Rundschreiben des Landeskirchenamtes an die Kirchenkreise betreffend Kirchlicher Datenschutz: Internet- und E-Mail-Nutzung 1. Datenschutzrechtliche Beurteilung der Internet- und E-Mail-Nutzung 2. Muster-Dienstvereinbarung zur Nutzung des Internets und der E-Mail-Dienste 3. Muster-Dienstanweisung für die Versendung und den Empfang elektronischer Post (E-Mail) und Telefax-Schreiben vom Arbeitsplatz (PC-Fax) 4. Merkblatt für eine sichere E-Mail-Nutzung[1]

Vom 6. Juli 2001 (Az.: A 14-03/01.09)

Immer mehr kirchliche Stellen binden ihre Personalcomputer (PC) oder ihre eigenen Netzwerke an das globale Datennetz „Internet“ an und schaffen so für ihre Mitarbeitenden die technische Möglichkeit, die entsprechenden Dienste (E-Mail, WorldWideWeb – WWW – usw.) direkt von ihrem Arbeitsplatz aus zu bedienen. Diese Internetanbindung dient sowohl der Informationsgewinnung als auch der Bereitstellung eigener Informationen für andere. E-Mail als Kommunikationsmittel wird zunehmend auch als Ersatz für die Briefpost oder den Faxversand eingesetzt.

Wegen der mit dem Anschluss an das Internet verbundenen Risiken und Gefährdungen für die Datensicherheit und den Datenschutz verweisen wir auf unser Rundschreiben vom 24.03.1999 (Az.: A 14 – 03/01.09) zur Thematik „Internet-Zugänge und Internet-Angebote“. Danach dürfen PC und PC-Netze kirchlicher Stellen an das Internet angeschlossen werden, soweit dies zur Erfüllung kirchlicher Aufgaben erforderlich ist und im Rahmen einer Kommunikations- und Risikoanalyse festgestellt wird, dass das Risiko des Anschlusses vertretbar ist. Für die Erstellung der Kommunikations- und Risikoanalyse sollte die vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellte Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet herangezogen werden (siehe Rundschreiben vom 05.02.2001 – Az.: A 14 – 03/01.09). Der Zugang an das WorldWideWeb darf nur über geeignete und sichere Zugänge eröffnet werden. Diese sollten insbesondere bei klei-

1 Redaktioneller Hinweis: Am 24. Mai 2018 ist das neu gefasste EKD-Datenschutzgesetz vom 15. November 2017 (Nr. 850) in Kraft getreten. Es wird zurzeit geprüft, ob und inwieweit eine Aktualisierung der Regelungen des Rundschreibens an das neue kirchliche Datenschutzrecht erforderlich ist.

neren kirchlichen Stellen möglichst über vom Netz abgekoppelte PC realisiert werden, um Schäden an und in den Verwaltungsnetzen fern zu halten. Sollten PC-Netze selbst mit dem Internet verbunden werden, müssen sie mittels einer so genannten Firewall abgesichert sein.

Bei der Internet- und E-Mail-Nutzung entstehen eine Reihe datenschutzrechtlicher und organisatorischer Fragen, z. B.

- ob nur eine dienstliche oder auch eine private Nutzung zugelassen werden soll,
- ob, in welchem Umfang und zu welchem Zweck eine Protokollierung der E-Mail-Nutzung und Internet-Nutzung erfolgen soll und wie lange solche Protokolle aufbewahrt werden sollen,
- welche organisatorischen Vorgaben für die Bearbeitung und damit auch die Kenntnisnahme von ein- und ausgehenden dienstlichen E-Mails gemacht werden sollen.

Zu diesem Schreiben finden Sie vier Anlagen.

In der **Anlage 1 „Datenschutzrechtliche Beurteilung der E-Mail- und Internet-Nutzung“** nehmen wir grundsätzlich zu den datenschutzrechtlich relevanten Fragestellungen ausführlich Stellung. Für die übrigen Fragen und Problemen bieten wir konkrete Lösungsansätze,

in der **Anlage 2 „Muster-Dienstvereinbarung zur Nutzung des Internets und der E-Mail-Dienste im Bereich der Ev. Kirche von Westfalen“**;

in der **Anlage 3 „Muster-Dienstanweisung für die Versendung und den Empfang elektronischer Post (E-Mail) und Telefax-Schreiben vom Arbeitsplatz (PC-Fax) im Bereich der Ev. Kirche von Westfalen“** sowie

in der **Anlage 4 „Merkblatt der Ev. Kirche von Westfalen für eine sichere E-Mail-Nutzung“**.

Zusammengefasst schlagen wir allen kirchlichen Stellen vor, die E-Mail- und Internet-Nutzung wie folgt zu regeln:

1. Die kirchlichen Stellen sollten nur eine dienstliche E-Mail- und Internet-Nutzung zulassen und die private Nutzung ausdrücklich ausschließen.
2. Eine vollständige Protokollierung aller Internet-Zugriffe der Mitarbeitenden zur Verhaltens- und Leistungskontrolle ist nicht erforderlich und damit unzulässig.
3. Die Mitarbeitervertretungen sind spätestens bei der Einführung von E-Mail-Systemen und der Zulassung der Internet-Nutzung zu beteiligen. Mit ihnen sind Regelungen – gegebenenfalls auch Dienstvereinbarungen – über das Verfahren der Protokollierung, der Kontrolle und der Auswertung der Protokolle zu treffen.

4. Nur innerhalb des landeskirchlichen Intranets können Dokumente mit vertraulichen und personenbezogenen Daten sicher versandt werden (automatische Verschlüsselung durch das Meldewesen-Mailprogramm GroupWise).
5. Es sind organisatorische Regelungen für die Versendung und den Empfang von E-Mails und PC-Faxen zu treffen (siehe Anlage 3).
6. Wir bitten zu beachten, dass die Muster-Dienstvereinbarung (Anlage 2), die Muster-Dienstanweisung (Anlage 3) und das Merkblatt (Anlage 4) an die jeweiligen gegebenen technischen und organisatorischen Gegebenheiten vor Ort anzupassen sind.

Anlage 1

Datenschutzrechtliche Beurteilung der E-Mail- und Internet-Nutzung (dienstliche und private E-Mail- und Internet-Nutzung sowie Zulässigkeit von Virencheck, Inhaltskontrolle und Protokollierung) – Stand: 6. Juli 2001 –

1. Dienstliche und private Nutzung von E-Mail

Aufgrund der nachfolgend dargestellten Rechtslage wird empfohlen, nur die dienstliche E-Mail-Nutzung zuzulassen und die private Nutzung ausdrücklich auszuschließen.

Wenn die private Nutzung des E-Mail-Dienstes gestattet würde, wäre die kirchliche Stelle insoweit als Anbieter von Telediensten einzuordnen und unterläge damit in Bezug auf die Protokollierung den Vorschriften des Teledienste-Datenschutzgesetzes (TDDSG) über die Verarbeitung personenbezogener Daten. Bei Zulassung der privaten E-Mail-Nutzung wäre eine dauerhafte Speicherung der Verbindungsdaten nicht zulässig; denn § 6 TDDSG erlaubt eine Speicherung nur, um der Nutzerin oder dem Nutzer die Inanspruchnahme des Dienstes zu ermöglichen sowie zu Abrechnungszwecken.

Im Hinblick auf den Inhalt der privaten E-Mails der Beschäftigten hat die kirchliche Stelle auch das Fernmeldegeheimnis nach § 85 Telekommunikationsgesetz (TKG) zu wahren. Daraus folgt insbesondere, dass es der kirchlichen Stelle untersagt ist, sich oder anderen über das für die Erbringung des Dienstes erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Die Weitergabe von Informationen, die dem Fernmeldegeheimnis unterliegen, ist strafbewährt. Daraus folgt bei Zulassung der privaten E-Mail-Nutzung, dass die Inhalte privater E-Mails grundsätzlich von der kirchlichen Stelle nicht zur Kenntnis genommen werden dürfen. Soweit darüber hinaus dienstliche und private E-Mails aus technischen oder organisatorischen Gründen nicht unterschiedlich behandelt werden (gleiche E-Mail-Adresse), würde das bedeuten, dass sämtliche dienstlichen E-Mails rechtlich nach den für die private E-Mail geltenden Rechtsvorschriften zu verarbeiten sind. Dies würde zu einer erheblichen Erschwerung der Verarbeitung dienstlicher E-Mails führen, da eine Kontrolle oder Weiterleitung der E-Mails an die Vertretung nicht zulässig wäre.

Zum Teil wird versucht, dieses Problem dadurch zu lösen, dass den Beschäftigten für die dienstliche und private Benutzung von E-Mail verschiedene E-Mail-Adressen zugewiesen werden. Auch bei dieser Konstruktion kann das Fernmeldegeheimnis allerdings nicht vollständig gewahrt werden, da zumindest die Systemadministration technisch in der Lage ist, den Inhalt privater E-Mails zur Kenntnis zu nehmen.

Eine rechtlich einwandfreie Lösung erfordere die Einwilligung aller privaten Nutzerinnen und Nutzer in die Verarbeitung ihrer Daten (§ 3 TDDSG).[1] In der mit jeder Mitarbeiterin oder jedem Mitarbeiter abzuschließenden Vereinbarung über die Bedingungen der Nutzung der E-Mail für private Zwecke wäre festzulegen, welche Überprüfungen von der DV-Systemadministration oder von der Dienststellenleitung wahrgenommen werden müssten. Die Vereinbarung müsste – gegebenenfalls durch Verweis auf eine Nutzungsordnung – den Umfang des Verzichts auf die Rechte beschreiben (z. B. die mögliche Kenntnisnahme des Inhalts privater E-Mails durch die DV-Systemadministration, soweit dies zur Missbrauchskontrolle oder durch dienstliche Vertretungspersonen, soweit dies zur Wahrnehmung der Vertretungsaufgaben notwendig ist). Mitarbeiterinnen und Mitarbeiter, die die Einwilligung hierzu verweigern, wären von der privaten Nutzung auszuschließen.

2. Dienstliche und private Internet-Nutzung

Es wird empfohlen, die private Internet-Nutzung nicht zuzulassen.

Bei dem Bereitstellen eines Internet-Zugangs für die ausschließliche dienstliche Nutzung handelt es sich nicht um einen Teledienst im Sinne des Teledienstegesetzes (TDG). Die kirchliche Stelle bietet dem Arbeitnehmer keinen Dienst an, sondern stellt ihm lediglich ein Arbeitsmittel zur Verfügung.[2] Damit finden die Vorschriften des TDDSG auf die Protokollierung einer ausschließlich dienstlichen Nutzung von Telediensten keine Anwendung.

Wird dagegen die private Internet-Nutzung zugelassen, handelt es sich um die Nutzung eines Teledienstes im Sinne des TDG. Damit gilt – wie bei der E-Mail-Nutzung unter Ziffer 1 beschrieben – das TDDSG sowie das Fernmeldegeheimnis nach § 85 TKG. Zu einer rechtlich einwandfreien Lösung bedarf es individueller Nutzungsvereinbarungen mit den Beschäftigten.

---

1 Das TDDSG verbietet dem Diensteanbieter zwar, die Erbringung des Teledienstes von der Einwilligung der nutzenden Personen in zusätzliche Datenverarbeitung abhängig zu machen, das gilt jedoch nur, soweit der Diensteanbieter eine Monopolstellung innehat. Letzteres trifft auf kirchliche Stellen nicht zu, denn sie sind nicht verpflichtet, den Bediensteten die Nutzung des Internets überhaupt zu ermöglichen.

2 Bei diesem „In-Sich-Verhältnis“ fehlt das von § 3 TDG vorausgesetzte Merkmal, dass es sich bei dem Diensteanbieter und der nutzenden Person um zwei unterschiedliche Rechtssubjekte handelt.

Zu beachten ist in diesem Zusammenhang, dass nicht nur auf Servern oder durch Firewalls, sondern auch am PC der Beschäftigten Daten über aufgerufene Internetseiten – je nach Einstellung der Browser – gespeichert werden. Bei der Protokollierung ist eine Trennung nach dienstlicher und privater Nutzung des Internets technisch nicht möglich.

3. Zulässigkeit von Virencheck, Inhaltskontrolle und Protokollierung

Sowohl bei dienstlicher als auch bei privater Nutzung bestehen grundsätzlich gegen eine Kontrolle auf Virenbefall mittels automatischem Virencheck keine Bedenken, soweit die Kontrolle automatisch und die Kenntnisnahme von den Inhalten privater E-Mails durch Beauftragte der Dienststelle nicht ohne Einwilligung der Mitarbeitenden erfolgt.

Eingehende dienstliche E-Mails können sich Vorgesetzte wie bei herkömmlicher Post von den betreffenden Mitarbeitenden vorlegen lassen. Die oder der Mitarbeitende hat auf Verlangen der kirchlichen Stelle Ausdrucke der E-Mails auszuhändigen bzw. den Ausdruck der E-Mails zu ermöglichen. Diese Aussagen gelten grundsätzlich auch für ausgehende dienstliche E-Mails. Die Kontrolle der Inhalte durch die Vorgesetzten ist daher ohne Weiteres zulässig.

Für die Aufrechterhaltung eines regelgerechten Firewall-Betriebs (z. B. für die Fehlersuche und -behebung) können Protokollierungen aus technischer Sicht unabdingbar sein. Die Notwendigkeit kann auf § 9 des Kirchengesetzes über den Datenschutz der EKD (DSG-EKD)[1] nebst Anlage gestützt werden. Die Zweckbindung der erhobenen Daten ist insbesondere für eine weitergehende Datenverarbeitung und -nutzung zu beachten (siehe § 5 DSG-EKD[1]).

Bei der dienstlichen Internet-Nutzung hat der Arbeitgeber grundsätzlich auch das Recht zu prüfen, ob das Surfen der Mitarbeitenden im WWW tatsächlich vollständig dienstlich motiviert war. In der Regel geht es darum zu vermeiden, dass Mitarbeitende in der Arbeitszeit und unter Nutzung dienstlicher Ressourcen aus rein privatem Interesse auf Informationen zugreifen. Aus diesem Grunde sollte man bekannte Angebote (z. B. erotische Angebote, Spiele oder Börsenkurse) grundsätzlich sperren.

1 Nr. **850 Archiv-1**.

Sowohl für den ausgehenden dienstlichen E-Mail-Verkehr als auch für die Internet-Nutzung stößt eine automatisierte Vollkontrolle im Hinblick auf das Persönlichkeitsrecht der Beschäftigten auf erhebliche Bedenken, denn sämtliche Maßnahmen der Inhaltskontrolle und Protokollierung sind geeignet, die Beschäftigten einer kirchlichen Stelle zu überwachen und ihre Leistung und ihr Verhalten zu kontrollieren. Daher muss für die Betroffenen transparent sein, welche potenziell zur Überwachung ihres Verhaltens geeigneten Maßnahmen aktiviert sind. Derartige Maßnahmen unterliegen außerdem ohne Ausnahmen der Mitbestimmung der gewählten Mitarbeitervertretungen. Wir empfehlen, die Mitarbeitervertretungen schon bei der Planung und Einführung der E-Mail- und Internet-Nutzung zu beteiligen. Es bietet sich an, in entsprechenden Dienstvereinbarungen das Verfahren der Protokollierung, der Kontrolle und der Auswertung der Protokolle verbindlich zu regeln. Diese Regelung kann auch vorsehen, dass eine Protokollierung nur in begründeten Verdachtsfällen (z. B. unerwünschte Nutzung) geschieht. Die Protokollierung ist so auszugestalten, dass ein datenschutzrechtlicher Missbrauch vermieden wird, das heißt:

- Der Umfang der Protokolle sollte im Rahmen des Möglichen minimal sein,
- auf Grund des kirchlichen Datenschutzgesetzes dürfen Protokolldaten nicht für andere Zwecke verwendet werden,
- Protokolle sind durch Zugriffsmaßnahmen vor unbefugter Kenntnisnahme zu sichern,
- es sind technisch-organisatorische Auswertungsverfahren festzulegen,
- es sind möglichst kurze Löschfristen vorzusehen.

4. Staatliche Rechtsvorschriften im Internet

Die zitierten staatlichen Rechtsvorschriften sind auch über das Internet abrufbar:

http://jurcom5.juris.de/bundesrecht/index.html

www.lvz-muenchen.de/~rgerling/gesetzen/index.htm

www.netlaw.de/gesetze/index.htlm

Anlage 2

Muster-Dienstvereinbarung zur Nutzung des Internets und der E-Mail-Dienste im Bereich der Ev. Kirche von Westfalen – Stand: 6. Juli 2001 –

Die folgende Muster-Dienstvereinbarung regelt sehr detailliert die Inhaltskontrolle und die Protokollierung bei dienstlicher Telekommunikation. Es ist zu beachten, dass aus Sicht des Datenschutzes „ein Weniger an Kontrolle“ immer zulässig ist.

Die Muster-Dienstvereinbarung wird in der Regel nie genau auf die eigentliche Situation der kirchlichen Stelle passen und ist daher entsprechend den organisatorischen und technischen Gegebenheiten vor Ort anzupassen.

Muster-Dienstvereinbarung

Zwischen ..... und der Mitarbeitervertretung der .....

(Name der kirchlichen Stelle) (Name der kirchlichen Stelle)

wird folgende Dienstvereinbarung nach § 36 Mitarbeitervertretungsgesetz (MVG)[1] geschlossen:

Inhaltsübersicht

1 Nr. **780**.

§ 1
Gegenstand der Dienstvereinbarung

Die Dienstvereinbarung regelt die Nutzung des Internets und der E-Mail-Dienste durch die Mitarbeiterinnen und Mitarbeiter bei .....

(Name der kirchlichen Stelle)

§ 2
Zielsetzung

Die Nutzung des Internets soll die Mitarbeiterinnen und Mitarbeiter in die Lage versetzen,

- sich über das World Wide Web (WWW) die für ihre Arbeit benötigten Informationen in kurzer Zeit zu verschaffen,
- über den E-Mail-Dienst die rasche Kommunikation und den Austausch von elektronischen Dokumenten vorzunehmen.

§ 3
Dienstliche Nutzung

[1]Die Nutzung des Internets und der E-Mail-Dienste ist ausschließlich zu dienstlichen Zwecken gestattet und auf das notwendige Maß zu beschränken. [2]Die Nutzung entgeltpflichtiger Angebote im Rahmen der Informationsbeschaffung (z. B. juristische Abfragen aus Datenbanken) bedarf einer Genehmigung.

§ 4
Internet-Zugänge/Schulungen

(1) Für gelegentliche Informationsbeschaffung steht ein zentraler Internet-Zugang an einem dafür eingerichteten Arbeitsplatz zur Verfügung .....

(ggf. Standort angeben)

(2) [1]Für dienstliche Aufgaben mit dauerhaftem Nutzungsbedarf ist die Einrichtung eines Internet-Anschlusses am Arbeitsplatz einer Mitarbeiterin oder eines Mitarbeiters möglich. [2]Dazu ist ein begründeter Antrag an die Leitung der kirchlichen Stelle zu richten.

(3) Im Rahmen vom Schulungen wird über den Aufbau des Internets, sparsame Benutzungsmöglichkeiten, Hilfestellungen zur Benutzung von Browsern und Suchmaschinen sowie über Datensicherheits- und Datenschutzaspekte informiert.

§ 5
E-Mail-Nutzung

(1) [1]E-Mails werden als ein Medium der flüchtigen und spontanen Kommunikation angesehen, das insoweit mit dem Telefon vergleichbar ist. [2]Bei rechtsverbindlichen Äußerungen ist die Verwendung von E-Mails nicht ausreichend.

(2) Für alle Mitarbeitenden wird das E-Mail-Programm GroupWise zur dienstlichen internen und externen Nutzung zur Verfügung gestellt.

(3) Einzelheiten zur Nutzung der E-Mail- und PC-Fax-Dienste werden durch Dienstanweisung geregelt.

§ 6
Allgemeine Schutzmaßnahmen

(1) Die Mitarbeiterinnen und Mitarbeiter haben die Bestimmungen des Datenschutzes zu beachten.

(2) Aus Sicherheitsgründen ist es untersagt,

- einen nicht von der DV-Systemverwaltung bereitgestellten Internet-Anschluss (z. B. Modem) zu nutzen;
- Änderungen in den Voreinstellungen des Internet-Zugangs am Arbeitsplatz-PC vorzunehmen;
- Programme (auch Spiele) aus dem Internet per Download auf den Arbeitsplatz-PC zu laden;
- Seiten mit pornographischen, gewaltverherrlichenden oder rassistischen Inhalten aufzurufen;
- sich fremde Zugangsberechtigungen zu verschaffen oder eigene Zugangsberechtigungen an Dritte weiterzugeben;
- sensible – insbesondere personenbezogene oder vertrauliche – Daten ohne sichere Verschlüsselung über das externe Internet zu übermitteln.

(3) Beim Auftreten sicherheitsrelevanter Ereignisse (ungewöhnliches Systemverhalten, unerklärlicher Verlust oder Veränderung von Daten und Programmen, Verdacht auf unzulässige Internetnutzung) ist die Systemverwaltung umgehend zu informieren.

§ 7
Schutzmaßnahmen (Inhaltskontrolle, Protokollierung)

(1) [1]Auf sämtlichen am E-Mail-Verkehr und an der Internet-Nutzung beteiligten PCs und Servern werden Informationen zum Übertragungs- und Nutzungsverhalten gespeichert.

[2]Zum Schutz des internen Computernetzes vor Angriffen durch Hacker, vor Viren und anderen schädlichen Inhalten finden Inhaltskontrollen und Protokollierungen (z. B. zum Erkennen von Missbrauch) des Datenverkehrs automatisiert statt.

(2) Als Inhaltskontrollen werden durchgeführt:

- die Kontrolle der empfangenen/zu versendenden E-Mails auf Viren (zentrale Virenscannung);
- Kontrolle der eingehenden http-Daten auf ActiveX-Controlls und Java-Applets.

(3) [1]Protokolliert wird ausschließlich der via Gateway über das landeskirchenweite Intranet und das (externe) Internet abgewickelte Datenverkehr. [2]Die Nutzung des Intranets der ..... (Netzwerk) wird nicht protokolliert.

(Name der kirchlichen Stelle)

[3]Es werden folgende Daten protokolliert:

1. Dienstliche Kennung des Benutzers oder des PCs, von dem aus zugegriffen wurde,
2. Datum und Uhrzeit,
3. die Dauer der Übertragung der Daten,
4. Menge der übertragenen Daten in Byte,
5. Adresse des Zielrechners, auf den zugegriffen wird,
6. URL (interner Pfad auf dem Zielrechner, der angibt, wo sich die abgerufenen Information dort befindet),
7. (gegebenenfalls:) weitere Informationen (genau beschreiben, z. B. vollständiger Header der übertragenen Datenpakete).

[4]Die Protokolldaten werden für einen Zeitraum von einem Monat aufbewahrt und dann wochenweise von der DV-Systemverwaltung gelöscht.

(4) [1]Weitere Kontrollmaßnahmen finden nicht statt. [2]Insbesondere werden eingehende Informationen (E-Mails und WWW-Abrufe) nicht anhand von Suchwörtern auf bestimmte Inhalte geprüft.

§ 8
Durchführung der Inhaltskontrollen

(1) [1]Die Kontrolle der eingehenden E-Mail erfolgt ausschließlich automatisiert. [2]Finden sich in eingehenden E-Mails Viren oder andere schädliche Inhalte, so entscheidet die DV-Systemverwaltung, ob sie zurückgeschickt, gelöscht oder geöffnet werden. [3]Die Mitarbeiterin oder der Mitarbeiter, an die oder den die E-Mail gerichtet war, wird informiert.

(2) Die Mitarbeiterinnen und Mitarbeiter werden darauf hingewiesen, dass ihnen bestimmte Funktionen einiger Internet-Angebote nicht zur Verfügung stehen, weil ActiveX-Controls und Java-Applets ausgefiltert werden.

§ 9
Auswertung der Protokolldaten

(1) [1]Die Protokolldaten dürfen ausschließlich für die im Folgenden aufgeführten Zwecke verwendet werden. [2]Eine nachträgliche Änderung des Zwecks oder eine Verwendung zu anderen Zwecken (z. B. Verhaltens-/Leistungskontrolle) ist ausgeschlossen.

(2) [1]Für das Erkennen und Beseitigen technischer Probleme, für die Optimierung der Netzlastverteilung, zum Erkennen und zur Abwehr von Angriffen dürfen die oben in § 7 Abs. 3 unter den Nummern 2 bis 7 genannten Protokolldaten verwendet werden. [2]Der Zugriff auf diese Daten zu den genannten Zwecken ist nur den mit der DV-Systemverwaltung betrauten Mitarbeiterinnen und Mitarbeitern gestattet.

(3) [1]Für Zwecke der Kontrolle der dienstlichen Nutzung des Internet-Anschlusses und der E-Mail-Nutzung dürfen die oben in § 7 Abs. 3 unter den Nummern 2 bis 7 genannten Protokolldaten verwendet werden.

[2]Die Kontrolle darf nur gemeinsamen durch Vertreter der Dienststellenleitung und der Mitarbeitervertretung erfolgen. [3]Es werden dabei keine Protokolldaten verwendet, die älter als eine Woche sind.

[4]Stellen sich bei der Kontrolle Anhaltspunkte für eine missbräuchliche Nutzung des Internet-Anschlusses heraus, so werden alle Mitarbeiterinnen und Mitarbeiter darauf hingewiesen, dass im Wiederholungsfall die Kontrolle des persönlichen Nutzungsverhaltens erfolgen kann. [5]Missbräuchliche Nutzung ist vor allem der Zugriff auf solche Informationen im Internet, die dienstlich nicht erforderlich sind. [6]Häufen sich die missbräuchlichen Zugriffe auf bestimmte URL, werden diese gesperrt.

[7]Finden sich bei einer erneuten Kontrolle wiederum Anhaltspunkte für eine missbräuchliche Nutzung, so werden auch die nach § 7 Abs. 3 Nr. 1 gespeicherten Protokolldaten herangezogen, um festzustellen, welche Mitarbeiterin oder welcher Mitarbeiter für den Missbrauch verantwortlich ist. [8]Es wird sichergestellt, dass auf diese Daten nur durch Vertreter der Dienststellenleitung, die für den Datenschutz fachlich zuständigen Personen (zukünftig die oder der Behördenbeauftragte für den Datenschutz), die oder der Betriebsbeauftragte für den Datenschutz/Vertreterinnen und Vertreter der Mitarbeitervertretung[1] gemeinsam zugegriffen werden kann. [9]Technisch wird dies dadurch realisiert, dass der zusätzliche Zugriff nur bei Verwendung zweier Passwörter oder eines geteilten Passworts (Vier-Augen-Prinzip) möglich ist.

---

1 Unzutreffendes streichen

[10]Den betreffenden Mitarbeiterinnen und Mitarbeitern ist Gelegenheit zur Stellungnahme zu geben, wobei die Protokolldaten möglichst nicht älter als 2 Wochen sein sollten. [11]Im Einzelfall kann den Mitarbeiterinnen und Mitarbeitern, denen eine missbräuchliche Nutzung nachgewiesen werden kann, der Zugang zum Internet oder zum E-Mail-Programm entzogen werden. [12]Weitere dienst- oder arbeitsrechtliche Maßnahmen bleiben unberührt.

(4) [1]Wurden Informationen aus Protokolldaten unter Nichtbeachtung der o. a. Regelungen gewonnen, so dürfen sie nicht zur Grundlage personeller Einzelmaßnahmen gemacht werden. [2]Ihre Verwendung als Beweismittel für solche Maßnahmen ist nicht zulässig.

An die Stelle von § 7 Abs. 3 und § 9 kann folgende wesentlich vereinfachte Regelung treten: „Bei eingehenden Daten werden nur die abgewiesenen Verbindungen protokolliert. Es erfolgt keine Protokollierung der ausgehenden Daten. Zusätzliche Protokollierungen werden im Einzelfall vorgenommen, wenn sicherheitskritische Ereignisse eintreten, insbesondere, wenn konkrete Angriffe auf das System erkennbar werden. In diesen Fällen erfolgt unverzüglich die Benachrichtigung der Mitarbeitervertretung sowie der für den Datenschutz zuständigen Personen (zukünftig der oder des Behördenbeauftragten für den Datenschutz) / der oder des Betriebsbeauftragten für den Datenschutz. Der Mitarbeitervertretung und die für den Datenschutz zuständigen Personen (zukünftig die oder der Behördenbeauftragte für den Datenschutz)/die oder der Betriebsbeauftragte für den Datenschutz/die Vertreterinnen und Vertreter der Mitarbeitervertretung[1] sind zur Auswertung der Protokolldaten heranzuziehen.“

§ 10
Wartung

Externe Personen, die Wartungsarbeiten an der Hard- und Software des Internetzugangs oder des E-Mail-Dienstes durchführen, sind zu verpflichten, dass sie die ihnen zur Kenntnis gelangten personenbezogenen Daten und Informationen weder weitergeben noch verwenden dürfen.

§ 11
Technische Weiterentwicklung

Die Mitarbeitervertretung sowie die für den Datenschutz zuständigen Personen (zukünftig die oder der Behördenbeauftragte für den Datenschutz)/die oder der Betriebsbeauftragte für den Datenschutz werden über geplante Verfahrens-, Programmänderungen frühzeitig informiert.

1 Unzutreffendes streichen

§ 12
Internet-Anschluss für die Mitarbeitervertretung

Die Mitarbeitervertretung erhält auf Antrag einen eigenen E-Mail-Anschluss. Sie erhält die Möglichkeit, sich den Mitarbeitern und Mitarbeiterinnen im internen Netz der kirchlichen Stelle zu präsentieren.

§ 13
Einhaltung der Dienstvereinbarung

Die Einhaltung der Datenverarbeitungsbestimmungen dieser Dienstvereinbarung wird durch die für den Datenschutz zuständigen Personen (zukünftig der oder die Behördenbeauftragte/r für den Datenschutz), die Betriebsbeauftragte oder den Betriebsbeauftragten für den Datenschutz[1] und durch die Mitarbeitervertretung überwacht.

§ 14
In-Kraft-Treten

(1) Die Dienstvereinbarung tritt am Tag nach ihrer Unterzeichnung in Kraft.

(2) Alle Mitarbeitenden erhalten ein Exemplar der Dienstvereinbarung.

Ort, Datum, Unterschriften

1 Unzutreffendes streichen.

Anlage 3

Muster-Dienstanweisung für die Versendung und den Empfang elektronischer Post (E-Mail) und Telefax-Schreiben vom Arbeitsplatz (PC-Fax) im Bereich der Ev. Kirche von Westfalen – Stand: 6. Juli 2001 –

Die Muster-Dienstanweisung ist in der Regel den technischen und organisatorischen Gegebenheiten vor Ort anzupassen.

Inhaltsverzeichnis

Die Nutzung des Internets und der E-Mail-Dienste werden für alle Mitarbeiterinnen und Mitarbeiter durch Dienstvereinbarung vom ..... geregelt. Nach § 5 „E-Mail-Nutzung“ werden Einzelheiten zur Nutzung der E-Mail- und PC-Fax-Dienste durch Dienstanweisung geregelt.

1. Geltungsbereich

Diese Dienstanweisung gilt für den Betrieb und die Nutzung der bei der

.....

(Name der kirchlichen Stelle)

bereitgestellten Dienste für die Versendung und den Empfang von elektronischer Post (E-Mail) sowie von Telefax-Schreiben unmittelbar über den Personalcomputer (PC-Fax). Andere Dienstanweisungen über den EDV-Einsatz, den Datenschutz und die Datensicherheit sowie sonstige spezielle Regelungen bleiben unberührt.

2. Allgemeine Grundsätze

Elektronische Post (E-Mail) kann als Kommunikationsmittel zur Beschleunigung und Vereinfachung von Verwaltungsvorgängen genutzt werden, soweit keine technischen, rechtlichen oder wirtschaftlichen Gründe dem entgegenstehen. Die Dienstanweisung regelt Empfang und Versand elektronischer Dokumente.

Dokumente im Sinne dieser Regelung ist Schriftgut mit dienstlichem Inhalt, das nach den allgemeinen Grundsätzen der Schriftgutverwaltung dauerhaft zu den Akten zu nehmen ist (gegebenenfalls konkrete Dienstanweisung zitieren).

Nachrichten untergeordneter Bedeutung, die Beschäftigten unmittelbar zugehen bzw. durch diese versandt werden können und die üblicherweise nicht zu den Akten zu nehmen sind, z. B. Arbeitsentwürfe von Arbeitsgruppen, Terminabstimmungen, Fachinformationen und Ähnliches, sind in der Regel keine Dokumente im Sinne dieser Dienstanweisung. Diese Nachrichten können im Dokumentenverwaltungssystem für einen begrenzten Zeitraum gespeichert werden.

Der E-Mail- und der PC-Fax-Dienst dürfen grundsätzlich nur für dienstliche Zwecke genutzt werden.

3. Organisatorische Grundsätze

Voraussetzung für die direkte Teilnahme von Mitarbeiterinnen und Mitarbeitern am elektronischen Postdienst ist ein Arbeitsplatzcomputer mit E-Mail- und/oder PC-Fax-Funktionalität einschließlich der organisatorischen und funktionsbezogenen Zugangsberechtigung.

Elektronische Dokumente sind, soweit sie für den Geschäftsgang von Bedeutung sind, in Papierform zu den Akten zu nehmen. Weitere Einzelheiten sind insbesondere unter Ziffer 4 „Empfang von elektronischen Dokumenten“ und unter Ziffer 5 „Versand von elektronischen Dokumenten“ geregelt.

Es ist dabei sicherzustellen, dass sich Verfügung, Abzeichnung, Schlusszeichnung sowie elektronische Zustellungsnachweise beim Vorgang befinden.

4. Empfang von elektronischen Dokumenten

4.1 Unmittelbarer Zugang von elektronischen Dokumenten an einzelne Mitarbeitende:

Jede Mitarbeiterin oder jeder Mitarbeiter hat das jeweilige elektronische Postfach regelmäßig, mindestens jedoch einmal täglich zu überprüfen.

Die Empfängerin oder der Empfänger der E-Mail oder des PC-Faxes oder die vertretende Person entscheidet selbst, ob die Dokumente in den Geschäftsgang einzusteuern sind. Zu diesem Zweck sind die elektronischen Dokumente auszudrucken und der Poststelle zur Registrierung und Weiterleitung zu übergeben. Die Vorgesetzten sind in geeigneter Weise über elektronische Posteingänge zu unterrichten, soweit dies wegen der Bedeutung des Vorgangs geboten ist.

Ist die Empfängerin oder der Empfänger der E-Mail oder des PC-Faxes nicht zuständig, wird die E-Mail unverzüglich an den zuständigen Adressaten weitergeleitet, soweit dieser im elektronischen Adressbuch enthalten ist. Im anderen Fall erfolgt die Weiterleitung an die elektronische Poststelle oder das elektronische Dokument ist auszudrucken und in Papierform weiterzugeben. Die empfangene E-Mail sollte auch aus dem eigenen Postfach gelöscht werden.

Elektronisch versandte Nachrichten können im Anhang Anlagen enthalten, die im Einzelfall Computerviren oder sonstige Schadensfunktionen enthalten können. Soweit kein zentrales Virenscannung erfolgt, müssen die E-Mails einschl. Anhänge auf Viren in jedem Einzelfall überprüft werden.

Die im Rahmen des E-Mail-Systems gespeicherten elektronischen Dokumente sollen gelöscht werden, wenn ihre Speicherung zur Aufgabenerfüllung nicht mehr erforderlich ist.

4.2 Eingang von elektronischen Dokumenten bei der zentralen elektronischen Poststelle:

Geht eine E-Mail bei der elektronischen Poststelle mit der Adresse

.....@.....

(Bezeichnung angeben)

ein, so ist diese für den Empfang, die Speicherung und die Weiterleitung der elektronischen Posteingänge verantwortlich.

Die Aufgaben der elektronischen Poststelle sind:

- Das Postfach für elektronische Dokumente an allen Arbeitstagen regelmäßig, mindestens jedoch einmal vormittags und einmal nachmittags zu überprüfen.
- Im Postfach gespeicherte elektronische Dokumente an eindeutige Empfänger weiterzuleiten oder die eingegangenen Dokumente auszudrucken, mit dem Eingangsstempel zu versehen und in den Geschäftsgang zu geben.
- Die eingegangenen Dokumente elektronisch zu verwalten (Registrierung, Ablegen, Löschen des Postfaches).

- Fehlgeleitete elektronische Post ist an den richtigen Empfänger weiterzuleiten oder der Absender ist über die unrichtige Zuständigkeit zu informieren.

5. Versand von elektronischen Dokumenten

5.1 Zum Versand geeignete Dokumente

Per E-Mail oder PC-Fax dürfen grundsätzlich alle Schreiben und sonstigen Dokumente versandt werden, für die nicht zwingend eine eigenhändige Unterschrift vorgesehen ist oder bei denen sonstige Formvorschriften (Einhaltung des Dienstweges) nicht entgegenstehen. Bei rechtsverbindlichen Äußerungen ist die Verwendung von E-Mails oder PC-Faxen nicht ausreichend.

Die zu versendenden Dokumente sollten speicherminimiert sein (z. B. ohne grafische Elemente).

5.2 Prüfung der Versandadresse

Der Absender ist dafür verantwortlich, dass die E-Mail oder das PC-Fax alle erforderlichen Angaben zum Absender und Adressaten enthält.

Die elektronische Versandadresse muss mit der im Text des elektronischen Dokumentes angegebenen Anschrift übereinstimmen.

Technische Möglichkeiten zur Verhinderung von Fehlleitungen, wie z. B. die Nutzung von hinterlegten Adressen (Adressbücher, Verteilerlisten) oder der Versand aus dem Dokument heraus, sollen genutzt werden.

6. Aufbau der elektronischen Dokumente

6.1 Erforderliche Angaben

Die E-Mail muss die Angaben zum Absender (kirchliche Stelle, Abteilung oder Dezernat, bearbeitende Person, Geschäftszeichen, Datum, Telefon, Fax) und zum Adressaten (Versandadresse = Adresse auf dem Dokument) enthalten.

6.2 Formate

Elektronische Dokumente dürfen nur in einem festgelegten und für den Adressaten verarbeitbaren Format versandt werden. Auf komplizierte Formatierungen und Grafiken sollte verzichtet werden.

6.3 Anlagen in E-Mails

Die in einem elektronischen Dokument beigefügten Anlagen sind im Anschreiben einzeln aufzuführen, um der empfangenden Stelle oder Person eine Überprüfung der Anzahl und des Formats der Anlagen zu ermöglichen.

Anlagen sind im Originalformat zu versenden. Datenformate, die nicht allgemein gebräuchlich sind, sollen nur dann als Anlage versandt werden, wenn bekannt ist, dass die empfangende Stelle oder Person dieses Datenformat auch verarbeiten kann. Umfangreiche Anlagen sollen komprimiert werden, soweit bei der empfangenden Stelle oder Person eine Dekomprimierung möglich ist.

6.4 Schlusszeichnung; Zeichnungsbefugnis

Schreiben, die elektronisch hergestellt und versandt werden, sind mit der Namensangabe unter dem elektronischen Dokument zu versehen. Sofern absendende Person und unterzeichnende Person nicht identisch sind, hat die absendende Person vor Absendung des Dokuments die Zustimmung der unterzeichnenden Person hierzu einzuholen und zu dokumentieren.

6.5 Dokumentation

Zur Dokumentation ist die elektronische Absendebestätigung zusammen mit dem Text des Dokumentes auszudrucken und zu den Akten zu nehmen. Anstelle der Absendebestätigung kann auf dem für die Akten bestimmten Ausdruck des Dokuments auch handschriftlich das Datum, die Uhrzeit der Absendung und das Namenszeichen der absendenden Person vermerkt werden.

Sofern der Zugang eines elektronisch versandten Dokuments nachgewiesen werden muss, ist zusätzlich die automatische Zustellbestätigung auszudrucken und zu den Akten zu nehmen.

7. Datenschutz und Datensicherheit

7.1 Datenschutz bei Dokumenten mit personenbezogenen Daten

Innerhalb der Ev. Kirche von Westfalen besteht ein kirchliches Intranet, bei dem das Produkt GroupWise zum Einsatz kommt, das die Verschlüsselung aller E-Mails ermöglicht. Damit ist es zulässig, auch Dokumente mit vertraulichen oder personenbezogenen Daten zu einer kirchlichen Stelle, die dem kirchlichen Intranet angehört, zu versenden, da innerhalb des kirchlichen Intranets eine automatische Verschlüsselung erfolgt.

Die elektronische Übermittlung von Dokumenten mit vertraulichen oder personenbezogenen Daten **an externe Stellen oder Personen (außerhalb des kirchlichen Intranets)** ist ausnahmsweise zulässig, als durch geeignete zusätzliche Maßnahmen, insbesondere einer Verschlüsselung, eine angemessene Datensicherheit gewährleistet wird.

7.2 Mailing von Software

Das Mailing von ausführbarer Software ist aus Sicherheits- und Urheberrechtsgründen prinzipiell unzulässig. Nur in begründeten Ausnahmefällen und mit Zustimmung der DV-Systemverwaltung ist dies erlaubt. Unzulässig empfangene Software darf nicht angewandt werden.

7.3 Virenschutz

Die Empfänger von E-Mails sind für die Prüfung der eingehenden Dateien auf eventuelle Schadfunktionen (Viren) zuständig. Hierfür ist geeignete Virenschutzsoftware einzusetzen, soweit nicht zentral im Netzwerk ein Virenscanner installiert ist. Über eingegangene Dateien mit Schadensfunktionen sind die DV-Systemverwaltung und der Absender zu informieren.

7.4 Rechte

E-Mail darf nur von den dazu berechtigten Bediensteten genutzt werden.

7.5 Protokollierung/Serversicherheit

Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen E-Mail-Betriebes erhoben und gespeichert werden (Protokolldaten), unterliegen der Zweckbindung nach § 5 Absatz 1 des Kirchengesetzes über den Datenschutz der Ev. Kirche in Deutschland. Eine Auswertung solcher Daten erfolgt nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiterinnen und Mitarbeiter.

8. Technische Betreuung und Schulung

Die für das Versenden und den Empfang von E-Mails und von PC-Fax-Schreiben notwendige Software wird von der DV-Systembetreuung zur Verfügung gestellt. Technische Probleme und Fragestellungen sind der DV-Systembetreuung mitzuteilen.

Die Benutzung des E-Mail-Systems sowie der Einsatz von PC-Fax setzt eine Einweisung der Mitarbeiterinnen und Mitarbeiter durch die zuständigen Personen (DV-Systemverwaltung oder Fachbereich) voraus.

9. Merkblatt zur sicheren E-Mail-Nutzung

Die im Merkblatt der Ev. Kirche von Westfalen enthaltenen Hinweise für eine sichere E-Mail-Nutzung sind zu beachten.

10. In-Kraft-Treten

Diese Dienstanweisung tritt am … in Kraft.

Anlage 4

Merkblatt der Ev. Kirche von Westfalen[1]
für eine sichere E-Mail-Nutzung
– Stand: 6. Juli 2001 –

1. Allgemeine Schutzmaßnahmen

- Nutzen Sie das E-Mail-System ausschließlich dienstlich.
- E-Mails sollten keine Inhalte enthalten, die Sie nicht auch in Papierform veröffentlichen würden.
- Sofern kein zentrales Virenscanning erfolgt, sollte am PC-Arbeitsplatz stets ein aktuelles Virenschutzprogramm eingesetzt werden, das im Hintergrund läuft und bei bekannten Computerviren Alarm schlägt.
- Nur innerhalb des landeskirchlichen Intranets (im Bereich des einheitlichen Meldewesens) wird über den Einsatz des Mailprogramms GroupWise eine Verschlüsselung sichergestellt. Versenden Sie daher außerhalb dieses Bereiches, insbesondere an externe E-Mail-Empfänger, keine sensitiven Informationen, außer wenn beide Seiten eine zusätzliche Verschlüsselung sicherstellen.
- Bitte Passwörter für Mailprogramme auf keinen Fall dauerhaft speichern, da die Passwörter oft im Klartext auf der Festplatte abgelegt werden (Sicherheitsrisiko).
- Um Bedrohungen wie E-Mail-Bomben entgegen zu wirken, sollte die eigene E-Mail-Adresse nur gezielt weitergegeben werden, deshalb
  - in der Regel keine Artikel in Newsgruppen posten
  - sich nur auf vertrauenswürdigen Mailinglisten eintragen.

2. Hinweise zur Behandlung eingehender E-Mails

2.1 Allgemeine Regeln

- Vorsicht beim Umgang mit nicht sinnvollen E-Mails unbekannter Absender, am besten sofort löschen.
- Vertrauen Sie nicht auf Absenderangaben. E-Mail-Adressen können leicht gefälscht werden. Deshalb prüfen Sie E-Mails von vermeintlich bekannten Absendern darauf, ob der Text der Nachricht auch zum Absender passt und ob die Anlage auch erwartet wurde.

1 Das Merkblatt ist den technischen und organisatorischen Gegebenheiten vor Ort anzupassen.

- Nur vertrauenswürdige E-Mail-Anlagen öffnen (z. B. nach telefonischer Absprache). Es ist zu beachten, dass die Art des Dateianhangs (Attachment) bei Sabotageangriffen oft getarnt ist und in seiner Form als Icon nicht als sicher erkannt werden kann.
- Aktivieren Sie den Makro-Virenschutz von Anwendungsprogrammen (Winword, Excel und andere) und beachten Sie die Warnmeldungen.
- Anlagen von außerhalb
  - in Form von ausführbaren Programmen (*.com, *.exe),
  - Scriptsprachen (*.vbs, *.bat),
  - Bildschirmschonern (*.scr) und
  - gepackter komprimierter Form
  - von nicht von der kirchlichen Stelle zugelassenen Programme

  sind vor dem Öffnen der DV-Systemverwaltung zur Prüfung zuzuleiten.
- Besondere Vorsicht ist geboten beim Öffnen von Anlagen, die Sie von außerhalb erhalten:

  

  Anlagen bitte zunächst in einem Download-Verzeichnis speichern, auf Viren scannen und erst danach zur weiteren Verarbeitung öffnen.
- Bitte die organisatorischen Regelungen zur Behandlung eingehender E-Mails (regelmäßige Überprüfung des elektronischen Postfachs, Geschäftsgang, Weiterleitung, Ausdruck für die Akten) beachten.
- Sofern kein zentrales Virenschutzprogramm eingesetzt wird, sollte man keine Dateien ungeprüft weiterleiten.
- Elektronische Dokumente bitte nur so lange speichern, wie dies zur Aufgabenerfüllung erforderlich ist, ansonsten regelmäßig löschen oder eine automatisierte Löschung vorsehen.

2.2 Empfohlener Umgang beim Einsatz von GroupWise mit E-Mail-Anlagen (Attachment)

- Aktivieren Sie bei der erstmaligen Ansicht von E-Mails mit GroupWise in der Menü-Leiste/Symbolleiste grundsätzlich die „Blitzvorschau“. Darüber können Sie Nachrichten und Dokumente nur anzeigen, aber nicht bearbeiten.
- Aktivieren Sie in der Symbolleiste der Blitzvorschau das Symbol „Anlagenfenster“.

- Sehen Sie sich in der Blitzvorschau von GroupWise zunächst die Anlage der E-Mail an (Mauszeiger auf die Anlage, rechte Maustaste „Öffnen“).
- Speichern Sie zur weiteren Bearbeitung die Anlage in ein Zwischenverzeichnis (z. B. „Download“).
- Scannen Sie die Anlage in diesem Verzeichnis auf Viren.
- Speichern Sie dann die Anlage in das endgültige Verzeichnis.
- Öffnen Sie nun die Anlage über die Standardsoftware und bearbeiten Sie diese weiter.

2.3 Besondere Hinweise für gepackte (komprimierte) Anlagen

- Sofern auf Ihrem PC ein Entpackungsprogramm installiert ist, sollte es so konfiguriert sein, dass zu entpackende Dateien nicht automatisch gestartet werden.
- Anhänge in Form von gepackten (komprimierten) Dateien sollen erst in einem „Download“ Verzeichnis entpackt und dann auf Viren geprüft werden, bevor sie im System in entpackter Form genutzt werden.

3. Hinweise zur Behandlung ausgehender E-Mails

- Das E-Mail-System ausschließlich dienstlich nutzen, deshalb keine unnötigen E-Mails mit Scherz-Programmen oder Ähnliches versenden, da diese häufig virenträchtig sind.
- E-Mails möglich nicht im HTML-Format versenden.
- Winword-Dokumente verbergen das Risiko einer Verbreitung von Makro-Viren, deshalb prüfen, ob diese im externen Bereich im RTF-Format versandt werden können.
- Bitte möglichst hinterlegte Adressbücher und Verteilerlisten nutzen, um Fehlleitungen zu verhindern.
- Bei Rückantworten (Replay): Die bei einem Replay übernommene E-Mail-Anschrift bitte daraufhin überprüfen, ob sie korrekt ist. Sie kann durch Konfigurationsfehler inhaltlich falsch oder auch vorsätzlich gefälscht worden sein.
- Bei Virenwarnungen handelt es sich oft um irritierende und belästigende Mails mit Falschmeldungen (sog. Hoax-Viren). Bitte nicht an Freunde, Bekannte oder Mitarbeitende, sondern nur an die DV-Systemadministration weiterleiten.
- Bitte die organisatorischen Vorgaben zum Versand von E-Mails beachten (Dienstweg, Beachtung von Formvorschriften, Aufbau der elektronischen Dokumente mit zwingend erforderlichen Angaben, Schlusszeichnung, Dokumentation).

- Bitte regelmäßig die E-Mails im Ausgangspostkorb überprüfen, ob sie von einem selbst verfasst wurden.