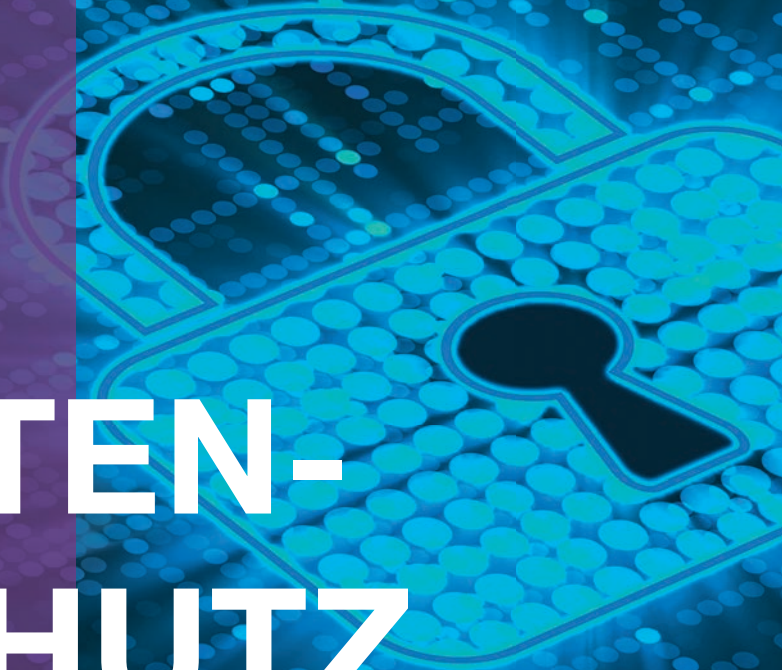


DATEN- SCHUTZ



Broschüre für Mitarbeiter:innen
im Diakonischen Werk
Innere Mission Leipzig e.V.

Inhalt

Für wen ist diese Datenschutzbrochüre gedacht?	3
Was ist wichtig für den datenschutzkonformen Arbeitsalltag in unserem Werk?	4
Datenschutz beginnt bei Ihnen!	4
Worum geht es im Datenschutz?	4
Welche gesetzliche Grundlage gilt für mich bei der Datenverarbeitung?	5
Welche Daten sind zu schützen?	5
Wie schütze ich die Daten?	6
Wann darf ich personenbezogene Daten verarbeiten?	7
Was muss ich unbedingt bei der Bearbeitung der personenbezogenen Daten beachten?	7
Wann muss ich betroffene Personen über die Verarbeitung ihrer Daten informieren?	10
Welche Rechte haben Personen, deren Daten verarbeitet werden?	10
Die 10 Grundregeln am Arbeitsplatz:	12
Wie verhalte ich mich, wenn es zum Datenverlust kommt?	14
Wann werden personenbezogene Daten gelöscht? ...	14
Wer kann mir bei Fragen zum Datenschutz helfen? ...	14

Wo finde ich weitere Informationen zum Datenschutz in unserem Werk?	14
Verantwortung für den Datenschutz in meiner Organisation	15
Begriffsverzeichnis	16
Wie fit sind Sie im Datenschutz? Prüfen Sie selbst!	21

Für wen ist diese Datenschutzbrochure gedacht?

Die Ihnen vorliegende Datenschutzbrochure ist explizit für Sie – als Mitarbeitende(r) in unserer Organisation – vorgesehen. Sie hat das Ziel, Ihnen in einer verständlichen Weise die Grundsätze des Datenschutzes sowie die geläufigen Datenschutzbegriffe vorzustellen. Vor allem soll die Datenschutzbrochure Ihnen erklären können, wozu Sie den Datenschutz in unserer Organisation verpflichtend zu beachten haben.

Die Praxis / Erfahrungen zeigen, dass gerade der Mensch das schwächste Glied im Datenschutzsystem ist.

Unabhängig davon, ob Sie als Führungskraft oder als Praktikant in unserer Organisation tätig sind, müssen Sie sich mit den Grundsätzen des Datenschutzes auskennen, um die gesetzlichen Vorgaben bei eigenen Entscheidungen zur Datenverarbeitung in Ihrem Aufgabenfeld zu beachten. Nur so können Sie bewusst und sorgsam mit Daten umgehen und nur wenn Ihnen die Schadensrisiken bewusst werden, werden Sie sich um die datenschutzkonforme Verarbeitung der Daten kümmern.

Selbstverständlich bleiben Sie mit Ihren Fragen und Zweifeln nicht allein. In allen Fragen zum Datenschutz steht Ihnen unsere betriebliche Datenschutzbeauftragte zur Verfügung.

Was ist wichtig für den datenschutzkonformen Arbeitsalltag in unserem Werk?

Datenschutz beginnt bei Ihnen!

Aufgrund des breiten Spektrums der Dienstleistungen unserer Organisation gehen wir mit einer Vielzahl von Informationen um, die durch Datenschutzvorschriften geschützt werden müssen.

Als Mitarbeitende in unserem Werk müssen Sie sich daher mit den Grundsätzen des Datenschutzes auskennen. In Ihrem Arbeitsalltag werden Sie mit personenbezogenen Daten der Betreuten, der Kunden, der Mitarbeitenden und/oder Daten anderer Personengruppen arbeiten und dafür die Verantwortung übernehmen. Dabei sind Sie verpflichtet, die gesetzlichen Anforderungen des Datenschutzes zu beachten.

Worum geht es im Datenschutz?

Beim Datenschutz geht es um das Recht auf informationelle Selbstbestimmung eines jeden Menschen. Nicht die Daten als solche soll der Datenschutz schützen, sondern die Menschen, die hinter den Daten stehen. Jeder Mensch hat das Recht, selbst zu entscheiden wem er welche seiner

Daten offenbart (zugänglich macht) und zu erfahren zu welchen Zwecken die Daten verwendet werden.

Welche gesetzliche Grundlage gilt für mich bei der Datenverarbeitung?

Für unser Diakonisches Werk gelten die Vorschriften, die im Datenschutzgesetz der Evangelischen Kirche Deutschland (DSG-EKD) gefasst sind. Das DSG-EKD ist im Einklang mit der Datenschutzgrundverordnung (DSGVO), die europaweit die Grundlagen der datenschutzkonformen Datenverarbeitung regelt. Das DSG-EKD ist speziell auf unseren Tätigkeitsbereich angepasst und berücksichtigt die Besonderheiten des kirchlichen und diakonischen Auftrags in der Gesellschaft.

Welche Daten sind zu schützen?

Alle Informationen, die sich auf eine natürliche Person beziehen oder ermöglichen, eine natürliche Person zu identifizieren, sind sogenannte **personenbezogene Daten**. Als Personen sind hier gemeint unsere Betreuten, Kunden, Lieferanten, Mitarbeitenden, Praktikanten, Bewerber, Besucher und andere Personen, die mit unserer Organisation in irgendwelcher Weise verbunden sind (mit uns etwas zu tun haben).

Es gibt keine unwichtigen personenbezogenen Daten. Somit müssen geschützt werden die Stammdaten einer Person wie Name, Adresse, Geburtsdatum, Telefonnummer, E-Mailadresse, Sachdaten wie Bankverbindungen und besonders sensible Daten wie Gesundheitsdaten, Religionszugehörigkeit oder ethnische Herkunft.

Wie schütze ich die Daten?

Um Ihre Arbeitsaufgaben zu erfüllen, erhalten Sie Befugnis, nur die personenbezogenen Daten zu verarbeiten, die zur Erfüllung Ihrer Aufgaben notwendig sind. Wir sprechen hierbei von einem **berechtigten Zugang** zu personenbezogenen Daten. Dies bedeutet, dass Sie einen Zugang zu personenbezogenen Daten bekommen und in Ihrer Verantwortung der datenschutzkonforme Umgang mit den Daten liegt.

Dabei sind Sie verpflichtet, die **Schweigepflicht** (die Sie in Ihrem Arbeitsvertrag erklärt haben) zu beachten. Dies bedeutet, dass Sie keine personenbezogenen Daten an Unbefugte offenbaren dürfen. Unbefugte können sowohl andere Mitarbeitende (Deine Arbeitskollegen und -kolleginnen), Kunden, Ihre Familie oder andere Personen sein, die keinen berechtigten Zugang zu den Daten haben.

Wann darf ich personenbezogene Daten verarbeiten?

Im Datenschutz gilt das Prinzip: „*Was nicht erlaubt ist, ist verboten*“

Die Verarbeitung der personenbezogenen Daten ist nur dann erlaubt, wenn es dafür eine rechtliche Grundlage (zum Beispiel ein Gesetz) gibt oder eine Einwilligung der betroffenen Person vorliegt oder sie notwendig ist, um die Erfüllung der durch einen Vertrag vereinbarten Aufgaben zu gewährleisten.

Was muss ich unbedingt bei der Bearbeitung der personenbezogenen Daten beachten?

Damit Sie rechtskonform mit den Ihnen anvertrauten Daten umgehen können, sind von Ihnen folgende Grundregeln zu beachten:

Vertraulichkeit: Personenbezogene Daten müssen vertraulich behandelt werden. Nur Befugte dürfen einen Zugang zu den Daten haben und sie dürfen nur die Daten verarbeiten, die für deren Aufgabenbereich notwendig sind.

Beispiel: Sie haben eine E-Mail von einem Mitarbeitenden mit seinen für die Erfüllung Ihrer Aufgaben in der Personalabteilung notwendigen personenbezogenen Daten erhalten. Da sich in der E-Mail auch Angaben befinden, die für die Buchhaltung relevant sind, leiten Sie die gesamte E-

Mail an die genannte Abteilung weiter, sodass ein Teil der personenbezogenen Daten unbefugte Personen erreicht. Um die Vertraulichkeit der Datenverarbeitung zu sichern, hätten Sie vor dem Absenden der E-Mail alle Daten löschen müssen, die nur für die Verarbeitung in Ihrem Aufgabenbereich notwendig sind und den betroffenen Mitarbeitenden darüber informieren, welche Daten zu welchen Zwecken an wen weitergegeben werden.

Zweckbindung: Daten dürfen nur für eindeutig festgelegte Zwecke erhoben und verarbeitet werden. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Beispiel: wurde eine private E-Mail-Adresse einer Mitarbeiterin ausschließlich für den Versand ihrer Lohnabrechnung erfasst, darf sie nicht genutzt werden für den Versand von Newslettern, Einladungen zu Veranstaltungen oder anderen Information des Unternehmens.

Erforderlichkeit: Die Verarbeitung der Daten ist auf ein notwendiges Maß zu beschränken. Nur die Daten verwenden, die tatsächlich für die Erreichung der vorgesehenen Zwecke der Verarbeitung notwendig sind. Es gilt generell das Prinzip: „So viele Daten wie nötig, so wenige Daten wie möglich.“

Beispiel: Wenn eine Einrichtung ihren Mitarbeitenden Sicherheitsschuhe zur Verfügung aber keine Schutzkleidung

stellt, so darf nicht neben der Schuhgröße auch die Konfektionsgröße der Mitarbeitenden erfasst werden.

Richtigkeit: Die personenbezogenen Daten müssen immer auf dem aktuellen Stand und sachlich richtig sein, sie müssen aus zuverlässigen Quellen stammen. Unrichtige oder veraltete Daten müssen unverzüglich nach Bekanntgabe korrigiert werden.

Beispiel: Eine der Mitarbeitenden hat innerhalb der Organisation ihre Position als Pflegefachkraft von einer Einrichtung in eine andere gewechselt. In der Personalakte wurde die Änderung nicht durchgeführt und somit kommt es zu einer Verarbeitung unrichtiger Daten. Die Regelmäßige Aktualisierung / Überprüfung der Datenbestände ist für das Erhalten der Richtigkeit der Daten notwendig.

Speicherbegrenzung: werden personenbezogene Daten nicht mehr benötigt, müssen sie gelöscht werden. Nur die Daten, die gesetzlichen Aufbewahrungsfristen unterliegen, bleiben für die gesetzlich festgelegten Fristen aufbewahrt und werden jedoch nicht weiterverarbeitet.

Beispiel: Nach einem E-Mail-Kontakt hat sich herauskristallisiert, dass es zu keiner Zusammenarbeit / Geschäftsbeziehung mit einem Dienstleister kommt. So müssen die Kontaktdaten von dem Dienstleister gelöscht werden, weil es keine gesetzliche Grundlage für deren Speicherung besteht.

Transparenz: Für den Betroffenen muss immer ersichtlich sein, welche Daten von ihm für welche Zwecke verarbeitet werden. Eine Verarbeitung von Daten ohne dass der Betroffene davon weiß ist unzulässig.

Beispiel: Sie erfassen personenbezogene Daten von einem neuen Betreuten in Ihrer Einrichtung. Es ist dabei notwendig, dass Sie dem Betreuten in einer verständlichen Form erklären, zu welchen Zwecken Sie die Daten nutzen werden. Wenn notwendig, nutzen Sie eine einfache Sprache, um sicher zu stellen, dass für den Betroffenen nachvollziehbar ist, was mit welchen seinen Daten passiert.

Wann muss ich betroffene Personen über die Verarbeitung ihrer Daten informieren?

Bereits bei der Datenerhebung muss die betroffene Person über den Zweck, die Speicherdauer sowie mögliche Empfängerkategorien (bei Weitergabe der Daten) informiert werden. Zugleich ist ein Hinweis auf das Widerspruchsrecht der betroffenen Person zu erläutern.

Welche Rechte haben Personen, deren Daten verarbeitet werden?

Betreute, Klienten oder Kunden, Lieferanten und andere Personen, deren Daten Sie verarbeiten, haben gesetzlich

festgelegte Rechte, die sie jederzeit geltend machen können. Dazu gehören folgende Rechte:

Auskunft

Personen, deren Daten verarbeitet werden, haben das Recht, über den Umfang und den Zweck der Datenverarbeitung eine Auskunft zu erhalten. Dies bedeutet, dass die betroffenen Personen darüber zu unterrichten sind.

Die Pflicht zur Unterrichtung entfällt nur dann, wenn die betroffene Person bereits Kenntnis von dem Umfang und Zweck der Verarbeitung der Daten hat.

Berichtigung

Unrichtige Daten dürfen nicht verarbeitet werden. Auf Antrag der betroffenen Person müssen die Daten unverzüglich berichtigt werden.

Löschung

Nicht für die Verarbeitung notwendige Daten (ohne Zweckbindung) sind zu löschen. Nach Ablauf von Aufbewahrungsfristen sind Daten ebenso zu löschen.

Einschränkung der Verarbeitung

Wird die Richtigkeit der Daten von der betroffenen Person bestritten oder die Verarbeitung der Daten erfolgt nicht rechtmäßig oder bei Löschpflicht werden die Daten zur Rechtsverfolgung benötigt, sind diese zu sperren.

Datenübertragbarkeit

Auf Verlangen der betroffenen Person müssen die personenbezogenen Daten von der verantwortlichen Stelle einem anderen Dritten übermittelt werden.

Widerspruch

Gegen die Datenerhebung und -verarbeitung kann die betroffene Person jederzeit Widerspruch erheben.

Die 10 Grundregeln am Arbeitsplatz:

- **Clean Desk:** keine Dokumente mit personenbezogenen Daten (wie bspw. Verträge, Bewerbungsunterlagen) offen herum liegen lassen
- **Bildschirm sperren** beim Verlassen des Arbeitsplatzes
- **Sicheres Passwort** nutzen (10 oder mehr Zeichen, Groß und Kleinbuchstaben, Zahlen und Sonderzeichen). Das Passwort darf niemandem weitergegeben werden und darf nicht unter der Tastatur, am Bildschirm etc. befestigt werden
- nicht mehr benötigte **Papierdokumente** oder **Datenträger** mit personenbezogenen Daten nicht in den Papierkorb werfen, sondern im Schredder oder

durch Fachunternehmen **datenschutzkonform vernichten** lassen.

- **Faxübermittlung:** beim Versenden die eingegebene Nummer überprüfen und die Entgegennahme des Empfängers sicherstellen.
- **Drucken und kopieren:** Ausdrucke und kopierte Unterlagen mit personenbezogenen Daten nie im Drucker bzw. Kopierer liegen lassen
- In der **E-Mail-Kommunikation** auf die Weitergabe der Inhalte und Anhänge mit personenbezogenen Daten achten. Übermittlung von besonders sensiblen Daten in verschlüsselter Form durchführen (im Zweifelsfall per Post)
- **Schutz vor Mithören:** Gespräche / Telefongespräche sind so zu führen, dass unbefugte Personen keine vertraulichen Inhalte / Daten mitbekommen bzw. mitverfolgen können
- **Datentransport:** personenbezogene Daten sind auf Datenträgern (USB-Stick, Laptop, Smartphone, etc.) verschlüsselt zu transportieren

Wie verhalte ich mich, wenn es zum Datenverlust kommt?

Sollen Sie feststellen, dass personenbezogene Daten abhanden gekommen sind, melden Sie dies unverzüglich Ihrem Vorgesetzten. Abhängig vom Ausmaß des Schadens bei der betroffenen Person wird die Organisationsleitung über das Erfordernis einer Meldung an die betroffene Person und die Aufsichtsbehörde entscheiden.

Wann werden personenbezogene Daten gelöscht?

Grundsätzlich sind personenbezogene Daten zu löschen, wenn sie nicht mehr gebraucht werden, also die Zwecke, für welche sie erhoben und verarbeitet wurden, erreicht wurden. Dabei sind gesetzliche Aufbewahrungsfristen zu beachten. Die einzelnen Arbeitsbereiche einer Organisation haben ein entsprechendes Löschkonzept vorzuhalten.

Wer kann mir bei Fragen zum Datenschutz helfen?

Der betriebliche Datenschutzbeauftragte steht Ihnen bei allen Fragen zum datenschutzrechtlichen Umgang mit personenbezogenen Daten zur Verfügung.

Wo finde ich weitere Informationen zum Datenschutz in unserem Werk?

Eine übersichtliche Kurzfassung der Datenschutzregeln finden Sie in der *Datenschutzrichtlinien Diakonisches Werkes Innere Mission e.V.* (Fassung Juli 2019). Einzelne Themen, Formulare und Muster sind im Intrex zu finden.

Verantwortung für den Datenschutz in meiner Organisation

Als Führungskraft

haben Sie die Aufgabe, die Datenschutzregelungen umzusetzen und deren Einhaltung in Ihrem Verantwortungsbereich zu kontrollieren.

Sie erteilen die Befugnisse für die Verarbeitung der personenbezogenen Daten, unterstützen und sensibilisieren die Mitarbeitenden für die Bedeutung des Datenschutzes.

Als Mitarbeitende

haben Sie die Aufgabe, die Datenschutzregelungen einzuhalten. Für die zur Verarbeitung bestimmten personenbezogenen Daten haben Sie Befugnis erhalten und Sie sind verpflichtet, die Daten vor unbefugtem Zugriff und unberechtigter Weitergabe zu schützen. Im Falle des Datenverlustes informieren Sie Ihren Vorgesetzten

Begriffsverzeichnis

Anonymisieren

Daten werden so verändert/behandelt, dass deren Zuweisung zu einer Person nicht mehr möglich ist

Auftragsdatenverarbeitung

Zur Erfüllung eigener Aufgaben werden andere Unternehmen beauftragt. Die Verarbeitung der eigenen personenbezogenen Daten durch die anderen Unternehmen wird Auftragsdatenverarbeitung (Verarbeitung der Daten im Auftrag) genannt. Die Verantwortung für die Verarbeitung der Daten sowie die Weisungsrechte bleiben beim Auftragsgeber. Datenschutzrechtliche Vorgaben sind in einem Vertrag zwischen Auftraggeber und Auftragnehmer zu verfassen.

Auskunftsrecht

Jede Person hat das Recht zu erfahren, welche Daten von ihr zu welchen Zwecken gespeichert und verarbeitet werden.

Betroffene Person

Jede Person (z.B. Mitarbeiter, Betreuer, Lieferant, Kunde) deren Daten gespeichert und verarbeitet sind.

Besondere Kategorie personenbezogener Daten (sensible Daten)

Sensible Daten, wie Gesundheitsangaben, religiöse oder sexuelle Ausrichtung, ethnische Herkunft, politische Orientierung, Gewerkschaftszugehörigkeit. Bei der Verarbeitung von sensiblen Daten sind besonders strenge datenschutzrechtliche Maßstäbe zu setzen.

Datenschutzbeauftragte(r) / betrieblicher Datenschutzbeauftragte(r)

Unabhängige Stelle, die die Einhaltung des Datenschutzrechts in einer Organisation überwacht. Zu seinen Aufgaben gehören die Schulung der Mitarbeitenden sowie die Beratung der Geschäftsführung und der Mitarbeitenden in allen datenschutzrechtlichen Fragen.

Datenschutz-Aufsichtsbehörde

Die zuständige Datenschutz-Aufsichtsbehörde kontrolliert die Einhaltung des Datenschutzes in der Organisation.

Datenschutzgrundverordnung (DSGVO)

ist eine Verordnung der Europäischen Union, die Vorschriften zum Schutz **natürlicher Personen** bei der Verarbeitung personenbezogener Daten enthält. Sie soll die Grundrechte und -freiheiten natürlicher Personen schützen und vor allem das Recht auf Schutz der persönlichen Daten.

Datensicherheit

Alle technischen und organisatorischen Maßnahmen einer Organisation, um personenbezogene Daten sicher zu verwahren sowie gegen Angriffe von außen zu schützen.

Datenverlust (Datenleck/Datenpanne)

Wenn personenbezogene Daten in unbefugte Hände gelangen, spricht man von Datenleck oder Datenverlust. Jeder Mitarbeiter, der Datenverlust (Datenleck) in Kenntnis genommen hat, hat dies unverzüglich an seinen Vorgesetzten zu melden. Abhängig von den Folgen des Datenverlustes wird durch die Geschäftsführung eine Entscheidung getroffen, ob dies als Datenpanne einzuordnen und an die Aufsichtsbehörde zu melden ist sowie ob die betroffenen Personen zu benachrichtigen sind.

Datenschutzgesetz der Evangelischen Kirche Deutschland (DSG-EKD)

Das Datenschutzgesetz der EKD ist die für den Bereich der Evangelischen Kirchen und ihrer Einrichtungen geltende Datenschutzregelung. Diese Datenschutzregelung ist im Einklang mit der DSGVO.

Einwilligung

Eine freiwillige Erklärung der betroffenen Person für die Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten. Eine Einwilligung bedarf nicht

immer einer schriftlichen Form, sie sollte jedoch aus Gründen der Nachweisbarkeit dokumentiert werden.

Erhebung der Daten

Die Beschaffung der personenbezogenen Daten über die betroffene Person.

Informationelle Selbstbestimmung

Das Recht eines jeden Menschen, selbst entscheiden zu können, was die anderen über ihn wissen dürfen und damit welche personenbezogenen Daten von ihm erfasst und verarbeitet werden sowie zu welchen Zwecken.

Schweigepflicht (Datengeheimnis)

Alle Mitarbeitende, die personenbezogene Daten verarbeiten, verpflichten sich der Organisation (also dem Diakonischen Werk Innere Mission Leipzig e.V.) gegenüber, die Vorschriften des Datenschutzes einzuhalten und die ihnen anvertrauten personenbezogenen Daten nicht unbefugt zu verarbeiten oder an Dritte zu geben. Die Schweigepflicht gilt auch nach Beendigung des Arbeitsverhältnisses.

Personenbezogene Daten

Alle Angaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person gehören zu den personenbezogenen Daten.

Pseudonymisierung

Das Ersetzen der Identifikationsmerkmale einer Person durch Kennzahlen, Schlüssel oder andere Namen, um die Feststellung der Identität der betroffenen Person wesentlich zu erschweren oder auszuschließen.

Verarbeitung der Daten

Das Speichern, Verändern, Übermitteln, Sperren, Löschen von personenbezogenen Daten.

Verzeichnis von Verarbeitungstätigkeiten

Eine detaillierte Auflistung der wesentlichen Verarbeitungen von Daten in einzelnen Bereichen / Abteilungen in einer Organisation.

Widerspruchsrecht

Ein Recht, das jeder natürlichen Person zusteht, sich gegen die Verarbeitung ihrer persönlichen Daten zu widersprechen.

Zweckbindung

Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie erhoben und gespeichert wurden.

Wie fit sind Sie im Datenschutz? Prüfen Sie selbst!

- 1. Datenschutz dient dem Schutz ...**
 - a. der natürlichen Personen vor unrechtmäßigem Umgang mit deren Daten
 - b. der Unternehmen
 - c. der Gesetze

- 2. Personenbezogene Daten dürfen erhoben werden, wenn ...**
 - a. eine Einwilligung vorliegt
 - b. dies zur Erfüllung eines Vertrages notwendig ist
 - c. es dafür eine gesetzliche Grundlage gibt

- 3. Die Verantwortung für den Datenschutz im Unternehmen hat / haben ...**
 - a. nur der Datenschutzbeauftragte
 - b. nur die Führungskräfte
 - c. alle Mitarbeitende

- 4. Die Schweigepflicht verlangt von allen Mitarbeitenden ...**
 - a. die Offenbarung der personenbezogenen Daten nur an die Geschäftsführung

- b. die Wahrung der Vertraulichkeit während und auch nach Beendigung des Arbeitsverhältnisses

5. Beim Verlassen des Arbeitsplatzes sind folgende Regeln zu beachten:

- a. Sie sperren den Bildschirm
- b. Sie schließen Akten mit sensiblen Daten in die dafür vorgesehenen Aktenschränke

6. Datenverarbeitung bedeutet, dass personenbezogene Daten werden ...

- a. gespeichert
- b. weitergegeben / übermittelt
- c. gelöscht

7. Personen, deren Daten verarbeitet werden, haben das Recht auf ...

- a. Auskunft
- b. Widerspruch
- c. Berichtigung der Daten

8. Die für unsere Organisation vorrangig geltenden Datenschutzregelungen sind gefasst ...

- a. in der Datenschutzgrundverordnung (DSGVO)
- b. im DSG-EKD (Datenschutzgesetz der Evangelischen Kirche Deutschland)

Auflösung: 1a; 2a,b,c; 3c; 4b, 5a,b; 6a,b,c; 7a,b,c; 8b

Diakonisches Werk Innere Mission Leipzig e.V.
Gneisenastraße 10
04105 Leipzig
T 0341 56 12-0
F 0341 56 12 11 35
info@diakonie-leipzig.de
www.diakonie-leipzig.de
www.instagram.com/diakonie_leipzig
www.facebook.com/diakonie.leipzig