ARBEITERWOHLFAHRT
Kreisverband Bielefeld e.V.

Datenschutzmanagementsystem DSMS 4.0.1
Kontaktdaten Datenschutzbeauftragte*r

Wir haben

Herrn Uwe Müller

als

Externen Datenschutzbeauftragten

bestellt.

Herr Müller steht allen Mitarbeiter*innen, Kund*innen und Partner*innen bei Fragen und Anliegen zum Datenschutz zur Verfügung.

EDV-Service Müller
Artur-Ladebeck-Str. 125, 33647 Bielefeld
Telefon: 0521 206872
E-Mail: datenschutz@awo-bielefeld.de

Bitte versenden Sie per E-Mail keine personenbezogenen oder betriebsinternen Daten an den Datenschutzbeauftragten. Nutzen Sie die E-Mail, um Ihre Rückrufnummer und Ihr Anliegen in wenigen Schlagworten zu übermitteln. Bitte vermerken Sie in Ihrer Nachricht, ob Sie eine Antwort per E-Mail wünschen.

Datenschutzmanagementsystem DSMS 4.0.2
Selbstverpflichtung zum Datenschutz

Stand 25.05.2018

Selbstverpflichtung zum Datenschutz

Der Datenschutz und die Vertraulichkeit der uns anvertrauten Informationen haben für uns einen hohen Stellenwert. Wir verarbeiten Ihre Daten nach den Vorgaben der EU-Datenschutzgrundverordnung und der jeweils geltenden Gesetze.

Verstöße gegen die Selbstverpflichtung

- Wir möchten über rechtswidriges Verhalten im AWO Kreisverband Bielefeld e.V. informiert werden, um solche Verhaltensweisen aufklären und abstellen zu können.
- Daher ermutigen wir Sie – egal ob (ehemalige) Mitarbeiter*innen, Kund*innen, Lieferanten oder Dritte – uns Hinweise auf Rechtsverstöße mitzuteilen.
- Ebenso können Sie sich auch unmittelbar an den/die Datenschutzbeauftragte/n wenden (Kontaktdaten: siehe Aushang).
- Allen Hinweisgeber*innen sichern wir Vertraulichkeit zu.

Bielefeld, 25.05.2018

AWO Kreisverband Bielefeld e.V.

K. Hopster

Kirsten Hopster | Markus Wrobbel

Kreisvorstand

Datenschutzmanagementsystem DSMS 4.0.3
Unternehmensrichtlinie zum Datenschutz

Stand 25.05.2018

---

§ 1 Bedeutung, Ziel

1. Diese Unternehmensrichtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten im AWO Kreisverband Bielefeld e.V. (im Folgenden AWO).
2. Mit dieser Unternehmensrichtlinie sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden.

§ 2 Geltungsbereich und gesetzliche Grundlage

1. Diese Richtlinie findet Geltung für alle Einrichtungen des AWO Kreisverbands Bielefeld e.V. sowie alle Unternehmen, an denen die AWO eine Beteiligung von mindestens 50 % mittelbar oder unmittelbar hält oder deren wirtschaftliche Führung sie innehat. Sie gilt jedoch nur, wenn der Sitz oder eine Niederlassung des auftraggebenden Unternehmens in Deutschland ist.
2. Sie gilt persönlich für alle Beschäftigten sowie leitenden Angestellten der AWO.
3. Die Gebote und Verbote dieser Unternehmensrichtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig, ob dieser elektronisch oder in Papierform vonstattengeht. Ebenso beziehen sie alle Arten von Betroffenen (Kunden, Beschäftigte, Lieferanten etc.) in ihren Geltungsbereich ein.
4. Gesetzliche Grundlage dieses Dokumentes ist die EU-Datenschutz-Grundverordnung (EU-DSGVO).

§ 3 Begriffsbestimmungen

1. Es gelten hierbei die jeweiligen Begriffsbestimmungen aus Art. 4 EU-DSGVO.

§ 4 Datenschutzorganisation

1. Die AWO hat eine*n Datenschutzbeauftragte*n nach Maßgabe des in §2 genannten Datenschutzgesetzes (Art. 37 EU DSGVO und § 5 Bundesdatenschutzgesetz (neu)) bestellt. Diese*r ist erreichbar unter den im Aushang bekannt gegebenen Kontaktdaten.
2. Der/die Datenschutzbeauftragte überwacht und gewährleistet die Einhaltung der gesetzlichen Vorgaben sowie die Vorgaben dieser Richtlinie. Der/die Datenschutzbeauftragte berät den Vorstand zu Fragen des Datenschutzes, ist zuständig bei der Kommunikation mit Betroffenen und Aufsichtsbehörden und berichtet regelmäßig dem Vorstand über die Umsetzung des Datenschutzes im Unternehmen. Ausgewählte Prozesse werden stichprobenartig und in angemessenen Zeitabständen durch ihn/sie auf ihre Datenschutzkonformität hin kontrolliert.
3. Der/Die Datenschutzbeauftragte nimmt seine/ihre Aufgaben weisungsfrei und unter Anwendung seiner/ihrer Fachkunde wahr. Er/Sie ist dem Vorstand unmittelbar unterstellt.
4. Die AWO bzw. ihre Mitarbeiter*innen haben den/die Datenschutzbeauftragte*n bei der Erfüllung seiner/ihrer Aufgaben zu unterstützen.
5. Der/Die Datenschutzbeauftragte fertigt mindestens jährlich einen Bericht an, den er/sie dem Vorstand zur Verfügung stellt.

§ 5 Umgang mit personenbezogenen Daten

1. Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit den Datenumgang.
2. Die AWO hat hierzu Verfahren in Kraft gesetzt, die anhand dieser Anforderung gestaltet sind.

2.1 Personenbezogene Daten dürfen nach dem in §2 genannten Gesetz grundsätzlich erhoben, verarbeitet oder genutzt werden:

- bei einem bestehenden Vertragsverhältnis mit dem/der Betroffenen;
- im Zuge der Vertragsanbahnung oder -abwicklung mit dem/der Betroffenen;
- wenn und soweit der/die Betroffene eingewilligt hat;
- wenn eine spezielle Rechtsvorschrift außerhalb der in §2 genannten gesetzlichen Regelung die Verarbeitung erfordert.

2.2 Personenbezogene Daten sind für einen zuvor festgelegten Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit dem ursprünglich festgelegten Zweck vereinbar ist. Eine Datenhaltung ohne Zweck, so beispielsweise die Vorratsdatenspeicherung, ist unzulässig.

2.3 Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist ebenfalls nur mit einer gesetzlichen Erlaubnisnorm oder der Einwilligung des/der Betroffenen zulässig.

2.4 Personenbezogene Daten sollen grundsätzlich direkt beim Betroffenen erhoben werden. Eine Erhebung aus anderen Quellen (Internet, Warndienste, Auskunfteien) ist ohne ein zwingendes gesetzliches Erfordernis unzulässig. Besteht ein gesetzliches Erfordernis, ist der/die Betroffene unverzüglich über die Datenerhebung zu informieren, soweit eine gesetzliche Regelung dem nicht entgegensteht.

2.5 Der/Die Betroffene ist bei der Erhebung seiner/ihrer personenbezogenen Daten über die Zweckbestimmung, die Identität der verantwortlichen Stelle sowie die Empfänger seiner/ihrer personenbezogenen Daten zu informieren.

2.6 Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Der Umfang der Datenverarbeitung muss hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

2.7 Falls möglich, wird auf einen personenbezogenen Datenumgang verzichtet. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen.

§ 6 Besondere Kategorien personenbezogener Daten

1. Besondere personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des/der Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis bzw. Verpflichtung erhoben, verarbeitet oder genutzt werden.
2. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z.B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

§ 7 Datenübermittlung/Datenweitergabe

1. Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis bzw. Verpflichtung oder der Einwilligung des/der Betroffenen zulässig.
2. Befindet sich der/die Empfänger*in personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

§ 8 Externe Dienstleister

1. Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der/die Datenschutzbeauftragte vorab zu informieren.
2. Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und berücksichtigt insbesondere die folgenden Aspekte:

2.1 Personenbezogene Daten sind für einen zuvor festgelegten Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit dem ursprünglich festgelegten Zweck vereinbar ist. Eine Datenhaltung ohne Zweck, so beispielsweise die Vorratsdatenspeicherung, ist unzulässig.

2.2 Technisch-organisatorische Sicherheitsmaßnahmen

2.3 Erfahrung der Anbieter am Markt

2.4 Sonstige Aspekte, die auf eine Zuverlässigkeit der Anbieter schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

3. Sollen Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.
4. Die Dienstleister sind im Hinblick auf die mit ihnen vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

§ 9 Datenvermeidung, Datenminimierung, Privacy by design, Privacy by default

1. Der Umgang mit personenbezogenen Daten wird an dem Ziel ausgerichtet, so wenige Daten wie möglich von einem/r Betroffenen zu erheben, zu verarbeiten oder zu nutzen. Insbesondere werden personenbezogene Daten anonymisiert oder pseudonymisiert, soweit dies nach dem Verwendungszweck möglich ist (Privacy by default)
2. Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz wird in die Spezifikationen und die Architektur von Datenverarbeitungssystemen integriert, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern (Privacy by design).

§ 10 Rechte von Betroffenen

1. Betroffene haben das Recht auf Auskunft über die in der AWO über ihre Person gespeicherten personenbezogenen Daten.
2. Die Auskunftserteilung erfolgt auf schriftlichem Weg und beinhaltet neben den zur Person vorhandenen Daten auch die Empfänger von Daten sowie den Zweck der Speicherung.
3. Der/Die Datenschutzbeauftragte steht bei der Bearbeitung von Auskunftsbegehren beratend zur Verfügung.
4. Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen.
5. Personenbezogene Daten sind unter den folgenden Voraussetzungen zu löschen:

5.1 Ihre Speicherung ist unzulässig, oder

5.1.1 es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder

5.1.2 die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich.

5.2 An die Stelle einer Löschung kann eine Sperrung von Daten treten, wenn

5.2.1 eine Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung zwar nicht mehr erforderlich ist, jedoch gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, oder

5.2.2 schutzwürdige Interessen der Betroffenen beeinträchtigt würden, oder

5.2.3 eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

6. Widerspricht der/die Betroffene der Verarbeitung oder Nutzung seiner/ihrer Daten für Zwecke der Werbung (vgl. § 13 und Art. 21 EU-DSGVO), ist eine weitere Verarbeitung oder Nutzung für diese Zwecke unzulässig.

§ 11 Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Kunden oder Beschäftigte der AWO, ist eine Weitergabe von Informationen nur zulässig, wenn

- die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und
- eine gesetzliche Norm zur Auskunft verpflichtet, sowie
- die Identität des/der Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

§ 12 Verfahrensmeldung, Verzeichnis von Verarbeitungstätigkeiten

1. Dem/Der Datenschutzbeauftragten sind vor Einführung einer Verarbeitungstätigkeit, das den Umgang mit personenbezogenen Daten zum Inhalt hat, durch die jeweils fachlich verantwortliche Person alle notwendigen Informationen zur Ausgestaltung dieser Verarbeitung zur Verfügung zu stellen.
2. Sofern hier besondere Kategorien personenbezogener Daten verarbeitet werden sollen, muss die jeweils fachlich verantwortliche Person mit Unterstützung der/des Datenschutzbeauftragten eine vorherige Kontrolle und die Datenschutzfolgeabschätzung durchführen und dokumentieren.
3. Der/Die Datenschutzbeauftragte führt eine Übersicht über die von den jeweils fachlich verantwortlichen Personen gemeldete Verarbeitungstätigkeit zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten (Verzeichnis von Verarbeitungstätigkeiten).
4. Die Verantwortung für die Richtigkeit des Verzeichnisses von Verarbeitungstätigkeiten obliegt den jeweils fachlich verantwortlichen Personen.

§ 13 Werbung

1. Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax oder E-Mail ist grundsätzlich nur zulässig, wenn der/die Betroffene zuvor in die Verwendung seiner/ihrer Daten zu Werbezwecken eingewilligt hat.
2. Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm (z.B. per Gesetz) zulässig.

§ 14 Schulung

1. Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, werden in geeigneter Weise über die datenschutzrechtlichen Vorgaben geschult.

§ 15 Datengeheimnis

1. Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie werden vor Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet. Die Verpflichtung erfolgt durch den Vorstand unter Verwendung des hierzu vorgesehenen Formulars.
2. Mitarbeiter*innen mit besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis nach §88 TKG) werden vom Vorstand ergänzend darauf schriftlich verpflichtet.

§ 16 Beschwerden

1. Jede/r Betroffene hat das Recht, sich über eine Verarbeitung seiner/ihrer Daten zu beschweren, sollte er/sie sich hierdurch in seinen/ihren Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Unternehmensrichtlinie jederzeit anzeigen.
2. Die zuständige Stelle für die oben genannten Beschwerden ist der/die Datenschutzbeauftragte als interne unabhängige und weisungsfreie Instanz.

§ 17 Audits

1. Um ein hohes Datenschutzniveau zu gewährleisten, werden relevante Prozesse durch regelmäßige Audits interner Stellen oder durch externe Auditoren überprüft. Im Falle der Feststellung eines Verbesserungspotentials werden unmittelbare Abhilfemaßnahmen getroffen.
2. Die beim Audit gewonnenen Erkenntnisse werden dokumentiert. Die Dokumentation wird dem/der Datenschutzbeauftragten, dem Vorstand, dem/r Qualitätsmanagementbeauftragten QMB sowie den Fachverantwortlichen für den jeweiligen Prozess übergeben.

§ 18 Interne Ermittlungen

1. Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis werden unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchgeführt. Insbesondere müssen die dabei erhobenen und verwendeten Daten zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen der Betroffenen verhältnismäßig sein.
2. Der/Die Betroffene wird so bald wie möglich über die zu seiner/ihrer Person durchgeführten Maßnahmen informiert.
3. Bei allen Formen der internen Ermittlungen wird der/die Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einbezogen.

§ 19 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

1. In Abhängigkeit der Art der Daten und deren Schutzbedürftigkeit erfolgt für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Risikoanalyse. Dies gilt insbesondere für besondere personenbezogene Daten.
2. Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept erstellt, das für alle Verfahren verbindlich ist. Hierin sind insbesondere Mittel und Maßnahmen zur Verschlüsselung und Datensicherung vorgesehen.
3. Es wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume werden verschlossen. Wirksame Maßnahmen zur Zugangskontrolle an Geräten sind vorhanden und aktiviert. Systemzugänge werden in Abwesenheit stets gesperrt.
4. Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es wird sichergestellt, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen eine minimale Länge von 8 Zeichen aufweisen und aus einem Zeichenmix bestehen. Passwörter dürfen nicht in einem Wörterbuch vorkommen oder aus leicht zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit der AWO stehen.
5. Zugriffe auf personenbezogene Daten erhalten nur diejenigen Personen, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen. Zugriffsberechtigungen werden genau und vollständig festgelegt und dokumentiert.
6. Datenübertragungen durch öffentliche Netze werden nach Möglichkeit verschlüsselt. Eine Verschlüsselung erfolgt zwingend, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.
7. Zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden getrennt voneinander verarbeitet. Die Trennung von Daten wird durch geeignete technische und organisatorische Maßnahmen sichergestellt.
8. Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister werden beaufsichtigt. Ferner wird gewährleistet, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge werden nur im Einzelfall gewährt und folgen dem Prinzip der minimalen

Rechtevergabe. Fernwartungsaktivitäten werden nach Möglichkeit aufgezeichnet oder protokolliert.

§ 20 Unrechtmäßige Kenntniserlangung von Daten

1. Sollten Daten unrechtmäßig Dritten offenbart worden sein, wird darüber unverzüglich der/die Datenschutzbeauftragte informiert.
2. Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.
3. Die Erfüllung einer etwaigen Informationspflicht gegenüber Betroffenen oder Aufsichtsbehörden erfolgt durch den/die Datenschutzbeauftragte*n (72-Stunden-Regelung).

§ 21 Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

§ 22 Aktualisierung dieser Richtlinie

1. Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.
2. Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten werden umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis gesetzt.