Orientierungshilfe
„Datenschutz in der Mitarbeitervertretung“[1]

(Stand: 07.02.2012)

Die Orientierungshilfe konzentriert sich auf die Themen, die für die Arbeit der Mitglieder in der Mitarbeitervertretung (MAV) aus datenschutzrechtlicher Sicht von Bedeutung sind:

I. Rechtsgrundlagen
II. Datengeheimnis/Schweigepflicht
III. Personalunterlagen, MAV-Vorgänge und kirchlicher Datenschutz
IV. Datenschutz- und Datensicherungsmaßnahmen

Die Orientierungshilfe richtet sich an die MAV und die Dienststellenleitungen der kirchlichen Stellen in der Ev. Kirche in Hessen und Nassau.

I. Rechtsgrundlagen

Die Mitarbeitervertretung hat bei der Wahrnehmung ihrer Tätigkeit kirchliches Datenschutzrecht zu beachten. Dies sind im Einzelnen:

1. Bereichsspezifische Datenschutzbestimmungen

1.1 Arbeitsrechtsregelungen (z. B. KDAVO);
1.2 Mitarbeitervertretungsgesetz (MAVG) und besondere Regelungen in anderen kirchlichen Rechtsvorschriften (z. B. § 24 DSG-EKD).

2. Allgemeine Datenschutzbestimmungen

2.1 Kirchengesetz über den Datenschutz der EKD (DSG-EKD);
2.2 Verordnung zur Durchführung des Kirchengesetzes über den Datenschutz der EKD (DSVO);
2.3 Kirchengesetz über den Einsatz von Informationstechnologie (IT) in der kirchlichen Verwaltung der Ev. Kirche von Westfalen (Geltungsbereich Kirchengemeinden);
2.4 Dienst- und Organisationsanweisungen für den Einsatz und Betrieb in der Informations- und Kommunikationstechnik (IuK-Technik) sowie für die Durchführung des Datenschutzes und der Datensicherheit, soweit sie von den kirchlichen Stellen erlassen wurden;
2.5 Dienstvereinbarungen zur IuK-Technik sowie für die Durchführung des Datenschutzes und der Datensicherheit, soweit entsprechende Vereinbarungen mit den kirchlichen Stellen geschlossen wurden.
2.6 die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zum Datenschutz und zur Datensicherheit, insbesondere die IT-Grundschutzkataloge in der jeweils aktuellen Fassung.

[1] Diese Orientierungshilfe wurde vom Arbeitskreis Datenschutz, dem als Mitglieder die Ev. Kirche im Rheinland (EKiR), die Ev. Kirche von Westfalen (EKvW), die Lippische Landeskirche (LLK) und deren Diakonischen Werke angehören, in seiner Sitzung am 28. März 2012 verabschiedet und vom Beauftragten für Datenschutz der EKHN und EKKW an die rechtlichen Rahmenbedingungen in der EKHN angepasst.

II. Datengeheimnis/Schweigepflicht

1. Grundsätzlich gilt für alle Mitarbeitenden das Datengeheimnis nach § 6 DSG-EKD i.V.m. § 2 DSVO, wonach es untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.
2. Zusätzlich gilt für die Mitglieder der MAV die Schweigepflicht nach § 20 MAVG (unabhängig von den arbeitsvertraglichen oder beamtenrechtlichen Schweigepflichten). Die Mitglieder der MAV sind verpflichtet, über die ihnen im Rahmen ihrer Aufgaben oder Befugnisse bekannt gewordenen Angelegenheiten und Tatsachen grundsätzlich Stillschweigen zu bewahren. Die MAV erhält sensible personenbezogene Informationen im Rahmen der Beteiligung in personellen Angelegenheiten oder durch die Mitarbeitenden selbst. Die allgemeinen Persönlichkeitsrechte dieser Mitarbeitenden gebieten es daher, dass Außenstehende keine Information über diese Daten erhalten. Ausgenommen von der Schweigepflicht sind offenkundige Tatsachen oder Angelegenheiten, deren Vertraulichkeit ausdrücklich ausgenommen ist. Ebenso wird mit Zustimmung der betroffenen Person die Schweigepflicht durchbrochen, wenn deren Angelegenheiten z. B. mit der Dienststelle besprochen werden sollen. Geheimhaltungspflichtig sind Personalangelegenheiten, bis das formelle Beteiligungsverfahren in den Fällen der Mitberatung und Mitbestimmung begonnen hat, insbesondere bis der MAV ein Antrag auf Zustimmung zu einer Maßnahme vorliegt. Dies ist damit zu begründen, dass in der Praxis viele Fälle vorstellbar sind, in denen eine Information der oder des Betroffenen nicht zweckmäßig sein dürfte, ehe die Dienststellenleitung eine klare Willensbildung vollzogen hat, etwa wenn eine Kündigung oder eine Beförderung erwogen oder wieder verworfen wird. Andererseits muss die MAV das Recht haben, im Rahmen des förmlichen Beteiligungsverfahrens (z. B. Antrag auf Zustimmung zu einer Maßnahme) die betroffene Person zu hören.

   Innerhalb der MAV gilt die Geheimhaltungspflicht nach § 22 Abs. 3 MAVG nicht. Eine Zusammenarbeit und auch viele Beschlüsse sind nur möglich, wenn die anderen Mitglieder ausreichend informiert sind. Innerhalb der MAV muss Offenheit und Zusammenarbeit das tragende Prinzip sein. Deshalb können auch Informationen aus Gesprächen, die einzelne Mitglieder mit Mitarbeitenden führen, innerhalb der Sitzung offenbart werde; es sei denn die betroffene Person hat dem ausdrücklich widersprochen.
3. Als Rechtsfolgen[2] bei Verletzung des Datengeheimnisses oder der Schweigepflicht sind denkbar:
   - Ausschluss eines Mitglieds aus der MAV bzw. Auflösung der MAV gemäß § 14 MAVG, wenn ein grober Missbrauch oder eine grobe Verletzung der Schweigepflicht vorliegt (z.B. ein MAV Mitglied plaudert bedenkenlos geheimhaltungspflichtige Tatsachen aus);
   - arbeitsrechtliche Sanktionen wie Abmahnung oder ordentliche und außerordentliche Kündigung (Verstoß gegen die Treuepflicht); bei Kirchenbeamtinnen und Kirchenbeamten auch entsprechend dienstrechtliche Sanktionen;
   - haftungsrechtliche Inanspruchnahme.

[2] Strafrechtliche Folgen auf Grundlage der §§ 203 Abs. 2 Nr. 3, 353b Abs. 1 Nr. 3 StGB sind ausgeschlossen (Fey/Rehren, MVG.EKD, § 22 Rdn. 14).

III. Personalunterlagen, MAV-Vorgänge und kirchlicher Datenschutz

1. Allgemeine Hinweise

1.1 Zur Vorbereitung von Entscheidungen in Personalangelegenheiten (z. B. Einstellung von Stellenbewerberinnen und -bewerbern, Veränderungen und Beendigung von Beschäftigungsverhältnissen) erhält die MAV von der Dienststellenleitung schriftliche Personalunterlagen zugesandt oder ausgehändigt (siehe auch § 22 MAVG). In diesem Zusammenhang hat die Dienststelle zu entscheiden, in welchem Umfang es für die Beratung in der MAV erforderlich ist, Personalunterlagen der MAV zur Verfügung zu stellen. Diese Unterlagen können allen Mitgliedern der MAV im Rahmen der Sitzung zugänglich gemacht werden.

1.2 Ein namentlich genanntes Mitglied der MAV darf die Personalakte einer Mitarbeiterin oder eines Mitarbeitenden nur einsehen, wenn die schriftliche Zustimmung der betroffenen Person eingeholt worden ist (§ 22 Abs. 3 MAVG).

1.3 Niederschriften über die Sitzungen der MAV enthalten die Beratungsergebnisse und geben zum Teil den Verlauf der Beratungen in vielen Details wieder. Bewerbungsunterlagen, die die MAV im Rahmen des förmlichen Beteiligungsverfahren erhalten kann, enthalten zum Teil sehr sensible Informationen, z. B. Zeugnisse, Beurteilungen, Anerkennung einer Schwerbehinderung. Über Gespräche mit Mitarbeitenden können von Mitgliedern der MAV Gesprächsvermerke gefertigt werde. Der Vertrauensschutz sowie die Fürsorgepflicht der kirchlichen Stellen gegenüber ihren Beschäftigten und ihren Stellenbewerberinnen und Stellenbewerben gebieten es, mit den Personalunterlagen sorgfältig umzugehen, sie sicher aufzubewahren und sie nur soweit zu offenbaren,

- als hierfür eine Rechtsgrundlage vorhanden ist,
- die betroffene Person zugestimmt hat oder
- die Personalangelegenheit von der Dienststellenleitung öffentlich gemacht wird (z.B. Bekanntgabe einer Umsetzung, Höhergruppierung, Beförderung durch die Dienststellenleitung).

2. Empfehlungen

2.1 Es ist zu prüfen, in welchem Umfang die MAV Personalunterlagen für eine Entscheidung benötigt[3]. Nach § 22 MAVG ist die MAV zur Durchführung ihrer Aufgaben rechtzeitig und umfassend zu unterrichten. Abs. 1 und 2 konkretisieren diese Verpflichtung dahingehend, dass die für die Entscheidungen der MAV „erforderlichen“ Unterlagen (bei Einstellungen auf Verlangen der MAV auch sämtliche Bewerbungen) vorzulegen sind.

2.2 Personalunterlagen (Kopien) sind seitens der Personalverwaltung deutlich mit einem hervorgehobenen Aufdruck als „streng vertrauliche Personalunterlagen“ zu kennzeichnen. Es empfiehlt sich, dass die von der Dienststelle zur Verfügung gestellten Personalunterlagen für den Beratungsprozess bei der oder dem Vorsitzenden verbleiben und im Rahmen des mündlichen Vortrags bei der MAV-Sitzung eingesehen werden können.

[3] Die Datenübermittlung von Personalunterlagen durch die Dienststelle an die MAV, die diese zur Erfüllung ihrer gesetzlichen Verpflichtungen benötigt (Erforderlichkeitsgrundsatz), unterliegt keinen besonderen Beschränkungen des Datenschutzrechts (Fey/Rehren, MVG.EKD, § 22 Rdn. 8a).

2.3 Soweit Personalunterlagen im Rahmen einer Einladung zu einer MAV-Sitzung versandt werden, ist deren Anonymisierung zu prüfen. An Stelle einer Anonymisierung kann auch eine Pseudonymisierung der Personalunterlagen vorgenommen werden. Dabei werden die identifizierenden Angaben zu einer Person (z. B. Name, Anschrift, Aktenzeichen) unkenntlich gemacht bzw. durch andere Namen und Bezeichnungen ersetzt. In der Sitzung können die Namen der Personen offenbart werden.

2.4 Personalunterlagen, die die oder der Vorsitzende bzw. die MAV-Mitglieder erhalten, dürfen nur im verschlossenen Umschlägen weitergegeben werden. Bei der Adressierung ist darauf zu achten, dass sie ausschließlich an das jeweilige MAV-Mitglied, ggf. mit dem Hinweis „persönlich“, erfolgt.

2.5 Bewerbungs- und Personalunterlagen sind nach Beendigung der MAV-Sitzung an die Dienststellenleitung zurück zu geben und von dieser auf Vollständigkeit zu prüfen. Das Kopieren dieser Unterlagen durch MAV-Mitglieder ist unzulässig.

2.6 Nicht mehr benötigte Personalunterlagen sind unverzüglich sachgerecht zu vernichten (z. B. mit einem Aktenvernichter der Sicherheitsstufe 3 nach DIN 32757[4]).

2.7 MAV-Akten (insbesondere die Niederschriften) sind, solange sie noch von rechtlicher Bedeutung sind, aufzubewahren[5]. Am Ende der Aufbewahrungsfrist ist wie folgt zu verfahren:

a. Soweit die MAV-Akten keine besonderen Vorkommnisse enthalten (z. B. Verfahren vor Schlichtungsstelle, Gutachten, ausführliche Gesprächsvermerke zu rechtlich relevanten Problemen), sind diese Unterlagen sachgerecht zu vernichten, ggf. ist die Archivwürdigkeit der MAV-Unterlagen mit dem zuständigen Archiv zu klären.
b. Die übrigen MAV-Unterlagen sind dem zuständigen kirchlichen Archiv zur Archivierung anzubieten. Soweit die Archivwürdigkeit der Unterlagen nicht vorliegt, sind sie mindestens unzugänglich (Sperrung) zu machen, sonst zu vernichten (siehe auch Punkt 2.6).

2.8 Die MAV sollte unter Beachtung dieser Orientierungshilfe grundsätzliche Regelungen über die Behandlung von Personalunterlagen treffen (ggf. in einer Geschäftsordnung nach § 24 Abs. 2 MAVG) und sich mit der Dienststellenleitung über das Verfahren verständigen.

2.9 Mitarbeitende kann es im Rahmen einer Heim-/Telearbeit erlaubt werden zu Hause zu arbeiten. Dies kann auch die Tätigkeit in der MAV mit einbeziehen. Soweit sie als MAV-Mitglieder Personalunterlagen und MAV-Vorgänge erhalten, sind neben den vertraglichen Regelungen zur Heim-/Telearbeit folgende Empfehlungen zu beachten:

a. Die Unterlagen sind sicher und für Dritte unzugänglich aufzubewahren.
b. Nicht mehr benötigte Personalunterlagen sind an die Dienststelle zurückzugeben.
c. MAV-Vorgänge (z. B. Gesprächsvermerke, Protokolle) sind, soweit sie nicht mehr benötigt werden oder Aufbewahrungsfristen bzw. Archivierungsvorschriften nicht zu beachten sind, sachgerecht und sicher zu entsorgen (z. B. über einen Aktenvernichter – siehe Punkt 2.7).

2.10 Bei Beendigung der Mitgliedschaft in der MAV haben die Mitarbeitenden alle in ihrem Besitz befindlichen Unterlagen, die sie in ihrer Eigenschaft als Mitglied der MAV erhalten haben, der MAV auszuhändigen (§ 21 Abs. 1 MAVG). In diesem Zusammenhang

[4] Zu den Sicherheitsstufen siehe: http://de.wikipedia.org/wiki/Aktenvernichter#Sicherheitsstufen_nach_DIN_32757

[5] Küfner-Schmitt, Berliner Kommentar zum MVG.EKD hält unter Bezugnahme auf § 257 Abs. 4 HGB und die Kommentierung Richardi/Thüsing, BetrVG, § 34 einen Zeitraum von 10 Jahren für ausreichend. MAV-Vorgänge mit rechtlicher Relevanz, die mehrere Amtsperioden betreffen, sind nach § 21MAVG der nachfolgenden MAV zu übergeben.

sind die Aufbewahrungsfristen und Archivierungsvorschriften zu beachten (siehe auch Punkt 2.7). Nicht mehr benötigte MAV-Unterlagen (insbesondere Duplikaten mit Gesprächsvermerken, Tagesordnungen, Protokollen usw.[Handakten]) sind sachgerecht und sicher zu entsorgen (z. B. über einen Aktenvernichter siehe Punkt 2.6).

2.11 Soweit eine MAV eigene Datenerhebungen (z. B. Fragebogenaktion zu Arbeitszeiten) vornimmt oder von der Dienststelle für ihre Tätigkeit die Grundstammdaten der Mitarbeitenden (Personalnummer, Name, Vorname, Geburtsdatum, Dienst- und Berufsbezeichnung, organisatorische Zugehörigkeit, Besoldung-, Vergütungs-, Lohngruppe, Beginn des Beschäftigungsverhältnisses, Vollzeit- oder Teilzeitbeschäftigung) erhält, unterliegen diese Daten und Dateien dem Datenschutz:

a. Allgemeine Anforderungen
   - Erforderlichkeit und Datensparsamkeit, Vorhaltung und Speicherung nur solange wie es für die Tätigkeit der MAV erforderlich ist (Zweckbestimmung),
   - regelmäßige Aktualisierung des Datenbestandes bzw. Löschung des veralteten Datenbestandes,
   - Löschungsfristen,
   - Datenübermittlungen (z. B. an Berufsverbände, Gewerkschaften) sind unzulässig.

b. ggf. Aufnahme in die Übersicht über die automatisierte Verarbeitung nach § 14 Abs. 2 DSG-EKD;

c. Kontrollrecht der oder des Gemeinsamen Datenschutzbeauftragten (§ 19 DSG-EKD),

d. Auskunftspflichten gegenüber anfragenden Personen (§ 15 DSG-EKD), Berichtigung, Löschung und Sperrung von Daten (§ 16 DSG-EKD),

e. Beachtung und Einhaltung der Vorgaben aus IT-Sicherheitskonzepten und der Dienst- und Organisationsanweisungen für den Einsatz und Betrieb der Informations- und Kommunikationstechnik sowie für die Durchführung des Datenschutzes und der Datensicherheit .

2.12 Anstelle der Übermittlung von Grundstammdaten der Mitarbeitenden kann die Dienststelle der MAV auch einen von den Zugriffsrechten entsprechend begrenzten Zugang zu einem Personalverwaltungssystem einräumen (siehe auch Punkt 2.11).

2.13 Jubiläumslisten dürfen für die MAV jahresbezogen erstellt werden.

2.14 Seitens der Dienststellenleitung und der MAV kann eine Geburtstagsliste unter Beachtung des Widerspruchsrechts nach § 16 Abs. 4a DSG-EKD geführt werden.

IV. Datenschutz- und Datensicherungsmaßnahmen

1. Büropersonal

Soweit für die Büroarbeiten der MAV (Erledigung schriftlicher Arbeiten wie das Schreiben von Protokollen, Gesprächsnotizen, Korrespondenz mit Mitarbeitenden und Dienststellenleitung, Einordnen und Führen der Unterlagen) Mitarbeitende der Dienststelle zur Verfügung stehen, sind diese auf die Schweigepflicht nach § 20 Abs. 1 MAVG und auf das Datengeheimnis nach § 6 DSG-EKD hinzuweisen.

2. Räume, Büromöbel, technische Ausstattung

Nach § 23 Abs. 3 MAVG hat die Dienststelle in erforderlichem Umfang Räume, sachliche Mittel, dienststellenübliche technische Ausstattung und Büropersonal für die Sitzungen, die Sprechstunden und die laufende Geschäftsführung der MAV zur Verfügung zu stellen. Seitens der MAV ist bei Nutzung der Räume und der technischen Ausstattung Folgendes zu beachten:

2.1 Räume:

Büro- und Besprechungsräume, die von der MAV genutzt werden, müssen baulich so beschaffen sein, dass vertraulich geführte Gespräche von Dritten nicht mitgehört bzw. die Räume von Dritten nicht eingesehen werden können.
Büroräume sollten abschließbar sein, ansonsten sind die MAV-Unterlagen immer in einem Schrank oder Schreibtisch zu verschließen, wenn das Büro verlassen wird.
Sofern Dritte (Reinigungskräfte, Hausmeister etc.) Zugang zu normalerweise verschlossenen MAV-Büroräumen haben, sind diese auf die Schweigepflicht nach § 20 Abs. 1 MAVG und auf das Datengeheimnis nach § 6 DSG-EKD hinzuweisen. Die MAV-Unterlagen sind nach Beendigung der Tätigkeit zu verschließen.

2.2 Büromöbel / Schränke:

Für die Akten der MAV muss ein abschließbarer Schrank vorhanden sein, damit Unbefugte nicht in die vertraulichen Unterlagen Einsicht nehmen können.

2.3 Faxgerät:

Ein der MAV zur Verfügung gestelltes Telefax-Gerät muss so aufgestellt werden, dass Dritte die ein- und ausgehenden Faxe nicht zur Kenntnis nehmen können (z. B. im abgeschlossenen Büro der MAV). Für den Fall, dass ein in der Dienststelle allgemein zugängliches Faxgerät genutzt wird, sind bei der Übermittlung sensibler Daten die besonderen Sicherheitsmaßnahmen zu beachten.

2.4 Diktiergeräte:

Cassetten von Diktiergeräten sind so aufzubewahren, dass sie Dritten nicht zugänglich sind. Eine Cassette mit schützenswertem Inhalt ist zu löschen, sobald ein Schreiben gefertigt und abgenommen ist.

2.5 Kopierer:

Soweit die MAV über einen eigenen Kopierer in ihren Büroräumen verfügt, ist beim Austausch oder Verkauf der Geräte darauf zu achten, dass eventuell im Kopierer vorhandene Speichermedien gelöscht oder unbrauchbar gemacht werden. Soweit der MAV die Nutzungsmöglichkeit des Kopierers der Dienststelle eingeräumt worden ist, haben die MAV-Mitglieder bei Kopiervorgängen sicherzustellen, dass Dritte die Vorgänge nicht zur Kenntnis nehmen können.

3. IT-Technik (Computer, Software, Wartung, Netzwerk)

3.1 Einzelgeräte (PC, Laptop, Notebook etc.) ohne Anbindung an ein Netzwerk

Einzelgeräte (PC, Laptop, Notebook etc.) ohne Anbindung an ein Netzwerk sind so zu schützen, dass Dritte die Geräte möglichst nicht entwenden können. Seitens der MAV sind regelmäßige Datensicherungen (3-Generationen-Prinzip) vorzusehen. Die Updates für Betriebssystem, Browser, Software sind entsprechend der Empfehlungen der IT zeitnah zu übernehmen. Die Daten sind im Rahmen der Vorgaben des IT-Sicherheitskonzeptes der Dienststelle zu schützen (Benutzerkennung, Passwortschutz, Firewall bei Internetanschluss, Virenschutz, Verschlüsselung), dass Dritte sie nicht unbefugt nutzen können.

3.2 Einzelgeräte/Clients (PC, Laptop, Notebook etc.) mit Anbindung an ein Netzwerk

Einzelgeräte/Clients mit Anbindung an ein Netzwerk müssen die organisatorischen und technischen Voraussetzungen erfüllen, die sich insbesondere aus den Anforderungen des IT-Grundschutz-Kataloges des BSI bzw. des IT-Sicherheitskonzeptes der kirchlichen Stelle ergeben. Der MAV ist für ihre elektronisch verarbeiteten Dateien ein eigener Verzeichnis- und Dateipfad im Netzwerk einzurichten. Im Rahmen des Berechtigungskonzeptes ist sicherzustellen, dass nur MAV-Mitglieder den Verzeichnis- und Dateipfad einsehen und bearbeiten können.

Mitarbeitende der IT/EDV (Administratoren) dürfen die gespeicherten elektronischen Dokumente der MAV nicht öffnen. Im Einzelfall haben die Mitarbeitenden der IT/EDV eine besondere Vertraulichkeitserklärung zu unterschreiben, wenn eine berechtigte Notwendigkeit zum Öffnen einer Datei besteht.

Unberechtigte Zugriffe auf elektronische Dokumente der MAV können grundsätzlich für alle Mitarbeitenden arbeitsrechtliche Maßnahmen (einschließlich einer außerordentlichen Kündigung) nach sich ziehen.

Um elektronische MAV-Dokumente zu schützen, ist es oft softwareseitig (z. B. bei MS-Office) möglich, ein Passwort bei der Speicherung einzugeben. Dies setzt voraus, dass das Passwort nur den MAV-Mitgliedern bekannt ist. Ein Passwortwechsel ist aber sehr aufwändig, da alle elektronischen Dokumente mit einem neuem Kennwort versehen werden müssten. Es kann auch geprüft werden, ob eine Protokollierung aller Zugriffe auf den Verzeichnis- und Dateipfad der MAV (einschließlich lesender Zugriffe) technisch mit einem vertretbarem Aufwand umgesetzt werden kann, um bei einem bestehendem Verdachtsfall prüfen zu können, wer Zugriff auf die elektronischen Dokumente hatte.

Der Hessische Datenschutzbeauftragte[6] schlägt vor, zu prüfen, ob die Mitarbeitenden der IT/EDV die Rechte auf Verzeichnisse mit vertraulichen Daten benötigen; sie also entzogen werden können: *„Für die Sicherung und Wiederherstellung dieser (von der MAV genutzten) Ordner würde man softwareseitig seitens des Betriebssystems die Rolle „Sicherungsoperator“ nutzen. Zusätzlich wären derartige Operationen zu protokollieren, damit die Zugriffe der Mitarbeitenden der IT/EDV nachvollziehbar wären.*

Alternativ könnten Dateien mit vertraulichem Inhalt verschlüsselt werden. Softwareseitig werden unterschiedliche Lösungen angeboten. Das Windows-Betriebssystem enthält das EFS (Encrypted File System). Um auf die Daten zugreifen zu können, auch wenn das

[6] 39. Tätigkeitsbericht 2010 des Hessischen Datenschutzbeauftragte, Auszug aus 5.1.2.1

Mitglied der MAV das Passwort vergessen hat, muss ein Recovery-Agent oder Wiederherstellungsagent eingebunden sein. Dies erklärt sich daraus, dass die EFS-Verschlüsselung eine Dateieigenschaft (Attribut des Ordners bzw. des Dokuments) ist. Das Passwort des MAV-Mitglieds ist Bestandteil des Schlüssels. Wird dieses durch Mitarbeitende der IT/EDV zurückgesetzt, sind alle verschlüsselten Dokumente des MAV-Mitglieds nicht mehr lesbar. Deshalb wird ein weiterer Benutzer, der Recovery-Agent, durch das Betriebssystem als zugriffsberechtigt eingetragen und es wird für ihn ein eigener Schlüssel mit gespeichert. Falls eine Datenverschlüsselung die Kenntnisnahme von Daten durch Mitarbeitende der IT/EDV verhindern soll, darf das Passwort des Wiederherstellungsagenten den Mitarbeitenden der IT/EDV nicht bekannt sein.
Wird die Dateiverschlüsselung nicht gewünscht und die Nutzung von EFS gesperrt, so sollte ein Wiederherstellungsagent erstellt und eingebunden werden. Dadurch wird verhindert, dass ein MAV-Mitglied eine Datei irrtümlich oder gewollt so verschlüsseln kann, dass die übrigen MAV-Mitglieder darauf keinen Zugriff haben.

3.3 Zentraldrucker

Soweit die MAV über keinen eigenen Drucker verfügt, ist bei Ausdrucken über einen Zentraldrucker sicherzustellen, dass Dritte die Ausdrucke nicht unbefugt zur Kenntnis nehmen können. Vorteilhaft sind Zentraldrucker, deren Ausdrucke nur nach Eingabe eines persönlichen Passwortes entnommen werden können.

3.4 externe Wartung und Systembetreuung

Bei der **externen Wartung und Systembetreuung** ist sicherzustellen, dass die damit betrauten Personen vertrauliche Daten nicht unbefugt zur Kenntnis nehmen können.

4. Telekommunikation, Intranet/Internet

4.1 Festnetz- und Mobiltelefone

Bei Festnetz- und Mobiltelefonen für MAV-Mitglieder ist wegen der Sensibilität der Telefonate sicherzustellen, dass Zielnummern nicht gespeichert werden (Gebührenerfassung ist zulässig). Vertraulich geführte Gespräche, die über schnurlose Telefone oder Mobiltelefone geführt werden, können heutzutage ohne großen Aufwand abgehört werden; daher sind für diese Gespräche ausschließlich Festnetztelefone zu verwenden oder die anrufenden Personen über die Risiken aufzuklären. Dienstlich zur Verfügung gestellte Mobiltelefone einschließlich PDAs, Smartphones etc. sind so zu schützen, dass sie Dritten nicht zugänglich bzw. die Daten (SMS, Verbindungsdaten) einsehbar sind.

4.2 Telefonanrufbeantworter

Soweit seitens der MAV Telefonanrufbeantworter eingesetzt werden, ist sicherzustellen, dass Dritte keinen Zugang auf die gespeicherten Anrufe haben.

4.3 Intranet:

Es wird der MAV in der Regel gestattet sein, in organisationsinternen Rechnernetzen **(Intranet)** auch eigene Inhalte einzustellen und damit zu verbreiten (BAG vom 03.09.2003 - 7 ABR 12/03, AiB 2004, 194). Nutzt die MAV die Möglichkeit, ist sie in der inhaltlichen Gestaltung frei. Allerdings muss die MAV die Grundsätze der vertrauensvollen Zusammenarbeit beachten und in den Grenzen ihrer Aufgaben und Zuständigkeiten bleiben. Es ist nicht zulässig, der Niederschriften der MAV im Intranet einzustel-

len. Zulässig und geradezu geboten ist hingegen die Veröffentlichung von Beschlüssen der MAV, die sich etwa auf grundsätzliche Regelung (wie zum Beispiel auf die zukünftige Gestaltung der Arbeitszeit; Abschluss von Dienstvereinbarungen) beziehen. Ebenso können die Zusammensetzung der MAV mit Funktionen und Aufgaben sowie die dienstlichen Adressdaten veröffentlicht werden. Weitere Daten der Mitarbeitenden wie Fotos, private Adressen usw. dürfen nur mit Einwilligung der Betroffenen ins Intranet eingestellt werden.

4.4 Internet:
Bei der Veröffentlichung von Inhalten auf den Internetseiten der Dienststelle wird sich die MAV auf allgemein zugängliche Informationen, wie z. B. Zusammensetzung und Zuständigkeit beschränken müssen, denn die Daten von Mitarbeitenden, dazu gehören auch die Mitglieder der MAV, sind über § 24 DSG-EKD besonders geschützt. Die Veröffentlichung von Name, Vorname, Amts- oder Dienstbezeichnung, der dienstlichen Telefon- und Faxnummer, der dienstlichen E-Mail-Adresse des vorsitzenden Mitglieds der MAV ist datenschutzrechtlich unbedenklich. Es besteht keine Notwendigkeit, die Namen und dienstlichen Adressen der weiteren MAV-Mitglieder auf der Homepage zu veröffentlichen. Ggf. ist hierzu die Einwilligung der MAV-Mitglieder für eine Veröffentlichung einschl. des Umfangs der Daten einzuholen. Dies gilt insbesondere für Fotos, private Adressen und weitere personenbezogene Daten.

5. Nutzung von E-Mail für die Arbeit der MAV[7]

In der heutigen Zeit verfügen nahezu alle kirchlichen Stellen über die entsprechenden Voraussetzungen, um eine Kommunikation mittels E-Mail zu ermöglichen[8].
Ist in einer kirchlichen Stelle der interne Mailverkehr eröffnet, kann der "Zugang" als für alle teilnehmenden Mitarbeitenden eröffnet gelten:

5.1 Die Mitarbeitenden haben ihrerseits die Möglichkeit, Anfragen und Anregungen an die MAV zu senden. Diese hat die MAV nach § 33 Abs. 2 Buchstabe b MVG.EKD formal aufzunehmen und zu behandeln. Soweit die MAV eine eigene E-Mail-Adresse erhalten hat (z. B. MAV@kirche.de), ist sie verpflichtet, das E-Mail-Postfach regelmäßig und zeitnah auf Eingänge zu überprüfen, im Falle der Abwesenheit der oder des Vorsitzenden ist dies durch Aktivierung der Abwesenheitsfunktion oder andere Maßnahmen (z. B. Vertretungsreglung) sicherzustellen. Es ist zu gewährleisten, dass E-Mails der MAV-Mitglieder von Dritten[9] (z. B. im Rahmen der Vertretung) nicht eingesehen werden kön-

[7] Unter Einbeziehung der Quelle aus LexisNexis Recht online: Jordan, in Jordan: Personalvertretungsrecht

[8] § 2 des Verwaltungsverfahrens- und -zustellungsgesetz der EKD (VVZG-EKD) enthält Regelungen für kirchliche Körperschaften (Kirchengemeinden, Kirchenkreise, kirchliche Verbände) zur elektronische Kommunikation. Durch die Angabe der E-Mail-Adresse auf dem Briefkopf oder auf der Homepage der kirchlichen Körperschaft erklärt die kirchliche Behörde zunächst grundsätzlich ihre Bereitschaft, Erklärungen auch auf diesem Weg (elektronisch) entgegenzunehmen. Die kirchliche Körperschaft hat zu gewährleisten, dass der Zugang regelmäßig auf Eingänge überprüft wird, ähnlich wie ein Postfach oder der Posteingang in der Poststelle einer Verwaltung. Die kirchlichen Stellen können sich nicht mehr ohne weiteres darauf berufen, eine Information sei ihnen nicht zugegangen. Rechtserheblich können diese Erklärungen nur werden, wenn eine kirchliche Vorschrift dies zulässt, wobei dies im Regelfall voraussetzt, dass qualifizierte Signaturen eingesetzt werden, damit ein Nachweis dafür vorhanden ist, dass die digital übermittelte Erklärung wirklich von der absendenden Person und nicht von jemand anders stammt (siehe Fußnote 14). In den kirchlichen Normen finden sich zur Zeit keine Regelungen, die eine Übermittlung rechtserheblicher Erklärungen per E-Mail zulassen. Für die kirchliche Behörde bedeutet dies, dass sie bei E-Mails, die rechtserhebliche Erklärungen (z. B. Antragstellung, Widerspruch) enthalten und nicht handschriftlich unterschrieben sein können, Kontakt mit der Person oder Stelle aufnimmt und sie bittet, die Erklärung schriftlich oder per Fax nochmals einzureichen

[9] Mitarbeitende der IT/EDV (Administratoren) dürfen die E-Mails der MAV nicht öffnen, um so ggf. vertrauliche Inhalte zu erfahren (siehe auch Ausführungen zu Ziffer IV. 3.2).

nen (z. B. eigene E-Mail-Adresse für MAV-Mitglieder, auf die Dritte nicht zugreifen können). Bei einem E-Mail- Kontakt der MAV mit einem Mitarbeitenden ist zu berücksichtigen, dass vertretungsberechtigte Personen des Mitarbeitenden Kenntnis vom E-Mail-Inhalt erhalten könnten. Bei Beantwortung mit vertraulichem Inhalt ist aus diesem Grunde ggf. das persönliche Gespräch, ein Telefonat oder eine Antwort in Papierform vorzuziehen.

5.2 Der allgemeine Kontakt zu den Mitarbeitenden und deren Information über die Tätigkeiten der MAV bietet sich per E-Mail an. Die MAV sollte mit der Dienststellenleitung die Einrichtung bzw. den Zugang zu dem Adressbuch „Alle" oder „Mitarbeitende“ vereinbaren, dies kann auch durch eine Dienstvereinbarung zum Einsatz von Intranet und E-Mail geschehen. In diesem Zusammenhang ist für die Mitarbeitenden, die über keinen Zugang zum E-Mail-System verfügen, eine Regelung vorzusehen, wie sie von der MAV oder der kirchlichen Stelle die Informationen zeitnah erhalten.

5.3 Innerhalb der MAV kann die Kommunikation per E-Mail vorteilhaft sein, denn dadurch wird eine wesentlich bessere Information, als das mit traditionellen Verfahren möglich war, eröffnet. Dabei ist der Schutz der Vertraulichkeit von Informationen in den Vordergrund zustellen (siehe auch Ausführungen zu Ziffer 5). Unproblematisch und datenschutzrechtlich zulässig ist es, über E-Mail einfache Informationen, z. B. die Mitteilung von Terminen, Einladungen zu Begehungen im Rahmen des Arbeitsschutzes oder Nachfragen zu aktuellen Ereignissen oder auch die Mitteilung der Tagesordnung für die gemeinschaftliche Besprechung nach § 34 Abs. 2 MAVG zu übermitteln, wenn sie keine vertraulichen oder personenbezogene Daten enthält.

5.4 Soweit das MAVG die Schriftform vorsieht (z. B. bei der Zustimmung oder Ablehnung im Mitbestimmungsverfahren - § 39 Abs. 1 und 3 - oder beim Initiativantrag der MAV - § 42 Abs. 2 MAVG), kann sie in der Regel nicht durch ein elektronisches Dokument ersetzt werden[10].

5.5 Im **E-Mail-Verkehr innerhalb der MAV und zwischen der MAV und der Dienstellenleitung oder den Mitarbeitenden** ist grundsätzlich zu beachten, dass im Hinblick

[10] Siehe auch Ausführungen in der **Fußnote 8**. Soweit das kirchliche Recht eine elektronische Kommunikation zulässt, müsste das jeweilige Dokument durch eine qualifizierte elektronische Signatur gesichert und eindeutig identifizierbar gemacht werden. Die elektronische Signatur ist ein von einem Zertifizierungs-Diensteanbieter nach dem Signaturgesetz (SigN) vergebene Datei, die einem elektronischen Dokument zugefügt werden kann und eine eindeutige Authentifizierung ermöglicht (§ 2 SigG). Zusätzlich muss die E-Mail verschlüsselt werden und dazu verfügen Absender und Empfänger über einen elektronischen Schlüssel, mit dem der Absender das Dokument "verschlüsseln" und nur der Empfänger es wieder "entschlüsseln" und identifizieren kann. Die elektronische Signatur ersetzt die im klassischen Schriftverkehr üblich handschriftliche Unterschrift und / oder das Siegel. Nur mit der zertifizierten Signatur ist das Dokument gegen die ansonsten im E-Mail-Verkehr relativ leicht mögliche Fälschung von Inhalt und Herkunft gesichert. Sollte die E-Mail durch Fehlbedienung den falschen Empfänger erreicht haben, ist dieser nicht in der Lage, ein signiertes Dokument zu öffnen. Da zur Absendung eines elektronischen Dokuments in der Regel ein Knopfdruck genügt, ist ein Versand an den falschen Empfänger (oder sogar eine beliebig große Gruppe von Empfängern, etwa sämtlichen E-Mail berechtigten Beschäftigten einer Dienststelle) leicht möglich.
Das Bundesarbeitsgericht hat jedoch in zwei jüngeren Entscheidungen (BAG, 09.12.2008, 1 ABR 79/07; BAG, 10.03.2009, 1 ABR 93/07, AuR 2009, 226) festgestellt, dass eine Zustimmungsverweigerung eines Betriebsrats den Anforderungen von § 99 Abs. 3 BetrVG (fristgerecht, begründet und schriftlich) und § 126b BGB (Schriftform) auch dann genügt, wenn sie per unsignierter Mail an den Arbeitgeber gelangt. Voraussetzung sei nur, dass der Absender und der Unterzeichner klar erkennbar sind. Das BAG begründet seine Auffassung damit, dass mit der Zustimmungsverweigerung lediglich eine Willenserklärung abgegeben und kein Rechtsgeschäft im eigentlichen Sinne abgeschlossen werden soll. Eine eigenhändige Unterschrift (= elektronische Signatur) sei dann nicht zwingend erforderlich. §§ 126 ff BGB seien allenfalls analog anzuwenden. Im letzten entschiedenen Fall hatte die Arbeitgeberin den Eintritt der Zustimmungsfiktion geltend gemacht, weil die Zustimmungsverweigerung nur mittels E-Mail erfolgt sei. Es ist fraglich, ob diese Entscheidungen auf den kirchlichen Bereich übertragbar sind. Wegen der etwas anderen Verhältnisse in den kirchlichen Verwaltungen, z. B. der Geltung von § 2 VVZG-EKD, wird empfohlen, Mitteilungen, z. B. an die Dienststellenleitung, bei denen die Schriftform vorgeschrieben ist, weiterhin auf traditionellem Wege als Schriftstück mit eigenhändiger Unterschrift des vertretungsberechtigten Mitglieds der MAV zu senden.

auf die mögliche Sensibilität des Dokuments der Datenschutz (z. B. die Übermittlung vertraulicher personenbezogener Daten) mittels unsigniertem E- Mail-Verkehrs nur eingeschränkt zulässt:

a. Soweit innerhalb eines Intranets die E-Mails **verschlüsselt** von der absendenden Person zur empfangenen Person über geschützte (getunnelte) Leitungen übermittelt werden, existiert aus Sicht des Datenschutzes ein grundsätzlich sicheres E-Mail-System, dass von außen normalerweise nicht angreifbar ist. Es ist innerhalb des E-Mail-Systems sicherzustellen, dass Dritte (z. B. Mitarbeitende über Vertretungsregelungen) nicht auf die E-Mails des MAV-Mitglieds zugreifen können. Durch organisatorische Regelung kann auf die Vertraulichkeit der Information hingewiesen werden, so dass Vertretungspersonen erkennen können, dass diese E-Mails nicht von ihr geöffnet werden dürfen (z. B. „Vertrauliche Mitteilung an die MAV-Mitglieder“). Einige E-Mail-Verfahren bieten systemseitig die nachfolgend aufgeführten Möglichkeiten, vertrauliche E-Mails zu senden:
    - Über „Regeln“ kann festgelegt werden, dass beispielsweise E-Mails mit dem Betreff „MAV“ bei dem jeweiligen MAV-Mitglied automatisiert als „privat“ gekennzeichnet werden und somit nur noch vom MAV-Mitglied (nicht von einer vertretungsberechtigten Person) gesehen und aufgerufen werden können.
    - E-Mails werden vor dem Versand mit der Eigenschaft „privat oder vertraulich“ gekennzeichnet und sind im Vertretungsfall nicht sichtbar oder aufrufbar, soweit nichts anderes im Vertretungszugriff festgelegt ist.
b. Eine sichere E-Mail-Kommunikation liegt aber auf keinen Fall vor, wenn der E-Mail-Verkehr über dass **Internet** abgewickelt wird, da die technischen Möglichkeiten es zulassen, dass Dritte unbefugterweise den Inhalt zur Kenntnis nehmen oder sogar verändern können.
c. Die kirchlichen E-Mail-Server sind so einzustellen, dass nur noch verschlüsselte Übertragungen möglich sind. Soweit **kein sicheres E-Mail-System** vorhanden ist, ist die Übermittlung personenbezogener Daten aus datenschutzrechtlicher Sicht nicht zulässig. Dies gilt zum Beispiel für die Übermittlung der Tagesordnung mit TOPs zu konkret zur Beratung anstehenden Personalangelegenheiten für eine Sitzung der MAV per E-Mail. Anders sieht es aus, wenn nur der Termin der Sitzung und der Sitzungsraum (ohne personenbezogenen Daten) übermittelt wird. Es kann alternativ überlegt werden, auf die schriftliche Einladung mit ausführlich bezeichneten Verhandlungsgegenständen zu verzichten und die vollständigen Tagesordnungen, Niederschriften der MAV, Gesprächsvermerke von einzelnen MAV-Mitgliedern usw. in einem geschützten, nur den MAV-Mitgliedern zugänglicher Speicher- und Dateipfad im Netzwerk der Dienststelle zugänglich zu machen (siehe auch Ausführungen zu Ziffer IV. 3.2). Denn die Mitglieder der MAV haben Anspruch zu erfahren, welche personellen Angelegenheiten zur Beratung und Beschlussfassung anstehen, um sich auf eine Sitzung angemessen vorbereiten zu können.