Erzdiözese Freiburg

mav

Rahmen-Dienstvereinbarung IT-Einsatz und kirchlicher Datenschutz

Rahmendienstvereinbarung IT-Einsatz und kirchlicher Datenschutz

Dienstvereinbarung IT-Einsatz und Datenschutz 2
Präambel 2
§ 1 Räumlicher Geltungsbereich 2
§ 2 Gegenstand 3
§ 3 Drittwirkung 3
§ 4 Begriffsbestimmung und Anlagen 3
§ 5 Beschäftigungssicherung 4
§ 6 Arbeitsgruppe der MAVen 4
§ 7 Hardware und Anwendungen 4
§ 8 Ergonomie und Arbeitsschutz 5
§ 9 Zulässige Funktionen 5
§ 10 Verarbeitung personenbezogener Daten 5
§ 11 Auswertung personenbezogener Daten 6
§ 12 Nebendatenverarbeitung 7
a) Zulässige Nebendatenverarbeitung 8
b) Delegation der Berechtigung zur Nebendatenverarbeitung an Assistenzen 8
c) Vorläufige Zustimmung 9
§ 13 Berechtigungskonzept/-rollen 9
§ 14 Schnittstellen 9
§ 15 Datenschutz 10
§ 16 Datenschutzbeauftragter 10
§ 17 Datensicherheit 10
§ 18 Auftragsverarbeitung 11
§ 19 Qualifizierung 11
§ 20 Leistungs- und Verhaltenskontrolle 11
§ 21 Rechte der Mitarbeitenden 11
§ 22 Verdacht von Straftaten oder schwerwiegenden Vertrags- und Dienstpflichtverletzungen 12
§ 23 Beweisverwertungsverbot 14
§ 24 Rechte der MAV 14
§ 25 Konfliktklausel 15
§ 26 Schlussbestimmung 15
§ 27 Inkrafttreten 15
§ 28 Kündigungsfrist und Nachwirkung 16
§ 29 Salvatorische Klausel 16
Anlage 1: Begriffsbestimmungen 17
Anlage 2: Unterrichtung der MAV gemäß MAVO 18
Anlage 3: Einzeldienstvereinbarungen 19
Anlage 4: Besondere Zugriffsberechtigungen 21
Anlage 5: Muster der Verpflichtungserklärung 22
Merkblatt Datenschutz 24
Fachbegriffe und Abkürzungen 26

Rahmendienstvereinbarung IT-Einsatz und kirchlicher Datenschutz

gem. § 38 Abs. 1 Ziff. 11 MAVO

zwischen

der Röm. Kath. Kirchengemeinde
Sigmaringen K.d.ö.R.
vertreten durch den Verwaltungsvorstand,
Herrn Pfarrer Stefan Schmid und
Herrn Pfarreiökonom Andreas Rösch

und

der Mitarbeitervertretung der Röm. Kath.
Kirchengemeinde Sigmaringen K.d.ö.R. vertreten durch
den Vorsitzenden, Herrn Joachim Stopper

Präambel

Dienstgeber und MAV sind sich einig, dass elektronische Datenverarbeitungs- und Kommunikationssysteme für die Erfüllung der anfallenden dienstlichen Aufgaben, zur Sicherstellung der ordnungsgemäßen internen und externen Rechnungslegung, für die Einhaltung der Wirtschaftlichkeit sowie der gesetzlichen Vorschriften unerlässlich sind. Diese dienen sowohl einer effizienten als auch transparenten einheitlichen Aufgabenerfüllung. Dienstgeber und MAV sind sich weiter darüber einig, dass beim Einsatz solcher Systeme Persönlichkeitsrechte der Mitarbeiter betroffen sein können.

Ziel dieser Dienstvereinbarung ist es, die Persönlichkeitsrechte der Mitarbeitenden unter Beachtung aller jeweils maßgeblichen gesetzlichen Bestimmungen zu sichern und dennoch den Einsatz technischer Einrichtungen zu ermöglichen.

Dienstgeber und MAV möchten daher Rahmenbedingungen zum Datenschutz beim Einsatz von Datenverarbeitungs-, IT- und TK-Systemen sowie Kommunikations- und Kollaborationslösungen festlegen.

Bestehende Dienstvereinbarungen im Anwendungsbereich der elektronischen Datenverarbeitungs- und Kommunikationssysteme werden in diese Rahmendienstvereinbarung integriert. Neue Dienstvereinbarungen sollen, wenn möglich, als spezifische Dienstvereinbarungen Besonderheiten regeln und als integraler Bestandteil zu dieser Rahmendienstvereinbarung genommen werden.

Das vorausgeschickt vereinbaren die Parteien was folgt:

§ 1 Räumlicher Geltungsbereich

Diese Dienstvereinbarung gilt räumlich für alle Mitarbeitenden der Röm. Kath. Kirchengemeinde Sigmaringen K.d.ö.R. im Zuständigkeitsbereich der Mitarbeitervertretung (MAV) gem. § 3 (1) MAVO.

§ 2 Gegenstand

a) ist die Sicherstellung und Präzisierung der Rechte der Mitarbeitenden und der MAV in Bezug auf die Nutzung der Informationstechnik in der Einrichtung.

b) sind Planung, Einführung und Anwendung von mitbestimmungspflichtigen Verfahren und Systemen der Informationstechnik. Diese Rahmen-DV gilt für bereits bestehende und im Einsatz befindliche IT-Systeme und deren Änderung ebenso wie für die Einführung neuer Anwendungssysteme. Bestehende Dienstvereinbarungen und sonstige verbindliche Regelungen (Bestandsregelungen) bleiben grundsätzlich in Kraft. Soweit im Einzelfall Widersprüche zwischen Bestandsregelungen und dieser Dienstvereinbarung bestehen, gehen die Regelungen dieser Dienstvereinbarung im Anwendungsbereich vor, es sei denn, dass die Bestandsregelungen günstiger sind für die Beschäftigten. Soweit Bestandsregelungen hinter diese Rahmendienstvereinbarung zurückfallen, gelten die strengeren Bestimmungen dieser Dienstvereinbarung.

c) ist die Verarbeitung personenbezogener Daten von Mitarbeitenden des Dienstgebers durch den Einsatz von Anwendungssystemen der elektronischen Datenverarbeitung i.S.d. § 36 Abs. 1 Nr. 9 MAVO, die dazu geeignet sind, das Verhalten oder die Leistung von Mitarbeitenden zu überwachen, unabhängig davon, in welchen Systemen, Programmen oder Applikationen diese Daten gespeichert sind.

§ 3 Drittwirkung

Die Regelungen dieser Dienstvereinbarung gelten entsprechend für alle im Sinne von § 36 Abs.1 Nr. 9 MAVO mitbestimmungspflichtigen Verträge mit betriebsfremden Personen, Stellen und Firmen, die direkten oder indirekten Zugriff auf die IT-Systeme haben oder im Rahmen von Auftragsverarbeitung für die Einrichtung tätig sind.

Daher stellt der Dienstgeber durch entsprechende Gestaltung von Werk-, Dienst- und Dienstleistungsverträgen mit Dritten sicher, dass die Einhaltung dieser Dienstvereinbarung und der Einzeldienstvereinbarungen gemäß § 7 und die ordnungsgemäße Wahrnehmung der Mitbestimmungsrechte der MAV gewährleistet sind.

§ 4 Begriffsbestimmung und Anlagen

Es gelten die Begriffsbestimmungen sowie die in Anlage 1 definierten Begriffe.

Folgende Anlagen und ihre Fortschreibungen sind Bestandteile dieser Dienstvereinbarungen:

Anlage 1:	Begriffsbestimmungen
Anlage 2:	Formblatt Unterrichtung der MAV
Anlage 3:	Einzeldienstvereinbarungen
Anlage 4:	Besondere Zugriffsberechtigungen
Anlage 5:	Muster der Vertraulichkeitsverpflichtung

Für einvernehmliche Änderungen und Fortschreibungen der Anlagen ist eine Kündigung der Dienstvereinbarung nicht notwendig. Gleiches gilt für die Anhänge der Einzeldienstvereinbarungen. Änderungen der Einzeldienstvereinbarungen (Anlage 3) unterliegen den Vorschriften des § 38 MAVO.

§ 5 Beschäftigungssicherung

Die Vertragspartner stimmen darin überein, dass die Einführung informationstechnischer Systeme vorrangig der Optimierung der Arbeitsprozesse dient, hiermit jedoch in der Regel kein Arbeitsplatzabbau verbunden ist. Falls ein Arbeitsplatzabbau im Zusammenhang mit der Einführung geplant ist, wird die MAV darüber informiert. Weitergehende Beteiligungsrechte der MAV bleiben unberührt.

§ 6 Arbeitsgruppe der MAVen

Die MAV kann eine AG IT beauftragen, in der die aktuelle Projektgruppe MAV Einführung SAP aufgeht.

Die Arbeitsgruppe IT erarbeitet für die MAVen Vorschläge für Regelungen im Kontext von Entwürfen von Musterdienstvereinbarungen bei der Einführung neuer zentraler Systeme oder deren Änderungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Mitarbeitenden zu überwachen.
Sie informiert MAVen, die sie beauftragen, über ihre Arbeit und steht mit den MAVen, die dies wünschen, in einem Austausch bezüglich ihres jeweiligen Arbeitsprozesses und Arbeitsergebnisses.

Die Beteiligungsrechte der einzelnen MAVen werden durch die Arbeit der AG IT nicht berührt. Die einzelnen MAVen entscheiden nach § 36 (1) 9 MAVO, ob sie den von der AG IT erarbeiteten Ergebnissen zustimmen.

Zusammensetzung und Arbeitsweise der AG IT der MAVen werden in einer Regelungsabrede außerhalb dieser Dienstvereinbarung geregelt.

§ 7 Hardware und Anwendungen

Die MAV erhält Zugriff auf eine ggf. in der Einrichtung eingesetzte Soft- und Hardware-Inventarisierungssoftware. Hierzu werden für die MAV alle notwendigen Abfragen und Reports ermöglicht, die Aufschluss über die an den Arbeitsplätzen eingesetzte Hardware und über die in der Einrichtung eingesetzten Anwendungen geben.

Ist keine Soft- und Hardware-Inventarisierungssoftware im Einsatz, oder werden Informationen über einzelne Anwendungen nicht von der Inventarisierungssoftware erfasst, sind der MAV auf Anforderung die notwendigen Angaben in elektronischer Listenform (z.B. Excel-Liste) zur Verfügung zu stellen.

Alle zum Einsatz kommenden mitbestimmungspflichtigen technischen Einrichtungen und Anwendungen, mit denen personenbezogene Daten der Mitarbeitenden erhoben, verarbeitet und/oder ausgewertet werden können, bedürfen einer Einzeldienstvereinbarung gemäß Anlage 3. Abweichende Regelungen in Einzeldienstvereinbarungen gehen den Regelungen dieser Vereinbarung vor, soweit sie günstiger sind für die Beschäftigten. Die Einzeldienstvereinbarungen sind unabhängig von der vorliegenden Dienstvereinbarung unter Beachtung der gesetzlichen Vorschriften der MAVO einzeln kündbar.

§ 8 Ergonomie und Arbeitsschutz

Der Dienstgeber verpflichtet sich, bei Betrieb und Neueinrichtung von Bildschirmarbeitsplätzen die Vorschriften des Arbeitsschutzgesetzes, der Arbeitsstättenverordnung, die berufsgenossenschaftlichen Vorschriften sowie die Handreichungen des Bundesamtes für Arbeitsmedizin und Arbeitsschutz umzusetzen. Hierbei sind die gesicherten arbeitswissenschaftlichen Erkenntnisse zu berücksichtigen. Insbesondere sind sowohl bei Bildschirmarbeitsplätzen als auch bei sonstigen zum Einsatz kommenden elektronischen Arbeitsmitteln Gefährdungsbeurteilungen gemäß § 5 ArbSchG bzw. § 3 BetrSichV durchzuführen.

Dies gilt insbesondere auch für speziell programmierte und/oder individuell angepasste (customized) Anwendungen. Hier muss die Umsetzung der Anforderungen nach Absatz 1 bereits bei Auftragsvergabe (z.B. durch Lasten-, Pflichtenhefte) gewährleistet sein.

Die Einhaltung der ergonomischen Grundsätze ist in den Einzeldienstvereinbarungen nach § 7 zu berücksichtigen. Die Dokumentation gemäß § 6 ArbSchG bzw. § 3 (8) BetrSichV ist den Einzeldienstvereinbarungen als Anhang beizufügen.

Eine Überprüfung der Arbeitsplätze und Arbeitsmittel erfolgt auf Antrag der MAV durch diese in Zusammenarbeit mit der Fachkraft für Arbeitssicherheit und dem Betriebsarzt. Das Protokoll dieser Überprüfung wird dem Dienstgeber übergeben. Die Beseitigung etwaiger Mängel ist unverzüglich durch den Dienstgeber umzusetzen.

§ 9 Zulässige Funktionen

In den Anhängen der Einzeldienstvereinbarungen gemäß § 7 zu jeweils zum Einsatz kommenden technischen Einrichtungen werden die zulässigen Funktionen abschließend aufgeführt, die von den Benutzern genutzt werden können.

Neue mitbestimmungsrelevante Funktionen werden nach Zustimmung der MAV bereitgestellt und genutzt. Die entsprechenden Anhänge werden fortgeschrieben.

§ 10 Verarbeitung personenbezogener Daten

Die Daten werden nach den Grundsätzen zur informationellen Selbstbestimmung (Normenklarheit, Verhältnismäßigkeit, Zweckbindung) erfasst und verarbeitet.
Die Erhebung, Verarbeitung und Nutzung der Daten erfolgt ausschließlich zweckbestimmt. Daten auf Vorrat werden nicht erfasst. Die Daten sind unverzüglich zu löschen, wenn ihre Zweckbestimmung entfällt.

In den Anhängen der Einzeldienstvereinbarungen zu jeweils zum Einsatz kommenden Anwendungen und Verfahren werden die Datenfelder der personenbezogenen Daten abschließend aufgeführt, die erhoben, verarbeitet oder genutzt werden (Datenkataloge).

Die Beschreibung ist wie folgt zu gliedern:

Feldname mit Erläuterung
Datentyp
Länge
Muss-/ Kann-Feld
Zweck der Speicherung
Dauer der Speicherung
Falls abweichend: Dauer der Nutzung

Neue Datenfelder mit personenbezogenen Daten werden nach Zustimmung der MAV in den Anwendungen zur Nutzung freigegeben und genutzt. Ausgenommen sind hiervon ausschließlich neue Datenfelder aufgrund gesetzlicher Vorschriften. In diesen Fällen ersetzt die Information der MAV über die gesetzliche Verpflichtung die Zustimmung. Die entsprechenden Anhänge werden fortgeschrieben.

Bewerberdaten sind bei erfolgter Ablehnung unverzüglich zu löschen, wenn kein rechtliches Interesse mehr an der Aufbewahrung besteht (z. B. Ablauf der Fristen nach § 15 Abs. 4 AGG). Eine Speicherung in einem „Bewerberpool" ist nur zulässig, wenn der Betroffene seine Zustimmung zur weiteren Speicherung schriftlich erteilt hat. Hierbei ist dem Bewerber die Speicherdauer seiner Daten mitzuteilen.

Die Datenkataloge werden regelmäßig im Sinne der Durchführungsverordnung zum KDG gemeinsam daraufhin überprüft, ob die aufgeführten Datenfelder noch erforderlich sind. Nicht mehr erforderliche Datenfelder sind zu löschen oder zu sperren und aus den Katalogen zu entfernen.

§ 11 Auswertung personenbezogener Daten

In den Anhängen der Einzeldienstvereinbarungen der jeweils zum Einsatz kommenden mitbestimmungspflichtigen Anwendungen und Verfahren werden die Auswertungen der personenbezogenen Daten abschließend aufgeführt, die erhoben, verarbeitet oder genutzt werden (Auswertungskataloge). Die Beschreibung ist wie folgt zu gliedern:

Name der Auswertung
Kurzbeschreibung
Ausgewerteter Personenkreis
Zweck der Auswertung
Empfänger der Auswertung
Aufbewahrungsort, Aufbewahrungsform und Speicherdauer bzw.
Aufbewahrungsfrist
Angaben zur Gewährleistung der Sicherheit der Verarbeitung

Jede Auswertung erhält ein Standdatum. Die Nutzung der Auswertungen wird protokolliert, wenn dies technisch möglich ist.

Neue Auswertungen von personenbezogenen Daten werden nach Zustimmung der MAV in den Anwendungen bereitgestellt und genutzt. Ausgenommen sind hiervon ausschließlich neue Auswertungen aufgrund gesetzlicher Vorschriften. In diesen Fällen ersetzt die Information der MAV über die gesetzliche Verpflichtung die Zustimmung. Die entsprechenden Anhänge werden fortgeschrieben.

Vor einer Auswertung personenbezogener Daten ist von der Möglichkeit der Pseudonymisierung Gebrauch zu machen, soweit dies nach dem Verwendungszweck möglich ist.

Ad-hoc-Auswertungen personenbezogener Daten außerhalb der vorher festgelegten dienstlichen Zweckbindung sind nicht erlaubt.

Die Auswertungskataloge werden regelmäßig im Sinne der Durchführungsverordnung zum KDG gemeinsam daraufhin überprüft, ob die aufgeführten Auswertungen noch erforderlich sind. Die Nutzung von Auswertungen deren Erforderlichkeit im Rahmen dieser Prüfung nicht nachgewiesen werden kann ist zukünftig untersagt. Sie sind aus den Katalogen zu entfernen.

Sollen in den Einrichtungen Business-Intelligence-Lösungen zum Einsatz kommen (Data-Warehouse), die eine Leistungs- und Verhaltenskontrolle ermöglichen, ist eine entsprechende Einzeldienstvereinbarung abzuschließen.

§ 12 Nebendatenverarbeitung

Nebendatenverarbeitung ist jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten außerhalb von kollektivrechtlich geregelten Systemen und Verfahren (z.B. wenn dies in oder aus Excel-Tabellen, Access-Datenbanken etc. erfolgen soll).

Nebendatenverarbeitung ist grundsätzlich untersagt. Hintergrund des Verbots der Nebendatenverarbeitung ist, dass personenbezogene Daten in der Regel innerhalb von anerkannten kollektivrechtlich geregelten Datenverarbeitungssystemen verarbeitet werden, weil diese ein höheres Maß an Datensicherheit und Wahrung der Persönlichkeitsrechte bieten.

Die Parteien dieser Vereinbarung verfolgen daher das Ziel, erforderliche Nebendatenverarbeitungen unter Wahrung der datenschutzrechtlichen Bestimmungen kollektivrechtlich zu legitimieren und hierfür verbindliche Grundsätze aufzustellen.

a) Zulässige Nebendatenverarbeitung

In folgenden Fällen ist die Nebendatenverarbeitung zugelassen:

Nebendatenverarbeitung ist nur dann zulässig, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten innerhalb von kollektivrechtlich geregelten Systemen und Verfahren objektiv unmöglich ist.

In den Anhängen der Einzeldienstvereinbarungen zu jeweils zum Einsatz kommenden Anwendungen und Verfahren werden die nach dieser DV zugelassenen Nebendaten-verarbeitungen abschließend aufgeführt, insbesondere welche Daten erhoben, verarbeitet oder genutzt werden (Nebendatenverarbeitungskataloge).

Die Beschreibung ist wie folgt zu gliedern:

Gegenstand der Verarbeitung
Zweck der Verarbeitung
Genutztes Programm
Dateiname
Ersteller der Nebendatenverarbeitung
Berechtigte Nutzer
Ggf. weitere Empfänger
Löschfristen

Neue mitbestimmungspflichtige Nebendatenauswertungen mit personenbezogenen Daten werden nach Zustimmung der MAV bereitgestellt und genutzt. Die entsprechenden Anhänge werden fortgeschrieben. Der MAV ist die aktuelle nutzbare Version der Nebendatenverarbeitung zu übergeben.

Die Nebendatenauswertungskataloge werden regelmäßig im Sinne der Durchführungsverordnung zum KDG gemeinsam daraufhin überprüft, ob die aufgeführten Auswertungen noch erforderlich sind. Die Nutzung von Auswertungen, deren Erforderlichkeit im Rahmen dieser Prüfung nicht nachgewiesen werden kann, ist zukünftig untersagt. Sie sind aus den Katalogen zu entfernen.

Jede mitbestimmungspflichtige Änderung oder Anpassung genehmigter Nebendatenverarbeitungen ohne Zustimmung der MAV ist untersagt.

b) Delegation der Berechtigung zur Nebendatenverarbeitung an Assistenzen

Der nach den Regelungen der jeweiligen Einzeldienstvereinbarungen Empfangs- bzw. Nutzungsberechtigte darf im Rahmen der eigenen Befugnisse die Datennutzung bzw. Verarbeitung auch von der jeweiligen, ihm unterstellten Assistenz durchführen lassen. Eine schriftliche oder textliche Beauftragung im Einzelfall ist erforderlich.

c) Vorläufige Zustimmung

In begründeten Ausnahmefällen kann der Dienstgeber auch in einem vereinfachten Verfahren die vorübergehende Zustimmung zu einer Datenverarbeitung beantragen, wenn die Durchführung des Verfahrens nach a) aus sachlichen Gründen nicht möglich ist. Der Dienstgeber kann in diesen Fällen die/den Vorsitzende/n der MAV über die beabsichtigte Nebendatenverarbeitung mit den gleichen Informationen wie im Regelfall mit Bitte um Zustimmung beteiligen. Erfolgt binnen einer Woche keine abschlägige Reaktion, gilt die Zustimmung vorläufig als erteilt. Die vorläufige Zustimmung gilt bis zur nächsten regulären Sitzung der MAV. Diese entscheidet dann verbindlich.

§ 13 Berechtigungskonzept/-rollen

Berechtigungen werden gemäß den Inhalten des Berechtigungskonzeptes in dem dort beschriebenen Verfahren restriktiv vergeben.

Sie sind in den Anhängen zu den Einzeldienstvereinbarungen gemäß § 7 abschließend funktionsbezogen aufzuführen. Änderungen sind durch den Dienstgeber unverzüglich einzupflegen.

Die MAV erhält lesenden Zugriff auf die relevanten Berechtigungen. Erhebt die MAV Widerspruch gegen die Vergabe einer Berechtigung, ist dies im Rahmen des § 25 dieser Dienstvereinbarung zu behandeln.

Eine Änderung bzw. Neueinrichtung von Zugriffsberechtigungen ist von den zuständigen Vorgesetzten schriftlich oder textlich (per Email) den Administratoren unter Angabe des Arbeitsfeldes des betroffenen Users anzuweisen. Eine Einrichtung bzw. Änderung auf Zuruf ist untersagt. Die Einrichtung der Zugriffsberechtigungen erfolgt nach dem Vier-Augen-Prinzip.

Der Dienstgeber teilt den Administratoren die berechtigten Vorgesetzten ebenfalls schriftlich mit.

In der Anlage 4 sind die Zugriffsberechtigten abschließend namentlich aufgeführt, die im System oder in Einzelanwendungen Administratorenrechte besitzen. Änderungen sind unverzüglich einzupflegen.

§ 14 Schnittstellen

Die genutzten Schnittstellen werden in den Anhängen der Einzeldienstvereinbarungen abschließend aufgeführt.

Die Schnittstellenbeschreibungen enthalten folgende Angaben:

Empfangendes oder übergebendes System bzw. empfangende oder übergebende Anwendung
Beschreibung der auszutauschenden Daten
Art der Übergabe Zeitraum
der Übergabe Zweck/ Anlass
der Übergabe

Zusätzlich sind dort die zum Datenaustausch Berechtigten abschließend namentlich aufgeführt. Der Datenaustausch wird gemäß Durchführungsverordnung KDG protokolliert.

Bestandteil der Protokollierung ist u.a.

Name des Users
das zugreifende oder übergebende System
die zum Einsatz kommende Zugriffs- oder Übergabesoftware inkl. Versionsbezeichnung
Zeitraum der Übergabe

Diese Protokolle sind für die MAV jederzeit einsehbar.

§ 15 Datenschutz

Alle Mitarbeitenden, die Zugriff auf personenbezogene Daten haben, sowie alle Mitarbeitenden der IT-Abteilung, werden gemäß der geltenden rechtlichen Bestimmungen hinsichtlich des Datenschutzes und aller diesbezüglich relevanten Vorschriften geschult und haben nach erfolgter Schulung eine gesonderte Verpflichtung zu unterzeichnen. Die erfolgreiche Teilnahme an der Schulungsmaßnahme sowie deren wesentlichen Inhalte sind den Mitarbeitenden schriftlich zu bestätigen. Das Muster für diese Verpflichtung ist Anlage 5 dieser Dienstvereinbarung. Ein Einsatz ohne die Abgabe dieser Erklärung ist ausgeschlossen.

Personenbezogene Daten, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden (§ 6 (5) KDG). Eine Auswertung außerhalb der Zweckbindung sowie eine Weitergabe dieser Daten, Auswertungen und Erkenntnisse an Personen, die nicht für die Datenschutzkontrolle oder Sicherstellung des ordnungsgemäßen IT-Betriebes zuständig sind, sind untersagt.

Die Bewegungsdaten der Systeme, die der besonderen Zweckbindung unterliegen, enthalten keine direkten Personenidentifizierungen. Die Speicherung erfolgt nur so lange, wie die Daten zur Steuerung des Arbeitsprozesses erforderlich sind, höchstens jedoch für 30 Tage. Für längerfristige Speicherungen erfolgt eine Pseudonymisierung im Sinne der gesetzlichen Vorschriften gemäß den jeweiligen Verwendungszwecken, so dass der Personenbezug der ursprünglichen Daten nicht mehr erkennbar ist.

Zur Einhaltung der in den Anlagen und Anhängen definierten Lösch- und Sperrfristen wird sichergestellt, dass ein Zugriff auf vorhandene Sicherungsstände ausschließlich zum Zweck der System- und/oder Datenbankwiederherstellung möglich ist. Der Zugriff darf nur durch den hierzu berechtigten Systemadministrator gemäß Anlage 4 erfolgen. Hierbei sind Art und Zweck des Zugriffs genau zu bestimmen. Zugriffe auf Sicherungsstände werden der MAV unverzüglich mitgeteilt.

§ 16 Datenschutzbeauftragter

Die Auswahl des Datenschutzbeauftragten erfolgt nach den gesetzlichen Vorgaben.

Fertigt der Datenschutzbeauftragte aufgrund seiner Tätigkeit Berichte (derzeit den Jahresbericht) an, die die Verarbeitung von Daten zu Mitarbeitenden betreffen, erhält sie die MAV durch den Dienstgeber unverzüglich in Kopie.

§ 17 Datensicherheit

Der Dienstgeber stellt sicher, dass die Datensicherheit gemäß den gesetzlichen Vorgaben, i.V.m. den Anforderungen des IT-Grundschutzkompendiums des Bundesamtes für Sicherheit in der Informationstechnik in der jeweiligen Fassung, gewährleistet ist.

§ 18 Auftragsverarbeitung

Alle mitbestimmungsrelevanten Verträge zur Auftragsverarbeitung sind so zu gestalten, dass die Kontrollrechte der MAV aus dieser Dienstvereinbarung und weiteren Dienstvereinbarungen nach § 7 gewährleistet sind. Dies gilt analog für den Umfang der Weisungs- und Kontrollbefugnisse, die sich der Dienstgeber gegenüber dem Auftragnehmer vorbehält.

Bestehende und zukünftige mitbestimmungsrelevante Verträge zur Auftragsverarbeitung sind der MAV zur Überprüfung der Sicherstellung ihrer Rechte nach Absatz 1 vorzulegen.

Die Festlegung der Art der zu übermittelnden Daten und der zulässigen Verarbeitungen unterliegen der Mitbestimmung. Eventuelle weitere Mitbestimmungsrechte der MAV bleiben davon unberührt.

Die bestehenden Auftragsverarbeitungen sind system-/ verarbeitungsbezogen in den Anhängen der jeweiligen Einzel-DV abschließend aufgeführt.

§ 19 Qualifizierung

Die Mitarbeitenden werden vor Aufnahme der Arbeit mit neuen grundlegenden Anwendungen und/oder Arbeitsmitteln entsprechend eines mit der MAV abzustimmen- den, in Art und Umfang angemessenen Qualifizierungskonzeptes geschult. Die Qualifizierungsmaßnahmen werden durch entsprechende Angebote kontinuierlich fortgeführt.

Dies gilt entsprechend für Updates, Versions- und Releasewechsel, die die Arbeitsumgebung der Mitarbeiter wesentlich verändern.

Der Dienstgeber stellt sicher, dass die IT-Systembetreuung ausschließlich durch in Datenschutzfragen geschultes Personal erfolgt. Dies ist insbesondere bei der Einführung neuer Technologien bezüglich der mit ihnen verbundenen Datenschutzproblematiken zu beachten.

§ 20 Leistungs- und Verhaltenskontrolle

Eine individuelle Leistungs- und Verhaltenskontrolle der Mitarbeitenden findet nicht statt. Etwas anderes gilt nur, wenn eine Einzeldienstvereinbarung dies ausdrücklich zulässt oder bei Vorliegen einer Ausnahme nach § 22 dieser Vereinbarung.

§ 21 Rechte der Mitarbeitenden

(1) Die Mitarbeitenden werden über den Inhalt dieser Dienstvereinbarung informiert.

(2) Die Mitarbeitenden werden über Art und Umfang der zu ihrer Person erhobenen Daten gemäß §§ 14 ff. KDG informiert. Der Dienstgeber unterrichtet die Mitarbeitenden umfassend über wesentliche Änderungen des IT-Systems sowie bei Änderungen der Zweckbestimmung der Daten.

(3) Den Mitarbeitenden stehen die Rechte nach § 17 ff. KDG im dort beschriebenen Umfang zu: Jeder Mitarbeitende hat das Recht auf Auskunft nach § 17 KDG („Recht auf Auskunft"). Unter den gesetzlichen Voraussetzungen hat jeder Mitarbeiter das Recht auf Berichtigung nach § 18 KDG („Recht auf Berichtigung"), das Recht auf Einschränkung der Verarbeitung nach § 20 KDG („Recht auf Einschränkung der Verarbeitung") oder das Recht auf Löschung („Recht auf Vergessenwerden") nach § 19 KDG. Zudem hat jeder Mitarbeitende das Recht auf Herausgabe der von ihm bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format („Recht auf Datenübertragbarkeit") nach § 22 KDG, sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt und auf einer Einwilligung nach § 8 KDG beruht.

Hierfür stellt der Dienstgeber Antragsformulare zur Verfügung. Nach Einreichung durch die Mitarbeitenden, werden die Anträge an die zuständigen Stellen in der Dienstelle, Einrichtung oder Kirchengemeinde weitergeleitet.

Alle Anträge sind innerhalb eines Monats zu bescheiden. Werden Anträge negativ beschieden, ist dies zu begründen und auf das Beschwerderecht bei der Datenschutzaufsicht hinzuweisen.

(4) Beruht die Verarbeitung auf einer Einwilligung kann jeder Mitarbeitende die erteilte Einwilligung in die Verarbeitung personenbezogener Daten jederzeit widerrufen (§ 8 Abs. 6 KDG).

(5) Jeder Mitarbeitende kann sich mit einer Beschwerde an die Dienstgeberin, an den Datenschutzbeauftragten, die MAV sowie an die Datenschutzaufsicht wenden.

(6) Zusätzlich zu den vorgenannten Rechten steht jedem Mitarbeitenden ein einzelfallbezogenes Widerspruchsrecht i.S.d. § 23 KDG zu: Mitarbeitende haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von § 6 Abs. 1 f oder g erfolgt, Widerspruch einzulegen. Im Falle des Widerspruchs wird die Dienstgeberin personenbezogene Daten des Mitarbeitenden nicht mehr verarbeiten, es sei denn, die Dienstgeberin kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten des Mitarbeitenden im Einzelfall überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(7) Abweichungen von dieser DV dürfen von Vorgesetzten nicht angewiesen werden.

§ 22 Verdacht von Straftaten oder schwerwiegenden Vertrags- und Dienstpflichtverletzungen

Besteht der Verdacht einer Straftat, schwerwiegenden Vertrags- und Dienstpflichtverletzung, schwerwiegenden Verletzung der Bestimmungen dieser Dienstvereinbarung oder einer Einzeldienstvereinbarung, gelten folgende Regelungen:

(1) In diesem Fall müssen zu dokumentierende, tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat oder schwerwiegende Pflichtverletzung begangen hat. Es muss die Verarbeitung zur Aufdeckung erforderlich sein. Das schutzwürdige Interesse des Beschäftigten am Ausschluss der Verarbeitung darf nicht überwiegen, insbesondere Art und Ausmaß dürfen im Hinblick auf den Anlass nicht unverhältnismäßig sein oder eine Rechtsvorschrift muss die Verarbeitung vorsehen (§ 53 Abs. 2 KDG).

(2) Sind diese Voraussetzungen aus Sicht des Dienstgebers gegeben, hat er die Zustimmung der MAV zur Verarbeitung einzuholen. Dabei ist der Dienstgeber dazu verpflichtet, den auslösenden Verdacht der MAV in Textform mitzuteilen. Er muss dabei den genauen Zweck, den Umfang der zu erhebenden Daten und den Zeitraum der beabsichtigten Leistungs- und Verhaltenskontrolle festlegen und der MAV mitteilen.
Die Zustimmung gilt als erteilt, wenn die MAV nicht binnen einer Woche (bei Sondervertretungen binnen zwei Wochen) nach Eingang des Antrags in Textform Einwendungen erhebt. Auf Antrag der MAV kann der Dienstgeber die Frist um eine weitere Woche verlängern.

Erhebt die MAV Einwendungen, so haben Dienstgeber und MAV mit dem Ziel der Einigung zu verhandeln, falls nicht der Dienstgeber von der beabsichtigten Maßnahme und Entscheidung Abstand nimmt. Der Dienstgeber setzt den Termin für die Verhandlungen fest und lädt dazu ein. Die MAV erklärt innerhalb drei Tagen nach dem Verhandlungstermin in Textform, ob sie die Zustimmung erteilt oder verweigert. Äußert sie sich innerhalb dieser Frist nicht, gilt die Zustimmung als erteilt.

Verweigert die MAV die Zustimmung, so kann die Dienststelle die Einigungsstelle anrufen. Die Einigungsstelle entscheidet dann endgültig.
Bei der Durchführung der Leistungs- und Verhaltenskontrolle ist ein MAV-Mitglied hinzuzuziehen.

(3) Nach der Auswertung ist die MAV über das Ergebnis zu informieren.

(4) Bestätigt sich der Verdacht nicht, sind alle erhobenen Daten, Auswertungen und sonstigen Erkenntnisse unverzüglich zu vernichten.

(5) Bestätigt oder verstärkt sich der Verdacht, ist der Mitarbeitende anzuhören. Hierbei ist der Mitarbeitende darauf hinzuweisen, dass auf dessen Wunsch eine Mitarbeitervertreterin / ein Mitarbeitervertreter hinzugezogen werden kann.

(6) Begründen die dokumentierten tatsächlichen Anhaltspunkte den Verdacht einer schwerwiegenden Verletzung von Strafvorschriften, hat der Dienstgeber die MAV entsprechend Abs. 2 in Textform über den Verdacht zu informieren. Des Weiteren ist der MAV der Zeitpunkt der beabsichtigten Leistungs- und Verhaltenskontrolle mitzuteilen und ein MAV-Mitglied einzuladen. Auf Wunsch der MAV können bei der Durchführung der Leistungs- und Verhaltenskontrolle zwei MAV-Mitglieder anwesend sein.

Als schwerwiegender Verstoß gegen strafrechtliche Vorschriften gelten insbesondere:

- Straftaten nach den §§ 184, 184a, 184b und 184c StGB
- schwere Vermögensdelikte zu Lasten des Dienstgebers
- Arbeitszeitbetrug im erheblichen Umfang

Im Übrigen gelten die Absätze 3, 4 und 5.

§ 23 Beweisverwertungsverbot

(1) Arbeitsrechtliche Maßnahmen, die auf einer nach dieser Vereinbarung rechtswidrigen Datenerfassung oder -nutzung basieren, sind unzulässig. Informationen, die in diesen Fällen bei Nichtbeachtung der in dieser DV enthaltenen Bestimmungen gewonnen wurden, dürfen nicht als Grundlage oder Rechtfertigung oder Beweismittel für eine personelle Einzelmaßnahme herangezogen werden. Insoweit besteht ein Beweisverwertungsverbot.

(2) Der Nachweis der Rechtmäßigkeit der IT-Auswertung liegt beim Dienstgeber.

(3) Im Falle unzulässiger Datenverarbeitung sind alle darauf beruhenden Maßnahmen rückgängig zu machen.

(4) Den betroffenen Mitarbeitenden steht der Rechtsweg offen.

§ 24 Rechte der MAV

Der Dienstgeber unterrichtet die MAV unverzüglich über geplante mitbestimmungsrelevante Änderungen der IT-Systeme. Die Mindestanforderungen an die Unterrichtung ergeben sich aus dem Formblatt in Anlage 2.

Die MAV hat im Rahmen ihrer allgemeinen Aufgaben ein Informations- und Überwachungsrecht hinsichtlich der Einhaltung dieser Dienstvereinbarung. Im Rahmen dieses Rechts ist der Zugang zu den Arbeitsplätzen, an denen die IT-Systeme eingesetzt werden, ebenso zu gewähren wie die dazu notwendigen Informationen. Weiterhin hat die MAV das Recht, elektronische Endgeräte in Augenschein zu nehmen.

Die MAV hat außerdem das Recht, sich an dem ihr zur Verfügung gestellten Rechner alle Funktionen anzuzeigen und auszudrucken, die unter anderem Aufschluss über den Systemzustand, installierte Anwendungen, vergebene Zugriffsrechte und aktive Protokolle geben.

Die MAV erhält Einsicht in sämtliche Systemänderungsprotokolle, Schnittstellendateien, System- und Anwendungsunterlagen.

Der Dienstgeber stellt der MAV in Absprache mit diesem die für die MAV-Arbeit notwendigen Abfragen und Reports in den jeweiligen Systemen zur Verfügung.

Entsprechend § 13 (2) a) der Durchführungsverordnung KDG wird der MAV innerhalb von zwei Jahren ein geeignetes Verfahren ggfls. mit Software-Unterstützung vom Dienstgeber zur Verfügung gestellt, die es ihr ermöglicht, ihre Daten durch Verschlüsselung vor unberechtigtem Zugriff zu schützen. Gleiches gilt für die Installation einer Software zur endgültigen Datenlöschung.

Weiterhin erhält die MAV innerhalb von zwei Jahren nach in Krafttreten dieser Dienstvereinbarung entsprechend § 12 (2) e) der Durchführungsverordnung KDG ein Verfahren ggfls. mit Software zur Verfügung gestellt, die das verwendete Email-Programm dahingehend erweitert, dass Emails verschlüsselt werden können.

Jeder Zugriff auf Daten der MAV durch Personen, die nicht Mitglieder der MAV sind, ist untersagt, es sei denn, der Zugriff erfolgt aufgrund eines Antrags der MAV. Jede Änderung von Zugriffsberechtigungen der MAV und von Zugriffsberechtigungen ihrer Mitglieder im Zusammenhang mit ihrer MAV-Tätigkeit bedarf der vorherigen Zustimmung des Gremiums.

Bei der mitbestimmungspflichtigen Einführung neuer IT-Systeme (insbesondere bei neuen Technologien), bei der Einführung oder Erweiterung von Verarbeitungen personenbezogener Daten der Mitarbeitenden und zur Überprüfung der Einhaltung dieser Dienstvereinbarung und der sie ergänzenden Regelungen kann die MAV Sachverständige ihrer Wahl unter Berücksichtigung der Vorgaben des § 17 Abs. 1 MAVO hinzuziehen.

§ 25 Konfliktklausel

Werden Tatsachen bekannt, die den Vereinbarungen dieser Dienstvereinbarung zuwiderlaufen, sei es

- der Gebrauch nicht genehmigter Anwendungen oder Verfahren
- der Gebrauch nicht genehmigter technischer Einrichtungen
- die Erfassung nicht genehmigter Daten
- eine nicht genehmigte Auswertung derselben
- die nicht rechtskonforme Vergabe von Zugriffsberechtigungen

oder werden nach genehmigter Einführung von Anwendungen, Verfahren, technischen Einrichtungen, Datenerfassungen und Datenauswertungen bzw. nach der Vergabe von Zugriffsberechtigungen Tatsachen bekannt, die dem Sinne dieser Vereinbarung widersprechen, so ist auf Antrag der MAV die Verwendung der entsprechen- den Anwendungen, Verfahren, technischen Einrichtungen, Datenerfassungen oder Auswertungen bzw. die Nutzung von Zugriffsberechtigungen bis zu einer einvernehmlichen Regelung unverzüglich zu unterbinden.

§ 26 Schlussbestimmung

Ergeben sich bei Anwendung oder Auslegung dieser DV zwischen Dienstgeber und MAV Streitigkeiten, werden beide Seiten eine einvernehmliche Lösung anstreben. Kommt diese innerhalb von zwei Monaten nicht zustande, wird die Einigungsstelle angerufen.
Die betroffenen Mitarbeiter sind anzuhören. Im Übrigen steht der Rechtsweg offen.

§ 27 Inkrafttreten

Die Dienstvereinbarung tritt sofort nach Unterzeichnung in Kraft.

§ 28 Kündigungsfrist und Nachwirkung

Diese Dienstvereinbarung kann von den Parteien mit einer Frist von 3 Monaten zum Monatsende gekündigt werden, frühestens jedoch zum 31.12.2027. Nach Ausspruch der Kündigung sind unverzüglich Verhandlungen über eine ersetzende Dienstvereinbarung aufzunehmen. Bis zum Abschluss einer ersetzenden Dienstvereinbarung wirken die Regelungen der vorliegenden Dienstvereinbarung in vollem Umfang nach.

§ 29 Salvatorische Klausel

Änderungen dieser Vereinbarung können nur in Schriftform als Änderungskündigung zwischen den Parteien vereinbart werden. Die Unwirksamkeit einzelner Bestimmungen dieser Dienstvereinbarung berührt die Wirksamkeit der Dienstvereinbarung im Übrigen nicht. Die Parteien verpflichten sich, die unwirksamen Regelungen unverzüglich durch rechtlich gültige gleichen Sinnes zu ersetzen.

Sigmaringen, den 9.10.26

Röm. Kath. Kirchengemeinde Sigmaringen

Dienstgeber	Mitarbeitervertretung
.....	.....
Vertreter des Dienstgebers	Vorsitzender der Mitarbeitervertretung
Herr Pfarrer Stefan Schmid / Herr Pfarreiökonom Andreas Rösch	Herr Joachim Stopper

Anlage 1: Begriffsbestimmungen

Zentrale Systeme:
Zentrale Systeme sind technische Einrichtungen, die von mehreren Dienststellen und/oder Einrichtungen zu vergleichbaren Zwecken genutzt werden.

Zentrale Verfahren:
Zentrale Verfahren sind Verfahren bei denen Daten von Dienststellen und/oder Einrichtungen in zentralen Systemen verarbeitet werden oder Daten aus zentralen Systemen in den Dienststellen und/oder Einrichtungen weiterverarbeitet werden.

Schnittstellen:
Schnittstellen im Sinne dieser Betriebsvereinbarung sind Stellen und Verfahren, durch die Daten an andere Systeme übergeben werden, durch die Daten an andere Software übergeben werden, durch die andere Systeme Zugriff auf Daten des Systems erhalten oder Daten anderer Systeme in das System gelangen.

Ad-Hoc-Auswertungen:
Ad-hoc-Auswertungen sind vom Benutzer direkt und interaktiv zusammengestellte Auswertungen. Sie unterscheiden sich von vorgefertigten Auswertungen dadurch, dass der Benutzer Inhalt und Aussehen der Auswertung selbst bestimmen kann. Im Gegensatz zur vorgefertigten Auswertung, deren Struktur, Aussehen und Auswahlmöglichkeiten vom Ersteller vorgegeben ist, hat der Endbenutzer innerhalb des vorbereiteten Rahmens (Metadatenstruktur) alle Gestaltungsmöglichkeiten selbst in der Hand.

Anlage 2: Unterrichtung der MAV gemäß MAVO

System/Projektbeschreibung: Zweck, geplanter Aufwand, geplante Ziele, Start/Ende des Projektes, Projektgruppen

Sachmitteleinsatz: Beschreibung des Systems (Lasten- /Pflichtenheft, die auf die kirchlichen Bedürfnisse des Programms angepasste (customized) Version des Programms), der Hardware, der Anwendungen (u.a. White Paper, Handbücher etc. in deutscher Sprache mit Modulen und Schnittstellen, Neben-Datenverarbeitungen; weitere Beschreibungen in verständlicher Form und deutscher Sprache); Einsatzorte; betroffene Abteilungen, Arbeitsplätze; Wert in T€

Personelle Auswirkungen: Auswirkungen auf bisherige Aufgaben, Arbeitsabläufe und Arbeitsplätze; Veränderung der Arbeitsbedingungen §4 ArbSchG, der Arbeitsplatzgestaltung, der Entlohnungsmethoden; direkte und indirekte Rationalisierungsmaßnahmen mit personellen Auswirkungen, Fremdpersonaleinsatz (Verträge)

Datenschutz: Geplante Erfassung, Verarbeitung personenbezogener Daten (vollständiger Datenkatalog); geplante Auswertungen (vollständiger Auswertungskatalog); Zugriffskonzept, Datenschutz-Folgenabschätzung, Verträge zur Auftragsverarbeitung, Stellungnahme des betrieblichen Datenschutzbeauftragten, Verzeichnis der Verarbeitungstätigkeiten (§ 31 KDG)

Besondere Maßnahmen: Arbeitsschutz, Gefährdungsbeurteilung §5 ArbSchG bzw. §3 BetrSichV; Unfallverhütung (ArbeitsstättenVO usw.); Qualifizierung

Sonstige notwendige Angaben:

Anlage 3: Einzeldienstvereinbarungen
zur Dienstvereinbarung IT-Einsatz und Datenschutz über die Planung, den Einsatz und Betrieb von IT-gestützten Informations- und Verarbeitungssystemen.

Muster:

1. Geltungsbereich
Falls abweichend.

2. Gegenstand der Dienstvereinbarung
Benennung System oder Verfahren.

Diese Dienstvereinbarung ist Anlage der Dienstvereinbarung IT und Datenschutz.

3. Systembeschreibung:
u. a. Zweck, Einsatzorte; Betroffene Abteilungen, Arbeitsplätze (Anhänge). Allgemein verständliche Überblicksbeschreibung des Systems.

4. Zulässige Funktionen
Bei Software z.B. eingesetzte Module, bei Hardware zulässige Funktionen (z.B. bei Telefonanlagen Weiterleitung, Mithören etc.) gem. § 9 der Dienstvereinbarung (Anhänge), Schnittstellen

5. Personelle Auswirkungen:
Auswirkungen auf bisherige Aufgaben, Arbeitsabläufe und Arbeitsplätze; Veränderung der Arbeitsbedingungen § 5 Abs. 1 Nr. 4 ArbSchG, der Arbeitsplatzgestaltung, der Entlohnungsmethoden; direkte und indirekte Rationalisierungsmaßnahmen mit personellen Auswirkungen

6. Art und Umfang der erhobenen/verarbeiteten personenbezogenen Daten:
Erfassung, Verarbeitung personenbezogener Daten gem. § 10 der Dienstvereinbarung (Anhänge).

7. Art und Umfang der Auswertungen:
geplante Auswertungen gem. § 11 der Dienstvereinbarung (Anhänge)
geplante Nebendatenauswertungen gem. § 12 der Dienstvereinbarung (Anhänge)

8. Berechtigte Nutzer, Auswerter, Empfänger:
Namentlich oder funktionsbezogen (Anhänge)

9. Datenschutz:
Verarbeitungsverzeichnis (§ 31 KDG), Datenschutzfolgeabschätzung, Stellungnahme des betrieblichen Datenschutzbeauftragten

10. Besondere Maßnahmen:
Unter anderem: Arbeitsschutz, Unfallverhütung (ArbStättV, BetrSichV usw.), Dokumentation der Gefährdungsbeurteilung (Anhang); Ergonomie und Barrierefreiheit, Qualifizierung

11. (ggf.) Sonstige Regelungen:
Auftragsverarbeitung

12. Inkrafttreten, Kündigungsfrist, Nachwirkung

Anlage 4: Besondere Zugriffsberechtigung

Die Mitarbeitenden mit Administratorenrechten sind derzeit durch das Erzbischöfliche Ordinariat noch nicht benannt.

Der Dienstgeber wird nach §13, Abs. 6 an dieser Stelle ein geeignetes Formular zur Verfügung stellen

Anlage 5: Verpflichtungserklärung

Verpflichtungserklärung
zum Datengeheimnis und zur Einhaltung der datenschutzrechtlichen Anforderungen des Gesetzes über den Kirchlichen Datenschutz (KDG) sowie
Belehrung
über das Verbot der Nutzung dienstlicher digitaler Mittel zu privaten Zwecken

Name, Vorname .....

geboren am .....

Dienststelle .....

(1) Ich verpflichte mich, zur Einhaltung des Datengeheimnisses (§ 5 KDG) und zur Einhaltung des kirchlichen Datenschutzgesetzes und der dazu erlassenden Verordnung in der jeweils gültigen Fassung.

Ich versichere, dass ich alle personenbezogenen Daten, die ich im Rahmen meiner Tätigkeit verarbeite oder die mir zur Kenntnis gelangen, vertraulich behandele. Das Datengeheimnis besteht auch nach Beendigung meiner Tätigkeit fort.

(2) Mir ist bekannt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist (§ 6 KDG). Die Grundsätze des kirchlichen Rechts für die Verarbeitung personenbezogener Daten (§ 7 Abs.1 KDG) habe ich zur Kenntnis genommen. Sie beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Transparenz");
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung");
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit");
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung");

- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Ich bin darüber belehrt worden, dass ein Verstoß gegen die Vorschriften des KDG und die anderen für meine Tätigkeit geltenden Datenschutzvorschriften ein Verstoß gegen arbeitsrechtliche Pflichten darstellt, der rechtliche Folgen haben kann, wie sie im beigefügten Merkblatt beschrieben sind.

(3) Ich bin darauf hingewiesen worden, dass die Nutzung von Telefax, E-Mail, Internet/Intranet sowie sonstiger im Rahmen meines Auftrages zur Verfügung gestellter Hard- und Software für private Zwecke nicht zulässig ist.

Weitere sich aus dem Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtungen werden durch diese Erklärung nicht berührt.

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung und das Merkblatt Datenschutz (Rückseite) habe ich erhalten.

.....,	.....,
.....Ort, Datum	.....Ort, Datum
.....	.....
Unterschrift der/des Verpflichteten	Unterschrift der/des Verantwortlichen

Original: Personalakte
1 Kopie: Verpflichtete(r)

Merkblatt Datenschutz

Im Rahmen Ihrer Tätigkeit arbeiten Sie mit personenbezogenen Daten z. B. unserer Mitglieder, Mitarbeitenden und Geschäftspartnerinnen und -partner oder es gibt für Sie die Möglichkeit des Zugriffs auf solche Daten. Deshalb müssen Sie sich mit den wichtigsten Grundsätzen des Datenschutzes vertraut machen.

(1) Die wichtigste Grundlage für den Datenschutz bei uns ist das KDG. Das kirchliche Datenschutzgesetz schützt personenbezogene Daten. Das sind alle Informationen, die sich auf einen identifizierten oder identifizierbaren Menschen („natürliche Person") beziehen. Anonyme Daten fallen nicht unter die Datenschutzgesetze.

(2) Geschützt wird das informationelle Selbstbestimmungsrechts jedes Einzelnen: Jeder soll grundsätzlich selbst darüber bestimmen dürfen, wer welche Daten über ihn kennt und verarbeitet. Deshalb dürfen personenbezogene Daten nur verarbeitet werden, wenn hierfür eine Einwilligung der betroffenen Person vorliegt oder eine Erlaubnis im Gesetz oder einem Vertrag vorhanden ist.

(3) Besonders schützenswerte „sensible" Daten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetische Daten, Gesundheit, Sexualleben, strafrechtliche Verurteilungen, Straftaten oder damit verbundene Sicherungsmaßnahmen) dürfen regelmäßig nicht verarbeitet werden. Für das Beschäftigungsverhältnis gibt es aber für erforderliche Verarbeitungen gesetzliche Ausnahmen. Außerdem besteht die Möglichkeit einer ausdrücklich auf diese Daten bezogenen Einwilligung.

(4) Eine Einwilligung muss immer freiwillig, klar und unmissverständlich sein. In vielen Fällen ist eine Datenverarbeitung nach dem Gesetz aber auch ohne Einwilligung zulässig. z. B.:

- zur Beantwortung von Anfragen;
- zur Erfüllung eines Vertrags, z. B. wenn wir Daten unserer Mitglieder, Mitarbeitenden oder Kundinnen/Kunden zur Durchführung des Arbeits-, Kauf- oder Dienstleistungsvertrages verarbeiten;
- in vielen Fällen, in denen die Verarbeitung zur Aufgabe der Kirche gehört.

(5) Die Transparenz der Datenverarbeitung ist eine wichtige Voraussetzung für das informationelle Selbstbestimmungsrecht. Deshalb muss die betroffene Person bei Erhebung ihrer Daten oder beim erstmaligen Kontakt umfassend informiert werden und hat auch nachträglich ein Recht auf Auskunft.

(6) Bei Vorliegen der gesetzlichen Voraussetzungen hat jede betroffene Person außerdem die Rechte auf Berichtigung, Löschung, Beschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und Datenübertragbarkeit, sowie ein Recht auf Beschwerde bei der Datenschutzaufsichtsbehörde.

(7) Schließlich müssen unsere Mitglieder, Beschäftigten und Vertragspartnerinnen und -partner darauf vertrauen können, dass ihre personenbezogenen Daten bei uns

sicher sind. Datenschutz und Datensicherheit haben zwei wichtige Grundlagen: eine persönliche und eine technische.

Persönlich müssen Sie als Mitarbeitende/r die Vertraulichkeit der Verarbeitung beachten, zu der Sie sich umseitig verpflichtet haben. Außerdem müssen Sie unsere Weisungen im Umgang mit personenbezogenen Daten befolgen und Datenschutz- oder Datensicherheitsverletzungen unverzüglich melden.

Bitte beachten Sie, dass ein Verstoß gegen die datenschutzrechtlichen Bestimmungen ein Verstoß gegen arbeitsrechtliche Pflichten darstellt, der entsprechend geahndet werden kann. Dies kann ggf. Geldbußen, Geldstrafen oder gar Freiheitsstrafe bis zu einem Jahr bedeuten. Entsteht der betroffenen Person durch die unbefugte Verarbeitung ein Schaden, kann ebenfalls ein Schadensersatzanspruch entstehen.

Technisch und organisatorisch muss die Datensicherheit durch geeignete Maßnahmen sichergestellt werden, um personenbezogenen Daten gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen und den Schutz der Rechte der betroffenen Personen und die Einhaltung der anwendbaren datenschutzrechtlichen Bestimmungen der Erzdiözese Freiburg, der Europäischen Union und der Bundesrepublik Deutschland zu gewährleisten.

(8) Helfen Sie dabei, die Ihnen anvertrauten personenbezogenen Daten zu schützen, indem Sie selbst weisungsgemäß und sorgfältig damit umgehen und verdächtige Beobachtungen und Datenschutz- oder Datensicherheitsverletzungen Ihren Vorgesetzen oder dem betrieblichen Datenschutzbeauftragten melden. Dort erhalten Sie auch weitere Informationen zum Datenschutz.

Fachbegriffe und Abkürzungen:

Administratoren
Ein Administrator ist eine spezielle Rolle eines Benutzers in Betriebssystemen, Netzwerken oder Anwendungsprogrammen. Um spezielle Aufgaben wie das Verwalten von Inhalten zu erfüllen und die jeweiligen Benutzungsrichtlinien durchzusetzen, hat ein Administrator erweiterte Benutzerrechte

ArbSchG
Arbeitsschutzgesetz

BetrSichV
Betriebssicherheitsverordnung

Business-Intelligence-Lösungen
Geschäftsanalytik, englisch Business Intelligence ist ein der Wirtschaftsinformatik zuzuordnender Begriff, der Verfahren und Prozesse zur systematischen Analyse des eigenen Unternehmens bezeichnet. Dies umfasst die Sammlung, Auswertung und Darstellung von Daten in elektronischer Form.
Ziel ist die Gewinnung von Erkenntnissen aus vorhandenen Daten zur Unterstützung von Leitungsentscheidungen. Die Auswertung von Daten geschieht mit Hilfe spezialisierter Software und IT-Systeme. Mit den gewonnenen Erkenntnissen können Geschäftsabläufe sowie Kunden- und Lieferantenbeziehungen beurteilt werden. Weitere Aspekte können aber auch Kostensenkung, Risikoreduzierung und Wertschöpfung sein (siehe: Wikipedia Artikel: Business Intelligence)

Data Warehouse
Ein Data Warehouse (wörtlich Datenlager) ist eine für Analysezwecke optimierte zentrale Datenbank, die Daten aus mehreren unterschiedlichen Quellen zusammenführt. Der Inhalt eines Data Warehouse entsteht durch Kopieren und Aufbereiten von Daten aus diesen unterschiedlichen Quellen (siehe Wikipedia Artikel: Data Warehouse).

IT-Grundschutzkompendium
Wird jährlich vom Bundesamt für Sicherheit in der Informationstechnik veröffentlicht. Es bildet die Basis für alle, die sich umfassend mit Informationssicherheit beschäftigen möchten. Die einzelnen Bestandteile bilden den aktuellen Stand der Technik ab

KDG
Kirchliches Datenschutzgesetz

Pseudonymisierung
Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (zumeist ein Code bestehend aus mehrstelligen Buchstaben- oder Zahlenkombinationen) ersetzt, um die Feststellung der Identität des Betroffenen auszuschließen oder wesentlich zu erschweren.
Im Gegensatz zur Anonymisierung bleiben bei der Pseudonymisierung Bezüge verschiedener Datensätze, die auf dieselbe Art pseudonymisiert wurden, erhalten.

Releasewechsel
beschreibt die Aktualisierung von Standardsoftware. Sie erfolgt durch die Installation einer vom Hersteller ausgelieferten, neuen Version.

User
Benutzer sind Personen oder Personengruppen, die sich zur Wahrnehmung ihrer Aufgaben einer Datenverarbeitungsanlage bedienen und dabei in unmittelbarem Kontakt mit der Anlage stehen.
Anwender sind Organisationen oder Institutionen, die die Anschaffung und den Betrieb der Anlage oder Software verantworten (Auswahl, Lizenz, Installation).