Deutsches Rotes Kreuz

Merkblatt zum Datenschutz

Sehr geehrte(r) Mitarbeiter(in),

es wäre sicherlich nicht in Ihrem Sinne, wenn Daten über Ihre Person und Ihre persönlichen Verhältnisse Unbefugten zur Kenntnis gelangen würden. Davor schützen Sie das Bundesdatenschutzgesetz und andere bereichsspezifische Datenschutzregelungen.

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

Sie sind dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung verarbeitet (erhoben, gespeichert, verändert, übermittelt, gesperrt, gelöscht) oder genutzt werden. Nach der Begriffsbestimmung gemäß §3 Abs.1 BDSG sind unter personenbezogenen Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zu verstehen. Jede Information persönlicher oder sachlicher Natur kann eine Einzelangabe in diesem Sinne sein, sofern sie sich auf eine natürliche Person bezieht. Jeder Missbrauch und jede unbefugte Weitergabe dieser Daten sind unzulässig und strafbar.

Sie wurden auf das Datengeheimnis verpflichtet, das auch nach Beendigung Ihrer Tätigkeit in unserem Unternehmen fortbesteht (§5 BDSG).

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 Paßwort 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.

Vom Verband angeschaffte DV-Geräte aller Art sowie die verbandseigenen DV-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 DV-Geräten, Programmen, CDs, DVDs 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 DV-Geräten einschl. Datenträgern bzw. von DV-Programmen ist außerhalb der Geschäftsräume nicht erlaubt.
Dies gilt nicht für

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

Private DV-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 BenutzerInnen 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!**

Jede(r) AnwenderIn 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, von der/dem BenutzerIn mindestens 6 Monate aufzubewahren.

Von der/dem AnwenderIn sind, falls erforderlich, spezielle Sicherungsmaßnahmen zum Schutz seiner Dateien zu ergreifen.

Dokumentation der individuellen Datenverarbeitung (IDV)

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

(2) Dokumentationspflichtig im Sinne einer Programmdokumentation sind insbesondere solche IDV-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 die/der AnwenderIn selbst, ob eine Programmdokumentation notwendig ist.

(3) Es ist untersagt, geschützte personenbezogene Daten zu einem anderen als zur Erfüllung der satzungsgemäßen Aufgaben zu verarbeiten, zugänglich zu machen oder anderweitig zu nutzen. Dieses Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Verpflichtung der/des IDV-Anwenderin/IDV-Anwenders

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

Das Problem von Computerviren ist bis heute technisch nicht gelöst, so dass jederzeit neue Gefährdungen auftreten können. Insbesondere durch die zunehmende Vernetzung der Systeme (lokal und übergreifend) ist die Übertragung von Rechner zu Rechner sehr schwer zu kontrollieren. Um so 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.

Die Verwendung von Raubkopien ist in unserem Hause strikt verboten!

Das Netzwerk ist durch folgende Maßnahmen abgesichert:

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

2. Bei jeder Anmeldung auf einem der Netzwerke-PC’s wird automatisch eine Virenprüfung gestartet.

3. Die IT-Administration sorgt dafür, dass die jeweils neuesten Virenprüfprogramme installiert sind.

Nach dem neuen Bundesdatenschutzgesetz muss die/der Beauftragte für den Datenschutz eine Vorabkontrolle durchführen, wenn die Einführung neuer Verfahren geplant ist, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen **(Vorabkontrolle).** Diese Risiken gelten immer dann als gegeben, wenn Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben erhoben und verarbeitet werden. Bitte melden Sie dies unbedingt schriftlich an unsere(n) Beauftragte(n) für den Datenschutz und warten seine weitere Stellungnahme ab.

Über das Mailsystem kann jede(r) MitarbeiterIn Daten über das Internet verschicken. Beachten Sie dabei bitte folgende Regeln:

Nutzung des eMail-Systems

1. eMails 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 herkömmliche Übermittlungsarten wie z.B. Briefpost, Fax (nach vorheriger Absprache mit dem Empfänger!) etc. oder bei elektronischem Versand mit Passwort geschützte ZIP-Dateien oder verschlüsselte eMails, um auf Nummer Sicher zu gehen.

2. Bitte öffnen Sie bei eingehenden eMails keine Dateien unbekannter Herkunft, die Ihnen unaufgefordert zugesandt wurden.

3. eMails mit archivierungspflichtigem geschäftlichen Inhalt müssen in Analogie zu sonstigen Anwendungsdateien aufbewahrt werden (Datenspeicherung im zutreffenden Netzlaufwerk, Archivierung in Papierform). Die Verantwortung trägt jede(r) MitarbeiterIn für ihren/seinen Zuständigkeitsbereich.

4. 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 eMails, die nicht eindeutig zu identifizieren sind.

   Empfangene Programme und Anlagen dürfen nicht ungeprüft angewandt werden. Es muss durch die IT-Administrator insbesondere geprüft werden, ob sie frei von Schadfunktionen/Viren sind und keinerlei Kompatibilitätsprobleme bestehen. Die/Der EmpfängerIn 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 die/der AbsenderIn der elektronischen Post informiert werden.

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

Internet-Nutzung

1. Die Nutzung des Internets wird zum dienstlichen Gebrauch eingerichtet.

2. 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.

3. Durch die weltweite Verfügbarkeit des Internets ist es möglich, dass Inhalte des Internets gegen bundesdeutsche Rechtsvorschriften, insbesondere gegen Zivil- und Strafgesetze, verstoßen. Jede(r) BenutzerIn 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/den Beschäftigte(n) weitergeleitet.

4. 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.

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

Bei der Vergabe Ihres persönlichen Paßwortes beachten Sie bitte folgendes:

Sicherheitsstandard für Paßwörter

1. Jede(r) BenutzerIn eines DV-Systems in unserem Hause erhält von der IT-Administration einen individuellen Benutzernamen, der sie/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.

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

3. Die von der/dem BenutzerIn gewählten Paßwörter müssen folgenden Regeln entsprechen:

   a) Sie müssen eine Länge zwischen 6 und 8 Zeichen haben.

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

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

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

      Auf keinen Fall aufschreiben, sondern im Gedächtnis behalten!

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

4. Die Gültigkeitsdauer der Paßwörter ist zeitlich begrenzt. Nach Ablauf dieser Frist wird der/die BenutzerIn automatisch beim nächsten Zugang in das jeweilige System aufgefordert, ein neues Paßwort zu vergeben. Unabhängig davon sollten Sie auch vor Ablauf dieser Frist ein neues Paßwort vergeben, sobald Sie den Verdacht haben, dass ein(e) Dritte(r) von Ihrem Paßwort Kenntnis erlangt hat.

Bei Fragen zum Datenschutz oder in Zweifelsfragen wenden Sie sich bitte an Ihre(n) Vorgesetzte(n) oder an unsere(n) (externe(n))

Datenschutzbeauftragte(n)	Frau / Herrn: _____ Anschrift: _____ Tel.: _____ eMail: _____