Datenschutzrichtlinie

DRK Kreisverband Rostock e.V.

Inhaltsverzeichnis

Präambel

Der Schutz der personenbezogenen Daten der Mitarbeiter und Kunden des DRK Kreisverband Rostock e.V. und der mit ihm verbundenen Unternehmen (nachstehend DRK Rostock genannt) unterliegt der höchsten Priorität. Das vorliegende Konzept beschreibt, wie Datenschutz beim DRK Rostock berücksichtigt, umgesetzt und gelebt wird. Es wird für die Datenverarbeitung nach folgender Datenschutzrichtlinie verfahren.

Die Verarbeitung personenbezogener Daten soll unter Berücksichtigung

- der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
- der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
- der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung)

gewährleistet werden. Die Sicherheitsmaßnahmen werden in der Datenschutzrichtlinie in die Bereiche

- Allgemeine Datenverarbeitung
- Automatisierte Datenverarbeitung
- Nutzung der Internetdienste
- Nutzung der Telekommunikationsdienste und
- Zusatzmaßnahmen für sensible personenbezogene Daten

gegliedert und geben mithin ein hohes Sicherheitsniveau vor.

1. Bedeutung, Ziel, Zugänglichkeit, Inhalt und Zweck

Diese Richtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten beim DRK Rostock.

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

Mit ihr sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden.

Diese Richtlinie muss für alle Beschäftigten und Mitarbeiter jederzeit leicht zugänglich sein.

2. Geltungsbereich

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten beim DRK Rostock. Die festgelegten Sicherheitsmaßnahmen gelten als Mindestanforderungen für den DRK Kreisverband Rostock e.V.

Alle Mitarbeiter sind zur Einhaltung dieser Richtlinie verpflichtet.

Sie richtet sich ebenfalls an:

- DRK Rostock gGmbH für Menschen in Not
- DRK Rostocker Kinder- und Jugendhilfe gGmbH
- Rostocker DRK Werkstätten gGmbH
- DRK Rostock Wohnen und Pflege gGmbH

Die Gebote und Verbote dieser Richtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform vonstattengeht. Ebenso beziehen sie alle Arten von betroffenen (Mitglieder, Kunden, Beschäftigte, Mitarbeiter, Lieferanten etc.) in ihren Geltungsbereich ein.

3. Begriffsdefinitionen

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener). Beispiele: Name, Vorname, Geburtstag, Adressdaten, Bestelldaten, E-Mail-Inhalte.

Besondere Arten personenbezogener Daten sind Angaben über rassische, ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetische Daten, biometrische Daten

Verantwortliche Stelle ist juristische Person innerhalb des DRK Rostock, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Erheben ist das Beschaffen von Daten über den Betroffenen.

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von personenbezogenen Daten.

Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem verhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des betroffenen auszuschließen oder wesentlich zu erschweren.

Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle

Auftragsdatenverarbeitung ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch einen Auftragnehmer für einen Auftraggeber. Der Auftragnehmer darf personenbezogene Daten nur nach Weisung des Auftraggebers erheben, verarbeiten oder nutzen. Die Verantwortung für den Datenumgang verbleibt beim Auftraggeber als verantwortliche Stelle.

4. Der betriebliche Datenschutzbeauftragte

Der DRK Kreisverband Rostock e.V. und seine mit ihm verbundenen Unternehmen haben nach Maßgabe des Art. 37 EU-DSGVO und § 5 BDSG (neu) einen betrieblichen Datenschutzbeauftragten (bDSB) bestellt.

Es handelt sich um:

Ziar Kabir
SCO-CON:SULT GmbH
Hauptstraße 27
50634 Bad-Honnef

Dieser nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung der Fachkunde wahr.

Dem betrieblichen Datenschutzbeauftragten wird von DRK Rostock ein Datenschutzkoordinator als Erfüllungsgehilfe zur Seite gestellt. Dieser unterstützt den betrieblichen Datenschutzbeauftragten.

Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden ist allein der bDSB zuständig. Die Fachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen.

Jeder Mitarbeiter des DRK Kreisverband Rostock e.V. und seine mit ihm verbundenen Unternehmen kann sich unmittelbar mit Hinweisen, Anregungen oder

Beschwerden an den bDSB oder dessen Erfüllungsgehilfen wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

5. Umgang mit personenbezogenen Daten

Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn eine Rechtsgrundlage für die Datenverarbeitung vorliegt, insbesondere eine Einwilligung der betroffenen Person nach Art. 6 Abs. 1a i. V. m. Art. 7 f. DSGVO oder eine Rechtsgrundlage nach Art. 6 Abs. 1b DSGVO.

6. Besondere personenbezogene Daten

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

7. Datenübermittlung/Datenweitergabe

Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig. Befindet sich der Empfänger 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

Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte vorab zu informieren.

Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen.

Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsdatenverarbeitung. Hierin sind Datenschutz- und Datensicherheitsaspekte zu regeln.

Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen.

9. Datenvermeidung, Datensparsamkeit

Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist.

10. Rechte von Betroffenen

Unter den Rechten der betroffenen Person sind die Rechte jedes Einzelnen gegenüber den für die Verarbeitung Verantwortlichen gemeint.

Insbesondere sind dies folgende

Informationsrecht
Die Informationspflicht ist wichtiger Bestandteil zur Wahrung der informellen Selbstbestimmung. Die genauen Informationspflichten werden im Art. 13 und Art. 14 DSGVO geregelt.

Auskunftsrecht der betroffenen Person
Die betroffene Person hat das Recht zu erfahren, ob von ihr personenbezogene Daten verarbeitet werden. Ist dies der Fall, hat Sie das Recht auf Auskunft über diese Daten und auf die im Art. 15 Abs. 1 näher beschriebenen Informationen. Dieses Recht kann schriftlich oder elektronisch wahrgenommen werden und die Antwort muss innerhalb eines Monats erfolgen. Erfolgte das Auskunftsersuchen elektronisch, so ist es auch elektronisch zu beantworten.

Recht auf Berichtigung
Resultiert eine Datenverarbeitung in unrichtigen personenbezogen Daten des Betroffenen, so hat dieser ein Recht auf unverzügliche Berichtigung (Art. 16 DSGVO). Dabei ist jedoch der Zweck der Verarbeitung zu berücksichtigen, sodass etwa bei Datenverarbeitungen im öffentlichen Interesse eine längere Zeitspanne bis zur Berichtigung angesetzt werden kann.

Recht auf Löschung
Die betroffene Person hat das Recht, vom Verantwortlichen zu verlangen, das die betreffenden personenbezogenen Daten gelöscht werden, sofern die unter Art. 17 Abs. 1 DSGVO genannten Gründe zutreffen.
Eine Löschung scheidet aus, sofern gesetzliche Aufbewahrungsfristen bestehen.

Das Recht auf Einschränkung der Verarbeitung
Der Betroffene hat ein Recht auf Einschränkung der Verarbeitung, wenn einer der Gründe gemäß Art. 18 Abs.1 vorliegen.

Daraus ergibt sich eine doppelte Mitteilungspflicht. Es sind die Empfänger der personenbezogenen Daten darüber zu informieren, dass der Betroffene von seinen Rechten nach Art. 16 – 18 DSGVO Gebrauch gemacht hat. Der Betroffene ist bei verlangen über die entsprechenden Empfänger aufzuklären.

Recht auf Datenübertragbarkeit
Eine betroffene Person hat das Recht, seine dem DRK Kreisverband Rostock e.V. oder einer seiner ihm angegliederten Tochtergesellschaften zur Verarbeitung überlassenen Daten ohne Behinderung durch den dafür Verantwortlichen an einen anderen für die Verarbeitung Verantwortlichen zu übermitteln.

11. Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Mitarbeiter oder Beschäftigte des DRK Kreisverband Rostock e.V., 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 Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

12. Verfahrensverzeichnis

Die eingesetzten Verfahren sind in eine Bestandsliste aufzunehmen.

Jedes eingesetzte Verfahren ist zu dokumentieren. Dazu sind im DRK Kreisverband Rostock e.V. und dessen Tochtergesellschaften Verzeichnisse aller Verarbeitungstätigkeiten zu führen, die ihrer Zuständigkeit unterliegen.

Dieses Verzeichnis enthält sämtliche folgenden Angaben:

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

b) die Zwecke der Verarbeitung

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

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

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

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

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

Die Rechte für den Zugriff auf die Verfahren sind von den jeweiligen Geschäftsführern zu regeln. Sie sind innerhalb der Verfahren auf das notwendige Maß zu beschränken und zu dokumentieren.

Die Rechteverwaltung ist durch die IT-Abteilung umzusetzen.

13. Auftragsdatenverarbeitung

Wenn der DRK Kreisverband Rostock e.V. oder eine der ihm angeschlossenen Tochtergesellschaften externe Dritte mit der Verarbeitung von Daten beauftragt, so

liegt in der Regel eine Auftragsdatenverarbeitung vor und es wird ein Vertrag für die Auftragsdatenverarbeitung gemäß Art. 28 Abs. 3 DSGVO vereinbart.

Die datenschutzrechtliche Verantwortung für die Verarbeitung und Nutzung der personenbezogenen Daten verbleibt beim DRK Kreisverband Rostock e.V..

Die für die Auftragsdatenverarbeitung verantwortliche Stelle muss mit dem Auftragnehmer die technischen und organisatorischen Maßnahmen zur Datensicherung und zur Gewährleistung der Vertraulichkeit in einem Vertrag schriftlich vereinbart werden.

14. Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz

Der DRK Kreisverband Rostock e.V. und seine ihm angeschlossenen Tochtergesellschaften treffen zum Schutz der von ihm verarbeitenden personenbezogenen Daten geeignete technische und organisatorische Maßnahmen und weist diese nach.

Dies sind insbesondere:

1. Pseudonymisierung

2. Verschlüsselung

3. Gewährleistung der Vertraulichkeit

4. Gewährleistung der Integrität

5. Gewährleistung der Verfügbarkeit

6. Gewährleistung der Belastbarkeit der Systeme

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

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

a. Zutrittskontrolle

Ist die physische Erreichbarkeit von Servern und Clients, insbesondere die Möglichkeit, Gebäude des DRK Kreisverband Rostock e.V. und der ihm angeschlossenen Tochtergesellschaften körperlich zu betreten.

b. Zugangskontrolle

Hiermit wird die Möglichkeit der Nutzung der informationstechnischen Systeme gemeint. In der Regel bezeichnet es die Möglichkeit der Anmeldung an die IT-Systeme.

c. Zugriffskontrolle

Dieser Begriff bezeichnet die Möglichkeit, auf konkrete Inhalte (Dateien, Ordner usw.) zugreifen zu können, also die dafür nötigen Berechtigungen zu besitzen.

d. Weitergabekontrolle

Hiermit ist die Übertragung von Daten an Empfänger gemeint. Diese hat gesichert und nachvollziehbar zu erfolgen.

e. Eingabekontrolle

Unter Eingangskontrolle ist gemeint, ob und von wem Daten erfasst, verändert und entfernt wurden.

f. Auftragskontrolle

Diese Kontrolle gewährleistet, dass die Verarbeitung von Daten im Auftrag durch Dritte, gemäß den Weisungen im Rahmen des dafür erteilten Auftrages erfolgen.

g. Verfügbarkeitskontrolle

Hierbei spricht man von der Vermeidung der Zerstörung und des Verlustes von personenbezogenen Daten.

h. Trennungsgebot

Bezeichnet die Beachtung der Zweckbindung, dass heißt die Einschränkung der Datennutzung auf den Zweck, zu dem sie erhoben wurden.

15. Verfahren zur Pseudonymisierung und Anonymisierung

Die Verfahren zur Pseudonymisierung und Anonymisierung werden nach dem jeweils aktuellen Stand der Technik durchgeführt.

16. Werbung

Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.

Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig.

17. Schulung

Beschäftigte, Mitarbeiter und ehrenamtlich Aktive, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben, verarbeiten oder nutzen, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Der Datenschutzbeauftragte entscheidet über Form und Turnus der entsprechenden Schulungen. Die Teilnahme und Durchführung dieser Schulungen ist zu dokumentieren.

18. Datengeheimnis

Die Mitarbeiter des DRK Kreisverband Rostock und der ihm angegliederten Tochtergesellschaften müssen sich ihrer Verantwortung beim Umgang mit personenbezogenen Daten bewusst sein.

Art. 5 DSGVO schreibt vor, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die Person nachvollziehbaren Weise verarbeitet werden müssen. Des Weiteren legt Art. 5 DSGVO dem Verantwortlichen die Pflicht auf, die Einhaltung dieser Vorgabe nachweisen zu können (sog. Rechenschaftspflicht). Darauf aufbauend wird jeder Mitarbeiter des DRK Kreisverband Rostock e.V. und seine ihm angegliederten Tochtergesellschaften schriftlich auf die Vertraulichkeit gemäß § 53 BDSG (neu) verpflichtet.

Die Verpflichtung erfolgt durch die Personalabteilung unter Verwendung des hierzu vorgesehenen Formulars.

19. Beschwerden

Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Unternehmensrichtlinie jederzeit anzeigen.

Die zuständige Stelle für die oben genannten Beschwerden ist der Datenschutzkoordinator als interne unabhängige und weisungsfreie Instanz.

20. Verfügbarkeit, Vertraulichkeit und Integrität von Daten

Verfügbarkeit, Vertraulichkeit und Integrität sind Schutzziele der Datensicherheit. Ihr Ziel ist es, die Systeme vor Gefahr bzw. Bedrohungen zu schützen, Schaden zu vermeiden und Risiken zu minimieren. Die Umsetzung dieser Ziele hat durch gezielten Einsatz von technischen und organisatorischen Maßnahmen zu erfolgen.

21. Unrechtmäßige Kenntniserlangung von Daten („Datenpanne“)

Sollten personenbezogene Daten unrechtmäßig offenbart worden sein, ist darüber unverzüglich der Datenschutzbeauftragte zu informieren. Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangene Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten. Die Erfüllung einer etwaigen Informationspflicht gegenüber Betroffenen oder Aufsichtsbehörden erfolgt ausschließlich durch den Datenschutzbeauftragten.

22. Folge 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.

23. Aktualisierung der Richtlinie

Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin geprüft.

Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und Mitarbeiter sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.