BO Nr. 6074 – 23.11.2011
PfReg. B 2.2

Richtlinie für die Nutzung des diözesanen Intranets sowie für die Nutzung von Internet und E-Mail durch Mitarbeiterinnen und Mitarbeiter der Diözese Rottenburg-Stuttgart

Aus Gründen der besseren Lesbarkeit wurde in der Richtlinie die männliche Schreibweise verwendet. Es wird ausdrücklich darauf hingewiesen, dass unter der maskulinen Schreibweise männliche und weibliche Personen zusammengefasst sind.

§ 1 – Geltungsbereich der Richtlinie

(1) Persönlicher Geltungsbereich: Die vorliegende Richtlinie ist für alle Nutzer des Intranets der Diözese Rottenburg-Stuttgart verbindlich. Das Intranet ist die gesicherte Kommunikationsplattform für Einrichtungen in der Diözese Rottenburg-Stuttgart. Dies gilt unabhängig davon, aus welchem Rechtsgrund die Nutzung erfolgt. Die Geltung der Richtlinie wird durch die Nutzung des Intranets konkludent anerkannt.

(2) Sachlicher Geltungsbereich: Die Richtlinie regelt die Nutzung des Intranets der Diözese Rottenburg-Stuttgart, den Umgang mit elektronischer Post (E-Mail) sowie den Gebrauch des Internets, der den Nutzern über das diözesane Intranet ermöglicht wird.

§ 2 – Zweck der Richtlinie

(1) Nutzen: Die Nutzung der Medien Intranet, Internet und E-Mail dient der internen und externen Kommunikation, dem Austausch von Daten und Dokumenten sowie der Informationsgewinnung auf elektronischem Wege. Sie hat das Ziel, Arbeitsabläufe und den Zugang zu Informationen zu verbessern. Die Regelungen der Nutzungsrichtlinie sollen insbesondere
- eine sparsame und effektive Nutzung der elektronischen Medien und der sie vermittelnden technischen Ausrüstung ermöglichen,
- eine störungsfreie und reibungslose Nutzung der Informationstechnik sicherstellen,
- Sicherheitsrisiken minimieren,
- Datenschutz und Rechtskonformität gewährleisten und gleichzeitig
- die Mitarbeiter vor unzulässiger Überwachung schützen.

(2) Sicherheitsrisiken: Angesichts der mit der Nutzung von Internet und elektronischer Post verbundenen Gefahren und Risiken haben die Nutzer zur Sicherstellung eines verantwortungsvollen Umgangs mit diesen Medien deren technische Risiken zu berücksichtigen. Insbesondere ist folgenden Gefahren nach Möglichkeit zu begegnen:
- Es besteht die Gefahr des Ausspähens oder Veränderns elektronischer Nachrichten auf dem Übertragungsweg. Über das Internet übertragenen E-Mails kommt eine Vertraulichkeit zu, die der einer Postkarte vergleichbar ist. Bei unverschlüsselten Nachrichten besteht daher grundsätzlich keine Sicherheit mit Blick auf die Identität des Absenders oder die Authentizität des Inhalts. Daher dürfen nur Nachrichten, die eines entsprechenden Sicherheitsstan-

dards nicht bedürfen, über das Internet versandt und zur Grundlage von Entscheidungen herangezogen werden.

– Zu beachten ist des Weiteren das Risiko einer Schädigung von Daten oder Software durch Viren. Beim Herunterladen von Internet-Seiten oder dem Öffnen von E-Mails können Dateien mit Viren infiziert werden. Viren können sich von selbst weiter verbreiten und Daten manipulieren oder zerstören. Daher ist insoweit größtmögliche Sorgfalt anzuwenden und Anweisungen und Hinweisen der IT-Abteilung der Diözese Folge zu leisten.

– Schließlich besteht auch die Gefahr des Einschleusens von versteckten Programmen. Beim Herunterladen von Internet-Seiten oder dem Öffnen von E-Mails können versteckte Ausführungsprogramme eingeschleust werden mit dem Ziel, Daten oder Passwörter auszuspionieren oder zu manipulieren. Aus diesem Grund sind Maßnahmen zu vermeiden, die erkennbar zu Schäden führen können. Durch die Einrichtung werden dem Nutzer für die dienstliche Nutzung EDV-Systeme zur Verfügung gestellt, die in Ihrer Grundkonfiguration den diözesanen Datenschutzvorgaben entsprechen.[1]

§ 3 – Begriffsbestimmungen

(1) Datenverarbeitung: Unter einer Datenverarbeitung ist jeder Vorgang zu verstehen, der sich auf die Eingabe, Speicherung, Übertragung, Transformation und Ausgabe von Daten bezieht und mittels elektronisch gesteuerten Datenverarbeitungsanlagen erfolgt.

(2) E-Mail: Als eine elektronische Post (E-Mail) wird der asynchrone Austausch von Informationen und Dateien auf elektronischem Wege bezeichnet, wobei die Übertragung im Netz wie bei einer Postkarte öffentlicher Art ist. Gesendete Informationen sind demnach grundsätzlich von jedermann lesbar.

(3) E-Mail-Server: Die E-Mail-Server stellen die elektronischen Postempfangs- und -verteilstellen innerhalb des Netzes dar. An nicht vernetzten Einzelarbeitsplätzen wird die Funktionalität durch den Zugang zum diözesanen Intranet mittels eines abgesicherten virtuellen privaten Netzwerks bereitgestellt.

(4) E-Mail-Gateway: Das E-Mail-Gateway ist der Verbindungspunkt des internen Mailsystems mit dem Internet. Zur Erhöhung der Sicherheit werden alle ein- und ausgehenden Mails an diesem Verbindungspunkt auf Viren überprüft. Die Überprüfung findet vollautomatisch statt. Zusätzlich wird am E-Mail-Gateway eine automatisierte regelbasierte Mail-Weiterleitung an Nicht-drs.de-Adressen unterbunden.

(5) Firewall, Proxy-Server: Die technischen Komponenten der Firewall und des Proxy-Servers sind dem Internet vorgeschaltet, um unberechtigte Zugriffe (Hacker) aus dem Internet vom diözesanen Intranet abzuwehren und erwünschte Kontakte simultan auf Viren zu überprüfen. Um ungerechtfertigten Anschuldigungen gegen die Diözese oder ihre Mitarbeiter begegnen zu können, ist eine Protokollierung aller Nutzer-Aktionen (Verkehrsdaten) bezogen auf den Durchgang zum Internet erforderlich. Für einzelne Benutzergruppen kann dort der Zugriff auf bestimmte Web-Inhalte über ein Inhaltsfilter zusätzlich eingeschränkt werden.

(6) Internet: Das Internet ist ein weltweites, elektronisches Netzwerk aus voneinander unabhängigen einzelnen Netzwerken. Es umfasst damit eine Gesamtheit von öffentlichen, standardisierten Diensten. Hierzu zählen insbesondere

[1] Nähere Informationen zu dieser Richtlinie, Antworten auf häufig gestellte Fragen zur Richtlinie, sowie Beispiele zu den möglichen Gefahren finden Sie im Mitarbeiter-Portal unter der Web-Adresse https://www.map.drs.de/index.php?id=INR

- E-Mail: weltweiter Nachrichtenaustausch
- http (www): weltweite Informationsveröffentlichung und Suche (World Wide Web)
- ftp: weltweites Verteilen / Kopieren von Dateien
- News: weltweiter Zugang zu speziellen Diskussionsforen

Der Zugang zum Internet wird im Rahmen des diözesanen Intranets zur Verfügung gestellt. Der Übergang vom diözesanen Intranet in das externe Internet wird durch ein Firewall-System geschützt.

(7) World Wide Web (www): Das World Wide Web umfasst die Gesamtheit aller Rechner und Informationen, zu denen in weltumspannender, weitgehend unkontrollierter Form kostenlos oder gegen Gebühr Zugang gewährt wird.

(8) Intranet: Das Intranet ist ein Rechnernetzwerk, das auf den gleichen Techniken wie das Internet basiert, jedoch nur von einer festgelegten Gruppe von Mitgliedern einer Organisation genutzt wird. Das Intranet der Diözese Rottenburg-Stuttgart soll als ein diözesanweites sicheres Kommunikationsmedium zur Beschaffung und Bereitstellung von Informationen genutzt werden. Mitarbeiter innerhalb der Diözese erhalten Zugang zum Intranet der Diözese.

(9) drsIntra: Unter dem drsIntra ist das diözesane Intranet der Diözese Rottenburg-Stuttgart zu verstehen. Der Zugang steht lediglich einem beschränkten Anwenderkreis offen, der sich über Benutzerkennung und Passwort autorisiert. Zum drsIntra zählen zunächst alle Geräte und / oder Verbindungen, die es ermöglichen, zwischen zwei oder mehr Computern in kirchlichen Dienststellen der Diözese Rottenburg-Stuttgart Signale zu senden, empfangen, übertragen oder zu vermitteln, ohne das Internet bzw. Dienste Dritter zu nutzen. Benutzer von drsIntra können über eine Firewall in das Internet gelangen.

(10) Virtuelles Privates Netzwerk (VPN): Das Virtuelle Private Netzwerk (VPN) stellt eine Technologie für den Zugang zu einem Intranet dar. Die Daten werden nach der Einwahl über eine verschlüsselte Datenstrecke direkt zum Serverstützpunkt des Intranet geleitet. Bei drsIntra wird das VPN durch ein gesichertes Netz der Firma „T-Systems“ betrieben. Die zentralen Serverstützpunkte sind in zwei Rechenzentren am Standort Rottenburg.

(11) Update-Dienste: Durch Betriebssystem- und andere Software-Hersteller werden über Update-Dienste automatisiert neue Versionen ihrer Software angeboten, die Lösungen für neu entdeckte Sicherheitslücken in deren Software schließen. Mit dem Intranet verbundene PC-Systeme sind zur Aufrechterhaltung der Sicherheit mit aktivierten Update-Diensten zu betreiben.

(12) Fernwartung: Fernwartungsprogramme ermöglichen es dem entfernt sitzenden Servicetechniker, direkt auf dem zu wartenden Rechnern Aktionen durchzuführen. Tastaturanschläge, Mausbewegungen und Bildschirminhalt werden übertragen. Der Servicetechniker sieht die Bildschirmausgabe auf dem eigenen Bildschirm. Manche Fernwartungsprogramme verfügen darüber hinaus über Möglichkeiten zur direkten Übertragung von Dateien zwischen den beiden verbundenen Rechnern.

(13) sTransfer-Plattform: Die Diözese stellt unter der Internet-Adresse sTransfer.drs.de eine Plattform zur sicheren und datenschutzkonformen Übertragung von Dokumenten / Dateien an Nutzer außerhalb des diözesanen Intranet zur Verfügung. Eine Nutzungsanleitung ist auf der sTransfer-Startseite hinterlegt.

§ 4 – Verantwortlichkeit des Internet-Nutzers

(1) Beachtung der Sicherheitsstandards: Technische Maßnahmen (insbesondere Firewall, Virenschutz und Updatedienste) begrenzen die Risiken aus der Nutzung des Internets. Grundsätzlich hat jeder Nutzer Maßnahmen zu unterlassen, die die Wirkung dieser technischen Mittel beein-

trächtigen können. Sind Umstände erkennbar, die für den Einsatz und die Funktionsfähigkeit dieser Technik von Bedeutung sind, ist unverzüglich die IT-Abteilung des Bischöflichen Ordinariats der Diözese zu informieren.

(2) Ausschluss eines Missbrauchs der Nutzung: Eine Nutzung der Medien des Internets zu Zwecken, die das Ansehen der Diözese in der Öffentlichkeit schädigen oder gegen geltende Rechtsvorschriften verstoßen kann, ist zu unterlassen. Insbesondere ist das Abrufen, Nutzen oder Verbreiten von Inhalten, die gegen Normen des staatlichen und kirchlichen Rechts, datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, sowie das Abrufen, Nutzen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen oder pornografischen Äußerungen, Darstellungen oder Abbildungen untersagt.

(3) Nutzung ausschließlich zu dienstlichen Zwecken: Das Medium des Internets ist stets verantwortungsvoll, sparsam und wirtschaftlich sowie grundsätzlich nur für dienstliche Zwecke zu nutzen. Davon unberührt bleibt der Abschluss einer Dienstvereinbarung nach § 38 MAVO zur eingeschränkten privaten Nutzung.

§ 5 – Pflichten im Umgang mit elektronischer Post (E-Mail)

(1) Versendung und Bearbeitung von E-Mails: Für den Umgang mit elektronischer Post ist jeder Benutzer primär selbst verantwortlich. Er hat deshalb allein Zugriff auf seine E-Mails und über deren Verwendung und Bearbeitung eigenverantwortlich zu entscheiden. Dienstliche Weisungen der Vorgesetzten, allgemeine Anordnungen der Dienstleitung und der IT-Abteilung im Rahmen ihrer Zuständigkeit sowie die geltenden Regeln der Schriftgutverwaltung sind zu beachten. Jeder Besitzer eines E-Mail-Kontos hat regelmäßig seine E-Mails zu bearbeiten. Diese Regelmäßigkeit ist bei einer täglichen Bearbeitung bzw. an den nach Dienstplan zu arbeitenden Tagen gewährleistet. Zur Vertretung in Urlaubs- und Abwesenheitsfällen kann der Besitzer eines E-Mail-Kontos eine Person seines Vertrauens damit beauftragen, seine E-Mails zu bearbeiten. Ferner kann er automatisch dem Absender mitteilen lassen, dass er abwesend ist und die E-Mails vorübergehend nicht bearbeitet oder innerhalb des Intranet an ein anderes Mailkonto weitergeleitet werden. Die Entscheidung ist nach pflichtgemäßem Ermessen im Rahmen der jeweils geltenden Postordnung zu treffen. Das E-Mail-System ist so konfiguriert, dass bei E-Mails innerhalb der diözesaneigenen Domäne „drs.de“ die Identität des Absenders sowie die Authentizität des Inhaltes im Sinne des Datenschutzes gewährleistet sind. Dies ist bei der Bearbeitung von E-Mails zu beachten.

(2) Vermeidung von Rechtsverstößen: Eine Nutzung der elektronischen Post zu Zwecken, die das Ansehen der Diözese in der Öffentlichkeit schädigen oder gegen geltende Rechtsvorschriften verstoßen kann, ist zu unterlassen. Insbesondere hat jeder Nutzer zu beachten, dass das mittels elektronischer Post erfolgende Nutzen oder Verbreiten von Inhalten, die gegen Normen des staatlichen und kirchlichen Rechts verstoßen oder datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verletzen, grundsätzlich untersagt ist. Ebenso untersagt ist das Nutzen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen oder pornografischen Äußerungen, Darstellungen oder Abbildungen durch die Versendung von E-Mails. Als Standard-Mailadresse ist für die dienstliche Nutzung die Einrichtungs-Mailadresse oder eine spezielle Bereichs-Mailadresse zu nutzen.

(3) Besondere Maßgaben bei elektronischer Post außerhalb der diözesaneigenen Domäne „drs.de“: Ein E-Mail-Empfänger befindet sich außerhalb der diözesaneigenen Domäne, wenn die E-Mail-Adresse nicht die Endung „drs.de“ aufweist. Besitzt ein E-Mail-Empfänger mehrere Adressen, ist nach Möglichkeit die mit „drs.de“ endende Adresse zu verwenden. Befindet sich ein E-Mail-Empfänger außerhalb der diözesaneigenen Domäne, so sind vertrauliche Vorgänge sowie schutzwürdige personenbezogene oder datenschutzrelevante Daten nicht oder nur über eine gesicherte Plattform wie sTransfer.drs.de zu übermitteln. Über das Internet erhaltene elektronische Post mit auffälligen Betreffzeilen, Anhängen oder unbekannten Absendern ist vorsichtig zu handhaben. Sind Anzeichen für das Vorliegen von Gefahren ersichtlich, die von solchen E-Mails für das Intranet und dessen Nutzer sowie für die Informationstechnik ausgehen können, ist nach pflichtgemäßem Ermessen der Benutzerservice der IT-Abteilung zu informieren.

(4) Vertretungsregelungen: Um eine zeitnahe Bearbeitung der dienstlichen E-Mail sicherzustellen sind für das Einrichtungs-Mailkonto Vertretungszugriffe einzurichten. Für das persönliche Mailkonto ist durch den Nutzer sicherzustellen:

- Bei vorhersehbarer Abwesenheit (Fortbildung, Urlaub) ist eine Abwesenheitsregel mit automatischer Rückantwort über den Abwesenheitszeitraum zu aktivieren oder alternativ einem Vertreter Zugriff auf das E-Mail-Konto einzuräumen.
- Bei längerer, nicht vorhersehbarer Abwesenheit ist, sofern nicht bereits Vertretungsrechte eingeräumt wurden, umgehend vom Vorgesetzten die Intranet-Hotline zu informieren, damit dort auf schriftlichen Antrag des Vorgesetzten eine Abwesenheitsregel auf dem betreffenden Mailkonto eingerichtet wird.

§ 6 – Maßgaben für die Nutzung des diözesanen Intranets und dienstlicher Hard- und Software

(1) Schutz technischer Vorrichtungen: Die Einpflege zusätzlicher Software oder anderer Dienste im Intranet der Diözese Rottenburg Stuttgart bedarf der vorherigen Zustimmung derselben. Eine Einstellung von Programmen oder Programmteilen mit Schadensfunktion oder Reproduktion (Viren) oder von Programmen, die Inhalte umfassen, die andere Rechner manipulieren, beeinträchtigen oder beschädigen können, ist untersagt. Die Nutzung privater Datenverarbeitungssysteme, Datenträger und Programme zu dienstlichen Zwecken ist lediglich dann zulässig, wenn sie zur Erfüllung der dienstlichen Aufgaben unabweislich oder zwingend geboten ist und eine Genehmigung der Diözese eingeholt wurde. Eine Nutzung von Datenverarbeitungssystemen der Dienststelle für private Zwecke ist unzulässig. Ihre Nutzung für dienstliche Zwecke außerhalb der Dienstselle bedarf der Genehmigung. Der Zugang zum Intranet darf über lokale technische Installationen (z. B. Router) nicht direkt an das Internet weitergeleitet werden. Die erteilten Zugangsberechtigungen sind personenbezogen und als vertraulich zu behandeln.

(2) Urheberrechtsschutz und Recht am eigenen Bild: Bei der Verwertung von geschützten Werken im Sinne des Urheberrechtsgesetzes, zu denen insbesondere Bilder, Texte, Tondokumente und Software-Programme zählen, sind die geltenden urheberrechtlichen Bestimmungen zu beachten. Die Publikation von Bildern von Personen bedarf der vorherigen Einwilligung der betreffenden Personen. Letzteren steht das sogenannte Recht am eigenen Bild zu, dem grundsätzlich Vorrang vor dem Informationsinteresse der Öffentlichkeit zukommt.

(3) Datenschutzrechtliche Bestimmungen: Vor der Publikation personenbezogener Daten ist ihre Vereinbarkeit mit den geltenden Bestimmungen zum Datenschutz zu überprüfen. Hierbei sind die Vorschriften der Anordnung über den kirchlichen Datenschutz (KDO) in der jeweils gültigen Fassung zugrunde zu legen.[2] Das Kopieren von Datenträgern oder einzelnen Dateien ist lediglich zu Zwecken der Datensicherung und Programmpflege sowie ausnahmsweise auch zum Zweck einer aus dienstlichen Gründen erforderlichen Weitergabe an Dritte jeweils unter Beachtung der datenschutzrechtlichen Bestimmungen zulässig. Sobald Datenträger oder Dateien zur Erfüllung der Aufgaben des Nutzers nicht mehr benötigt werden und keine zwingenden dienstlichen Gründe für deren Aufbewahrung sprechen, sind aus Gründen des Datenschutzes personenbezogene Daten zu vernichten.

§ 7 – Protokollierung von Daten

Für die Protokollierung von Daten und der Verwendung der Protokolldaten findet die zwischen der Diözese Rottenburg-Stuttgart und der DiAG-MAV abgeschlossene Dienstvereinbarung zur Nutzung aller informationstechnischen Einrichtungen (BO Nr. A 1683 – 15.07.2009), veröffentlicht im Kirchlichen Amtsblatt Nr. 15 / 2009, entsprechende Anwendung.

§ 8 – Fernwartung

(1) Schutz vor unberechtigtem Zugriff: Aus Gründen des Datenschutzes und der Datensicherheit muss stets gewährleistet sein, dass ein Zugriff auf einzelne Rechner in Einrichtungen der Diözese mittels Fernwartung nicht ohne die explizite Zustimmung oder Beteiligung des aktuell angemeldeten Benutzers erfolgen kann. Nach Abschluss der Fernwartung ist die Verbindung zu deaktivieren. Dies gilt nicht für zentrale Service-Systeme, die durch die IT-Abteilung der Diözese regelmäßig gewartet werden.

(2) Umfang der Fernwartung: Bei der Fernwartung darf lediglich auf diejenigen Programme sowie auf die diesen Programmen zugeordneten Daten zugegriffen werden, für die eine Fernwartung vereinbart wurde. Der die Wartungsarbeiten freigebende Sachbearbeiter hat die Einhaltung der datenschutzrechtlichen Bestimmungen zu gewährleisten.

§ 9 – Möglichkeiten der Weiterbildung

Die Gewährleistung eines effizienten und verantwortungsvollen Umgangs mit den informationstechnologischen Medien setzt eine sachgerechte Nutzung derselben durch die Mitarbeiter der Diözese voraus. Jedem Benutzer des diözesanen Intranets sind daher passende Schulungsangebote zu unterbreiten.

§ 10 – Fortschreibung der Nutzungsrichtlinie

Bei grundsätzlichen technologischen Veränderungen oder Veränderungen bei der Speicherung oder Auswertung von Daten ist die Nutzungsrichtlinie zu überarbeiten und fortzuschreiben.

---

[2] Die jeweils gültige Fassung der Anordnungen über den kirchlichen Datenschutz wird im Kirchlichen Amtsblatt veröffentlicht und kann in der Internet-Rechtssammlung der Diözese unter der Internet-Adresse http://www.drs.de/index.php?id=776 abgerufen werden.

§ 11 – Mitarbeitervertretung

Die Diözesane Arbeitsgemeinschaft wurde zur vorliegenden Fassung der Nutzungsrichtlinie gemäß § 29 MAVO Abs. 1 Ziffer 1, 3 und 15 beteiligt.

§ 12 – Inkrafttreten

Die Nutzungsrichtlinie tritt mit der Veröffentlichung im Kirchlichen Amtsblatt der Diözese Rottenburg-Stuttgart in Kraft. Nach Inkraftsetzung wird die Richtlinie allen Nutzern des diözesanen Intranets, neben der Veröffentlichung im Kirchlichen Amtsblatt, über eine direkte Mail-Zusendung an deren drs.de-Mailadresse bekanntgemacht.[3]

Rottenburg, den 23.12.2011

Dr. Clemens Stoppel
Generalvikar

[3] Mit Inkrafttreten wird den Nutzern ein erläuterndes Informationsblatt im Mitarbeiterportal unter der Adresse https://www.map.drs.de/index.php?id=inr zur Verfügung gestellt. Das Informationsblatt wird ergänzend zur Richtlinie nach Inkrafttreten und bei jeder neuen Fassung an alle Intranet-Nutzer per E-Mail versandt.