# 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.

- 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

Ralf Radons, Großer Platz 12, 27432 Bremervörde, Email: Datenschutzbeauftragter@drk-bremervoerde.de, Telefon: 04761 / 99 37 14