Orientierungshilfe für Dienststellenleitungen und Mitarbeitervertretungen

„Datenschutz in der Mitarbeitervertretung"

(Stand: 17.12.2013)

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).

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 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 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 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.

3. Als Rechtsfolgen bei Verletzung des Datengeheimnisses oder der Schweigepflicht sind denkbar:
   - Ausschluss eines Mitglieds aus der MAV bzw. Auflösung der MAV gemäß § 17 MVG-K, wenn ein grober Missbrauch oder eine grobe Verletzung der Schweigepflicht vorliegt;
   - arbeitsrechtliche Sanktionen wie Abmahnung, ordentliche oder außerordentliche Kündigung (Verstoß gegen die Treuepflicht); bei Kirchenbeamtinnen und Kirchenbeamten auch entsprechend dienstrechtliche 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 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 (insbesondere die Niederschriften) sind, solange sie noch von rechtlicher Bedeutung sind, aufzubewahren. Am Ende der Aufbewahrungsfrist (5 Jahre) ist wie folgt zu verfahren:

a. Soweit die MAV-Akten keine besonderen Vorkommnisse enthalten (z. B. Verfahren vor der Schiedsstelle, 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 (Archivdirektor Dr. Otte fragen!) zur Archivierung anzubieten. Soweit die Archivwürdigkeit der Unterlagen nicht vorliegt, sind sie mindestens unzugänglich (Sperrung) zu machen, sonst zu vernichten (siehe auch Punkt 2.7).

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 Folgendes 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.

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 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 solange gespeichert werden, wie es für die Tätigkeit der MAV erforderlich ist.
c. Vorhandene Datenbestände müssen regelmäßig gelöscht bzw. aktualisiert werden. Aufbewahrungsfristen sind dabei zu beachten.
d. Die Datenübermittlung an Dritte z.B. Berufsverbände oder Gewerkschaften ist unzulässig.
e. 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.
f. Dem Beauftragten für den Datenschutz sind Prüfrechte gemäß § 19 DSG-EKD eingeräumt.

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 Jubiläumslisten dürfen für die MAV jahresbezogen erstellt werden.

2.10 Dienststellenleitung und MAV können eine Geburtstagsliste führen, soweit die betroffenen Personen dieser nicht widersprechen.

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 hinzuweisen.

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 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 § 23 Abs. 2 MVG-K 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 soll 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, kann dies dadurch sichergestellt werden, dass das eingehende Fax durch eine berechtigte Person direkt in Empfang genommen wird.

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:

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.
Soweit der MAV die Nutzungsmöglichkeit des Kopierers/Scanners der Dienststelle eingeräumt worden ist, haben die MAV-Mitglieder bei Kopier-/Scanvorgängen sicherzustellen, dass Dritte die Vorgänge nicht zur Kenntnis nehmen können.

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

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

Einzelgeräte ohne Anbindung an ein Netzwerk sind so zu schützen, dass Dritte die Geräte möglichst nicht entwenden können. Seitens der MAV sind regelmäßige Datensicherungen vorzusehen. Betriebssystem, Browser und Software sind über Updates regelmäßig zu aktualisieren. Vorhandene Daten sind zu schützen (z. B. Benutzerkennung, Passwortschutz, Firewall bei Internetanschluss, Virenschutz), so dass Dritte diese nicht unbefugt nutzen können.

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. Es ist sicherzustellen, dass nur MAV-Mitglieder den Verzeichnis- und Dateipfad einsehen und bearbeiten können.
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 elektronische Dokumente der MAV können grundsätzlich für alle Mitarbeitenden arbeitsrechtliche Maßnahmen nach sich ziehen.
Elektronische MAV-Dokumente sollten, soweit softwareseitig möglich, bei der Speicherung mit einem Passwort versehen werden. Dieses Passwort darf nur den MAV-Mitgliedern bekannt sein.

3.3 Drucker

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 durch die MAV im organisationsinternen Intranet bzw. über das Internet dürfen personenbezogene Daten Dritter (z. B. Niederschriften der MAV) nicht veröffentlicht werden. Möglich ist dagegen die Veröffentlichung von Beschlüssen 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 sind sowohl für das Intranet als auch das Internet grundsätzlich die Einwilligungen 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. Jeder MAV muss eine eigene E-Mail 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 von Dritten (z. B. im Rahmen der Vertretung) nicht eingesehen werden können (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 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 kann 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 zustellen. 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 Obwohl jüngere Bundesarbeitsgerichtsurteile auch die Zustimmungsverweigerung eines Betriebsrates per unsignierter E-Mail für zulässig erachten, sollte immer dann, wenn das MVG-K die Schriftform vorsieht, der Brief oder das Fax als entsprechende Norm gewählt werden, um den fristgerechten Zugang und dessen Nachweisbarkeit sicher zu stellen.

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 auf die mögliche Sensibilität des Dokuments der Datenschutz 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 empfangenden Person über geschützte (getunnelte) Leitungen übermittelt werden, 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. Durch organisatorische Regelung kann auf die Vertraulichkeit der Information hingewiesen werden, so dass Vertretungspersonen erkennen können, dass diese E-Mails nicht von ihnen 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. An der technischen Umsetzung sowohl bezüglich der „evlka-Adressen" als auch anderer E-Mail-Adressen wird noch gearbeitet. Diese Orientierungshilfe wird insoweit zu einem späteren Zeitpunkt ergänzt. 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.