

Kirchliches Amtsblatt

FÜR DIE DIÖZESE FULDA

Fernsprechnummer: (06 61) 87-0

Telefax: (06 61) 87-578

STÜCK IV

FULDA, DEN 18. März 2002

118. JAHRGANG

Nr. 51 EDV-Ordnung

Nr. 52 Geschäftsordnung

Nr. 51 EDV-Ordnung des Bistums Fulda

Inhaltsverzeichnis

1. Allgemeines	2
1.1. Geltungsbereich und Zweck	2
1.2. Datenschutz und rechtliche Qualifikation von E-Mail ..	2
2. Begriffsbestimmungen und Grundsätze der Netzverwaltung	3
2.1. Nutzungsberechtigung	3
2.2. Zugangsberechtigung	3
2.3. Zugriff	3
2.4. Elektronische Kommunikation	3
2.5. Firewall	3
2.6. Organisationseinheiten und Einrichtungen	4
3. Nutzungsberechtigung	4
3.1. Allgemeines	4
3.2. Erwerb, Änderung und Beendigung der Nutzungs- und Zugangsberechtigung	5
4. Dienstliche und private Nutzung	5
5. Sicherheitsregeln	6
5.1. Allgemeines	6
5.2. Sicherheitspflichten der Anwender	6
6. Nutzung von Dateiablagen	7
6.1. Allgemeines	7
6.2. Gemeinsame Dateiablage	7
6.3. Einzelablage von Dateien	8
6.4. Schutzbereich des Bischofs	8
7. Elektronische Kommunikation	8
7.1. Allgemeine Hinweise	8
7.2. Teilnahme auswärtiger Stellen am internen Kommunikationssystem	9
7.3. Bedeutung der E-Mail-Funktion	9
8. Einsatz von Software	9
8.1. Allgemeines	9
8.2. Kategorisierung und Meldung von Software	9
8.3. Anzeigepflicht	10
8.4. Durchführung der Kategorisierung	10
9. EDV-Systemverwaltung	11
9.1. Allgemeines	11
9.2. EDV-Fachbeauftragte	11
9.3. EDV-Systemverwaltung	11
9.4. Systempflege und Entstörungsmaßnahmen	11
9.5. Benutzerunterstützung, Beratung und Schulungen ..	13
10. Organisatorische und technische Sicherheitsüberwachung ..	13
11. Datenschutzbeauftragter	13

1. Allgemeines

1.1. Geltungsbereich und Zweck

- (1) Diese Ordnung regelt die Bedingungen für den Einsatz und die Nutzung der elektronischen Datenverarbeitung (EDV), insbesondere im Bereich vernetzter Kommunikationsmedien in den Verwaltungen des Bistums und der der bischöflichen Aufsicht unterstehenden Rechtsträger und Einrichtungen. Voraussetzung für ihre Anwendung ist, dass die jeweilige gesetzliche Vertretung des Rechtsträgers oder die Leitung einer kirchlichen Einrichtung die EDV-Nutzung beschlossen und die Nutzungsberechtigung für die Mitarbeiterinnen und Mitarbeiter festgelegt hat. Die Nutzungsberechtigung darf im Einzelfall nur gewährt werden, wenn der oder die betreffende Person sich zuvor verpflichtet hat, diese EDV-Ordnung und sonstige Nutzungsvorschriften zu beachten. Andernfalls gilt die Nutzungsberechtigung als nicht erteilt.
- (2) Die Einrichtung und Nutzung von EDV und elektronischen Informationsmedien soll dazu dienen, die organisatorischen Abläufe effizienter zu gestalten und die Arbeitsmöglichkeiten der sie nutzenden Personen zu optimieren mit dem Ziel, die Aufgabenerfüllung der Verwaltungsstellen und Einrichtungen für den Dienst am Menschen und die kirchlichen Aufgaben zu verbessern. Jeder der die elektronischen Kommunikationsmedien und Techniken nutzt, ist verpflichtet, sie so zu gebrauchen, dass Art und Weise ihrer Nutzung und das mit der Nutzung erzielte Arbeitsergebnis nicht gegen die Interessen des kirchlichen Dienstgebers und die Lehre der katholischen Kirche (Loyalitätspflichten) verstößt.
- (3) Diese Ordnung gilt für den Einsatz von EDV-Anlagen und die Nutzung elektronischer Kommunikationstechnologien, insbesondere in Netzwerken durch:
 1. das Bistum, die Kirchengemeinden und die Kirchengemeindeverbände;
 2. den Diözesan-Caritasverband, seine Untergliederungen und ihm zuzuordnende Fachverbände, ohne Rücksicht auf ihre Rechtsform;
 3. die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und sonstige kirchliche Rechtsträger, ohne Rücksicht auf ihre Rechtsform.

Andere Rechtsträger, die nicht dem Diözesanbischof unterstehen, können durch Entscheidung ihrer zuständigen Organe diese Ordnung übernehmen.

- (4) Diese Ordnung regelt nicht die Frage, ob in einer Verwaltungsstelle oder Einrichtung EDV-Anlagen und elektronische Kommunikationstechniken eingesetzt und welche Personen oder Stellen zu ihrer Nutzung zugelassen werden. Soweit bei diesen Entscheidungen nach Abs. 1 Satz 1 Rechte der Mitarbeitervertretung nach § 36 Abs. 1 Nr. 9 und 10, sowie § 37 Abs. 1 Nr. 9 und 10 MAVO betroffen sind, bleiben diese unberührt. In diesen Fällen ist möglichst die Regelung durch eine Dienstvereinbarung nach § 38 MAVO anzustreben.

1.2. Datenschutz und rechtliche Qualifikation von E-Mail

- (1) Jeder Nutzer von EDV-Anlagen und elektronischer Kommunikationstechnologie ist verpflichtet, daran mitzuwirken, dass der Schutz personenbezogener Daten gewährleistet bleibt. Die Anordnung über den kirchlichen Datenschutz und die hierzu ergangenen Ausführungsbestimmungen sind in ihrer jeweiligen Fassung zu beachten. Zur Zeit gilt die Anordnung über den Kirchlichen Datenschutz vom 07. Februar 1994 (Kirchl. Amtsblatt 1994, Nrn. 36, 75, 90, 137), die aufgrund dieser Anordnung ergangenen weiteren Ausführungsbestimmungen sowie die Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Fulda vom 30. August 1995 (Kirchl. Amtsblatt 1995, Nr. 121). Zweifelsfälle können über die Leitung der betreffenden Einrichtung dem Datenschutzbeauftragten des Bistums vorgelegt werden, der in seinem Zuständigkeitsbereich gemäß den geltenden Vorschriften eine Entscheidung des vorgelegten Falles treffen kann.
- (2) Soweit nicht durch anderweitige Anordnung (z. B. Einzelweisung oder Dienstanweisung) für die jeweilige Organisationseinheit oder Einrichtung festgelegt, gelten elektronisch ausgetauschte Informationen, insbesondere durch E-Mails als ein flüchtiges Medium für die schnelle und formlose Kommunikation untereinander. Elektronische Informationen sind in diesen Fällen daher nicht als alleiniges Medium für die Übermittlung von rechtsverbindlichen Vorgängen zu verwenden.

2. Begriffsbestimmungen und Grundsätze der Netzverwaltung

2.1. Nutzungsberechtigung

Nutzungsberechtigung im Sinne dieser Ordnung wird durch die schriftliche Verfügung der zuständigen Leitung einer Organisationseinheit oder Einrichtung erteilt. Hierdurch wird eine Person (Anwender) berechtigt, in der rechtlich vorgeschriebenen Weise die EDV und die elektronischen Kommunikationseinrichtungen der Organisationseinheit oder Einrichtung zu nutzen.

2.2. Zugangsberechtigung

Zugangsberechtigung im Sinne dieser Ordnung ist die Kombination aus einem Benutzernamen (Benutzerkennung) und einem geheimen Passwort (Kennwort), die aufgrund einer erteilten Nutzungsberechtigung ausgegeben wird. Die Kenntnis von Benutzerkennung und Kennwort ist notwendig, um Zugriff auf den EDV-Anlagen zu erhalten.

2.3. Zugriff

Der Zugriff im Sinne dieser Ordnung ist die tatsächliche technische Nutzung der EDV oder der elektronischen Kommunikationssysteme.

2.4. Elektronische Kommunikation

Im Sinne dieser Ordnung ist elektronische Kommunikation, die mit Hilfe von elektronischen Datenverarbeitungsanlagen betriebsintern oder -extern durchgeführte oder versuchte Informationsübermittlung zwischen mindestens zwei Personen. Dabei können nach dem derzeitigen Stand der Technik unter Nutzung der in einer Organisationseinheit oder Einrichtung vorhandenen vernetzten oder nicht vernetzten EDV-Anlagen vor allem folgende Dienste genutzt werden:

1. Internetdienste zum Transfer von Web-Seiten und damit verknüpften Daten z.B. mit Hilfe des Protokolls HTTP (Hyper Text Transfer-Protokoll);

2. E-Mail (Elektronic-Mail) - Internetdienste zum Versenden und zum Empfangen von elektronischen Nachrichten.

3. FTP (File Transfer-Protokoll) - ein Internetdienst zur Übertragung von Dateien von und zu entfernten Rechnern;

4. Telnet - Ein Internetdienst zum Einloggen und Arbeiten auf einem entfernten Rechner.

Die Aufzählung der vorgenannten Internetdienste ist lediglich als beispielhaft zu verstehen.

2.5. Firewall

Eine Firewall ist eine Kombination von Hardware- und Softwarekomponenten und bezeichnet ein Konzept zur Abgrenzung und zum Schutz des internen Netzes vom Internet. Das geschieht z.B. durch Kontrolle und Protokollierung des Datenverkehrs und der Dienste (Filterung etc.). Die Systemkonfiguration und die Filterregeln müssen gewährleisten, dass nur die erlaubten Verbindungen zugelassen werden. Es ist das unter den gegebenen finanziellen Möglichkeiten des jeweiligen Rechtsträgers technisch sicherste Konzept zu installieren.

2.6. Organisationseinheiten und Einrichtungen

Organisationseinheiten im Sinne dieser Ordnung sind das Bischöfliche Generalvikariat, seine Abteilungen, der Geschäftsbereich des Bischofs, das Offizialat und die nicht mit eigener Rechtspersönlichkeit versehenen selbständig geführten Dienststellen des Bistums und des Bischöflichen Stuhls.

Unter Einrichtung wird die Dienststelle einer kirchlichen Körperschaft oder eines sonstigen selbständigen Rechtsträgers sowie ein selbständig geführter Betrieb der Kirchengemeinden, Kirchengemeindeverbände, des Diözesan-Caritasverbandes, seiner Regionalverbände und zugeordneten Fachverbänden, der öffentlichen juristischen Personen des kanonischen Rechts sowie der sonstigen, dem Diözesanbischof gesetzlich zugeordneten Rechtsträger, unabhängig von der Rechtsform, verstanden.

Soweit mehrere Organisationseinheiten oder Einrichtungen ein gemeinsames internes Netzwerk haben, ist die technische Systemverwaltung von einer Stelle aus einheitlich zu organisieren. Soweit keine anderweitige Absprache zwischen den beteiligten Einrichtungen und Organisationseinheiten besteht, wird zum Zeitpunkt ihrer Schaffung die Stelle bei der Einheit oder Einrichtung angesiedelt, bei der die meisten Zugangsberechtigungen bestehen. Die Kosten für die technische Einrichtung und Verwaltung eines gemeinsamen Netzwerkes sind mangels anderweitiger Absprachen nach dem Verhältnis der zum letzten Kalenderjahresende bestehenden Zugangsberechtigungen zu verteilen.

3. Nutzungsberechtigung

3.1. Allgemeines

- (1) Die Nutzungsberechtigung für die EDV-Anlagen und die elektronischen Kommunikationssysteme erteilt die

jeweilige Leitung einer Organisationseinheit oder Einrichtung nach den jeweils gegebenen dienstlichen oder betrieblichen Erfordernissen. Für das Bischöfliche Generalvikariat und andere einbezogene Dienststellen gelten die diesbezüglichen Regelungen der Geschäftsordnung des Bischöflichen Generalvikariats. Der Generalvikar ist ermächtigt, erforderlichenfalls für die Organisationseinheiten des Bistums und die Einrichtungen der kirchlichen Rechtsträger weitere Ausführungsbestimmungen zu erlassen.

- (2) Die Zugangsberechtigung besteht aus einer aufgaben- oder personenbezogenen Benutzerkennung (Adresse) und einem geheimen Passwort, für dessen Geheimhaltung der Zugangsberechtigte stets Sorge zu tragen hat. Dieses Passwort ist keiner anderen Person, weder einem Dienstvorgesetzten noch einem anderen Mitarbeiter /einer anderen Mitarbeiterin mitzuteilen. Für den gemeinsamen Zugriff auf Ressourcen mehrerer Personen hat die Leitung einer Organisationseinheit oder Einrichtung spezielle Anordnungen und technische Voraussetzungen zu schaffen.
- (3) Die technische Systemverwaltung hat dafür Sorge zu tragen, dass nur den Personen die Zugangsberechtigung gewährt wird, die eine Nutzungsberechtigung nach Absatz 1 haben. Alle Unterlagen, die die Errichtung, Änderung oder Löschung von Nutzungs- und Zugangsberechtigungen betreffen, sind schriftlich der zuständigen Systemverwaltung vorzulegen. Die Systemverwaltung archiviert diese Anträge, Berechtigungsnachweise und sonstige relevante Unterlagen und dokumentiert die daraufhin durchgeführten technischen Änderungen.
- (4) Mit dem Antrag auf Zuteilung der technischen Zugriffsvoraussetzungen gibt der Zugriffsberechtigte eine Verpflichtungserklärung nach einem festzulegenden Muster ab, in der er sich verpflichtet, diese Ordnung sowie die sonstigen für die jeweilige Organisationseinheit oder Einrichtung bestehenden relevanten Vorschriften zu beachten. Er bestätigt dabei, über die Anforderungen des Datenschutzes unterrichtet zu sein und ein Exemplar der jeweils gültigen Fassung der EDV-Ordnung erhalten zu haben.

3.2. Erwerb, Änderung und Beendigung der Nutzungs- und Zugangsberechtigung

- (1) Soweit die Nutzungsberechtigung nicht nach Ziff. 3.1. Abs. 1 durch entsprechende eigene Bestimmungen der Leitungen von Organisationseinheiten und Einrichtungen über Erwerb, Änderung und Beendigung geregelt ist, gelten subsidiär die folgenden allgemeinen Vorschriften:
 - a) Die Nutzungsberechtigung und ihre Änderung erfolgt stets aufgrund eines Antrags an das Vertretungsorgan des betreffenden Rechtsträgers oder die von diesem beauftragten Stellen. Benötigt der Antragsteller lediglich Zugriff auf die Ressourcen einer Abteilung oder vergleichbaren Unterteilung einer Organisationseinheit oder Einrichtung, so muss der Antrag über den/die zuständige Leiter/ Leiterin dieser Einheit gestellt und befürwortet werden. Benötigt ein Anwender Zugriff auf die Ressourcen mehrerer Unterteilungen einer Organisationseinheit oder Einrichtung, so ist das Benehmen der jeweils zuständigen Stellenleiter erforderlich, was zu vermerken ist.

Die Gewährung einer Nutzungsberechtigung kann zeitlich befristet werden. Bei einer Befristung sperrt die EDV-Systemverwaltung die Zugangsberechtig-

ung automatisch zum Ende des genehmigten Zeitraums. Für den Zugriff auf das Internet und besondere Dienste ist im Rahmen der Zugangsberechtigung eine entsprechende gesonderte Berechtigung erforderlich. Die zuständige technische EDV-Systemverwaltung weist dem/der Zugangsberechtigten die vorgesehene individuelle oder sachbezogene Benutzerkennung und ein anfängliches Passwort zu, das von dem/der Zugangsberechtigten sofort nach Erhalt zu ändern ist.

Die EDV-Systemverwaltung wählt die Benutzerkennung nach technischen Kriterien. Ein Recht auf die Zuweisung eines bestimmten Benutzernamens besteht nicht.

- b) Benötigt ein Anwender Zugriff auf einen geänderten Satz von Ressourcen (z. B. aufgrund Abteilungswechsel, neue Aufgabenbereiche), ist ein Änderungsantrag einzureichen. Um sicherzustellen, dass die neue Zuweisung von Ressourcen korrekt ist, ist analog zu vorstehendem Buchstaben a) für die geänderte Zugangsberechtigung das Benehmen mit allen betroffenen internen Stellenleitern erforderlich. Die EDV-Systemverwaltung ändert die Nutzungsberechtigung in der Weise, dass der Anwender lediglich Zugang auf die in der Zugangsberechtigung bezeichneten Ressourcen erhält. Die Berechtigung für alle weiteren Ressourcen wird entzogen.
 - c) Ist ein Anwender nicht mehr berechtigt auf Ressourcen zuzugreifen, so ist dies von der zuständigen Leitung an die EDV-Systemverwaltung zu melden, die die Zugangsberechtigung sperrt. Entsprechendes gilt, wenn die Nutzungsberechtigung teilweise entzogen wird.
- (2) Die EDV-Systemverwaltung berichtet den zuständigen Leitungen der Organisationseinheiten und Einrichtungen in der Regel einmal jährlich oder auf Anforderung über die bestehenden Nutzungs- und Zugangsberechtigungen. Die Leitung prüft die Nutzungsberechtigung und teilt der EDV-Systemverwaltung mit, wenn Nutzungs- und Zugangsberechtigung nicht übereinstimmen.

4. Dienstliche und private Nutzung

Soweit in einer Organisationseinheit oder Einrichtung die rechtlichen oder organisatorischen Voraussetzungen (Datenschutz, MAV-rechtliche Voraussetzungen usw.) für private Nutzungen nicht vorliegen, dürfen die EDV einschließlich der elektronischen Kommunikationssysteme - gleichgültig ob vernetzt oder nicht vernetzt - nur dienstlich genutzt werden. Die Privatnutzung ist dann möglichst technisch/organisatorisch auszuschließen und den Mitarbeiter/innen untersagt.

5. Sicherheitsregeln

5.1. Allgemeines

Über EDV und elektronische Kommunikationsmedien werden Informationen verarbeitet, die hohe Anforderungen an den Datenschutz stellen. Daher sind die nachfolgenden grundlegenden Sicherheitsrichtlinien, die den unbefugten Zugriff auf die EDV und die gespeicherten Informationen verhindern sollen, unbedingt zu beachten. Insbesondere sind alle Anwender und mit der Systemverwaltung beauftragten Stellen verpflichtet, ihnen bekannte Sicherheitsprobleme, die zu einem nichtautorisierten Zugang zu den in der EDV-Anlage gespeicherten Informationen führen können, unverzüglich an den Leiter der Organisationsein-

heit oder Einrichtung und die EDV-Systemverwaltungsstelle weiterzugeben.

5.2. Sicherheitspflichten der Anwender

- (1) Das mit der Zugangsberechtigung erhaltene Passwort zum Zugriff auf die Anlage ist vom Anwender geheim zu halten. Es darf unter keinen Umständen an andere Personen (Kollegen, Dritten) weitergegeben werden. Das Passwort soll vom Anwender in regelmäßigen Abständen (alle 6 Monate) geändert werden. Für das zu wählende Passwort gelten, soweit nichts anderes festgelegt wurde, folgende Regeln:

- es muss mindestens 6 Zeichen enthalten, von denen 2 Zeichen keine Buchstaben sind;
- nach mehreren aufeinanderfolgenden, fehlerhaften Eingaben wird die Zugangsberechtigung automatisch gesperrt; die Anzahl der Eingaben wird von der Systemadministration bestimmt.
- ein bestimmtes Passwort darf erst nach 5 Änderungen wiederverwendet werden;
- das Passwort darf nicht niedergeschrieben werden.

Wurde die Zugangsberechtigung gesperrt oder das Passwort vergessen, so ist der Systemadministration der Erhalt des neuen Passwortes schriftlich zu bestätigen. Bei Weitergabe des neuen Passwortes an den Mitarbeiter ist dessen Identität festzustellen. Dies geschieht entweder persönlich (ggf. nach Vorlage des Personalausweises) oder über den Vorgesetzten des betroffenen Mitarbeiters, der das Schreiben der EDV-Systemverwaltung aushändigt.

- (2) Der Anwender hat dafür zu sorgen, dass ein Zugriff mittels seiner Zugangsberechtigung auf die EDV für nicht-berechtigte Dritte nicht möglich ist. Alle EDV-Nutzer sind verpflichtet, in Arbeitspausen den Zugriff für Nichtberechtigte durch einen Bildschirmschoner mit Passwortschutz zu verhindern und sich bei längeren Pausen und beim Verlassen des Arbeitsplatzes vom System abzumelden.
- (3) Es ist untersagt, ohne Zustimmung der EDV-Systemverwaltung die Arbeitsplatzsysteme zu öffnen. Eine Öffnung ist nur in Anwesenheit der EDV-Systemverwaltungsstelle zulässig. Der Anschluss von separaten elektronischen Kommunikationsgeräten (z. B. Modems, ISDN-Karten etc.) an das Arbeitsplatzsystem ist nur aufgrund einer besonderen schriftlichen Verfügung der Leitung der Organisationseinheit oder der Einrichtung und unter Mitwirkung der EDV-Systemverwaltung erlaubt. Arbeitsplatzsysteme dürfen nur durch die EDV-Systemverwaltung an das Netzwerk angeschlossen werden.
- (4) Es ist Anwendern untersagt, Programme auszuführen, die zum Ausspähen des Datenverkehrs oder zum Ausspähen oder Erlangen von Passwörtern geeignet sind.
- (5) Die EDV-Systemverwaltung hat geeignete Zugriffsschutzmaßnahmen einzurichten, die sicherstellen, dass ein nichtautorisierter Zugriff auf Informationen unter normalen Umständen nicht möglich ist.
- (6) Weitere Sicherheitsvorgaben sind ggf. in einer gesonderten Sicherheitsrichtlinie durch die Leitung der Organisationseinheit oder Einrichtung anzuordnen. Die Sicherheitsrichtlinie bedarf der kirchenaufsichtlichen Genehmigung, soweit es kirchliche Körperschaften betrifft, die der bischöflichen Aufsicht unterstehen.

6. Nutzung von Dateiablagen

6.1. Allgemeines

Dateiablagen sind Verzeichnisse oder Laufwerke, die den Anwendern der EDV-Anlage zur persönlichen oder gemeinsamen Datenspeicherung zur Verfügung stehen. Diese Dateiablagen befinden sich auf zentralen Geräten oder bei Einzelplatzsystemen auf dem PC. Alle zentralen Dateiablagen werden so mit Zugriffsrechten geschützt, dass entweder nur einem bestimmten Mitarbeiter oder einer Gruppe von Mitarbeitern (z. B. allen Mitarbeitern einer Abteilung) der Zugriff ermöglicht wird. Die EDV-Systemverwaltung verwaltet die Zugriffsrechte auf diese Dateiablagen und sichert die Dateiablagen vor Datenverlust.

Alle verarbeiteten Informationen, die Arbeitsergebnisse oder relevante Zwischenergebnisse darstellen, sind nach Maßgabe der folgenden Ziffern 6.2. bis 6.4. innerhalb dieser Dateiablagen zu speichern. Im EDV-Netzwerk ist die Speicherung dieser Informationen direkt auf den Laufwerken des Arbeitsplatzsystems nicht gestattet. Die Speicherung auf Disketten oder anderen Wechselmedien der Arbeitsplatzsysteme darf lediglich zu Zwecken des Datenaustausches mit Systemen außerhalb der Vernetzung erfolgen, soweit die Art der Daten eine solche ungesicherte Speicherung zulässig erscheinen lässt. Zur Speicherung besonders schützenswerter Informationen steht der persönliche Ablagebereich der Anwender zur Verfügung (s. 6.3.).

Die Anwender werden darauf hingewiesen, dass die durch die EDV-Systemverwaltung durchgeführte Datensicherung keine Archivierung darstellt. Sofern eine Archivierung von Informationen notwendig ist, hat der Anwender diese weiterhin auf dem hierzu üblichen Weg durchzuführen; bis auf weiteres bleibt es bei dem bisherigen Verfahren.

Unterliegen Dateien von einzelnen Anwendern oder Teilen der Organisationseinheit besonderen Sicherheitsanforderungen und sollen Inhalte vor Einsicht durch andere Anwender, auch den Systemverwalter geschützt sein, kann die Verschlüsselung von Dateien genehmigt werden. Die Entscheidung hierüber obliegt dem Leiter der Organisationseinheit oder Einrichtung, bei der persönlichen Dateiablage ggf. dem Leiter der Untergliederung einer Organisationseinheit. Die Genehmigung erfolgt schriftlich. Die Anwendung von Datenverschlüsselung ist der Systemadministration in jedem Fall schriftlich mitzuteilen.

Wie und ob der Schlüssel aufbewahrt bzw. hinterlegt wird und wer hierauf in besonderen Fällen Zugriff nehmen kann, ist in der Sicherheitsrichtlinie zu regeln.

6.2. Gemeinsame Dateiablage

Innerhalb des EDV-Netzwerkes werden gemeinsame Dateiablagen zur Nutzung durch die Organisationseinheiten oder deren Untergliederungen eingerichtet. Die Organisationseinheiten regeln die Strukturierung dieser Ablagebereiche eigenständig und eigenverantwortlich. Sie werden dabei von den Systemverwaltern gemäß Ziff. 9.3. unterstützt. Die Organisationseinheiten bestimmen auch, welche Informationen Arbeitsergebnisse oder relevante Zwischenergebnisse darstellen. In Zweifelsfällen entscheidet die Leitung der Organisationseinheit oder Einrichtung.

Die Systemverwaltung ist berechtigt, notwendige Pflegeaufgaben und die von den Organisationseinheiten und Einrichtungen gewünschten Änderungen am jeweiligen Ablage- und Zugriffsplan eigenständig durchzuführen. Hierzu werden die Systemverwalter mit den notwendigen

Zugriffsrechten ausgestattet. Sie sind berechtigt, auf die dort gespeicherten Informationen im erforderlichen Umfang Zugriff zu nehmen. Sie bedürfen hierbei der Zustimmung des/der zuständigen Abteilungsleiters/Abteilungsleiterin oder des/der Leiters/Leiterin der Organisationseinheit bzw. Einrichtung.

Sofern wegen besonderen Sicherheitsbedarfes für die Geschäftsbereiche des Bischofs und des Offizialates eigene Dateiablagen ohne Zugriff durch Dritte benötigt werden, können diese auf Arbeitsstationen ohne Anschluss an Netzwerke oder in einem eigenen Netzwerk eingerichtet werden. Unbeschadet dessen besteht die Möglichkeit der Datenverschlüsselung.

6.3. Einzelablage von Dateien

Jedem Anwender des Netzwerks steht nach Weisung des Vorgesetzten in dem erforderlichen Umfang für Dienstzwecke eine Einzelablage von Dateien zur Verfügung, für die besondere betriebliche Regelungen zu schaffen sind. Der Systemverwaltung ist die Einsichtnahme hierauf nicht gestattet.

Auf Weisung des Leiters/der Leiterin der Organisationseinheit oder Einrichtung kann in dringenden Fällen der Zugriffsschutz auf diese Bereiche in der Weise aufgehoben werden, dass ein vom Leiter benannter Anwender auf die Daten Zugriff erhält (z. B. im Fall längerer Krankheit), sofern der Anwender nicht dem Schutzbereich des Bischofs zugeordnet ist. Ist der Anwender dem Schutzbereich zugeordnet, ist eine Übertragung des Zugriffsrechtes nur mit Einwilligung des Mitarbeiters oder des Bischofs möglich.

6.4. Schutzbereich des Bischofs

Es wird davon ausgegangen, dass Mitarbeiter, die dem Schutzbereich des Bischofs zugeordnet sind, Informationen verarbeiten, die höchster Vertraulichkeit unterliegen. Für diese Gruppe von Anwendern gelten bei der Arbeit im EDV-Netz folgende Sonderregelungen:

1. Informationen höchster Vertraulichkeit werden von den Mitarbeitern in ihren persönlichen Dateiablagen gespeichert.
2. Die Systemverwalter dürfen nur in Anwesenheit und auf Verlangen des Mitarbeiters Zugriff auf diese Informationen in den persönlichen Dateiablagen nehmen.
3. Die Informationen werden nicht im Rahmen der allgemeinen Datensicherung, sondern auf separaten Speichermedien gesichert. Sie dienen lediglich zum Schutz der Anwender vor Datenverlust bei Systemausfällen.

7. Elektronische Kommunikation

7.1. Allgemeine Hinweise

Die EDV-Anlagen verfügen in der Regel über eine Reihe von Systembestandteilen, die die elektronische Kommunikation (siehe Begriffsbestimmung) ermöglichen und deren Nutzung den Anwendern möglich ist. Die Nutzung dieser Systembestandteile unterliegt verschiedenen gesetzlichen Bestimmungen, deren Einhaltung durch die Nutzer der Anlagen eingehalten werden müssen (KDO, Telekommunikationsgesetz). Die Nutzung der elektronischen Kommunikation zur Kommunikation mit Stellen außerhalb der Kernvernetzung soll durch eigene Bestimmungen der Organisationseinheiten und Einrichtungen geregelt werden.

Es wird darauf hingewiesen, dass auch bei der elektronischen Kommunikation (z. B. mit Hilfe elektronischer Nachrichten - E-Mail) die Datenschutzbestimmungen bezüglich der übermittelten Inhalte einzuhalten sind. Hierzu ist im

Einzelfall die Zulässigkeit der Übertragung vom Nutzer zu prüfen. Die übermittelten Inhalte sind nach Maßgabe ihrer Schutzwürdigkeit und dienstlicher Weisung während der Übertragung an externe Stellen zu verschlüsseln.

Nach dem Stand der Technik sind zum Schutz der EDV-Anlagen vor unbefugtem Eindringen und zum Schutz vor schädlichen Inhalten automatisierte Kontrollen des Datenverkehrs durchzuführen. Näheres kann erforderlichenfalls durch dienstliche Weisungen oder in "Dienstvereinbarungen" geregelt werden.

7.2. Teilnahme auswärtiger Stellen am internen Kommunikationssystem

Die Anbindung externer Stellen (z. B. Pfarrämter, Kindergärten) an das interne Kommunikationssystem einer EDV-Anlage kann zugelassen werden. Diese Anbindung von Außenstellen erlaubt die gemeinsame Nutzung von Informationssystemen und Kommunikationsanlagen.

Voraussetzung der Anbindung von externen Stellen ist die Abgabe einer Verpflichtungserklärung durch deren Mitarbeiter, diese Ordnung sowie sonstige relevante Bestimmungen sorgfältig einzuhalten. Diese Verpflichtungserklärung bezieht etwaige Dienstvereinbarungen ein.

7.3. Bedeutung der E-Mail-Funktion

Für die Kommunikation mit allen Stellen werden E-Mails grundsätzlich als ein Medium der flüchtigen und spontanen Kommunikation angesehen, das insoweit mit dem Telefon vergleichbar ist. Bei rechtsverbindlichen Äußerungen ist die Verwendung von E-Mails nicht ausreichend. Soweit rechtsverbindliche Erklärungen durch besondere Vorschriften zugelassen sind, sollen sie immer (zusätzlich) in herkömmlicher Schriftform abgegeben werden, sofern mit der jeweiligen Stelle keine andere Vereinbarung getroffen wurde.

Im Falle der Zulassung von rechtsverbindlichen Erklärungen für den Bereich der Kernvernetzung und die am internen Kommunikationssystem angeschlossenen auswärtigen Stellen sind diese mit der digitalen Signatur des Ausstellers zu versehen und als rechtsverbindliche Äußerung zu kennzeichnen.

8. Einsatz von Software

8.1. Allgemeines

Soweit nichts anderes festgelegt ist, dienen die EDV-Anlagen auch als Infrastruktur zum Betrieb unterschiedlicher Arten von Software. Der Einsatz von Software basiert auf dem Bedürfnis der Anwender, die Lösung von Problemen mit Hilfe der EDV zu bewältigen. Diese Bedürfnisse unterliegen Veränderungen.

Um die Kooperationsmöglichkeiten der Nutzer zu optimieren und die Kosten für den Betrieb der Anlagen zu minimieren, ist es notwendig, die Entscheidung über den Einsatz bestimmter Software zu koordinieren. Diese Aufgabe wird grundsätzlich durch die Leitung der Organisationseinheit oder Einrichtung wahrgenommen, die sich der fachlichen Unterstützung der Systemverwaltung oder externen Sachverständiges bedienen soll.

8.2. Kategorisierung und Meldung von Software

Jede Software ist formal zu kategorisieren. Diese Kategorisierung dient der Beschreibung der Bedeutung und der Pflege der Informationssysteme. Falls betrieblich gewollt, ist zu jeder eingesetzten Software ein verantwortlicher Betreuer zu bestimmen, der für die Pflege der Software zuständig ist und den Anwendern der Software als An-

sprechpartner zur Verfügung steht. Soweit keine Bestimmung des Betreuers vorliegt, ist die mit der Systemverwaltung beauftragte Stelle zuständig.

Die Kategorisierung sieht drei Stufen vor:

Kategorie A Software, die an jedem Arbeitsplatz der EDV-Anlage verfügbar ist. Zur Aufnahme einer Software in die Kategorie A ist die Zustimmung der Leitung der Einrichtung nach Empfehlung der EDV-Systemverwaltung erforderlich.

Zuständig für Betrieb und Pflege der Software der Kategorie A ist die EDV-Systemverwaltung.

Kategorie B Software, die an einem oder mehreren Arbeitsplätzen eingesetzt wird, und die zur Erlangung von Arbeitsergebnissen unverzichtbar oder zumindest von erheblichem Nutzen ist.

Zur Aufnahme einer Software in die Kategorie B ist die Zustimmung der Leiterin/des Leiters der Abteilung, der Organisationseinheit oder der Einrichtung notwendig, in der diese Software eingesetzt wird. Weiter ist durch die Systemverwaltung zu prüfen, ob der Einsatz der Software von einheits- oder einrichtungsübergreifendem Interesse ist. In letzterem Fall wird die Einführung der Software entsprechend der Kategorie A gehandhabt.

Für eine Software der Kategorie B ist in der Abteilung oder Organisationseinheit ein verantwortlicher Betreuer zu benennen, der deren Einsatz und Unterstützung organisiert.

Kategorie C Software, die zur Erlangung von Arbeitsergebnissen nicht notwendig ist, und die somit aus anderen Gründen (z. B. Evaluation) eingesetzt wird.

Software der Kategorie C dürfen nur während einer zeitlich begrenzten Phase zur Erlangung von Arbeitsergebnissen eingesetzt werden. Hierfür ist in Absprache mit der Systemadministration die Zustimmung der Leitung der Organisationseinheit bzw. der Untergliederung, wenn die Software nur hier eingesetzt wird, einzuholen.

Solange keine andere Kategorisierung vorliegt, ist eine Software der Kategorie C zugeordnet.

Regelung zum Zeitpunkt der Einführung eines EDV-Netzwerksystems:

Jede Software, die nicht durch die Leitung der Einrichtung (im Bischöflichen Generalvikariat durch die Abteilungsleiterkonferenz) in Kategorie A oder B eingeordnet wurde, ist zunächst der Kategorie C zugeordnet. Innerhalb von 6 Monaten nach Inbetriebnahme der Vernetzung am jeweiligen Arbeitsplatz ist die eingesetzte Software zu kategorisieren.

8.3. Anzeigepflicht

In der Regel soll es nur der Systemverwaltung möglich und gestattet sein, Software zu installieren. In diesem Fall ist die Systemverwaltung für die Registrierung und Lizenzie-

rung der Software sowie erforderlichen Nachweis verantwortlich.

Im Einzelfall kann die Berechtigung, Software zu installieren von der Systemverwaltung übertragen werden. In diesem Fall ist die berechtigte Person für die Lizenzierung und den Nachweis verantwortlich. Alle Lizenznachweise sind bei der Systemverwaltung zu hinterlegen

Lizenzpflichtige Software darf nur mit gültiger Lizenz eingesetzt werden. Die Anwendung freier Software ist der Systemverwaltung schriftlich zu melden. Die Systemverwaltung führt ein Verzeichnis jeder eingesetzten Software einschließlich der Lizenznummern.

Der Einkauf von Software, Lizenzierung und Updates soll soweit wie möglich zentralisiert werden.

8.4. Durchführung der Kategorisierung

Entsteht an den Arbeitsplätzen der Organisationseinheit oder der Einrichtung der Bedarf, ein Problem mit Hilfe einer noch nicht vorhandenen Software zu lösen, so entscheidet zunächst der/die zuständige Leiter/Leiterin der Organisationseinheit oder Einrichtung, ob das Problem mit Hilfe der EDV gelöst werden soll.

Bei Zustimmung des Leiters/der Leiterin ist die Leitung der Organisationseinheit oder Einrichtung über das Problem und die mögliche Lösung des Problems (z. B. käufliche Software, Entwicklungsauftrag) zu informieren.

Diese prüft das Problem und den Lösungsweg unter den Aspekten:

- Kann das Problem mit bereits vorhandenen Mitteln gelöst werden?
- Besteht von Seiten anderer Organisationseinheiten ein identischer/ähnlicher Bedarf?
- Wer ist der verantwortliche Betreiber der Software?
- Wie kann der Betrieb der Software unterstützt werden (Support)?
- Ggf. Durchführung einer Kosten-/Nutzenanalyse.
- Ggf. Technische Prüfung des Lösungswegs in Zusammenarbeit mit der EDV-Systemverwaltung.
- Ggf. Empfehlung eines alternativen Lösungswegs.

Der Leiter/Die Leiterin einer Organisationseinheit/Abteilung kann mit Zustimmung des Generalvikars oder des/der Leiters/Leiterin der Einrichtung die Prüfung des Lösungsansatzes auf diese Aspekte an Dritte delegieren und Entscheidungen auf Basis der Empfehlungen Dritter treffen.

9. EDV-Systemverwaltung

9.1. Allgemeines

Die EDV-Systemverwaltung ist für den technischen Betrieb der EDV-Anlage zuständig. Dies umfasst alle Aspekte, die für die Entwicklung, Aufrechterhaltung und Absicherung des Betriebs notwendig sind. Darüber hinaus unterstützt die EDV-Systemverwaltung die Anwender durch Schulungen und Beratung. Die Organisationseinheit/ Einrichtung trägt für eine angemessene Schulung der Mitarbeiter der Systemverwaltung Sorge, damit diese ihrem Auftrag, zu unterstützen, zu schulen und für die Sicherheit des Netzes zu sorgen nachkommen können.

Der EDV-Systemverwaltung obliegt i.d.R. die Bewirtschaftung der Mittel für Anschaffung und externe Dienstleistungen einschließlich Schulung im Bereich der Hardware und Software für alle Bereiche einer Organisationseinheit. Hierdurch soll gewährleistet werden, dass den

Grundsätzen der Wirtschaftlichkeit Rechnung getragen wird, die Komponenten einer EDV-Anlage möglichst einheitlich sind und die EDV-Entwicklung besser steuerbar wird.

9.2. EDV-Fachbeauftragte

Zur Entlastung der Benutzerunterstützung durch die EDV-Systemverwaltung kann in jeder Organisationseinheit (Abteilung) ein Fachbeauftragter für die Nutzung der EDV-Anlagen benannt werden.

Aufgabe des Fachbeauftragten ist es, die Nutzung der EDV-Anlage in seinem Bereich bei auftretenden Problemen und Anforderungen zuerst zu unterstützen und die EDV-Systemverwaltung umgehend zu informieren und nach deren fachlicher Weisung bei der Problemlösung zu unterstützen.

9.3. EDV-Systemverwaltung

Die EDV-Systemverwaltung kann mit eigenen Mitarbeiterinnen und Mitarbeitern ausgestattet sein oder im Rahmen eines Auftrags von Dritten wahrgenommen werden. Diese Mitarbeiter oder Auftragnehmer genießen eine besondere Vertrauensstellung die auf ihrer technischen Befähigung beruht, Sicherheits- und Zugriffsschutzverfahren innerhalb der EDV-Anlage zu modifizieren.

Sie sind verpflichtet, sicherzustellen, dass die von ihnen durchgeführten Maßnahmen dem Sinn der Sicherheits- und Zugriffsschutzmaßnahmen nicht entgegenstehen. Sie sind berechtigt, für die Durchführung von Tätigkeiten, die die Sicherheits- und Zugriffsschutzmaßnahmen betreffen, schriftliche Anweisungen zu verlangen und diese im Zweifelsfall durch den Generalvikar bzw. den Leiter/die Leiterin der Einrichtung bestätigen zu lassen.

9.4. Systempflege und Entstörungsmaßnahmen

Die EDV-Systemverwaltung ist berechtigt, zur Durchführung von Tätigkeiten zur Pflege und zum Ausbau der EDV-Anlage, Teile der EDV-Anlage oder das Gesamtsystem zeitweise außer Betrieb zu nehmen. Diese Maßnahmen unterliegen verschiedenen Prioritäten, die von der EDV-Systemverwaltung nach Maßgabe der Umstände einzuhalten sind:

Priorität 1: Entstörung der Sicherheitseinrichtungen der EDV-Anlage

Werden Fehler in den Sicherheitseinrichtungen festgestellt, die die Sicherheit der EDV-Anlage gefährden, ist die EDV-Systemverwaltung verpflichtet, die Entstörung unverzüglich vorzunehmen. Bis zur erfolgten Entstörung werden alle Einrichtungen, die von der Störung der Sicherheitseinrichtungen betroffen sind (insbesondere Einrichtungen zur Kommunikation außerhalb des Netzwerks), unverzüglich deaktiviert.

Priorität 2: Entstörung zentraler Einrichtungen der EDV-Anlage

(Zentrale technische Einrichtungen und Software der Kategorie A, die Gesamtheit aller Arbeitsplatzsysteme)

Werden Fehler in diesem Bereich festgestellt, welche die Funktionsfähigkeit der EDV-Anlage ganz oder teilweise beeinträchtigen, werden die Entstörungsmaßnahmen sofort eingeleitet. Sind zur Entstörung zeitweise wei-

tere Funktionsbeeinträchtigungen zu erwarten, kann die Entstörung nach Ermessen der EDV-Systemverwaltung verzögert werden.

Priorität 3: a) Pflege zentraler Einrichtungen der EDV-Anlage

(Zentrale technische Einrichtungen und Software der Kategorie A, die Gesamtheit aller Arbeitsplatzsysteme)

Um die Funktionsfähigkeit der zentralen Einrichtungen der EDV-Anlage aufrechtzuerhalten, sind Maßnahmen zur (routinemäßigen oder außerordentlichen) Pflege von zentralen Einrichtungen mit hoher Priorität durchzuführen. Sofern die Maßnahmen mit Funktionseinbußen verbunden sind, sind sie den Anwendern mit einer Ankündigungsfrist von zwei Arbeitstagen mitzuteilen.

b) Pflege und Entstörung weiterer Einrichtungen der EDV-Anlage

(Besondere technische Einrichtungen und Software der Kategorie B)

Erforderliche Pflege- oder Entstörungsmaßnahmen im Bereich technischer Einrichtungen und im Bereich von Software, die der Kategorie B zugeordnet ist. Sofern die Maßnahmen mit Funktionseinbußen verbunden sind, sind sie den Anwendern mit einer Ankündigungsfrist von zwei Arbeitstagen mitzuteilen.

Priorität 4: Entstörung von Arbeitsplatzsystemen (Einzelne Arbeitsplatzsysteme)

Treten technische Probleme an den Arbeitsplatzsystemen auf, sind diese spätestens nach Abschluss von Arbeiten der Prioritäten 1 - 3 zu lösen.

Folgende Maßnahmen stehen zur Verfügung:

- Versuch der Fehlerbehebung am Arbeitsplatz durch Modifikation des Systems. Maximale Zeitdauer des Entstörungsversuches: 1 Arbeitsstunde
- Neuinstallation des Systems nach vorheriger vollständiger Löschung oder alternativ
- Austausch des Systems.

Sofern spezifische Software der Kategorie B auf dem System eingesetzt wird, unterstützen die Softwareverantwortlichen, EDV-Fachbeauftragten und die EDV-Systemverwaltung den Anwender bei der Neueinrichtung dieser Software. Software der Kategorie C wird nicht berücksichtigt.

Die Anwender werden darauf hingewiesen, dass die Speicherung von Informationen auf den oben beschriebenen Dateiablagen zu erfolgen hat. Hierdurch wird sichergestellt, dass verarbeitete Informationen durch die Entstörungsmaßnahmen nicht vernichtet werden.

Die Priorisierung berechtigt die EDV-Systemverwaltung, nachgeordnete Aufgaben zeitlich zu verzögern. Treten Störungen auf, die den Prioritäten 1 und 2 zugeordnet sind, kann die EDV-Systemverwaltung nachgeordnete Aufgaben abrechnen.

9.5. Benutzerunterstützung, Beratung und Schulungen

Die EDV-Systemverwaltung wie auch die EDV-Fachbeauftragten und Softwareverantwortlichen unterstützen die Anwender durch Beratung, Schulungsmaßnahmen und bei technischen Problemen.

10. Organisatorische und technische Sicherheitsüberwachung

Aufgabe des Datenschutzbeauftragten ist die Überwachung der Sicherheitsvorkehrungen der EDV-Anlage. Der Datenschutzbeauftragte inspiziert in der Regel einmal jährlich die Sicherheitseinrichtungen der EDV-Systemverwaltung. Ziel der Inspektionen sind die regelmäßige Kontrolle der Sicherheitsvorkehrungen. Der Datenschutzbeauftragte kann auf Kosten der Einrichtung diese Inspektion unter seiner Verantwortung einem geeigneten Dritten delegieren.

Die Inspektionen umfassen:

- die Kontrolle der Benutzerverwaltung und deren Dokumentation
- die Kontrolle der Sicherheitseinrichtungen des Netzwerks (z. B. Firewall, Virenschutz) auf korrekten Betrieb und Vollständigkeit der Dokumentation
- die Kontrolle der Zugriffsrechte auf Ressourcen der EDV-Umgebung
- die Kontrolle sonstiger sicherheitsrelevanter Anlagen und Programme.

Die Inspektion kann nach Maßgabe des Datenschutzbeauftragten in Form von Stichproben oder vollständig erfolgen.

Die EDV-Systemverwaltung ist verpflichtet, die Inspektion in jeder Form zu unterstützen.

Sofern der Datenschutzbeauftragte Mängel feststellt, ist die EDV-Systemverwaltung verpflichtet, die Beseitigung der Mängel umgehend zu veranlassen. Der Abschluss der Mängelbeseitigung ist dem Datenschutzbeauftragten anzuzeigen.

Der Datenschutzbeauftragte ist verpflichtet, der EDV-Systemverwaltung die Durchführung der Inspektion zu bestätigen.

Der Datenschutzbeauftragte berichtet dem Leiter/der Leiterin der Organisationseinheit oder Einrichtung über die Ergebnisse der Inspektionen. Diese Berichte des Datenschutzbeauftragten sind vertraulich und als Dienstgeheimnisse einzustufen.

11. Datenschutzbeauftragter

Die Befugnisse des Datenschutzbeauftragten werden im übrigen durch die Regelung dieses Abschnitts nicht berührt. Auf Anforderung des Datenschutzbeauftragten ist die EDV-Systemverwaltung verpflichtet, diesen bei der Wahrnehmung seiner Aufgaben zu unterstützen.

Fulda, den 1.12.2001

+ Heinz J. Algermissen
Bischof von Fulda

Nr. 52 Änderungsverordnung zur Geschäftsordnung für das Bischöfliche Generalvikariat

Aufgrund der Neuinstallation und Vernetzung von Telefon- und EDV-Anlagen im Bischöflichen Generalvikariat (Kernvernetzung) wird die Geschäftsordnung für das Bischöfliche Generalvikariat Fulda vom 20.03.1980 i. d. F. v. 19.05.1994 wie folgt geändert:

I. § 8 (Telefonverkehr) wird durch die folgende Bestimmung ersetzt:

§ 8

Zugang und Umfang der Telefonnutzung

- (1) Hinsichtlich des Telefonverkehrs gilt für das Bischöfliche Generalvikariat, gleichermaßen wie für alle mit ihm räumlich/technisch verbundenen kirchlichen/bischöflichen Einrichtungen der Bistumsverwaltung - soweit eine vernetzte Kommunikationsanlage vorhanden ist oder tragbare Endgeräte (Handy usw.) ausgegeben werden - dass alle Stellen der Bistumsleitung im Sinne von § 3 dieser Geschäftsordnung (analog bei den sonstigen Einrichtungen) unbeschränkt systemüblichen Zugang zum Telefonverkehr haben. Über Nutzungsumfang und den Zugang zu Auslandstelefonverbindungen oder zu tragbaren Endgeräten entscheidet der Generalvikar oder in seinem Auftrag und gemäß seiner allgemeinen Weisung der zuständige Abteilungsleiter für die ihm zugeordneten Mitarbeiterinnen und Mitarbeiter. Im übrigen wird allen Bediensteten Zugangsberechtigung und Nutzung des Telefons mit der am konkreten Arbeitsplatz vorgegebenen technischen Ausstattung unter Beachtung der nachfolgenden Bestimmungen des Abs. 2 sowie der sonstigen dienstlichen oder arbeitsrechtlichen Vorschriften eingeräumt.
- (2) Das Telefon ist grundsätzlich nur für den Dienstgebrauch bestimmt. Ausnahmsweise und unter dem Vorbehalt jederzeitigen Widerrufs kann die Telefonanlage für Privatgespräche (aus- und eingehende Gespräche) genutzt werden. Voraussetzung ist, dass die Privatnutzung durch den Generalvikar oder durch die Leitung der Einrichtung zugelassen wurde und die Kommunikationsanlage eine besondere Funktion zur Kennung und automatischen Registrierung der Kosten von Privatgesprächen besitzt. In diesem Fall ist die private Nutzung nur in besonders wichtigen oder unaufschiebbaren Angelegenheiten zulässig. Die Privatnutzung ist in der Regel entsprechend dem aufgezeichneten Nutzungsumfang dem Nutzer in Rechnung zu stellen. Dabei ist es zulässig, mindestens folgende Daten elektronisch zu speichern: Anzahl der Gespräche oder der Nutzungen, Datum, Uhrzeit und Gebührenkenngrößen. Die Bestimmungen über den kirchlichen Datenschutz sowie die einschlägigen zwingenden gesetzlichen Telekommunikationsrechtsvorschriften bleiben unberührt.

II. Nach § 9 der Geschäftsordnung für das Bischöfliche Generalvikariat werden unter den Bezeichnungen § 9a, § 9b und § 9c folgende Bestimmungen über den elektronischen Postverkehr (E-Mail) sowie die Nutzung weiterer Netzwerkdienste eingefügt:

§ 9a

Allgemeine Bestimmungen zum Elektronischen Postverkehr (E-Mail)

- (1) Das Bischöfliche Generalvikariat hat eine zentrale elektronische Postadresse (E-Mail-Adresse), die durch den Generalvikar festgelegt wird. Diese zentrale E-Mail-Adresse ist bei allen Arten von ausgehenden Dokumenten des Bischöflichen Generalvikariates (z.B. per Post, Fax, E-Mail) als Standard für den zentralen Posteingang zu benennen. Die zentrale E-Mail-Adresse dient in erster Linie als zentraler Posteingang für alle dienstlichen Belange und Informati-

onsanfragen sowie zum Versenden von E-Mails an externe Verteilerlisten, sofern dieses Recht nicht anderen Benutzern gewährt wurde.

Die Zuständigkeit für die Benutzung der zentralen E-Mail-Adresse des Bischöflichen Generalvikariates liegt grundsätzlich beim Leiter/bei der Leiterin der Posteingangsstelle/Registrierung oder bei den unter seiner/ihrer Weisung damit betrauten Mitarbeiterinnen bzw. Mitarbeitern.

- (2) Alle nicht dem Generalvikariat zugehörigen Stellen oder rechtlich selbständigen Einrichtungen, insbesondere die Geschäftsbereiche des Offizialates und des Bischofs erhalten eigene E-Mail-Adressen, die auch auf Briefbögen dieser Stellen und in anderen Informationen (z.B. Schematismus) ausdrücklich genannt werden sollen. Der Generalvikar kann im Bischöflichen Generalvikariat zulassen, dass Abteilungen, Stabstellen und Referate von eigenständiger Bedeutung – nachfolgend Untergliederungen genannt - eigene E-Mail-Adressen erhalten.
- (3) Soweit die technischen Voraussetzungen im hauseigenen EDV-Netz gegeben sind und die Nutzungsberechtigung erteilt wurde (Abs. 7), sind alle Mitarbeiterinnen und Mitarbeiter, die nach den betrieblichen Beschaffungsvorschriften an ihrem Arbeitsplatz mit einem netzwerkfähigen PC oder sonstigem geeigneten Endgerät ausgestattet wurden, berechtigt, am internen elektronischen Postverkehr (interner E-Mail-Verkehr) teilzunehmen. Sie können bei dienstlicher Notwendigkeit außerdem entsprechend Abs.2 (letzter Satz) eine E-Mail-Adresse für die Kommunikation mit externen Personen oder Stellen erhalten. Die Beurteilung des Kriteriums der dienstlichen Notwendigkeit liegt im Einzelfall bei der Leitung der jeweiligen Abteilung oder Einrichtung.
- (4) Die Nutzung des elektronischen Postverkehrs ist ausschließlich für dienstliche Vorgänge zulässig. Private Nutzungen können nur durch eine allgemeine Verwaltungsanordnung des Generalvikars eingeführt werden, in der auch die Zugangs- und Nutzungsbedingungen zu regeln sind.
- (5) Grundsätzlich dient der E-Mail-Verkehr lediglich als flüchtiges Medium für die schnelle und formlose Kommunikation untereinander und kann daher nicht für die Übermittlung von rechtsverbindlichen Vorgängen verwendet werden. Ausnahmen hiervon können durch eine Verwaltungsanordnung des Generalvikars zugelassen werden.
- (6) Sofern der Inhalt einer E-Mail für einen dienstlichen Vorgang wichtig oder dokumentationswürdig ist, muss ein Aktenvermerk angefertigt werden, dem ein Ausdruck der E-Mail beigefügt wird. Für die weitere Behandlung sind hiernach die Vorschriften für den dienstlichen Schriftverkehr zu beachten. Im Zweifelsfall ist immer die Leitung der Untergliederung zu unterrichten und ihre Entscheidung einzuholen. Jede E-Mail-Adresse ist mit einem elektronischen Postfach verbunden, in dem die eingehenden und in der Regel auch die ausgehenden E-Mails gespeichert werden. Zugriff auf dieses Postfach hat der Nutzungsberechtigte nach Maßgabe von § 9b Abs. 4. Der Nutzer von elektronischen Kommunikationsmedien und Netzwerkdiensten unterliegt den besonderen Sorgfaltspflichten, die sich aus der Eigenart des kirchlichen Dienstes und den besonderen Loyalitätspflichten des kirchlichen Arbeitsrechts ergeben.
- (7) Die Nutzungsberechtigung wird durch Aushändigung der technischen Unterlagen und gegen Abgabe einer schriftlichen Bestätigung des Nutzers/ der Nutzerin über die Einhaltung der Bestimmungen dieser Ordnung und der sie ergänzenden jeweiligen Vorschriften der EDV-Ordnung des Bistums, der Dienstvereinbarungen und der dienstlichen und arbeitsvertraglichen Geheimhaltungs- und Datenschutzbestimmungen erteilt.

- (8) Soweit eine Speicherung von personenbezogenen Daten im internen Netzwerk unabdingbar erfolgen muss, gelten die Bestimmungen der Kirchlichen Datenschutzordnung. Diese gespeicherten Daten sind durch die mit der technischen Netzwerkverwaltung beauftragte Stelle geheim zu halten. Näheres kann durch Dienstvereinbarung nach § 38 MAVO geregelt werden.

§ 9b

Verwaltungsmäßige Behandlung des Elektronischen Postverkehrs

- (1) Unter der zentralen E-Mail Adresse eingehende elektronische Post wird stets an die Posteingangsstelle/Registrierung geleitet und in ihrem elektronischen Postfach gespeichert. Dort wird die Zuständigkeit und weitere Bearbeitung geprüft und die elektronische Post über das Netzwerk an die nach den Posteingangsregeln zuständigen Stellen (§ 9 Abs. 2, 4 und 5) weitergeleitet. Wird die Weiterleitung der E-Mail nicht automatisiert gekennzeichnet, ist der E-Mail bei interner Weiterleitung ein entsprechender Vermerk mitzugeben. Das gleiche gilt für alle Stellen, die eine E-Mail nach Ansicht intern weiterleiten. Ein Ausdruck durch die Registrierung erfolgt nur bei Bedarf.
- (2) Eine Registrierung wie bei normaler Post entfällt, da eine E-Mail ohne digitale Signatur als flüchtiges Medium gilt und nicht für Mitteilungen mit rechtsverbindlichem Charakter genutzt werden kann (vgl. § 9a Abs.5). Statt einer Registrierung werden E-Mails für einen Zeitraum von drei Monaten gespeichert und nach Ablauf dieses Zeitraums durch die Systemverwaltung gelöscht. Erscheint bei einzelnen eingegangenen E-Mails eine längere Speicherung angezeigt, kann die Registrierung bzw. die Leitung der Untergliederung oder der Einrichtungen mit eigenem elektronischen Postfach entscheiden, dass die E-Mail in einem gesonderten Datei-Ordner gespeichert wird, für den die Lösungsfrist 1 Jahr beträgt (befristete Registrierung).
- (3) Gehen E-Mails bei den elektronischen Postfächern der Untergliederungen oder bei Postfächern von Mitarbeiter/-n/-innen ein, so müssen die Leitungen dieser Untergliederungen oder die zuständigen Personen prüfen, welche Bedeutung der Inhalt für dienstliche Belange hat und ob ein Aktenvermerk nach § 9a Abs. 6 anzufertigen ist oder eine Unterrichtung anderer Stellen zu erfolgen hat. Ist die E-Mail bzw. ihr Inhalt für eine andere oder mehrere Stellen oder den Generalvikar bestimmt, so wird sie mit einem entsprechenden Vermerk weitergeleitet. Hierbei ist der Dienstweg einzuhalten. Bestehen vom Inhalt her Zweifel über den Empfänger der E-Mail oder über die Zuständigkeit und die weitere Verteilung, wird die E-Mail mit einem entsprechenden Vermerk an die Registrierung weitergeleitet.
- (4) Die Berechtigung, ein elektronisches Postfach der Einrichtung oder einer Untergliederung zu öffnen und die gespeicherten E-Mails zu lesen und ggf. weiterzuleiten, kann von der Leitung der Abteilung oder Einrichtung delegiert werden. Dies gilt nicht für die Postfächer von Bediensteten. Der/Die Mitarbeiter/-in hat vor Abwesenheit dafür Sorge zu tragen, dass eingehende E-Mails stets an ein aktives Postfach umgeleitet werden und der Absender der E-Mail einen automatischen Hinweis auf die vorübergehende Abwesenheit des Postfachinhabers bekommt. Bei nicht vorherschaubarer Abwesenheit des/der Mitarbeiter/-s/-in hat der zuständige Leiter der Untergliederung für die Schaltung der Umleitung und des Hinweises durch die Systemverwaltung zu sorgen. Über die Delegation von Postfachberechtigungen ist die Systemverwaltung und die Registrierung zu informieren. Die Registrierung erhält von der Systemverwaltung jederzeit aktuelle Informationen über die bestehenden elektronischen Postfächer. Die Berechtigung, eine E-Mail unter einer

bestimmten Absender-Adresse zu versenden, kann nicht delegiert werden. Es ist aber möglich, andere Personen zu berechtigen, E-Mails "Im Auftrag" zu versenden. Hierbei ist der eigentliche Absender kenntlich zu machen.

- (5) Bei ausgehendem elektronischen Postverkehr werden E-Mail-Adressen wie folgt genutzt:

Über die zentrale E-Mail-Adresse des Bischöflichen Generalvikariates versendet die Leitung der Registratur nach den vom Generalvikar erteilten Einzelweisungen oder Richtlinien. Über die E-Mail-Adressen der Einrichtung oder Untergliederungen versenden die jeweiligen Leitungsbechtigten bzw. die durch Delegation hierzu Ermächtigten. Ansonsten werden E-Mails direkt durch die Mitarbeiter/-innen versandt, sofern ein Versenden "Im Auftrag" nach Abs. 4 von der Leitung der Untergliederung oder Einrichtung nicht ausdrücklich angeordnet wird. Sofern es die Sache oder der Inhalt der E-Mail erfordern ist ein Ausdruck zu den Akten zu nehmen und der Leitung der Untergliederung oder Einrichtung zur Kenntnis zu geben.

- (6) Für Mitteilungen an die Presse oder andere Medien gelten die §§ 10 Abs. 6 und 15 dieser Geschäftsordnung entsprechend.

§ 9c

Nutzung weiterer Netzwerkdienste

Für den Zugang zu weiteren Netzwerkdiensten (Internet usw.) gelten § 9a Abs. 4 und 7 entsprechend. Der/Die Nutzungsrechte für diese Dienste darf diese nur zu dienstlichen Zwecken nutzen. Aufgrund der ausschließlich zu Dienstzwecken zulässigen Nutzung von sonstigen Netzwerkdiensten (z.B. Internet-Nutzung) sind die Ergebnisse dieser Nutzungen entsprechend § 9a Abs. 6 zu behandeln. Die Nutzungsrechte an den Arbeitsergebnissen solcher Nutzungen stehen dem Dienstgeber zu.

III. Die Bestimmungen der §§ 8, 9a, 9b und 9c gehen anderen Vorschriften und Dienstvereinbarungen vor, falls Widersprüche auftreten. Die vorstehende vorläufige Änderung der Geschäftsordnung des Bischöflichen Generalvikariates tritt zum 01. Januar 2002 in Kraft und gilt ad experimentum für zwei Jahre. Ihre Weitergeltung bedarf dann der erneuten Inkraftsetzung durch den Diözesanbischof.

Fulda, den 03. Dezember 2001

+ Heinz J. Algermissen
Bischof von Fulda