Gesamtausschuss der Mitarbeitervertretungen der Ev.-luth. Landeskirche Hannovers
Vorsitzender: Siegfried Wulf, ☎ 05151/9509-24
stellv. Vors.: Andreas Miehe, ☎ 0151/233 00 407
Schriftführerin: Ilka Müller, ☎ 04161/500 80 44
E-Mail: gamav@evlka.de
Internet: www.gamav.de

Gesamtausschuss d. MAV, Bahnhofsplatz 1, 31785 Hameln

Orientierungshilfe für Dienststellenleitungen und Mitarbeitervertretungen „Datenschutz in der Mitarbeitervertretung“

(Stand: 01.02.2018)

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 Dienststellenleitungen und die Mitarbeitervertretungen in der hannoverschen Landeskirche.

I. Rechtsgrundlagen

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

1. Arbeitsrechtsregelungen (z. B. DVO, TV-L),
2. Mitarbeitervertretungsgesetz (MVG-K),
3. Kirchengesetz über den Datenschutz der EKD (DSG-EKD),
4. Gemeinsames Datenschutz-Anwendungsgesetz (DSAG),
5. Datenschutzdurchführungsverordnung (DATVO),
6. Verwaltungsvorschriften für die Durchführung des Kirchlichen Datenschutzes (VV-DS),
7. Dienstvereinbarung IUK-Technik (soweit vorhanden) .

Da die MAV in datenschutzrechtlicher Hinsicht als Teil der Dienststellenleitung anzusehen und kein sogenannter „Dritter“ (nicht berechtigte Personen) ist, gibt es zwischen Dienststellenleitung und MAV insoweit keine Übermittlungseinschränkungen. Als Maßstab für die Weiterleitung personenbezogener Daten von der Dienststellenleitung an die MAV ist § 24 DSG-EKD sowie die Bestimmungen des MVG-K oder Dienstvereinbarungen heranzuziehen.

EVANGELISCH-LUTHERISCHE LANDESKIRCHE HANNOVERS

II. Datengeheimnis/Schweigepflicht

1. Grundsätzlich gilt für alle Mitarbeitenden das Datengeheimnis nach § 6 DSG-EKD, 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 § 23 MVG-K (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 Stillschweigen zu bewahren, soweit die Geheimhaltung der Natur der Sache nach erforderlich oder von der Mitarbeitervertretung beschlossen oder die Angelegenheit von der Dienststellenleitung für vertraulich erklärt worden ist. Die MAV erhält sensible personenbezogene Informationen im Rahmen der Beteiligung in personellen Angelegenheiten oder durch die Mitarbeitenden selbst. Die allgemeinen Persönlichkeitsrechte der 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 gegenüber den betroffenen Mitarbeitenden, 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 (und gegenüber anderen an den Sitzungen teilnehmenden Personen wie Sprecher der Jugendlichen und Auszubildenden/Vertrauensperson der Schwerbehinderten) gilt die Geheimhaltungspflicht nach § 23 Abs. 3 MVG-K 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 werden; es sei denn, die betroffene Person hat dem ausdrücklich widersprochen.

   Als Rechtsfolge bei Verletzung des Datengeheimnisses oder der Schweigepflicht ist für MAV-Mitglieder der Ausschluss aus der MAV denkbar, bzw. die Auflösung der MAV gemäß § 17 MVG-K, wenn ein grober Missbrauch oder eine grobe Verletzung der Schweigepflicht vorliegt.

3. Für Personen außerhalb der MAV kann es bei Verletzung des Datengeheimnisses oder der Schweigepflicht zu arbeitsrechtlichen Sanktionen wie Abmahnung, ordentliche oder außerordentliche Kündigung (Verstoß gegen die Treuepflicht) kommen; bei Kirchenbeamtinnen und Kirchenbeamten auch zu entsprechenden dienstrechtlichen Sanktionen.

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 Personalunterlagen zugesandt oder ausgehändigt (siehe auch § 35 MVG-K).

1.2. Ein namentlich genanntes Mitglied der MAV darf die Personalakte einer Mitarbeiterin oder eines Mitarbeiters nur einsehen, wenn die schriftliche Zustimmung der betroffenen Person eingeholt worden ist (§ 35 Abs. 4 MVG-K).

1.3. Niederschriften über die Sitzungen der MAV enthalten die Beratungsergebnisse und geben zum Teil den Verlauf der Beratungen in vielen Details wieder. Bewerbungsunterlagen enthalten zum Teil sehr sensible Informationen, z. B. Zeugnisse, Beurteilungen, Anerkennung einer Schwerbehinderung.

1.4. Über Gespräche mit Mitarbeitenden können von Mitgliedern der MAV Gesprächsvermerke gefertigt werden.

1.5. Der Vertrauensschutz, der Datenschutz sowie die Fürsorgepflicht der kirchlichen Stellen gegenüber ihren Mitarbeitenden und ihren Stellenbewerberinnen und Stellenbewerbern gebieten es, mit den Personalunterlagen sorgfältig umzugehen, sie sicher aufzubewahren und sie nur insoweit 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).

2. Empfehlungen

2.1. Es ist zu prüfen, in welchem Umfang die MAV Personalunterlagen für eine Entscheidung benötigt. Nach § 35 MVG-K ist die MAV zur Durchführung ihrer Aufgaben rechtzeitig und umfassend zu unterrichten. Absatz 3 konkretisiert diese Verpflichtung dahingehend, dass die für die Entscheidungen der MAV „erforderlichen“ Unterlagen (bei Einstellungen auf Verlangen der MAV auch sämtliche Bewerbungen) vorzulegen sind. Die Prüfung obliegt der Dienststellenleitung und der MAV.

2.2. Personalunterlagen werden als Original oder in Kopie der MAV zur Verfügung gestellt. Dabei erfolgt ein Hinweis, dass es sich um vertrauliche Personalunterlagen handelt. Dieses kann durch einen auf einem verschlossenen Umschlag hervorgehobenen Aufdruck „vertrauliche Personalunterlagen“ geschehen.

2.3. Bewerbungs- und Personalunterlagen sind nach Beendigung der MAV-Sitzung gemäß Absprache mit der Dienststellenleitung vollständig und datenschutzgerecht zu vernichten bzw. zurückzugeben.

2.4. MAV-Akten sind, solange sie noch von rechtlicher Bedeutung sind, aber für zumindest eine Amtszeit aufzubewahren.

Daten dürfen von der MAV nur so lange aufbewahrt werden, wie sie benötigt werden. Hier ist ggfls. ein Nachweis erforderlich, z.B. durch einen Vermerk auf der Akte, warum sie aufbewahrt wird.

2.5. Soweit Mitarbeitende im Rahmen einer Heim-/Telearbeit zu Hause arbeiten und als MAV-Mitglieder Personalunterlagen und MAV-Vorgänge erhalten, ist neben den vertraglichen Regelungen zur Heim-/Telearbeit insbesondere Folgendes zu beachten:

a) Die Unterlagen sind sicher und für Dritte unzugänglich aufzubewahren.
b) Nicht mehr benötigte Unterlagen, die von der Dienststelle zur Verfügung gestellt wurden, sind an diese 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.

2.6. 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 (§ 18 Abs. 5 MVG-K). Nicht mehr benötigte MAV-Unterlagen (insbesondere Duplikate mit Gesprächsvermerken, Tagesordnungen, Protokollen usw. [Handakten]) sind durch die MAV datenschutzgerecht zu entsorgen.

2.7. Die der MAV durch eigene Erhebung oder Mitteilung über die Dienststelle bekannt gewordenen personenbezogenen Daten Dritter unterliegen dem Datenschutz. Dabei ist Folgendes zu beachten:

a) Es dürfen nur Daten erhoben werden, die erforderlich sind. Dabei ist mit der Datenerhebung sparsam umzugehen.

b) Die Daten dürfen nur so lange gespeichert werden, wie es für die Tätigkeit der MAV erforderlich ist.

c) Die Datenübermittlung an Dritte, z.B. Berufsverbände oder Gewerkschaften, ist unzulässig.

d) Gegenüber der betroffenen Person besteht eine Auskunftspflicht über die zu ihr gespeicherten Daten und die Verpflichtung zur Berichtigung, Löschung oder Sperrung dieser Daten auf Verlangen der betroffenen Person.

2.8. Anstelle der Übermittlung von Grundstammdaten der Mitarbeitenden kann die Dienststelle der MAV auch einen von den Zugriffsrechten entsprechend begrenzten Zugang zu einem Personalverwaltungssystem einräumen.

2.9. Listen von Dienstjubiläen dürfen für die MAV jahresbezogen von der Personalstelle erstellt werden.

2.10. Dienststellenleitung und MAV können eine Geburtstagsliste führen, soweit die betroffenen Personen ihr Einverständnis dazu erklärt haben.

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 § 23 Abs. 2 MVG-K und auf das Datengeheimnis nach § 6 DSG-EKD zu verpflichten.

2. Räume, Büromöbel, technische Ausstattung

Nach § 31 Abs. 1 MVG-K 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:

Büroräume der MAV müssen abschließbar sein. Ist dies nicht gegeben, 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 § 23 Abs. 2 MVG-K und auf das Datengeheimnis nach § 6 DSG-EKD zu verpflichten.

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).

2.4. Diktiergeräte:

Digitale Dateien von Diktaten bzw. Kassetten von Diktiergeräten sind so aufzubewahren und zu sichern, dass sie Dritten nicht zugänglich sind. Enthalten sie personenbezogene Daten im Sinne des § 2 DSG-EKD, so ist der Inhalt nach Anfertigung des Schreibens zu löschen.

2.5. Kopierer/Scanner:

Kopierer und Zentraldrucker können mit einer PIN geschützt werden, damit keine andere Person Zugriff hat, wenn der MAV kein eigener Drucker/Kopierer zur Verfügung steht.

Soweit die MAV über einen eigenen Kopierer/Scanner in ihren Büroräumen verfügt, ist beim Austausch oder Verkauf der Geräte darauf zu achten, dass eventuell im Kopierer/Scanner vorhandene Speichermedien gelöscht oder unbrauchbar gemacht werden.

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

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

Arbeitsplatzgeräte und Daten sind gegen unbefugten Zugriff durch Dritte, Manipulation und Diebstahl zu schützen. Jeder Anwender erhält individuelle Zugangsdaten, mit deren Hilfe er mit individuellen Rechten auf dienstliche Anwendungen und geschützte Daten Zugriff erhält. Die unberechtigte Nutzung von Programmen und Daten durch Unbefugte ist zu verhindern. Wenn sensible Informationen der MAV auf der lokalen Festplatte gespeichert werden, dann sollte dies verschlüsselt erfolgen. Seitens der MAV sind regelmäßige Datensicherungen auf ein externes Speichermedium vorzunehmen. Betriebssystem, Browser und Software sind über Updates regelmäßig zu aktualisieren. Das Einzelgerät ist durch zusätzliche Sicherheitsfunktionen wie Firewall und Virenscanner zu schützen. Diese müssen ebenfalls durch Updates aktuell gehalten werden.

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

Für die MAV ist ein eigener Verzeichnis- und Dateipfad im Netzwerk einzurichten und mit einem Passwort zu versehen. Es ist sicherzustellen, dass nur MAV-Mitglieder den Verzeichnis- und Dateipfad einsehen und bearbeiten können. In diesem Verzeichnis sind alle MAV-relevanten Dokumente zu speichern. Die Datensicherung muss dann über Tools des genutzten Serversystems erfolgen.

Administratoren oder externe Systembetreuer dürfen die gespeicherten elektronischen Dokumente der MAV nicht öffnen. Besteht durch diese trotzdem eine berechtigte Notwendigkeit zum Öffnen einer Datei, ist im Einzelfall eine besondere Vertraulichkeitserklärung zu unterschreiben. Unberechtigte Zugriffe auf elektroni-

sche Dokumente der MAV können grundsätzlich für alle Mitarbeitenden arbeitsrechtliche Maßnahmen nach sich ziehen.

3.3. Drucker (siehe Hinweis auf PIN unter 2.5)

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.

4. Telekommunikation, Intranet/Internet

4.1. Festnetz- und Mobiltelefone

Bei Festnetz- und Mobiltelefonen für MAV-Mitglieder ist wegen der Sensibilität der Telefonate sicherzustellen, dass die letzten drei Ziffern der Zielnummer nicht gespeichert werden (Gebührenerfassung ist zulässig). Vertraulich geführte Gespräche, die über schnurlose Telefone oder Mobiltelefone geführt werden, können heutzutage ohne großen Aufwand abgehört werden; dessen sollte man sich bei der Nutzung derartiger Geräte bewusst sein. Dienstlich zur Verfügung gestellte Mobiltelefone einschließlich PDAs, Smartphones etc. sind so zu schützen, dass sie Dritten nicht zugänglich bzw. die Daten (SMS, Verbindungsdaten) nicht einsehbar sind.

4.2. Telefonanrufbeantworter

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

4.3. Internet/Intranet

Bei Veröffentlichungen der MAV im organisationsinternen Intranet bzw. über das Internet dürfen personenbezogene Daten nicht veröffentlicht werden. Auch Protokolle der MAV dürfen nicht ungeschützt ins Intra-/Internet gestellt werden. Möglich ist dagegen die Veröffentlichung von Beschlüssen (ohne die konkrete Benennung von Personen) zu grundsätzlichen Regelungen wie z. B. zukünftige Gestaltung der Arbeitszeit, Dienstvereinbarungen, aber auch allgemeine Informationen zum Arbeitsrecht und zur Entwicklung der Dienststelle. Sollen neben den dienstlichen Daten der oder des Vorsitzenden der MAV im Internet auch die entsprechenden Daten bzw. Fotos der anderen MAV-Mitglieder veröffentlicht werden, so ist vorher deren Einwilligung einzuholen. Für die Veröffentlichung weiterer Daten von Mitarbeitenden sowie deren Fotos ist sowohl für das Intranet als auch das Internet grundsätzlich die schriftliche Einwilligung der Betroffenen einzuholen.

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

5.1. E-Mail-Kommunikation gehört inzwischen zur üblichen Ausstattung von Mitarbeitervertretungen. Jedem Mitglied der MAV muss neben seiner persönlichen dienstlichen Adresse eine separate persönliche MAV-Adresse zur Verfügung gestellt werden. Die

MAV ist 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 (z.B. Weiterleitung) oder andere Maßnahmen (z. B. Vertretungsregelung) sicherzustellen. Es ist zu gewährleisten, dass E-Mails der MAV-Mitglieder an ihren Arbeitsplätzen oder im privaten Umfeld von „Dritten" (z. B. im Rahmen der Vertretung) nicht eingesehen werden können.

Bei einem E-Mail-Kontakt der MAV mit einem Mitarbeitenden ist zu berücksichtigen, dass die den Mitarbeitenden in seiner Abwesenheit vertretende Person Kenntnis vom E-Mail-Inhalt erhalten könnte. Bei vertraulichen Inhalten 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 über eine Dienstvereinbarung mit der Dienststellenleitung die Nutzung der dienstlichen E-Mail-Adressen vereinbaren.

Für Mitarbeitende, die über keinen Zugang zum E-Mail-System verfügen, ist eine Regelung vorzusehen, wie sie die Informationen von der MAV oder der kirchlichen Stelle zeitnah erhalten.

5.3. Bei der E-Mail-Kommunikation innerhalb der MAV ist der Schutz der Vertraulichkeit von Informationen in den Vordergrund zu stellen. 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 zu kommunizieren. Das Übermitteln von vertraulichen oder personenbezogenen Daten ist unverschlüsselt (s. Punkt 5.5) nicht zulässig.

5.4. Im E-Mail-Verkehr innerhalb der MAV und zwischen der MAV und der Dienstellenleitung oder den Mitarbeitenden ist grundsätzlich zu beachten, dass im Hinblick auf die mögliche Sensibilität des Dokuments der Datenschutz die Übermittlung vertraulicher personenbezogener Daten mittels unverschlüsselten E-Mail-Verkehrs nur eingeschränkt zulässt:

a. Soweit innerhalb des Kirchennetzes die E-Mails von der absendenden Person zur empfangenden Person über geschützte (getunnelte) Leitungen **verschlüsselt** übermittelt werden (Transportverschlüsselung), existiert aus Sicht des Datenschutzes ein grundsätzlich sicheres E-Mail-System, das 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.

b. Eine sichere E-Mail-Kommunikation liegt aber auf keinen Fall vor, wenn der E-Mail-Verkehr über das **Internet** abgewickelt wird, da die technischen Möglichkeiten es zulassen, dass Dritte unbefugt den Inhalt zur Kenntnis nehmen oder sogar verändern können.

c. Soweit **kein sicheres E-Mail-System** vorhanden ist, ist die Übermittlung personenbezogener Daten ohne weitere Verschlüsselungsmaßnahmen nicht zulässig. Dies gilt zum Beispiel für die Übermittlung der Tagesordnung der MAV-Sitzung mit TOPs zu konkret zur Beratung anstehenden Personalangelegenheiten per E-Mail. Anders sieht es aus, wenn nur der Termin der Sitzung und der Sitzungsraum übermittelt werden. 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 zugänglichen Speicher- und Dateipfad im Netzwerk der Dienststelle zugänglich zu machen. 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.

d. Beim Versenden von Protokollen und anderen Dateien per E-Mail zwischen Mitgliedern der MAV oder zwischen MAV und Dienststellenleitungen kann der Datenschutz und die Datensicherheit durch **Verwendung eines Verschlüsselungsprogramms zur Verschlüsselung der versendeten Dateien** sichergestellt werden. So wird verhindert, dass Unbefugte Zugriff auf diese Daten erhalten.

Zusätzlich muss gewährleistet werden, dass auf einem Rechner erstellte Dateien, die personenbezogene Daten beinhalten, sicher abgespeichert werden. Dies gilt insbesondere auch für private Rechner. Dafür gibt es eigens für diesen Zweck vorgesehene Programme, die es ermöglichen, Dateien oder ganze Ordner mit mehreren Dateien zu verschlüsseln und für Unberechtigte unzugänglich zu machen.