
Merkblatt zum Datenschutz

Sehr geehrte Mitarbeiter, sehr geehrte Mitglieder,

es wäre sicherlich nicht in Ihrem Sinne, wenn Daten über Ihre Person und Ihre persönlichen Verhältnisse Unbefugten zur Kenntnis gelangen würden. Davor schützen Sie die verschiedenen gesetzlichen Regelungen zum Datenschutz.

Nach diesen Gesetzen sind auch Sie im Rahmen Ihrer beruflichen oder ehrenamtlichen Tätigkeit dazu verpflichtet, die personenbezogenen Daten anderer vertraulich, rechtmäßig und weisungsgerecht zu behandeln. Bitte gehen Sie mit den Daten anderer mindestens so um, wie Sie Ihre eigenen Daten behandelt haben möchten.

Sie sind in Ihrer Tätigkeit dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung verarbeitet (dazu gehören erheben, erfassen, organisieren, ordnen, speichern, anpassen oder verändern, auslesen, abfragen, verwenden, offenlegen durch übermitteln, verbreiten oder in anderer Form bereitstellen, abgleichen oder verknüpfen, einschränken, löschen oder vernichten) oder genutzt werden.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Mitglieds- oder Personalnummer, zu Standortdaten wie Wohnanschrift oder Arbeitsstelle, zu einer Online-Kennung wie Benutzer-Account oder Mailadresse zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Jeder Missbrauch und jede unbefugte Weitergabe dieser Daten sind unzulässig und strafbar.

Sie wurden auf Vertraulichkeit verpflichtet, welche auch nach Beendigung Ihrer Tätigkeit in und für das Deutsche Rote Kreuz fortbesteht. Insgesamt streben wir in unserem Hause einen gleichmäßigen Schutz aller Daten an – sowohl für die personenbezogenen Daten als auch für alle anderen sensiblen betriebsinternen Daten.

Insbesondere sind Sie persönlich dafür verantwortlich, dass

- die Ihnen anvertrauten Daten, Datenträger und Listausdrucke unter Verschluss gehalten werden, sofern Sie nicht unmittelbar daran arbeiten. Dies gilt einerseits für Akten und Schriftstücke, in denen sich nicht allgemein zugängliche Daten befinden, und andererseits für alle auf dem Bildschirm abrufbaren Informationen. Bitte aktivieren Sie daher generell einen kennwortgeschützten Bildschirmschoner mit einem Ihren Arbeitsgewohnheiten adäquatem Zeitlimit. Dieser schaltet sich nach der eingestellten Zeit automatisch ein, kann bei Verlassen des Raumes aber auch von Hand aktiviert werden. Bei längerer Abwesenheit ist es ratsam, sich ganz von den Systemen abzumelden, um z.B. eventuelle Systemarbeiten nicht zu behindern.

- Ihr Computer, Ihre Anwendung und Ihr Kennwort keinem Unbefugten zugänglich gemacht werden.
- nicht mehr benötigte Datenträger und Listausdrucke datenschutzgerecht vernichtet werden, damit

eine missbräuchliche Verwendung der Daten nicht möglich ist. Datenschutz im DRK Kreisverband Bremervörde e.V.

- an Druckern und Faxgeräten keine Ausdrucke mit personenbezogenen Daten oder sonstigen sensiblen betriebsinternen Daten liegen gelassen werden.

Von uns angeschaffte IT-Geräte aller Art sowie die verbandseigenen IT-Programme und Daten sind ausschließlich für den dienstlichen Gebrauch bestimmt. Ihre Nutzung für jede Art von nicht-dienstlichen Zwecken ist unzulässig. Untersagt ist auch der Einsatz von IT-Geräten, Programmen, CDs, ITDs und USB-Sticks o.ä. für dienstliche Zwecke, die nicht durch den Verband beschafft bzw. geprüft wurden.

Der Datenaustausch zwischen dienstlichen und privaten PCs ist verboten. Das Kopieren von Lizenzprogrammen sowie Dokumentationen und Handbüchern kann nach dem Urheberrecht strafrechtlich verfolgt werden. Die Verwendung von IT-Geräten einschl. Datenträgern bzw. von IT-Programmen ist außerhalb der Geschäftsräume nicht erlaubt.

Dies gilt nicht für

- das während einer Dienstreise benötigte Material;
- den dienstlichen Transport zwischen Betrieben;
- den dienstlich veranlassten Datenaustausch mit externen Stellen.

Private IT-Geräte bzw. Programme dürfen nicht in die Räume des Verbandes mitgebracht werden.

Festplatten von PCs stellen, da sie in den Büros frei zugänglich sind, ein Sicherheitsrisiko dar. Speichern Sie daher **–** wenn eben möglich **–** Daten nur auf unseren Servern ab. Dort sind die Daten räumlich gesichert und nur autorisierten Benutzern zugänglich. Außerdem findet dort eine regelmäßige Sicherung der Daten statt. Generell gilt: **Solange Sie Daten lokal auf der Festplatte Ihres PCs abspeichern, bleiben Sie für die Sicherheit und Sicherung der Daten persönlich verantwortlich!**

Jeder Anwender ist verpflichtet, die für PCs sowie andere Off-Line-Systeme vorgesehene Sicherungssoftware bei der Speicherung/Verarbeitung personenbezogener Daten eigenverantwortlich einzusetzen. Soweit beim Einsatz der Sicherungssoftware bei PCs Protokolldokumente anfallen, sind diese, sofern nicht andere Bestimmungen gelten, vom Benutzer mindestens 6 Monate aufzubewahren.

Vom Anwender sind, falls erforderlich, spezielle Sicherungsmaßnahmen zum Schutz seiner Dateien zu ergreifen.

Dokumentation der individuellen Datenverarbeitung

Der Anwender muss den zuständigen Stellen jederzeit darüber Auskunft geben können, welche personenbezogenen Daten bzw. Mitarbeiterdaten er verarbeitet und welchem Zweck die Speicherung/Verarbeitung dient (manuelle oder maschinelle Aufzeichnung der Anwendungen).

Dokumentationspflichtig im Sinne einer Programmdokumentation sind insbesondere solche Anwendungen, die

- Daten für die interne und externe Rechnungslegung;
- Daten mit Bestandsführungsfunktion für personen-/personalbezogene Daten;
- Daten als Grundlage für die Unternehmenssteuerung.

verarbeiten. In weiteren Anwendungsfällen entscheidet der Anwender selbst, ob eine Programmdokumentation notwendig ist.

Weitere konkrete Regelungen zur Handhabung sind in internen Richtlinien des Verbandes bzw. der Gesellschaft festgelegt. Eine Nichtbeachtung dieser Regelungen und der in diesem Merkblatt aufgeführten Bestimmungen gilt als Verstoß und kann rechtliche Konsequenzen nach sich ziehen.

Viren und Malware stellen ein erhebliches Sicherheitsrisiko dar. Umso wichtiger ist es daher, sicherzustellen, dass auf keinen Fall Viren von außen in die Netzwerke eingeschleppt werden. Am häufigsten erfolgt eine „Infektion" mit Computerviren durch die Verwendung von Wechseldatenträgern wie z.B. CDs, USB-Sticks mit Raubkopien und/oder sonstigen infizierten Datenbeständen oder über E-Mails aus nicht vertrauenswürdigen Quellen.

Die Verwendung von Raubkopien ist in unserem Hause strikt verboten!

Das Netzwerk ist durch folgende Maßnahmen abgesichert:

- Dateien auf externen Datenträgern wie z.B. USB-Sticks, CDs, Disketten etc. werden beim Öffnen bzw. Kopieren automatisch auf Viren geprüft.

- Bei jeder Anmeldung auf einem der Netzwerke-PC's wird automatisch eine Virenprüfung gestartet.
- Die IT-Administration sorgt dafür, dass die jeweils neuesten Virenprüfprogramme installiert sind.

Nutzung des E-Mail-Systems

Über das Mailsystem kann jeder Mitarbeiter Daten über das Internet verschicken. Beachten Sie dabei bitte folgende Regeln.

- E-Mails sind nicht abhörsicher, sie sind wie Postkarten! Bedenken Sie dies bitte beim Umgang mit geschützten Daten, wie Personaldaten oder sonstige Betriebsinterna, und wählen Sie zum Transport derselben lieber herkömmlichen Übermittlungsarten wie z.B. Briefpost. Bei elektronischem Versand sind dem Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden. Bitte machen Sie sich mit den aktuellen Regelungen vertraut.

- Bitte öffnen Sie bei eingehenden E-Mails keine Dateien unbekannter Herkunft, die Ihnen unaufgefordert zugesandt wurden.

- E-Mails mit archivierungspflichtigem geschäftlichem Inhalt müssen in Analogie zu sonstigen Anwendungsdateien aufbewahrt werden (Datenspeicherung im zutreffenden Netzlaufwerk, Archivierung in Papierform). Die Verantwortung trägt jeder Mitarbeiter für seinen Zuständigkeitsbereich.

- Das Übermitteln, Empfangen und Öffnen von ausführbaren Programmen ist grundsätzlich nicht zulässig. Ausgenommen davon ist das für dienstliche Zwecke Notwendige nach vorheriger Absprache mit der IT-Administration. Gleiches gilt für Anlagen von E-Mails, die nicht eindeutig zu identifizieren sind.

- Empfangene Programme und Anlagen dürfen nicht ungeprüft angewandt werden. Es muss durch die IT-Administration insbesondere geprüft werden, ob sie frei von Schadfunktionen/Viren sind und keinerlei Kompatibilitätsprobleme bestehen. Der Empfänger elektronischer Post ist für die Prüfung der eingehenden Dateien auf Schadfunktionen verantwortlich. Die IT-Administration trägt dafür Sorge, dass geeignete Scan-Programme zur Verfügung stehen. Wird eine Datei mit Schadfunktion entdeckt, ist unverzüglich die IT-Administration zu informieren. Dies gilt auch, wenn das Anti-

Virenprogramm einen Virus erkannt und als gelöscht angezeigt hat. Außerdem sollte der Absender der elektronischen Post informiert werden.

Internet-Nutzung

Mitarbeiter, die im Rahmen ihrer Tätigkeit Zugriff auf das Internet haben, müssen sich mit den folgenden Regeln vertraut machen:

• Die Nutzung des Internets wird zum dienstlichen Gebrauch eingerichtet.

• Es dürfen nur die von der IT-Administration bereitgestellten Programme für die Nutzung des Internets gebraucht werden. Es ist nicht gestattet, dass sich Beschäftigte eigenmächtig Programme installieren. Dies liegt darin begründet, dass bei neuen Versionen oft mit neuen/unbekannten Sicherheitslücken zu rechnen ist.

• Durch die weltweite Verfügbarkeit des Internets ist es möglich, dass Inhalte des Internets gegen bundesdeutsche Rechtsvorschriften, insbesondere gegen Zivil- und Strafgesetze, verstoßen. Jeder Benutzer ist selbst dafür verantwortlich, dass keine solchen Vorschriften verletzt werden. Sollten von dritter Seite an das Unternehmen Ansprüche wegen unrechtmäßiger Internetnutzung einer/eines Beschäftigten gestellt werden, so wird dieser Schadensersatzanspruch gegebenenfalls an die Beschäftigten weitergeleitet.

• Der Datenverkehr zwischen dem lokalen Netzwerk und dem offenen Netz unterliegt einer automatischen Protokollierung. Diese Protokolle dienen ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit und zur Sicherstellung eines ordnungsgemäßen Betriebes. Sie werden nicht zur Leistungskontrolle verwendet.

• Bei Zuwiderhandlungen gegen diese Regeln behält sich das Unternehmen u.a. vor, den Internetzugang zu deaktivieren.

Sicherheitsstandard für Kennwörter

Bei der Vergabe Ihres persönlichen Kennwortes beachten Sie bitte folgendes:

• Jeder Benutzer eines IT-Systems in unserem Hause erhält von der IT-Administration einen individuellen Benutzernamen, der ihn beim Zugang zu einem der Systeme identifiziert und autorisiert. Über ihn werden die jeweiligen Berechtigungen und verfügbaren Anwendungen angesteuert sowie alle Aktivitäten im jeweiligen System registriert.

• Zu jedem Benutzernamen gehört ein Kennwort, das im Gegensatz zum Benutzernamen immer verdeckt eingegeben wird. Dieses Kennwort wird von dem Mitarbeiter selbst vergeben und darf niemandem sonst bekannt werden – auch nicht den Mitarbeitern der IT-Administration, dem Vorgesetzten oder dem Datenschutzbeauftragten.

• Die von dem Benutzer gewählten Kennwörter müssen folgenden Regeln entsprechen:

a) Sie müssen eine Länge von mindestens 8 Zeichen haben (je länger desto besser).

b) Sie müssen mindestens einen Buchstaben und mindestens eine Ziffer enthalten.

c) Sie sollten keine leicht zu erratenden Trivial-Kennwörter sein wie z.B. Vornamen oder Geburtsdaten.

d) Andererseits sollte die Kombination aus Ziffern und Buchstaben leicht zu behalten sein.

e) Sinnvoll sind Eselsbrücken wie z.B. die Folge von Anfangsbuchstaben eines Liedes oder eines Spruchs in Kombination mit ein oder zwei Ziffern.

- Die Gültigkeitsdauer der Kennwörter ist zeitlich begrenzt. Nach Ablauf dieser Frist wird der Benutzer automatisch beim nächsten Zugang in das jeweilige System aufgefordert, ein neues Kennwort zu vergeben. Unabhängig davon sollten Sie auch vor Ablauf dieser Frist ein neues Kennwort vergeben, sobald Sie den Verdacht haben, dass eine Dritter von Ihrem Kennwort Kenntnis erlangt hat.

Bei Fragen zum Datenschutz oder in Zweifelsfragen wenden Sie sich bitte an Ihren Vorgesetzten oder an unseren Datenschutzbeauftragten, Großer Platz 12, 27432 Bremervörde, Email: Datenschutzbeauftragter@drkbremervoerde.de, Telefon: 04761 / 99 37 14

Verpflichtung auf Vertraulichkeit

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Ihnen auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.

Nach diesen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugter Offenlegung oder unbefugtem Zugang führt.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche bzw. aus dem Mitgliedschaftsverhältnis entstehende Pflichten dar, der entsprechend geahndet werden kann.

Soweit Ihre Tätigkeit das Fernmeldegeheimnis berührt, dürfen Sie sich nicht über das erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Sie dürfen derartige Kenntnisse grundsätzlich nicht an Dritte weitergeben.

Soweit Ihre Tätigkeit das Sozialgeheimnis berührt und Daten verarbeitet werden, die dem Sozialgeheimnis unterliegen, haben Sie diese im gleichen Umfang geheim zu halten, wie die ursprünglich übermittelnde Stelle.

Soweit Sie im Rahmen Ihrer Tätigkeit an der beruflichen oder dienstlichen Tätigkeit eines Berufsgeheimnisträgers mitwirken, ist es Ihnen untersagt, fremde Geheimnisse, namentlich zum persönlichen Lebensbereich gehörende Geheimnisse oder Betriebs- oder Geschäftsgeheimnisse unbefugt zu offenbaren.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung des Beschäftigungs- bzw. Mitgliedsverhältnisses fort.

Frau/Herr Abteilung/Tätigkeit

_____ _____

erklärt, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten.

Mit Ihrer Unterschrift bestätigen Sie zugleich den Empfang einer Kopie dieser Niederschrift nebst Anlage zur Verpflichtung auf Vertraulichkeit sowie das Merkblatt zum Datenschutz.

Ort, Datum	Verpflichteter	zusätzlich gesetzl. Vertreter b. Minderjährigen
_____	_____,	_____

Anlage zur Verpflichtung auf Vertraulichkeit

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: **„Personenbezogene Daten“** [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: **„Verarbeitung“** [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen […] auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen […] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese

Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung **–** insbesondere durch **Vernichtung, Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden **–** verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer **Verletzung** des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG

(1) Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder

2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder

2. durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

Fernmeldegeheimnis

§ 88 TKG

(1) 1Dem Fernmeldegeheimnis unterliegen der **Inhalt der Telekommunikation und ihre näheren Umstände**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist

oder war. 2 Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) 1Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. 2Die Pflicht zur Geheimhaltung besteht **auch nach dem Ende der Tätigkeit** fort, durch die sie begründet worden ist.

(3) 1Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. 2Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. 3Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. 4Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. […]

Sozialgeheimnis

§ 78 Abs. 1 Satz 2 & 3 SGB X: […] 2Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. 3Die Dritten haben die Daten **in demselben Umfang geheim zu halten** wie die in § 35 [SGB I] genannten Stellen.

Berufsgeheimnis

§ 203 StGB

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes, 6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. […]

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als **mitwirkende Person** oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. [...]

Nutzungsbedingungen für Internet (dienstlich und privat) und E-Mail (rein dienstlich) über Arbeitsplatzrechner im DRK Kreisverband Bremervörde e.V.

1. Die Nutzung von E-Mail und Internet ist nur zur Durchführung von dienstlichen Aufgaben und zur Unterstützung des dienstlichen Informationsaustausches zulässig. Eine Nutzung des Internetzuganges für private oder gewerbliche Zwecke ist untersagt.

2. Der Internetzugang steht den Mitarbeiter als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse. Die private Nutzung ist nur in den Pausen zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden. Sie wird rechtlich als dienstliche Nutzung behandelt.

3. Das Abrufen von kostenpflichtigen Informationen für den Privatgebrauch ist unzulässig. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden. Eine Unterscheidung von privater und dienstlicher Nutzung auf technischem Weg erfolgt nicht. Ein privater E-Mail-Verkehr ist nicht erlaubt.

4. Für die Nutzung des Internets ist nur Software zu verwenden, die von der IT-Administration bereitgestellt wird! Es ist nicht gestattet, dass sich Beschäftigte eigenmächtig Programme herunterladen oder installieren: Software kann dem Unternehmen schaden, wenn z.B. im Hintergrund Informationen an den Hersteller versendet werden. Auch neuere Versionen oder Aktualisierungen (Update) von Software können Sicherheitslücken aufweisen und die ITInfrastruktur des Unternehmens schädigen!

5. Downloads (heruntergeladene Daten) müssen auf der lokalen Festplatte in ein besonderes Verzeichnis abgelegt werden und dürfen nicht direkt ins Hausnetz gespeichert werden.

6. Das Internet ist nicht abhörsicher, deshalb dürfen sensible Informationen wie personenbezogene Daten oder Betriebsinterna nicht ohne die Nutzung von Verschlüsselungstechnologien über das Internet ausgetauscht werden. Dies gilt auch für den Fall, dass der Adressat berechtigt ist, diese Daten zu empfangen.

7. Durch die weltweite Verfügbarkeit des Internets ist es möglich, dass Inhalte des Internets gegen bundesdeutsche Rechtsvorschriften, insbesondere gegen Zivil- und Strafgesetze, verstoßen. Jeder Benutzer ist selbst dafür verantwortlich, dass keine solchen Vorschriften verletzt werden. Sollten von dritter Seite an das Unternehmen Ansprüche wegen unrechtmäßiger Internetnutzung einer/eines Beschäftigten gestellt werden, so wird dieser Schadensersatzanspruch gegebenenfalls an die Beschäftigten weitergeleitet. Unzulässig ist insbesondere jede absichtliche oder wissentliche Nutzung des Internets, die geeignet ist, den Interessen des Kreisverbandes oder seinen angeschlossenen Unternehmen oder dessen Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des IT-Netzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt. Dies gilt vor allem für

- das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,

- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen Äußerungen oder Abbildungen.

8. Je nach System unterliegt der Datenverkehr zwischen dem lokalen Netzwerk und dem offenen Netz einer automatischen Protokollierung. Diese Protokolle dienen ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit und zur Sicherstellung eines ordnungsgemäßen Betriebes. Sie werden nicht zur Leistungskontrolle verwendet. Auswertungen jedweder Art sind mitbestimmungspflichtig.

9. Die Mitnahme von dienstlichem Schriftverkehr oder von Dateien und das Speichern von dienstlichem Schriftverkehr oder Dateien auf privaten Rechnern ist verboten.

10. Bei Zuwiderhandlungen gegen diese Regeln behält sich das Unternehmen u.a. vor, den Internetzugang zu deaktivieren und gegebenenfalls auch strafrechtliche Untersuchungen einzuleiten.

Hiermit willige ich in den Tatbestand ein, dass meine private Nutzung von eMail und Internet beim **DRK Kreisverband Bremervörde e.V.** derart rechtlich behandelt wird, als wäre sie dienstlich. Mit dieser Einwilligung wird mir die private Nutzung von eMail und Internet durch meinen Arbeitgeber gestattet. Die Gestattung kann jederzeit vom Arbeitgeber ohne Angabe von Gründen zurückgezogen werden. Über die Folgen der Behandlung meiner privaten Nutzung von eMail und Internet analog der dienstlichen Nutzung bin ich durch das beigefügte Merkblatt informiert worden und habe dies zur Kenntnis genommen.

…….., …….. ……

Ort Datum Name, Vorname

……

Unterschrift

Einwilligungserklärung zur (dienstlichen und privaten) Nutzung von Internet und E-Mail

Merkblatt zur dienstlichen und privaten Nutzung von Internet und E-Mail

Dieses Merkblatt soll alle Beschäftigten des DRK Kreisverband Bremervörde e.V. über die Nutzung von E-Mail und Internet am Arbeitsplatz informieren.

Die private E-Mail und Internetnutzung am Arbeitsplatz ist beim **DRK Kreisverband Bremervörde e.V.** verboten.

Allen Beschäftigten möchte das DRK allerdings weiterhin die private Nutzung dieser Dienste am Arbeitsplatz ermöglichen. Voraussetzung dafür ist die Unterzeichnung der Einwilligungserklärung durch alle Beschäftigten. Sollten Beschäftigte diese Einwilligung nicht abgeben und unterzeichnen, so ist für sie die private Nutzung von E-Mail und Internet am Arbeitsplatz verboten.

Die Notwendigkeit zur Einholung einer solchen Einwilligung ergibt sich für das Deutsche Rote Kreuz aus einigen rechtlichen Anforderungen. In den weiteren Ausführungen dieses Merkblattes soll versucht werden, die juristische Notwendigkeit dieses Vorgehens verständlich zu erläutern.

Beim DRK ist die Nutzung von E-Mail und Internet ein fester Bestandteil des täglichen Arbeitsprozesses und des Workflows. Insbesondere aufgrund der zahlreichen internen und externen Geschäftsabläufe rund um den Globus, kann auf diese Formen der Kommunikationstechnologie nicht mehr verzichtet werden. Auf diese dienstliche Nutzung von E-Mail und Internet hat diese Einwilligungserklärung keinerlei Einfluss.

Bislang wurde beim **DRK Kreisverband Bremervörde e.V.** nicht zwischen privater und dienstlicher Nutzung unterschieden. Dies kann aufgrund gewisser rechtlicher Anforderungen zukünftig nicht beibehalten werden, weshalb eine solche Einwilligung notwendig wird.

Um die Dienste E-Mail und Internet zu ermöglichen, darf der Arbeitgeber die hierfür erforderlichen personenbezogenen Daten der Beschäftigten verarbeiten. Einige der anfallenden Daten werden auch zur Gewährleistung der Datensicherheit des Netzes benötigt und dürfen zu diesem Zweck in den entsprechenden Protokolldateien vorübergehend gespeichert werden. Damit ergeben sich vielfältige Fragen zur Wahrung der Privatsphäre der betroffenen Mitarbeiter. Je nach konkreter Ausgestaltung der Nutzungsmöglichkeiten sind folgende Vorschriften zu beachten:

- EU-Datenschutz-Grundverordnung (EU-DS-GVO)
- EU-E-Privacy-Verordnung
- Telemediengesetz (TMG),
- Telekommunikationsgesetz (TKG)
- Bundesdatenschutzgesetzes (BDSG)

Im Falle der ausschließlich dienstlichen Nutzung besteht zwischen Arbeitgeber und Beschäftigten kein Anbieter-Nutzer-Verhältnis, da es sich bei der Bereitstellung der Dienste nicht um ein Angebot von

Telekommunikation und Telediensten im Sinne des Telekommunikationsgesetzes bzw. Telemediengesetzes handelt. Die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten richtet sich nach den Vorschriften der EU-DS-GVO und des BDSG. Danach ist eine Abwägung der Interessen beider Seiten im Hinblick auf die Erforderlichkeit und Verhältnismäßigkeit der vorgesehenen Datenverarbeitung vorzunehmen. Hierbei kann das Grundrecht der Beschäftigten auf informationelle Selbstbestimmung tangiert werden.

Regelt der Arbeitgeber (wie bislang beim **DRK Kreisverband Bremervörde e.V.**) die private Nutzung des Internet nicht eindeutig, so gelten die Vorschriften des Telekommunikationsgesetzes bzw. die Regelungen des Telemediengesetzes, da der Arbeitgeber in diesem Fall seinen Beschäftigten gegenüber die Funktion eines Telekommunikations- bzw. Telediensteanbieters wahrnimmt. Als solcher hat er das Fernmeldegeheimnis zu beachten. Der Erlaubnisrahmen für die Verarbeitung der Verbindungs-, Nutzungs- und Abrechnungsdaten ist sehr eng gesteckt. Allgemein gesagt, dürfen die genannten Daten nur verarbeitet und genutzt werden, soweit dies für die Erbringung und Abrechnung der Dienste erforderlich ist.

Die sich aus dieser Rechtslage ergebenden unterschiedlichen Konsequenzen für die Durchführung von Kontrollmaßnahmen stellen den Arbeitgeber – will er die private Nutzung des Internet grundsätzlich regeln – in der Praxis vor das Problem, die dienstliche von der privaten Nutzung abgrenzen zu müssen.

Der **DRK Kreisverband Bremervörde e.V.** hat sich auf eine praktikable und aus Datenschutzsicht vertretbare Lösung verständigt. Diese sieht vor, keine Trennung der Verbindungs-/Nutzungsdaten nach dienstlicher und privater Nutzung vorzunehmen und dadurch die bei der privaten Nutzung anfallenden Daten in die Kontrollmaßnahmen für den Bereich der dienstlichen Nutzung einzubeziehen. In diese Lösung muss jeder Beschäftigte mit der beigefügten Erklärung einwilligen. Einwilligung und Kenntnisnahme des Merkblattes gestatten es den Beschäftigten weiterhin E-Mail und Internet auch privat am Arbeitsplatz zu nutzen. Eine individuelle Einwilligung in die Verarbeitung der bei der privaten Nutzung anfallenden Daten ist dann nicht mehr erforderlich. Denn sobald der Beschäftigte in Kenntnis der Regelung das Internet privat nutzt, liegt seine Einwilligung konkludent in seinem Verhalten, d. h., wenn er die Kontrollmaßnahmen nicht akzeptieren will, muss er die private Nutzung unterlassen.

Für die tägliche Praxis bedeutet diese Regelung keinerlei Änderung zur bisherigen Nutzung dieser Dienste.

Warum ist eine solche Regelung beim DRK Kreisverband Bremervörde e.V. notwendig?

Ein wesentlicher Grund für die Implementierung einer solchen Regelung liegt in den oben bereits angeführten Unterschieden zwischen der Funktion des Arbeitgebers als Telekommunikations bzw. Telediensteanbieters und einer rein dienstlichen Nutzung bzw. den dabei zu berücksichtigenden Gesetzen.

Eine eindeutige Regelung hat aber auch einige praktikable Vorteile, die an dieser Stelle am Beispiel der E-Mail-Nutzung verdeutlicht werden sollen. Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Beispielsweise kann der Vorgesetzte verfügen, dass ihm jede ein oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist. Private E-Mails dagegen sind wie private schriftliche Post zu behandeln und unterliegen dem Postgeheimnis. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails, der betreffende Mitarbeiter unverzüglich nach Bekanntwerden seines privaten Charakters zur alleinigen Kenntnis zu geben.

Um Irritationen beim Zugriff anderer Mitarbeiter auf Ihre E-Mails zu verhindern, wird daher dringend empfohlen, für private Kommunikation einen eigenen, privaten E-Mail-Account bei einem Web-Mailer, wie z.B. web.de oder gmx.de, zu nutzen!

Wird nicht zwischen dienstlicher und privater Nutzung unterschieden, so hat der Arbeitgeber keinerlei Zugriffsmöglichkeiten auf den E-Mail-Verkehr. Selbst bei längerfristiger Erkrankung oder einem plötzlichen Ausscheiden eines Beschäftigten hat der Arbeitgeber keine Rechte zur Einsicht. Dies kann zu schwerwiegenden Behinderungen des Workflows führen, da Mitarbeiter den Inhalt dienstlicher E-Mails nicht in Stellvertretung bearbeiten können.

Fazit:

Mit der Unterzeichnung der Nutzungsbedingungen für Internet (dienstlich und privat) und E-Mail (rein dienstlich) und der Kenntnisnahme dieses Merkblattes wird den Beschäftigten die private Nutzung von E-Mail und Internet am Arbeitsplatz gestattet. Für die tägliche Praxis bedeutet dies keinerlei Änderung zur bisherigen Nutzung dieser Dienste.

Mit der Einwilligung wird die private Nutzung mit der dienstlichen Nutzung gleichgestellt. Alle EMails und Internetzugriffe werden behandelt als wären sie dienstlich.

Für alle Beschäftigten, die diese Einwilligung nicht unterzeichnen und abgeben, ist die private Nutzung von Internet und E-Mail verboten.

Informationen zur Nutzung von WhatsApp

Die zwischenmenschliche Kommunikation findet heute zu einem großen Teil über Smartphones statt. Dabei wird nicht nur telefoniert, sondern vielfach werden Apps genutzt, welche einen Chat anbieten, über den auch Daten verschickt werden können.

Diese Richtlinie betrifft die Dienstliche Nutzung der App “WhatsApp“. Dabei liegt das Augenmerk darauf, welche datenschutzrechtlichen Risiken im Umgang mit der App verbunden sind und welches Verhalten bei der Nutzung empfohlen wird.

Schreibverhalten

Es wird darauf hingewiesen, dass die Weitergabe von dienstlich bekannt gewordenen Daten oder Informationen über den Arbeitgeber sowie verbundenen Einrichtungen, Partner oder Dienstleister bei WhatsApp ein Verstoß gegen die Pflicht der Wahrung von Betriebs- oder Geschäftsgeheimnissen darstellen kann.

Ferner ist dem Arbeitnehmer ausdrücklich untersagt, bei WhatsApp über Umstände, Vorfälle oder Informationen zu schreiben, welche im Rahmen der Tätigkeit bekannt werden. Durch die Kommunikation von Kenntnissen, Daten, Informationen, Vorfällen, Vorgängen oder Geheimnissen kann gegen die vertragliche und/oder gesetzliche Schweigepflicht verstoßen werden und einen Straftatbestand nach § 203 Strafgesetzbuch nach sich ziehen. Dieses Verbot umfasst alle Angaben über Personen, vor allem sensible Daten, wie Kontodaten, Sozialdaten und Gesundheitsdaten. Dieses Verbot schließt sämtlichen Versand von Bildern, Videos oder anderer Dateien ein, welche zu dienstlichen Zwecken oder während des Dienstes angefertigt wurden. Der Arbeitnehmer wird ausdrücklich darüber informiert, dass ein solches Verhalten zu arbeitsrechtlichen oder strafrechtlichen Konsequenzen führen kann, welche von einer Abmahnung über eine Kündigung bis zu einer Strafanzeige führen können.

Vor der Nutzung von WhatsApp sollte sich deshalb stets vor Augen geführt werden, ob der geplante Text eine Offenbarung von fremden Geheimnissen darstellt. Texte die bei WhatsApp geschrieben werden, können niemals vollständig gelöscht werden. Selbst wenn eine Nachricht durch den Verfasser gelöscht wird, bleiben die Daten auf den Servern von WhatsApp gespeichert.

Kontakte

Wenn WhatsApp auf dem Smartphone installiert wird, werden die Daten mit dem Telefonbuch des Smartphones abgeglichen. Das heißt, dass sämtliche Kontakte an WhatsApp weitergegeben werden und theoretisch auch durch Facebook auf die Daten zugegriffen werden kann. Zudem bekommen alle Kontakte, welche auch WhatsApp nutzen, angezeigt, dass sie auch bei WhatsApp registriert sind.

Nachrichtenübertragung

Die Nachrichtenübertragung bei WhatsApp ist zwar verschlüsselt, die Schlüssel sind aber beim Anbieter der App abgelegt. Eine sichere Ende-zu-Ende-Verschlüsselung liegt nicht vor. Hinzu kommt, dass das Unternehmen WhatsApp von Facebook übernommen wurde und stark anzunehmen ist, dass Facebook die Daten aus WhatsApp abzieht bzw. diese mit jenen zusammenführt, die Facebook über seine Nutzer sammelt.

Informationspreisgabe

Wenn die Einstellung bei WhatsApp nicht geändert wird, werden automatisch einige Informationen über den Arbeitnehmer preisgegeben. Theoretisch ist es jedermann möglich, Ihr Profilbild, Ihren Status und den Zeitpunkt einzusehen, an dem Sie zuletzt online waren. In den Einstellungen kann unter der Rubrik Datenschutz eingestellt werden, dass diese Informationen für jeden, nur die eigenen Kontakte oder niemanden einsehbar sind. Diese Einstellungen sollten dringend angepasst werden. Das der Chatpartner sieht, wenn an ihn eine Nachricht geschrieben wird, kann bei WhatsApp nicht ausgestellt werden.

PIN-Eingabe

WhatsApp verfügt über keinen eigenen PIN-Schutz. Deshalb ist es wichtig, dass das Smartphone selbst mit einer sicheren PIN versehen wird. Unbefugte könnten ansonsten die Daten bei WhatsApp einsehen, falls das Gerät verloren geht oder gestohlen wird.

Mit der Unterschrift bestätigen Sie die oben angeführten Risiken von WhatsApp zur Kenntnis genommen zu haben sowie die möglichst datenschutzfreundlichsten Einstellungen vorzunehmen und bei WhatsApp nichts über dienstliche Angelegenheiten zu schreiben.

Bremervörde,

_____

Unterschrift des Arbeitnehmers