ERZBISTUM KÖLN

Erzbistum Köln | Generalvikariat
Hauptabteilung Seelsorge Personal

Rahmen-Dienstvereinbarung

Informations- und Kommunikationstechnologien („RDV IuK“) der

Gemeindereferenten/-assistenten/Pastoralreferenten/-assistenten/-innen

zwischen dem

Erzbistum Köln

- nachfolgend kurz Dienstgeber genannt -

und

der Sondermitarbeitervertretung für Gemeindereferenten/-assistenten/Pastoralreferenten/-assistenten/-innen beim Erzbistum Köln (MAV GR/ PR)

- nachfolgend kurz MAV genannt -

- beide Parteien kurz „die Parteien“ genannt -

DIENSTVEREINBARUNG

Inhalt

1. Präambel

Der Dienstgeber und die MAV sind sich einig, dass elektronische Datenverarbeitungs- und Kommunikationssysteme für die Erfüllung der anfallenden dienstlichen pastoralen und seelsorgerlichen Aufgaben, zur Sicherstellung der ordnungsgemäßen internen und externen Dokumentation, für die Einhaltung der Wirtschaftlichkeit sowie auch um die Rahmenbedingungen der pastoralen Arbeit zu verbessern unerlässlich sind. Diese dienen sowohl einer effizienten als auch transparenten einheitlichen Aufgabenerfüllung. Sie sollen daneben die Arbeit der Mitarbeiter erleichtern und effizienter gestalten.

Der Dienstgeber und die MAV sind sich weiter darüber einig, dass beim Einsatz solcher Systeme Persönlichkeitsrechte der Mitarbeiter betroffen sein können.

Mit dieser Rahmen-Dienstvereinbarung (nachfolgend auch kurz „RDV" genannt) legen die Parteien Rahmenbedingungen zur Einführung und Anwendung von IuK-Systemen mit dem Ziel fest, den Interessen beider Seiten gleichermaßen gerecht zu werden und die schutzwürdigen Belange der Mitarbeiter unter Beachtung aller maßgeblichen gesetzlichen Regelungen zu sichern.

Die Parteien wollen mit dieser RDV einheitliche Standards bei dem Dienstgeber für die Einführung und den Einsatz von neuen und auf längere Sicht auch für bereits im Einsatz befindliche IuK-Systeme, für die die MAV zuständig ist, schaffen.

Die Parteien dieser RDV sind sich darüber einig, dass die Verarbeitung von persönlichen Daten der in Deutschland tätigen Mitarbeiter dem kirchlichen Datenschutzgesetz (KDG) unterliegt.

Durch diese RDV sollen die Beteiligungsrechte der MAV nach § 38 Abs. 1 Nr. 11 MAVO gesichert werden. Sie dient auch der Wahrung des Persönlichkeitsschutzes der Mitarbeitenden, insbesondere dem Schutz vor einer zweckwidrigen Überwachung des Verhaltens oder der Leistung durch technische Einrichtungen, und soll den Umgang mit personenbezogenen Daten transparent machen und regeln.

2. Geltungsbereich

Diese Rahmen-Dienstvereinbarung gilt

2.1.
räumlich für alle kategorialen und territorialen Einsatzstellen, auf denen GR/ PR und PA/ GA des Erzbistums Köln eingesetzt sind,

2.2.
persönlich für alle GR/ PR und alle GA/ PA des Erzbistums Köln,

2.3.
fachlich und sachlich für alle beim Dienstgeber gegenwärtig oder künftig eingesetzten IT-Systeme bzw. IT-Dienste, für die die MAV zuständig ist. Soweit es zu bereits eingesetzten IuK-Diensten

bereits bestehende Dienstvereinbarungen bei dem Dienstgeber gibt, gelten die Regelungen gemäß Ziffer 3.2 dieser RDV.

3. Gegenstand

3.1.
Gegenstand dieser RDV ist die Sicherstellung und Präzisierung der Rechte der MAV in Bezug auf die Planung, Einführung, Nutzung, Änderung und Erweiterung von IuK-Systemen im territorialen oder kategorialen Einsatzfeld.

3.2.
Diese Rahmen-Dienstvereinbarung 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 Rahmen-Dienstvereinbarung bestehen, gehen die Regelungen dieser Rahmen-Dienstvereinbarung im Anwendungsbereich vor, es sei denn, dass die Bestandsregelungen günstiger sind für die GR/ PR.

3.3.
Gegenstand dieser RDV ist zudem 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.

4. Drittwirkung

Die Regelungen dieser Rahmen-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 GR/ PR selbst und die territorialen oder kategorialen Einsatzfelder der GR/ PR tätig sind. Daher stellt der Dienstgeber durch entsprechende Gestaltung von Werk-, Dienst- und Dienstleistungsverträgen mit Dritten sicher, dass die Einhaltung dieser Rahmen-Dienstvereinbarung und der Einzeldienstvereinbarungen die ordnungsgemäße Wahrnehmung der Mitbestimmungsrechte der MAV gewährleistet sind.

5. Ziele

Diese RDV hat zum Ziel,

- den Schutz der Mitarbeitenden vor einer willkürlichen elektronischen Überwachung von Leistung und Verhalten sicherzustellen und sachlich begründete Fälle der zulässigen elektronischen Überwachung der Leistung und des Verhaltens festzulegen,

- die reibungslose Einführung und Anwendung von IuK-Systemen sicherzustellen,
- Störungen der betrieblichen Abläufe zu vermeiden,
- sicherzustellen, dass das individuelle Recht der Mitarbeitenden auf informationelle Selbstbestimmung im Rahmen der gesetzlichen und betrieblichen Regelungen gewährleistet wird und dass die Interessen der Mitarbeitenden in angemessenem Umfang berücksichtigt werden,
- sicherzustellen, dass die einschlägigen Gesetze, insbesondere das KDG und die MAVO eingehalten werden,
- sicherzustellen, dass der MAV ermöglicht wird, ihre gesetzlichen Mitbestimmungsaufgaben rechtzeitig und in angemessenem Umfang wahrzunehmen,
- den aktuellen Stand der den Mitbestimmungsrechten der MAV unterliegenden IuK-Systemen zu dokumentieren,
- die Regelungen zur Nutzung von IuK-Systemen transparenter und einheitlicher zu gestalten sowie
- die durch IuK-Systeme unterstützten Arbeitssysteme auf hohem Qualitätsniveau zu gestalten.

6. Begriffsbestimmungen

Unter IuK-Systemen werden alle elektronischen Hardware- oder Software-Systeme sowie IuK-Dienste zur Speicherung, Verarbeitung und Ausgabe von Daten in Zeichen, Bildern oder akustischer Form oder Systeme zur Übertragung von Daten (Zeichen, Bilder, akustische Information, Impulse) verstanden.

7. Allgemeine Regelungen zur Einführung und Anwendung von IuK-Systemen

Für die geplante Einführung und Anwendung von IuK-Systemen bei dem Dienstgeber, für die die MAV zuständig ist, gelten die nachfolgenden Regelungen.

7.1. Kategorisierung der IuK-Systeme

IuK-Systeme werden von dem Dienstgeber vor ihrer Einführung dahingehend geprüft, ob sie technische Einrichtungen im Sinne des § 38 Abs. 1 Nr. 11 MAVO sind, die dazu bestimmt oder geeignet sind, das Verhalten oder die Leistung der Mitarbeitenden zu überwachen.

Dabei ist „Überwachung" im Sinne von § 38 Abs. 1 Nr. 11 MAVO ein Vorgang, durch den Informationen über das Verhalten oder die Leistung von Mitarbeitenden erhoben und – jedenfalls in der Regel – aufgezeichnet werden, um sie auch späterer Wahrnehmung zugänglich zu machen.

Die Informationen müssen auf technische Weise ermittelt und dokumentiert werden, so dass sie zumindest für eine gewisse Dauer verfügbar bleiben und vom Dienstgeber herangezogen werden können. Die Überwachung muss durch die technische Einrichtung selbst bewirkt werden. Dazu muss diese aufgrund ihrer technischen Natur unmittelbar die Überwachung vornehmen. Das setzt voraus, dass die technische Einrichtung selbst und automatisch die Daten über bestimmte Vorgänge erhebt, speichert und/oder verarbeitet. Ausreichend ist, wenn lediglich ein Teil des Überwachungsvorgangs mittels einer technischen Einrichtung erfolgt. Auch reicht es aus, wenn die leistungs- oder verhaltensbezogenen Daten nicht auf technischem Weg durch die Einrichtung selbst gewonnen werden, sondern manuell eingegeben und von der technischen Einrichtung weiterverwertet werden.

Die IuK-Systeme werden von dem Dienstgeber folgenden Kategorien zugeordnet:

Kategorie I
IuK-Systeme, die technisch keine Leistungs- oder Verhaltensüberwachung ermöglichen (z. B. Erfassung nicht individualisierbarer Daten oder nur von Stammdaten).

Kategorie II
IuK-Systeme, die technisch dazu geeignet sind, das Verhalten oder die Leistung der Mitarbeitenden zu überwachen, deren Zweck eine solche Überwachung aber nicht ist (z. B. biometrische Zugangskontrollen).

Die Zuordnung hat der Dienstgeber in einer Liste zu dokumentieren und diese der MAV in jeweils aktueller Fassung zu übergeben.

7.2. IuK-Systeme der Kategorie I

IuK-Systeme der Kategorie I unterfallen nicht dem Anwendungsbereich des Mitbestimmungsrechts gemäß § 38 Abs. 1 Nr. 11 MAVO. Sie können daher von dem Dienstgeber ohne Beteiligung der MAV eingeführt und angewendet werden. Der Dienstgeber hat der MAV lediglich über die Einführung und Zuordnung zur Kategorie I zu informieren.

7.3. IuK-Systeme der Kategorie II

Zu jedem IuK-System der Kategorien II im Sinne dieser RDV, der bei dem Dienstgeber eingeführt werden soll, muss es eine entsprechende Anlage im **Anlagenteil 1** zu dieser RDV geben.

Die jeweilige Anlage hat Regelungen zu den folgenden Punkten zu beinhalten:

7.3.1. Geltungsbereich

In der Anlage ist konkret aufzuführen, für welche Bereiche das IuK-System eingesetzt werden soll.

7.3.2. Zuständigkeit MAV

Die Anlage hat eine Erklärung der Parteien dazu zu enthalten, ob das Mitbestimmungsrecht aus § 38 Abs. 1 Nr. 11 MAVO zu dem IuK-System in die Zuständigkeit der MAV fällt.

7.3.3. Beschreibung des IuK-Systems

Das IuK-System muss nach Hersteller, Produktname, Komponenten, Version und Datum der Version bezeichnet sein. Die nachträgliche Aufnahme von turnusmäßigen Updates im Sinne dieser RDV in die Anlage ist nicht erforderlich.

7.3.4. Zweck des IuK-Systems und Gegenstand der Anlage

Es muss beschrieben werden, zu welchem Zweck das IuK-System bei dem Dienstgeber eingesetzt werden soll.

Dabei ist insbesondere in der Anlage zu IuK-Systemen der Kategorie II aufzuführen, ob der Dienstgeber das IuK-System ausnahmsweise (auch) dazu verwenden darf, das Verhalten und die Leistung von Mitarbeitenden zu überwachen.

Für IuK-Systeme der Kategorie II, bei denen diese Verwendung zulässig ist, müssen Art und Umfang der zulässigen Verhaltens- und Leistungsüberwachung konkret beschrieben werden. In dem Fall muss in der Anlage auch aufgeführt sein, ob und ggf. in welchem Umfang Stichproben zur Verhaltens- und Leistungsüberwachung zulässig sind.

7.3.5. Besondere Regelungen

Hier sind die Regelungen aufzuführen, die speziell für das jeweilige IuK-System gelten sollen.

7.3.6. Laufzeit der Anlage

Die Anlage hat eine Vereinbarung über deren Laufzeit zu enthalten. Sie kann auf unbefristete Zeit oder nur für einen befristeten Zeitraum abgeschlossen werden. Es ist auch möglich, eine Mindestlaufzeit zu vereinbaren.

7.3.7. Eventuelle Testphase

Es kann in der Anlage eine Testphase vereinbart werden, nach deren Ablauf erst die endgültige Entscheidung über die Einführung des IuK-Systems zwischen den Parteien getroffen werden soll.

7.3.8. Umfang und Dauer der Verwertung von personenbezogenen Daten

In der Anlage wird definiert, wie lange personenbezogene Daten, die Aussagen zu Verhalten und Leistung ermöglichen, ausgewertet werden dürfen.

7.3.9. Kreis der auf Mitarbeiterdaten zugriffsberechtigten Organisationseinheiten/Stellen (Berechtigungskonzept)

Die Parteien haben für IuK-Systeme der Kategorie II in der Anlage namentlich aufzuführen, welche Organisationseinheiten und Funktionen bei dem Dienstgeber und gegebenenfalls welche externen Stellen/Unternehmen zu welchem Zweck Zugriff auf die personenbezogenen Daten haben. Nicht zu benennen sind externe Stellen/Personen, denen auf Grund gesetzlicher Verpflichtungen der Zugriff zu gewähren ist.

7.3.10. Dauer der Speicherung von personenbezogenen Daten (Löschungskonzept)

Die Parteien haben für IuK-Systeme der Kategorie II in der Anlage des Weiteren konkret zu regeln, nach welchem Zeitraum in dem IuK-System gespeicherte personenbezogene Daten zu löschen sind oder zumindest nur noch in anonymisierter Form gespeichert bleiben dürfen.

8. Verfahren zur Einführung neuer IuK-Dienste der Kategorie II

Die Einführung und die Anwendung eines neuen IuK-Systems der Kategorie II, für die die MAV zuständig ist, sind nur zulässig, wenn dies vorher unter Beachtung des nachfolgenden Verfahrens in einer entsprechenden Anlage zum Anlagenteil 1 dieser RDV vereinbart worden ist. Eine „Duldung" eines IuK-Systems der Kategorie II ist unzulässig.

Die Parteien vereinbaren zur Vereinbarung einer entsprechenden Anlage zum Anlagenteil 1 zu dieser RDV das folgende Verfahren:

8.1. Information des Dienstgebers an die MAV über ein beabsichtigtes neues IuK-System

Zunächst hat der Dienstgeber die MAV rechtzeitig darüber zu informieren, welches IuK-System der Kategorie II der Dienstgeber neu einsetzen möchte. Mit dieser Information verbunden wird der Antrag auf Zustimmung des Dienstgebers nach § 36 Abs. 1 Nr. 9 i.V.m. § 33 MAVO. Das weitere Verfahren ergibt sich aus den benannten §§ der MAVO.

9. Verfahren zu den bereits vorhandenen IuK-Systemen nach § 38 Abs. 1 Nr. 11 MAVO

9.1. Verfahren zu bereits bestehenden Dienstvereinbarungen zu IuK-Systemen nach § 38 Abs. 1 Nr. 11 MAVO

Die Parteien sind sich darüber einig, dass zum Zeitpunkt des Inkrafttretens dieser RDV die in der **Anlage 2** aufgeführten Dienstvereinbarungen zu IuK-Systemen nach § 38 Abs. 1 Nr. 11 MAVO bereits bestehen. Diese Dienstvereinbarungen gelten unverändert weiter. Die Regelungen dieser RDV gelten für diese Dienstvereinbarungen nicht.

Die Parteien haben jedoch die Möglichkeit, die in der Anlage 2 aufgeführten Dienstvereinbarungen durch Vereinbarung von Anlagen zum Anlagenteil 1 zu dieser RDV auf rein freiwilliger Basis einvernehmlich abzulösen. Mit der Vereinbarung der Anlage endet die Laufzeit der Dienstvereinbarung und wird durch die Anlage sowie diese RDV abgelöst.

Die Parteien vereinbaren zu einer möglichen Ablösung einer bestehenden Dienstvereinbarung das folgende Verfahren:

9.1.1. Anlage nach Punkt 7.3.

Der Dienstgeber hat das IuK-System einer Kategorie gem. Punkt 7.1. RDV zuzuordnen und eine Anlage zu entwerfen, welche die in Punkt 7.3. dieser RDV aufgeführten Informationen zu enthalten hat. Dabei berücksichtigt der Dienstgeber die Regelungen aus der bestehenden Dienstvereinbarung. Den Entwurf für eine Anlage übermittelt der Dienstgeber der MAV. Damit zu verbinden ist der dann

notwendige Antrag auf Zustimmung nach § 36 Abs. 1 Nr. 9 i.V.m. § 33 MAVO. Das weitere Verfahren ergibt sich aus den benannten §§ MAVO.

9.2. Verfahren zu den bereits vorhandenen IuK-Systemen nach § 38 Abs. 1 Nr. 11 MAVO, deren Betrieb die MAV bislang noch nicht zugestimmt hat

Soweit die MAV der Nutzung eines IuK-Systems der Kategorie II, den der Dienstgeber derzeit im Betrieb einsetzt, noch nicht durch Beschluss zugestimmt hat, ist die weitere Verwendung ohne Zustimmung der MAV unzulässig. Eine „Duldung" eines bestehenden IuK-Systems der Kategorien II ist unzulässig.

Die Nutzung dieser IuK-Systeme wird zulässig, wenn für sie das Verfahren nach den Punkten 7 und 8 dieser RDV durchlaufen wurde und eine Anlage für den Anlagenteil 1 vereinbart wird.

10. Ausschluss von Leistungs- und Verhaltenskontrollen

Die Parteien sind sich darin einig, dass sich die technischen Möglichkeiten zur Verhaltens- und Leistungskontrolle der Mitarbeitenden durch den Einsatz von IuK-Systemen der Kategorien II sprunghaft erhöhen können. Mit dem Einsatz von IuK-Systemen bezweckt der Dienstgeber aber weder eine Verhaltens- noch eine Leistungskontrolle der Mitarbeitenden. Vielmehr beschränkt sich der Einsatz von IuK-Systemen ausschließlich auf die in Ziffer 5 dieser RDV näher beschriebenen Ziele.

Unter Berücksichtigung dessen vereinbaren die Parteien Folgendes:

Die bei der Arbeit mit IT-Systemen anfallenden Daten dürfen nicht zum Zwecke der Leistungsmessung, des Leistungsvergleichs, der Leistungs- und/oder Verhaltenskontrolle verwendet werden. Eine solche Datennutzung ist den Mitarbeitenden, die Zugang zu diesen Daten haben, grundsätzlich untersagt. Personelle Maßnahmen des Dienstgebers, die unter Verletzung der getroffenen RDV angeordnet bzw. durchgeführt werden, sind unwirksam.

Soweit IT-Systeme Benutzerkennungen und/oder Aktivitäten der Benutzer aufzeichnen, dürfen diese neben den Möglichkeiten zur Eigenkontrolle nur

- zur Gewährleistung der Systemsicherheit,
- zur Analyse und Korrektur technischer Fehler in den Systemen,
- zur Steuerung und Optimierung der Systeme und
- zur Abrechnung verbrauchter Systemleistungen

benutzt werden. Die Zugriffsrechte auf die entsprechenden Funktionen bleiben auf den Personenkreis beschränkt, der mit der technischen Administration der Systeme betraut ist.

Daten über Leistung und Verhalten von Mitarbeitenden, die nicht ordnungsgemäß entsprechend den vorstehenden Absätzen gewonnen worden sind, dürfen arbeits- oder dienstrechtlichen Maßnahmen des Dienstgebers gegen GR/ PR nicht zugrunde gelegt werden. Solche Daten sind unverzüglich zu löschen, nachdem ihre Verarbeitung als unzulässig erkannt worden ist. Dabei ist nach den anzuwendenden datenschutzrechtlichen Bestimmungen zu verfahren.

11. Nutzung IP-gestützter Kommunikationsmittel

11.1 Pflichten der GR/ PR

Es gelten für den Umgang mit allen dienstlichen Informations- und Kommunikationssystemen die in den folgenden Absätzen genannten Verhaltensgrundsätze.

Unzulässig ist jede Nutzung der dienstlichen Informations- und Kommunikationssysteme, die die Interessen oder das Ansehen des Erzbistums Köln in der Öffentlichkeit aus der Sicht eines objektiven Dritten in erheblicher Weise nachhaltig verletzen oder gegen geltende Rechtsvorschriften verstoßen. Dies gilt insbesondere für das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.
Das Abrufen von Informationen für private Zwecke (z. B. durch Herunterladen, Streaming) auf Kosten des Erzbistums Köln ist unzulässig. Auch dürfen keine eigenen kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden.

11.2. Nutzung von E-Mail und Internetzugang durch GR/ PR

Der Zugang zu IP-geschützten Kommunikationsmitteln wie E-Mail, Chats, Foren, Intranet, Internet und sozialen Netzwerken etc. wird vom Dienstgeber als Arbeitsmittel zur Verfügung gestellt und ist an eine gesonderte Berechtigung gebunden. Die Nutzung des Internets wird in angemessenem Umfang auch zur privaten Nutzung gestattet, soweit hierdurch der Betriebsablauf nicht beeinträchtigt wird.

In Abweichung zu den Regelungen in Ziffer 10 dieser RDV gilt folgendes:
Bei begründetem, konkretem Verdacht auf eine missbräuchliche, insbesondere strafrechtlich relevante Nutzung von IT-Systemen im Bereich der GR/ PR wird die MAV informiert und beteiligt. Ein Protokollzugriff darf nur erfolgen, wenn die MAV und der betriebliche Datenschutzbeauftragte von der Absicht, die Protokolle zu nutzen, unterrichtet wurden und Gelegenheit hatten, den Zugriff zu überwachen. Werden auf diese Weise gewonnene Daten nicht genutzt, sind sie spätestens nach drei Monaten zu löschen. Die MAV wird über die Löschung informiert.

12. Weitergabe von personenbezogenen Daten an externe Stellen

12.1.Strafverfolgungs- und Ordnungsbehörden

Die Weitergabe von personenbezogenen Daten an Strafverfolgungsbehörden oder Ordnungsbehörden ist nur zulässig, soweit eine Weitergabe dieser Daten gesetzlich zulässig ist und ein eigenes rechtliches oder wirtschaftliches Interesse des Dienstgebers an der Strafverfolgung besteht.

Der Dienstgeber hat die MAV umgehend über die Anfrage der Strafverfolgungs- oder Ordnungsbehörde zu informieren.

12.2.Andere externe Stellen (z.B. Kirchengemeinden, Krankenhäuser, Justizvollzugsanstalten)

Eine Weitergabe von personenbezogenen Daten an externe Stellen außerhalb des Dienstgebers ist zulässig, soweit dies in Punkt 7.3.9. dieser RDV vereinbart worden ist oder dies auf Grund von gesetzlichen Vorschriften erforderlich ist oder der betroffene Mitarbeitende dies wünscht.

13.Änderungen an den IuK-Systemen

13.1.
Änderungen an den IuK-Systemen der Kategorie II bedürfen der vorherigen Zustimmung der MAV, soweit hierdurch die technischen Möglichkeiten einer Leistungs- und Verhaltenskontrolle objektiv erweitert werden. Die Zustimmung erfolgt durch die Vereinbarung einer geänderten Anlage zum Anlagenteil 1. Hierfür gilt das Verfahren zu Punkt 9 entsprechend.

13.2.
Erweiterungen und/oder Veränderungen bestehender IuK-Systeme, insbesondere Software-Updates und der Austausch technischer Geräte, die die Eignung, das Verhalten und die Leistung der Mitarbeitenden zu überwachen, nicht verändern, insbesondere, weil die erhobenen personenbezogenen Daten sowie deren Verarbeitung nicht verändert werden, darf der Dienstgeber ohne vorherige Zustimmung der MAV vornehmen. Die MAV ist jedoch vor der Änderung zu unterrichten. Jede Änderung und der Inhalt der Änderung ist zu dokumentieren.

14. Rechte der MAV

14.1.
Die MAV erhält jederzeit aktuelle Auszüge aus den Verzeichnissen von Verarbeitungstätigkeiten. Der aktuelle Inhalt dieser Auszüge ergibt sich aus dem **Anlagenteil 3**.

14.2.
Die MAV hat das Recht, sich bei allen IuK-Systemen der Kategorien II jederzeit in Begleitung einer zur Administration dieser Einrichtung berechtigten Person mit Administratorrechten anzumelden, um die Funktion und die Einhaltung dieser RDV zu überprüfen. Die Überprüfung erfolgt durch die MAV.

14.3.
Die MAV erhält die Möglichkeit, unter den Voraussetzungen des § 17 MAVO einen Sachverständigen hinzuzuziehen, der ihn bei der Beurteilung und Kontrolle der Einhaltung dieser RBV unterstützt.

15. Datenschutz

15.1. Verarbeitung von Daten

Die Verarbeitung von personenbezogenen Daten erfolgt ausschließlich zu den in dieser RDV sowie den Anlagen genannten Zwecken.
Personenbezogene Daten, die zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke gem. § 6 Abs. 5 KDG verwendet werden. 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 Verarbeitung von personenbezogenen Daten ist zulässig, soweit diese RDV nebst Anlagen und das KDG sie erlauben oder soweit sie aufgrund gesetzlicher Vorschriften zur Durchführung des Arbeitsverhältnisses oder Sicherung der Einhaltung von Rechten und Pflichten aus dem Arbeitsverhältnis oder zur Feststellung der Eignung für eine vorgesehene Tätigkeit erforderlich ist.

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 Sperrfriste 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 erfolgen. Hierbei sind Art und Zweck des Zugriffs genau zu bestimmen.

Eine Veränderung dieser Zwecke bedarf der vorherigen schriftlichen Zustimmung der MAV.

Die Daten bzw. Datenkategorien, die verarbeitet werden sollen, sind in der jeweiligen gesonderten Anlage zu dem Einsatz eines IuK-Systems im Einzelnen zu beschreiben.

Die personenbezogenen Daten der Mitarbeitenden bleiben jeweils nur so lange gespeichert, bis die Voraussetzungen für ihre Löschung gem. Ziffer 15.7. der RDV vorliegen.

Soweit die Verarbeitung personenbezogener Daten nicht notwendig ist, sind die Daten in anonymer Form zu verwenden. Als anonym gilt eine Auswertung, in der keine personenidentifizierbaren Daten enthalten sind, wie z. B. Namen, Geburtsdaten, Personalnummern, dienstliche Telefonnummern, Adressen. Rückverfolgungen anonymer Auswertungen auf Einzelpersonen oder individualisierbare Gruppen sind nicht gestattet.

Sofern die Verarbeitung der personenbezogenen Daten oder die Erbringung von anderen Leistungen durch Dritte i. S. d. KDG erfolgt, wird der Dienstgeber mit geeigneten Mitteln dafür Sorge tragen, dass die hier getroffenen Regelungen auch von diesen Dritten eingehalten werden, unabhängig von deren Standort.

Nicht in den Anlagen oder in dieser RDV benannte personenbezogene Daten dürfen nicht ohne eine entsprechende vorherige einvernehmliche Regelung mit der MAV verarbeitet werden.

15.2. Wahrung des Seelsorgegeheimnisses

Insbesondere Daten, die dem Beicht- und Seelsorgegeheimnis unterliegen, sind personenbezogene Daten, die in einem hohen Maße schutzbedürftig sind. Personenbezogene Daten, die sich aus dem Beichtgeheimnis ergeben, dürfen nicht verarbeitet werden. Personenbezogene Daten aus dem Seelsorgegeheimnis unterliegen einem hohen Schutzniveau und dürfen nur bei besonderer Würdigung unter Berücksichtigung besonderer technischer und organisatorischer Maßnahmen verarbeitet werden.

15.3. Dateiablage/ Struktur

In der Regel erfolgt die Dateiablagestruktur orientiert am Rahmenaktenplan des Erzbistums Köln. Vorerst wird eine Ablage je Seelsorgebereich beibehalten, um flexibel auf die größer werdenden pastoralen Einheiten reagieren zu können. Damit bleibt die Berechtigungsverwaltung flexibel bei Versetzung eines GR/ PR in einen anderen Seelsorgebereich.

15.4. Zugriffs- und Berechtigungskonzept (Zugriffe externer Personen, Dienstleister etc., Abgrenzung Zugriffe vor Ort und EGV)

Berechtigungen werden gemäß den Inhalten des Berechtigungskonzeptes in den beschriebenen Verfahren der jeweiligen Einzeldienstvereinbarungen zwischen dem Dienstgeber und der MAV vereinbart. Sie sind in den Anhängen zu den Einzeldienstvereinbarungen abschließend funktionsbezogen aufzuführen. Nachträgliche Änderungen sind durch den Dienstgeber sind nur zulässig, wenn sie vorher zwischen den Parteien (Dienstgeber und MAV) in einer Ergänzung zu dieser RDV vereinbart worden sind.

Die MAV erhält jeweils eine aktuelle Übersicht auf die relevanten Berechtigungen in den einzelnen Dienstvereinbarungen.

Eine Änderung bzw. Neueinrichtung von Zugriffsberechtigungen ist erst nach einer Vereinbarung zwischen Dienstgeber und der MAV im Sinne von Ziffer 15.4, erster Absatz von den zuständigen Vorgesetzten schriftlich oder textlich (per E-Mail) den Administratoren unter Angabe der Funktion und des Arbeitsfeldes des betroffenen Users anzuweisen. Eine Einrichtung bzw. Änderung auf Zuruf ist untersagt. Die Einrichtung der Zugriffsberechtigungen erfolgt nach dem Vier-Augen-Prinzip. Den Administratoren werden die berechtigten Vorgesetzten ebenfalls schriftlich bekannt gegeben.

Die Liste der berechtigten Administratoren, die im System oder in Einzelanwendungen Administratorenrechte besitzen, wird in der Abteilung Informationstechnologie des Erzbischöflichen Generalvikariates namentlich aktuell hinterlegt und ist jederzeit einsehbar. Änderungen sind unter Beachtung der Regelungen in Punkt 15.4 unverzüglich einzupflegen.

15.5. Benutzerkennung und Passwort

Zur erstmaligen Benutzung der Hardware werden Benutzername und Startkennwort genutzt, die über den Dienstleister ausgegeben werden.

Veränderte Umstände und gewachsene Anforderungen an die IT-Sicherheit bedingen, dass die gewohnten **Anforderungen an die Windows-Kennwörter an die Empfehlungen des Bundesamtes für Sicherheit und Informationstechnik** angepasst worden sind. Das bedeutet, dass das Kennwort in Zukunft nur noch **alle 365 Tage geändert** werden muss, da ein komplexes Kennwort, welches lange gilt, sicherer ist als ein nicht komplexes Kennwort, das alle 90 Tage geändert wird.

Es gelten nachfolgende Konventionen:

- Die Mindest-Kennwortlänge beträgt 8 Zeichen.
- Das Kennwort enthält Zeichen aus drei der folgenden Kategorien, um als komplex akzeptiert zu werden.
- **Großbuchstaben** europäischer Sprachen (A bis Z, mit diakritischen Zeichen, griechischen und kyrillischen Zeichen)
- **Kleinbuchstaben** europäischer Sprachen (a bis z, mit diakritischen Zeichen, griechischen und kyrillischen Zeichen)
- **Basis 10 Ziffern** (0 bis 9)
- **Nicht alphanumerische Zeichen** (Sonderzeichen):

15.6. Datenschutzerklärung und notwendige Voraussetzungen (Verpflichtungserklärung, Onlineschulungen etc.)

Der Dienstgeber weist auf Folgendes hin:

Der Dienstgeber beabsichtigt, dass alle GR/ PR, die Zugriff auf personenbezogene Daten haben, sowie alle Mitarbeitenden des Erzbistums Köln einschließlich der DV-Dienstleister hinsichtlich des Datenschutzes und aller diesbezüglich relevanten Vorschriften geschult werden und nach erfolgter Schulung eine gesonderte Verpflichtung unterzeichnen sollen. Die erfolgreiche Teilnahme an der Online-Schulungsmaßnahme sowie deren wesentlichen Inhalte sind den GR/ PR schriftlich zu bestätigen.

Im Übrigen sieht das Kirchliche Datenschutz-Gesetz (KDG) in Kombination mit der dazu seit dem 08.01.2019 in Kraft getretenen Durchführungsverordnung (KDG-DVO) Maßnahmen vor, mit denen Mitarbeiterinnen und Mitarbeiter über die Inhalte und Vorschriften des KDG im notwendigen Maß unterrichtet werden.

Hierzu hat das Erzbistum Köln eine Schulung zum kirchlichen Datenschutz vorbereitet. Um darüber hinaus der Nachweispflicht gegenüber der Aufsichtsbehörde nachkommen zu können, wurde diese Schulung als *Pflichtschulung* konzipiert. Es handelt sich um eine Online-Schulung, die sich unter dem folgenden Link https://datenschutz.erzbistum-koeln.de/ findet. Die Zugangsdaten werden gesondert über die Hauptabteilung Seelsorge-Personal zugänglich gemacht. Im Anschluss daran beabsichtigt der Dienstgeber, dass die Mitarbeitenden eine Verpflichtungserklärung KDG und DV-IT ausfüllen, die dann in die Personalakte der GR/ PR verfügt werden:

15.7. Löschung von personenbezogenen Daten (Löschungskonzept)

15.7.1.
Personenbezogene Daten sind von dem Dienstgeber zu löschen, wenn sie für die Zwecke, für die sie verarbeitet wurden, nicht mehr erforderlich sind. Dies ist der Fall, wenn die Daten zur Erfüllung des Zwecks der Erhebung oder Speicherung sowie im Zusammenhang mit der Erfüllung gesetzlicher, kollektivvertraglicher oder einzelvertraglicher Verpflichtungen bzw. der Durchsetzung entsprechender Rechte nicht mehr benötigt werden.

Um der gesetzlichen Verpflichtung und dem Recht auf Löschung gem. § 19 KDG Rechnung zu tragen, hat der Arbeitgeber zu einem IuK-Dienst in der Anlage zum Anlagenteil 1 im Sinne von Punkt 7.3.10. ein Löschungskonzept im Hinblick auf die jeweilige konkrete Verarbeitung personenbezogener Daten der Mitarbeitenden zu erstellen, um – soweit technisch möglich und zumutbar – durch Maßnahmen der Gestaltung der IT-Systeme selbst die definierten Löschvorgänge unter Einhaltung der gesetzlichen Aufbewahrungspflichten und -rechte automatisch durchzuführen. Soweit eine Löschung technisch nicht möglich ist, werden die Daten vor jedem Zugriff gesperrt.

15.7.2.
Daneben sind personenbezogene Daten, wenn sie auf Grundlage einer Einwilligung des Betroffenen erhoben und verarbeitet wurden, nach dem Widerruf der Einwilligung zu löschen, wenn nicht die Verarbeitung aufgrund eines anderen Zweckes zulässig und notwendig ist.

16. Anspruch auf Information und Schulung der Mitarbeitenden

Die Mitarbeitenden werden vor Aufnahme der Arbeit mit neuen grundlegenden Anwendungen und/oder Arbeitsmitteln entsprechend eines mit der MAV abzustimmenden, in Art und Umfang angemessenen Qualifizierungskonzeptes geschult. Darunter sind auch zu verstehen verschiedene Online-Angebote, Webinare und Lernvideos etc. Die Qualifizierungsmaßnahmen werden durch entsprechende Angebote kontinuierlich fortgeführt.

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.

Die Schulungsmaßnahmen gelten als Arbeitszeit. Die Kosten der Schulungsmaßnahmen trägt der Dienstgeber.

17. Arbeitsschutz

17.1. Arbeitsschutzmaßnahmen – Pflichten des Dienstgebers im 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 mit dem zurzeit eingesetzten Dienstleister des betrieblichen Arbeitsschutzes, der B.A.D. GmbH, 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 Anwendungen. Hier muss die Umsetzung der Anforderungen bereits bei Auftragsvergabe gewährleistet sein.

17.2. Gestaltung von Arbeitsplätzen, Ergonomie

Eine Überprüfung der Arbeitsplätze und Arbeitsmittel erfolgt auf Antrag des einzelnen GR/ PR und der MAV in Zusammenarbeit mit der Fachkraft für Arbeitssicherheit und dem Betriebsarzt. Das Protokoll dieser Überprüfung wird auf den Verantwortlichen, dem die Übertragung der Unternehmerpflichten zum Arbeitsschutz übertragen worden sind und der Koordinierungsstelle für den Arbeitsschutz im Erzbistum Köln übergeben, die dann ggf. den Dienstgeber hinzuzieht. Die Beseitigung etwaiger Mängel ist unverzüglich durch die Koordinierungsstelle für Arbeitsschutz im Erzbistum Köln in Absprachen mit dem Dienstgeber umzusetzen.

17.3. Abgrenzung dienstliche und private Arbeitsbereiche

Grundsätzlich dient die IT-Ausstattung rein dienstlichen Zwecken. Eine Öffnung ist ausschließlich in dem unter Punkt 11.2 und benannten restriktiven Umfang zulässig.

18. Meinungsverschiedenheiten

Meinungsverschiedenheiten, die aus der Auslegung oder Durchführung dieser RDV entstehen, sind durch Verhandlungen zwischen dem Dienstgeber und der MAV zu regeln.

Sollten die vertragsschließenden Parteien bei Meinungsverschiedenheiten zu keiner Einigung über die Auslegung dieser RDV kommen, entscheidet die Einigungsstelle verbindlich.

19. Inkrafttreten der Dienstvereinbarung und salvatorische Klausel

Diese Rahmendienstvereinbarung tritt zum 15. Juni 2022 in Kraft und ersetzt die RDV vom 15.05.2021.

Sie kann von den Parteien mit einer Frist von 3 Monaten zum Monatsende gekündigt werden, frühestens jedoch zum 31.12.2023. 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.

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