In Wahrnehmung der gemeinsamen Verantwortung für den Dienst in der Kirche schließen

der EOK der Evangelischen Landeskirche in Baden, vertreten

durch

die Geschäftsleitung

und

die Mitarbeitendenvertretung der Evangelischen Landeskirche in Baden, im Folgenden „Mitarbeitendenvertretung" genannt,

gemäß §§ 35, 36, 40 Buchstabe b) sowie g) bis k) MVG-Baden folgende

Dienstvereinbarung über den Einsatz, die Nutzung und den Betrieb von Informationstechnologie

(DV IT)

§ 1 Ziel

Der Evangelische Oberkirchenrat und die Mitarbeitendenvertretung legen mit dieser Dienstvereinbarung Rahmenbedingungen für den Einsatz, die Nutzung und den Betrieb von Telekommunikationsanlagen und IT-Systemen mit dem Ziel fest, die Aufgabenerfüllung zu gewährleisten, die Persönlichkeitsrechte sowie den Schutz der personenbezogenen Daten der Mitarbeitenden unter Beachtung aller maßgeblichen Bestimmungen zu sichern und eine soziale Kommunikation bei weitreichender technischer Unterstützung sicherzustellen. Auf der Grundlage gegenseitigen Vertrauens und des geltenden Rechts werden damit Regeln entwickelt, die den Interessen beider Seiten gerecht werden.

§ 2 Geltungsbereich

Diese Dienstvereinbarung gilt für alle Mitarbeitenden des Evangelischen Oberkirchenrats im Sinne von § 2 Mitarbeitervertretungsgesetz.

§ 3 Begriffsbestimmungen

(1) Es gelten die Begriffsbestimmungen nach § 4 DSG-EKD.
(2) Systemfunktionen sind Programme und Programmteile, Auswertungen, Datenfelder, Verarbeitungsanweisungen, Listings u. ä. Systemfunktionen schließen Dateninhalte unbedingt mit ein.
(3) Informations- und Techniksysteme (IT-Systeme) sind komplexe Systeme, die in der Regel aus Hardware, Software, Daten, Netzen, Sprachübertragungssystemen und verschiedenen Prozessen bestehen.
(4) Unter Unified Communications wird die Vereinigung unterschiedlicher Kommunikationswege, speziell (Video-)Telefonie, Austausch von Sofortnachrichten, Desktop- und Dateifreigaben sowie virtuelle Konferenzen verstanden.

(5) Der Büroarbeitsplatz ist ein Arbeitsplatz, an dem Informationen erzeugt, bearbeitet und ausgewertet, empfangen und weitergeleitet werden. In erster Linie sind das Planungs-, Entwicklungs-, Projekt-, Beratungs-, Leitungs-, Verwaltungs- oder Kommunikationstätigkeiten und diese Aufgaben unterstützende Funktionen.

(6) Für Bildschirmarbeitsplätze, Bildschirmgeräte und Telearbeitsplätze gelten die Begriffsbestimmungen gem. § 2 Abs. 5 bis 7 der Arbeitsstättenverordnung – ArbStättV.

(7) Beschäftigte an einem Bildschirmarbeitsplatz sind Mitarbeitende, die gewöhnlich an ihrem Arbeitsplatz für einen Teil ihrer normalen Arbeit ein Bildschirmgerät benutzen.

§ 4 Grundsätze Informations- und Prüfrechte der MAV

(1) Die Beteiligung der Mitarbeitendenvertretung ist in den §§ 33, 34, 38 in Verbindung mit 40 Buchstabe b, g bis k MVG geregelt.

(2) Über den Bestand der in Betrieb befindlichen IT- Systeme kann die Mitarbeitendenvertretung bei der Abteilungsleitung IT Einsicht nehmen und erhält bei Bedarf Auszüge direkt aus den datenführenden Systemen wie Softwareverteilung und Bestandsdatenbank (CMDB) sowie weitere, allgemeinverständliche, Erläuterungen hierzu. Software-Updates und -Upgrades sind insoweit mitzuteilen, als dass diese die Mitbestimmungsrechte der Mitarbeitendenvertretung betreffen.

(3) Dem/Der Vorsitzenden der Mitarbeitendenvertretung oder einer Vertretung ist jederzeitige Prüfung auf Einhaltung der Bestimmungen dieser Dienstvereinbarung zu ermöglichen. Hierbei ist der Weg über die Dienststellenleitung einzuhalten.

§ 5 Datenschutz und IT-Sicherheit, Wartungs- und Reparaturarbeiten

(1) Die jeweils geltenden Bestimmungen zum Datenschutz und zur Datensicherheit sind zu beachten. Insbesondere sind so wenige personenbezogene Daten wie möglich zu erfassen und zu speichern.

(2) Inhaltsdaten von Gesprächen, E-Mails, Internet-Verkehr werden weder erfasst noch gespeichert. Zeitpunkt und Dauer sowie Verkehrsdaten von Gesprächsteilnehmenden werden in einem Anrufprotokoll dargestellt.

(3) Über die zu beachtenden Vorschriften zum Datenschutz und zur Datensicherheit sind die Mitarbeitenden in geeigneter Weise zu informieren und zu verpflichten. Die Dienststellenleitung und die Mitarbeitenden haben die datenschutzrechtlichen Bestimmungen zu beachten. Für jeden Mitarbeitenden werden in regelmäßigen Abständen verpflichtende Schulungen durchgeführt.

(4) Die IT-gestützte Personaldatenverarbeitung findet ausschließlich zu Zwecken der Personalwirtschaft, insbesondere zur Lohn- und Gehaltsabrechnung, Stellenplanverwaltung, Personaldatenverwaltung, Fort- und Weiterbildung, zur Erfüllung von Verpflichtungen aus Gesetzen, Verordnungen, Tarifverträgen, Dienstvereinbarungen, Arbeitsrechtsregelungen und Arbeitsverträgen statt. Die Vertragsparteien tragen hierbei dem Persönlichkeitsschutz der einzelnen Arbeitnehmerin bzw. des einzelnen Arbeitnehmers Rechnung.

(5) Die im Rahmen der Zweckbestimmung dieser Dienstvereinbarung erforderlichen personenbezogenen Daten (Stammdaten und Bewegungsdaten) sind in den jeweiligen Programmbeschreibungen festgelegt und werden dort auch fortgeschrieben.

(6) Die Dienststellenleitung gewährleistet, dass personenbezogene Daten umfassend gegen Missbrauch gesichert werden. Dazu gehört die Erfüllung der in § 5 Absatz 6 des DSG-EKD genannten Anforderungen sowie die innerbetrieblich festgelegten Maßnahmen zur Datensicherheit.

(7) Es ist den Mitarbeitenden der IT-Abteilung nicht erlaubt, personenbezogene und / oder personenbeziehbare Daten oder Dateien aus einem Berechtigungskreis in einen anderen zu übertragen. Dienstliche Anweisungen dieser Art sind nicht erlaubt und deshalb abzulehnen.

(8) Administrations-, Betreuungs-, Wartungs- und Reparaturarbeiten an von der IT-Abteilung der Landeskirche bereitgestellten IT-Systemen, sind ausschließlich durch die IT-Abteilung oder von Personen/Firmen durchzuführen, die durch die IT-Abteilung damit beauftragt sind. Die mit Administrations-, Betreuungs-, Wartungs- und Reparaturarbeiten betrauten Mitarbeitenden der IT-Abteilung oder aber beauftragte externe Personen und Mitarbeitenden externer Firmen sind auf das Fernmeldegeheimnis und die Einhaltung der jeweils geltenden Bestimmungen des Datenschutzes und der Datensicherheit zu verpflichten. Etwaige im Rahmen ihrer Tätigkeit zur Kenntnis gelangte Informationen dürfen nicht verwertet werden und sind vertraulich zu behandeln. Bei beauftragten externen Personen oder Firmen sorgt der Auftraggeber für die Einhaltung der Inhalte dieser Dienstvereinbarung.

(9) Bei notwendiger Nutzung einer Fernwartung durch autorisiertes Personal des Geräteherstellers ist sicherzustellen, dass Unbefugte keinen Zugang zu der Anlage erhalten. Die Zugriffsmöglichkeit für Beschäftigte des Geräteherstellers kann nur über die örtlich zuständigen Mitarbeitenden (Systembetreuer) gesteuert werden. Dabei sind folgende Maßnahmen einzuleiten:
- Der Fernwartungszugang wird besonders geschützt.
- Ein Zugriff auf die Systeme durch Externe ist nur nach fallbezogener Freischaltung durch die IT-Abteilung möglich.
- Die Fernwartung wird automatisch protokolliert.

(10) Die Weitergabe von persönlichen Passwörtern ist nicht gestattet, da die Weitergabe zu IT-Sicherheitstechnischen Problemen führen können. Sofern der IT-Abteilung die Weitergabe von Passwörtern bekannt wird, wird das betroffene Benutzerkonto bis zur vollständigen Klärung gesperrt. Der zuständige örtlich Beauftragte für den Datenschutz sowie die Mitarbeitendenvertretung werden hierüber informiert.

(11) Alle Mitarbeitenden sind verpflichtet die Zwei-Faktor-Authentifizierung, zur Erhöhung der Sicherheit des eigenen Benutzeraccounts, zu verwenden. Sofern den Mitarbeitenden kein dienstliches Endgerät, z.B. Smartphone, zur Verfügung steht, und diese ihr privates mobiles Endgerät nicht nutzen möchten, wird dem Mitarbeitenden ein entsprechender Sicherheitstoken zur Verfügung gestellt.

§ 6 Arbeits- und Gesundheitsschutz, Sehhilfen

(1) Die geltenden Arbeits- und Gesundheitsschutzbestimmungen sind zu beachten und einzuhalten; Insbesondere die Anforderungen und Maßnahmen zur Gestaltung von Bildschirmen, Bildschirmgeräten und Bildschirmarbeitsplätzen gemäß Abschnitt 6 des Anhangs der Arbeitsstättenverordnung.

(2) Bei Bildschirmarbeitsplätzen obliegt die Verpflichtung nach Abs. 1 der Dienstgeberseite.

(3) Spezielle Sehhilfen, das heißt, Sehhilfen, die ohne Tätigkeit am Bildschirmgerät nicht erforderlich wären, werden von der Dienststellenleitung mit bis zu 100 € je Glas und 20 € für das Gestell bezuschusst, wenn die Ergebnisse einer Untersuchung ergeben, dass sie notwendig und normale Sehhilfen nicht geeignet sind.

§ 7 Nutzung, Einverständniserklärung durch Mitarbeitende

(1) Die zur Verfügung gestellten IT-Systeme dienen grundsätzlich der Erledigung dienstlicher Aufgaben.
(2) Die private Nutzung des Internetzugangs sowie der Telefonie ist in einem Umfang zulässig, sodass die dienstliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für dienstliche Zwecke nicht beeinträchtigt werden.
(3) Private E-Mails dürfen grundsätzlich nur über die Nutzung von Webmail-Diensten eines privaten Anbieters versandt und empfangen werden. Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind wie persönliche schriftliche Post gemäß der Dienstordnung des Evangelischen Oberkirchenrats zu behandeln und somit dem Empfänger direkt zuzuleiten.
(4) Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Beschäftigten erklären durch die private Nutzung ihre Einwilligung in die Protokollierung und Kontrolle für den Bereich der privaten Nutzung.

§ 8 Ausstattung Büroarbeitsplatz

(1) Mitarbeitende mit Büroarbeitsplatz erhalten eine Basisausstattung von der jeweiligen Dienststelle, die mindestens beinhaltet:
- ein Notebook inkl. Dockingstation mit aktuellem Betriebssystem und Officeprodukten. An einzelnen Arbeitsplätzen kann auch ein festinstallierter PC zum Einsatz kommen.
- eine Bildschirmausstattung nach den aktuellen technischen Standards, die die aktuellen Vorgaben des Arbeitsschutzes erfüllt.

§ 9 E-Mail, Filterung, Protokollierung, Auswertung, Löschung und Zugriffsberechtigungen von Daten

(1) Die elektronischen Kommunikationssysteme für E-Mail stehen den Mitarbeitenden als Arbeitsmittel im Rahmen der Aufgabenerfüllung am PC-Arbeitsplatz zur Verfügung.
(2) Die Anlage und Abschaltung von E-Mailadressen erfolgt durch Meldung der Personalverwaltung an die IT-Abteilung. Die Abschaltung erfolgt mit dem Tag des Ausscheidens und kann auf Antrag maximal 4 Wochen verzögert werden.
(3) Das Empfangen und Versenden von dienstlichen E-Mails mit privaten mobilen Endgeräten ist grundsätzlich möglich. Details sind in den Durchführungsbestimmungen zur Datensicherheit mobiler und lokaler Endgeräte geregelt. Diese sind zu beachten.
(4) Um den Datenschutz zu gewährleisten, dürfen Nachrichten, die personenbezogene Daten enthalten, per E-Mail nur über verschlüsselte Strecken oder Verbindungen verschickt werden.
(5) Alle eingehenden E-Mails werden durch eine Firewall, einen Spam-Filter sowie Virenscanner geprüft. Einzelheiten der Filterung sind unter folgender Adresse einsehbar: www.ekiba.de/it
(6) Protokolle, die durch Maßnahmen nach Abs. 5 entstehen, werden nach den zeitlichen Vorgaben der Softwarehersteller automatisch gelöscht. Löschfristen, die im Einflussbereich der IT-Abteilung liegen, werden mit 30 Tagen festgesetzt. Sollte ein aktueller Verdacht auf Missbrauch bestehen, kann die Löschung nach vorheriger Zustimmung der Mitarbeitendenvertretung durch die Dienststellenleitung ausgesetzt werden.
(7) Eine Einsichtnahme in die systemseitigen automatischen Protokolle ist nur durch Anordnung der Dienststellenleitung und nach vorheriger Zustimmung der Mitarbeitervertretung gemäß § 40 Buchstabe j MVG zulässig.
(8) Daten, die aus der Nutzung entstehen, werden nicht zur Verhaltens- und Leistungskontrolle der Mitarbeitenden eingesetzt.

(9) Auswertungen von personenbezogenen Daten zum Zwecke der Leistungs- und /oder Verhaltenskontrolle der Mitarbeitenden finden grundsätzlich nicht statt. Auswertungen von personenbezogenen Daten zum Zwecke der Leistungs- und /oder Verhaltenskontrolle der Mitarbeitenden sind nur in begründeten Einzelfällen, wie z.B. Verdacht auf strafrechtlich relevantes Verhalten, und nach vorheriger Abstimmung mit der MAV zulässig. Die betroffenen Mitarbeitenden sind vor der Einführung einer solchen Maßnahme hierüber zu informieren. Bei begründetem Verdacht des Missbrauchs können die jeweiligen vorgesetzten Personen gemeinsam mit der Mitarbeitendenvertretung eine Auswertung von personenbezogenen Daten vornehmen. Personelle Maßnahmen, die auf Informationen (auch zufällig) beruhen, die unter Verletzung dieser Dienstvereinbarung gewonnen wurden, sind unwirksam und rückgängig zu machen. Ein Verstoß gegen diese Bestimmungen kann arbeitsrechtliche oder dienstrechtliche Konsequenzen zur Folge haben.

(10) Ausgenommen von Absatz 9 sind Maßnahmen auf Grund eines strafrechtlich relevanten Verhaltens. Die Mitarbeitendenvertretung ist im Vorfeld oder in unmittelbarer zeitlicher Nähe der Durchführung zu informieren.

(11) Jede Auswertung ist mit folgenden Daten zu protokollieren:

- Anfordernde Stelle
- Name der Auswertung
- Zweck der Auswertung
- Daten, die in die Auswertung eingehen
- Form der Auswertung (Listenbild usw.)
- Zeitpunkt der Auswertung

(12) Datenzugriffe und Datenübermittlungen in vorgangs- und dokumentenführenden Systemen sind automatisch zu protokollieren.

(13) Der Datenzugriff ist über Zugriffsberechtigungskonzepte festzulegen. Die fachliche und technische Systemadministration ist zur Wahrung des Vier-Augen-Prinzips grundsätzlich zu trennen. Die Systemadministratoren sind namentlich zu benennen.

(14) Protokolle, welche durch die Automatisierung der Auswertung durch Systemdienste generiert werden und im Falle von gravierenden Verstößen gegen die IT-Sicherheit Alarme oder Meldungen an die IT-Abteilung übermitteln, unterliegen einer umfassenden Überprüfung seitens der IT-Abteilung. Sollte es sich ergeben, dass einzelne Mitarbeitende unmittelbar betroffen sind, wird in Abhängigkeit von dem Grad der Kritikalität eine temporäre Sperrung des betroffenen Accounts vorgenommen. Dies geschieht unter Berücksichtigung und Einbeziehung der Mitarbeitendenvertretung, um darauf basierend weitere notwendige Maßnahmen zu erörtern und festzulegen.

§ 10 Telefon, elektronisches Telefonbuch, Protokollierung, Auswertung und Löschung und Zugriffsberechtigung von Verbindungsdaten

(1) Aufgrund der Nutzung unterschiedlicher technischer Lösungen in den verschiedenen Dienststellen kann keine einheitliche, zentrale Regelung getroffen werden.

(2) Die Festlegung von Regelungen erfolgt individuell im Einvernehmen zwischen der Mitarbeitendenvertretung (MAV) und der jeweils zuständigen Dienststelle.

§ 11 Internet

(1) Die Nutzung des Internets erfordert ein besonders hohes Maß an Sicherheit. Dies ist in der Sicherheitsvereinbarung für die Nutzung des Internets (Anlage 2) zu dieser Dienstvereinbarung geregelt.

§ 12 Unified Communications

(1) Eine Unified Communications-Anwendung dient der Kommunikation und Zusammenarbeit in Echtzeit zwischen den Mitarbeitenden oder mit anderen Personen, die räumlich voneinander getrennt sind.
(2) Die Nutzung des vollen Funktionsumfangs dieser Systeme ist freiwillig.
(3) Die Nutzung folgender Funktionen wird mit dieser Dienstvereinbarung vereinbart:
   - Präsenzstatus
   - Standortanzeige
   - Instant Messaging (Chat)
   - Telefonie und Videotelefonie
   - Videokonferenz
(4) Für die Verwendung des Präsenzstatus wird folgendes festgelegt:
   a. Je nach eingesetzter Anwendung können alle Anwenderinnen und Anwender den Präsenzstatus gegenseitig einsehen oder die Freigabe des Präsenzstatus individuell steuern. Wenn die Freigabe nicht individuell gesteuert werden kann, gibt es die Möglichkeit einzelne Kontakte zu blockieren.
   b. Die Anwenderinnen und Anwender können selbst in eigener Verantwortung ihren Präsenzstatus setzen oder deaktivieren („Als offline anzeigen"), ohne dass daraus negative Schlüsse für sie gezogen werden. Sie können sich insbesondere jederzeit auf „abwesend" oder „nicht stören" setzen, wenn die Anwenderinnen und Anwender das für sinnvoll halten.
(5) Alle Führungskräfte wurden darauf hingewiesen, dass der Präsenzstatus der Mitarbeitenden, sofern dieser verwendet wird, nicht zur Leistungs- und Verhaltenskontrolle verwendet werden darf.

§ 13 Vertretungsregelung

(1) Bei geplanter Abwesenheit ist die Abwesenheitsbenachrichtigung (Autoresponder) für die Dauer der Abwesenheit zu aktivieren und sicherzustellen, dass alle betriebsrelevanten digitalen Unterlagen im DMS oder gemeinsam zugänglichen Datenspeichern abgelegt sind.
(2) Bei ungeplanter Abwesenheit wird die Abwesenheitsbenachrichtigung der bzw. des abwesenden Mitarbeitenden durch den IT-Support auf Anweisung der bzw. des Vorgesetzten aktiviert. Die gewünschte Abwesenheitsbenachrichtigung ist in diesem Zuge zu übermitteln.
(3) Um während geplanter und ungeplanter Abwesenheit einen Zugriff auf den Posteingang zu gewährleisten, muss dauerhaft eine Vertretung berechtigt werden. Dies gilt auch für etwaige Anrufweiterleitungen.
(4) Ein Zugriff auf den Maileingang einer bzw. eines abwesenden Mitarbeitenden kann, sofern diese nicht durch die bzw. den Mitarbeitenden im Mailsystem zuvor freigegeben wurde, nur durch die Referatsleitung für die zuständige Vertretung veranlasst werden. Der abwesende Mitarbeitende ist unmittelbar nach der Rückkehr hierüber zu informieren.
(5) Für die Mitglieder der Mitarbeitendenvertretung und der Jugend- und Auszubildendenvertretung sowie der Schwerbehindertenvertretung und beauftragten Personen (wie z. B. Datenschutz, Mobbing, sexuelle Diskriminierung, Gleichstellung) werden die E-Mails auf Wunsch mit dem Kennzeichen „vertraulich" versandt, so dass die Einsichtnahme durch die Vertretung technisch unterbunden ist.

§ 14 Qualifizierung der Mitarbeitenden

(1) Die Mitarbeitenden erhalten in angemessenem Umfang Schulung und Ausbildung, die sie auf eine sachgerechte und effiziente Nutzung der Hard- und Software vorbereitet. Die Schulung soll sie fortlaufend in die Lage versetzen, die IT-Systeme optimal zu nutzen.

(2) Neben der Schulung für die Anwendersoftware sind die Mitarbeitenden insbesondere im Umgang mit digitalen Prozessen regelmäßig zu unterweisen. Hierbei sollten insbesondere folgende Kenntnisse vermittelt werden:

   a. Inhalte der „Sicherheitsvereinbarung für die Nutzung des Internets“ (Anlage 2)
   b. Anwendung der Datenschutzvorschriften
   c. Protokollierte Benutzerdaten
   d. Dienstliche (arbeitsrechtliche), gesetzliche und ethische Grundsätze und Vorschriften bei der Nutzung von Externen Diensten (z. B. „Nettikette“).

   Diese Informationen erfolgen in Kooperation mit dem IT-Sicherheits- und Datenschutzbeauftragten sowie der Abteilung „Digitalisierung, Organisation und Projekte“.

(3) IT-Koordinatoren*innen werden für ihre Aufgabenwahrnehmung im notwendigen Umfange vorbereitet und nötigenfalls intern bzw. extern zusätzlich geschult. Dies gilt insbesondere bei größeren Maßnahmen oder Umstellungen der von IT-Systemen.

§ 15 Betreuung und Support, Wartung

(1) Hard- und Software, welche durch die IT-Abteilung bereitgestellt und dem festgelegten Standard des EOK entspricht, werden durch die IT-Abteilung betreut. Eine Installation von Software auf diesen IT-Systemen, welche von Standard abweichen, sind nicht zulässig.

(2) In den einzelnen Bereichen der Landeskirche werden IT-Koordinator*innen bestellt, die die Verbindungsstellen zur IT-Abteilung bilden. Sie sind die ersten Ansprechpersonen der Mitarbeitenden bei auftretenden Problemen und Fragestellungen zu den IT-Systemen.
Den Mitarbeitenden stehen IT-Koordinator*innen in den Bereichen für die Beantwortung von Fragen zu den IT- Systemen zur Verfügung. Eine Übersicht der IT-Koordinator*innen kann im Kundenportal der IT-Abteilung eingesehen werden.

(3) Die Mitarbeitenden können sich bei IT-Problemen zudem telefonisch oder per E-Mail an die, in der IT-Abteilung angesiedelte Hotline, (IT-Hotline) wenden. Entsprechendes gilt für Anfragen zu den IT-Systemen.

(4) Geplante Wartungstermine an Systemen werden i.d.R. im Vorjahr im Intranet veröffentlich. Dringende Wartungstermine können auch mit kurzfristiger Ankündigung durchgeführt werden.

(5) Der in der IT-Abteilung eingerichtete IT-Support für die IT-Systeme hat die Möglichkeit sich per Fernwartung auf die Endgeräte der Mitarbeitenden zuzugreifen. Hierfür ist bei jedem Zugriff eine Bestätigung der Fernwartung durch den Benutzer*in betroffenen Mitarbeitenden erforderlich.

(6) Durch die IT-Abteilung werden im Kundenportal der IT-Abteilung für die vorhandenen Endgeräte, Hard- und Software aktuelle Handbücher bzw. FAQ zur Verfügung gestellt.

§ 16 Einführung neuer IT-Systeme

(1) Werden neue IT-Systeme, Funktionen, Programme bzw. Systemausweitungen in den Bereichen der Informations- und Telekommunikationsmedien eingeführt und dadurch gegebenenfalls die Arbeitsplatzanforderungen der Mitarbeitenden geändert, werden die Mitarbeitendenvertretung sowie die beauftragten Person*en für den Datenschutz und die IT-Sicherheit bereits während der Vorbereitung von Entscheidungen informiert und frühzeitig an den Planungen beteiligt, so dass ihre Eingaben bei der Planung berücksichtigt werden können, sofern dies im Einflussbereich des Evangelischen Oberkirchenrats liegt.

(2) Die von informationstechnisch begründeten Umstrukturierungsmaßnahmen betroffenen Mitarbeitenden werden über die beabsichtigten Maßnahmen im Rahmen der geltenden Grundsätze für die Projektarbeit in der Evangelischen Landeskirche in Baden rechtzeitig und umfassend durch die Dienststellenleitung informiert.

(3) Bei der Erneuerung von IT-Systemen, die Einflüsse auf die Arbeitsorganisation haben, ist darauf zu achten, dass das Arbeitsfeld der einzelnen Mitarbeitenden ein breites Spektrum unterschiedlicher Tätigkeiten enthalten soll, damit durch geeignete Belastungs- und Beanspruchungswechsel eine dauerhafte Unter- und Überforderung verhindert wird.

(4) Mitarbeitende, die infolge der Einführung der Systeme bzw. deren Änderung/Erweiterung in ihrer bisherigen Tätigkeit nicht weiterbeschäftigt werden können, werden im Rahmen der betrieblichen Möglichkeiten zumutbare andere Tätigkeiten angeboten. Dabei ist die Möglichkeit einer weiteren Qualifizierung zu prüfen und ggf. zu veranlassen, um die zusätzlich benötigten Kenntnisse oder Fertigkeiten zu erlangen. Im Rahmen der bestehenden Regelungen über die Fort- und Weiterbildung sind auch Vereinbarungen von angemessener zeitlicher Bindung der Mitarbeiterin bzw. des Mitarbeiters möglich.

(5) Das Mitbestimmungsverfahren gilt bei Einführung neuer bzw. Erweiterung bestehender IT-Systeme, die Einfluss auf die Arbeitsorganisation haben.

(6) Sofern im Vorfeld bei der Einführung von IT-Systemen Pilotphasen stattfinden ist die Mitarbeitendenvertretung rechtzeitig zu informieren. An Pilotphasen können maximal sechs Arbeitsbereiche teilnehmen. Wenn weitere Arbeitsbereiche Interesse an der Pilotphase aufzeigen, gilt hierbei das Mitbestimmungsverfahren. Eine Pilotphase darf maximal ein halbes Jahr andauern unter Absprache mit der Mitarbeitendenvertretung kann diese bis zu einem Jahr verlängert werden. Während der Pilotphase verpflichtet sich die Mitarbeitendenvertretung aktiv bei den, zu Beginn der Pilotphase benannten Ansprechpersonen den Arbeitsbereichen nach Erfahrungswerten nachzufragen und diese zu evaluieren. Im Anschluss der Pilotphase werden die Erfahrungswerte mit der IT evaluiert und erörtert und das weitere Vorgehen abgesprochen.

§ 17 Einführung neuer Funktionen in Clouddiensten (Microsoft 365)

(1) Der Evangelische Oberkirchenrat und die Mitarbeitendenvertretung erkennen an, dass Microsoft 365 kontinuierlich weiterentwickelt wird und neue Funktionen in der Cloud hinzugefügt werden können.

(2) Um den Mitarbeitenden die Nutzung neuer Funktionen in Microsoft 365 zu ermöglichen und eine zeitnahe Anpassung an neue Arbeitsweisen zu gewährleisten, bedarf es keiner gesonderten Genehmigung durch die Mitarbeitendenvertretung.

(3) Die Dienststellenleitung informiert die Mitarbeitendenvertretung im Rahmen der regelmäßigen Termine über größere Funktionsaktualisierungen und die möglichen Auswirkungen auf die Arbeitsabläufe und Datenschutzaspekte.

(4) Sollten neue Funktionen in Microsoft 365 zu erheblichen Veränderungen in den Arbeitsabläufen führen oder datenschutzrechtliche Bedenken aufwerfen, ist die Mitarbeitendenvertretung zu informieren und berechtigt eine detaillierte Information einzufordern und mit der Dienststellenleitung über mögliche Anpassungen zu beraten.

(5) Die Mitarbeitendenvertretung ist befugt, bei Bedarf Schulungen oder Informationsveranstaltungen für die Mitarbeitenden zu neuen Funktionen in Microsoft 365 einzufordern, um eine angemessene Nutzung sicherzustellen.

(6) Sollte es aus berechtigten Gründen aus Sicht der Mitarbeitendenvertretung oder der IT notwendig sein, den Zugriff auf bestimmte Funktionen in Microsoft 365 einzuschränken oder zu deaktivieren, erfolgt dies in Absprache mit beiden Parteien und unter Berücksichtigung datenschutzrechtlicher Aspekte. Bei Meinungsverschiedenheiten kann eine externe Expertise zur neutralen Klärung hinzugezogen werden.

(7) Die Mitarbeitenden sind verpflichtet, die neuen Funktionen in Microsoft 365 im Rahmen ihrer dienstlichen Aufgaben und unter Einhaltung der geltenden Datenschutzbestimmungen zu nutzen.

(8) Die Dienststellenleitung und die Mitarbeitendenvertretung fördern eine offene Kommunikation und den regelmäßigen Austausch über die Nutzung neuer Funktionen in Microsoft 365, um mögliche Herausforderungen frühzeitig zu erkennen und gemeinsam zu bewältigen.

§ 18 Einsatz und Umgang mit künstlicher Intelligenz (KI)

(1) Der Evangelische Oberkirchenrat und die Mitarbeitendenvertretung erkennen die Chancen und Potenziale des Einsatzes von künstlicher Intelligenz (KI) an, um die Arbeitsabläufe zu optimieren und die Aufgabenerfüllung zu verbessern. Dabei steht der Grundsatz der Letztentscheidungsbefugnis des Menschen im Umgang mit KI im Vordergrund.

(2) Bei der Nutzung von KI-Technologien ist das Transparenzgebot zu beachten. Die Mitarbeitenden haben das Recht, nachvollziehbare Informationen über die Funktionsweise und die Auswirkungen von KI-Entscheidungen zu erhalten, soweit dies technisch und rechtlich möglich ist.

(3) Die Verwendung von KI-Systemen darf nicht zu diskriminierenden oder ungerechten Handlungen führen. Die Dienststellenleitung stellt sicher, dass bei der Entwicklung und Implementierung von KI-Algorithmen Maßnahmen ergriffen werden, um Diskriminierung bestmöglich zu verhindern.

(4) Die Nutzung von KI zur Leistungs- und Verhaltenskontrolle der Mitarbeitenden ist grundsätzlich nicht zulässig, Ausnahmen hiervon sind in §9 Abs. 9 abschließend geregelt. Die Persönlichkeitsrechte und der Schutz der Privatsphäre der Mitarbeitenden werden umfassend gewahrt.

(5) Bei der Einführung und Nutzung von KI-Systemen gilt das Mitbestimmungsverfahren gemäß §40 MVG Buchstabe g bis j. Des Weiteren ist bei KI-Systemen darauf zu achten, dass diese nachhaltig und fair gestaltet sind. KI-Systeme dürfen nur für legitime Zwecke eingeführt werden, z.B. für die IT-Sicherheit, Schadensverhütung oder aber für die Entlastung von Mitarbeitenden. KI-Systeme dürfen nicht zu einer Erhöhung des Arbeitsdrucks oder aber zur Entlassung von Mitarbeitenden führen.

(6) Die Dienststellenleitung verpflichtet sich, die Mitarbeitendenvertretung im Rahmen der regelmäßigen Termine über den Einsatz von KI-Technologien zu informieren und diese aktiv in die Entscheidungsfindung einzubeziehen.

(7) Die Mitarbeitenden werden über die Einführung neuer KI-Systeme und die damit verbundenen Auswirkungen auf ihre Arbeitsabläufe frühzeitig und umfassend informiert.

§ 19 In- Kraft-Treten, Anpassung, Kündigung

(1) Diese Dienstvereinbarung tritt am 1. Februar 2025 in Kraft.

(2) Eine Überprüfung und bei Bedarf eine Anpassung ist gemeinsam zwischen der Dienststellenleitung und Mitarbeitendenvertretung vorzunehmen.

(3) Die Dienstvereinbarung kann mit einer Frist von drei Monaten zum Quartalsende schriftlich gekündigt werden. Im Falle einer Kündigung verpflichten sich die Dienststellenleitung und die Mitarbeitervertretung, unverzüglich über den Abschluss einer neuen Dienstvereinbarung zu verhandeln. Die Dienstvereinbarung ist bis zum In-Kraft-Treten einer neuen Vereinbarung weiter anzuwenden, soweit dies rechtskonform möglich ist.

Karlsruhe, den 31. Januar 2025

Für den Evangelischen Oberkirchenrat:

Kai Tröger-Methling
Geschäftsleitung

Für die Mitarbeitendenvertretung:

Laura Škarnulytė
Vorsitzende

Tillmann Häfner
Vorsitzender