Gesamtausschuss

**der Mitarbeiter und Mitarbeiterinnen im kirchlichen und diakonischen Dienst
für den Bereich der Evangelischen Landeskirche in Baden und
des Diakonischen Werkes der Evangelischen Landeskirche in Baden e. V.**

Arbeitsgruppe " Multimedia / EDV / neue Technologien in Kirche und Diakonie"

CHECKLISTE " EDV "

Ob wir wollen oder nicht, der Personalcomputer oder die EDV (elektronische Datenverarbeitung) bestimmen heute unseren (Arbeits-)Alltag mit und werden es in Zukunft noch mehr tun.

Die Einstellung zur Einführung neuer Systeme ist sehr ambivalent, man erkennt die vielleicht vorhandenen Vorteile, sieht jedoch, manchmal auch mit wachsender Sorge, die Nachteile oder die drohenden Gefahren.

Die Erstellung dieses Merkblattes geschieht mit der Absicht, unseren Mitarbeitervertretungen bei der Wahrnehmung Ihrer Aufgaben im Zusammenhang mit Datenverarbeitungssystemen und -Programmen behilflich zu sein.
Es soll auf Beachtenswertes hinweisen, über MAV-Rechte aufklären und Problemfelder aufzeigen.
Ein Anspruch auf Vollständigkeit wäre jedoch vermessen.

Für Verbesserungsvorschläge und Anregungen jeglicher Art sind wir stets dankbar.

Internet: www.ga-baden.de

Inhalt:

---

1 Rechtliche Grundlagen

1.1 Rechte der MAV aus dem MVG

Liste der wichtigsten Mitbestimmungs-Rechte im MVG, die durch die Einführung von EDV-Anlagen zum Tragen kommen können:

- *§ 39 c* Aufstellung von Grundsätzen zur Aus-, Fort- und Weiterbildung sowie die Teilnehmerauswahl
  Hier kann die MAV mitbestimmen, indem sie Einfluss auf die Festlegung der Grundsätze und der Teilnehmerauswahl nimmt (z.B. welche Arbeitsbereiche wie geschult werden z.B. Computerkurse für Anwender etc.).

- *§ 40 b* Maßnahmen zur Verhütung von Unfällen und gesundheitlichen Gefahren
  Im Bezug auf Bildschirmarbeitsplätze sollte die MAV überwachen, ob die gesetzlichen Vorschriften (→Bildschirmarbeitsverordnung, Berufsgenossenschaft →siehe auch Punkt 9) zum Schutz der MitarbeiterInnen auch eingehalten werden. Dies gilt für die Arbeitsplatzgestaltung ebenso wie für vorgeschriebene Untersuchungen (z.B. Augen).

- *§ 40 d* Beginn und Ende der täglichen Arbeitszeit und der Pausen
  Da hier zum Beispiel bei Bildschirmarbeitsplätzen besondere Regelungen gelten, sollte die MAV auf die Einhaltung der entsprechenden gesetzlichen Vorschriften achten. Nähere Informationen findet man in der Bildschirmarbeitsverordnung und den Veröffentlichungen der zuständigen Berufsgenossenschaften.

- *§ 40 g* Grundsätze der Arbeitsplatzgestaltung
  Da hier zum Beispiel bei Bildschirmarbeitsplätzen besondere Regelungen gelten, sollte die MAV auf die Einhaltung der entsprechenden gesetzlichen Vorschriften achten.(siehe Bildschirmarbeitsverordnung und Merkblatt zur Arbeitsplatzgestaltung)
- *§ 40 h* Einführung grundlegend neuer Arbeitsmethoden *(-Neueinrichtung)*
  Wird an einem Arbeitsplatz zum ersten Mal eine technische Einrichtung zur elektronischen Datenverarbeitung installiert, ist die MAV mitbestimmungsberechtigt.

Dies gilt auch im Bezug auf die Zumutbarkeit der Umstellung auf neue Techniken für z.B. ältere MitarbeiterInnen.

- *§ 40 i* Maßnahmen zur Hebung der Arbeitsleistung und zur Erleichterung des Arbeits ablaufs
  In Betracht kommen hier unter Anderem:
  - alle Maßnahmen und Geräte, die die Arbeitsleistung einzelner MitarbeiterInnen erfassen: z.B. Fahrtenschreiber, speichernde Codeschlösser etc.
  - alle Maßnahmen und Geräte, die die Arbeitsabläufe erleichtern: z.B. Handy's, ISDN-Anlagen, Netzwerke etc.

- *§ 40 j* Einführung und Anwendung von Maßnahmen, die **geeignet** sind, das Verhalten oder die Leistung der MitarbeiterInnen zu überwachen .
  Wichtig ist hier das Wort "geeignet". Es spielt keine Rolle, ob der Arbeitgeber diese Geräte oder entsprechende Software tatsächlich zur Kontrolle nutzen will, entscheidend ist die technische Möglichkeit, dies zu tun.
  Beispiele: Zeiterfassung (Stechuhr), Telefon- (ISDN-) Anlagen, Zugangskontrolle zu Arbeitsbereichen (Codeschlösser), Mobiltelefone/Handys, Fahrtenschreiber, Datensicherungssysteme mit Zugangskontrolle. Entscheidend ist dabei immer, ob Daten (auch aus mehreren Quellen) Rückschlüsse auf die Leistung und das Verhalten einzelner MitarbeiterInnen ermöglichen.

- § 40 k Regelung der Ordnung in der Dienststelle und des Verhaltens der MitarbeiterInnen im Dienst
  Dies kann sich sowohl auf die Weisungen zum System- und Datenschutz (siehe Punkte 6 und 7), als auch auf die Regelung der Pausen beziehen. Für Bildschirmarbeitsplätze gibt es hier besondere Regelungen für Arbeitsunterbrechungen (siehe Punkt 9.6).

1.2 Bildschirmarbeitsverordnung

§ 2 Begriffsbestimmungen:

*(1) **Bildschirmgerät** im Sinne dieser Verordnung ist ein Bildschirm zur Darstellung von alphanumerischen Zeichen oder zur Graphikdarstellung, ungeachtet des Darstellungsverfahrens.*

*(2) **Bildschirmarbeitsplatz** im Sinne dieser Verordnung ist ein Arbeitsplatz mit Bildschirmgerät, der ausgestattet sein kann mit:*

1. Einrichtungen zur Erfassung von Daten

2. Software, die dem Beschäftigten bei der Ausführung seiner Aufgaben zur Verfügung steht,

3. Zusatzgeräten und Elementen, die zum Betreiben oder Benutzen des Bildschirmgerätes gehören, oder

4. sonstigen Arbeitsmitteln,

sowie die unmittelbare Arbeitsumgebung.

*(3) **Beschäftigte** im Sinne dieser Verordnung sind Beschäftigte, die gewöhnlich bei einem **nicht unwesentlichen** Teil ihrer normalen Arbeit ein Bildschirmgerät benutzen.*
(Der Begriff "nicht unwesentlich" kann bereits bei einem Viertel der Arbeitszeit zutreffen.)

1.3 Gesundheitsschutz bzw. -vorsorge/Gestaltung der Arbeitsplätze

Bei allen nachfolgenden Punkten ist die Bildschirmarbeitsverordnung vom 20. Dezember 1996 verbindlich anzuwenden. Hier sind eindeutige Standards festgeschrieben. Die Bildschirmarbeitsverordnung gilt sofort für alte und neu eingerichtete Bildschirmarbeitsplätze.
Hingewiesen wird noch auf 2 Merkblätter der Verwaltungsberufsgenossenschaft Ludwigsburg: *"Flächennutzung im Büro" Druckschrift BGI 523 und "Hilfen für die Gestaltung an Bildschirmgeräten in Büro und Verwaltung" Veröffentlichung BGI 650*

- **Bildschirmgeräte**
  Die Anzeige auf Bildschirmgeräten muss so gestaltet sein, dass zu hohe Belastungen der Beschäftigten an Bildschirmarbeitsplätzen nicht auftreten können.

- **Tastaturen**
  Tastaturen müssen vom Bildschirmgerät getrennt aufgestellt werden können, damit die Tastatur den jeweiligen Arbeitsbedürfnissen entsprechend umgestellt oder verschoben werden kann. Die Aufstellpunkte der Tastatur müssen rutschhemmend sein, damit die Tastatur während der Benutzung nicht unbeabsichtigt verschoben werden kann. Von diesen Festlegungen darf nur bei Kompaktgeräten/Kompaktanlagen abgewichen werden.

- **Schriftstücke zur Übertragung in den PC**
  Die Ausführung und Gestaltung muss eine leichte Lesbarkeit gewährleisten; es sei denn, eine Einflussnahme auf die Vorlagengestaltung ist nicht möglich.

- **Vorlagenhalter**
  Bildschirmarbeitsplätze sind mit ergonomisch gestalteten Vorlagenhaltern auszustatten, weil sonst stark ermüdende oder gesundheitsschädliche Körperhaltungen nicht ausgeschlossen werden können.

- **Bildschirm-Arbeitstische**
  Die Abmessungen von Bildschirm-Arbeitstischen müssen den geltenden ergonomischen Vorschriften entsprechen, damit stark ermüdende und/oder gesundheitsschädliche Körperhaltungen vermieden werden.

- **Bürostühle und -sessel, Fußstützen**
  An Bildschirmarbeitsplätzen müssen höhenverstellbare Drehstühle bzw. -sessel sowie, falls erforderlich, Fußstützen eingesetzt werden.

- **Anordnung der Arbeitsmittel (PC, Bürostuhl, Arbeitstisch etc.)**
  Die Arbeitsmittel von Bildschirmarbeitsplätzen müssen so angeordnet werden, dass entsprechend der jeweiligen Arbeitsaufgabe die Beschäftigten so gering wie möglich belastet werden.

- **Flächenbedarf von Bildschirm-Arbeitsplätzen**
  Hinsichtlich des Flächenbedarfs von Bildschirm-Arbeitsplätzen sind die genannten Richtlinien der Bildschirmarbeitsverordnung einzuhalten.

- **Beleuchtung an Bildschirm-Arbeitsplätzen**
  Die Beleuchtung muss so angeordnet und bemessen sein, dass sich aus der Art der Beleuchtung keine Unfall- und/oder Gesundheitsgefahren ergeben.

- **Raumklima**
  Hinsichtlich der Raumgröße ist ein Mindeststandard einzuhalten (siehe Arbeitsstättenverordnung). Dieser darf nicht unterschritten werden! Die Wärmebelastung durch die vorhandenen Geräte muss gemessen werden und es darf eine Höchstgrenze nicht überschritten werden.

- **Überprüfung des Sehvermögens**
  Der Arbeitgeber hat den Beschäftigten vor Aufnahme ihrer Tätigkeit an Bildschirmgeräten, anschließend in regelmäßigen Zeitabständen sowie bei Auftreten von Sehbeschwerden, die auf die Arbeit am Bildschirmgerät zurückgeführt werden können, eine angemessene Untersuchung der Augen und des Sehvermögens durch eine qualifizierte Person anzubieten. Erweist sich auf Grund der Ergebnisse einer Untersuchung eine augenärztliche Untersuchung als erforderlich, ist diese zu ermöglichen.
  Hier sollen auch die Standards der Verwaltungsberufsgenossenschaft zu arbeitsmedizinischen Vorsorgeuntersuchungen (BGV A4) Berücksichtigung finden, da in diesem Punkt die Bildschirmarbeitsverordnung sehr oberflächlich ist.

- **Fachkräfte für Arbeitssicherheit**
  Das **Arbeitssicherheitsgesetz (ASiG)** verpflichtet die Arbeitgeber zur Bestellung von **Betriebsärzten (§ 2 ASiG) und Fachkräften für Arbeitssicherheit (§ 5 ASiG)**. Dies kann auch durch Verpflichtung eines überbetrieblichen Dienstes (privater Anbieter) geschehen. Die Aufgaben/Pflichten des Betriebsarztes bzw. der Fachkraft für Arbeitssicherheit sind in diesem Gesetz geregelt; genauso ist vorgeschrieben, welche berufliche Qualifikation vorausgesetzt wird. Die Bestellung unterliegt der Mitbestimmung durch die MAV **(§ 40 a MVG)**. Kopien der Prüfberichte des Betriebsarztes, aber vor allem der Fachkraft für Arbeitssicherheit sind an die MAV weiterzuleiten. So kann die MAV kontrollieren, ob der Arbeitgeber die festgestellten Mängel beseitigt.
  Außerdem ist ein **Arbeitsschutzausschuß** zu bilden, dem die MAV angehört **(§ 11 ASiG)**.

- **Sicherheitsbeauftragte**
  Die Sicherheitsbeauftragten haben die Fachkräfte für Arbeitssicherheit zu unterstützen, die ja nicht permanent anwesend sein können. Dabei handelt es sich um Freiwillige aus dem Kreis der Beschäftigten, die von den Berufsgenossenschaften entsprechend geschult werden, damit sie ihre Aufgaben bewältigen können. Die Kosten für die Schulungen übernimmt die entsprechende Berufsgenossenschaft. Für diese Kurse erfolgt eine Arbeitsbefreiung durch den Arbeitgeber unter Fortzahlung aller Bezüge. Die Sicherheitsbeauftragten sind per Urkunde vom Arbeitgeber zu bestellen. Die gesetzlichen Grundlagen sind im SGB VII § 22 und 23 geregelt.

2. Bestandsverzeichnis

Für jeden Arbeitsplatz mit einem Gerät zur elektronischen Datenverarbeitung sollte ein vom Mitarbeiter gegengezeichnetes "Bestandsverzeichnis" existieren und bei Veränderungen fortgeschrieben werden.
Dort sollen nicht nur die einzelnen Hardwarekomponenten der Anlage mit ihrer Leistungsfähigkeit aufgeführt werden, sondern auch alle auf diesem Gerät eingesetzte "Software" (Programme, Betriebssystem) mit der Versionsnummer und ihrem Verwendungszweck.

3. Vernetzung zu anderen Anlagen/Dienststellen

Über Vernetzungen und Modemverbindungen können in kurzer Zeit große Mengen Daten geladen, gelöscht oder verändert werden. Es ist sicherzustellen, dass die Datenschutzbelange gewährleistet sind und unbefugter Zugriff auf geschützte Daten verhindert wird
→ siehe auch Punkt 5 B.
Maßnahmen sind zum Beispiel die Vergabe von Passwörtern, die den Nutzer nur auf Daten zugreifen lassen, die er zur Erfüllung seiner Aufgabe braucht.
Der Aufbau und die Betreuung der Anlage sollte von geschulten Fachkräften betrieben werden, wobei Art und Umfang der Vernetzung sehr unterschiedlich sein können (internes Netzwerk (Intranet), externes Netzwerk (Internet etc.), WAN).

4. Betreuung der Anlage

Die Betreuung durch Fachkräfte sollte bereits mit der Anschaffung sichergestellt sein, sie kann je nach Größe der Einrichtung und Umfang der Anlage durch eigene MitarbeiterInnen oder externe Firmen geschehen.
Dies dient der dauerhaften Funktionalität der Anlage ebenso wie einem zweckentsprechenden Datenschutz mit den dazugehörigen Unterweisungen.
Das Vorgenannte gilt ebenso für Umrüstung, Aufrüstung, Softwareinstallation und Systempflege (z.B. Defragmentierung) der gesamten Anlage.

5. Datensicherung

A. Grundsätze zur Datensicherung

(Auszug aus der Bekanntmachung des Bundesministers des Innern, BAnz Nr. 17 vom 25. Januar 1978)

- ... wurden "Grundsätze zur Datensicherung ..." formuliert, die der Vereinheitlichung der Datensicherung dienen sollen
- ... sind als allgemeine Grundlage anzusehen, auf der fachspezifische und aufgabenbezogene Detailregelungen aufgebaut werden können
- ... erscheint einerseits möglich, die Ziele der Datensicherung allgemeingültig und auch weitgehend vollständig anzugeben; andererseits ist es jedoch problematisch, organisatorische Maßnahmen, die sich technischer und personeller Hilfsmittel bedienen, allgemein verbindlich vorzuschreiben
- Die Vielfalt der Aufgabenstellungen ... und die daraus resultierenden unterschiedlichen organisatorischen Strukturen erfordern differenzierte, auf den Einzelfall abgestellte Maßnahmen, die weitgehend von den spezifischen Randbedingungen abhängen ...

- ... Forderung nach der Angemessenheit der Mittel: es muss davon ausgegangen werden, dass bei Behörden oder anderen Einrichtungen mit unterschiedlichen Aufgabenstellungen auch das Sicherheitsbedürfnis und damit auch die Bewertung der einzelnen Datensicherungsziele hinsichtlich der Notwendigkeit ihrer Erreichung unterschiedlich ist. Dies hat zur Folge, dass der Einsatz einer speziellen Maßnahme im einen Falle angemessen und notwendig, im anderen Falle jedoch völlig unangemessen und für eine optimale Aufgabenerfüllung sogar hinderlich ist.

B. Ziele der Datensicherung

Bei der Formulierung der Ziele der Datensicherung müssen zwei Aspekte berücksichtigt werden:

- **Sicherung der Daten gegen unbefugten Zugriff und Missbrauch**
- **Sicherung der Daten gegen Verlust, Verstümmelung und Zerstörung aufgrund organisatorischer und/oder technischer Mängel**

Bei der automatisierten Datenverarbeitung sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind...

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen und den zugehörigen Archiven zu verwehren (**Zugangskontrolle**)

2. Personen, die in der Datenverarbeitung tätig sind, daran zu hindern, dass sie Datenträger unbefugt entfernen (**Abgangskontrolle**)

3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (**Speicherkontrolle**)

4. die Benutzung von Datenverarbeitungssystemen, aus denen oder in die Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern (**Benutzerkontrolle**)

5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (**Zugriffskontrolle**)

6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Daten durch selbsttätige Einrichtungen übermittelt werden können (**Übermittlungskontrolle**)

7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**)

8. zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**)

9. zu gewährleisten, dass bei der Übermittlung von Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können (**Transportkontrolle**)

Zur Sicherung der Daten nach den 9 o.g. Punkte sind Fehlerquellen zu minimieren und zweifelsfrei erkennbar zu machen, und es muss eine einwandfreie Rekonstruktion (z.B. durch Bestandsführung nach dem „Großvater-/Vater-/Sohn-Prinzip“)[1] möglich sein.

[1] Erläuterung siehe Punkt 10

6. Datenschutz

Bund

Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz-BDSG)

§ 1
Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Kirche EKD

Kirchengesetz über den Datenschutz der EKD (DSG-EKD)

vom 12. November 1993

§ 1
Zweck und Anwendungsbereich
(1) Zweck dieses Kirchengesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
(2) ...gilt für...kirchliche Behörden und sonstige Dienststellen und Einrichtungen der Ev. Kirche in Deutschland und der Gliedkirchen (kirchliche Stellen).

Kirche Baden

Kirchliches Gesetz zur Ausführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (AusG-DSG-EKD)

Vom 26. April 1994

(siehe Rechtssammlung EKIBA)

Gilt auch für diakonische Einrichtungen und Rechtsträger, da jedes Mitglied im DW Baden per Satzung das kirchliche Datenschutzrecht anerkennt.

Was ist neben den Bestimmungen der Datenschutzgesetze zu beachten ?

Bei jeder Art von "Datenfluss" ist grundsätzlich alles verboten, was nicht ausdrücklich gesetzlich erlaubt ist.

- **Verpflichtungserklärung**
  Jeder, der mit pers.bezog. Daten zu tun hat bzw. dienstlich die Möglichkeit/en hat, an entsprechende Daten heranzukommen, ist schriftlich unter Hinweis auf §§ 43 und 44 BDSG (Straf- und Bußgeldvorschriften) zum Datengeheimnis zu verpflichten, also neben den eigenen z.B. auch die Mitarbeiter externer Dienstleistungsunternehmen (s. auch Durchführungsbestimmungen zu § 6 des Kirchengesetzes über den Datenschutz) siehe Anl. A "Verpflichtungserklärung z. Datenschutz" + Anl. B "Merkblatt z. Verpflichtungserklärung"

- **Abstimmung**
  Es sollte eine Abstimmung zwischen MAV und Dienststellenleitung bezüglich der Datenschutzbelange erfolgen (z.B. Kopiermöglichkeiten von Daten nicht zulassen, Einführung von Passwörtern gegen Missbrauch, Abschließmöglichkeiten für den PC schaffen, etc.)

- **Datensicherheit**
  Mit der Dienststellenleitung sind Datensicherheitsbestimmungen und die Handhabung derselben festzulegen (Stichworte: Zugangskontrolle, Benutzerkontrolle, Zugriffskontrolle, etc.)

- **Dienstvereinbarungen**
  Zu den o.g. Punkten sind Dienstvereinbarungen auszuhandeln. Musterdienstvereinbarungen sind bei der Geschäftsstelle des Gesamtausschusses abrufbar.

7. Fortbildung

Bei der Ersteinführung von Geräten und Programmen der EDV sowie bei der Erweiterung bestehender Anlagen oder/und Programmen ist eine rechtzeitige und umfassende Einweisung bzw. Einarbeitung der entsprechenden MitarbeiterInnen unbedingt notwendig. **Das MVG sieht in § 39 c auch ein Mitbestimmungsrecht der MAV bei der Aufstellung von Grundsätzen für die Aus- , Fort- und Weiterbildung sowie bei der Teilnehmerauswahl vor.** Aus diesem Paragraphen heraus lässt sich ganz klar der Anspruch ableiten, dass ein entsprechender Passus in eine Dienstvereinbarung aufgenommen werden kann.
Es sollte auch vereinbart werden, dass die Fortbildungsmaßnahmen in der Arbeitszeit stattzufinden haben (Kategorie 1). Geht dies in Ausnahmefällen nicht, ist es trotzdem Arbeitszeit. Die Zeit ist auszugleichen oder zu vergüten (siehe entsprechende Paragraphen im TVöD bzw. in den AVR).

8. Sonstige schutzwürdige Interessen der Mitarbeiter/innen

8.1 Ärztliche Untersuchungen der Augen

Die Untersuchungen sind auch in der schon erwähnten Bildschirmarbeitsverordnung vorgeschrieben, allerdings dort ziemlich unverbindlich formuliert. Genaueres findet sich in der arbeitsmedizinischen Vorsorgeuntersuchungs-Richtlinie BGV A4 der Verwaltungs-Berufsgenossenschaft.
Tipps: Die Untersuchungen sind vor der ersten Arbeitsaufnahme am PC zwingend vorgeschrieben. Sie sind von einem Augenarzt oder Arbeitsmediziner vorzunehmen. Kontrolluntersuchungen sind in einem festen Rhythmus von nicht mehr als drei Jahren durchzuführen. Die Kosten für die Untersuchungen und spezielle Sehhilfen für die Arbeit am PC trägt der Arbeitgeber.

8.2 Schutz vor einer niedrigeren Eingruppierung

Die Umstellung einer Tätigkeit auf EDV soll so vorgenommen werden, dass sie sich auf die bisherige Eingruppierung nicht negativ auswirkt.

8.3 Schutz bei gesundheitlichen Einschränkungen

Kann eine Kollegin / ein Kollege auf Grund einer gesundheitlichen Untersuchung nicht mehr an einem Bildschirmarbeitsplatz oder Arbeitsplatz mit Bildschirmunterstützung beschäftigt werden, sollte geregelt sein, dass sie/er möglichst einen gleichwertigen Arbeitsplatz als Ersatz erhält, um eine Herabgruppierung zu vermeiden. Falls notwendig, sind Fort- und Weiterbildungsmaßnahmen durch den Arbeitgeber anzubieten.

8.4 Arbeitsunterbrechungen

Kolleginnen und Kollegen an einem Bildschirmarbeitsplatz ist nach einer jeweils fünfzigminütigen Tätigkeit am PC Gelegenheit zu einer Arbeitsunterbrechung von zehn Minuten zu geben. Arbeitsunterbrechung heißt nicht Pause, sondern es soll nur etwas anderes getan werden - z.B. kopieren gehen (siehe auch Bildschirmarbeitsverordnung).

8.5 Leistungs- und Verhaltenskontrolle

Eine Leistungs- und Verhaltenskontrolle über EDV sollte generell nicht zugelassen werden. Die Kontrollmöglichkeiten sind schier unbegrenzt und können sehr schnell zu einer unerträglichen Arbeitssituation führen. Die normalen - auch bisher üblichen - Kontrollmöglichkeiten, ob jemand seine Arbeit vernünftig macht, reichen aus. Nur im begründeten Einzelfall sollte davon abgewichen werden, z.B. wenn die Dienststelle die anfallenden Fehlzeiten (Krankheit, Kur, Arbeitsbefreiung) per EDV erfassen will. Eine solche Ausnahme sollte mit Auflagen verbunden sein: Passwort schutz für diese Datei, nur ganz wenige zugangsberechtigte Personen (Dienststellenleitung und 1 bis 2 Verwaltungskräfte), statistische Auswertungen auf einzelne MitarbeiterInnen bezogen, sind der MAV innerhalb kurzer Frist unter Angabe von Gründen mitzuteilen bzw. vorzulegen.

9. Unterstützung / Beratung

Fragen an und Unterstützung durch die Arbeitsgruppe Multimedia über vogt@ga-baden.de

10. Abkürzungen und Fachbegriffe

EDV - elektronische Datenverarbeitung

Firewire - von Apple und Sony (iLink) benutzte Methode um externe Geräte wie Festplatten oder Videogeräte mit dem Rechner zu verbinden (entspricht USB). Firewire gibt es in 2 unterschiedlichen schnellen Versionen (400 und 800).

Hub - als Hub (deutsch) bezeichnet man Verteiler, die den Anschluss von Geräten wie Maus und Tastatur u.ä. erlauben, wenn die in Computern bereits eingebauten USB-Buchsen nicht ausreichen. Hubs benötigen eine zusätzliche Stromversorgung (meist mitgeliefert), wenn die vom Computer zur Verfügung gestellte Stromversorgung nicht ausreicht. Hubs können hintereinander angeschlossen werden.

IP-Telefonie - auch bekannt unter VoIP (engl. Voice over IP), benutzt das Internet als weltweites Telefonnetz

Intranet - ein betriebseigenes Netzwerk

ISDN (engl. Integrated Services Digital Network) - erlaubt den Betrieb von mehreren Telekommunikationsgeräten (Telefon, Anrufbeantworter, Fax, Computer u.ä.) an einem einzigen Telefonanschluss

LAN (engl. Local Area Network) - bezeichnet ein lokales Netzwerk, z.B. ein privates Heimnetzwerk

USB (engl. Universal Serial Bus) - dient dem Anschluss von externen Geräten wie Maus und Tatstatur, Drucker, Scanner, Kameras, Speichergeräten wie Festplatten und Sticks. USB-Verteiler (sog. Hubs) erlauben den Anschluss von zusätzlichen externen Geräten wenn die am Computer bereits verfügbaren USB-Buchsen nicht ausreichen. Es gibt mittlerweile drei Versionen (1.1,2, 3), die mit aufsteigender Versionsnummer höhere Datenflussgeschwindigkeiten erlauben.

WAN (engl. Wide Area Network, dtsch. Weitverkehrnetz) - bezeichnet ein Rechnernetz, das sich im Unterschied zu einem LAN über einen sehr großen geografischen Bereich erstreckt.
Die Anzahl der angeschlossenen Rechner ist auf keine bestimmte Anzahl begrenzt. WANs erstrecken sich über Länder oder sogar Kontinente. WANs werden benutzt, um verschiedene LANs, aber auch einzelne Rechner miteinander zu vernetzen. Einige WANs gehören bestimmten Organisationen und werden ausschließlich von diesen genutzt. Andere WANs werden durchInternetdienstanbieter errichtet oder erweitert, um einen Zugang zum Internet anbieten zu können.

WLAN - (engl. Wireless Local Area Network) ein drahtloses lokales Netzwerk (Computer).

Das **Grossvater-Vater-Sohn-Rotationsprinzip** bei der Datensicherung bedeutet folgende Abfolge: bei der Erstsicherung meiner Daten erstelle ich zunächst mindestens drei Kopien des Gesamtbestandes meiner Festplatte auf drei individuellen Datenträgern. Wenn ich mich für eine tägliche Datensicherung entschieden habe, so wird der Datenbestand des Folgetages auf dem ‘Grossvater’-Datenträger gesichert. Die Sicherungskopie des darauf folgenden Tages wird auf dem ‘Vater’Datenträger gesichert und die des darauf folgenden nächsten Tages auf den ‘Sohn’-Datenträger usw. usf. Analog gilt dies für wöchentliche bzw. 2-wöchentliche Sicherungen. Wir empfehlen allerdings mindestens eine wöchentliche Datensicherung vorzusehen - wenn der zu sichernde Datenbestand nicht sehr gross ist. Wichtig dabei ist, dass jederzeit auf mindestens drei zeitlich aufeinanderfolgende Sicherungskopien zurückgegriffen werden kann.

Verpflichtungserklärung zum Datengeheimnis

(Muster)

Über die Bedeutung des Datengeheimnisses nach den Bestimmungen des Kirchengesetzes über den Datenschutz vom 12. November 1993 (Abl. EKD 1994 S. 505) sowie die dienst- bzw. arbeitsrechtlichen, urheberrechtlichen, strafrechtlichen, disziplinarischen und ggf. haftungsrechtlichen Folgen eines Verstoßes gegen datenschutzrechtliche Bestimmungen wurde ich durch Übergabe eines Merkblatts zur Verpflichtung von Mitarbeitern/innen auf das Datengeheimnis belehrt.

Mir ist bekannt, dass ich geschützte personenbezogene Daten nur zu dem zur rechtmäßigen Aufgabenerfüllung gehörenden Zweck erheben, verarbeiten, bekannt geben, speichern, zugänglich machen oder sonst nutzen darf. Ferner wurde ich darauf hingewiesen, dass ich das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu wahren habe.

Ich verpflichte mich, die kirchlichen Bestimmungen zum Datenschutz und die für alle geltenden Gesetze zum Schutz vor Missbrauch von Daten sorgfältig einzuhalten.

Diese Niederschrift wurde mir vor Unterzeichnung vorgelesen. Eine Abschrift der Verpflichtungserklärung zum Datengeheimnis sowie ein Merkblatt zur Verpflichtung von Mitarbeitern/innen auf das Datengeheimnis wurde mir von dem Verpflichtenden ausgehändigt.

_____	_____
(Unterschrift des/der Verpflichtenden) - Leiter/in der Dienststelle -	(Unterschrift des/der Verpflichteten) - Mitarbeiter/in -

_____
(Ort, Datum)

Merkblatt
zur Verpflichtung von Mitarbeitern/innen auf das Datengeheimnis
(Muster)

Für den Datenschutz in der Evangelischen Landeskirche in Baden sind folgende Rechtsvorschriften zu beachten:

- Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 12. November 1993 (ABl. EKD S. 505) in der jeweils gelten Fassung

- Kirchliches Gesetz zur Ausführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (AusG-DSG-EKD) vom 26. April 1994 (GVBl. S. 107) in der jeweils geltenden Fassung

In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften der Evangelischen Kirche in Deutschland und der Evangelischen Landeskirche in Baden zu beachten.

Für den Schutz personenbezogener Daten gelten insbesondere folgende Grundsätze:

• Personenbezogene Daten dürfen nur für die rechtmäßige Erfüllung kirchlicher Aufgaben erhoben, verarbeitet und genutzt werden. Maßgebend sind die durch das kirchliche Recht bestimmten oder herkömmlichen Aufgaben auf dem Gebiet der Verkündigung, Seelsorge, Diakonie und Unterweisung sowie der kirchengemeindlichen und pfarramtlichen Verwaltung. Einzelheiten sind u.a. den §§ 1 bis 5 und §§ 11 bis 13 DSG-EKD zu entnehmen.
Personenbezogene Daten sind Einzelangaben über persönliche Verhältnisse (z. B. Name, Geburtsdatum, Anschrift, Konfession, Beruf, Familienstand) oder sachliche Verhältnisse (z. B. Grundbesitz, Rechtsbeziehungen zu Dritten) einer bestimmten oder bestimmbaren natürlichen Person (z. B. Gemeindeglieder, kirchliche Mitarbeiter/innen).

• Daten und Datenträger (z. B. Belege, Karteikarten, EDV-Listen, Magnetbänder, Magnetplatten, Disketten) sind stets sicher und verschlossen zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen.

• Daten oder Datenträger dürfen nur kirchlichen MitarbeiternInnen zugänglich gemacht werden, die aufgrund ihrer dienstlichen Aufgaben zum Empfang der Daten ermächtigt und ausdrücklich zur Wahrung des Datengeheimnisses verpflichtet worden sind.

• Auskünfte aus Datensammlungen (Dateien) dürfen nur erteilt und Abschriften oder Ablichtungen von Listen und Karteien sowie Duplizierungen von Disketten, Magnetbändern usw. nur angefertigt werden, wenn ein berechtigtes kirchliches Interesse nachgewiesen ist. Auskünfte zur geschäftlichen oder gewerblichen Verwendung der Daten dürfen in keinem Fall gegeben werden.

• Datenbestände, insbesondere Dateien, Listen und Karteien, die durch neue ersetzt und auch nicht aus besonderen Gründen weiterhin benötigt werden, müssen unverzüglich in einer Weise vernichtet oder gelöscht werden, die jeden Mißbrauch der Daten ausschließt.

• Alle Informationen, die ein/e Mitarbeiter/in aufgrund seiner/ihrer Arbeit an und mit Akten, Dateien, Listen und Karteien erhält, sind von ihm/ihr vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung des Dienstverhältnisses.

• Verstöße gegen das Datengeheimnis sind Verletzungen der Dienstpflicht im Sinne des Disziplinarrechts und der arbeitsrechtlichen Vorschriften und können Schadensersatzansprüche des Dienstherrn oder Dritter begründen.

• Die Vorschriften über die Amtsverschwiegenheit der kirchlichen Mitarbeiter/innen (§ 18 PfDG; Kirchenbeamtengesetz i.V.m. § 79 Landesbeamtengesetz; § 9 BAT) und über sonstige Geheimhaltungspflichten (z. B. Steuergeheimnis) bleiben unberührt.

• Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, werden durch das Strafgesetzbuch mit Strafe bedroht. Auf die Straftatbestände § 202a (Ausspähen von Daten), § 263a (Computerbetrug), § 269 (Fälschung beweiserheblicher Daten), § 270 (Täuschung im Rechtsverkehr bei Datenverarbeitung), § 303a (Datenveränderung), § 303b (Computersabotage) wird besonders hingewiesen. Danach macht sich insbesondere derjenige strafbar, der rechtswidrig Daten verändert oder beseitigt, der den Ablauf der Datenverarbeitung einer Behörde stört, der sich oder einem Dritten unbefugt besonders gesicherte Daten aus fremden Datenbanksystemen verschafft und der fremdes Vermögen durch unbefugtes Einwirken auf einen Datenverarbeitungsvorgang schädigt.

• Nach urheberrechtlichen Bestimmungen (§ 106 UrhG i.V.m. § 69a UrhG) ist weiterhin die Vervielfältigung lizensierter Softwareprodukte und deren Weitergabe an Dritte sowie die Eigennutzung von Raubkopien strafbar. Die zeitlich parallele Mehrfachnutzung eines Originaldatenträgers und/oder davon angefertigter Sicherungskopien sowie die Mehrfachnutzung über ein Netzwerk ist unzulässig, sofern vertraglich nichts anderes vereinbart worden ist. Insbesondere ist der Einsatz privater Programme auf einem dienstlichen Personalcomputer nicht zulässig.

• Mängel beim Datenschutz, der Datensicherung und der ordnungsgemäßen Verarbeitung und Nutzung sind dem jeweiligen Vorgesetzten unverzüglich anzuzeigen.