Datenschutz
Handreichung für die Mitarbeitervertretung (MAV)

Für die MAV ist der Datenschutz in zweierlei Hinsicht von Bedeutung:

MAV und Dienstgeber

Im Hinblick auf den Beschäftigtendatenschutz nach § 49 Datenschutzgesetz der EKD (DSG-EKD) hat die MAV ein Kontrollrecht nach § 35 III b Mitarbeitervertretungsgesetz EKD (MVG).

MAV als Gremium

In Angelegenheiten ihrer Geschäftsführung muss die MAV gemäß § 22 III MVG für die Einhaltung des Datenschutzes selbst sorgen.

1. Allgemeines zu Datenschutz

Die Datenschutzgrundverordnung (**DSGVO**) ist eine Verordnung der EU, mit der die Regeln zur Verarbeitung personenbezogener Daten EU-weit vereinheitlicht werden. Ziele: Schutz der personenbezogen Daten innerhalb der EU und Gewährleistung des freien Datenverkehrs innerhalb des europäischen Binnenmarktes.
Eine EU-Verordnung hat im Gegensatz zu einer Richtlinie unmittelbare Wirkung in allen EU-Mitgliedsstaaten. D.h., sie muss nicht in nationales Recht umgesetzt werden; Öffnungsklausel geben Handlungsspielraum; die Harmonisierung darf jedoch nicht unterlaufen werden. Eine solche Öffnungsklausel betrifft z. B. den Beschäftigtendatenschutz (Art. 88 DGSVO: Rechtsvorschriften oder Kollektivvereinbarungen).
Für EKD und Diakonie gilt das DSG-EKD.

§ 4 Nr. 1 DSG-EKD: **Personenbezogene Daten** sind alle Informationen, die sich auf natürliche Personen beziehen oder zumindest beziehbar sind und dadurch Rückschlüsse auf deren Person erlauben. Besonders schützenswert sind Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität, Gewerkschaftszugehörigkeit (sog. besondere Kategorien personenbezogener Daten, § 4 Nr. 2 DSG-EKD). Recht auf informationelle Selbstbestimmung (BVerfG).

§ 4 Nr. 3 DSG-EKD: **Verarbeitung** ist jede Maßnahme, die mit den personenbezogenen Daten - gleichgültig ob manuell oder automatisiert - durchgeführt werden.

Grundsätze des Datenschutzes, § 5 DSG-EKD
§§ 5 I 1., 6 Nr. 1 DSG-EKD: Rechtmäßigkeit = Erlaubnisvorbehalt
Gesetz, Dienstvereinbarung, Einwilligung
Verhältnismäßigkeit, Treu und Glauben, Transparenz
§ 5 I 2. DSG-EKG: Zweckbindung
§ 5 I 3. DSG-EKD: Datensparsamkeit
§ 5 I 4. DSG-EKD: Richtigkeit
§ 5 I 5. DSG-EKD: Speicherbegrenzung
§ 5 I 6. DSG-EKD: Integrität und Vertraulichkeit
§ 5 II DSG-EKD: Rechenschaftspflicht der verantwortlichen Stelle; z.B. Verarbeitungsverzeichnis, § 31 DSG-EKD.

Pflichten, die Mitarbeitende beim Umgang mit personenbezogen Daten haben, § 26 DSG-EKD
Dienstanweisung (grundsätzlich kein Mitbestimmungs- oder sonstiges Beteiligungsrecht der MAV)
Intranet der ELKB
https://www2.elkb.de/intranet/node/19999

2. Beschäftigtendatenschutz: § 49 DSG-EKD

Schutz bei Erhebung, Nutzung und Verarbeitung von Arbeitnehmerdaten oder aus Daten aus dem Arbeitsverhältnis; Schutzrecht der Mitarbeitenden gegen Dienstgeber

Es dürfen nur Daten verarbeitet werden, die im Zusammenhang stehen mit der Be-gründung (dazu gehören auch die Bewerberdaten, allgemeine Kontaktdaten und das Tätigkeitsprofil), Erfüllung und Beendigung des Arbeitsverhältnisses (=Zweckbin-dung).
Die Mitarbeitenden haben das Recht auf Löschung, Auskunft, Berichtigung und Widerruf, §§ 16 ff DSG-EKD.

Grundsatz: Erlaubnisvorbehalt (= alles ist verboten, es sei denn, es gibt eine gesetzliche Erlaubnis oder eine Erlaubnis aus einer Dienstvereinbarung). Gibt es keine gesetzliche Vorschrift und auch keine Dienstvereinbarung, die den Eingriff erlaubt, muss die schriftliche Einwilligung der MitarbeiterIn eingeholt werden. Die Einwilligung muss freiwillig abgegeben werden. Wegen der Abhängigkeit im Beschäftigungsverhältnis sind an die Beurteilung der Freiwilligkeit strenge Maßstäbe zu stellen. Es sind die Umstände, unter denen die Einwilligung erteilt wurde zu berücksichtigen. § 49 III DSG-EKD.
Freiwilligkeit kann vorliegen, wenn für die MitarbeiterIn ein rechtlicher oder wirtschaftlicher Vorteil gegeben ist oder Dienstgeber und MitarbeiterIn gleichgelagerte Interessen haben (§ 49 III S. 2 DSG-EKD).
z.B.: Vorteil: BEM; gleichgelagerte Interessen: Geburtstagsliste, Fotos fürs Intranet.

Spannungsfeld: Dienstgeber muss die Daten minimieren, die Datenschutzvor-schriften beachten; für Aufklärungsmaßnahmen braucht er aber ein Maximum an Informationen, § 49 II DSG-EKD.
Das bedeutet z.B.:
Keine heimliche Überwachung durch Keylogger (Spähsoftware), BAG 27.7.2016, 2 AZR 681/16
Video-/Kameraüberwachung nur bei konkretem Verdacht auf Straftat, BAG 22.9.2016, 2 AZR 848/15
Kein Zugriff auf persönliche E-Mail-Accounts, die auch privat genutzt werden

§ 45 DSG-EKD: Geldbußen, wenn die verantwortliche Stelle eine wirtschaftliche Tätigkeit ausübt
§ 48 DSG-EKD: Schadensersatz
§ 36 DSG-EKD: örtlicher Datenschutzbeauftragter
§ 39 DSG-EKD: Aufsichtsbehörde EKD-Süd: Dr. Axel Gutenkunst, Ulm
sued@datenschutz.ekd.de; oberster Datenschützer: OKR Michael Jakob
info@datenschutz.ekd.de
https://datenschutz.ekd.de

3. Datenschutz innerhalb des Gremiums: § 22 III MVG

Die Mitarbeitervertretung (MAV) ist Teil der Dienststelle, unterliegt aber wegen ihrer Unabhängigkeit vom Dienstgeber nicht der Kontrollbefugnis des örtlichen Datenschutzbeauftragten.
Seit 1.1.19 gilt § 22 III Mitarbeitervertretungsgesetz EKD (MVG): „Die Mitarbeitervertretung hat für die Einhaltung des Datenschutzes in den Angelegenheiten ihrer Geschäftsführung zu sorgen."
Die MAV muss selbst für den Datenschutz in ihren eigenen Angelegenheiten sorgen.

Die Dienststelle ist „verantwortliche Stelle" im Sinn des § 4 Nummer 9. Daten-schutzgesetz EKD (DSG-EKD). Die Mitarbeitervertretung (MAV) ist Teil der Dienststelle und nicht „Dritte" im Sinne des § 4 Nummer 12. DSG-EKD. Der örtliche Datenschutzbeauftragte hat keine Kontrollbefugnis gegenüber der MAV. Die MAV-Mitgliedschaft ist ein Ehrenamt, also keine zu vergütende Arbeitsleistung. Dies begründet die Unabhängigkeit der MAV-Mitglieder (Loseblatt-Kommentar Fey-Rehren, § 19 MVG.EKD, Rd.nr. 2). MAV-Mitglieder sind vor Benachteiligungen der Dienstgeberseite geschützt und im Rahmen ihrer MAV-Tätigkeit von fachlichen Weisungen befreit. Der/die Datenschutzbeauftragte wird von Dienstgeberseite ausgewählt. Die Unabhängigkeit der MAV-Mitglieder ist unvereinbar mit der Kontrolle durch eine Beauftragte/einen Beauftragten des Dienstgebers (so auch Bundesarbeitsgericht (BAG), Beschluss vom 11.11.1997, AZ: 1 ABR 21/97 zu Betriebsratstätigkeit/Datenschutzkontrolle).

§ 22 III MVG n. F. normiert eine eigene Verpflichtung der MAV, auf die Einhaltung des Datenschutzes zu achten.

Das bedeutet im Einzelnen:

a) MAV-Büro

Die Bürotür nicht offen lassen, wenn das Büro nicht besetzt ist oder kurz verlassen wird. Es muss sichergestellt sein, dass niemand Akten oder Schriftstücke aus dem Büro entfernen kann. Die MAV hat über das MAV-Büro das Hausrecht. D.h., nur die MAV-Mitglieder haben Zugang zum Büro bzw. legen fest, wer das MAV-Büro betreten darf. Der Schlüssel ist im alleinigen Gewahrsam der MAV (grundsätzlich der/des MAV-Vorsitzenden).

Es ist sicherzustellen, dass keine Akten/Schriftstücke offen einsehbar sind.
Akten bzw. Schriftstücke, die nicht für die aktuelle Arbeit gebraucht werden, sind wegzuschließen.
Der Dienstgeber ist verpflichtet, der MAV abschließbare Schränke zur Verfügung zu stellen.

Bei Gesprächen im Rahmen der Sprechstunden oder Telefonaten mit vertraulichem Inhalt ist dafür Sorge zu tragen, dass keine andere Person mithören kann (Schließen von Fenster und Tür).

Nach § 30 I MVG.EKD (MVG) hat die MAV einen Anspruch auf ein Büro, soweit dies erforderlich ist. Die MAV hat das alleinige Hausrecht über das MAV-Büro, Loseblatt-Kommentar Fey/Rehren, § 30 MVG Rd.nr. 3. Dieses Hausrecht beinhaltet das Recht, dass ausschließlich MAV-Mitglieder den Schlüssel zu diesem Raum besitzen.
Abschließbare Schränke gehören zu den erforderlichen Sachmitteln (Fey/Rehren, § 30 Rd.nr. 7).
Nach § 28 I MVG kann die MAV Sprechstunden einrichten.
Der Schutz der Vertraulichkeit von Gesprächen und der Korrespondenz ist notwendiger Bestandteil der MAV-Arbeit. Dieser Schutz ist eine Abwehrpflicht gegenüber außenstehenden Personen und ein Abwehrrecht gegen den Dienstgeber.

b) PC/Laptop/Smartphone

Jeder PC/Laptop, jedes Smartphone muss ein Passwort haben. Passwörter dürfen nicht öffentlich zugänglich sein und nicht weiter gegeben werden.

Der Dienstgeber hat kein Einsichtsrecht für den MAV-Account.

Jede MAV muss einen eigenen E-Mail-Account (z. B. institutionelle E-Mail über das Intranet der ELKB, z.B. mav.dekanat.xy@elkb.de) haben.

Der Account darf nicht über einen Server im EU-Ausland bedient werden. D.h.: keine Provider wie z.B. yahoo und gmail. Nicht gesichert und damit nicht empfehlenswert sind z. B. gmx, T-Online und Freenet. Empfehlenswert ist z. B. das Sichere Kirchennetz der ELKB. Die Registrierung erfolgt über das Intranet der ELKB - *https://www2.elkb.de/intranet*

Der Dienstgeber ist verpflichtet, der MAV eine eigene geschützte Funktions-Adresse zur Verfügung zu stellen. Es kann auch innerbetriebliche personalisierte E-Mail-Adressen geben, die von den normalen personalisierten Dienstadressen zu trennen und als solche als MAV-Adressen gekennzeichnet sind.
Hat der Dienstgeber keine Möglichkeit, einrichtungseigene Mail-Adressen zu vergeben, kann im Intranet der ELKB die Vergabe einer Mail-Adresse beantragt werden. Dies ist auch für MAVen der Diakonie in Bayern möglich. Die Registrierung erfolgt über das Intranet der ELKB - *https://www2.elkb.de/intranet*

Es dürfen keine Onlinedienste genutzt werden, die nicht dem Standard des DSG-EKD entsprechen. D.h.: keine dienstliche Nutzung von Onlinediensten wie WhatsApp, Instagram, Twitter. Von EKD und Diakonie Deutschland empfohlen wird SIMSme business *https://www.sims.me/business/de und https://www.wgkd.de/rahmenvertrag/deutsche-post.html*

Der Bildschirm sollte nur für die-/denjenigen einsehbar sein, der mit dem PC/Laptop arbeitet. Laptop und Smartphone müssen eine Blickschutzfolie haben.

Keine gefundenen USB-Sticks ausprobieren.

Keine dubiosen Mails öffnen; Vorsicht ist bei dem Öffnen von Links geboten.

Die MAV hat nach § 30 I MVG einen Anspruch auf dienstübliche technische Ausstattung im erforderlichen Umfang. Dazu können gehören PC/Laptop und der Zugang zum Internet (BAG Beschluss vom 14.07.2010, AZ: 7 ABR 80/08, zu Internet-Zugang für jedes Betriebsratsmitglied).
Der MAV muss erlaubt sein, eine eigene E-Mail-Adresse einzurichten. Die Korrespondenz der MAV muss geschützt sein.
Der Dienstgeber hat dann keinen Zugriff auf den Mail-Verkehr, wenn die MAV eine institutionalisierte E-Mail-Adresse hat. Den Inhalt von Dienst-E-Mails dagegen kann der Dienstgeber in Ausnahmefällen einsehen (wenn keine private Nutzung erlaubt ist, eine Dienstvereinbarung existiert und z.B. Verdacht auf Straftaten besteht – BAG Urteil vom 27.07.2017, AZ: 2 AZR 681/16 - oder wenn die/der Mitarbeitende überraschend für lange Zeit ausfällt).
Die Datenübermittlung muss dem Datenschutzniveau der DGSVO entsprechen, § 10 DSG-EKD. Solange keine Standardschutzklauseln auf EU-Niveau bzw. keine Abkommen mit den USA bestehen, sind Provider wie gmail und yahoo ausgeschlossen. Es empfiehlt sich deshalb eine E-Mail-Adresse der ELKB, wenn der Dienstgeber keine einrichtungseigene E-Mail-Adresse anbieten kann.
Für dienstlich genutzte Smartphones verbieten sich Onlinedienste wie Whatsapp, Instagram oder Twitter. Die Wirtschaftsgesellschaft der Kirchen in Deutschland mbH (WGKD) hat mit der Deutschen Post einen deutschlandweiten Rahmenvertrag für die Nutzung von SIMSme Business geschlossen. Sowohl die Einrichtungen aus Kirche, Caritas und Diakonie als auch ihre Angestellten können mit SIMSme Business chatten.

c) Versand von personenbezogenen Daten

Personenbezogene Daten sind sämtliche Daten, die auf irgendeine Weise einer Person zugeordnet sind oder zugeordnet werden können.

Personenbezogene Daten nur in sichtgeschützten und geschlossenen Mappen oder sonstigen Behältnissen weiterleiten; wenn nötig, muss die persönliche Weitergabe an den Empfänger erfolgen.

Beim Schreiben von E-Mails ist auf den Verteiler zu achten. Es ist abzuwägen, ob tatsächlich alle Personen im Verteiler die Informationen kennen müssen.

Kennen sich die E-Mail-Empfänger untereinander nicht, sind die Mails in Blind-Kopie (Bcc) zu versenden.

Erhaltene E-Mails dürfen nicht einfach weitergeleitet werden. Es ist zu prüfen, welche Daten notwendigerweise weitergegeben werden müssen.

Unterlagen nicht einfach einscannen und per Mail weiterleiten. Auch hier prüfen, welche Daten notwendigerweise weitergegeben werden müssen.

Personenbezogene Daten, die außer Haus gehen sollen, dürfen nur dann per E-Mail weiter geleitet werden, wenn sie mit Passwort geschützt sind und das Kennwort auf anderem Wege bekannt gegeben wird. Trägerübergreifend können personenbezogene Daten auch über die Cloud der ELKB geteilt werden. Ansonsten sind die Daten zu anonymisieren.

d) Aufbewahrung von personenbezogen Daten und sonstigen Unterlagen

Es ist regelmäßig zu überprüfen, welche Unterlagen noch gebraucht werden.

Grundsatz 1: Unterlagen sind aufzubewahren, solange sie von rechtlicher Bedeutung sind.
Grundsatz 2: Alles, was in der Personalakte niedergelegt ist, braucht die MAV nicht zusätzlich selbst aufzubewahren.

- Bewerbungsunterlagen sind grundsätzlich sofort nach Besetzung der Stelle zu vernichten.
- Unterlagen aus Beratungen sind solange aufzubewahren, wie sie notwendig sind.
- Beschlussprotokolle sind mindestens drei Jahre lang aufzubewahren.
- Wahlunterlagen sind fünf Jahre aufzubewahren.
- Buchungsbelege sind 10 Jahre aufzubewahren.
- Dienstvereinbarungen und Beschlüsse sind aufzubewahren, solange sie gültig sind.
- Die Geschäftsordnung verliert mit der Neuwahl des Gremiums ihre Gültigkeit. Das Gremium muss erneut darüber beschließen.

Ausgenommen der Aufbewahrungspflicht für Wahlunterlagen (§ 13 Wahlordnung MVG (WahlO) – gibt es für MAVen keine Vorschriften über Aufbewahrungsfristen. Die allgemeine Verjährungsfrist des § 195 Bürgerliches Gesetzbuch (BGB) von drei Jahren zieht das Schrifttum für die Aufbewahrung von Unterlagen allgemeiner Art heran; für die Aufbewahrung von Buchungsbelegen die 10-Jahresfrist des § 257 IV Handelsgesetzbuch (HGB).

e) Vernichtung von Unterlagen

Nicht mehr benötigte Unterlagen sind zu schreddern.
Bei größeren Mengen ist eine Entsorgungsfirma zu beauftragen.

Bei der Entsorgung von Festplatten/PC /Laptop/Smartphone muss die MAV dafür sorgen, dass die darauf befindlichen Daten gelöscht werden.

Der Dienstgeber ist dazu verpflichtet, die Kosten für die Entsorgung zu übernehmen. Es ist zu gewährleisten, dass die Dienstgeberseite auch bei der Datenvernichtung keinen Zugriff auf

die Unterlagen/Daten hat. D. h. z.B., dass getrennte Entsorgungscontainer für die Unterlagen aufzustellen sind bzw. eine externe Firma mit der Datenlöschung zu beauftragt ist.

Die MAV verwaltet ihre Unterlagen eigenverantwortlich. Der Dienstgeber darf zu keinem Zeitpunkt Zugriff auf die Daten der MAV haben (Landesarbeitsgericht Düsseldorf, Beschluss vom 7.2.2012, AZ: TaBV 87/11 zum Thema Zugriffsrecht des Arbeitgebers auf Laufwerk des Betriebsrats). Dies hat notwendiger Weise die separate Datenvernichtung zur Folge.

f) Außerhalb des MAV-Büros und der MAV-Sitzung

Grundsatz: Informationen, die nicht für andere bestimmt sind, dürfen nicht an Außenstehen weitergegeben werden.

MAV-Mitglieder, die unterwegs sind mit Laptop/Smartphone oder Unterlagen in Papier müssen die Arbeitsmaterialien vor den Blicken anderer Personen schützen. Im Zweifel ist darauf zu verzichten, jetzt die Arbeiten auszuführen.

g) Informationsrecht der MAV, Auskunftspflicht des Dienstgebers

- **Bewerbungsunterlagen**

Der MAV sind auf Verlangen sämtliche Bewerbungsunterlagen vollständig und nicht anonymisiert zu überlassen.

Nach § 34 III MVG sind der MAV auf Verlangen sämtliche Bewerbungsunterlagen vorzulegen. Um eine Beurteilung überhaupt abgeben zu können, sind die Bewerbungsunterlagen vollständig und nicht anonymisiert zu überlassen.

- **Bruttolohnlisten**

Die MAV hat das Recht, halbjährlich die Bruttolohnlisten vollständig und nicht anonymisiert ausgehändigt zu bekommen

Die MAV hat das Recht, halbjährlich die Bruttolohnlisten ausgehändigt zu bekommen (Beschluss des Kirchengerichtshofs der EKD vom 19.6.2018, AZ: KGH.EKD II-0124/6-2018). Die Bruttolohnlisten dürfen vom Dienstgeber nicht anonymisiert werden (LAG Niedersachsen, Beschluss vom 22.10.2018, AZ: 12 TaBV 23/18).

- **Betriebliches Eingliederungsmanagement (BEM) und Unterlagen**

Der Dienstgeber informiert die MAV über die Mitarbeitenden, die innerhalb der letzten zwölf Monate insgesamt sechs Wochen arbeitsunfähig erkrankt waren.

Ist die MAV am BEM-Verfahren beteiligt, erhält sie sämtliche Unterlagen in nicht anonymisierter Form.

Das BEM ist in § 167 II SGB IX geregelt.
Im Rahmen der Mitbestimmung aus § 40 Lit. b MVG hat die MAV die Aufgabe der Rechtskontrolle und der Klärung von Verfahrensregelungen (Fey/Rehren, § 40 Rd.nr. 12).
Der Dienstgeber ist verpflichtet, der MAV die Namen der Mitarbeitenden zu nennen, die die Voraussetzungen des BEM erfüllt haben (BAG Beschluss vom 7.2.2012, AZ: 1 ABR 46/10 zum Recht des Betriebsrats).
Der Dienstgeber muss die betreffende Mitarbeiterin/den betreffenden Mitarbeiter fragen, ob BEM und wenn ja, ob eine Beteiligung der MAV gewünscht ist. Über das Ergebnis hat der Dienstgeber die MAV zu informieren. Wenn BEM unter Mitwirkung der MAV gewünscht ist, hat die MAV Zugriff auf alle Unterlagen/Daten.

- **MAV- Wahl**

Der Dienstgeber gibt der MAV bzw. dem Wahlvorstand sämtliche Daten über die Mitarbeitenden, die für die Prüfung des aktiven und passiven Wahlrechts notwendig sind. Dies sind insbesondere:

Vor- und Zuname; Ort der Tätigkeit; Art der Tätigkeit; Geburtsdatum; Beginn der Arbeitsaufnahme; Mutterschutz, Beschäftigungsverbot; Elternzeit; Pflegezeit; Beurlaubung; Bezug einer Erwerbsunfähigkeitsrente; häusliche Gemeinschaft mit Ehegatte/LebenspartnerIn, Verwandte/Verschwägerte ersten Grades, die der Dienststellenleitung angehören; Abordnung

Die Dienststellenleitung leistet für die Erstellung der Wählerlisten Amtshilfe, § 4 III WahlO MVG.
Die MAV bzw. der Wahlvorstand prüft das aktive und passive Wahlrecht der Mitarbeitenden nach §§ 9, 10 MVG. Auch von anderen Dienststellen abgeordnete Mitarbeitende können ein Wahlrecht haben.
Bei den Wahlbewerbern sind auch Art und Ort der Tätigkeit anzugeben, § 7 I WahlO MVG.
Die Vorschriften des MVG geben der MAV das Recht auf Erhalt der für die Durchführung der Wahl notwendigen Daten.

4. Empfehlung

Ein MAV-Mitglied übernimmt die Überwachung des Datenschutzes. Dieses MAV-Mitglied ist speziell zu schulen. Die Kosten für die Schulung hat der Dienstgeber zu tragen.

§ 22 III MVG verlangt ausdrücklich, dass die MAV den Schutz ihrer Daten kontrolliert. Dies ist nicht ohne entsprechende Kenntnis des Datenschutzrechts möglich. Eine entsprechende Schulung ist nach § 19 III MVG zu gewähren.