

Vereinbarung über die datenschutzgerechte Übernahme und Vernichtung von Datenträgern gem. Art. 28 EU- DSGVO

Zwischen

(„Verantwortlicher“ - im Folgenden „Auftraggeber“ genannt)

und

Diakoniewert- Diakonische Behindertenhilfe Bad Salzungen Schmalkalden e.V.

Sitz des Vereins	Verwaltungsanschrift
Beierstal 10	Markt 9
98596 Brotterode-Trusetal	36433 Bad Salzungen

(„Auftragsverarbeiter“ – im Folgenden „Auftragnehmer“ genannt)

1. Präambel

Ziel des vorliegenden Vertrags ist die datenschutzkonforme Durchführung gemäß des § 28 DSGVO jeglicher aufgrund des Hauptvertrags stattfindender Datenverarbeitung. Dies betrifft sowohl die Verarbeitung von Daten, welche der Auftraggeber an den Auftragsverarbeiter übergibt, als auch Daten, die im Auftrag des Auftraggebers erstmalig durch den Auftragsverarbeiter erhoben werden.

2. Gegenstand und Dauer des Vertrages

2.1 Gegenstand

- (1) Der Vertrag regelt die Übernahme und die datenschutzgerechte Vernichtung von Datenträgern gemäß den Vorgaben der DIN 66399:2012, Teil 1. Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle.
- (2) Der Auftragnehmer verpflichtet sich zur ordnungsgemäßen Übernahme und Vernichtung der Datenträger nach den Weisungen des Auftraggebers.
- (3) Die Menge der zu vernichtenden Datenträger, Abholungszeit und -Ort werden separat vereinbart und auf dem Lieferschein (im Folgenden „Leistungsvereinbarung“ genannt) festgehalten.
- (4) Das Schriftgut ist durch den Auftraggeber in Schutzklasse 2 gemäß DIN 66399 Teil 1 eingestuft. Die jeweilige Sicherheitsstufe wird nach Art der Daten (Sensibilität) festgelegt.

Folgende Sicherheitsstufe wird vereinbart:

- ✓ Sicherheitsstufe 3 (P3)
- ✓ Sicherheitsstufe 4 (P4)

- (5) Die Sicherheitsstufe 4 wird bei Papiermaterial durch die Partikelgröße P3 mit nachgelagertem Verwirbeln und Verpressen des Datenmaterials erreicht.
- (6) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in der Bundesrepublik Deutschland statt. Eine Verlagerung in ein Drittland ist nicht vorgesehen.

2.2 Die Dauer der Verarbeitung

- (1) Der Auftrag (zutreffendes bitte ankreuzen und ausfüllen):

- | | |
|-------------------------------------|---|
| <input type="checkbox"/> beginnt am | und erfolgt bis auf unbestimmte Zeit bis zur Kündigung einer Partei |
| <input type="checkbox"/> beginnt am | und endet nach einmaliger Ausführung. |

3. Konkretisierung des Auftragsinhalts

3.1 Art und Zweck der vorgesehenen Verarbeitung

Dieser Vertrag regelt die Übernahme und Vernichtung von ausgesonderten Datenträgern des Auftraggebers gemäß einzelnen Beauftragungen. Die einzelnen Beauftragungen werden in der Regel formlos per E-Mail, Telefon, mündlich oder Fax erteilt.

3.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind zu vernichtenden Dokumente des Auftraggebers oder Dritter, die folgende Datenart/-kategorien beinhalten können:

(1) Datenarten/ -kategorien

Im Zusammenhang mit Kunden oder Lieferanten/ Dienstleistern:

- | | |
|---|---|
| <input type="checkbox"/> Angaben zur Person (Tel.Nr., E-Mail, Adresse, ...) | <input type="checkbox"/> Identifikationsdaten (Steuer-ID,...) |
| <input type="checkbox"/> Vertragsbezogene Daten von Produkten Dritter | <input type="checkbox"/> Gesundheitsdaten (sensitive Daten) |
| <input type="checkbox"/> Finanzlage, Bonität | <input type="checkbox"/> Daten zum Arbeitsverhältnis |
| <input type="checkbox"/> Geschäft- und Unternehmenskunden | <input type="checkbox"/> |
| <input type="checkbox"/> Vertragsabrechnungs- und Zahlungsdaten | <input type="checkbox"/> |
| <input type="checkbox"/> Mitarbeiterdaten | <input type="checkbox"/> |
| <input type="checkbox"/> Bank- und Finanzdaten, Wertpapier-Einlageinformationen | |

(2) Kategorien betroffener Personen

Nach Art. 28 Abs. 3a) DSGVO umfasst der Kreis der etwaig Betroffenen folgende Personenkategorien (zutreffendes ist vom Auftraggeber bitte ankreuzen/ergänzen)

- | | |
|--|---|
| <input type="checkbox"/> Kunden | <input type="checkbox"/> Geschäftspartner |
| <input type="checkbox"/> Beschäftigte i.S. § 26 Abs. 8 BDSG (2018) | <input type="checkbox"/> Interessent |
| <input type="checkbox"/> Lieferanten | <input type="checkbox"/> Behörden |
| <input type="checkbox"/> Berater / Handelsvertreter | <input type="checkbox"/> Dienstleister |
| <input type="checkbox"/> Ansprechpartner | <input type="checkbox"/> Mitarbeiter |
| <input type="checkbox"/> Klienten | <input type="checkbox"/> |
| <input type="checkbox"/> Kostenträger | <input type="checkbox"/> |

(3) Sensitive Daten betroffener Personen

(zutreffendes ist vom Auftraggeber bitte ankreuzen/ergänzen)

- | | |
|--|--|
| <input type="checkbox"/> Rasse oder ethnische Herkunft | <input type="checkbox"/> Körperliche oder geistige Gesundheit |
| <input type="checkbox"/> Religiöse oder weltanschauliche Überzeugungen | <input type="checkbox"/> Passdaten |
| <input type="checkbox"/> Politische Meinungen | <input type="checkbox"/> Gewerkschaftsmitgliedschaft |
| <input type="checkbox"/> Sexualleben | <input type="checkbox"/> Rating, Qualitätsbewertungsdaten |
| <input type="checkbox"/> Internetnutzungs- und Webtracking-Informationen | <input type="checkbox"/> Biometrische Daten |
| <input type="checkbox"/> Nationale Identifizierungsnummer, (SV-Nummern, Führerscheinnummer, ...) | <input type="checkbox"/> Anklagen, Tatverdachtsfälle, Straftaten, Verurteilungen |

3.3 Übernahme und Vernichtung der Datenträger

- (1) Der Auftrag für die Übernahme und Vernichtung der einzelnen Datenträger kann mündlich (telefonisch, o.Ä.), schriftlich, per E-Mail, Briefpost oder Fax übermittelt werden. Die Leistungsvereinbarung wird auf dem Lieferschein festgehalten und vom Auftraggeber unterschrieben.
- (2) Je nach Vereinbarung stellt der Auftragnehmer dem Auftraggeber geschlossene und abschließbare Behälter zur Verfügung. Die Anzahl der benötigten Sicherheitsbehälter wird einvernehmlich zwischen den Vertragspartnern und den entsprechenden Erfordernissen festgelegt. Für Anlieferungen durch den Kunden trägt dieser für den Transport bis zur Annahme in der Anlieferungszone selbst die Verantwortung.
- (3) Die Abholung/ Der Austausch erfolgt nach vorheriger Terminvereinbarung. Der zur Übernahme der Datenträger berechnete Beauftragte des Auftragnehmers wird auf der Leistungsvereinbarung namentlich

hinterlegt. Die Leistungsvereinbarung wird von den befugten Mitarbeitern beider Vertragspartner abgezeichnet. Weiterhin wird auf der Leistungsvereinbarung die Sicherheitsbehälternummer, Datum und Uhrzeit bei der Anlieferung und Abholung dokumentiert.

- (4) Die übernommene Menge Datenträger ist vom Auftragnehmer in seiner Werkstatt zu vernichten. Die Datenträger gelten als vernichtet, wenn die vereinbarte Sicherheitsstufe erreicht worden ist. Nach der Vernichtung ist eine schriftliche Bestätigung (Vernichtungsprotokoll) an den Vertragspartner abzugeben.

3.3 Transport

3.3.1 Transport durch den Auftragnehmer

- (1) Der Transport der Datenträger darf nur in ge- und verschlossenen Fahrzeugen des Auftragnehmers und/oder Sicherheitsbehältnissen mit vom Auftragnehmer verpflichtetem Personal durchgeführt werden. Dabei muss sichergestellt sein, dass keine Datenträger verloren gehen oder entnommen werden können. Dies geschieht durch eine Begleitprotokollierung des Auftragnehmers.

3.3.2 Transport durch den Auftraggeber

- (1) Findet der Transport der Datenträger durch den Kunden selbst statt, ist dieser für die Einhaltung der datenschutzrechtlichen Bestimmungen selbst verantwortlich. Die datenschutzrechtliche Verantwortungsübernahme geschieht erst nach der Übernahme der Datenträger durch einen verantwortlichen Mitarbeiter der diakoniewert.

3.4 Vernichtungsprozess

- (1) Die übernommenen Datenträger sind zeitnah zu vernichten. Die Lagerung und Entleerung der Sicherheitsbehälter findet ausschließlich innerhalb eines geschlossenen und überwachten Bereichs statt. Dabei muss sichergestellt werden, dass Unbefugte keinen Zutritt haben und die Datenträger nicht mit denen anderer Auftraggeber vermischt werden. Die Art und Weise der Vernichtung richtet sich nach der Art, der Vertraulichkeit und Beschaffenheit der Datenträger nach dem jeweiligen Stand der Technik unter Beachtung der jeweils gültigen Normen (DIN 66399:2012). Der Auftragnehmer sichert die Vernichtung gemäß der in der Leistungsvereinbarung angegebenen Sicherheitsstufe zu.
- (2) Ein Nachweis, dass geeignete Maschinen zur Vernichtung nach der jeweils gültigen Norm (DIN 66399:2012) verwendet werden, wird vom Auftragnehmer erbracht und dokumentiert. Der Auftragnehmer hat über die Vernichtung der Datenträger ein schriftliches Vernichtungsprotokoll nach Angaben aus der jeweils gültigen Norm (DIN 66399:2012) abzugeben.

4. Technisch-organisatorische Maßnahmen

- (1) Der Auftragnehmer verpflichtet sich in seinem betrieblichen Verantwortungsbereich alle technischen und organisatorischen Maßnahmen gemäß der in Anlage 1 beschriebenen Sicherheitsmaßnahmen einzuhalten. Die dokumentierten Maßnahmen werden Vertragsbestandteil. Ändern sich die Kundenanforderungen oder die gesetzlichen Vorgaben, müssen diese zwischen den Parteien vereinbart, angepasst und schriftlich festgehalten werden.
- (2) Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3c, Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich hierbei um Maßnahmen, welche der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus

hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit, sowie der Belastbarkeit der Systeme, dienen. Hierbei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, und

die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne des Art. 32 Abs 1. DSGVO zu berücksichtigen.

- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen um-

zusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Berichtigung, Einschränkung und Löschung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder einschränken. Ersucht eine betroffene Person diesbezüglich beim Auftragnehmer Auskunft, wird diese an den Auftraggeber weiterverwiesen.

6. Unterauftragsverhältnisse

- (1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.
- (2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
- (3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
- (4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- (5) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

7. Rechte und Pflichten des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- (2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (4) Sabotage oder Manipulation an den (Sicherheits-) Behältern während der Standzeit beim Auftraggeber sind durch entsprechende organisatorische bzw. sonstige Sicherungsmaßnahmen zu verhindern. Die Anfertigung von Kopien überlassener Schlüssel von Sicherheitsbehältern, z.B. zur Mehrfachbenutzung, ist nicht gestattet. Die Vergabe von Schlüsseln ist zu dokumentieren. Der Verlust eines Schlüssels ist dem Auftragnehmer unverzüglich schriftlich anzuzeigen.
- (5) Schäden oder sonstige Veränderungen an den Behältern sind dem Auftragnehmer unverzüglich schriftlich anzuzeigen.
- (6) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, falls ihm Umstände bekannt werden, die eine ordnungsgemäße und sichere Vernichtung irgendwie beeinträchtigen könnten. Dem Auftraggeber obliegt die Verhinderung und sofortige Beseitigung solcher Umstände, soweit sie seinem Einfluss- bzw. Verantwortungsbereich zuzuordnen sind.
- (7) Der Auftraggeber trägt dafür Sorge, dass nur zu vernichtendes Datenmaterial in die Sicherheitsbehälter eingefüllt wird. Bei vorhanden sein von Fremdmaterial (z.B. Speisereste oder hausmüllähnlicher Abfall, Metallteile o.Ä.) in den Sicherheitsbehältern haftet der Auftraggeber für die dem Auftragnehmer entstehenden Kosten (Müllentsorgung, Reinigung der Behälter, Instandsetzung der Maschine etc.).
- (8) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder im Einzelfall durch einen zu benennenden Prüfer stichprobenartig vor Ort zu kontrollieren. Die Kontrolle muss rechtzeitig an-

gemeldet sein und darf den betriebsinternen Ablauf nicht stören. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Bedingt durch einen hohen technischen Mehraufwand für eine Besichtigung des Vernichtungsbereiches bei einer Kontrolle, fällt ein finanzieller Mehraufwand für den Auftraggeber an.

- (9) Kontrollen seitens des Auftraggebers finden nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftraggeber eine Kontrolle aus dringlichen Gründen anders anzeigt, ist diese rechtzeitig und dokumentiert dem Auftragnehmer mitzuteilen und terminlich abzustimmen.
- (10) Der Auftraggeber unterwirft sich gemäß § 30 Absatz 5 Satz 3 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz; veröffentlicht in ABl. EKD 2017, S. 353) der kirchlichen Datenschutzaufsicht. Die Unterwerfung erstreckt sich auf die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht nach §§ 43, 44 EKD-Datenschutzgesetz. Das EKD-Datenschutzgesetz ist eine Umsetzung der DSGVO.

8. Rechte und Pflichten des Auftragnehmers

- (1) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt.
- (2) Der Auftragnehmer sichert zu, beim Transport und bei der Vernichtung der Datenträger nur eigenes Personal einzusetzen, das nach § 26 DSGVO (Datenschutzgesetz der evangelischen Kirche Deutschland) auf das Datengeheimnis verpflichtet worden ist. Das eingesetzte Personal wurde mit den für sie relevanten datenschutzrechtlichen Bestimmungen vertraut gemacht. Das Personal verarbeitet die Daten nur entsprechend den festgelegten Weisungen des Auftraggebers.
- (3) Beim Auftragnehmer ist als Beauftragter für den Datenschutz Frau **Juliane Möller** bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- (4) Der Auftragnehmer erwirbt keine Rechte an den in seinen Besitz gelangten Datenträgern und darauf verzeichneten Daten, schriftlichen oder bildlichen Darstellungen. Die Einsichtnahme in die Datenträger sowie deren Weitergabe oder sonstige Verwendung durch den Auftragnehmer ist untersagt (soweit dies durch die DIN 66399:2012 gefordert wird).
- (5) Das durch die Vernichtung gewonnene Abfallgut geht in das Eigentum des Auftragnehmers über.

9. Mitteilungspflichten des Auftragnehmers

- (1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
 - a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

- (3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
- (4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. Weisungsbefugnis

- (1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Der Umgang mit den Daten erfolgt im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers.
- (2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 2. Unter befugten Personen sind die verantwortlichen Ansprechpartner der Einrichtungen zu verstehen, welche die Aufträge verwalten und erteilen.
- (3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- (4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11. Kontrolle

- (1) Der Auftraggeber ist berechtigt, den Transport und die Vernichtung der Datenträger zu überwachen. Der Auftragnehmer verpflichtet sich, die Anwesenheit von Beauftragten des Auftraggebers bei allen mit dem Transport und der Vernichtung zusammenhängenden Dienstleistungen und in allen dabei benutzten Räumen, Fahrzeugen und Betriebseinrichtungen zu dulden. Er gestaltet den Betriebsablauf so, dass die Überwachung durch den Beauftragten des Auftraggebers jederzeit gewährleistet ist. Der Auftragnehmer verpflichtet sich, die von der zuständigen Aufsichtsbehörde bei einer möglichen Überprüfung festgestellte Mängel unverzüglich abzustellen, den Auftraggeber über die Überprüfung zu unterrichten und ihm Einsicht in die Prüfberichte der Aufsichtsbehörde zu gewähren. Sollte der konkrete Auftrag von den festgestellten Mängeln betroffen sein, so ist die für den Auftraggeber zuständige Aufsichtsbehörde, mit in den Prozess einzubeziehen.
- (2) Werden im Vernichtungsprozess datenschutzrechtliche Verstöße festgestellt (Datenmaterial gelangt in fremde Hände bzw. wird vertragswidrig verwendet), so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren, damit dieser ggf. im Sinne des § 42a BDSG tätig werden kann.

12. Maßnahmen bei Funktionsstörungen

- (1) Der Auftragnehmer verpflichtet sich, geeignete Maßnahmen für den Fall von schwerwiegenden Funktionsstörungen in seinem Betriebsablauf zu treffen, um zu verhindern, dass auf die zur Vernichtung vorgesehenen Datenträger unbefugt zugegriffen wird. Der Auftraggeber ist über solche schwerwiegenden Funktionsstörungen unverzüglich zu verständigen.
- (2) Ansprechpartner für Meldungen von Unregelmäßigkeiten bei der Abwicklung von Arbeiten sowie für die Erteilung und Entgegennahme von weiteren Weisungen des Auftraggebers über Art, Umfang und Verfahren der Datenträgervernichtung sind:

für den Auftraggeber
für den Auftragnehmer Herr Stefan Heymel

- (3) Änderungen in der Person der Ansprechpartner teilen sich die Vertragspartner unverzüglich schriftlich mit. Weitere Weisungen des Auftraggebers bedürfen ebenfalls der Schriftform.

13. Vergütung

- (1) Die Vergütung des Auftragnehmers richtet sich nach der vereinbarten Menge und Auftragsleistung und wird gesondert in der Leistungsvereinbarung festgehalten.

14. Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder nach Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen die im Zusammenhang mit dem Auftragsverhältnis stehen (Lieferscheine, Rechnungen, Vernichtungsprotokolle, Kundendaten) unter Einhaltung der gesetzlichen Aufbewahrungsfrist datenschutzgerecht zu vernichten.

15. Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht. Beide Seiten sind in diesem Fall verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.
- (3) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch eine Insolvenz- oder Vergleichsverfahren oder sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (4) Für Nebenabreden ist die Schriftform erforderlich.

Ort, Datum

Unterschrift Auftraggeber

Unterschrift i.A. berechnigte Person

Fambach, 20.05.2019

Ort, Datum

Unterschrift Vorstand Auftragnehmer



Unterschrift i.A. Werkstattleiter

Anlage 1 Technische und organisatorische Maßnahmen

Der Auftragnehmer sichert zu, folgende technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 3 DSGVO getroffen zu haben:

Vorwort:

Die Maßnahmen lehnen sich eng an die Vorgaben der technischen Richtlinie DIN SPEC 66399 an. Sie erfüllen die Vorgaben gemäß Art. 28 Abs. 3c und Art. 32 DSGVO. Können einzelne Maßnahmen nicht 1:1 umgesetzt werden, werden gleichwertige Maßnahmen ergriffen, um ein mindestens vergleichbares Sicherheitsniveau zu gewährleisten.

1. Vertraulichkeit

Zutrittskontrolle

Der Auftragnehmer verwehrt den Zutritt unbefugter Personen zu dem Datenvernichtungsbereich. Die Bereiche in denen personenbezogene Daten verarbeitet werden, sind vor dem Zutritt Unberechtigter angemessen geschützt.

Der Zugang des Datenverarbeitungsbereichs ist videoüberwacht. Bei einer Videoaufzeichnung ist diese vor unbefugten Zugriffen geschützt.

Der Vernichtungsbereich ist ein baulich abgetrennter Bereich innerhalb eines Gebäudes der diakoniewert Diakonische Behindertenhilfe Bad Salzungen Schmalkalden e.V. Der Bereich ist nur mit Sicherheitsschlüsseln zu öffnen.

Der Zutritt ist nur für berechtigte Mitarbeiter, welche auf das Datengeheimnis verpflichtet wurden, möglich. Die verantwortlichen Mitarbeiter werden regelmäßig über die datenschutzrechtlichen Vorgaben belehrt. Dies wird dokumentiert und von den Belehrteten unterzeichnet.

Zugangskontrolle

Der Auftragnehmer verhindert die Nutzung durch unbefugte Personen von Datenverarbeitungssystemen. Der Auftragnehmer wird ausschließlich eigene Mitarbeiter oder zugelassene Mitarbeiter von Unterauftragsunternehmen Zugang zu Anwendungen, in denen personenbezogenen Daten verarbeitet werden, nur dem Umfang entsprechend gewähren, der zur Erfüllung der Aufgaben und Funktionen erforderlich ist. Der Auftragnehmer sichert zu, dass die Zugangskontrolle bei Verwaltungsarbeiten, welche im Zusammenhang mit der Auftragsabwicklung stehen (z.B. Erstellung Leistungsvereinbarung), mit einem Authentifizierungssystem (durch Eingabe des Benutzernamens und Benutzerkennwort) unterstützt wird.

Zugriffskontrolle

Der Auftragnehmer gewährleistet, dass die Benutzung der Datenverarbeitungssysteme mittels eines Berechtigungskonzeptes geschützt ist. Die Mitarbeiter haben nur auf die für Sie zugriffsberechtigten Inhalte und Funktionen unter Ihrer Berechtigung Zugang. Unbefugte Aktionen (z.B. Löschen, Mitlesen) außerhalb der Berechtigung sind nicht möglich.

Es erhalten die Mitarbeiter nur die Zugriffsrechte, welche Sie für den Zweck Ihrer Tätigkeit benötigen.

Der Physische Zugriff auf die Datenträger ist durch entsprechende Sicherheitsbehälter verhindert. Die Sicherheitsbehälter sind verschlossen und werden auch verschlossenen bei den Kunden aufgestellt. Bei einer Schlüsselübergabe für den Sicherheitsbehälter an den Kunden, wird dies auf der Leistungsvereinbarung dokumentiert. Die Konstruktion der Sicherheitsbehälter lässt einen Zugriff ohne Schlüssel nicht zu.

Trennungskontrolle

Der Auftragnehmer gewährleistet, dass das Datenmaterial des Auftraggebers von Daten anderer Kunden und eigener Daten logisch oder physisch voneinander getrennt verarbeitet werden. Die Identifizierung der verantwortlichen Stelle ist zu jedem Zeitpunkt der Verarbeitung möglich.

Die Sicherheitsbehälter mit dem Datenmaterial der einzelnen Kunden sind bis zur Öffnung im Sicherheitsbereich der Datenvernichtungsanlage voneinander getrennt. Bei der Zuführung zur Vernichtungsmaschine können die Datenträger der einzelnen Kunden vermischt werden.

2. Integrität

Weitergabekontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierbei ist feststellbar an welchen Stellen der Einrichtung eine Datenübertragung stattfindet oder vorgesehen ist.

Werden Datenträger in einer Umgebung verarbeitet welche über keine Zugriffskontrolle verfügen, werden diese Daten, wenn nötig verschlüsselt.

Der Transport der Sicherheitsbehälter vom Kunden durch den Auftragnehmer bis zur Vernichtungsanlage erfolgt verschlossen. Verwendete Fahrzeuge verfügen über einen geschlossenen Sicherheitsaufbau der von außen keinen Einblick auf das Transportgut ermöglicht. Der Transport der Sicherheitsbehälter vom Kunden zur Vernichtungseinrichtung wird immer mit zwei Mitarbeitern durchgeführt. Das Transportfahrzeug ist geschlossen solange sich kein Mitarbeiter im oder unmittelbar am Fahrzeug befindet. Der Transport findet gegebenenfalls im Rahmen einer Sammeltour statt.

Die Sicherheitsbehälter werden vom LKW unmittelbar in den Sicherheitsbereich der Vernichtungsanlage gebracht. Außerhalb des Sicherheitsbereiches werden die Fahrzeuge dauerhaft von autorisiertem Personal überwacht.

Die Sicherheitsbehälter werden ausschließlich in dem geschlossenen Sicherheitsbereich entleert und der Vernichtungsanlage zeitnah zugeführt. Falls eine Zwischenlagerung notwendig ist, wird diese gemäß der DIN 66399 Teil 3 erbracht.

Die Räume des Sicherheitsbereichs sind so ausgestattet, dass Datenmaterial auch bei Durchzug nicht nach außen gelangen kann.

Besucher müssen auf die datenschutzrechtlichen Regelungen im Vernichtungsbereich hingewiesen und schriftlich darauf verpflichtet werden. Besucherzutritte werden dokumentiert.

Eingabekontrolle

Der Auftragnehmer gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben werden oder entfernt worden sind.

Es dürfen nur autorisierte Mitarbeiter des Auftragnehmers Änderungen an personenbezogene Daten vornehmen. Die Änderungen der personenbezogenen Daten werden protokolliert.

Die Kontrolle der übergebenen Datenträger durch den Auftragnehmer entfällt. Welche Daten und Datenträger übergeben wurden stellt der Auftragnehmer nicht fest. Die Datenträger werden der Vernichtung zugeführt. Es wird lediglich die Behälteranzahl, die Art und gegebenenfalls das Gewicht der übergebenen Datenträger erfasst. Trennungen und Vermischungen der Datenträger finden in der Sicherheitszone statt.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Der Auftragnehmer gewährleistet, dass die personenbezogenen Daten gegen eine zufällige Zerstörung oder einen Verlust geschützt sind. Bei einem totalen Systemausfall versucht der Auftragnehmer die Durchführung der Services zeitplanmäßig zu erbringen und umzusetzen.

Die Sicherheitsbehälter werden bei Anlieferung sofort in den Sicherheitsbereich gebracht. Eine Zwischenlagerung findet in einem Sicherheitsbereich oder einen überwachten Bereich entsprechend der DIN 66399

statt.

Die Sicherheitsbehälter werden vor jedem neuen Gebrauch kontrolliert. Die Kontrolle umfasst eine Sichtung von Beschädigungen am Behälter und einer Sichtkontrolle über eventuell noch vorhandenes Datenmaterial

im Behälter. Vor jedem Ausliefern, wird der Behälter erneut kontrolliert. Bei Verunreinigungen oder Beschädigungen muss der Behälter gesäubert oder Instand gesetzt werden.

Die Vernichtungsmaschinen sind eigens für diesen Zweck konstruierte Maschinen. Sie entsprechen den Anforderungen der DIN 66399 Teil 1 und werden regelmäßig gewartet.

Das Material wird vor der Vernichtung sortiert. Dies soll mögliche Fremdstoffe oder Ordner, Hefter oder andere Gegenstände herausfiltern, um eine gute Recyclingqualität zu ermöglichen. Das vernichtete Datenmaterial wird dem Recycling durch die Papierindustrie zugeführt.

Im Falle eines Komplettausfalls der Vernichtungsanlage werden Maßnahmen in Abstimmung mit dem Auftraggeber für eine vertragsgemäße Lagerung oder Weitergabe an eine Partner-Werkstatt für behinderte Menschen ermöglicht.

Wiederherstellbarkeit

Eine Wiederherstellbarkeit der vernichteten Datenträger ist nicht vorgesehen.

4. Regelmäßige Überprüfung, Bewertung und Evaluierung des Verfahrens (Art. 32 Abs. 1 DSGVO; Art. 25 Abs. 1 DSGVO)

Der Auftragnehmer sichert dem Auftraggeber zu, dass die personenbezogenen Daten welche im Auftrag verarbeitet werden, entsprechend den Weisungen des Auftraggebers ausgeführt werden. Der Auftraggeber bleibt verantwortliche Stelle und besitzt Kontrollrechte.

Der Auftragnehmer sichert zu, technische und organisatorische Maßnahmen

- unter Berücksichtigung des Stands der Technik, Implementierungskosten und Art des Umfangs/ der Umstände/ der Zwecke der Verarbeitung, und
- unter Berücksichtigung der unterschiedlichen Eintrittswahrscheinlichkeiten, und dem damit verbundenen Risiko für die Rechte und Freiheiten natürlicher Personen

zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung, als auch zum Zeitpunkt der Verarbeitung selbst, zu erbringen.

Ort, Datum

Unterschrift Auftraggeber

Unterschrift i.A. berechnigte Person

Fambach, 20.05.2019

Ort, Datum

Unterschrift Vorstand Auftragnehmer

Unterschrift i.A. Werkstattleiter



Anlage 2 Berechtigte Personen (siehe Punkt 10.2)

Bitte geben Sie Ihre weisungsbefugten Mitarbeiter für den Bereich der Aktenvernichtung an.

Diakoniewert

Herr Stefan Heymel (Werkstattleitung)
Herr Silvio Schulze (Gruppenleiter Aktenvernichtung)
Frau Tina Göhring (Sekretariat)