



Datenschutz und Datensicherheit

Meine Daten gehören mir!

Vom richtigen Umgang mit personenbezogenen Daten

Vorwort	3
Datenschutz und Datensicherheit – Was ist das?	4
Voraussetzung und Grundsätze für die Datenerhebung und -nutzung	6
Die Rechte der betroffenen Personen	8
Regeln zur Auskunftserteilung	8
Praxis-Tipps zum Datenschutz	9
Datenschutzverletzung - was tun?	11
Hinweise geben – sicher und anonym	11
Ansprechpartner	12



Mehr und mehr hört man von Hackerangriffen auf Unternehmen und organisiertem Datenklau. Durch die öffentlichen Skandale der letzten Jahre sind die Themen Datenschutz und Datensicherheit mittlerweile in aller Munde. Das Vertrauen in digitale Datenspeicherung steht auf dem Prüfstand. Umso wichtiger ist es, auch als Arbeitnehmer zu wissen, worauf bei der Datensicherheit zu achten ist.

Wir vom Caritasverband Lünen-Selm-Werne stellen uns der Verantwortung für die uns übertragenen personenbezogenen Daten. Dieser kompakte Ratgeber soll Sie bei dem sicheren Umgang mit diesen Daten unterstützen und mögliche Fragen beantworten.

Hans-Peter Benstein

Gibt es einen Unterschied zwischen Datenschutz und Datensicherheit? Oder sind das nur unterschiedliche Begriffe für das gleiche Thema? Die Begrifflichkeiten unterscheiden sich kaum, sie verfolgen jedoch unterschiedliche Ziele. Trotzdem sind sie voneinander abhängig und Datenschutz kann ohne Datensicherheit nicht funktionieren.

Wie dies zusammenhängt und was Sie persönlich, insbesondere in Ihrem Arbeitsumfeld, zu einem sensiblen Umgang mit gespeicherten Daten beitragen können, erfahren Sie auf den folgenden Seiten.

Heike Homann

Datenschutz und Datensicherheit

Was ist das?

Datenschutz

Datenschutz beschäftigt sich mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Er wird durch das Bundesdatenschutzgesetz (BDSG) und insbesondere für uns durch das Gesetz über den kirchlichen Datenschutz (KDG) gesetzlich geregelt. Der Datenschutz soll dafür Sorge tragen, dass das Persönlichkeitsrecht der Menschen durch den Umgang mit ihren Daten nicht negativ beeinflusst wird. Er verbietet die unerlaubte Erfassung, Speicherung oder Nutzung personenbezogener Daten. Das nennt man auch das „Datengeheimnis“. Beim Datenschutz geht es um die zentrale Frage, ob personenbezogene Daten überhaupt erhoben und verarbeitet werden dürfen oder nicht.

Datensicherheit

Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Maße gegen Manipulation, Verlust oder unberechtigte Kenntnisnahme durch Dritte zu sichern.

Im Unterschied zum Datenschutz betrifft die Datensicherheit alle Daten im Unternehmen, unabhängig davon, ob diese einen Personenbezug haben oder nicht. Unter diesen Begriff fallen daher auch solche Daten, die keinen Personenbezug haben, wie z.B. Baupläne.

Zur Erreichung der Datensicherheit sind Unternehmen verpflichtet, entsprechende Maßnahmen und Vorkehrungen zu treffen. Selbst wenn Sie keine personenbezogenen Daten erheben, verarbeiten oder nutzen sollten, müssen sie die Anforderungen an die Datensicherheit erfüllen.



Bedeutung und Geltungsbereiche

	Datenschutz	Datensicherheit
Schutz von	natürlichen Personen	Hardware, Software, IT-Infrastruktur
Schutz vor	Verletzungen der Persönlichkeitsrechte	unberechtigte Daten-Zugriffe, Datenmissbrauch, Daten-Diebstahl, Daten-Verlust
Schutz-gegenstand	personenbezogene Daten	alle (Unternehmens-) Daten
Basis	Grundgesetz, Bundesdatenschutzgesetz, Gesetz über den kirchlichen Datenschutz (KDG)	interne Vereinbarungen, Anweisungen

Gemeinsamkeiten

Interessenkonflikte



Datenerhebung und Datennutzung

Voraussetzung

Personenbezogene Daten kommen in jedem Unternehmen jeder Größenordnung vor. Beispiele für personenbezogene Daten sind:

- Persönliche Daten (z.B. Name, Geburtsdatum, Adresse, Telefonnummer ...)
- Mitarbeiterdaten (z.B. Ausbildungsberuf, Familienstand, Urlaub ...)
- Lohn- und Gehaltsdaten
- E-Mail-Adressen, die einer bestimmten Person mittelbar zugeordnet werden können, weil sie z.B. Vor- oder Zunamen enthalten
- Konsumverhalten

Zwei Voraussetzungen erlauben die Erhebung und Nutzung personenbezogener Daten: Zum einen die ausdrückliche Zustimmung der oder des Betroffenen, zum anderen eine rechtliche Erlaubnisgrundlage, wie z.B. Gesetze, Verträge oder Betriebsvereinbarungen.

Ansonsten ist die Erhebung und Nutzung personenbezogener Daten grundsätzlich verboten!

Grundsätze

Erforderlichkeit

Prüfen Sie, ob die Verarbeitung der Daten wirklich erforderlich oder doch vermeidbar ist.

Datenvermeidbarkeit

Prüfen Sie stets, ob die angefragten oder bearbeiteten Daten alle für die jeweilige Anforderung erforderlich sind. Beschränken Sie sich auf die notwendigen Daten.

Datensparsamkeit

Löschen Sie Daten, die nicht mehr benötigt werden. Beachten Sie dabei die unterschiedlichen Aufbewahrungsfristen.

Direkterhebung

Erheben Sie Daten nur bei dem Betroffenen selbst. Auskünfte, die Sie von Dritten bekommen, sind nicht verwertbar!

Zweckbindung

Erheben und verarbeiten Sie nur die Daten, die im Voraus festgelegt wurden. Wenn Sie diese selbst festlegen, dokumentieren und begründen Sie dies schriftlich.

Datenqualität

Erheben Sie nur Fakten, keine Meinungen, Einschätzungen, Annahmen. Formulieren Sie so, dass es auch für unbeteiligte Dritte nachvollziehbar ist. Berichtigen Sie Fehler und löschen Sie falsche Angaben.

Grundsätzlich gilt: Haben Sie Zweifel, wenden Sie sich an Ihre Vorgesetzte bzw. Ihren Vorgesetzten !



Betroffenen-Rechte

Alle „Betroffene“ (Beschäftigte, Kunden, Lieferanten, Bewerber/-innen ...), über die Daten gespeichert sind, haben Recht auf ...

- **Auskunft:**
Vollständige Auskunftserteilung durch die verantwortliche Stelle
- **Berichtigung:**
Unverzögliche Korrektur falscher Daten
- **Sperrung:**
Sofortige Sperrung strittiger und/oder nicht (mehr) erforderlicher Daten
- **Löschung:**
Sofortige Löschung nicht (mehr) erforderlicher Daten
- **Schadenersatz:**
Schadenersatz bei Verletzung des Persönlichkeitsrechtes (Datenschutzes)
- **Nutzungs-Widerspruch:**
Keine Nutzung oder Übermittlung der Daten für Zwecke der Werbung

Regeln zu Auskünften

- Eine Auskunft kann in der Regel nur zu einem Einzelfall gegeben werden.
- Die Anfrage muss einen konkreten Sachverhalt beschreiben.
- Der Anfragende muss berechtigt sein die Auskunft zu erhalten: es handelt sich um seine eigenen Daten oder die seiner Bezugsperson oder die Auskunft ist für die Durchführung von Aufgaben des Anfragenden erforderlich.
- Ein Versand von Originalakten ist nicht möglich. Nur Kopien dürfen überlassen werden.
- Bei Unsicherheiten ziehen Sie Ihren Vorgesetzten hinzu oder bitten Sie um eine schriftliche Anfrage an datenschutz@caritas-luenen.de.
- Ausschließlich der tatsächlich geforderte und für die Aufgabenerfüllung erforderliche Informationsumfang darf offenbart bzw. in Dokumenten übersandt werden. (Ggf. nicht relevante Stellen vor dem Kopieren abdecken.)
- Die Anfrage mit Namen, Datum, Uhrzeit und den gegebenen Auskünften unbedingt kurz dokumentieren.

Praxis-Hinweise zum Datenschutz

Passwörter

Schützen Sie den PC vor unbefugtem Zugriff durch sichere Passwörter. Diese sind mind. 12 Zeichen lang und enthalten Ziffern, Buchstaben (groß und klein) und Sonderzeichen. Wählen Sie verschiedene Passwörter für unterschiedliche Anwendungen und notieren/speichern Sie diese nicht an Ihrem Arbeitsplatz. Geben Sie Ihre Passwörter niemals weiter.

Viren und Trojaner

Schützen Sie ihren PC und ihre Daten vor Viren und Trojanern, indem Sie E-Mails unbekannter Herkunft und unerwartete Anhänge nicht öffnen. Sollte es passieren, dass sich ein Virus oder Trojaner auf Ihrem PC installiert, sofort den PC abschalten und unverzüglich Ihren Vorgesetzten sowie die EDV-Abteilung informieren.

Internet

Ihre Identität ist im Internet nicht geschützt. Was Sie im Internet tun, tun Sie nicht anonym. Seien Sie daher generell vorsichtig bei Kommentaren und Informationen in sozialen Netzwerken oder Foren. Sie dürfen dort ausschließlich als Privatperson und nicht vom Arbeitsplatz aus aktiv sein.

E-Mails

Wenn Sie nach außen kommunizieren, verwenden Sie offene E-Mail-Verteiler nur, wenn sämtliche Empfänger nachweisbar eingewilligt haben, dass ihre E-Mail-Adresse für Dritte sichtbar ist. In allen anderen Fällen senden Sie Mails an Ihre eigene Adresse – und setzen die eigentlichen Empfänger ins Bcc-Feld (Blindkopie - sollte Bcc im Mailprogramm nicht angezeigt werden, muss dieses in den Einstellung zuvor aktiviert werden).

Messenger-Dienste

Viele Messenger-Dienste entsprechen in Bezug auf den Datenschutz nicht den gesetzlichen Vorgaben (z.B. WhatsApp). Der Austausch personenbezogener und vertraulicher Daten über diese Dienste ist daher nicht zulässig.

Office-Dateien

Versenden Sie Office-Dateien (Word, Excel, Powerpoint) nur dann als solche, wenn sie vom Empfänger weiter bearbeitet werden sollen. Ansonsten erstellen Sie ein PDF-Dokument, um die Weitergabe unserer Vorlagen, Signaturen, Verweise und anderer interner Informationen zu vermeiden. Sensible Daten verschlüsseln Sie darüber hinaus mit einem Passwort und versenden dieses separat.

KEINE private Nutzung

Eine Nutzung privater Hardware (auch Speichermedien wie USB-Sticks, Speicherkarten und Festplatten) sowie privater Software ist nicht gestattet, sofern nicht anders mit dem Vorgesetzten vereinbart. Ebenso ist das Speichern privater Daten auf dem Dienst-PC untersagt. Dienstlich beschaffte Soft- oder Hardware darf nicht privat verwendet werden.



Praxis-Tipps zum Datenschutz

Sicherheit mobiler Geräte

Schützen Sie dienstliche Mobiltelefone oder Laptops vor unbefugten Zugriffen und Diebstahl.

Aufgeräumter Schreibtisch

Räumen Sie Ihren Arbeitsplatz auf, wenn Sie diesen verlassen, so dass keine Daten an Unbefugte gelangen können. Schließen Sie Dokumente ein und sperren Sie Ihren PC.

Entsorgung

Beachten Sie die jeweiligen unterschiedlichen Aufbewahrungsfristen für Dokumente. Nicht mehr benötigte sensible Unterlagen müssen geschreddert, nicht über den Papiermüll entsorgt werden. Datenträger mit sensiblen Inhalten müssen sicher gelöscht oder zerstört werden.

Telefonische Auskünfte

Vorsicht bei telefonischen Auskünften, seien Sie skeptisch und fragen Sie bei Zweifeln genauer nach (siehe Seite 8).

Kopierer

Denken Sie daran nur relevante Dokumente zu kopieren. Vergessen Sie keine Dokumente am Kopierer und denken Sie ggf. daran bestimmt Inhalte zu schwärzen.

Post

Öffnen Sie nur Briefe, die auch für Sie bestimmt sind oder zu deren Öffnung Sie berechtigt sind.

Datenschutzverletzung - was tun?

Eine Datenschutzverletzung kann trotz aller Vorsicht schnell passieren. Sie liegt vor, wenn

- personenbezogene Daten unbeabsichtigt oder unrechtmäßig vernichtet, verloren oder verändert wurden
- es zur unbefugten Offenlegung oder unbefugten Zugang zu personenbezogenen Daten kommt.

Eine solche Datenpanne ist verpflichtend innerhalb von 72 Stunden von uns an die zuständige Aufsichtsbehörde zu melden. Informieren Sie daher in jedem Fall unverzüglich Ihren Vorgesetzten.

Hinweise geben – sicher und anonym

Dinge wie unethisches Verhalten oder illegales Vorgehen – egal, ob vorsätzlich oder unbewusst – schadet der Vertrauenswürdigkeit und dem Ansehen und gefährdet womöglich viele Arbeitsplätze. Dies gilt es zu verhindern. Hinweise aus der Belegschaft helfen dabei oder machen dies überhaupt erst möglich.

Das Hinweisgeberschutzgesetz (HinSchG) legt fest, dass Mitarbeitende Hinweise über Missstände am Arbeitsplatz geben können ohne Nachteile für sich befürchten zu müssen.

In unserem Caritasverband gibt es eine Meldestelle, die Hinweise vertraulich aufnimmt, ihnen nachgeht und Maßnahmen ergreift, ohne dass der Hinweisgeber in Erscheinung tritt oder genannt wird. Da Datensicherheit und Anonymitätssicherung Hauptanforderungen an die Meldestelle sind, erfolgt die Angliederung an unseren Datenschutz. Eine Kontaktaufnahme mit der Meldestelle erfolgt über die Mail-Adresse datenschutz@caritas-luenen.de.

Nutzen Sie die Möglichkeit und informieren Sie die Meldestelle, wenn Dinge nicht korrekt laufen. Sie sind geschützt und bleiben anonym.

Kontakt – Noch Fragen?



Weitere Informationen zum Datenschutz und zur Datensicherheit erhalten Sie bei:

Sonja Hupfer
Datenschutzkoordinatorin

Tel.: 02306 7004-1234
datenschutz@caritas-luenen.de



Bernd-Tim Konerding
Datenschutzkoordinator

Tel.: 02306 7004-1264
konerding@caritas-luenen.de

Caritasverband Lünen-Selm-Werne e.V.
Lange Straße 84
44532 Lünen

Caritasverband Lünen-Selm-Werne e. V.

Lange Straße 84
44532 Lünen
Tel. 02306 7004-0
info@caritas-luenen.de