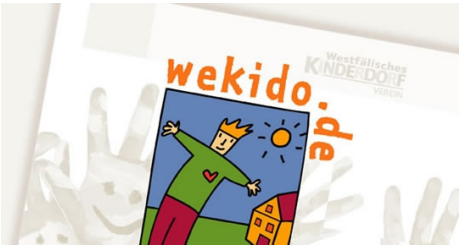
Beschreibung des Datenschutzkonzeptes des Westfälischen Kinderdorf e. V.

Westfälisches Kinderdorf e. V.
Haterbusch 32
D-33102 Paderborn
Telefon: 00 49 (0) 52 51 / 89 71 - 0
Telefax: 00 49 (0) 52 51 / 89 71 – 20
E-Mail: info@wekido.de
Internet: http://www.wekido.de/



Externer Datenschutzbeauftragter:
Dirk Fromm
Datenschutzbeauftragter und –auditor (TÜV® PersCert)
Information Security Officer - ISO 27001 (TÜV® PersCert)
CE21 - Gesellschaft für Kommunikationsberatung mbH
Bergfeldstr. 11, 83607 Holzkirchen

Wir über uns

Verein Westfälisches Kinderdorf — Wir sind Zukunft

Benachteiligten Kindern eine neue Familie, eine neue Heimat zu geben, war das Motiv interessierter Bürger, die sich vor mehr als 57 Jahren, am 12. April 1961, in Paderborn trafen. Ihre Vision war es, das erste Kinderdorf in Nordrhein-Westfalen zu eröffnen. Zwei Monate später wurde der Verein Westfälisches Kinderdorf ins Leben gerufen. Heute betreiben wir rund ein Dutzend Einrichtungen der Kinder- und Jugendhilfe im Dreieck der Städte Paderborn, Barntrup (Lippe) und Dissen (Niedersachsen). Darunter sind Kitas, offene Kinder- und Jugendtreffs, zwei Kinderdörfer, ein Lehrbauernhof und eine Ausbildungsküche sowie eine ganze Reihe von betreuten Wohngruppen für junge Erwachsene. Der Verein, dem eine gemeinnützige GmbH und eine Stiftung zur Seite stehen, beschäftigt aktuell rund 400 Mitarbeiterinnen und Mitarbeiter.

Der weit in das Umland wirkende Verein ist selbstständig und nicht Teil eines größeren Zusammenschlusses. Als überkonfessionelles Kinderdorfwerk ist das Westfälische Kinderdorf e. V. staatlich anerkannter freier Träger der Jugendhilfe. Seit 1987 ist der Verein Westfälische Kinderdörfer Mitglied im Deutschen Paritätischen Wohlfahrtsverband (DPWV).

Rund 1300 Mitglieder sowie rund 11000 Spender und Förderer ermöglichen dem Verein, die entgeltfinanzierten Erziehungshilfen zukunftsfähig zu gestalten und neue Angebote für Kinder, Jugendliche und deren Familien im Freizeit- und Förderbereich zu entwickeln und zu finanzieren.

Die von der Mitgliederversammlung gewählten ehrenamtlichen Gremien, Kuratorium und Vorstand, wahren die Tradition der Familienpflege und stellen sich gleichzeitig an die Spitze pädagogischer und organisatorischer Innovationen. Mit der zweiköpfigen hauptamtlichen Geschäftsführung verfolgen sie gesellschaftliche Entwicklungen und Umbrüche in den Sozial(dienst)leistungen aufmerksam und entwickeln Konzept und Organisation des Kinderdorfwerkes laufend weiter.

Wir leben Datenschutz!

Durch das Internet, die automatisierte Datenverarbeitung und den Datenaustausch besteht zunehmend die Gefahr, dass Daten ohne Wissen des Betroffenen an Dritte weitergegeben werden oder unbekannt abhanden kommen können. Dabei liegt uns der Schutz der uns anvertrauten Kinder besonders am Herzen und es hat für uns eine hohe Priorität diese personenbezogenen Daten zu schützen.
Um personenbezogene Daten zu schützen und jeden Datenmissbrauch zu verhindern, haben wir einen hauptberuflichen externen Datenschutzbeauftragten bestellt. Mit ihm gemeinsam haben wir ein Datenschutzkonzept entwickelt welches gewährleistet, dass alle datenschutzrechtlichen Anforderungen umgesetzt werden und sichergestellt ist, dass alle personenbezogenen Daten gesetzeskonform verwaltet werden. Unser Konzept basiert auf der Europäischen Datenschutzverordnung (EU DS-GVO). Auf den folgenden Seiten finden Sie die wichtigen Bausteine unseres Datenschutzkonzeptes.

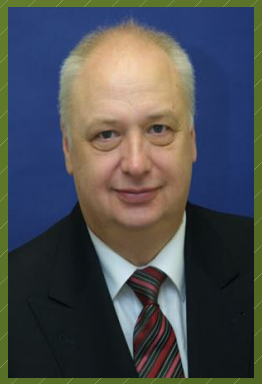
Vorstand und Datenschutzbeauftragter:

Friedrich -Martin Dreier
Vorstandsvorsitzender
Westf. Kinderdorf e.V.

Jürgen Scholz
Vorstand
Westf. Kinderdorf e.V

Birgit Flato
Vorstand
Westf. Kinderdorf e.V.

Externer Datenschutzbeauftragter des Westfälischen Kinderdorf e. V.



Dirk Fromm (Jurist)
Bergfeldstraße 11
83607 Holzkirchen
Tel: 089 71672111-30
E-Mail: dirk.fromm@ce21.de

Zertifizierter Datenschutzbeauftragter und Datenschutzauditor (TÜV® PersCert)
Information Security Officer - ISO 27001 (TÜV® PersCert)
CE21 - Gesellschaft für Kommunikationsberatung mbH

Inhalte:

- Umsetzung von Datenschutzanforderungen
- Aufbau des Datenschutzkonzeptes
- Verfahren
- Technische und organisatorische Maßnahmen zur Sicherheit personenbezogener Daten

Einige wichtige Begriffe im Datenschutz

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Diese Person ist im Datenschutz der **Betroffene**.

Eine **besondere Art personenbezogener Daten** sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschafts-zugehörigkeit, Gesundheit, Sexualleben sowie Biometrische und Genetische Daten. Solche Daten werden bei uns besonders stark geschützt.

Aufbau unseres Datenschutzkonzeptes

Das Datenschutzkonzept des Westfälischen Kinderdorf e. V. erfüllt den Sozialdatenschutz für Kinder als auch das Bundesdatenschutzgesetz Teil I und II (BDSG) und die Europäischen Datenschutzanforderungen (EU DS-GVO).
Im Schwerpunkt ist es auf folgende Gesetze und Verordnungen ausgerichtet:

- Sozialdatenschutz gem. §§ 67 ff. SGB X. Der Grundsatz des Sozialdatenschutzes (Sozialgeheimnis) ist in § 35 SGB I normiert. Für die öffentliche Kinder- und Jugendhilfe gelten darüber hinaus die spezifischen Bestimmungen der §§ 61-68 SGB VIII.
- Bei uns in Arbeit: Umsetzung der Europäische Datenschutzverordnung
- (EU DS-GVO vom 06.04.2016, veröffentlicht im Gesetzblatt der EU am 24.05.2016).
- Die EU DS-GVO tritt am 25.05.2018 in Kraft und ersetzt das gesamte bestehende Deutsche Datenschutzrecht.
- Der technische Datenschutz basiert auf den Grundlagen der DIN ISO/IEC 27001.

Neben diesen Gesetzen und Verordnungen kommen je nach Fall und Anforderung weitere gesetzliche Anforderungen hinzu, z.B. aus dem Steuerrecht (AO, GoBD), Medienrechtsrahmengesetz (MRRG), Telekommunikationsgesetz (TKG), Telemediengesetz (TMD) sowie Rechtsverordnungen aus dem Bundes-, Landesrecht.
Alle zwei Jahre wird ein Datenschutzbericht erstellt. Sollten durch den Datenschutzbeauftragten Mängel festgestellt werden, so werden diese der Geschäftsleitung unverzüglich mitgeteilt. Die Anweisung und Kontrolle der Mängelbeseitigung erfolgt durch die Geschäftsleitung des Westfälischen Kinderdorf e. V. in Zusammenarbeit mit dem Datenschutzbeauftragten.

Aufbau des Datenschutzkonzeptes

Der Datenschutz in des Westfälischen Kinderdorf e. V. basiert auf dem sogenannten **ROT** – Prinzip und hat damit drei tragende Säulen:

Rechtliche Voraussetzungen: Hier wird sichergestellt und geprüft, ob die Anforderungen der EU DS-GVO, des SGB und andere datenschutzrechtliche Anforderung eingehalten werden.

Organisation des Datenschutzes: Kein Schutz von personenbezogenen Daten ohne die richtige Organisation. Hier wird festgelegt, wie der Datenschutz einzuhalten ist und wie nach Vorschrift zu handeln ist. Personenbezogene Daten werden einer Risikoanalyse unterzogen und entsprechend den Risiken in unterschiedliche Sicherheitsstufen eingeteilt. Wie jeder Mitarbeitende mit personenbezogene Daten umzugehen hat wir in Verfahrensanweisungen gem. Art. 30 EU DS-GVO detailliert beschrieben.

Technische Sicherheit bei automatisierter Datenverarbeitung: Wie diese in des Westfälischen Kinderdorf e. V. sichergestellt ist und gelebt wird, ist in Dokumenten, wie die vorgegebenen „technisch organisatorischen Maßnahmen gem. Art. 32 EU GS-GVO und dem „IT-Sicherheitskonzept“, dokumentiert.

Aufbau des Datenschutzkonzeptes

Rechtliche Anforderungen und Voraussetzungen

Alle Vorgaben verschiedener datenschutzrechtlicher Gesetze müssen eingehalten werden, ohne das es hierbei Differenzen und Widersprüche gibt. Im Mittelpunkt steht derzeit hier des Sozialdatenschutz für Kinder.
Wir erfüllen die Anforderungen der „EU Datenschutzgrundverordnung (EU DS-GVO)“.
Wichtige rechtliche Grundsätze sind neben vielen anderen die:

- Verpflichtung aller Mitarbeiterinnen und Mitarbeiter auf das Datengeheimnis Art. 28 Abs. 3b EU DS-GVO).
- Kontrolle, wann Daten erhoben, gespeichert, verändert oder genutzt werden dürfen § 35 SBG I; § 62 SGB VIII; § 67a, 67b SGB X; Art. 5 und 6 EU DS-GVO).
- Einhaltung der unabdingbaren Rechte der Betroffenen (§§ 81, 83, 83a, 84, 84a SGB X; Art. 12ff EU DS-GVO).
- Einhaltung und Überwachung technischer und organisatorischer Maßnahmen zur IT-Sicherheit
- § 78a SGB X; Art. 24, 24, 32, 35, 36 EU DS-GVO).
- Übermittlungsgrundsätze §§64 SGB VIII; §§ 68-77 SGB X und Konkrete vertragliche Vorgaben und Kontrolle bei der Weitergabe an Dritte (Auftragsdatenverarbeitung Art. 28 EU DS-GVO).
- Bestellung eines zertifizierten Datenschutzbeauftragten zur Konzeptentwicklung, Beratung und Prüfung der Einhaltung aller Vorgaben § 38 BDSG, Art. 37 EU DS.GVO).
- Regelmäßige Schulung unserer Mitarbeiterinnen und Mitarbeiter zum Datenschutz und zur Informationssicherheit gem. Art. 32 EU DS-GVO).

Aufbau des Datenschutzkonzeptes

Organisatorische Anforderungen und Voraussetzungen

Alle gesetzlichen Vorgaben helfen nur dann, wenn es eine Organisation gibt die dafür Sorge trägt, dass alle datenschutzrechtlichen Anforderungen auch umgesetzt werden.
Hierzu gehören insbesondere:

- Wichtige Formulare um schnell und zielgerichtet handeln zu können (Formular über Datenauskunft an den Betroffenen, das öffentliche Verfahrensverzeichnis oder Formulare zur ordnungsgemäßen Datenvernichtung).
- Eine Reihe von Verfahrensanweisungen, wie Mitarbeiter/innen im Einzelfall vorzugehen haben (Beispiel: mit Personaldaten, mit Finanzdaten, Sozialdaten, Familienbetreuung, Wohngruppen, mit Word-Dokumenten, mit E-Mail usw.).
- Die Erfassung der Softwareapplikationen mit denen personenbezogene Daten verarbeitet werden, ihre Risikoeinschätzung und die Anweisung wie mit personenbezogenen Daten hier umzugehen ist (Applikationsverzeichnis).
- Die Dokumentation welche Rechte jede Mitarbeiterin und jeder Mitarbeiter an seinem Arbeitsplatz hat, z.B. darf er Daten nur ansehen, oder auch verändern, speichern oder löschen (Vertraulichkeit und Datenintegrität).
- Mitarbeiter und Mitarbeiterinnen dürfen nur die Daten erheben, verarbeiten und speichern, die sie zwingend zur Umsetzung Ihrer Aufgaben benötigen.

In diesem Umfeld gibt es ständige Herausforderungen und Beratungsbedarf, so dass die Verwaltungsprozesse nicht zum erliegen kommen, aber die datenschutzrechtlichen Voraussetzungen konsequent eingehalten werden.
Auch unterliegt der Datenschutz einem Qualitätsmanagement. In regelmäßigen Abständen werden in einzelnen Bereichen Audits durchgeführt um sicherzustellen, dass die datenschutzrechtliche Organisation einwandfrei und rechtskonform verläuft.

Aufbau des Datenschutzkonzeptes

Technische und organisatorische Anforderungen und Voraussetzungen

Bei den personenbezogenen Daten hat sich das Verhältnis zwischen Papierdokumenten und automatisiert erfassten Daten sehr stark zu Lasten der automatisiert erhobenen Daten verändert. Heute werden über 90% der datenschutzrelevanten Daten in Computersystemen und Datenbanken gespeichert. Daher ist die technische Prüfung der IT- und Datensicherheit sehr wichtig. Nirgendwo können Daten in großen Mengen schneller abhandenkommen als hier.
Demzufolge wird in der IT in des Westfälischen Kinderdorf e. V. sehr großen Wert auf IT-Sicherheit und Datenschutz gelegt. Die festgelegten Anforderungskriterien sind in § in der Anlage zu § 78a SGB X; Art. 32 EU DS-GVO festgeschrieben. Sie sind in einem IT-Konzept umgesetzt und werden durch Audits des Datenschutzbeauftragten ständig überwacht.
Auf den Datenträgern Endgeräte dürfen sich keine personenbezogenen Daten befinden. Sie liegen ausschließlich auf Servern in der Zentrale des Westfälischen Kinderdorf e. V.. Der Betrieb des Rechenzentrums erfolgt durch qualifizierte eigene IT-Mitarbeiter/innen. Der Zutritt zum Rechenzentrum ist streng geregelt und wird überwacht. Für Mitarbeiterinnen und Mitarbeiter gibt es feste Regeln für den Zugriff auf Daten. Hierzu gehören Anweisungen, wie die Passwörter zu erstellen sind, wie lang diese sein müssen und in welchen Abständen das Passwort zu erneuern ist. Namen und Geburtsdaten dürfen in Passwörtern nicht verwendet werden. Über eine Zugriffskontrolle werden Rechte vergeben, so dass jede Mitarbeiterin und jeder Mitarbeiter nur die Daten sehen darf, die zu ihrem oder seinem Aufgabengebiet gehören.
Auch Themen wie Datenverschlüsselung, Datensicherheit durch regelmäßige Datensicherung der Systeme, Notfall- und Brandschutzmaßnahmen gehören hier zum Aufgabengebiet der IT.
Mit dem Einzug neuer Technologien verändert sich auch hier permanent das Aufgabenspektrum, so wird durch die Einführung von Smart Phones und Tablet-PCs auch hier ein spezifiziertes Sicherheitskonzept notwendig, um den Datenschutz auch hier zu gewährleisten. Vor jeder Einführung neuer Technologien wird vom Datenschutzbeauftragten deren datenschutzrechtliche Relevanz geprüft, sicherheitskritische Bereiche dokumentiert und damit verbundene Risiken der Geschäftsführung mitgeteilt.

Verfahren

Applikations- und Anwenderverzeichnis

Zur Übersicht und Kontrolle wird ein Applikationsverzeichnis geführt.

1. Applikationsverzeichnis

Es enthält alle Informationen über eingesetzte Applikationen (Softwareanwendungen), die datenschutzrechtlich relevant sein können.

Es ist in 5 Abschnitte eingeteilt:

a. Applikationsbeschreibung (laufende Nummer, Applikationsname, Applikationsbeschreibung).
b. Betriebsdaten und Ansprechpartner.
c. Spezifische, datenschutzrelevante Informationen
d. (Anwendergruppe, welche Daten werden verarbeitet, Datenklassifikation, Schutzbedarf, Zugangsschutz, Verschlüsselung, Einverständniserklärung des Betroffenen, Vorabkontrolle, Verfahrensbeschreibung).
e. Sicherheitseinstufung (Vertraulichkeit, Integrität und Verfügbarkeit)
f. d. Zusätzliche Informationen zur Hardware und zu den Applikationen:

(Einsatz der Software auf RZ-Server, Server und Client, Kunden-Server, Lizenznummer, Anzahl der Lizenzen).

1. **Zugriffsreche von Mitarbeitenden**

Alle Zugriffberechtigungen und die Mandantentrennung werden über ein Aktive Directory umgesetzt.

Verfahren
Spezielle Verfahrensbereiche

Personenbezogene Daten in der Betreuung von Kindern: Der Umgang mit personenbezogenen Daten mit Kindern ist projektbezogen in verschiedenen Verfahren nach den Anforderungen des Art. 30 EU DS-GVO schriftlich festgelegt.
Personenbezogene Daten in Wohngruppen: Für den Umgang mit personenbezogene Daten in Wohngruppen gibt es ein festgelegtes schriftliches Verfahren nach den Anforderungen des Art. 30 EU DS-GVO.
Finanz- und Rechnungsdaten: Für den Umgang mit personenbezogene Daten Finanz- und Rechnungswesen gibt es ein festgelegtes schriftliches Verfahren nach den Anforderungen des Art. 30 EU DS-GVO..
Personalstammdaten: Organisatorische Verfahrensanweisungen, Erfassung der Applikationen und der Berechtigungen der Mitarbeiterinnen und Mitarbeiter, die mit personenbezogenen Daten arbeiten. Sensibilisierung für besonders schutzwürdige Daten im Personalwesen. Kontrolle der Clientarbeitsplätze durch Sichtung (Schreibtisch, Papierkorb, Bildschirmschoner mit Passwort, Festlegung der Passwortlänge und Art).
Internetnutzung: Private Internet- und E-Mail Nutzung ist verboten. Web-Filter, Regelungen und Vorgehensweise bei Verstößen durch Mitarbeiterinnen und Mitarbeiter. Regelungen zur sporadischen Kontrolle (TrafficLog). Kontrolle der Einhaltung der Löschungspflicht. Das interne Netz ist durch ein Firewallsysteme mit speziellen Sicherheitszonen (DMZ) vom Internet getrennt und somit vor Angriffen aus dem Internet nach Stand der Technik sicher.
Kommunikation (Telefonanlage, E-Mail): Datenschutzrechtliche Anforderungen im Umfeld der Kommunikation, insbesondere der IP-Telefonie. Telefongespräche sind nach dem SRTP Standard zu verschlüsseln. Gespräche auf Anrufbeantwortern sind zu verschlüsseln.

Verfahren

Auskunft an den Betroffenen gem. § 83 SGB X; § 34 BDSG; Art. 13f EU DS-GVO

Sobald ein Betroffener Auskunft über von ihm gespeicherte Daten verlangt, wird der Vorgang durch einen vom Datenschutzbeauftragten festgelegten Prozess und ein speziell dafür entwickeltes Formular standardmäßig behandelt.
Die Auskunft hat zeitnah (möglichst innerhalb von 7 Tagen) zu erfolgen.
Im Auskunftsprozess wird die Identität des Antragstellers überprüft :

- Persönlich bekannt
- Kopie des Personalausweises
- Im Onlineverfahren z. B. Geburtsdatum

Der Betroffene erhält:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Verfahren (Verzeichnis von Verarbeitungstätigkeiten)

Artikel 30 EU DS-GVO Verzeichnis von Verarbeitungstätigkeiten enthalten folgende Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Verfahren

Datenverarbeitung im Auftrag (ADV) gem. Art. 28 EU DS-GVO

Die Weitergabe von Sozialdaten ist nur in Rahmen des SGB möglich. In wenigen Ausnahmefällen können personenbezogene Daten an Dritte weitergegeben werden (z. B. Drucken von Einladungen, Digitalisierung von Papierunterlagen). Meist geschieht dies durch gesetzliche Vorgaben oder organisatorische Veränderungen, wenn z.B. die archivierten Papierakten durch eine Firma digitalisiert werden, um die Verwaltung effizienter zu gestalten. In solch einem Projekt müssen zwangsweise personenbezogene Daten an den Auftragnehmer übergeben werden. Damit hier alles korrekt verläuft, wird der Auftragnehmerin oder dem Auftragnehmer genau vorgeschrieben, wie sie oder er mit den Daten umzugehen hat und zuvor geprüft, ob sein Unternehmen die datenschutzrechtlichen Anforderungen voll erfüllt.
Der Vertrag, der die einzuhaltenden Vorgaben genau regelt, ist der Auftragsdatenverarbeitungsvertrag (ADV). Die Inhalte, die zu erfüllen sind, werden durch Art. 28 EU DS-GVO genau festgelegt. Es müssen 10 Punkte klar im Vertrag geregelt sein (siehe nächste Folie). Wichtige Punkte dabei sind die Kontrollpflichten des Westfälischen Kinderdorf e. V., ob die Daten vertragsgemäß verarbeitet werden, die Prüfung der Zuverlässigkeit des Auftragnehmers, die Gewährleistung, dass die Daten nur in Deutschland gespeichert werden dürfen, wie und wann die Daten zurückgegeben werden oder wie sie, wenn der Zweck entfällt, gesetzeskonform zu löschen sind. Die Weitergabe außerhalb des Vertragsverhältnisses ist ausgeschlossen.

Die Auftragsdatenverarbeitung ist in dem Westfälischen Kinderdorf e. V. nur in wenigen Ausnahmefällen erlaubt.

Verfahren

Datenverarbeitung im Auftrag (ADV) gem. Art. 28 EU DS-GVO

Werden Personenbezogen Daten zur Weiterverarbeitung an Dritte übergeben, wir hierzu ein Vertrag zur Auftragsdatenverarbeitung (ADV) geschlossen. Damit wird sichergestellt, dass mit den übergebenen Daten gesetzeskonform und NUR nach Weisung des Westfälischen Kinderdorf e. V. verfahren werden darf.
Jeder Vertrag zur Auftragsdatenverarbeitung regelt folgende Inhalte konkret:

a) Der Auftragsverarbeiter darf Ihre personenbezogenen Daten ausschließlich nur auf Weisung des Vereins Westfälisches Kinderdorf verarbeiten. Ihre personenbezogenen Daten bleiben Innerhalb der EU DS-GVO.
b) Wir gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
c) alle gemäß Artikel 32 erforderlichen Maßnahmen wurden von uns umgesetzt;
d) Weitere Auftragsverarbeiter dürfen nur mit unsrer ausdrücklichen Genehmigung eingesetzt werden;
e) personenbezogenen Daten werden einer Risikoanalyse unterzogen, ein Verzeichnisse von Verarbeitungstätigkeiten erstellt und entsprechend dem Risiko sicherheitstechnisch behandelt.
f) nach Abschluss der Erbringung der Verarbeitungsleistungen werden alle personenbezogenen Daten entweder löscht oder vom Auftragsverarbeiter zurückgegeben.
g) Eingesetzte Auftragsverarbeiter werden, in Bezug auf die Einhaltung der EU DS-GVO von uns vor Ort kontrolliert.

Verfahren

Einteilung personenbezogener Daten in verschiedene Datenschutzklassen.

Personenbezogene Daten werden in des Westfälischen Kinderdorf e. V. gem. den Anforderungen der EU DS-GVO auf Basis der DIN ISO/IEC 27001 eingestuft. Sie reichen von öffentlichen Daten bis hin zu streng vertraulichen Daten und orientieren sich an den Voraussetzungen der DIN ISO/IEC 27001 und den Anforderungen des Art. 32 EU DS-GVO. In einem festgelegten Prozess werden alle personenbezogenen Daten Schutzklassen zugeordnet.

Schutzklasse 3 – **:**
z. B. alle besondere Arten von personenbezogenen Daten gem. Art. 9 EU DS-GVO.

Schutzklasse 2 –vertraulich
Da es nur wenige als vertraulich eingestufte Daten in des Westfälischen Kinderdorf e. V. gibt, werden diese der Schutzklasse 3 zugeordnet, z.B. Bewerbungen, Zeugnisse, Bankdaten etc.

Schutzklasse 1 – intern
z.B. Alle Unternehmensdaten und personenbezogenen Daten die nicht streng vertraulich oder öffentlich sind.

Schutzklasse 0 – öffentlich
z.B. frei im Internet verfügbare Daten, Daten aus Adress- und Telefonbüchern, Dokumente die als öffentlich gekennzeichnet sind (Broschüren, Informationsmaterial etc.)
Eine genaue und abschließende Beschreibung der Zuordnung einzelner Datenkategorien ist in einem Schutzklassenverzeichnis enthalten, welches allen Mitarbeitern zur Einsichtnahme und als Arbeitshilfe zur Verfügung steht.

Verfahren

Technische & organisatorische Maßnahmen (TOM), gem. Art. 32 EU DS-GVO Seite 1

Die technischen & organisatorischen Maßnahmen sind in einem gesonderten Dokument beschrieben und umfassen folgende Punkte:

- Einhaltung gesetzlicher Vorgaben
- Zutrittskontrolle
- Eingabekontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabe-, Übertragungskontrolle
- Mandantentrennung
- Risikobewertung
- Sicherheit der Verarbeitung

Verfahren

Datenschutzverpflichtung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter

Alle Mitarbeiterinnen und Mitarbeiter des Westfälischen Kinderdorf e. V. sind auf das Datengeheimnis verpflichtet.
Diese Verpflichtung erfolgt Art. 28 Abs. 3b EU DS-GVO.
Um die Akzeptanz für den Datenschutz zu erhöhen und die Umsetzung der erforderlichen Maßnahmen zum Datenschutz zu gewährleisten, werden alle Mitarbeiterinnen und Mitarbeiter regelmäßig in einer Schulung auf den Umgang mit personenbezogenen Daten im Sinne der EU DS-GVO sensibilisiert.
In den Schulungen werden datenschutzrechtliche Grundlagen, neue gesetzliche Anforderungen und der Sichere Umgang mit Informationstechnologie (Informationssicherheit) vermittelt.
Mitarbeiterinnen und Mitarbeiter, die mit streng vertraulichen Daten in Berührung kommen, erhalten speziell darauf abgestimmte Schulungen.
Alle zwei Jahre werden die Mitarbeiter zum Thema Informationssicherheit und Datenschutz geschult. Die letzte Schulung ist im März 2018 erfolgt.

Verfahren

Kontrolle und Audits

Der Datenschutzbeauftragte (DSB) kontrolliert regelmäßig alle Einrichtungen des Westfälischen Kinderdorf e. V., in denen personenbezogene Daten verarbeitet werden und überprüft die Einhaltung der Datenschutzrichtlinien.
Dazu gehört die Prüfung der Arbeitsplätze, die Einhaltung der Verfahrensbeschreibungen, die Einhaltung der technischen und organisatorischen Maßnahmen im Rechenzentrum.
Mängel werden direkt vor Ort den Mitarbeiterinnen und Mitarbeitern mitgeteilt und Wege aufgezeigt, wie datenschutzkonform gearbeitet werden kann.
Ziel ist nicht, die Mitarbeiterinnen und Mitarbeiter zu sanktionieren, sondern sie für ein datenschutzkonformes Arbeiten zu motivieren.
Werden dem Datenschutzbeauftragten Schwachstellen oder Verletzungen des Datenschutzes gemeldet, geht er diesen unverzüglich nach und prüft ob Mängel vorliegen.
Alle erkannten Mängel werden der Verwaltungsleitung unverzüglich gemeldet und Maßnahmen getroffen, um die Mängel unverzüglich zu beseitigen.
In einem jährlichen **Datenschutzbericht** wird der Status der Datenschutzumsetzung dokumentiert und gegebenenfalls werden weitere Maßnahmen zur Verbesserung des Datenschutzes aufgezeigt.

Historie:

Version:	Stand:	Erstellt durch:
Version 1.0 – Datenschutzkonzept-WEKIDA V1.0.pptx	Erstellt am 11.10.2017	Dirk Fromm
Version 1.1 - WEKIDO-Datenschutzkonzept 17.04.2018	Erstellt am 17.04.2018	Dirk Fromm