**Datenschutzkonzept**

**der MAV in XXXXXXXX**

Mit dem Datenschutz werden die Würde und die Persönlichkeit eines Menschen sowie die personenbezogenen Daten des einzelnen Menschen geschützt.

Grundlage des Datenschutzes ist somit das sogenannte Recht auf informationelle Selbstbestimmung, wonach jeder Mensch das Recht hat, selbst über die Preisgabe und Verwendung seiner ihn betreffenden personenbezogenen Daten zu bestimmen.

In der MAV der *(Dienststelle)* wird nach folgendem **Datenschutzkonzept** verfahren:

1. **Zuständig- und Verantwortlichkeiten**

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung trägt die MAV als Gremium Für die Einhaltung der jeweils anzuwendenden Vor­schriften zum Datenschutz und zur Datensicherheit sind alle Mitglieder ver­ant­wortlich.

1. **Überwachung**

Die Überwachung und Prüfung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen erfolgt durch das Gremium in regelmäßigen Abständen.

1. **Fortschreibung**

Das Datenschutzkonzept ist in regelmäßigen Abständen fortzuschreiben.

Dabei ist zu prüfen, ob sich die Datensicherheitsmaßnahmen bewährt haben.

1. **Unterrichtung der Mitglieder**

Die Mitglieder der MAV sind über die bei ihrer Tätigkeit anzuwendenden datenschutzrechtlichen Vorschriften zu unterrichten. Das Datenschutzkonzept ist ihnen auszuhändigen. Der Empfang ist vom Mitglied per Unterschrift zu bestätigen.

1. **Aktenführung und Aktenaufbewahrung/-vernichtung**

Pro Mitarbeiter wird eine Akte geführt. Personenbezogene Daten werden grundsätzlich in dieser Akte abgelegt, sofern sie aufbewahrt werden dürfen.

Akten, in denen sich personenbezogene Daten befinden, sind grundsätzlich in verschlossenen Schränken aufzubewahren, so dass eine Einsichtnahme durch unbefugte Dritte nicht möglich ist. Dies gilt auch für Vorgänge, die in der laufenden Bearbeitung sind (Clear-Desk-Anweisung).

Akten bzw. personenbezogene Daten sind grundsätzlich zu vernichten, wenn sie für die Aufgabenerledigung nicht mehr erforderlich sind und Aufbewahrungsfristen nicht entgegenstehen.

Folgende personenbezogene Unterlagen sollen in den Akten aufbewahrt werden:

* Zustimmungsvorlagen (Einstellungen, Höhergruppierungen, etc.)
* Vorlagen zur Kenntnis (Umsetzungen, Kostenstellenänderungen, etc.)
* Kenntnisnahmen (Kopie von Mitarbeitern an MAV, z.B. Wünsche auf AZ-Erhöhung, Überlastungsanzeigen)
* Beratungsprotokolle, wenn vom Mitarbeiter per Unterschrift bestätigt wurde, dass der Vorgang aufbewahrt werden darf.

Folgende Unterlagen sind unverzüglich zu vernichten:

* Unterlagen von in Rente gegangenen Mitarbeitern
* Bewerbungsunterlagen
* Beratungen zu Arbeitszeiterhöhungen

Besondere personenbezogene Daten (rassische und ethnische Herkunft, politische Meinung, religiöse und weltanschauliche Überzeugungen, Gewerkschafts­zugehörig­keit, Gesundheit oder Sexualleben) werden nur bei einem entsprechenden Anlass und mit Genehmigung des Betroffenen gespeichert

Zu vernichtende Akten und Vorgänge sind einer physikalischen Vernichtung zuzuführen, bei der gewährleistet ist, dass unbefugte Dritte keine Einsicht nehmen können. Geeignete Papier-Schredder sind in jedem Büro vorzuhalten.

Wahlunterlagen sind gemäß Gesetz nach 5 Jahren zu vernichten.

1. **Datenspeicherung in einem ACCESS-Programm**

Folgende Daten werden in einem speziellen Access-Programm gespeichert:

* Name
* Vorname
* Geburtsname
* Straße
* PLZ
* Ort
* Berufsbezeichnung
* Status
* Personalst?
* Einsatzort
* P-N?
* Eintritt
* Beschäftigungsumfang
* unbefr. AZ
* Tagewoche
* Wochenstunden
* Monatsstunden
* Vergütungsgruppe
* EGPL
* von
* bis
* MU/E
* ab
* bis
* Besonders
* Kostenstelle\_I
* Kostenstelle\_II
* FB
* EG\_NEU
* Befristung
* Prozent
1. **Tür- und Fenstersicherung**

Nicht besetzte Büro- und Arbeitsräume sind abzuschließen.

Schlüssel sind abzuziehen und sicher zu verwahren.

Bei längerer Abwesenheit und Dienstende sind alle Fenster zu schließen.

1. **Reinigungspersonal**

Das Reinigungspersonal darf die Räume der MAV nur im Beisein von Mitgliedern der MAV bzw. einer Sekretärin betreten. Es darf keinen Einblick in Akten oder Vorgänge erhalten

1. **Publikumsverkehr**

Es ist sicherzustellen, dass Mitarbeitende bei ihrem Besuch in der MAV andere, als die ihre Angelegenheit betreffende personenbezogene Daten, nicht zur Kenntnis nehmen können.

Bildschirme sind so aufzustellen, dass sie für Dritte nicht einsehbar sind.

1. **Hardware und Software**

Private Hard- und Software darf am Arbeitsplatz nicht eingesetzt werden

Die private Nutzung von dienstlicher Hard- und Software ist grundsätzlich nicht zulässig. Ausnahmen sind in der DV Internet am Arbeitsplatz aufgeführt.

1. **Datenspeicherung**

Dienstliche Daten dürfen nicht auf privaten Rechnern und private Daten nicht auf

dienstlichen Rechnern gespeichert werden

1. **Kennwörter**

Jedes MAV-Mitglied hat ein eigenes Benutzerprofil mit der Personalnummer als Benutzername. Für dieses Profil ist ein Passwort entsprechend den Richtlinien der Johannes-Diakonie zu verwenden.

1. **Arbeitsplatz-PC**

Beim kurzfristigen Verlassen des Arbeitsplatzes ist mit Windows + L der Bildschirmschoner zu aktivieren. Bei längerfristiger Abwesenheit muss sich der Benutzer abmelden bzw. den PC herunterfahren.

1. **Mobile PCs (Notebooks)**

Die Festplatten von Notebooks sind zu verschlüsseln.

1. **Datenträger**

Auf externe Datenträger (USB-Sticks) dürfen nur verschlüsselte Daten gespeichert werden. Nicht mehr benötigte Datenträger sind physikalisch zu zerstören

1. **Auskünfte, Datenübermittlung**

Bei einer Auskunftserteilung bzw. Datenübermittlung ist die Identität der bzw. des

Ersuchenden zu prüfen.

1. **Zentrale Drucker**

Es ist darauf zu achten, dass nicht Ausdrucke auf Druckern außerhalb der MAV erfolgen.

1. **E-Mail**

E-Mail-Eingänge sind wie allgemeine Posteingänge zu behandeln. Alle E-Mails werden nach spätestens einem Jahr gelöscht

Attachments mit ausführbaren Programmen und Dateien (Dateiendungen: z. B. EXE, COM, BAT und VBS) sind sofern diese E-Mails dienstlich nicht angefordert wurden, ohne weitere Überprüfung zu löschen.

1. **Telefaxgeräte**

Telefaxgeräte sind so aufzustellen, dass Unbefugte keine Kenntnis von Inhalten eingehender und übertragener Telefaxe erhalten können. Alle geräteseitigen Sicherungsmaßnahmen (z. B. Anzeige der störungsfreien Übertragung

oder der gesicherten Zwischenspeicherung) sind zu nutzen. Grundsätzlich sind Faxgeräte für den Direktsendebetrieb einzustellen. Sendeprotokolle sind dem Vorgang beizufügen.

1. **Mobiltelefone (Handys)**

Die Sim-Karte des Diensthandys ist mit einer Geheimnummer (PIN) zu versehen.

Der Verlust von Telefon, SIM-Karte oder PIN ist sofort der *Abteilung XY* zu melden. Apps, die nicht den europäischen Datenschutzrichtlinien entsprechen, sind auf Diensthandys nicht erlaubt.

1. **Inkrafttreten**

Das Datenschutzkonzept tritt am in Kraft.

Musterhausen, den xx.xx.2019