständen, die für den Sachverhalt nicht zutreffend sind
Unbefugte Offenlegung	-Auskunft an unberechtigte Anfrager -Offenlegung gegenüber Unberechtigten
unbefugter Zugang	-Einbruch -Schlüsseldiebstahl

Alle Prozesse, die zur Vernichtung, Verlust oder Veränderung von personenbezogenen Daten, zur unbefugten Offenlegung oder zum unbefugten Zugang führen, müssen hinsichtlich ihrer Risiken untersucht werden.

Im Geschäftsbetrieb des Unternehmens treten in den verschiedenen Einrichtungen o.g. Bedrohungslagen mit unterschiedlichen Eintrittswahrscheinlichkeiten auf. Zusammenfassend sind zwei verschiedene Ausgangsszenarien möglich, in denen Datenverlust oder -manipulation eintreten kann. Das Betreuungspersonal ermöglicht durch mangelndes Fachwissen eine Datenpanne durch nichtautorisiertes Offenbaren, oder aber ein Externer, auch durch Viren oder Trojaner, verschafft sich ungenehmigten Zutritt und verursacht Datendiebstahl.

Beiden Szenarien sind durch geeignete technisch organisatorische Maßnahmen sowie Schulungen zu begegnen. Bei der Festlegung entsprechender Maßnahmen ist eine Beurteilung der Risiken zusätzlich in Eintrittswahrscheinlichkeit und möglicher Schadenshöhe/-ausmaß notwendig.

6.5.2 Risikobeurteilung

Eine Risikobeurteilung erfordert nach der Identifizierung der Risiken auch Betrachtungen zum Schadensausmaß und zur Eintrittswahrscheinlichkeit.

In der DS-GVO wird mit ErwGr.75 in S. 1 zwischen physischen, materiellen oder immateriellen Schaden für den Betroffenen unterschieden. Mit § 64 Abs. 1, S. 2 BDSG wird bei der Risikobewertung ausdrücklich auf die Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwiesen.

„Der IT-Grundschutz des BSI ist eine bewährte Methodik, um das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen. Die Angebote des IT-Grundschutzes gelten in Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS) geht.“ (BSI, online im Internet)

Demnach werden die Eintrittswahrscheinlichkeiten im IT-Grundschutz folgendermaßen klassifiziert:

- „sehr wahrscheinlich“: einmal pro Woche und öfter
- „wahrscheinlich“: einmal pro Monat
- „möglich“: einmal pro Jahr
- „unwahrscheinlich“: alle 10 Jahre oder seltener

Unter Anwendung dieser Klassifizierungen und der bereits vorliegenden Erfahrungen ist die Eintrittswahrscheinlichkeit für Datenpannen im Beispielunternehmen, welche die Rechte Betroffener messbar und nachhaltig beeinflussen könnten, im Bereich von „möglich“ zu erwarten.

Ein mögliches Schadensausmaß wird durch das BSI im IT-Grundschutz in vier Abstufungen vorgenommen: „niedrig, mittel, hoch, sehr hoch“.

Die Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Art. 9 DS-GVO erfordert ein „dem Risiko angemessenes Schutzniveau“. In Anwendung des Standards „IT-Grundschutz“ ist das Risiko für eine mögliche Verletzung des Datenschutzes bei den personenbezogenen Daten der Klienten des „Gartenhaus“ e.V. folgendermaßen zu bewerten.

Abb.7 Schadenszenario Datenpanne Klientendaten

Wahrscheinlichkeiten		Auswirkung u.	Schaden	
	niedrig	mittel	hoch	sehr hoch
sehr wahrscheinlich	gering	mittel	hoch	sehr hoch
wahrscheinlich	gering	mittel	hoch	hoch
möglich	gering	gering	„Datenpanne“ Klientendaten	mittel
unwahrscheinlich	gering	gering	gering	gering

Quelle : eigene Darstellung in Anlehnung BSI

In Auswertung der Bedrohungslage sind die Risiken für die Verarbeitung personenbezogener Daten im Unternehmen wie folgt darstellbar:

Der Verlust oder die nichtautorisierte Veränderung von personenbezogenen Mitarbeiterdaten ist auf Grund der eingeschränkten Anzahl an Verarbeitern „unwahrscheinlich“ bis „möglich“. Die Schadensauswirkungen sind vergleichsweise gering. Hier sind nach Auffassung des Verarbeiters die bisher eingeleiteten Maßnahmen zum Datenschutz/Datensicherheit ausreichend.

Der Verlust, die Offenlegung oder die Manipulation von Klientendaten hingegen sind in der Betrachtung durchaus „möglich“. Das Schadensausmaß ist bei Eintritt einer solchen Datenpanne mit „hoch“ bis „sehr hoch“ zu verorten. Das Ansehen und die Gesundheit des Klienten können gefährdet werden, die berufliche Zukunft auf Grund der Gesundheitsdaten fraglich und somit der gesellschaftlicher Rang des Betroffenen vakant werden. Das Bundesdatenschutzgesetz gibt mit § 64 „Anforderungen an die Sicherheit der Datenverarbeitung“ weitere Anhaltspunkte für den Datenverarbeiter bei der Auswahl und Umsetzung von Vorbeugemaßnahmen.

6.6 Datenverarbeitung Klientendaten

6.6.1 Leistungsträger (ITP)

Für die Einführung des Integrierten Teilhabepfandes (ITP) in Mecklenburg-Vorpommern zeichnete eine Projektsteuerungsgruppe unter der Leitung des Sozialministeriums des Landes Verantwortung.

Die Arbeitsgemeinschaft Sozialamtsleiter in Mecklenburg-Vorpommern hat innerhalb dieser Projektsteuerungsgruppe mit Datum vom 08.11.2017 beschlossen, dass auf regionaler Ebene (Kreise und Kommunen) zu entscheiden ist, zu welchem Zeitpunkt die Leistungserbringer in den Prozess des Gesamtplanverfahrens hinzuzuziehen sind.

Der zuständige Leistungsträger für die Versorgungsregion Vorpommern-Rügen hat in der weiteren Folge festgelegt, verkündet auf einer Informationsveranstaltung am 11.04.2018, dass der Erstantrag und damit die Datenerhebung gem. § 67a Abs. 2 SGB X beim zuständigen Sachbearbeiter des Landkreises in Form einer Gesamtplankonferenz zu erfolgen hat.

Dabei sollen zur Verbesserung der Ansprechbarkeit für den Bürger und zur Effizienzsteigerung im Antragsverfahren die Leistungsträger SGB IX und SGB XII zusammengelegt werden. Somit hat der Antragssteller nur noch einen Ansprechpartner bei seinem zuständigen Leistungsträger. Der Kreis der Anwender für die sensiblen Daten des Leistungsberechtigten wird damit in der öffentlichen Verwaltung verkleinert. Eine Verpflichtung zur Mitwirkung des Hilfesuchenden dabei ergibt sich aus § 21 Abs. 2 SGB X i. V. m. § 60 SGB I.

Grundsätzlich gilt mit § 35 SGB I, „Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Absatz 2 Zehntes Buch) von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis).“ Die personenbezogenen Daten der Hilfesuchenden sollen so bei den Leistungsträgern geschützt werden.

Die Einwilligung zur Weitergabe der personenbezogenen Daten nach § 67b SGB X an einen Leistungserbringer gibt der Betroffene mit dem ITP-Ergänzungsbogen D „Rechtliche Aufklärung zum Datenschutz“ (Anlage 5) des ITP M-V. Darin werden explizit alle Empfänger, ggf. auch mehrere Leistungserbringer, für die personenbezogenen Daten aufgeführt. Gleichzeitig dient dieser Ergänzungsbogen dem Datenverarbeiter, hier Leistungsträger, als Nachweis der vollzogenen Aufklärung nach Art. 13, 14 DS-GVO.

Nach erteiltem Feststellungsbescheid kann der Leistungserbringer mit Übergabe des ITP und ggf. notwendiger Ergänzungsbögen die individuelle und personenzentrierte Hilfe laut Teilhabeplan anbieten.

Mangels vorhandener digitaler Verschlüsselungssysteme zwischen Leistungsträger und Leistungserbringer muss die Übermittlung der Daten in Form einer Papierakte (persönlich oder Post) erfolgen. Eine mögliche digitale Lösung für diesen Kommunikationsweg wird seitens des Landkreises Vorpommern-Rügen noch geprüft.

Die notwendige Zuarbeit vom Leistungserbringer, z.B. Bogen 7a, 7b und 8 des ITP (Überprüfung Zielerreichung ITP), erfolgt auf gesichertem manuellen oder postalischen Weg nach Zeitablauf des Feststellungsbescheides oder auf Einzelfallanfrage durch den Leistungsträgers.

6.6.2 Datenverarbeitung durch den Leistungserbringer

Die Verarbeitung der personenbezogenen Daten im Beispielunternehmen erfolgt ausschließlich durch autorisiertes Personal; die notwendigen Zugangs- und Zugriffsrechte sind nach Fach- und Hilfspersonal definiert (A3_TOM).

Kommt es im Vorfeld einer Betreuung zu einem Interessentengespräch bzw. einer Besichtigung der Einrichtung durch den Klienten, so ist bereits zu diesem Zeitpunkt über eine Datenerhebung (Anlaß/Zweck) mittels QMH B2 FM 7.2-3 i. V. m. QMH B2 FM 4.2.4-3 zu belehren.

Erhobene Daten mit dem ITP werden, so umfangreich wie für die individuelle Zielerreichung benötigt, in das Klientendokumentationsprogramm procure der Firma Moveo Software GmbH eingepflegt. Zusätzlich wird eine Handakte angelegt, um den laufenden Schriftverkehr und unterschriftspflichtige Dokumente z.B. Belehrungen abzulegen.

Grundsätzlich sollten die vom Leistungsträger im ITP erhobenen Daten bei der individuellen Therapieplanung für den Klienten ausreichend sein, damit der Arbeitsauftrag für den Leistungserbringer in Bezug auf die Umsetzung der Hilfen für Zielerreichung des Klienten klar definiert ist.

Das betreute Klientel im Beispielunternehmen, psychisch kranke Erwachsene, zeichnet sich auf Grund der Krankheitsbilder dadurch aus, dass es wegen seiner Beeinträchtigungen nicht immer Willenserklärungen zielführend und im Sinne einer effektiven Hilfeplanung abgeben kann.

Die Notwendigkeit zur Erhebung und Verarbeitung zusätzlicher Informationen kann deshalb im weiteren Therapieverlauf angezeigt sein. Aus diesem Grund und falls noch kein verbindlicher ITP im System hinterlegt wurde, muss der Leistungserbringer durch Einzelgespräche weitere Daten des Klienten sammeln und auswerten. In diesem Fall hat der Leistungserbringer seiner Informationspflicht gem. Art. 13f DS-GVO nachzukommen. (QMH B2 FM 4.2.4-3 Informationspflicht Klient)

Eine zusätzliche Einwilligungserklärung zur Erhebung weiterer personenbezogener Daten muss der Klient nur dann abgeben, wenn sich im Rahmen der Betreuung die Notwendigkeit für eine Verfolgung neuer Ziele (andere Zweckbindung) ergibt. Diese sind vor Antritt zur Sicherstellung der Finanzierung mit dem zuständigen Sachbearbeiter des Leistungsträgers zu kommunizieren und sich genehmigen zu lassen. Eine Trennbarkeit der jeweiligen Verarbeitung nach § 64 Abs. 3, S. 1, Nr. 14 BDSG muss dabei gewährleistet werden.

Hinweise zu Betroffenenrechten beim Leistungserbringer erfolgen in einer Datenschutzerklärung § 33 des jeweiligen Wohn- und Betreuungsvertrages (WuBV) mit dem Klienten. Für die teilstationären und ambulanten Angebote des „Gartenhaus“ e.V. muss eine einfache und leicht nachvollziehbare Verknüpfung zwischen Betreuungsvertrag und einer Belehrung gem. Art. 13, 14 DS-GVO noch erfolgen.

An den Betreuungsprozessen der sozialen Arbeit sind regelmäßig auch externe Partner, wie z.B. Ärzte, Psychologen beteiligt. Damit ein Informationsaustausch zwischen den Parteien stattfinden kann, unterzeichnet der Klient im Vorfeld einer notwendigen Kommunikation eine Schweigepflichtentbindung auf einem internen Formular des Qualitätshandbuches. Diese wirkt rechtlich wie eine Inanspruchnahme des Rechts auf Datenübertragung Betroffener nach Art. 20 Abs. 1, 2 DS-GVO. Eine allgemeine und andauernde Entbindung von der Schweigepflicht gegenüber Institutionen und Personengruppen ist rechtlich nicht wirksam.

Bestimmte Berufsgruppen unterliegen einer besonderen gesetzlichen Verschwiegenheitspflicht. So müssen Ärzte und Psychologen nach § 203 Abs. 1, Nr.1 StGB, aber auch staatlich anerkannte Sozialarbeiter/ Sozialpädagogen nach § 203 Abs. 1, Nr. 6 StGB damit rechnen, dass sie im Falle der nicht autorisierten Geheimnisoffenbarung gegenüber Dritten mit einer Freiheitsstrafe von 1 Jahr oder einer Geldbuße bestraft werden.

„Der Gesetzgeber hat mit der Einbeziehung des Sozialarbeiters/Sozialpädagogen das Signal gegeben, daß diesen Berufsangehörigen gegenüber sehr wohl eine persönliche Vertrauensbeziehung besteht und entsprechend geschützt werden soll.“

(Mörsberger, 1985, S.73)

Aber auch die „berufsmäßig tätigen Gehilfen“ der o.g. Berufsgruppen unterliegen der besonderen beruflichen Schweigepflicht. (§ 203 Abs.3 StGB).

Nach Krahmer und Stähler ist dabei das Tatbestandsmerkmal der Berufsmäßigkeit entscheidend, d.h. dem inneren Zusammenhang zur beruflichen Tätigkeit des Geheimnisträgers muss Rechnung getragen werden. „Der Schweigepflicht unterliegen zudem auch die in der entsprechenden Berufsvorbereitung befindlichen Personen, wie z.B. Praktikanten, Hospitanten, Referendare“ (Krahmer/Stähler, 2003, S.192)

Eine kontinuierliche und transparente Arbeitsweise in der Betreuung, im Beispielunternehmen findet diese im Bezugsbetruersystem statt, verschafft dem Klienten das Gefühl, dass seine persönlichen Daten und Informationen zielführend bei der Planung und Realisierung der Ziele laut Teilhabepflicht eingesetzt werden. Die Erstellung von Verlaufsdocumentationen zu den Klienten im Dokumentationssystem procure soll das beteiligte Betreuungsfachpersonal informieren, den Umfang der Zielerreichung darstellen sowie den Datenbestand zum Klienten laufend aktualisieren.

Das Dokumentationssystem procure ist dabei das zentrale Verarbeitungssystem, auf das alle Einrichtungen mittels IT-Terminalserver zugreifen. Die Zugriffsrechte sind entsprechend der Qualifikation und Regionalität im Unternehmen festgelegt. Der betreuende Mitarbeiter kann dabei nur auf die Datenbestände seiner Einrichtung zugreifen. Aus Gründen der Vertretbarkeit vor Ort ist es nicht möglich an dieser Stelle die Zugriffsrechte noch weiter zu beschneiden.

Um die jederzeitige Verfügbarkeit (§ 64 Abs. 3 Nr. 10 BDSG) des Systems procure zu gewährleisten besteht ein Softwarepflegevertrag mit der Firma Moveo Software GmbH. Eine Zusatzvereinbarung zum entsprechenden Pflegevertrag, auf Grund der Möglichkeit einer Einsichtnahme im Rahmen einer Fernwartung durch Moveo Software GmbH, liegt mit Datum 06.07.2018 dem Datenverarbeiter zur Prüfung und Unterschriftsleitung vor.

Verlassen Klienten die Betreuungsangebote des „Gartenhaus“ e.V. werden die Daten des Betroffenen in procure gesperrt und sind nicht mehr für die betreuenden Mitarbeiter

einsehbar. Eine endgültige Löschung des jeweils individuellen Datenbestandes kann nach § 630f BGB erst 10 Jahre nach Betreuungsschluss erfolgen.

Die geschlossenen Papierakten werden gem. VA 7.1-1 „Planung und Dokumentation der Betreuung“ in der Geschäftsstelle unter Doppelverschluss archiviert. Entsprechende Zutrittsrechte sind eingerichtet.

6.6.3 Kontrollrechte des Leistungsträgers

Der regional zuständige Landkreis Vorpommern-Rügen führt regelmäßige Heimaufsichten nach § 8 Abs. 1 i. V. m. § 2 Absatz 1 und 2 EQG M-V in allen vollstationären Einrichtungen im Zuständigkeitsbereich durch. Zusätzlich werden für die verhandelten Prüfungs- und Leistungsvereinbarungen sogenannte Anlage-H Prüfungen gem. § 20 Abs. 2 LRV M-V durchgeführt. Ziele der Prüfungsvorgänge sind die Überwachung der Qualitätsanforderungen sowie die Kontrolle auf Konformität zwischen der verhandelten sächlichen und personellen Ausstattung und der tatsächlich vorgefundenen Situation am Prüfungstag.

Im Zusammenhang mit diesen Prüfungsvorgängen werden personenbezogene Daten des Betreuungs- und Hilfspersonals sowie stichprobenhaft (aktuell 3 je Vorgang) auch die Klientendokumentationen gesichtet und bewertet. Das Recht zur Einsichtnahme wird durch den örtlichen Leistungsträger mit § 8 Abs. 3, Nr. 3 EQG M-V sowie § 20 Abs. 5, 6 HeimG begründet.

Dr. Stefan Walz, ehemaliger Landesdatenschutzbeauftragter in Bremen, formulierte in einem seiner Referate als Stellungnahme zum Konflikt zwischen Sozialgesetzgebung und dem Grundrecht auf informeller Selbstbestimmung wie folgt:

„Die effiziente Kontrolle des korrekten Leistungsbezuges ist ohne jeden Zweifel ein berechtigtes Instrument von Politik und Verwaltung, um auch angesichts zunehmend knapper Ressourcen Verteilungsgerechtigkeit zu sichern. Doch läßt sich feststellen, daß die Bekämpfung angeblicher und wirklicher Leistungsmißbräuche zu sensiblen Spezialdaten und Datenabgleichen führt, bei denen der Eingriff in die Datenschutzrechte der Betroffenen außer Verhältnis zum angestrebten Überprüfungszweck steht.“(Blobel, 1995, S.72)

Schwerpunkte der Prüfvorgänge sind, neben einer Kontrolle der Einhaltung aller rechtlichen und behördlichen Vorgaben, die Analysen, ob die im Teilhabeplan festgelegten Ziele der Klienten durch die Leistungserbringer sich in individuellen Therapieplänen in der vereinbarten Qualität wiederfinden lassen.

Die Zielformulierungen aus den Teilhabegesprächen erfordern in der sozialen Arbeit ein breites Spektrum an persönlichen Daten zur Zielerreichung. So sollten zur Datenminderung die Stamm- und die Verlaufsdaten zielführend dokumentiert werden. Damit können zusätzliche und nicht benötigte Dokumentationen im Interesse des Betroffenen vermieden werden. Die Mitwirkungspflicht und damit das Einverständnis des Betroffenen gem. §§ 60 bis 62, 65 SGB I wird vorausgesetzt.

Aus Anlass einer angemeldeten Heimaufsicht ist die Besichtigung von Bewohnerzimmern durch die Vertreter des Leistungsträgers ausdrücklich nur mit Zustimmung und in Anwesenheit des Betroffenen möglich.

6.6.4 Datenlöschung / Datenträgerentsorgung Klienten

Der Verbleib von Klientendaten in Dateisystemen des Gartenhaus e.V. wird durch zwei grundlegende Anforderungen geprägt.

Einerseits ist die Wahrscheinlichkeit der Wiederaufnahme eines Klienten nach der Entlassung aus der Betreuung, wenn er in seinem gewöhnlichen Wohnumfeld verbleibt, relativ hoch. Das Vorhandensein historischer Daten des Klienten erleichtern die weitere Betreuungsplanung. Die Reintegrationsrate, also der Anteil der Klienten, die nach einer Entlassung keine Hilfen nach SGB XII benötigen, lag 2015 im „Gartenhaus“ e.V. bei 12,9 % und 2016 bei ca. 9,8 % (Managementbericht, 2017, S.134).

Zusätzlich besteht die theoretische Möglichkeit von Anfragen nachgelagerter externer Betreuungsangebote, aber auch von Kliniken und Ärzten, zur bisherigen Krankengeschichte. Die Einwilligung bzw. Schweigepflichtsentbindung des Klienten vorausgesetzt, kann hier mit den erhobenen Daten wertvolle Unterstützung im Interesse einer weiteren Genesung des Klienten gegeben werden.

Nach Ablauf einer 10jährigen Frist (§630f BGB) werden die Klientenakten, wie im QMH in der Verfahrensanweisung „Planung und Dokumentation der Betreuung“ festgelegt, über einen zuverlässigen Datenträgerentsorger der Vernichtung zugeführt.

Die Freigabe dazu erteilt der betriebliche Datenschutzbeauftragte des Vereins. Eine lückenlose Transportkontrolle, § 64 Abs. 3, S. 1, 8. BDSG, wird durch persönliche Übergabe der Papierakten in verschlossenen Aktenvernichtungstonnen beim Entsorger, die Stralsunder Werkstätten gGmbH, sichergestellt. Die erfolgte Datenträgervernichtung wird durch ein Vernichtungsprotokoll dokumentiert.

Für die digitalen Daten der Klienten, im Klientendokumentationssystem, müssen Löschkonzepte entwickelt werden. Die Daten der Klienten im Dokumentationssystem procure befinden sich in ihrer Gesamtheit auf einem Server in der Geschäftsstelle, d.h. die Mitarbeiter der Einrichtungen dokumentieren mittels Terminalserver zentral. Zusätzlich sind aber auch noch Dokumente auf Windows-Ebene auf den Arbeitsplatzrechnern der Einrichtungen gespeichert. Hier soll ein einheitliches Ablagesystem das schnelle Auffinden und Löschen von Daten perspektivisch ermöglichen.

6.7 Datenverarbeitung Mitarbeiterdaten

Im Rahmen von Beschäftigtenverhältnissen ist es für den Arbeitgeber notwendig und gesetzlich vorgeschrieben, eine Vielzahl von personenbezogenen Daten seiner Angestellten zu erheben, zu dokumentieren und zu bearbeiten. Das betrifft sowohl abrechnungsrelevante, z.B. zur Lohn- und Gehaltserstellung, als auch nichtabrechnungsrelevante Daten, z.B. im Arbeits- und Gesundheitsschutz oder zur Berechnung der Schwerbehinderten-Ausgleichabgabe (§154 Abs. 1 SGB IX).

Bereits im Rahmen des Bewerbungsverfahrens ist es notwendig, personenbezogene Daten zu erfassen und für die Prüfung einer Eignung des Bewerbers zu selektieren.

Der Art. 6 Abs. 1 lit. b DS-GVO gestattet eine rechtmäßige Verarbeitung zur „...Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Betroffenen erfolgen.“ Fragen des Arbeitgebers in diesem Verfahren zu besonderen Kategorien personenbezogener Daten sind neben dem Art. 9 Abs. 1 DS-GVO und auch auf Grund von § 1 Abs. 1 Allgemeines Gleichstellungsgesetz (AGG) unzulässig.

Mit Einstellung des Beschäftigten sind die Arbeitgeber gem. § 41 Abs. 1 ESTG verpflichtet, Lohnkonten für die Arbeitnehmer zu führen. Diese dienen der Berechnung von Lohnsteuer und Sozialabgaben. Rechtsgrundlagen für die Erhebung und Abführung der Sozialversicherungsbeiträge finden sich im dritten Abschnitt SGB IV § 28 ff..

Die Rechtmäßigkeit der Verarbeitung resultiert aus Art. 6 Abs. 1, lits. b, c DS-GVO. Danach ist eine Verarbeitung rechtmäßig, wenn der Verarbeitende dies zur Erfüllung eines Vertrages, dessen eine Vertragspartei der Betroffene ist, erforderlich ist sowie wenn er auf Grund einer rechtlichen Verpflichtung handelt.

Weitere datenschutzrechtliche Rahmenbedingungen für den Beschäftigtendatenschutz sind in Art. 88 Absatz 1 u. 2 der DS-GVO festgeschrieben.

Die Öffnungsklausel in Art. 88, Absatz 1 „Die Mitgliedsstaaten können [...] spezifischere Vorschriften [...] vorsehen.“ bot dem deutschen Gesetzgeber die Möglichkeit in der aktuellen Fassung des BDSG vom 30.06.2017 mit § 26 weitere Regulierungen im Umgang mit Beschäftigtendaten vorzunehmen.

Der Arbeitgeber ist verpflichtet, seine Mitarbeiter nach Art. 13 DS-GVO über den Umgang mit den personenbezogenen Daten zu informieren. Dieser Verpflichtung kommt der Gartenhaus e.V. seinen Beschäftigten gegenüber in Textform, § 26 Abs. 2, S. 4 BDSG, mit dem Formular QMH B2 FM 4.2.4-2 nach. Besondere Bedeutung bekommt diese Verpflichtung zur Information im Beispielunternehmen, wie bei anderen Arbeitgebern auch, weil besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 2 lit. b DSGVO verarbeitet werden müssen.

Grundsätzlich ist eine zusätzliche Einwilligungserklärung des Arbeitnehmers zur Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. a DS-GVO, auch wegen der detaillierten Bedingungen nach Art. 7 Abs. 1ff. DS-GVO für den Zweck der Datenverarbeitung im Beschäftigungsverhältnis nicht notwendig. Einer Schriftform, wie in § 26 Abs. 2, S. 3 BDSG gefordert, bedarf es damit nur, wenn eine Einwilligung des Betroffenen die Rechtsgrundlage der Datenverarbeitung ist.

6.7.1 Abrechnungsrelevante Daten der Mitarbeiter

Die Eingabe und Pflege von Stammdaten bei Beschäftigungsaufnahme und bei Veränderungen erfolgen in QMH B2 FM 6.2-13/1 (bei Zuverdienst FM 6.2-13/2) sowie anschließend im lizenzierten Lohnprogramm „Standard Line Modul Lohn & Gehalt“ der Firma Helmerich-PCAS Software & Service GmbH. Zusätzlich werden Leistungsdaten erfasst, die zur Berechnung einer leistungsgerechten Vergütung sowie deren gesetzlicher Abgaben benötigt werden.

Die Verarbeitung von Stamm- und Leistungsdaten erfolgt an nur einem einzigen passwortgeschützten Arbeitsplatzrechner in der Personalbuchhaltung. Dieser Rechner muss zur Übertragung der Abrechnungsdaten (Lohnsteuer und Sozialversicherung) mit den Finanzbehörden sowie den Empfängern der Daten zur Sozialversicherung über das Internet verbunden sein.

Die Erfüllung der Anforderung einer Übertragungskontrolle gem. § 64 Abs. 3, S. 1, Nr. 6 BDSG ist durch den einen Datenverarbeitungsplatz gewährleistet. Die Rechtsgrundlagen für eine Datenweitergabe sind im Anhang 2.1, Verfahrensverzeichnis Lohn- und Gehaltsabrechnung, zusammengefasst.

Die Buchungskreise Personalbuchhaltung und Sachbuchhaltung (DATEV) sind im Beispielunternehmen getrennt. Zur Implementierung der Personalkosten in die Finanzbuchhaltung werden jeweils anonyme Kostenaufstellungen je Einrichtung ausgedruckt und manuell in die Sachbuchhaltung eingepflegt. Es gibt keine Schnittstellen zwischen den beiden Buchungskreisen. Somit ist eine ungewollte Datenveränderung über einen digitalen Datenimport ausgeschlossen. Gleichzeitig ist eine Ursachenforschung bei auftretenden Datenabweichungen vereinfacht möglich.

Die Übergabe des Datenbestandes zur Erstellung des Jahresabschlusses an das beauftragte Steuerberatungsbüro erfolgt für die Sach- und Personalbuchhaltung mittels verschlüsselten Datenträger. Die Steuerberatung handelt dabei, im Auftrag des Mandanten eigenverantwortlich und weisungsunabhängig. Sie ist somit kein Auftragsverarbeiter im Sinne Art. 28 Abs. 3 lit. a DS-GVO. Ihre Weitergabe der Betriebsdaten von Mandanten an ein unabhängiges Dienstleistungsrechenzentrum (DATEV) stellt jedoch eine Auftragsverarbeitung im Sinne des Art. 28 DS-GVO, hier dann jedoch für die Steuerberatung als Verantwortlichen dar.

Im Verlauf von Beschäftigtenverhältnissen werden dem Arbeitgeber weitere besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO bekannt. So sind Angaben zur Arbeitsunfähigkeit des Arbeitnehmers, Angaben zur Freistellung bei notwendiger Krankheitspflege des minderjährigen Kindes aber auch Gesundheitsdaten, z.B. im Rahmen des betrieblichen Eingliederungsmanagements nach § 84 Abs. 2 SGB IX beim Arbeitnehmer, zu verarbeiten. Entsprechende interne Verfahrensverzeichnisse wurden hierzu erstellt und sind in der Anlage der Thesis unter A2.1 bis A2.14 zu finden.

Eine weitere Rechtsgrundlage für die Verarbeitung von besonderen Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses bietet das BDSG mit § 26 Abs. 3. Danach ist die Verarbeitung rechtlich zulässig, wenn sie „... zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist.“

Zusätzlich enthält das QMH des Vereins, Stand Mai 2018, hierzu umfangreiche Festlegungen in den Verfahrensanweisungen. Diese sind für alle Mitarbeiter und Beschäftigte verbindlich. Für die Gewährleistung der Aktualität und zur Sicherstellung der Konformität werden auch an dieser Stellen regelmäßige Revision durchgeführt.

6.7.2 Personalentwicklung / Mitarbeiterführung

Im Personalentwicklungskonzept des QMH Teil A, Seite 3, vom 20.01.2009 sind die Schwerpunkte der Personalentwicklung im Unternehmen festgeschrieben. Es sind dies die Möglichkeit sich stetig fachlich und persönlich zu entwickeln, sich bei der Arbeit wohl zu fühlen und als Mitarbeiter auch Verantwortung zu übernehmen.

Dafür sind formale, systemische und prozessorientierte Maßnahmen notwendig.

A) Zu den formalen Personalentwicklungsmaßnahmen zählen neben detaillierten Arbeitsverträgen und Stellenbeschreibungen auch Weiterbildungssetats mit den entsprechenden zeitlichen Kapazitäten zur Teilnahme für die Mitarbeiter. Dabei ist es von Vorteil, neben der Kenntnis zur beruflichen Qualifikation auch Präferenzen bei den Fort- und Weiterbildungen der Beschäftigten in Erfahrung zu bringen und im Zusammenhang mit der Fortbildungsplanung zu verarbeiten.

„Die Speicherung von Schulungsdaten ist für die Durchführung des Arbeitsverhältnisses streng genommen nicht erforderlich. Sie ist aber für die Erfüllung eigener Geschäftszwecke zulässig, weil sie zur Wahrung berechtigter Interessen des Arbeitgebers nach Art. 6 Abs. 1 lit. f DS-GVO erforderlich.“ sind [Anm. d. Verf.]

(Wächter, 2017, S. 62)

Erhebungen zu Schulungsdaten sind gesetzlich durch Forderungen aus dem Einrichtungen- und Qualitätsgesetz (EQG MV), der Einrichtungenpersonalverordnung (EPersVO M-V) oder durch die Leistungs- und Prüfungsvereinbarung (LPV M-V) zur Ermittlung und dem Nachweis der Fachkraftquote gedeckt.

Rechtsgrundlage für das Erheben und Verarbeiten dieser Daten durch den Arbeitgeber ist der Arbeitsvertrag und damit die vom Arbeitnehmer anerkannte Umsetzung der Verfahrensanweisungen im Unternehmen. Hier ist der Arbeitgeber bei Beschäftigungsbeginn mit seiner Informationspflicht gem. Art. 13, 14 DS-GVO sorgsam nachzukommen, gefordert. In begründeten Einzelfällen kann eine Einwilligung des Beschäftigten nach Art. 6 Absatz 1 lit. a DS-GVO notwendig werden.

B) Systemische (periodische) Personalentwicklungsmaßnahmen sind die regelmäßigen Personalgespräche, siehe auch QMH B2 FM 6.2-11 (Anhang 4.4). In Auswertung des Fragenkataloges erhält der Interviewer, i.d.R. die Einrichtungsleitung, ein sehr umfassendes und tiefgreifendes Bild von den Interessen und Ansichten seiner Beschäftigten. Ob sich der Interviewer in dieser Situation auf den Sachgrund „Erfüllung eines Vertrages zwischen Betroffenen und Verarbeiter“ (Art. 22 Abs. 1 lit. a DS-GVO), berufen kann, bleibt im Einzelfall zu prüfen.

Zur datenschutzrechtlichen Klärung sollten sich beide Parteien, nach Auffassung des Verfassers, vor dem Gespräch eindringlich über die Zweckbindung und den Umfang der Daten verständigen und ggf. zur die Möglichkeit einer Einwilligung kommunizieren. Das entsprechende Formular QMH B2 FM 6.2-11 ist dahingehend zu verändern. Dem Mitarbeiter muss klar erkennbar sein, dass die Ergebnisse aus der Befragung, wenn auch nicht automatisiert verarbeitet, ein „Profiling“ nach Art. 4 Absatz 4 DS-GVO darstellen könnten. Die Betroffenenrechte nach Art. 22 Absatz 1 DS-GVO sind gewährleistet, da das Bewertungssystem transparent kommuniziert wird, keine automatischen Auswertungen erfolgen, und der Mitarbeiter jederzeit in der Lage ist, Fehlinterpretationen zu korrigieren.

C) Zu den prozessorientierten Personalentwicklungsmaßnahmen zählen Handlungsvorgänge, die aus dem laufenden Prozess und ohne wesentliche Standards, ergriffen werden. So können Mitarbeiter in Team- und Einzelreflexionen sowie Supervisionen auf innerbetriebliche Entwicklungsprozesse Einfluss nehmen. Diese Sitzungen finden unter fachkundiger Anleitung externer Supervisoren und ohne schriftliche Aufzeichnungen statt. Den Mitarbeitern des Beispielunternehmens wird von der Geschäftsleitung empfohlen an diesen Terminen teilzunehmen. Über zu behandelnden Themen kann dabei frei im Team entschieden werden.

6.7.3 Datenlöschung /Datenträgerentsorgung Mitarbeiter

Grundsätzlich hat jeder Betroffene nach Art. 17 Abs. 1 lit. a DS-GVO das Recht, bei Ablauf der Zweckbindung vom Datenverarbeiter, seine personenbezogenen Daten löschen zu lassen. Für die Betriebsunterlagen, hier seien die Stamm- und Leistungsdaten zur Abrechnung der Beschäftigung erwähnt, gelten die gesetzlichen Aufbewahrungsfristen in § 147 Abs. 3 Satz 1 AO.

Danach sind die Datenträger, auch aus Gründen der Datenminderungspflicht, Art. 5 Abs. 1 lit. c DS-GVO erst nach Ablauf von 6 Jahren, beginnend mit dem 31.12. des abgeschlossenen Geschäftsjahres, zu vernichten.

Entsprechende Datenträger sind im Unternehmen papierhaft und auch digital vorhanden. Während die Frist zur Vernichtung von Verwaltungsakten durch das letzte manuelle Bearbeitungsmerkmal gekennzeichnet ist, muss für die digitalen Daten ein Löschkonzept entworfen werden. Hier wirkt sich die personelle Beschränkung bei der Bearbeitung personenbezogener Daten in der Personalbuchhaltung positiv aus, da insgesamt nur 2 Arbeitsplatzrechner entsprechend präpariert werden müssen.

Eine Besonderheit stellt in den Unternehmen die notwendige Aufbewahrungsfrist von Unterlagen abgelehnter Bewerber dar. Danach kann es sinnvoll für das Unternehmen sein „... für einen gewissen Zeitraum – z.B. sechs Monate, zusammengesetzt aus der zweimonatigen Beschwerdefrist nach § 15 II S. 1 AGG (G/S BDSG § 35 Rn. 13b) und einem Sicherheitspuffer von 4 Monaten ...“ Unterlagen aufzubewahren, „...falls ein abgelehnter Bewerber wegen Verstoß gegen das AGG anwaltlich oder gerichtlich gegen das Unternehmen vorgeht.“ (Wächter 2017, S. 346) Eine gewissenhafte Dokumentation des Bewerbungsverfahrens durch den Personalverantwortlichen, z.B. durch persönliche Notizen, helfen im Klagefall eine zielgerichtete Abwehr der Ansprüche durchzuführen.

Die Entsorgung der papierhaften Personalverwaltungsakten soll, aus Gründen der Stärkung gemeinnütziger Träger in der Versorgungsregion, zukünftig auch bei den Stralsunder Werkstätten gGmbH erfolgen. Das Unternehmen war bereits in der Vergangenheit für den „Gartenhaus“ e.V. in der fachgerechten Entsorgung von sensiblen Akten tätig. Mit Datum 06.07.2018 wurde hierzu ein rechtsverbindlicher Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 Abs. 3 DS-GVO unterzeichnet.

Zusätzlich erfolgte am 09.05.2018 durch den Datenschutzbeauftragten des Vereins eine Inaugenscheinnahme der betrieblichen Abläufe bei den Stralsunder Werkstätten gGmbH. Die organisatorischen und technischen Voraussetzungen lassen eine Freigabe, unter Voraussetzung einer Zusatzvereinbarung „Auftragsdatenverarbeitung“, zu.

Digitale Datenträger z.B. alte Arbeitsplatzrechner und externe Datensicherungsfestplatten werden über die Firma Gecko mbH einer Demontage mit anschließender Löschung zugeführt.

Die entsprechende Zusatzvereinbarung wurde rechtsverbindlich zwischen dem Beispielunternehmen und Gecko mbH am 07.06.2017 vereinbart. Über eine erfolgte fachgerechte Vernichtung der Datenträger erhält der Auftraggeber eine Protokollabschrift.

6.7.4 Betriebsrat

Am 14.05.2018 wurde im Unternehmen „Gartenhaus“ e.V. ein neuer Betriebsrat gewählt. Betriebsräte sind nach § 3 BetrVG das gesetzliche Organ zur Wahrung der Arbeitnehmerinteressen gegenüber dem privaten Arbeitgeber. Nach § 26 Abs. 1 S. 1 BDSG ist der Betriebsrat als Interessenvertretung der Arbeitnehmer zur Verarbeitung von personenbezogener Daten im Rahmen von Beschäftigungsverhältnissen ermächtigt. Dabei haben die Mitglieder des Betriebsrates laut § 79 Abs. 1 BetrVG besondere Sorgfaltspflichten bei der Einhaltung des Datenschutzes zu beachten.

Gewählte Arbeitnehmervertreter gewinnen auf Grund ihrer Funktion und besonderen Stellung im Unternehmen, große Mengen an zusätzlichen personenbezogener Daten der Beschäftigten. Gleichzeitig können die Mitglieder des Betriebsrates aber eine Überwachung der Verarbeitungsvorgänge durch den Datenschutzbeauftragten ablehnen, sich aber von ihm eingehend beraten lassen. Betriebsratsmitglieder sind als Arbeitnehmer dem Datenschutz im Unternehmen gemäß der DS-GVO verpflichtet.

Der Betriebsrat hat nach § 87 ff BetrVG umfangreiche Mitbestimmungsrechte, die er nur durch Kenntniserlangung von Informationen durch Arbeitnehmer oder Arbeitgeber auch wirksam umsetzen kann. Um eine unabhängige Arbeitsweise gem. § 78 BetrVG gewährleisten zu können, wurde dem Betriebsrat im Beispielunternehmen ein mobiler Arbeitsplatzrechner mit eigener und geschützter „email-Domäne“ zur Verfügung gestellt.

Ein separates Büro wurde außerhalb der Betriebsstätten angemietet und eingerichtet. Durch die räumliche Trennung von Betriebsratsbüro und Betreuungseinrichtungen/Verwaltung ist eine Diskretion bei den Sprechzeiten gewährleistet. Rechtsgrundlage der Datenverarbeitung ist Art. 6 Abs. 1 lit. b DS-GVO zur Wahrnehmung der gesetzlichen Arbeitnehmerrechte.

6.8 Mitgliederverwaltung

Der „Gartenhaus“ Psychosozialer Trägerverein Stralsund e.V. ist ein gemeinnütziger Verein, der beim Amtsgericht in Stralsund unter der Registernummer VR 249 eingetragen ist. Der Verein hat derzeit 3 Mitglieder und besteht aus einem ehrenamtlichen Vorstand, einem geschäftsführenden Vorstand und einem weiteren Mitglied. Eine Verwaltung der Mitgliederdaten kann auf Grund der begrenzten Personenzahl manuell erfolgen. Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten bietet Art. 6 Abs. 1 lit. f DS-GVO.

Es besteht ein berechtigtes Interesse seitens des Vereins, die Kontaktdaten der Mitglieder zu verarbeiten, um zu Mitgliederversammlungen und Vorstandssitzungen einzuladen. Eine Notwendigkeit zur Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DS-GVO besteht nicht.

Ein Programm zur digitalen Verarbeitung ist nicht notwendig, Art und Umfang des Risikos bei Datenverlust ist zu vernachlässigen. Angaben zur Mitgliedschaft in einem gemeinnützigen Verein der Wohlfahrtspflege schaden nicht dem Ansehen und dem gesellschaftlichen Status des Betroffenen. Bankdaten werden nicht erhoben, da alle Mitglieder die Mitgliedsbeiträge überweisen.

6.9 Betroffenenrechte

Hauptanliegen der DS-GVO war neben einer Harmonisierung des Datenaustausches innerhalb der EU auch die Stärkung der informellen Selbstbestimmung der privaten Endverbraucher. Dazu, so schreibt Härting auf S. 159 in seinem Werk, wurden die Betroffenenrechte und die Datenschutzaufsicht gestärkt und die Aufsichtsbehörden mit neuen Aufgaben und Befugnissen versehen. Wächter stellt das Kontrollsystem in seinem Werk „Datenschutz im Unternehmen“ auf Seite 142, Abschnitt 312 mit der Dreisäulen-Theorie der Datenschutzkontrolle dar.

„Unterstützend und begleitend zur Eigenkontrolle (Säule 1) hat der Gesetzgeber die Kontrolle durch die Betroffenen –die Selbstkontrolle (Säule 2) – und durch eigene Aufsichtsbehörden für den Datenschutz – die Fremdkontrolle (Säule 3) – vorgesehen.“ (Wächter, 2017, S. 142)

Die Eigenkontrolle (Säule 1) wurde bereits in den vorherigen Kapiteln z.B. mit den Datenschutz-Folgeabschätzungen und den Verfahrensanweisungen beschrieben. Säule 3, die Fremdkontrolle, wird im weiteren Verlauf in Kap. 6.9.4 behandelt.

Im Folgenden soll nun die Säule 2, die Selbstkontrolle durch die Betroffenen, betrachtet werden. Die Stärkung der Betroffenenrechte lässt sich durch die Konkretisierung der Anforderungen im Umgang mit personenbezogenen Daten darstellen. Mit der DS-GVO sind die Betroffenenrechte nun umfangreich und detailliert geregelt. Beginnend mit der Informationspflicht nach Art. 13, 14 DS-GVO hat der Betroffene auch im weiteren Verlauf seiner Vertragsbeziehungen zum Datenverarbeiter ein hohes Maß an Autonomie über seine personenbezogenen Daten. Zusätzlich werden die Betroffenenrechte in der nationalen Gesetzgebung mit Kap. 2, § 32 BDSG geregelt.

6.9.1 Informationspflicht Art. 13 DS-GVO

In den Kapitel 6.6 (Klientendaten) und 6.7 (Mitarbeiterdaten) wurde bereits die Verfahrensweise bei Neuaufnahmen von Klienten bzw. Beschäftigungsantritt neuer Mitarbeiter bzgl. der Angabe personenbezogener Daten beschrieben. Auch die Inhalte der Informationspflicht wurden je nach Zweckbindung in den Kapiteln bereits dargestellt. Für die Mindestanforderungen seiner Informationspflicht hat der Datenverarbeiter durch die Abs. 1, 2 des Art. 13 DS-GVO konkrete Vorgaben, zu Inhalten, die er dem zu informierenden Betroffenen mitzuteilen hat. Die Nennung der Informationspflicht gem. Art.13 u. 14 DS-GVO an dieser Stelle der Thesis dient einer zusammenfassenden Darstellung aller Betroffenenrechte in der DS-GVO.

6.9.2 Auskunftsrecht Art. 15 DS-GVO

Der Betroffene hat das Recht, Auskünfte über die Verarbeitung seiner personenbezogenen Daten vom Datenverarbeiter zu verlangen. Während nach Art. 13 DS-GVO der Betroffene nur informiert wird, wie mit seinen Daten zu verfahren ist, beinhaltet Art. 15 DS-GVO auch das Recht auf Auskunft der tatsächlich gespeicherten und verarbeiteten Daten.

Diesem muss der Datenverarbeiter nach Abs. 1, Satz 3 mit einer Kopie der personenbezogenen Daten, die er an den Betroffenen auszuhändigen hat, entsprechen.

Alternativ kann der Betroffene auch nach Art. 20 Abs. 1 DS-GVO seinen festgestellten Datenbestand „in einem strukturierten, gängigen und maschinenlesbaren Format“ verlangen.

Weiterhin ist der Betroffene mit den erhaltenen Daten in der Lage, festzustellen, ob der erhobene Datenbestand mit der vereinbarten Zweckbindung gem. Art. 13 Abs. 1 lit. c DS-GVO übereinstimmt. Werden hier Abweichungen festgestellt, kann der betreffende Klient oder Mitarbeiter nachträglich verlangen, sie zu ändern oder auch zu löschen. In jedem Fall wird zu klären sein, wer die zusätzlichen, falschen oder nichtautorisierten Daten erhoben hat und warum. Eine wirksame Hilfe bei der Rückverfolgbarkeit ist hier die Umsetzung der Eingabekontrolle nach § 64 Abs. 3 Nr. 7 BDSG.

Zusätzlich besteht für den Klienten als Patienten ein Einsichtsrecht in seine Dokumentationen als Nebenpflicht aus einem Behandlungs-/Betreuungsvertrag unter Berücksichtigung von Treu und Glauben (§ 242 BGB) sowie des allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

„Einschränkungen des Einsichtsrechts können sich lediglich aus – ebenfalls grundrechtlich fundierten – Interessen des Arztes oder Dritter, über welcher in der Dokumentation auch persönliches preisgegeben werden könnte, sowie therapeutischen Vorbehalten zu Schutz des Patienten ergeben.“ (Schneider, 2014, S.16)

Danach kann es laut Schneider angezeigt sein, dem psychiatrischen Klienten im Einzelfall (Krisensituation) zum Eigenschutz nur Dokumentationen objektiver Tatbestände offenzulegen oder aber die Einsichtnahme generell in Anwesenheit eines Arztes vornehmen zu lassen. Hier muss das betreuende Fachpersonal den Einzelfall abwägen, um eine Verschlechterung des Gesundheitszustandes aus Gründen der Kenntniserlangung zu vermeiden.

In jedem Fall sind alle Anfragen Betroffener an den Datenschutzbeauftragten des Vereins zu richten, weiterzuleiten und zu kommunizieren. Dies soll eine einheitliche und vor allem rechtssichere Verfahrensweise bei der Sicherung der Betroffenenrechte ermöglichen. Verbindlichkeit erreicht diese Festlegung im Handbuch B1 VA 4.2.4.2 unter Punkt 5.3.

6.9.3 Recht auf Berichtigung und Löschung Art. 16, 17 DS-GVO

Sollte eine Klient oder ein Mitarbeiter feststellen, dass die von ihm gespeicherten Daten unkorrekt oder nicht aktuell sind, so kann er durch Art. 16 DS-GVO eine Berichtigung in der Dokumentation verlangen.

Grundsätzlich hat der Klient, wie jeder andere Betroffene auch, Anspruch auf Korrektur von offenbar unrichtigen Daten. Jedoch besteht die Möglichkeit, dass er in seiner Wahrnehmung offensichtlich falsche Tatsachen als objektiv und real empfindet. In diesem Fall muss der Bezugsbetreuer unter Einbeziehung des gesetzlichen Betreuers oder des behandelnden Arztes den tatsächlichen Wahrheitsgehalt herausfinden und die Dokumentation angleichen. Eine vertrauensvolle und transparente Dokumentation durch den Betreuer erleichtert eine Feststellung der objektiven Tatsachen.

Für die Löschung und Vernichtung von Klientenakten gelten in Anlehnung an die gesetzlichen Vorgaben aus § 630f BGB (Patientenakten), eine Aufbewahrungsfrist von 10 Jahren. Dieser Zeitablauf soll dazu dienen, eine Einsichtnahme von Patient und Arzt/Behandler vor allem zur Prüfung von Haftungsansprüchen bei Langzeitschäden zu ermöglichen. Danach sind sie zur ordnungsgemäßen Vernichtung freigegeben.

Eine Berichtigung von Mitarbeiterdaten löst i.d.R. eine Korrekturabrechnung in der Personalbuchhaltung aus. Die Korrektur der Daten veranlassen die Mitarbeiter mit dem Formular QMH B2 FM 6.2-13. Zur Vermeidung von unautorisierter Einsichtnahme der Daten auf dem Übermittlungsweg ist die Form als Papierformular festgelegt worden. Dadurch hat der auskunftserteilende Mitarbeiter die Möglichkeit, für die Mitteilung einen verschlossenen Umschlages zu nutzen.

Mit Art. 17 DS-GVO ist der Datenverarbeiter nun erstmals verpflichtet auf Verlangen des Betroffenen und wenn der Zweck erfüllt ist, Daten zu löschen. Die Erfüllung dieser Verpflichtung setzt u.a. voraus, alle Orte der Datenlagerung innerhalb und außerhalb des Unternehmens, bei erfolgter Weiterleitung an Dritte, identifiziert zu haben.

Die Datenbestände der beiden Server für die Windows-Anwendungen und das Klientendokumentationsprogramm procure (Anlage 3 TOM) müssen dabei durch eine automatische Datenlöschung bereinigt werden.

Hier sind die beiden IT-Unternehmen Gecko mbH und Moveo Software GmbH gefordert, wirksame und effiziente Lösungen anzubieten. Bis dahin gilt die Einschränkung der Daten gem. § 35 Abs. 1 BDSG i. V. m. Art 18 Abs. 1 DS-GVO.

Die Forderung nach Löschung bzw. Vernichtung der Handakten kann durch eine einfache Erfassung der Entlassungsdaten von Klienten und anschließender Aussonderung nach 10 Jahren mit Vernichtung bei den Stralsunder Werkstätten gGmbH erfüllt werden. Eine Inventur des Aktenbestandes ist im Archiv vorzunehmen und der Datenbestand entsprechend sukzessive zurückzufahren.

6.9.4 Verletzungen des Datenschutzes Art. 33, 34 DS-GVO

Bei Eintreten der Kenntnis von Verletzungen des Datenschutzes im Unternehmen, im Besonderen bei personenbezogenen Daten, ist durch den Verantwortlichen binnen 72 Stunden die zuständige Aufsichtsbehörde darüber zu informieren. Die zuständige Aufsichtsbehörde für das Beispielunternehmen „Gartenhaus e.V. ist gem. Art. 4 Nr. 21, 22 DS-GVO i. V. m. § 40 Abs. 1 BDSG der Landesdatenschutzbeauftragte Mecklenburg-Vorpommern mit seinem Dienstsitz in Schwerin.

Der Art. 33 Abs. 3 DS-GVO fordert in der Meldung eine Beschreibung der Datenschutzverletzung, die Angabe zur Kategorie nach Art. 9 Abs. 1 DS-GVO, den Umfang der betroffenen Datensätze, eine Darstellung der möglichen Folgen sowie die Angabe möglicher Lösungsansätze, um die Folgen abzumildern. Eine sichere Gewährleistung dieser Meldekette erfordert im Unternehmen die Festlegung zu verbindlichen Handlungsanweisungen, wie im QMH B1 VA 4.2.4.2 beschrieben.

Sollte die Datenschutzverletzung für den Betroffenen ein voraussichtlich hohes Risiko bedeuten, so ist auch die betroffene Person „in klarer und einfacher Sprache“ gem. Art. 34 Abs. 1 DS-GVO vom Verantwortlichen zu informieren.

Die Meldung über eine „unrechtmäßige Kenntniserlangung von Daten“ in der vorherigen Fassung des BDSG nach § 42a S. 1 hatte unverzüglich erfolgen. Insofern präzisiert die DS-GVO nun die Meldepflicht auf exakt 72 Stunden nach Bekanntwerden beim Datenverarbeiter bzw. seines Auftragsverarbeiters.

6.9.5 Haftungsansprüche Betroffener

Bisher war eine Haftung des Datenverarbeiters nur auf nationaler Ebene, in Deutschland nach § 7 BDSG aF, möglich. Die DS-GVO nimmt nun mit ihrem Art.82 Abs. 1 den Datenverarbeiter, falls vorhanden auch seinen Auftragsverarbeiter, für materielle und immaterielle Schäden in die Verantwortung. ErwGr. 146 meint hierzu, dass die Betroffenen „...einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten.“ sollten.

Eine Haftung des Geschäftsführers des Beispielunternehmens würde damit in einer gerichtlichen Auseinandersetzung im Schadensfall wahrscheinlich. Die Union Versicherungsdienst GmbH in Detmold, als beauftragter Versicherungsmakler des „Gartenhaus“ e.V., bietet in ihrem Portfolio zur Absicherung dieses Risikos eine erweiterte Betriebshaftpflichtversicherung an, die auch im Falle der wissentlichen Pflichtverletzung durch die Geschäftsführung, Schadensersatz leistet.

Grundsätzlich wird durch die Rechtsprechung zukünftig zu klären sein, mit welcher Höhe ein immaterieller Schaden, verursacht durch Verletzung des Datenschutzes, zu bemessen ist. Welche konkreten Beträge aus Haftungsansprüchen Betroffener lassen sich aus einer Datenschutzverletzung herleiten?

Eine rechtskräftige Verurteilung des Verantwortlichen für ein datenschutzrechtliches Vergehen, mit Feststellung eines erheblichen Schadensersatzanspruches, kann sicherlich im Einzelfall genau so empfindlich für den Beklagten sein, wie ein zusätzlich zu verhängendes Bußgeld der Aufsichtsbehörde. Die betriebswirtschaftlichen Auswirkungen sind wegen der unklaren Rechtslage bei der Bemessung nichtmaterieller Schäden im Datenschutz noch nicht abschätzbar.

In diesem Zusammenhang sei erwähnt, dass ein mögliches Bußgeld für Datenschutzvergehen von max. 300.000,00 € (§ 43 Abs.3 S. 1 BDSG aF) auf nun maximal 20 Mio. € (Art. 83 Abs. 5 DS-GVO) erhöht worden ist.

Sicherlich ist die Erhöhung von Bußgeldern für ein Vergehen ein entscheidendes Kriterium für die Akzeptanz und Umsetzung gesetzlicher Anforderungen bei den Unternehmen. Grundsätzlich aber sollte das Bewusstsein der Betroffenen im Umgang mit ihren Daten das weitaus größere Druckmittel gegenüber den Datenverarbeitern sein.

7 Diskussion und Empfehlung

Der „Gartenhaus“ Psychosozialer Trägerverein Stralsund e.V. ist ein etablierter Bestandteil der Helferlandschaft in der Versorgungsregion Vorpommern-Rügen, welcher mit seinen multiprofessionellen Teams psychisch kranke Erwachsene betreut. Auf Grund der jahrelangen Erfahrung kann der Verein eine qualitativ hochwertige Betreuungsarbeit vorweisen. Mit der Zertifizierung 2007 hat dieser Anspruch nochmal einen signifikanten Qualitätssprung gemacht.

Ausgehend von einer beherrschten und dokumentierten Prozesslandschaft im Kerngeschäft, sind die Herausforderungen aus den Anforderungen von Bundesteilhabegesetz (BTHG) und Datenschutz-Grundverordnung (DS-GVO) für den Verein umsetzbar.

Die Aufbauorganisation im Unternehmen ist klar strukturiert und muss aus Gründen der hier beschriebenen rechtlichen Veränderungen nicht weiter angepasst werden. Die Aufgabenbereiche und Kompetenzen in den Einrichtungen sind über die Stellenbeschreibungen klar strukturiert. Die erforderlichen Rollen für die Umsetzung eines wirksamen Datenschutzes sind mit Geschäftsführung, Datenschutzbeauftragter und Datenanwender (Beschäftigte) ausreichend aufgestellt. Im Mittelpunkt der Betrachtung der Betreuungsarbeit stehen die Mitarbeiter, die mit den ihnen anvertrauten personenbezogenen Daten der Klienten verantwortungsvoll umgehen. Sie handeln im Auftrag des Prozessverantwortlichen, dem „Gartenhaus“ e.V..

Der interne betriebliche Datenschutzbeauftragte berät den Verantwortlichen, vertreten durch den geschäftsführenden Vorstand, sowie seine Mitarbeiter in allen Fragen des Datenschutzes und wacht über deren Einhaltung. Damit sind die Anforderungen aus der DS-GVO in der Aufbauorganisation vollumfänglich erfüllt.

Im Rahmen einer „fortlaufenden Verbesserung“ (DIN EN ISO 9001:2015 Kap. 10.3) nimmt das Beispielunternehmen in der Ablauforganisation durch die sich ändernden Rechtslagen laufend Anpassungen vor. Festgestellte Nichtkonformitäten werden entsprechend der Normenforderung DIN EN ISO 9001:2015 Kap. 10.2 erkannt, Maßnahmen zur Korrektur ergriffen und der Prozess einer regelmäßigen Wirksamkeitsüberprüfung zugeführt.

Neben der Erstellung von Dokumentationen zu Datenschutzfolgeabschätzungen, Verfahrensverzeichnissen und technisch organisatorischen Maßnahmen sind auch die Verfahrensweisung „Datenschutz und Datensicherheit“ (QMH B1 VA 4.2.4-2), als verbindliche Handlungsleitlinie, einschließlich aller damit verbundenen Formulare, aktualisiert worden.

Die geänderten Prozesse werden im Rahmen der jährlichen Audits weiterhin auf ihre Wirksamkeit geprüft und fortgeschrieben. Die Umsetzung der eingeleiteten Maßnahmen hat im Beispielunternehmen zur Herstellung der Konformität mit DS-GVO und BDSG geführt. Der Gartenhaus e.V. ist damit rechtssicher aufgestellt und kann im Umgang mit den personenbezogenen Daten der Klienten ein hohes Schutz- und Sicherheitsniveau vorweisen. Darüber hinaus konnten weitere potentielle Verbesserungsmaßnahmen identifiziert werden, die nach einer Angemessenheitsprüfung, als Empfehlung zur Einführung dem geschäftsführenden Vorstand vorgelegt werden.

Regelmäßige Schulungen der Belegschaft

Das Ziel dieser internen Veranstaltungen soll eine Sensibilisierung und die weitere Erhöhung der Fachlichkeit in den relevanten IT-Anwendungen zur Minimierung des Risikos der ungewollten Datenveränderung im Datenbestand sein.

Die personellen und sächlichen Kapazitäten vorausgesetzt, hat der Gartenhaus e.V. mit seinen IT-Dienstleistern kompetente Ansprechpartner vertraglich gebunden, die eine Umsetzung inhaltlich begleiten können.

Vereinheitlichung von Dateistrukturen

Die bisher autonome Verfahrensweise bei der Ablage von Dateien in den Systemen der Einrichtungen hat eine breite Vielfalt an Strukturen entstehen lassen. Zur zielgerichteten Bearbeitung der Daten im Rahmen von Betreuungsarbeit, aber auch zur Wahrung der Betroffenenrechte (Kap. 6.9) ist eine Vereinheitlichung zwingend angezeigt. Dazu hat der Verantwortliche eine verbindliche Struktur festzulegen, welche die Gecko mbH zeitnah im Zusammenhang von Wartungsarbeiten in den Einrichtungen installiert.

Entwicklung eines Datenlösch- und Vernichtungskonzeptes

Die Datenorganisation ist im Beispielunternehmen so zu gestalten, dass neben einer Verfügbarkeit, dem Schutz vor Datenverlust auch die kontrollierte Datenlöschung mit Datenträgerentsorgung in beherrschten Prozessen ablaufen kann.

Für bereits bestehende Handakten über Klienten sind im Zentralarchiv und ggf. in den Einrichtungen Verzeichnissen anzulegen. Die digitalen Akten der Klienten sind nach dem Ende der Betreuung zu sperren und nach Ablauf von 10 Jahren aus den Dokumentationssystem procare und den Arbeitsplatzrechnern händisch zu löschen.

Jährliche Überwachung der technisch organisatorischen Maßnahmen

Damit der aktuelle Stand der IT-Technik und die Angemessenheit des Schutzniveaus in der Datenverarbeitung ständig Berücksichtigung findet (Art. 32 Abs. 1 DS-GVO), sollen die technisch organisatorischen Maßnahmen jährlich einer Überprüfung/Audit unterzogen werden.

Die notwendigen Untersuchungen hierzu finden in zwei Bereichen statt. So werden die Anforderungen aus der Verarbeitung mit den technischen Leistungsmerkmalen der vorhandenen Informationstechnik verglichen, um die Erfüllung der Anforderungen des § 64 BSDG zu prüfen und um Verbesserungspotentiale aufzuzeigen. Weiterhin sollen die tatsächlichen Abläufe in den relevanten Betreuungsprozessen hinsichtlich ihrer Konformität zur aktuellen Rechtsprechung und zu den Festlegungen aus dem QMH bewertet werden

Weiterentwicklung von Verhaltensregeln (Art. 40 DS-GVO)

In der Verfahrensanweisung QMH VA 1 4.2.4-2 sind Verhaltensregeln als verbindliche Handlungsleitlinien dokumentiert. Der weitere Ausbau dieser Verhaltensregeln wird durch die DS-GVO mit Art. 40 in den Anwendungen lits. a bis k ausdrücklich unterstützt. Ziel der Entwicklung von Verhaltensregeln ist neben der Sensibilisierung der Belegschaft vor allem auch die Verankerung rechtskonformen Verhaltens im Umgang mit sensiblen Daten.

So muss im Bereich der Kommunikation von Mitarbeitern eine klare Trennung von privater und dienstlicher Telefonie vorgenommen werden. Zu beachten ist dabei, wie Wächter auf S. 24, Abschnitt 45 in „Datenschutz im Unternehmen“ ausführt, dass die Datenverarbeitung durch Privatpersonen nicht in den Anwendungsbereich der DS-GVO fällt. „Dies bedeutet, dass Tätigkeiten von Mitarbeitern, die ihren privaten Account für geschäftliche Tätigkeiten nutzen, unter das Regime des Datenschutzrechts fallen.“

Insofern ist eine gemischte Nutzung von Mobiltelefonen nicht nur in der Betreuungsarbeit datenschutzrechtlich kritisch zu betrachten und grundsätzlich zu vermeiden. Die Nutzung sozialer Medien auf dienstlich und gemischt genutzten Kommunikationsgeräten ist aus Gründen der teilweise unklaren Weitergabe bzw. bei Weitergabe an einen Datenverarbeiter außerhalb der EU rechtlich bedenklich und damit im Sinne beherrschter Betreuungsprozesse nicht tolerierbar.

Klare und verbindliche Verhaltensregeln können bspw. sogenannte Clean Desk Regeln sein. Diese Regeln beinhalten Festlegungen zur Ordnung und Einsehbarkeit von Unterlagen in den Einrichtungen. Dabei haben die jeweils zu bearbeitenden Dokumente, so auch der Desktop der Arbeitsplatzrechner, so geschlossen oder verdeckt zu sein, dass der Unberechtigte nicht per Zufall Einblick nehmen kann.

Die Reinigung von Diensträumen hat bei Vergabe an eine Fremdfirma so zu erfolgen, dass die Arbeiten nur bei Anwesenheit von Betreuungspersonal erfolgt oder aber alle persönlichen und dienstlichen Unterlagen in verschlossenen Schränke verwahrt sind. Die Notwendigkeit einer Verpflichtungserklärung auf den Datenschutz muss im Einzelfall geprüft werden.

Ein weiteres Risiko der ungewollten Datenübertragung ist die Verfahrensweise bei gemischt genutzten Räumen, den Multifunktionsräumen, im Unternehmen. Dabei haben die Mitarbeiter nach Meetings oder Fortbildungen den Raum so zu hinterlassen, dass die nachfolgende Reinigung oder auch die Teilnehmer der nächsten Veranstaltung nicht mit sensiblen Daten an Tafeln, Flip-Charts, Pin-Wänden oder im Papierkorb konfrontiert werden.

Fotoaufnahmen von Personen, die aus Anlass von Ausflügen oder Veranstaltungen im Rahmen der sozialen Arbeit, erstellt und auf Flyern, im Internet, in Printmedien oder ähnlichem veröffentlicht werden sollen, sind grundsätzlich ohne Genehmigung des Abgebildeten gem. §§ 22, 23 KunstUrhG nicht erlaubt. Nach § 1 Abs. 2 S. 1 BDSG gehen andere Rechtsvorschriften des Bundes über den Datenschutz den allgemeine Rechtsvorschriften vor. Damit ist es unerheblich, ob es einen weiteren Rechtfertigungstatbestand außer der Einwilligung nach 6 Abs. 1 lit. a DS-GVO gibt. Für eine rechtssichere Anwendung der Fotoerlaubnis innerhalb des Beispielunternehmens wurde das Formular B2 FM 4.2.4-1 im Handbuch aufgenommen. Die individuellen Verhaltensregeln hierzu sind in den Hausordnungen der Einrichtungen festgeschrieben.

Haben Verhaltensregeln weitreichende Auswirkungen auf Betriebsabläufe, werden Persönlichkeitsrechte der Beschäftigten berührt bzw. müssen Prozesse aus Gründen solcher Regeln neu strukturiert werden, empfehlen sich zur Erhöhung der Akzeptanz Verhandlungen mit dem Betriebsrat mit dem Ziel von Betriebsvereinbarungen.

Betriebsvereinbarungen (BV)

In Kapitel 6.4.2 wurde bereits auf die Problematik der freien Nutzung des Internets am Arbeitsplatz hingewiesen. Eine Festlegung in einer Betriebsvereinbarung, welche die private Nutzung des Internets und den privaten email-Verkehr am Arbeitsplatz generell verbietet, würde gem. § 11 Abs. 1 S.1 Nr. 1 TMG beim Arbeitgeber zu einer Befreiung von den Datenschutzvorschriften des TMG führen.

Eine solche Regelung schafft Rechtsklarheit in den Beschäftigungsverhältnissen, beschränkt die Mitarbeiter aber in der freien Entfaltung ihrer Persönlichkeit.

Betriebsvereinbarungen im Beispielunternehmen sollten nach Auffassung des Datenschutzbeauftragten auch zur privaten Nutzung von dienstlichen Kommunikationsgeräten und zur Nutzung sozialer Medien am Arbeitsplatz geschlossen werden. Ziele, neben einer verbindlichen Handlungsanweisung in den Prozessen, sind auch zusätzliche Haftungsausschlüsse für die Verantwortlichen, die Gleichbehandlung aller Beschäftigten sowie Festlegungen zur ressourcenorientierten Nutzung der Arbeitszeit.

Entwicklung eines Datenschutzmanagement

Eine zusätzliche Verbesserung ist die geplante Einführung eines Datenschutzaudits als Systemaudit. Damit könnten weitere Schwachstellen in System identifiziert und ggfls. geeignete Maßnahmen zu deren Abhilfe getroffen werden. Weiterführend können bereits installierte Maßnahmen im Unternehmen zur Sicherstellung eines funktionierenden Datenschutzes weiter ausgebaut und optimiert werden. Langfristiges Ziel sollte dabei ein datenschutzspezifischen Zertifizierungsverfahrens sowie auch Datenschutzsiegel und –prüfzeichen sein. (Art. 42 DS-GVO) Ein bereits etabliertes Verfahren in Deutschland ist die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (Konzept BSI). Dabei wird ein Informationssicherheits-Managementsystem (ISMS) aufgebaut, welches vom Zertifizierer regelmäßig auditiert wird.

8 Zusammenfassung

Der „Gartenhaus“ Psychosozialer Trägerverein Stralsund e.V. ist durch seine Zertifizierung nach DIN EN ISO 9001:2015 in der Lage, den Anforderungen an eine qualitativ hochwertige Betreuung in der Versorgungsregion Vorpommern-Rügen auch in der Zukunft zu gewährleisten.

Das risikobasierte Denken der Norm ist in vielen Schlüsselprozessen bereits fest im Unternehmen verankert. Zahlreiche Handlungsanweisungen (Verfahrensweisungen) im Qualitätshandbuch spiegeln die Einstellung der Geschäftsführung und der Beschäftigten im Umgang mit den latenten Risiken wider.

Die bisherigen Festlegungen zum Datenschutz und zur Verbesserung der Datensicherheit haben im Unternehmen ein hohes Schutzniveau geschaffen. Die Aufbauorganisation im Verein entsprach in weiten Teilen schon den Vorgaben der DSGVO, bereits vor dem 25.05.2018 und musste dem zur Folge nicht verändert werden.

Die Ablauforganisation zur Herstellung der Konformität mit der DS-GVO wurde an einigen markanten Punkten in der Prozesslandschaft den geänderten Anforderungsprofilen angepaßt. So sind es ab 01.01.2018 die Leistungsträger, die in den Versorgungsregionen Mecklenburg-Vorpommerns die Datenhoheit für die Ersterhebung und das Fortschreiben im Integrierten Teilhabeplan für sich beanspruchen, somit auch im Vorfeld der Teilhabeplanung den betroffenen Klienten über die Verarbeitung der Daten aufklären müssen.

Damit wurden die Leistungserbringer in großen Teilen zu „Dritten“ im Empfang von sensiblen Klientendaten. Der Integrierte Teilhabeplan ist dabei das zentrale Steuerungselement im Hilfesystem, um den personenzentrierten Hilfen in der Zielerreichung für den Klienten eine optimale Grundlagen zu schaffen. Die Qualität der sozialpsychiatrischen Hilfen wird in großen Teilen durch die Qualität des ITP bestimmt. Dem ITP fällt damit eine zentrale Bedeutung nicht nur in der Hilfeplanung, sondern auch in der Verarbeitung personenbezogener Daten, zu.

Zur Darstellung eines angemessenen Sicherheitsniveaus wurden die Schlüsselprozesse mit den entsprechenden Sicherungsmaßnahmen beschrieben, Datenschutz-Folgeabschätzungen durchgeführt und Handlungsleitlinien modifiziert.

Den Beschäftigten wurden überarbeitete Formulare und Dokumente übergeben und eine Meldekette zur Aufsichtsbehörde bei möglichen Datenpannen installiert.

Zusammenfassend betrachtet, konnte der IST-Stand des Datenschutzes im Unternehmen den SOLL-Anforderungen aus der DS-GVO und BDSG (in ihrer Rechtsverbindlichkeit zum 25.05.2018) angeglichen werden. Durch den ständigen technologischen Fortschritt und der sich daran anpassenden Rechtsprechung wird es auch in Zukunft notwendig sein, die Schutzmaßnahmen für die uns anvertrauen Daten einem regelmäßigen Audit zu unterziehen, erforderliche Korrekturmaßnahmen einzuleiten.

Die Unternehmensleitlinien des „Gartenhaus“ e.V. sind definiert durch konkrete und verbindliche Festlegungen, die den Beschäftigten eine Grundlage für hochwertige Betreuungsarbeit bieten. Ziel dabei ist, dem Klienten, entsprechend seiner Beeinträchtigungen, ein hohes Maß an Selbstbestimmtheit über sein Leben zu ermöglichen. Dies bedeutet, neben den sozialpsychiatrischen Hilfen auch den Schutz der anvertrauten Daten im Rahmen der Teilhabeplanung.

Dabei schließen sich Datenschutz und erfolgreiche soziale Arbeit nicht aus!

Anhang

1. Datenschutzrechtliche Beurteilung von Verarbeitungstätigkeiten (DSFA)
 - 1.1 Entsorgung Datenmaterial
 - 1.2 Klientendokumentation
 - 1.3 Lohn- und Gehaltsabrechnungen
 - 1.4 Torvideoanlage Therapiezentrum

2. Verarbeitungsverzeichnisse
 - 2.1 Abrechnung Lohn und Gehalt
 - 2.2 Arbeitssicherheit
 - 2.3 Bewerbungsverfahren
 - 2.4 Fortbildungen
 - 2.5 Freistellung: Kind krank
 - 2.6 Führerscheinkontrolle
 - 2.7 Klientenverwaltung
 - 2.8 Lieferantenbeurteilung
 - 2.9 Mitarbeiter im Ehrenamt
 - 2.10 Personalakte
 - 2.11 Personalgespräch
 - 2.12 Torvideoanlage Therapiezentrum
 - 2.13 Vermietung
 - 2.14 Versicherungen

3. technisch organisatorische Maßnahmen-TOM (Betreuung und Verwaltung)

4. Qualitätshandbuch
 - 4.0 Teil A Organigramm Stand 05/2018
 - 4.1 Teil B1 VA 4.2.4-2 Datenschutz und Datensicherheit
 - 4.2 Teil B2 FM 4.2.4-1 Einwilligungserklärung Foto
 - 4.3 Teil B2 FM 4.2.4-2 Informationspflicht Angestellte
 - 4.4 Teil B2 FM 4.2.4-3 Informationspflicht Klienten
 - 4.5 Teil B2 FM 6.2-11 Personalgespräch
 - 4.6 Teil B2 FM 6.2-13 Personalfragebogen Lohn
 - 4.7 Teil B2 FM 7.2-3 Interessentengespräch
 - 4.8 Verpflichtungserklärung Datenschutz DS-GVO

5. Rechtliche Aufklärung zum Datenschutz ITP / Bogen D



Datenschutzrechtliche Beurteilung von Verarbeitungstätigkeiten Vorabkontrolle/Risikoanalyse nach BDSG/DS-GVO

1. Beschreibung der Verarbeitungstätigkeit (§ 4g Abs. 2 i.V.m. § 4e BDSG / § 30 DSGVO)

Entsorgung von Datenträgern (Papier und IT)

- Personenbezogene Klientendaten
- Personenbezogene Mitarbeiterdaten
- Betriebsdaten

2. Informationen zu den verarbeitenden Daten

2.1 personenbezogene Daten ja / ~~nein~~

2.2 Rechtsgrundlagen

Personenbezogene Daten von Klienten, Mitarbeitern

2.3 Datenkategorien nach § 22 Abs. 1 BDSG / Art. 9 Abs. 1 DSGVO

Ja

2.4 Prüfung auf Datenminderung gem. § 71 BDSG / Art. 5 Abs. 1 c DSGVO

Prozess dient der Datenminimierung im Unternehmen

2.5 Prüfung auf Anonymisierung

Daten sind personenbezogen erhoben und verarbeitet worden, eine Anonymisierung vor der Vernichtung wäre unverhältnismäßig

2.6 Datenherkunft / Wie werden die Daten erhoben ?

- Daten kommen aus allen Einrichtungen und Betriebsteilen des Unternehmens
- Daten werden direkt beim Betroffenen erhoben (ggfls. Datenherkunft ITP)

2.7 Information / Benachrichtigung

2.7.1 gesonderte Information des Betroffenen

Ja, bei Neuaufnahme erfolgt Information über Datenverwendung

2.7.2 Benachrichtigung über Verarbeitung

Nein, da Löschkonzept

2.8 Altdatenübernahme

Trifft nicht zu

2.9 Datenübermittlung an andere IT-Anwendungen / Stellen

Werkstatt für behinderte Menschen (WfbM) für Datenträger (Papierformat) zur Vernichtung
Firma Gecko zur Entsorgung Festplatten/ digitale Datenträger zur Vernichtung

3. Gewährleistung Auskunftsansprüche Art. 12+15 DSGVO, § 29 Abs. 1, § 34 BDSG

-schriftlicher Antrag an bDSB

4. Sperrung und Löschung gem. Art. 17 DSGVO

Löschung nach Ablauf Aufbewahrungsfrist

5. Berechtigungskonzept

- verschlossene Datentonne übergeben an Aktenentsorger vor Ort
- persönliche Übergabe Altrechner an Mitarbeiter der Firma Gecko

6. IT-Konzept

- trifft nicht zu

7. Feststellung Schutzbedarf der verarbeitenden Daten (BSI-Standard 100-1, Kap. 9.2.1)

Hoher Schutzbedarf

8. tolerierbare Ausfallzeit des Verarbeitungssystems

Variabel, je nach Anfall zu entsorgender Daten

9. Bedrohungsanalyse / Risikobewertung

9.1 Tabelle der Risikobewertung

Bedrohtes Objekt	Bedrohung	Bedrohtes Schutzziel	Klassifizierung	TOM
Papiertonne	Diebstahl	Vertraulichkeit	hoch	Doppelter Verschuß
	Unberechtigter Zugriff	Vertraulichkeit	hoch	Doppelter Verschuß
Festplatten	Diebstahl	Vertraulichkeit	Hoch	Verschuß
	Unberechtigter Zugriff	Vertraulichkeit	Hoch	Persönliche Übergabe

9.2 Erhöhte Eintrittswahrscheinlichkeit bei einzelnen Objekten

Geschäftsstelle, da dort zentrale Lagerung des Vernichtungsgutes

10. Datenschutz-/Datensicherheitsrelevante Aspekte vertraglich zu regeln

- Fernwartungsvertrag/ Supportservice mit Firma Gecko
Kontaktdaten : Gecko Gesell. Für ComputerKommunikation
NL Stralsund / Herr Hinkeldey
Philipp-Julius-Weg 1, 18437 Stralsund
Tel. 03831 / 3051-10
- Werkstatt für behinderte Menschen
Kontaktdaten : Stralsunder Werkstätten WfbM
Albert-Schweitz-Str.1, 18437 Stralsund
Tel. 03831 / 4701-0

11. Programmfunktionalitäten

11.1 Änderungsverfahren

Keine Angaben

11.2 Verantwortlichkeit

- Einrichtungsleitung aller entsorgenden Organisationseinheiten
- Schnittstelle Verwaltungsleiter : Übergabe WfbM und Gecko

12. Betreuer der Anwendung

Administrator und externer Support = Firma Gecko (Kontakt s.o.)
Papiertonne = betrieblicher Datenschutzbeauftragter

13. Abnahme und Freigabe der IT-Anwendung

Firma Gecko (Kontakt s.o.)
WfbM (Kontakt s.o.)

14. Schulung, Einweisung, Betreuung der Anwender

Firma Gecko (Kontakt s.o.)

15. Zusammenfassende Bewertung gem. Art. 35 DSGVO

~~Es besteht kein hohes Risiko bei der Verarbeitung für die Rechte und Freiheiten natürlicher Personen~~

Die mit der Verarbeitung verbundenen Gefahren (hohes Risiko) werden durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam beherrscht.

~~Die mit dem Verfahren verbundenen Gefahren werden durch die Beschriebenen technischen und organisatorischen Maßnahmen **nicht** wirksam beherrscht.
(Konsultation der Aufsichtsbehörde gem. Art. 36 DSGVO)~~

16. Prüfrhythmus der Risikoanalyse

- jährlich, beginnend in 05/2018

Gartenhaus e.V.
Verantwortlicher Art. 35 DSGVO

Nehls, Thomas
bDSB

Datenschutzrechtliche Beurteilung von Verarbeitungstätigkeiten

Vorabkontrolle/Risikoanalyse nach BDSG/DS-GVO



1. Beschreibung der Verarbeitungstätigkeit (§ 4g Abs. 2 i.V.m. § 4e BDSG / § 30 DSGVO)

Erfassung der Stammdaten und Dokumentation der Therapieverläufe von Klienten aus Teilhabeplanung (ITP) papierhaft und in Programm procure (Firma Moveo)

2. Informationen zu den verarbeitenden Daten

2.1 personenbezogene Daten ja/~~nein~~

2.2 Rechtsgrundlagen

Personenbezogene Daten von Klienten gem. Art. 6 (1)a, b, e DS-GVO

2.3 Datenkategorien nach § 22 Abs. 1 BDSG / Art. 9 Abs. 1 DSGVO

Muss-Stammdaten wie : Name, Vorname, Geb.Dat., Adresse, Diagnose, Medikation

Kann-Stammdaten wie : Angehörige, Beruf,

Verlaufsdaten : Anwesenheiten, Therapieverläufe, Zielerreichung Hilfeplan

2.4 Prüfung auf Datenminderung gem. § 71 BDSG / Art. 5 Abs. 1 c DSGVO

- in Abhängigkeit von den Krankheitsbildern und Verläufen schwierig, jedoch im Einzelfall möglich

2.5 Prüfung auf Anonymisierung

-Anonymisierung nicht möglich, da direkte Zuordnung für Dokumentation notwendig

-Überwachungsbehörde (Heimaufsicht) prüft Einsatz, Eignung, Effektivität der Hilfen

2.6 Datenherkunft / Wie werden die Daten erhoben?

-Daten werden direkt beim Klienten erhoben (Leistungsträger via ITP)

-verschriftlicht auf Formularen des QMH, zur Hilfenahme ITP vom Kostenträger

-via IT in procure Stammdaten/Verlaufsdaten

2.7 Information / Benachrichtigung

2.7.1 gesonderte Information des Betroffenen

Ja, bei Neuaufnahme oder Erstkontakt mit FM 4.2.4-3

2.7.2 Benachrichtigung über Verarbeitung

Ja, laufend mit Fortschreibung Teilhabeplanung (ITP) und Bewilligungsbescheiden

2.8 Altdatenübernahme

Nein, nicht notwendig

2.9 Datenübermittlung an andere IT-Anwendungen / Stellen

Nur auf Anforderung Leistungsträger (nicht digital)

3. Gewährleistung Auskunftsansprüche Art. 12+15 DSGVO, § 29 Abs. 1, § 34 BDSG

- schriftlicher Antrag an Einrichtungsleitung zwecks Einsichtnahme
- Einsichtnahme in der Einrichtung

4. Sperrung und Löschung gem. Art. 17 DSGVO

- Sperrung der Verlaufsdaten mit Rechnungserstellung
- Sperrung Stammdaten mit Verlassen Betreuungsangebot
- Stammdaten/Verlaufsdaten werden 10 Jahre papierhaft archiviert
- IT-Stamm-/Verlaufsdaten werden manuell nach 10 Jahren gelöscht – Löschkonzept

5. Berechtigungskonzept

- jeder Mitarbeiter der Betreuung kann für die Klienten seiner Einrichtung Stammdaten anlegen, Einsicht nehmen, Änderungen vornehmen jedoch nicht löschen
- die MitarbeiterIn der Rechnungserstellung verarbeitet auf Anweisung die Daten und verschickt postalisch die Rechnungen an die Leistungsträger
- Notfallkonzept = Ansprechpartner Moveo Software GmbH
- Verpflichtung zum Datengeheimnis in allen Arbeitsverträgen

6. IT-Konzept

- Eingabe/Ausgabe der personenbezogenen Daten über Arbeitsplatz der Einrichtungen
- Passwortgeschützt je Mitarbeiter
- Doppelanmeldung je Mitarbeiter wg. Terminalserver und procure nötig
- Verarbeitung der Daten auf Server „ Moveo“
- Netzeinbindung AP-Rechner und Server wg. updates
- Mandantensicherung siehe TOM

7. Feststellung Schutzbedarf der verarbeitenden Daten (BSI-Standard 100-1, Kap. 9.2.1)

Hoher Schutzbedarf

8. tolerierbare Ausfallzeit des Verarbeitungssystems

In Anhängigkeit individueller Bewilligungszeiträume bis zu einer Woche

9. Bedrohungsanalyse / Risikobewertung

9.1 Tabelle der Risikobewertung

Bedrohtes Objekt	Bedrohung	Bedrohtes Schutzziel	Klassifizierung	TOM
Laptop/ PC mit Daten	Diebstahl	Vertraulichkeit Verfügbarkeit	hoch	Verschuß
	Unberechtigter Zugriff	Vertraulichkeit Integrität	normal	Passwort Verschuß
	Sicherungskopie	Verfügbarkeit	normal	regelmäßig
	IT-Zugriff extern	Vertraulichkeit Integrität	normal	Firewall
Handakte	Diebstahl	Vertraulichkeit	hoch	Doppelverschuß
	Unberechtigter Zugriff	Vertraulichkeit	Hoch	Doppelverschuß

9.2 Erhöhte Eintrittswahrscheinlichkeit bei einzelnen Objekten

Serverstandort „procare“ in der Langenstrasse 51, 18439 Stralsund

10. Datenschutz-/Datensicherheitsrelevante Aspekte vertraglich zu regeln

- Fernwartungsvertrag/ Supportservice mit Firma Moveo
- Kontaktdaten : Moveo Software GmbH
Berliner Str. 74, 14467 Potsdam
Tel. 0331 / 90973-0

11. Programmfunktionalitäten

11.1 Änderungsverfahren

Releasewechsel und updates über Firma Moveo

11.2 Verantwortlichkeit

- alle EinrichtungsleiterInnen betreuender Organisationseinheiten sowie Abt. Rechnungslegung

12. Betreuer der Anwendung

Administrator und externer Support = Firma Moveo (Kontakt s.o.)

13. Abnahme und Freigabe der IT-Anwendung

Firma Moveo (Kontakt s.o.)

14. Schulung, Einweisung, Betreuung der Anwender

Firma Moveo (Kontakt s.o.)

15. Zusammenfassende Bewertung gem. Art. 35 DSGVO

~~Es besteht kein hohes Risiko bei der Verarbeitung für die Rechte und Freiheiten natürlicher Personen~~

Die mit der Verarbeitung verbundenen Gefahren (hohes Risiko) werden durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam beherrscht.

~~Die mit dem Verfahren verbundenen Gefahren werden durch die Beschriebenen technischen und Organisatorischen Maßnahmen nicht wirksam beherrscht.
(Konsultation der Aufsichtsbehörde gem. Art. 36 DSGVO)~~

16. Prüfrhythmus der Risikoanalyse

- jährlich, beginnend mit 05/2018

Gartenhaus e.V.
Verantwortlicher Art. 35 DSGVO

Thomas Nehls
bDSB

Datenschutzrechtliche Beurteilung von Verarbeitungstätigkeiten

Vorabkontrolle/Risikoanalyse nach BDSG/DS-GVO



1. Beschreibung der Verarbeitungstätigkeit (§ 4g Abs. 2 i.V.m. § 4e BDSG / § 30 DSGVO)

Verarbeitung von Beschäftigtendaten für Lohn- und Gehaltsabrechnungen
(incl. Arbeitsunfähigkeit, Urlaub, Reisekosten)

2. Informationen zu den verarbeitenden Daten

2.1 personenbezogene Daten ja/~~nein~~

2.2 Rechtsgrundlagen

personenbezogene Daten / § 26 Abs. 1 BDSG i.V.m. Art. 9 Abs. 2 b DS-GVO

2.3 Datenkategorien nach § 26 Abs. 1 BDSG / Art. 9 DSGVO

Stammdaten wie : Name, Vorname, Alter, Adresse, Kinder, Religionszugehörigkeit, Bankdaten,
SV-/Steuerrechtl. Ident.Nr., Mutterschutz, Krank

Verlaufsdaten wie : An- und Abwesenheit am Dienstplatz, Dienstreisen, Urlaub

2.4 Prüfung auf Datenminderung gem. § 71 BDSG / Art. 5 Abs. 1 c DSGVO

Keine Minimierung möglich, da grundsätzlich nur für die Verarbeitung relevante Daten erfasst

2.5 Prüfung auf Anonymisierung

-Anonymisierung nicht möglich, da direkte Zuordnung für Verarbeitung (Lohn) nötig
-Überwachungsbehörden (z.B.Heimaufsicht, Deutsche Rente, Finanzamt, etc.) prüfen fachliche
Eignung, Einsatz im Dienst, An- und Abwesenheiten

2.6 Datenherkunft / Wie werden die Daten erhoben?

-Daten werden direkt beim Arbeitnehmer erhoben
-schriftlich auf Formularen des QMH
-via IT in procure die Kontaktzeiten Mitarbeiter / Klient

2.7 Information / Benachrichtigung

2.7.1 gesonderte Information des Betroffenen

Ja, bei Einstellung über Personalfragebogen FM 6.2-13
Jedoch nicht notwendig, da gesetzliche Erlaubnisnorm gem. § 22 (1) 1a BDSG

2.7.2 Benachrichtigung über Verarbeitung

JA, mit Lohnscheinen, Jahresmeldung SV, Lohnsteuermeldung
Jedoch nicht notwendig, da gesetzliche Erlaubnisnorm gem. § 22 (1) 1a BDSG

2.8 Altdatenübernahme

Nein, nicht notwendig

2.9 Datenübermittlung an andere IT-Anwendungen / Stellen

Elster, SV-net, Dakota

3. Gewährleistung Auskunftsansprüche Art. 12+15 DSGVO, § 29 Abs. 1, § 34 BDSG

- schriftlicher Antrag an Geschäftsleitung zwecks Einsichtnahme
- Einsichtnahme in der Geschäftsstelle

4. Sperrung und Löschung gem. Art. 17 DSGVO

- Sperrung der Verlaufsdaten mit Jahresabschluss
- Stammdaten/Verlaufsdaten werden 10 Jahre papierhaft archiviert
- IT-Verlaufsdaten werden alle 3 Jahre (Beachtung Betriebsprüfungen) i.R. update gelöscht

5. Berechtigungskonzept

- Einrichtungsleiter arbeiten der Lohnbuchhaltung zu, in dem dienstliche Vorgänge „sachlich richtig“ gezeichnet werden
- nur die MitarbeiterIn der Lohnbuchhaltung empfängt die Daten
- nur die MitarbeiterIn der Lohnbuchhaltung verarbeitet auf Anweisung GF die Daten
- Notfallkonzept = Ansprechpartner Fa. Helmerich (Kontaktdaten)
- Verpflichtung zum Datengeheimnis in Arbeitsverträgen

6. IT-Konzept

- Bearbeitung der personenbezogenen Daten auf einem separaten Computer/Laptop
- Passwortgeschützt
- nicht im W-LAN eingebunden
- Netzeinbindung wg. Meldungen siehe Pkt. 2.9
- Mandantensicherung via Stic

7. Feststellung Schutzbedarf der verarbeitenden Daten (BSI-Standard 100-1, Kap. 9.2.1)

normal

8. tolerierbare Ausfallzeit des Verarbeitungssystems

Anhängig von Meldedaten SV bis zu einer Woche

9. Bedrohungsanalyse / Risikobewertung

9.1 Tabelle der Risikobewertung

Bedrohtes Objekt	Bedrohung	Bedrohtes Schutzziel	Klassifizierung	TOM
Laptop mit Daten	Diebstahl	Vertraulichkeit Verfügbarkeit	normal	Passwort Verschluss
	Unberechtigter Zugriff	Vertraulichkeit Integrität	normal	Passwort
	Sicherungskopie	Verfügbarkeit	normal	regelmäßig
	IT-Zugriff extern	Vertraulichkeit Integrität	normal	Firewall
Handakte	Diebstahl	Vertraulichkeit	normal	Doppelverschluss
	Unberechtigter Zugriff	Vertraulichkeit	normal	Doppelverschluss

9.2 Erhöhte Eintrittswahrscheinlichkeit bei einzelnen Objekten

Personalbuchhaltung Langenstrasse 51, 18439 Stralsund

10. Datenschutz-/Datensicherheitsrelevante Aspekte vertraglich zu regeln

- Fernwartungsvertrag/ Supportservice mit Firma Helmerich
- Kontaktdaten : Helmerich-PCAS Software & Service GmbH
Krögerweg 21, 48155 Münster
Tel. 0900/123321-1

11. Programmfunktionalitäten

11.1 Änderungsverfahren

Releasewechsel und updates über Firma Helmerich

11.2 Verantwortlichkeit

- Auf Anweisung des GF die MitarbeiterIn der Lohnbuchhaltung

12. Betreuer der Anwendung

Administrator und externer Support = Firma Helmerich (Kontakt s.o.)

13. Abnahme und Freigabe der IT-Anwendung

Firma Helmerich (Kontakt s.o.)

14. Schulung, Einweisung, Betreuung der Anwender

Firma Helmerich (Kontakt s.o.)

15. Zusammenfassende Bewertung gem. Art. 35 DSGVO

~~Es besteht kein hohes Risiko bei der Verarbeitung für die Rechte und Freiheiten natürlicher Personen~~

Die mit der Verarbeitung verbundenen Gefahren (hohes Risiko) werden durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam beherrscht.

~~Die mit dem Verfahren verbundenen Gefahren werden durch die Beschriebenen technischen und Organisatorischen Maßnahmen **nicht** wirksam beherrscht.
(Konsultation der Aufsichtsbehörde gem. Art. 36 DSGVO)~~

16. Prüfrhythmus der Risikoanalyse

- jährlich, beginnend 05/2018

Gartenhaus e.V.
Verantwortlicher Art. 35 DSGVO

Thomas Nehls
bDSB

Datenschutzrechtliche Beurteilung von Verarbeitungstätigkeiten

Vorabkontrolle/Risikoanalyse nach BDSG/DS-GVO



1. Beschreibung der Verarbeitungstätigkeit (§ 4g Abs. 2 i.V.m. § 4e BDSG / § 30 DSGVO)

Videoüberwachung (keine Aufzeichnung) Toranlage/Eingangsbereich
Therapiezentrum „Psychose & Sucht“ , Tribseer Strasse 12, 18439 Stralsund

2. Informationen zu den verarbeitenden Daten

2.1 personenbezogene Daten ja/nein

2.2 Rechtsgrundlagen

Personenbezogene Daten von Klienten, Mitarbeitern und Besuchern gem. Art. 6 (1) d, e

2.3 Datenkategorien nach § 22 BDSG / Art. 9 DSGVO

Trifft nicht zu

2.4 Prüfung auf Datenminderung gem. § 71 BDSG / Art. 5 Abs. 1 c DSGVO

Daten werden nicht aufgezeichnet

2.5 Prüfung auf Anonymisierung

Trifft nicht zu, da hier Erkennbarkeit Voraussetzung für Einlass Tor

2.6 Datenherkunft / Wie werden die Daten erhoben?

-Daten werden nur über eine Kamera in der Schließanlage erhoben

2.7 Information / Benachrichtigung

2.7.1 gesonderte Information des Betroffenen

Ja, bei Neuaufnahme oder Erstkontakt

Ja, durch Beschilderung an der Toranlage

2.7.2 Benachrichtigung über Verarbeitung

Information über Beschilderung an der Toranlage

2.8 Altdatenübernahme

Trifft nicht zu

2.9 Datenübermittlung an andere IT-Anwendungen / Stellen

nein

3. Gewährleistung Auskunftsansprüche Art. 12+15 DSGVO, § 29 Abs. 1, § 34 BDSG nF

-schriftlicher Anfrage an bDSB

4. Sperrung und Löschung gem. Art. 17 DSGVO

Trifft nicht zu , da keine Aufzeichnung

5. Berechtigungskonzept

- jeder Mitarbeiter der Einrichtung kann zu Kontrollzwecken die Toranlage im Videozuschnitt nur Live sehen (Vorgang ist mit Türöffnung abgeschlossen)
- Verpflichtung zum Datengeheimnis in allen Arbeitsverträgen

6. IT-Konzept

- nein

7. Feststellung Schutzbedarf der verarbeitenden Daten (BSI-Standard 100-1, Kap. 9.2.1)

normaler Schutzbedarf

8. tolerierbare Ausfallzeit des Verarbeitungssystems

Bis zu einer Woche wg. Sicherheit Klienten/Mitarbeiter, Gefährdung Therapieverlauf

9. Bedrohungsanalyse / Risikobewertung

9.1 Tabelle der Risikobewertung

Bedrohtes Objekt	Bedrohung	Bedrohtes Schutzziel	Klassifizierung	TOM
Laptop/ PC	Diebstahl	Vertraulichkeit Verfügbarkeit	hoch	Passwort Verschluss
Kamera	Diebstahl / Beschädigung	Verlust	gering	keines
	Unberechtigte Einsicht	Vertraulichkeit Integrität	normal	Verschluss
	IT-Zugriff extern	Vertraulichkeit Integrität	normal	Firewall

9.2 Erhöhte Eintrittswahrscheinlichkeit bei einzelnen Objekten

Nur am Standort selber vorhanden

10. Datenschutz-/Datensicherheitsrelevante Aspekte vertraglich zu regeln

- Fernwartungsvertrag/ Supportservice mit Firma Gecko
- Kontaktdaten : Gecko Gesell. Für ComputerKommunikation
NL Stralsund / Herr Hinkeldey
Philipp-Julius-Weg 1, 18437 Stralsund
Tel. 03831 / 3051-10

11. Programmfunktionalitäten

11.1 Änderungsverfahren

Releasewechsel und updates über Firma Gecko

11.2 Verantwortlichkeit

- Einrichtungsleitung der betreffenden Organisationseinheit auf Weisung der Geschäftsführung

12. Betreuer der Anwendung

Administrator und externer Support = Firma Gecko (Kontakt s.o.)

13. Abnahme und Freigabe der IT-Anwendung

Firma Gecko (Kontakt s.o.)

14. Schulung, Einweisung, Betreuung der Anwender

Firma Gecko (Kontakt s.o.)

15. Zusammenfassende Bewertung gem. Art. 35 DSGVO

~~Es besteht kein hohes Risiko bei der Verarbeitung für die Rechte und Freiheiten natürlicher Personen~~

Die mit der Verarbeitung verbundenen Gefahren (hohes Risiko) werden durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam beherrscht.

~~Die mit dem Verfahren verbundenen Gefahren werden durch die Beschriebenen technischen und Organisatorischen Maßnahmen **nicht** wirksam beherrscht.~~

~~(Konsultation der Aufsichtsbehörde gem. Art. 36 DSGVO)~~

16. Prüfrhythmus der Risikoanalyse

- jährlich, beginnend 05/2018

Gartenhaus e.V.
Verantwortlicher Art. 35 DSGVO

Thomas Nehls
bDSB



Verarbeitungsverzeichnis Lohn-, Gehalts-, und Reisekostenbrechnung

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Petra Name: Schmidt Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303710 Fax: 03831 303719 E-Mail: schmidt@gartenhaus-ev.
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: Lohn- und Gehaltsabrechnung Vorname: Petra Name: Schmidt Anschrift: Langenstrasse 51, 1439 Stralsund Telefon: 03831-303710 Fax: 03831- 303719 E-Mail: schmidt@gartenhaus-ev.de
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Abrechnung der Löhne / Gehälter Abrechnung Reisekosten Urlaubsabrechnung
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Arbeitsvertrag Art. 6 Abs. 1 c DS-GVO § 41 ff EStG (Anforderungen Lohnsteuerberechnung) § 29 b AO (Notwendigkeit der Erhebung pbD für Finanzverwaltung) § 147 AO (Aufbewahrungspflichten) §§ 169 bis 171 und §§ 22 bis 232 AO (steuerliche Verjährungsfristen) § 4, 6 LStDV (Anforderung Dokumentation Lohnkonto) § 157 HGB (Aufbewahrungspflichten) § 28 f Abs. 3 SGB IV (Beitragsnachweise) DEÜV (Datenerfassungs- und übermittlungsverordnung)

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Vorname, Name, Anschrift, Geburtstag, Telefonnummer,	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Bankdaten der Mitarbeiter	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	Arbeitszeitnachweise, Dienststunden	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	Religionszugehörigkeit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Angaben zu Kindern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1-5	Mitarbeiter (Stammpersonal und Zuverdienst)
5	Kinder der Mitarbeiter

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1-5	Finanzamt wg. Lohnsteuer
1-5	Sozialversicherungsträger wg. Sozialabgaben
1,3	Betriebsrat
1	Träger der Betriebsrente

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1 - 5	Mitarbeiter

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 25.05.2018
1	Geschäftsführung Krüssel, Guido
2	Personalsachbearbeitung Schmidt, Petra
3	Verwaltungsleiter Nehls, Thomas
4	EinrichtungsleiterInnen
5	Betriebsprüfung durch FA und Deutsche Rente

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1 - 5
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1 - 5
<input checked="" type="checkbox"/> Sonstiges:	Datensicherung Stic

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
<i>Standard Line-Modul Lohn & Gehalt</i>	<i>3.9/4.69 vom 15.05.2018</i>
(Firma Helmerich)	

9. Fristen für die Löschung der Daten

Frist für Löschung:	7 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genaue Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Arbeits- und Gesundheitsschutz

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Stephanie Name: Wallow Anschrift: Grünhufe 5f, 18437 Stralsund Telefon: 03831 494081 Fax: 03831 444158 E-Mail: wohnheim-gruenhufe@gartenhaus.de
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: alle EinrichtungsleiterInnen Vorname: Name: Anschrift: Telefon: Fax: E-Mail:
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Sicherstellung des Arbeits- und Gesundheitsschutzes am Arbeitsplatz
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Arbeitsschutzgesetz Arbeitsstättenverordnung Arbeitszeitgesetz Arbeitssicherheitsgesetz § 27 Abs. 1, 2 MSchG Jugendarbeitsschutzgesetz § 22 Abs. 1, 1a+b BDSG nF

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Vorname, Name, Anschrift, Geburtstag, Telefonnummer,	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Einrichtung	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Vorsorgetermine	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1-3	Mitarbeiter, Praktikanten, FSJler, Mitarbeiter im Ehrenamt

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1-3	Erhebung zur Weiterleitung zwecks Klärung
	Landesamt für Gesundheit und Soziales (LaGuS)
	Betriebsarzt
	Fachkraft für Arbeitsschutz und Sicherheit

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1 - 3	Mitarbeiter, Praktikanten, FSJler, Mitarbeiter im Ehrenamt

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 15.05.2018
1	Geschäftsführung Krüssel, Guido
2	Personalsachbearbeitung Schmidt, Petra
3	EinrichtungsleiterInnen nur nach Aufforderung GF
4	Arbeitsschutzbeauftragte des Vereins

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input checked="" type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1 - 3
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1-3
<input checked="" type="checkbox"/> Sonstiges: Papierakten (formfrei)	1-3

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
<i>Office Home und Business</i>	<i>2010</i>

9. Fristen für die Löschung der Daten

Frist für Löschung:	5 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genaue Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt



Verarbeitungsverzeichnis Bewerbungsverfahren

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Petra Name: Schmidt Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303710 Fax: 03831 303719 E-Mail: schmidt@gartenhaus-ev.de
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langentrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: Geschäftsführer Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 1439 Stralsund Telefon: 03831-303710 Fax: 03831- 303719 E-Mail: schmidt@gartenhaus-ev.de
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Sichtung und Auswahl der eingehenden Bewerbungen Bezüglich der Eignung eines Bewerbers
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Bürgerliches Gesetzbuch BGB Einrichtungspersonal VO Einrichtungsqualitätsgesetz Art. 6 Abs. 1 b DS-GVO Allgemeines Gleichstellungsgesetz AGG

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Vorname, Name, Anschrift, Geburtstag, Telefonnummer,	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Qualifikation	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Bewerbung	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	Angaben zu Kindern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Bewerberinterview	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1-5	Bewerber (Stammpersonal und Zuverdienst)

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1-5	Geschäftsführer zwecks Vorauswahl
1-4	LeiterInnen der Einrichtungen zwecks Zustimmung
1,3	Betriebsrat zwecks Zustimmung
1-4	Lohn- und Gehaltsabrechnung zwecks Gehaltsangabe
1-5	Personalaktenführung bei Einstellung

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1 - 5	Bewerber

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 15.05.2018
1	Geschäftsführung Krüssel, Guido
2	Personalsachbearbeitung Schmidt, Petra
3	EinrichtungsleiterInnen nur nach Aufforderung GF

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input checked="" type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1 - 5
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1 - 5
<input checked="" type="checkbox"/> Sonstiges: Papierakte QMH FM 6.2-0	1-5

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
Office home Bussiness	2010

9. Fristen für die Löschung der Daten

Frist für Löschung:	6 Monate
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genaue Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Fortbildungsplanung und -abrechnung



1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Madeleine Name: Effenberger Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 – 303730 Fax: 03831 - 303719 E-Mail: m.effenberger@gartenhaus-ev.de
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: alle EinrichtungsleiterInnen Vorname: Name: Anschrift: Telefon: Fax: E-Mail:
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Jährliche Erfassung der Bedarfe in den Einrichtungen Zur Sicherstellung der Betreuungsqualität, der Personalentwicklung Auswahl der Fortbildungen entsprechend Bedarf und persönlicher Präferenzen Bewertung und Untersuchung von Wirksamkeiten
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Einwilligung gem. Art. 6 Abs.1 a

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Name, Vorname, Einrichtung	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Kompetenzen	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Inhalte und Abläufe der FB	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	Bewertungen	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	Reisekostenabrechnungen	<input type="checkbox"/>	<input checked="" type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1	Mitarbeiter (Stammpersonal und Zuverdienst)

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1-5	EinrichtungsleiterInnen
1-5	Geschäftsführer auf Anforderung
1-5	FB-Beauftragte Frau Effenberger
1-5	Verwaltungsleiter Herr Nehls

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1 - 5	Mitarbeiter (Stammpersonal und Zuverdienst)
1,4	Veranstalter der Fortbildungen
1 - 5	EinrichtungsleiterInnen

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 15.05.2018
1	LeiterInnen der Einrichtungen
2	Geschäftsführer
3	FB-Beauftragte Frau Effenberger
4	Verwaltungsleiter Herr Nehls
5	Lohn - / Gehaltsabrechnung Frau Schmidt

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1 – 5
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1-5
<input checked="" type="checkbox"/> Sonstiges: Papierakte QMH FM 6.2.2-4 FM 6.2.2-5 bis FM 6.2.2-7	1-5

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
Office Paket	2010

9. Fristen für die Löschung der Daten

Frist für Löschung:	5 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genauere Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Freistellung „Kind krank“



1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Petra Name: Schmidt Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303710 Fax: 03831 303719 E-Mail: schmidt@gartenhaus-ev.
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	<p>Ansprechpartner Einrichtung/Abteilung: Lohn- und Gehaltsabrechnung</p> <p>Vorname: Petra</p> <p>Name: Schmidt</p> <p>Anschrift: Langenstrasse 51, 1439 Stralsund</p> <p>Telefon: 03831-303710</p> <p>Fax: 03831- 303719</p> <p>E-Mail: schmidt@gartenhaus-ev.de</p>
1.6	<p>Zeitangaben</p> <p>Datum der Einführung: 25.05.2018</p> <p>Datum der Erstbeschreibung: 25.05.2018</p> <p>Datum der letzten Änderung: 25.05.2018</p>

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	<p>Zweckbestimmung</p> <p>Erfassung der Zeiten zur Pflege des erkrankten Kindes</p> <p>Lohnfortzahlung bis zu 10 Tagen pro Kind und Kalenderjahr</p>
2.3	<p>Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden)</p> <p>§ 45 Sozialgesetzbuch V</p> <p>§ 26 BDSG nF</p>

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Vorname, Name, Anschrift, Geburtstag des Kindes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	Kalendertage zur Pflege	<input type="checkbox"/>	<input checked="" type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

lfd. Nummer	
1-2	Mitarbeiter mit anspruchsberechtigten Kindern

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

lfd. Nummer aus Ziffer 3	Empfänger der Daten
1-2	Sozialversicherungsträger wg. bezahlter Freistellung
1 - 2	EinrichtungsleiterInnen

lfd. Nummer aus Ziffer 3	Herkunft der Daten
1 - 2	Mitarbeiter

6. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nummer	Stand 25.05.2018
1	Geschäftsführung Krüssel, Guido
2	Personalsachbearbeitung Schmidt, Petra
3	EinrichtungsleiterInnen

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1 - 2
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1 - 2
<input checked="" type="checkbox"/> Sonstiges: Papierakte QMH FM 6.2-5	1-2

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
Office Home und Business	2010

9. Fristen für die Löschung der Daten

Frist für Löschung:	5 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

lfd. Nummer aus Ziffer 3	Genaue Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt



Verarbeitungsverzeichnis Führerscheinkontrollen

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Name: Anschrift: Telefon: Fax: E-Mail:
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: alle EinrichtungsleiterInnen Vorname: Name: Anschrift: Telefon: Fax: E-Mail:
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Halbjährliche Kontrolle der Führerscheine zur Sicherstellung der Berechtigung zum Führen von Dienstwagen und zur Beförderung von Klienten
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Fürsorgepflicht des Arbeitgebers vor dem unberechtigten Führen eines Kraftfahrzeuges § 22 Abs. 1, 1a+b BDSG nF

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Angaben auf den Führerscheinen	<input type="checkbox"/>	<input checked="" type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

lfd. Nummer	
1	Mitarbeiter (Stammpersonal und Zuverdienst)

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

lfd. Nummer aus Ziffer 3	Empfänger der Daten
1	Dokumentation der Vorlage Keine weitere Übermittlung

lfd. Nummer aus Ziffer 3	Herkunft der Daten
1	Mitarbeiter (Stammpersonal und Zuverdienst)

6. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nummer	Stand 15.05.2018
1	LeiterInnen der Einrichtungen
2	Geschäftsführer

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input checked="" type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input checked="" type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input type="checkbox"/> Server im Unternehmen	
<input type="checkbox"/> Externe Server	
<input type="checkbox"/> PC / Arbeitsplatzrechner	
<input checked="" type="checkbox"/> Sonstiges: Papierakte QMH FM 6.4.3	1

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
keine	

9. Fristen für die Löschung der Daten

Frist für Löschung:	2 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genauere Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Klientenverwaltung procare



1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Christine Name: Langner Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303715 Fax: 03831 303719 E-Mail: c.langner@gartenhaus-ev.
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	<p>Ansprechpartner Einrichtung/Abteilung: alle EinrichtungsleiterInnen</p> <p>Vorname:</p> <p>Name:</p> <p>Anschrift:</p> <p>Telefon:</p> <p>Fax:</p> <p>E-Mail:</p>
1.6	<p>Zeitangaben</p> <p>Datum der Einführung: 25.05.2018</p> <p>Datum der Erstbeschreibung: 25.05.2018</p> <p>Datum der letzten Änderung: 25.05.2018</p>

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	<p>Zweckbestimmung</p> <p>Stammdatenerhebung laut ITP</p> <p>Erarbeitung Therapieplan</p> <p>Dokumentation der Betreuungsarbeit = Erstellung von Bewegungsdaten</p> <p>Vernetzung der Angebote mit Kostenträgern (Sachbearbeiter, Heimaufsicht, Anlage H-Prüfung) und Medizinischen Fachpersonal (Ärzte und Kliniken)</p>
2.3	<p>Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden)</p> <p>Einwilligungserklärung nach Art. 6 Abs.1 a DS-GVO, wenn kein ITP oder Inhalte darüber hinaus</p> <p>Art. 6 Abs. 1 b DS-GVO wg. Leistungen- und Prüfungsvereinbarung gem. § 75 SGB XII i.V.m. LRV MV</p> <p>Art.6 Abs.1 d DS-GVO in Krisensituationen</p> <p>§ 630f BGB Aufbewahrungsfristen Klientenakten</p>

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Alle Daten zur Gewährleistung einer personenzentrierten Hilfe entsprechend den Anforderungen aus dem ITP <ul style="list-style-type: none"> - Stammdaten - Verlaufsdaten - Gesundheitsdaten 	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1	Klienten, die über den ITP dem Hilfesystem zugeführt wurden
2	Klienten, die nicht über den ITP dem Hilfesystem zugeführt wurden (z.B. Selbstzahler)

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1	Leistungserbringer Gartenhaus e.V.
1	Sachbearbeiter Kostenträger als beauftragter zur Datenerhebung ITP
1	Heimaufsicht Landkreis Vorpommern
1	Anlage H-Prüfung Landkreis Vorpommern
1	Behandelnder Arzt
1	Gesetzlicher Betreuer wg. Gesundheitssorge

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1	Klienten
1	Örtlicher Sozialhilfeträger via ITP
1	Behandelnde Fachärzte
1	Gesetzliche Betreuer (ggfls. Angehörige)

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 25.05.2018
1	Betreuungspersonal entsprechend Auswahl ITP
2	Abrechnung Anwesenheiten Rechnungslegung
3	Geschäftsführer auf Anfrage

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input checked="" type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input checked="" type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1
<input checked="" type="checkbox"/> Sonstiges: Rücksicherung Qnap	

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
Office Home und Business	2010
Procare Basislizenz (Moveo)	I/2018
Procare Userlizenz (Moveo)	I/2018

9. Fristen für die Löschung der Daten

Frist für Löschung:	10 Jahre nach Auszug
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genauere Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Lieferantenbewertung



1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Thomas Name: Nehls (Verwaltungsleiter) Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303710 Fax: 03831 303719 E-Mail: t.nehls@gartenhaus-ev.
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: Verwaltung Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 1439 Stralsund Telefon: 03831-303710 Fax: 03831- 303719 E-Mail: t.nehls@gartenhaus-ev.de
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Bewertung der Lieferanten mit Kriterienkatalog Ziel : Aussagen zur Qualität, Liefertreue, Preis/Leistung
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Art. 6 Abs. 1 b DS-GVO Bewertungsverfahren gem. Qualitätshandbuch

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Firma, Anschrift, Telefonnummer	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Mitarbeiter der Firma	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Bewertungsstandards 0 bis 10	<input type="checkbox"/>	<input checked="" type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

lfd. Nummer	
1-3	UnternehmerInnen

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

lfd. Nummer aus Ziffer 3	Empfänger der Daten
1-3	Jährliche Erhebung bei den Mitarbeitern zur Qualität
1-3	VerwaltungsleiterIn zur Erstellung „Liste der freigegebenen Lieferanten“

lfd. Nummer aus Ziffer 3	Herkunft der Daten
1 - 3	Mitarbeiter

6. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nummer	Stand 25.05.2018
1	Geschäftsführung Krüssel, Guido
2	EinrichtungsleiterInnen
3	Verwaltungsleiter Nehls, Thomas

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1 - 3
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner Verwaltung	1 - 3
<input checked="" type="checkbox"/> Sonstiges: Papierakte QMH FH 7.4.1/7.4.2	1 - 3

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
Home office	2010

9. Fristen für die Löschung der Daten

Frist für Löschung:	3 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

lfd. Nummer aus Ziffer 3	Genaue Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Verwaltung „ehrenamtliche Mitarbeiter“



GARTENHAUS
Psychosozialer Trägerverein Stralsund e.V.

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Petra Name: Schmidt Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303710 Fax: 03831 303719 E-Mail: schmidt@gartenhaus-ev.de
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: EinrichtungsleiterInnen Vorname: Name: Anschrift: Telefon: Fax: E-Mail:
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Nachweis der Anwesenheit zur Anmeldung Berufsgenossenschaft
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Art. 6 Abs. 1 a DS-GVO (Einwilligungserklärung) Art. 6 Abs. 1 c DS-GVO (gesetzliche Unfallversicherung im Ehrenamt) § 2 SGB VII

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Vorname, Name, Anschrift, Geburtstag, Telefonnummer,	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1	Ehrenamtliche Mitarbeiter

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1	Berufsgenossenschaft

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1	Ehrenamtliche Mitarbeiter

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 15.05.2018
1	Geschäftsführung Krüssel, Guido
2	Personalsachbearbeitung Schmidt, Petra
3	EinrichtungsleiterInnen

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1
<input checked="" type="checkbox"/> Sonstiges: Papierakten	1

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
Office Paket	2010

9. Fristen für die Löschung der Daten

Frist für Löschung:	2 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genauere Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Personalakte / Stammdaten



1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Petra Name: Schmidt Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303710 Fax: 03831 303719 E-Mail: schmidt@gartenhaus-ev.
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	<p>Ansprechpartner Einrichtung/Abteilung: Lohn- und Gehaltsabrechnung</p> <p>Vorname: Petra</p> <p>Name: Schmidt</p> <p>Anschrift: Langenstrasse 51, 1439 Stralsund</p> <p>Telefon: 03831-303710</p> <p>Fax: 03831- 303719</p> <p>E-Mail: schmidt@gartenhaus-ev.de</p>
1.6	<p>Zeitangaben</p> <p>Datum der Einführung: 25.05.2018</p> <p>Datum der Erstbeschreibung: 25.05.2018</p> <p>Datum der letzten Änderung: 25.05.2018</p>

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	<p>Zweckbestimmung</p> <p>Führen von papierhaften Personalakten zur Stammdatenpflege Mitarbeiter</p>
2.3	<p>Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden)</p> <p>Arbeitsvertrag</p> <p>Art. 6 Abs. 1 c DS-GVO</p> <p>§ 41 ff EStG (Anforderungen Lohnsteuerberechnung)</p> <p>§ 29 b AO (Notwendigkeit der Erhebung pbD für Finanzverwaltung)</p> <p>§ 147 AO (Aufbewahrungspflichten)</p> <p>§§ 169 bis 171 und §§ 22 bis 232 AO (steuerliche Verjährungsfristen)</p> <p>§ 4, 6 LStDV (Anforderung Dokumentation Lohnkonto)</p> <p>§ 157 HGB (Aufbewahrungspflichten)</p> <p>§ 28 f Abs. 3 SGB IV (Beitragsnachweise)</p>

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Vorname, Name, Anschrift, Geburtstag, Telefonnummer,	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Bankdaten der Mitarbeiter	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	Qualifikationen	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	Religionszugehörigkeit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Angaben zu Kindern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	Arbeitsrechtliche Verträge	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1-5	Mitarbeiter (Stammpersonal und Zuverdienst)
3	Kinder der Mitarbeiter

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1-5	Finanzamt wg. Lohnsteuer
1-5	Sozialversicherungsträger wg. Sozialabgaben
1,3,6	Betriebsrat
1	Träger der Betriebsrente

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1 - 5	Mitarbeiter

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 15.05.2018
1	Geschäftsführung Krüssel, Guido
2	Personalsachbearbeitung Schmidt, Petra
3	Betriebsprüfung FA und Deutsche Rente

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input checked="" type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input type="checkbox"/> Server im Unternehmen	
<input type="checkbox"/> Externe Server	
<input type="checkbox"/> PC / Arbeitsplatzrechner	
<input checked="" type="checkbox"/> Sonstiges: Papierakten QMH FM 6.2-1, FM 6.2-3, FM 6.2-9, FM 6.2-13, FM 6.2-14	1-6

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
keine	

9. Fristen für die Löschung der Daten

Frist für Löschung:	10 Jahre nach Ausscheiden Unternehmen
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genaue Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Personalgespräche



GARTENHAUS
Psychosozialer Trägerverein Stralsund e.V.

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 – 3037-0 Fax: 03831 - 303719 E-Mail: kruessel@gartenhaus-ev.de
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: alle EinrichtungsleiterInnen Vorname: Name: Anschrift: Telefon: Fax: E-Mail:
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Jährliche Personalgespräche (u.a. in der Probezeit) Zur Sicherstellung der Betreuungsqualität Zur Abfrage der Personalentwicklung Zur Erstellung von Beurteilungen
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Art. 6 Abs. 1 a+f DS-GVO Einwilligung

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Name, Vorname, Einrichtung	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Fachkompetenz	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	Teamkompetenz	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	Ökonomische Kompetenz	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	Zielvereinbarungen	<input checked="" type="checkbox"/>	<input type="checkbox"/>

		<input type="checkbox"/>	<input type="checkbox"/>	
--	--	--------------------------	--------------------------	--

4. Kreis der Betroffenen

Ifd. Nummer	
1	Mitarbeiter (Stammpersonal und Zuverdienst)

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1-6	EinrichtungsleiterInnen
1-6	Geschäftsführer auf Anforderung

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1	Mitarbeiter (Stammpersonal und Zuverdienst)

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 15.05.2018
1	LeiterInnen der Einrichtungen
2	Geschäftsführer

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input checked="" type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input checked="" type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input type="checkbox"/> Server im Unternehmen	
<input type="checkbox"/> Externe Server	
<input type="checkbox"/> PC / Arbeitsplatzrechner	
<input checked="" type="checkbox"/> Sonstiges: Papierakte QMH FM 6.2.10 FM 6.2.11, FM 6.2-12	1-5

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
keine	

9. Fristen für die Löschung der Daten

Frist für Löschung:	5 Jahre
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genauere Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Torvideoanlage im Therapiezentrum



1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Guido Name : Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831- 30370_ Fax: 03831 - 303719 E-Mail: Stralsund@gartenhaus-ev.de
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	<p>Ansprechpartner Einrichtung/Abteilung: Therapiezentrum Psychose & Sucht</p> <p>Vorname: Madeleine</p> <p>Name: Effenberger</p> <p>Anschrift: Tribseer Straße 12, 18439 Stralsund</p> <p>Telefon: 03831-278525</p> <p>Fax: 03831- 282654</p> <p>E-Mail: therapiezentrum@gartenhaus-ev.de</p>
1.6	<p>Zeitangaben</p> <p>Datum der Einführung: 25.05.2018</p> <p>Datum der Erstbeschreibung: 25.05.2018</p> <p>Datum der letzten Änderung: 25.05.2018</p>

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	<p>Zweckbestimmung</p> <p>Auf Grund der baulichen Voraussetzungen ist eine Videoanlage notwendig, um aus dem Betreuerbüro heraus die Toranlage nur für Berechtigte zu öffnen</p>
2.3	<p>Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden)</p> <p>Art. 6 Abs.1 f DS-GVO (berechtigtes Interesse des Verantwortlichen = Zugangskontrolle)</p>

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Videobild nur zur Ansicht (keine weitere Speicherung)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
		<input type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1	Mitarbeiter, Klienten, sonst. Besucher

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1	Keine Aufzeichnung und keine Übermittlung

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1	Mitarbeiter, Klienten, Besucher

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 15.05.2018
1	Nur aktuell anwesende Mitarbeiter

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)

<input type="checkbox"/> Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/> Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenübertragung (keine Speicherung)

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input type="checkbox"/> Server im Unternehmen	
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1
<input type="checkbox"/> Sonstiges:	

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum

9. Fristen für die Löschung der Daten

Frist für Löschung:	Keine Frist, da keine Aufzeichnung
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	Laufend, da keine Aufzeichnung

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genauere Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Verwaltung für Vermietung



GARTENHAUS
Psychosozialer Trägerverein Stralsund e.V.

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: t.nehls@gartenhaus-ev.
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 1439 Stralsund Telefon: 03831 - 303714 Fax: 03831 - 303719 E-Mail: t.nehls@gartenhaus-ev.de
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Abrechnung der Betriebskosten und verursachergerechte Umlage auf die Mieter in der Fährstrasse 6, 18439 Stralsund
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Mietverträge Art. 6 Abs. 1 b DS-GVO

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Name, Vorname, Adresse	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Individuelle Mietvereinbarungen	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Abrechnungsdaten der Versorger	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4. Kreis der Betroffenen

Ifd. Nummer	
1	Mieter des Objektes

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Empfänger der Daten
1-3	Ambulante Wohnbetreuer
1-3	Technischer Dienst des Vereins
1-3	Ggfls. gesetzl. Betreuer

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

Ifd. Nummer aus Ziffer 3	Herkunft der Daten
1-3	Klienten

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 25.05.2018
1	Ambulante Wohnbetreuer
2	Abrechnung Vermietung/Verwaltung
3	Geschäftsführer auf Anfrage

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1
<input checked="" type="checkbox"/> Sonstiges: Rücksicherung Qnap	

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
<i>Office Home und Business</i>	2010

9. Fristen für die Löschung der Daten

Frist für Löschung:	5 Jahre nach Auszug
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genaue Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt

Verarbeitungsverzeichnis Versicherungen



1. Name und Anschrift der Daten verarbeitenden Stelle

1.1	Name und Anschrift Verantwortlichen Name: Gartenhaus e.V. Anschrift : Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Telefax: 03831 303719 E-Mail: stralsund@gartenhaus-ev.de Webseite: http://www.gartenhaus-ev.de Vereinsregisternummer: VR 249, Amtsgericht Stralsund Steuer-ID: 082/141/01018 Wirtschafts-ID:
1.2	Geschäftsführer: Vorname: Guido Name: Krüssel Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 3037-0 Fax: 03831 303719 E-Mail: kruessel@gartenhaus-ev.de
1.3	Leitung Datenverarbeitung: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: t.nehls@gartenhaus-ev.de
1.4	Datenschutzbeauftragter: Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 18439 Stralsund Telefon: 03831 303714 Fax: 03831 303719 E-Mail: Datenschutz@gartenhaus-ev.de

1.5	Ansprechpartner Einrichtung/Abteilung: Verwaltung Vorname: Thomas Name: Nehls Anschrift: Langenstrasse 51, 1439 Stralsund Telefon: 03831 - 303714 Fax: 03831-303719 E-Mail: t.nehls@gartenhaus-ev.de
1.6	Zeitangaben Datum der Einführung: 25.05.2018 Datum der Erstbeschreibung: 25.05.2018 Datum der letzten Änderung: 25.05.2018

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1	Zweckbestimmung Verwaltung und Bearbeitung der Versicherungsverträge des Vereins zur Absicherung der Risiken aus dem Geschäftsbetrieb Erhebung von allgemeinen Daten Erhebung und Verarbeitung von individuellen Daten im Rahmen der Schadensabwicklung
2.3	Rechtsgrundlagen (ggf. nach Zweck der DV unterschieden) Art. 6 Abs. 1 b, f DS-GVO

3. Art der gespeicherten Daten (besondere Kategorie)

Ifd. Nummer		Datum nach § 46 Abs. 14 BDSG neu relevant? (DSGVO Artikel 4 Abs. 13,14,15)	
		Ja	Nein
1	Name, Vorname, Einrichtung	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	Führerscheindaten	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Angaben zum Personenschaden	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4. Kreis der Betroffenen

lfd. Nummer	
1	Mitarbeiter
2	Geschädigte, bzw. der Rechtsvertreter

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

lfd. Nummer aus Ziffer 3	Empfänger der Daten
1-3	Union-Versicherungsdienst Detmold
1-3	EinrichtungsleiterInnen
1-3	Rechtsbeistand RA Piel & Partner
1-3	Berufsgenossenschaft bei Personenschaden

5. Art regelmäßig übermittelter Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

lfd. Nummer aus Ziffer 3	Herkunft der Daten
1 -3	Mitarbeitern
1 – 3	Geschädigte, bzw. der Rechtsvertreter

6. Zugriffsberechtigte Personen oder Personengruppen

Ifd. Nummer	Stand 25.05.2018
1	Verwaltung Versicherung / Schadensabwicklung
2	EinrichtungsleiterInnen auf Anfrage
3	Geschäftsführer auf Anfrage

7. Technische und organisatorische Maßnahmen

Sensibilität der gespeicherten Daten	
<input checked="" type="checkbox"/>	Stufe A (frei zugängliche personenbezogene Daten)
<input checked="" type="checkbox"/>	Stufe B (keine besondere Beeinträchtigung)
<input checked="" type="checkbox"/>	Stufe C (Beeinträchtigung des Ansehens)
<input checked="" type="checkbox"/>	Stufe D (Beeinträchtigung der Existenz)
<input type="checkbox"/>	Stufe E (Gefahr für Gesundheit, Leben oder Freiheit)

8. Technik des Verfahrens

8.1 Datenspeicherung

Datenspeicherung	Art der Daten (Ifd. Nummer aus Ziffer 3)
<input checked="" type="checkbox"/> Server im Unternehmen	1-3
<input type="checkbox"/> Externe Server	
<input checked="" type="checkbox"/> PC / Arbeitsplatzrechner	1-3
<input checked="" type="checkbox"/> Sonstiges: Formlose Papierakten	1 - 3

8.2 Software

Eingesetzte Software (einschl. Standardverfahren)	Version/ Stand/ Datum
<i>Office Home und Business</i>	2010

9. Fristen für die Löschung der Daten

Frist für Löschung:	5 Jahre nach Schadensregulierung
Frist oder Zeitpunkt für die Überprüfung der Erforderlichkeit der Datenbestände:	5 Jahre

10. Datenübermittlung in Drittstaaten

Ifd. Nummer aus Ziffer 3	Genauere Angaben zum Empfänger (Firma, Land, Adresse)
	entfällt



1. Technische und organisatorische Maßnahmen: Betreuung und Verwaltung

Pseudonymisierung

Klientendaten

Nicht möglich, da ein individueller Hilfebedarf gewährleistet werden muss und Therapieerfolgskontrolle im Einzelfall notwendig ist.

Mitarbeiterdaten

Nicht möglich, da Abrechnung und Meldung Sozialversicherung/Finanzamt personenbezogen erfolgen muss

Verschlüsselung

Außenstandorte: VPN Verschlüsselung mit AES / AES256

WLAN (wo vorhanden) WPA/WPA2 Verschlüsselung

Datensicherung Server : Verschlüsselung AES128

Gewährleistung der Vertraulichkeit (Zutrittskontrolle, Zugangskontrolle)

Zutrittskontrolle alle Einrichtungen und Geschäftsstelle:

- Schließanlagen mit Schlüsselnachweis
- Klientenakten in verschlossenen Schränken
- Personalunterlagen unter separaten Verschluss Einrichtungsleitung

Zugangskontrolle alle Einrichtungen und Geschäftsstelle

a. Gruppenrichtlinien/ Domainstruktur

1. Ebene : interne / externe Einrichtungen

intern (Langenstrasse 51) / Verwaltung oder Betreutes Wohnen

extern / alle Standorte einzeln

2. Ebene : Mitarbeiter je Standort

b. Passwort

b.1 Passwortstärke

- 8 Zeichen lang und 3 von 4 Merkmalen zwingend
Groß-/ Kleinbuchstaben/ Zahlen/ Sonderzeichen

(

b. 2 Zeitraum für Passwortänderung

- jährliche Änderung (Systemvorgabe)

c. Datei- und Verzeichnissicherheit

4 Obergruppen : Geschäftsführung/ Vorstand, Verwaltung,
EinrichtungsleiterInnen, MitarbeiterInnen Betreuung

Untergruppen : jede(r) MitarbeiterIn der Einrichtung

d. Protokollierung auf Betriebssystemebene

- nur Protokollierung Terminalserver

Gewährleistung der Integrität (Zugriffskontrolle, Eingabekontrolle, Trennungskontrolle)

- auf den AP-Rechnern läuft das Standardmäßige Logverfahren
- auf den Servern nur Logverfahren mit Administratorrechten
- der Serverschrank im Serverraum ist immer verschlossen
- der Schlüssel ist bei der Geschäftsführung deponiert
- Die Daten der verschiedenen Anwendungen sind getrennt auf Servern

Gewährleistung der Verfügbarkeit (Verfügbarkeitskontrolle)

- Rauchmelder, Notstromaggregat und Klima in Serverlandschaft
- Es gibt einen Sicherungs- und Wiederherstellungsplan
- Die Rücksicherung wird mind. 1x / Jahr im Rahmen der Wartungsarbeiten getestet

Gewährleistung der Belastbarkeit der Systeme

- Alle Serversysteme werden via Monitoring überwacht
- Im gesamten Netz ist eine Firewall aktiviert

Verfahren der Wiederherstellung der Verfügbarkeit personenbezogener Daten nach physischen oder technischem Zwischenfall (Verfügbarkeitskontrolle)

Es gibt einen Sicherungs- und Wiederherstellungsplan

Die Rücksicherung wird mind. 1x / Jahr im Rahmen der Wartungsarbeiten getestet.

Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM's

Durch den Datenschutzbeauftragten und die Geschäftsführung werden regelmäßig Kontrollen über die Einhaltung der TOM's durchgeführt

8. Technik des Verfahrens

8.1 Rechner und Betriebssystem

Client:	<input checked="" type="checkbox"/> Desktop Win 7 Pro und Win 10 Pro <input type="checkbox"/> Mobiles System <input type="checkbox"/> Terminal / Netz-PC (ohne Laufwerk / Festplatte)
Betriebssystem: Win7 Pro SP1 und 10 Pro	<input type="checkbox"/> Unix <input checked="" type="checkbox"/> Windows <input type="checkbox"/> Sonstiges:

8.2 Vernetzung

<input checked="" type="checkbox"/> Server: 1.physikalischer Server	Betriebssystem:Windows Dell PowerEdge T420 BS: VMware ESXi 5.5 CPU: 1x Intel Xeon E5-2430 2.2 GHz / 32GB RAM HDD: 4x 300GB Raid 5
--	---

Gartenhaus e.V.

<p>2.physikalischer Server</p>	<p><u>Virtuelle Server auf Server 1</u></p> <p>Server a = Domänencontroller, File Server Anti Viren Management Console, Datev Server b = Exchange, Faxserver, Spamschutz EMail</p> <p>BS: Windows Server 2012 R2 Standard</p> <p>Dell PowerEdge T630</p> <p>BS: VMware ESXi 6.0 CPU: 2x Intel Xeon E5-2630 2.4 GHz / 96 GB RAM HDD: 11x 300GB Raid10</p> <p><u>Virtuelle Server auf Server 2</u></p> <p>Server c = SQL Server Server d = Terminalserver</p> <p>BS: Windows Server 2012 R2 Standard</p>
<p><input checked="" type="checkbox"/> Sonstiges</p> <p>Sicherung: <i>Sicherungsgeräte:</i> <i>Speichermedium:</i></p>	<p><input checked="" type="checkbox"/> Sonstige eingesetzte Hardware (Chipkarte und Kartenlesegerät für Banking, Video in der Toranlage Therapiezentrum)</p> <p>Verwaltung Sicherungsgerät: QNAP TS-269 Pro – 2x 1 TB HDD Raid 1 / Speichermedium: externe HDD: 500GB</p> <p>Server 1: täglich 22:00 Uhr Server 2: täglich 01:00 Uhr Server 3: täglich 02:00 Uhr Server 4: täglich 04:00 Uhr</p> <p>Wohnheim Grischow Sicherungsgerät: QNAP TS-131P – 1x 2 TB HDD Speichermedium: externe HDD: 2 TB</p> <p>PC01: täglich 12:00 Uhr PC02: täglich 12:00 Uhr</p> <p>Langenstrasse 54 Sicherungsgerät: QNAP TS-239Pro II+ – 2x 2 TB HDD Raid 1</p>

Gartenhaus e.V.

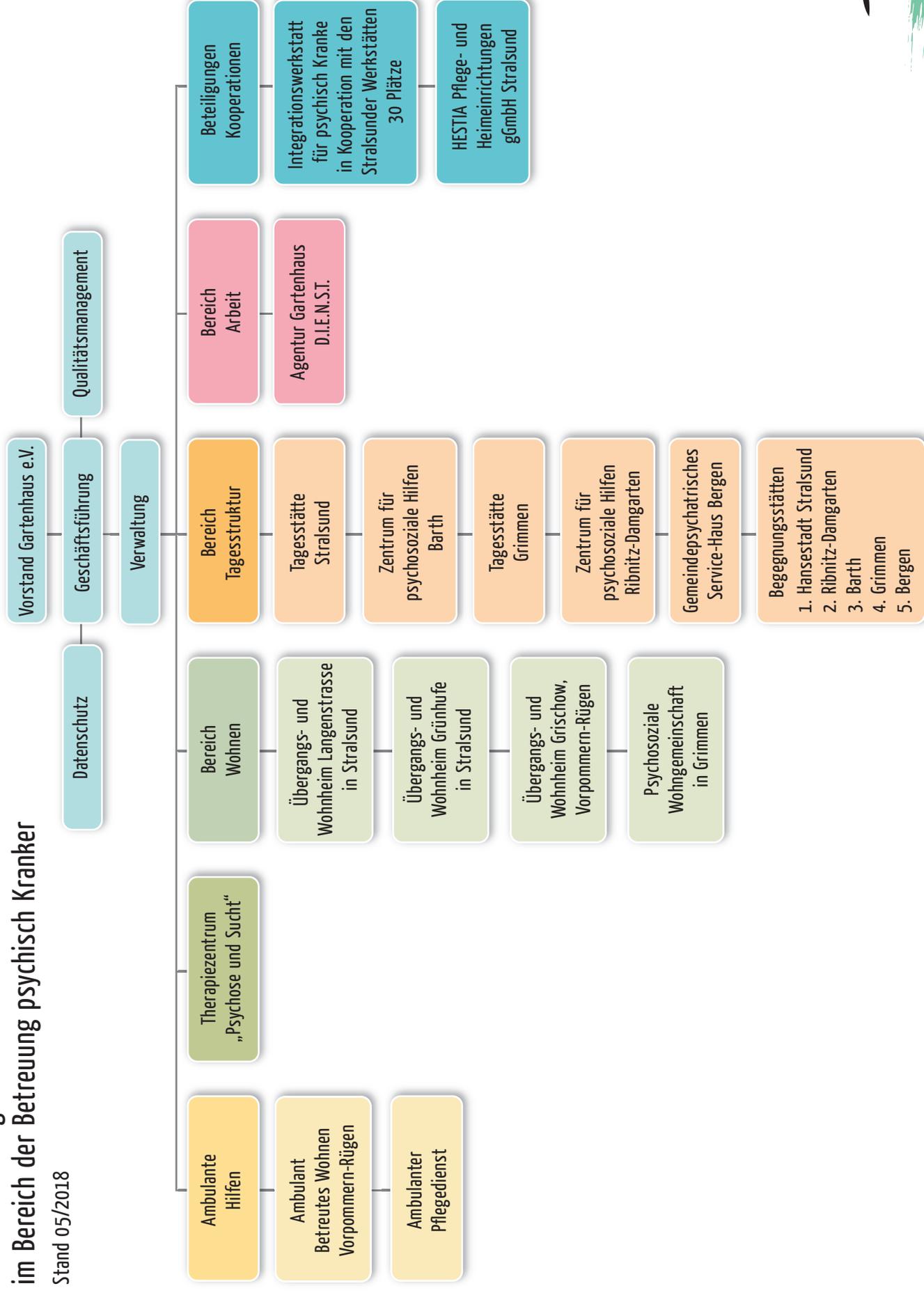
<u>USV:</u>	<p>Langenstrasse 54 Ordnerstruktur auf der QNAP QNAP Langenstrasse 54 sichert in Echtzeit auf QNAP Verwaltung</p> <p>Tagesstätte Bergen Sicherungsgerät: QNAP TS-112 – 1x 500GB HDD PC: täglich 11:45 Uhr</p> <p>Tagesstätte Ribnitz Sicherungsgerät: QNAP TS-231 – 2x HDD Ordnerstruktur auf QNAP Sicherung auf externe USB: täglich 21:00 Uhr</p> <p>Tagesstätte Grünhufe Sicherungsgerät: externe HDD PC: täglich 13:00 Uhr</p> <p>THZ Sicherungsgerät: Buffalo LinkStation Pro Duo PC: täglich 12:00 Uhr</p> <p>APC Smart-UPS 1500 für beide Server</p>
--------------------	--

8.2.1 Netzstruktur

<input checked="" type="checkbox"/> Netz im Unternehmen	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> Intranet <input checked="" type="checkbox"/> Sonstiges: WLAN
<u>Internet:</u> (Netz offen für jeden)	Watchguard Firewall à nicht genutzte Ports von außen gesperrt / Zugriff Websites offen
<u>WLAN in :</u> <i>WPA / WPA2</i>	<ul style="list-style-type: none">- Agentur D.I.E.N.S.T- Langenstrasse 54- Tagesstätte Barth- Tagesstätte Bergen- Tagesstätte Grimmen- Tagesstätte Ribnitz- Therapiezentrum- Wohnheim Grischow- Wohnheim Grünhufe

Struktur & Tätigkeitsfelder des Gartenhaus e.V. im Bereich der Betreuung psychisch Kranker

Stand 05/2018



GARTENHAUS
Psychosozialer Trägerverein Stralsund e.V.

VA 4.2.4-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 1 von 9

Arbeitsanweisung zum Normenkapitel mit dem Titel

Datenschutz und Datensicherheit

Diese Arbeitsanweisung dient dem Schutz sensibler personenbezogener und sachbezogener betriebsinterner Daten im Verein. Die Erhebung, Dokumentation und Auswertung von Daten ist notwendig für eine optimale Betreuung unserer Klienten und deren Dokumentation sowie zum Nachweis für auskunftsberechtigte externe Gremien.

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelenkte Vervielfältigen dieser Verfahrensanweisung ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese Verfahrensanweisung unterliegt dem Änderungsdienst.			
Revision 3	erstellt	geprüft	freigegeben
Datum	24.05.2018	24.05.2018	25.05.2018
Unterschrift	langner	Nehls-QMB	Krüssel-GF

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 2 von 9

Inhaltsverzeichnis dieser Verfahrensanweisung:		Seite
1.	Ziel und Zweck	3
2.	Geltungsbereich	3
3.	Begriffe	3
4.	Zuständigkeiten	3
4.1	Alle Mitarbeiter	3
4.2	Datenschutzbeauftragte(r)	3
5.	Beschreibung der Abläufe	4
5.1	Datenkatalogisierung	4
5.2	Datenerhebung	4
5.3	Datenverarbeitung	4
	-Personenbezogene Klientendaten	4
	-Personenbezogene Mitarbeiterdaten	6
	-Sachbezogene Betriebsdaten	7
5.4	Auftragsverarbeitung	8
5.5	Technisch organisatorische Maßnahmen	8
5.6	Betroffenenrechte	8
	Meldungen an den Datenschutzbeauftragten	
6.	Mitgeltende Unterlagen	9
7.	Vertraulichkeit	9
8.	Anhang	9

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 3 von 9

1. Ziel und Zweck

Die Erhebung von Daten, deren Dokumentation und die Weiterverarbeitung bzw. Auswertung sind notwendige Betriebsabläufe zur Realisierung unseres Betreuungsauftrages. Wir unterscheiden im Folgenden personenbezogenen Daten von Klienten, personenbezogene Daten von Mitarbeitern sowie betriebsinterne Daten ohne Personenbezug.

Oberstes Ziel soll es sein, nur die notwendige Mindestmenge an Daten zu ermitteln, zu verarbeiten und diese sicher vor Verlust und Missbrauch zu verwahren. Ein zielgerichteter Einsatz der Daten dient der Realisierung der Betreuungsziele unseres Klientels sowie zur Dokumentation gegenüber externen Kontrollgremien.

Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG sichergestellt. Dieses Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Geltungsbereich

Diese Verfahrensanweisung gilt in allen Organisationsbereichen unseres Vereins.

3. Begriffe

Datenschutz: beschreibt den Schutz des Bürgers vor Beeinträchtigung seiner Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten. Der Begriff bezeichnet ursprünglich den Schutz personenbezogener Daten vor Missbrauch. Der Zweck wird darin gesehen, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen Daten in seinem Recht auf informelle Selbstbestimmung beeinträchtigt wird. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönliche Daten zugänglich sein sollen.

Datensicherheit: umfasst das Konzept zur Sicherstellung der Integrität und Authentizität (Schutz der Daten vor Veränderung), der Vertraulichkeit und der Verfügbarkeit von Daten sowie der damit verbundenen Maßnahmen.

4. Zuständigkeiten

Alle Mitarbeiter des Vereins sind für die Einhaltung der Datenschutzbestimmungen und die Umsetzung der Datensicherheit verantwortlich. Jeder Mitarbeiter hat sich nur in dem vom Geschäftsführer bzw. Administrator für ihn freigegebenen Informationsbereich zu bewegen.

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 4 von 9

Datenschutzbeauftragte(r)

Der Verein hat zur Beratung der Geschäftsleitung und zur Unterstützung seiner Mitarbeiter eine(n) Datenschutzbeauftragte(n) berufen. Dieser Beauftragte berät die Mitarbeiter zu Fragen des Datenschutzes und überwacht die Einhaltung der gesetzlichen Vorgaben.

5. Beschreibung der Abläufe

5.1 Datenkatalogisierung

- 5.1.1 personenbezogene Klientendaten
Achtung : Art. 9 DS-GVO besondere Kategorien personenbezogener Daten
- 5.1.2 personenbezogene Mitarbeiterdaten
Achtung : Art. 9 DS-GVO besondere Kategorien personenbezogener Daten
- 5.1.3 sachbezogene Betriebsdaten

5.2 Datenerhebung

Sämtliche Daten und Informationen, die im Unternehmen zu erheben sind, dienen der Aufrechterhaltung der Arbeitsfähigkeit und sowie zur Sicherung der vereinbarten Betreuungsqualität. Gleichzeitig soll das betriebswirtschaftliche Gleichgewicht aufrecht erhalten werden.

Allgemeine Handlungshinweise :

- Für eine Datenerhebung/-verarbeitung sind entweder rechtliche Grundlagen oder aber die Einwilligung der betroffenen Personen notwendig. (Art. 6 Abs. 1 a-f)
- Diese Einwilligung muss eindeutig, unmissverständlich und freiwillig abgegeben werden. (Dokumentationspflicht nach Art. 7 Abs. 1 DS-GVO)
- Der Zweck der Datenerhebung und Verarbeitung muss eindeutig formuliert sein.
- Der Arbeitgeber / Leistungserbringer hat gegenüber dem Betroffenen eine Informationsverpflichtung gem. Art. 13,14 DS-GVO.
- Alle Mitarbeiter unterzeichnen bei Beschäftigungsaufnahme eine Verschwiegenheitserklärung zur Sicherstellung des Datenschutzes gem. der gesetzlich Vorgaben aus DS-GVO und BDSG.

5.3 Verarbeitung der Daten

5.3.1 personenbezogene Klientendaten

5.3.1.1 Verarbeitungswege

- a) Verarbeitung in EDV-Software procure der Moveo Software GmbH über Arbeitsplatz-Rechner auf dem Terminalserver in der Geschäftsstelle
- b) in office-Anwendung Windows an den Arbeitsplatzrechnern der Einrichtungen
- c) zusätzlich in handschriftlichen Akten, Aktenordner und Archiv

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 5 von 9

5.3.1.2 Zugriffsberechtigungen in procare

- a) in procare ist mit Hilfe von Benutzern und Benutzergruppen die Zugriffsberechtigung für einzelne Programmmodule hinterlegt.
- b) jeder Mitarbeiter, der mit procare arbeitet, muss vom Administrator als Benutzer angelegt werden und erstellt sein eigenes Passwort. Eine Anmeldung im Programm ist nur noch mit Benutzernamen und Kennwort möglich.
- c) Folgende Benutzergruppen sind in procare definiert:
 - Administratoren
 - Mitarbeiter der Betreuung mit Standortverwaltung zur laufenden Doku
 - Verwaltung zur Rechnungslegung

5.3.1.3 Einsichtnahme in Akten/Daten

- a) durch Mitarbeiter des Einrichtungsträgers
Jeder Mitarbeiter kann nur auf die ihm anvertrauten Klienten-Datenmenge der jeweiligen Organisationseinheit zugreifen. Weiterreichende Zugriffe sind nur mit Schweigepflichtentbindungen des betreffenden Klienten möglich.
- b) durch den Klienten gem. Art. 15 DS-GVO
Klienten ist die Einsichtnahme in Ihre Akte nach Kapitel 3 BDSG nF grundsätzlich zu gestatten.
Der Antragsteller (Klient oder sein gesetzlicher Betreuer) stellt einen begründeten schriftlichen Antrag an die datenverarbeitende Stelle, welchem innerhalb der nächsten 3 Tage, nach Rücksprache mit dem Datenschutzbeauftragten zu entsprechen ist. Auf Wunsch sollte dem Antragsteller zur Einsichtnahme ein separater Raum zur Verfügung gestellt werden.
- c) durch berechtigte Dritte
Gesetzliche Betreuer müssen für die angefragten Informationen den erforderlichen Umfang in ihrer Betreuungsvollmacht besitzen. So berechtigt z.B. die Vermögenssorge nicht automatisch zur Einsichtnahme in die Betreuungsdokumentation.

Die Aufsichtsbehörde ist im Rahmen ihrer Aufsichtstätigkeit (Heimaufsicht und Anlage H-Prüfung berechtigt, stichprobenweise (derzeit 3 Proben/Prüfvorgang) Einblicke in die Betreuungsdokumentation der zu prüfenden Einrichtung zu nehmen, um Aussagen hinsichtlich der angetroffenen Betreuungsqualität machen zu können.

- d) durch unberechtigte Dritte
Sonstigen Dritten ist eine Einsichtnahme nur mit ausdrücklicher, schriftlicher und vorheriger Genehmigung des Betroffenen möglich. Jegliche Offenlegung ohne Einwilligung oder Rechtsgrundlagen ist unzulässig.

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 6 von 9

5.1.3.4 Archivierung/Vernichtung

- a) Grundsätzlich wird die Klientenakte erst nach Verlassen des Betreuungsangebotes vom Verein archiviert. Dies geschieht zeitnah zentral in der Geschäftsstelle über den Datenschutzbeauftragten. Nur dieser ist nach Ablauf der Frist von 10 Jahren (§630f BGB) berechtigt, Klientenakten zu vernichten.
- b) die digitalen Datenbestände werden nach Ablauf der Frist entsprechend dem Löschkonzept automatisch oder auch manuell gelöscht

5.3.2 personenbezogene Mitarbeiterdaten

5.3.2.1 Verarbeitungswege

- a) Verarbeitung auf separatem Laptop in EDV-Software Standard Line-Modul Lohn & Gehalt der Firma Helmerich in der Geschäftsstelle
- b) office-Anwendungen Windows am Arbeitsplatzrechner Personalbuchhaltung
- c) zusätzlich handschriftliche Akten, Aktenordner und Archiv

5.3.2.2 Zugriffsberechtigungen

- a) die Stammdaten der Mitarbeiter werden zentral in der Personalbuchhaltung verwaltet. Dort haben nur die zuständige Personalbuchhalterin und der Geschäftsführer Zugriff. Auf die Lohnprogramm Fa. Helmerich hat nur die zuständige Personalbuchhaltung mittels Passwort Zugriff.
- b) die Bewegungsdaten (Arbeitszeitkarten, Dienststundennachweise, Reise- und Fortbildungsabrechnungen, etc.) werden in den Einrichtungen vom Mitarbeiter erstellt, vom zuständigen Leiter geprüft und zwecks Verarbeitung an die Zentralverwaltung in der Geschäftsstelle in einem verschlossenem Umschlag weitergeleitet.

5.3.2.3 Einsichtnahme in Personalakten

- a) durch den Mitarbeiter
Auf schriftlichen Antrag an den Geschäftsführer ist die Einsichtnahme in die eigene Personalakte zu ermöglichen
- b) durch die Personalbuchhaltung und dem Geschäftsführer
Der Geschäftsführer als Verantwortlicher und die Personalbuchhaltung als Vertreter des Verantwortlichen haben die Berechtigung zur Einsichtnahme in die Personalakten. Der jeweiligen Einrichtungsleitung ist auf Anfrage und nur über die Geschäftsführung Auskunft zu einzelnen Stammdaten des Mitarbeiters zu gewähren.
- c) durch berechtigte Dritte
Auf Verlangen der Aufsichtsbehörden
 - Finanzamt und Deutsche Rente i.R. einer Betriebsprüfung
 - Heimaufsicht und Anlage H i.R. Qualitätsüberwachung
 - Landesamt für Gesundheit und Soziales i.R. Überwachung Arbeits- und Mutterschutz
 - Integrationsamt i.R. Ausgleichabgabe

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 7 von 9

kann es notwendig werden, daß einzelne Daten aus den Personalakten einer Prüfung unterzogen werden müssen. Eine generelle und umfassende Einsichtnahme ist jedoch nicht gestattet.

5.3.2.4 Archivierung/Vernichtung

- a) Grundsätzlich wird die Mitarbeiterakte erst nach Beendigung des Beschäftigungsverhältnisses vom Verein archiviert. Dies geschieht zeitnah zentral in der Geschäftsstelle über den Datenschutzbeauftragten. Nur dieser ist nach Ablauf der Frist von 7 Jahren (§ 147 AO, 6 Jahre nach Ende Kalenderjahr) berechtigt, Mitarbeiterakten zu vernichten.
- b) die digitalen Datenbestände werden nach Ablauf der Frist entsprechend dem Löschkonzept automatisch oder auch manuell gelöscht

5.3.3 sachbezogene Betriebsdaten

5.3.3.1 Verarbeitungswege

- a) Verarbeitung auf 2 Arbeitsplatzrechnern in Software DATEV in der Geschäftsstelle
- b) office-Anwendungen Windows an den Arbeitsplatzrechner Sachbuchhaltung
- c) zusätzlich handschriftliche Akten, Aktenordner und Archiv

5.3.3.2 Zugriffsberechtigungen

- a) Geschäftsführung hat mittels Zugriff der entsprechenden Verwaltungsangestellten Einblick in die internen Betriebsdaten.
- b) Die Sachbuchhaltung hat wegen der notwendigen Verarbeitungstätigkeiten (DATEV) Zugriff auf die internen Daten

5.3.3.3 Einsichtnahme Dritter

- a) Berechtigte auf Grund Rechtsgrundlagen
 - Finanzamt i.R. Lohnsteuer und Jahresabschluss
 - Deutsche Rente i.R. Betriebsprüfung Sozialversicherung
 - Steuerberatung wetreu i.R. Jahresabschlussarbeiten
- b) Unberechtigte
Nur durch Einwilligung und Offenlegung durch die Geschäftsführung

5.3.1 bis 5.3.3 Datensicherung

Zur Sicherung des elektronischen Datenbestandes werden in regelmäßigen Abständen Sicherungskopien auf externen Datenspeichern verschlüsselt abgelegt und räumlich getrennt vom jeweiligen EDV-System verwahrt.

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 8 von 9

5.4 Auftragsdatenverarbeitung im Rahmen der IT-Betreuung

Grundsätzlich ist jedem außenstehenden unberechtigten Dritten die Einsichtnahme in personenbezogene und jegliche sachbezogene Betriebsdaten zu verweigern

- Ausnahmen davon:

Dauergenehmigungen für einen externen Zugriff/ Fernwartung haben derzeit nur Unternehmen für die Betreuung der Software i.R. der IT-Pflege :

- für Klientendokumentation procare (Moveo Software GmbH)
- Gehaltsprogramm (Helmerich)
- Buchführung via Datev (Gecko)

Diese Leistungserbringer wurden vertraglich verpflichtet, sicher zu stellen, dass auch Sie mit den dem Auftraggeber anvertrauten Daten (Klienten und Mitarbeiter) verantwortlich umgehen und keinerlei Informationen an Dritte weitergeben.

(Verschwiegenheitserklärung !)

5.5 technisch und organisatorische Massnahmen zur Datensicherheit

- a) Informationen von privaten Datenträgern, oder auch Daten aus dem Internet, dürfen nicht selbständig und unkontrolliert in das hauseigene EDV-System eingebracht werden. (z.B. privater PC oder auch Stic)
- b) Informationen per email sind grundsätzlich vor ihrer Öffnung und Verbreitung auf Ihre Unbedenklichkeit zu überprüfen.
- c) Alle Daten sind vor unberechtigtem Zugriff zu schützen. (Verschluss, Passwörter etc.)
- d) Zur Sicherung des elektronischen Datenbestandes werden in regelmäßigen Abständen Sicherungskopien auf externen Datenspeichern abgelegt und räumlich getrennt vom EDV-System verwahrt.
- e) Die Einrichtungen gewährleisten einen kontrollierten Zugang zur Datenverarbeitung nur für das autorisierte Personal.

5.6 Betroffenenrechte

5.6.1 Informationspflicht

Jeder Mitarbeiter hat den Klienten vor der Datenerhebung zu informieren über:

- Name und Kontakt des Datenverarbeiters (Gartenhaus e.V.)
- Kontaktdaten des Datenschutzbeauftragten
- Verarbeitungszweck für die erhobenen Daten
- Empfänger der Personenbezogenen Daten (z.B. Kostenträger)
hier auch : Folgen einer Nichtbereitstellung der Daten
- Die voraussichtliche Dauer der Speicherung
- das Recht des Betroffenen auf Auskunft, Berichtigung und Beschwerde

5.6.2 Meldepflicht bei Datenpannen

Erlangen die Mitarbeiter des Vereins Kenntnis von einer Datenschutzverletzung, so ist **umgehend** der Datenschutzbeauftragte schriftlich (email) zu informieren über :

- Beschreibung der Art der Verletzung
- Betroffene Personen, Kategorien der Daten, Umfang der betroffenen Daten
- Bereits eingeleitete Maßnahmen

VA 4.2.4.-2	Datenschutz und Datensicherheit	Kapitel
Juni 2008		Seite 9 von 9

6 Mitgeltende Unterlagen

FM Schweigepflicht für Mitarbeiter
FM Schweigepflichtentbindung
FM Informationspflichten

7 Vertraulichkeit

Innerhalb des QM-Systems erstellte QM-Dokumentationen stellen vertrauliche Unterlagen unseres Unternehmens dar. Sie dürfen nur mit Genehmigung der Geschäftsleitung an Dritte weitergegeben werden.

Alle QM-Dokumentationen für Qualitätsaufzeichnungen unterliegen grundsätzlich der Dokumentationspflicht. Bei Änderung ist ein Exemplar der Vorversion noch mindestens 3 Jahre durch das Qualitätsmanagement aufzubewahren.

Für das Vorliegen gültiger QM-Dokumentationen, die den Fachbereich betreffen, ist die Leitung des Fachbereichs zuständig. Die in den Fachbereichen vorliegenden Verfahrens- und Arbeitsanweisungen dienen nur der Information. Die Fachbereiche müssen vor Verwendung prüfen, ob das genutzte Dokument dem letzten Änderungsstand (Index) entspricht und gültig ist.

Bei Kopie des Originalexemplars in die verschiedenen Arbeitsbereiche und/oder Arbeitsplätze ist ein Vermerk zu machen um die Dokumentenlenkung zu gewährleisten. Der Austausch dieser Dokumente bei einer Überarbeitung ist vom Leiter des Fachbereiches durchzuführen.

8 Anhang

Kein Anhang

FM 4.2.4-2	Informationspflicht Art. 13, 14 DS-GVO	Kapitel
2018		Seite 1 von 1

**Informationspflicht des Arbeitgebers gegenüber dem Arbeitnehmer
gem. Art. 13,14 DS-GVO**

Der Arbeitgeber „Gartenhaus“ Psychosozialer Trägerverein Stralsund e.V.
Langenstr.51, 18439 Stralsund

muss im Rahmen des Beschäftigungsverhältnisses zum Zwecke der Entlohnung und der Abführung von Lohnsteuer, Sozialversicherung, betrieblicher Altersvorsorge vom Arbeitnehmer

.....
(Name, Vorname / Datum Arbeitsaufnahme)

personenbezogene Daten erheben, Verarbeiten und Speichern. Dies ist gesetzlich vorgeschrieben!
(Rechtsgrundlagen : Art.6, Abs. 1 c DS-GVO; § 147 AO; § 26 BDSG nF, § 4 Abs. 2 LStDV)

Datenverarbeitung : Personalbuchhaltung Frau Petra Schmidt
Langenstrasse 51, 18439 Stralsund
Tel. 03831 – 303710
email : schmidt@gartenhaus-ev.de

Datenschutzbeauftragter: Herr Thomas Nehls
Langenstrasse 51, 18439 Stralsund
Tel. 03831 – 303714
email : datenschutz@gartenhaus-ev.de

Empfänger der Daten : zuständiges Wohnsitzfinanzamt, Träger der Sozialversicherung,
ggfls. Versicherer der betrieblichen Altersvorsorge

Dauer Datenspeicherung: entsprechend Beschäftigungsverhältnis, zzgl. 6 Jahre nach Austritt

Umfang der Daten : entsprechend FM 6.2-13/2

Auskunftsrechte des Beschäftigten gem. Art. 13 Abs. 2 b) :

- Recht auf Auskunft, Berichtigung oder Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Recht auf Datenübertragbarkeit, Beschwerderecht

Diese Informationen habe ich heute zur Kenntnis genommen:

..... (Ort, Datum)
..... (Unterschrift)

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelentete Vervielfältigen dieser VA / FM ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese VA / FM unterliegt dem Änderungsdienst.			
Revision 0	erstellt	geprüft	freigegeben
Datum	24.05.2018	24.05.2018	24.05.2018
Unterschrift	QZ FM	Herr Nehls	Herr Krüssel

FM 4.2.4-3	Informationspflicht Art. 13, 14 DS-GVO	Kapitel
2018		Seite 1 von 1

Informationspflicht des Leistungserbringers gegenüber dem Klienten gem. Art. 13,14 DS-GVO

Der Leistungserbringer : „Gartenhaus“ Psychosozialer Trägerverein Stralsund e.V.
Langenstr.51, 18439 Stralsund

muss im Rahmen des Betreuungsverhältnisses zum Zwecke der Dokumentation der Umsetzung von Hilfeplänen sowie zum Nachweis der Zielerreichung beim Kostenträger für den Klienten

.....
(Name, Vorname / Datum Betreuungsaufnahme)

personenbezogene Daten erheben, Verarbeiten und Speichern. Dies ist gesetzlich vorgeschrieben!
(Rechtsgrundlagen : Art.6, Abs. 1 b DS-GVO, Leistungs- und Prüfungsvereinbarung gem. § 75 Abs. 3 Nr.1 und 3 SGB XII i. V. m. dem Landesrahmenvertrag MV gem. § 79 Abs. 1 SGB XII)

Datenverarbeitung:
(Stempel Einrichtung)

Datenschutzbeauftragter: Herr Thomas Nehls
Langenstrasse 51, 18439 Stralsund
Tel. 03831 – 303714
email : datenschutz@gartenhaus-ev.de

Empfänger der Daten sind: Gartenhaus e.V. / Planung und Dokumentation Teilhabe
Träger der Sozialhilfe/ Kostenträger

Dauer Datenspeicherung : entsprechend Betreuungsverhältnis,
nach Ausscheiden zzgl. 10 Jahre wg. § 630f BGB

Auskunftsrechte des Klienten gem. Art. 13 Abs. 2 b) :
- Recht auf Auskunft, Berichtigung oder Löschung, Einschränkung der Verarbeitung,
Widerspruchsrecht, Recht auf Datenübertragbarkeit, Beschwerderecht

Diese Informationen habe ich heute zur Kenntnis genommen:

.....
(Ort, Datum)

.....
(Unterschrift)

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelentete Vervielfältigen dieser VA / FM ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese VA / FM unterliegt dem Änderungsdienst.			
Revision 0	erstellt	geprüft	freigegeben
Datum	24.05.2018	24.05.2018	24.05.2018
Unterschrift	QZ FM	Herr Nehls	Herr Krüssel

FM 6.2-11	Personalgespräch jährlich	Kapitel
August 2007		Seite 1 von 6

Gesprächsprotokoll vom zur jährlichen Mitarbeiterbeurteilung

Name, Vorname : Einrichtung :

Beurteilungszeitraum:

Bereich 1 / Fachkompetenz

1.1 Umgang mit Klienten (Bewertung 1 – 2 – 3 – 4)

Wertschätzung, persönlicher Stil, Balance Empathie/Distanz, Freundlichkeit, Klarheit
therapeutische Haltung, Handeln mit fachlichen Hintergrund / Professionalität und
Reflexionsfähigkeit

1.2 Fachliches Wissen (Bewertung 1 – 2 – 3 – 4)

- 1.2.1 Theoretisches Wissen, Fachliteratur, Fachzeitschriften, Fortbildungen
- 1.2.2 Anwendung in der Praxis
(Beispiele nennen, z.B. Fortbildungsthemen und Anwendbarkeit, Hintergrund von eigener
professioneller Haltung)

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelenkte Vervielfältigen dieser Verfahrensanweisung ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese Verfahrensanweisung unterliegt dem Änderungsdienst.

Revision 2	erstellt	geprüft	freigegeben
Datum	I/2014	01.06.2014	01.07.2014
Unterschrift	Leitungsteam	Herr Krüssel	Herr Krüssel

FM 6.2-11	Personalgespräch jährlich	Kapitel
August 2007		Seite 2 von 6

Gesprächsprotokoll vom zur jährlichen Mitarbeiterbeurteilung

Name, Vorname : Einrichtung :

Beurteilungszeitraum: _____

Bereich 1 / Fachkompetenz

1.3 Durchführung von Arbeiten und Anforderungen (Bewertung 1 – 2 – 3 – 4)

Sorgfalt und Vollständigkeit in den Aufgaben (Betreuungorganisation, Dokumentation, Aktenführung, Schriftverkehr, IBRP u.ä.)

1.4 Umgang mit Angehörigen (Bewertung 1 – 2 – 3 – 4)

Einbeziehung in Betreuungsprozess des Klienten, Schweigepflicht, Distanz, Beratungspartner sein, Rollenverständnis bzgl. der Familiensysteme

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelentke Vervielfältigen dieser Verfahrensanweisung ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese Verfahrensanweisung unterliegt dem Änderungsdienst.			
Revision 2	erstellt	geprüft	freigegeben
Datum	I/2014	01.06.2014	01.07.2014
Unterschrift	Leitungsteam	Herr Krüssel	Herr Krüssel

FM 6.2-11	Personalgespräch jährlich	Kapitel
August 2007		Seite 3 von 6

Gesprächsprotokoll vom zur jährlichen Mitarbeiterbeurteilung

Name, Vorname : Einrichtung :

Beurteilungszeitraum: _____

Bereich 1 / Fachkompetenz

1.5 Zusammenarbeit mit externen Helfersystemen (Bewertung 1 – 2 – 3 – 4)

Freundlichkeit, Kooperation, Koordinationsfähigkeit / Klarheit in Absprachen,
Verlässlichkeit, Verhandlungsgeschick, Schweigepflicht

Bereich 2 / Teamkompetenz

2.1 Zusammenarbeit im Team (Bewertung 1 – 2 – 3 – 4)

Kommunikation untereinander, Fachliche Kommunikation, Transparenz im Handeln,
Verlässlichkeit in den Absprachen, Verständlichkeit, Übernahme von Arbeitsbereichen
und Verantwortung, Kooperatives Verhalten, Beweglichkeit bei unvorhergesehen
Arbeitsanforderungen/ Terminen, Wertschätzung der TeamkollegInnen, kollegiales
Verhalten, welcher Teamtyp ? –Abgrenzung /Gemeinsamkeit, Balance Persönliches/
Distanz

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungenehmigte Vervielfältigen dieser Verfahrensanweisung ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese Verfahrensanweisung unterliegt dem Änderungsdienst.

Revision 2	erstellt	geprüft	freigegeben
Datum	I/2014	01.06.2014	01.07.2014
Unterschrift	Leitungsteam	Herr Krüssel	Herr Krüssel

FM 6.2-11	Personalgespräch jährlich	Kapitel
August 2007		Seite 4 von 6

Gesprächsprotokoll vom zur jährlichen Mitarbeiterbeurteilung

Name, Vorname : Einrichtung :

Beurteilungszeitraum:

Bereich 2 / Teamkompetenz

2.2 Zusammenarbeit mit der Leitung (Bewertung 1 – 2 – 3 – 4)

Rollenklarheit bzgl. der Hierarchien, Umgang mit Anweisungen, Kenntnis und Einhaltung der Dienstwege

2.3 Verhalten bei Konflikten (Bewertung 1 – 2 – 3 – 4)

Erkennen und Benennen von Konfliktbereichen, Bereitschaft zur Klärung, Umgang mit Kritik, Kränkbarkeit, Impulsivität, Rückzug

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelenkte Vervielfältigen dieser Verfahrensanweisung ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese Verfahrensanweisung unterliegt dem Änderungsdienst.

Revision 2	erstellt	geprüft	freigegeben
Datum	I/2014	01.06.2014	01.07.2014
Unterschrift	Leitungsteam	Herr Krüssel	Herr Krüssel

FM 6.2-11	Personalgespräch jährlich	Kapitel
August 2007		Seite 5 von 6

Gesprächsprotokoll vom zur jährlichen Mitarbeiterbeurteilung

Name, Vorname : Einrichtung :

Beurteilungszeitraum:

Bereich 3 / Ökonomische Kompetenz

(Bewertung 1 – 2 – 3 – 4)

3.1 Wirtschaftlichkeit

Finanzielle Situation der Einrichtung im Blick haben, Realistisch Planen und Handeln

3.2 Umgang mit betrieblichen Arbeitsmittel

Achtsamkeit

3.3 Arbeitsorganisation

Planung der Arbeitsaufgaben, Zeitmanagement, Überstunden, Arbeitspensum und Zeitrahmen, Flexibilität bei dringenden Arbeitsaufgaben

Bereich 4

4.1 Rückblick

- welche Schwerpunkte hatte MA im letzten Jahr / Beurteilungszeitraum ?
- haben sich daraus besondere Erfahrungen ergeben ?
- besondere Herausforderungen / Reibungsflächen / Konflikte ?
- positive Erfahrungen, die sich weiterentwickeln lassen ?
- ergeben sich Änderungsbedarfe ? Zielformulierungen ?

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelenkte Vervielfältigen dieser Verfahrensanweisung ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese Verfahrensanweisung unterliegt dem Änderungsdienst.

Revision 2	erstellt	geprüft	freigegeben
Datum	I/2014	01.06.2014	01.07.2014
Unterschrift	Leitungsteam	Herr Krüssel	Herr Krüssel

FM 6.2-11	Personalgespräch jährlich	Kapitel
August 2007		Seite 7 von 6

FM 6.2-13/1	Personalfragebogen Lohn	Kapitel
Dezember 2013		Seite 1 von 1

Bei Beschäftigungsantritt: Informationspflicht gem. Art. 13,14 DS-GVO (FM 4.2.4-2)

(Änderungen bitte deutlich (X) kenntlich machen!) Bitte in Druckbuchstaben deutlich ausfüllen!

Name, Vorname:..... Geburtsname:.....

Geburtstag:.....Geburtsort:..... Staatsangehörigkeit:.....

Wohnhaft in:.....

Telefon/Funk:..... Konfession:

Steuerklasse: Kinderfreibetrag: Ident-Nr.:

Sozialversicherungs-Nr.:..... Krankenkasse.....

SEPA Kto-Verbindung:

BIC: IBAN:.....

- Ich bin**
- ledig
 - verwitwet
 - geschieden, seit dem
 - verheiratet, seit dem
 - getrennt lebend, seit dem
(bitte Datum eintragen)

Ich habe Kinder ja nein

Bitte reichen Sie rechtzeitig vor Aufnahme Ihrer Tätigkeit beim „Gartenhaus“ e.V. dieses ausgefüllte Formular nebst der Mitgliedsbescheinigung Ihrer Krankenkasse, ein polizeiliches Führungszeugnis sowie Ihr Gesundheitszeugnis ein.

Ich versichere, dass meine Angaben vollständig und richtig sind.
Mir ist bekannt, dass ich jede Änderung in meinen persönlichen Verhältnissen auf einem erneut ausgefüllten Personalfragebogen Lohn sofort mitzuteilen habe und dass ich zuviel gezahlte Bezüge zurückerstatten muss.

.....
Datum/Unterschrift

Fehler in unseren QM-Dokumenten sind unverzüglich zu melden, damit eine Korrektur stattfinden kann. Das ungelentkte Vervielfältigen dieser Verfahrensweisung ist untersagt. Hierzu wird das Einverständnis des QM-Beauftragten benötigt. Die Herausgabe und Verteilung erfolgt ausschließlich über ihn. Diese Verfahrensweisung unterliegt dem Änderungsdienst.			
Revision 7	erstellt	geprüft	freigegeben
Datum	20.06.2018	20.06.2018	01.07.2018
Unterschrift	Frau P.Schmidt	Herr Nehls	Herr Krüssel

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO_ab 25.05.2018)



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 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 dieser Verpflichtung habe ich erhalten.

Ort, Datum

Unterschrift des Verpflichtenden

Unterschrift des Verantwortlichen

Gemäß § 35 Abs. 1 SGB I hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 SGB X) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis).

Gemäß § 67 Abs. 1 SGB X sind Sozialdaten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.

Gemäß § 67 a SGB X ist das Erheben von Sozialdaten durch die maßgeblichen Stellen nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem SGB X erforderlich ist. Das heißt, es dürfen nur die Daten beim Betroffenen erhoben werden, die tatsächlich zur Leistungsgewährung erforderlich sind.

Dabei sind Sozialdaten grundsätzlich beim Betroffenen zu erheben. Sofern Sozialdaten nicht beim Betroffenen erhoben werden, ist dieser, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, über die Zweckbestimmung der Erhebung, der Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle zu unterrichten.

Des Weiteren dürfen Sozialdaten ohne Mitwirkung des Betroffenen nur gemäß § 67 a Abs. 2 Satz 2 SGB X erhoben werden.

Gemäß § 67 d Abs. 1 SGB X ist eine Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 - 77 SGB X oder nach einer anderen Rechtsvorschrift des SGB vorliegt. Gemäß § 67 d Abs. 2 SGB X trägt die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle.

Die Rechte des Einzelnen richten sich nach den §§ 81 ff. SGB X. Dort ist geregelt, dass sich jeder Betroffene, sofern er sich in seinen Rechten betreffend des Sozialdatenschutzes verletzt fühlt, an den Bundesbeauftragten für den Datenschutz oder an den nach Landesrecht zuständigen Datenschutzbeauftragten wenden kann.

Gemäß § 83 Abs. 1 SGB X ist den Betroffenen auf Antrag Auskunft zu erteilen:

1. über die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden und
3. den Zweck der Speicherung.

Ein solcher Antrag soll üblicherweise die Art der Sozialdaten, über die Auskunft erteilt werden soll, näher bezeichnen.

Des Weiteren hat der Betroffene ggf. ein Anspruch auf Berichtigung, Löschung und Sperrung von Daten sowie ein Widerspruchsrecht im Sinne des § 84 SGB X. Sozialdaten sind danach zu berichtigen, wenn sie unrichtig sind.

Außerdem sind Sozialdaten zu löschen, wenn ihre Speicherung unzulässig ist. Sozialdaten sind auch zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen beeinträchtigt werden.

Gemäß § 84 Abs. 1 a SGB X in Verbindung mit § 20 Abs. 5 Bundesdatenschutzgesetz dürfen Sozialdaten nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt.

Dies gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

Dies bedeutet, dass im Falle des Widerspruches gegen die Übermittlung der Daten zunächst geprüft werden muss, ob eine Rechtsvorschrift die Übermittlung im speziellen Fall erlaubt. Sollte dies nicht der Fall sein, wäre zu prüfen, ob das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation dem Interesse der verantwortlichen Stelle an der Verarbeitung bzw. Übermittlung überwiegt.

Erklärung zum Schutz personenbezogener Daten bezüglich der Hilfeplankonferenz

Die Hilfeplankonferenz hat die Aufgaben, über die weitere Versorgung von Menschen mit körperlicher oder geistiger Behinderung oder HIV/ AIDS-Erkrankung in der Region zu beraten und Empfehlungen auszusprechen. Ziel ist hierbei die Sicherstellung der adäquaten Versorgung der nachfragenden Personen. Grundlage der Beratung auf der Hilfeplankonferenz ist das Instrument des Integrierten Teilhabeplans (ITP).

Über die Erhebung, Speicherung und Weitergabe von Informationen im Rahmen der Integrierten Teilhabeplanung wurde ich informiert.

Ich bin damit einverstanden, dass die im Rahmen des Integrierten Teilhabeplans erhobenen und für die Eingliederungsleistung Betreutes Wohnen erforderlichen Daten vom Kostenträger erhoben, gespeichert und an die für die Leistungserbringung zuständigen Stellen / Einrichtungen weitergegeben werden.

Die im ITP erhobenen Daten werden im Rahmen der regionalen Teilhabeplanung folgenden Dienststellen / Personen zur Verfügung gestellt:

- Ich bitte um getrennte Planung der Hilfen im Bereich von Arbeit / Beschäftigung / Tagesstruktur
- Ich bitte um anonyme Beratung meines Hilfeplans. Das heißt ohne Nennung meines Namens
- Ich und/oder meine/e gesetzliche/r Betreuer/in möchte/n an der Hilfeplankonferenz teilnehmen.

Mit diesem Verfahren bin ich einverstanden und entbinde widerruflich die beteiligten Mitarbeiter/innen von ihrer Schweigepflicht, soweit dies für die Umsetzung des Teilhabeplans (ITP) erforderlich ist. Ich bin damit einverstanden, dass die Informationen des ITP an diejenigen Einrichtungen, Dienste und Bezugspersonen weitergegeben werden, die an der Erbringung der Hilfen beteiligt sind und die zu diesem Zweck obenstehend benannt werden.

Der Unterzeichner ist darüber informiert, dass der Übermittlung der Daten – ggf. auch zu einem späteren Zeitpunkt mit Wirkung für die Zukunft – widersprochen werden kann, sowie über die Rechte nach §§ 83, 84 SGB X.

Datum	Nachfragende Person	ggf. Bevollmächtigte/r, gesetzliche/r Betreuer/in
	Unterschrift/Nachfragende Person	Unterschrift/Bevollmächtigte/r, gesetzliche/r Betreuer/in

Literaturverzeichnis

- Bake, Ch. / Blobel, B. / Engel, K. / Koch, H. / Langrock, Kl. / Münch, P. / Pharow, P. / Tietze, B. / Wünscher, J.: Datenschutz und Datenschutz im Gesundheitsdienst und Sozialwesen. 2. Auflage, Datakontext-Fachverlag GmbH, 2004
- Blobel, B. (Hrsg.): Datenschutz in medizinischen Informationssystemen. Konflikte zwischen der Sozialgesetzgebung und dem Grundrecht auf informelle Selbstbestimmung. 1. Auflage, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, 1995
- Gräbig, Kl.: DIN EN ISO 9001:2015-Vergleich mit DIN EN ISO 9001:2008, Änderungen und Auswirkungen. 1.Auflage, Beuth Verlag GmbH, 2016
- Härtig, N.: Datenschutz-Grundverordnung. 1.Auflage, Verlag Dr. Otto Schmidt KG, 2016
- Krahmer, U. / Stähler, Th. P.: Sozialdatenschutz nach SGB I und X, 2.Auflage, Carl Hexmanns Verlag KG, 2003
- Mörsberger, Th.: Verschwiegenheitspflicht und Datenschutz – Ein Leitfaden für die Praxis der sozialen Arbeit. 1. Auflage, Lambertus-Verlag, 1985
- Schneider, U. Kl.: Einrichtungsübergreifende elektronische Patientenakten – Zwischen Datenschutz und Gesundheitsschutz. Dissertation, Springer-Verlag, 2014
- Tsolkas, A. / Schmidt, Kl.: Rollen und Berechtigungskonzepte – Identity- und Access-Management im Unternehmen. 2 Auflage, Springer Verlag, 2017
- Voigt, P. /Von dem Bussche, A: EU-Datenschutz-Grundverordnung – Praktikerhandbuch.1. Auflage, Springer-Verlag, 2017
- Von Boetticher, Arne: Das neue Teilhaberecht. 1. Auflage, Nomos Verlagsgesellschaft, 2018
- Wächter, M.: Datenschutz im Unternehmen. 5.Auflage, Verlag C.H.Beck, 2017
- Tinnefeld, M-T. /Buchner, B. /Petri, T. /Hof, H-J.: Einführung in des Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht. 6. Auflage, Walter de Gruyter GmbH, 2018

(EU) 2016/679, Datenschutz-Grundverordnung vom 24.05.2016, in Kraft getreten am 25.05.2018 (Abl. EU 04. Mai.2016 L 119 S. 1f)

BetrVG , Betriebsverfassungsgesetz vom 25.09.2001, (BGBl. I S. 2518)

BDSG nF, Bundesdatenschutzgesetz vom 30.06.2017, in Kraft getreten am 25.05.2018, (BGBl. I S. 2097)

BTHG, Bundesteilhabegesetz vom 23.12.2016, (BGBl. I S. 2541)

EQG M-V, Gesetz zur Förderung der Qualität in Einrichtungen für Pflegebedürftige und Menschen mit Behinderung sowie zur Stärkung ihrer Selbstbestimmung und Teilhabe vom 17.05.2010, (GVOBl. M-V S.241)

HeimG, Gesetz über Altenheime, Altenwohnheime und Pflegeheime für Volljährige vom 05.11.2001, (BGBl. I S.173)

KunstUrhG, Gesetz betreffend das Urheberrecht an Werken der Bildenden Künste und der Photographie vom 15.02.2001, (BGBl. I S. 266)

StGB, Strafgesetzbuch vom 13.11.1998, (BGBl. I S. 3322)

TKG, Telekommunikationsgesetz vom 22.06.2004, (BGBl. I S. 1190)

TMG, Telemediengesetz vom 26.02.2007, (BGBl. I S. 179)

Handbuch für das Qualitätsmanagement des Gartenhaus e.V.; Stand Mai 2018

Teil A4, Personalentwicklungskonzept ; Stand 20.01.2009

Krüssel, G.: Managementbericht des Gartenhaus e.V. 2016, erstellt Juni 2017

<https://wirtschaftslexikon.gabler.de/definition/it-governance-53193/version-276288>,
abgerufen am 26.05.2018

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html, abgerufen am 13.06.2018

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html;jsessionid=DCCE4EB985AA07B2BEA3D72C2CF20207.1_cid360, abgerufen am 10.07.2018

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Bachelor-Arbeit selbstständig und nur unter Zuhilfenahme der ausgewiesenen Hilfsmittel angefertigt habe. Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach anderen gedruckten oder im Internet verfügbaren Werken entnommen sind, habe ich durch genaue Quellenangaben kenntlich gemacht.

Diese Bachelor-Arbeit wurde in keinem anderen Studiengang als Prüfungsleistung verwendet.

Ort, Datum

Vorname u. Nachname