Amtsblatt des Bistums Limburg

KATHOLISCHE KIRCHE BISTUM LIMBURG

Nr. 4 **Limburg, 1. April 2026**

Der Apostolische Stuhl

Nr. 35 Botschaften von Papst Leo XIV.

Papst Leo XIV. hat mehrere Botschaften veröffentlicht:

1. Botschaft zum 60. Welttag der sozialen Kommunikationsmittel: https://www.vatican.va/content/leo-xiv/de/messages/communications/documents/20260124-messaggio-comunicazioni-sociali.html
2. Botschaft zum 40. Weltjugendtag: https://www.vatican.va/content/leo-xiv/de/messages/youth/documents/20251007-messaggio-xl-gmg.html
3. Botschaft zum 63. Weltgebetstag um geistliche Berufungen 2026: https://www.vatican.va/content/leo-xiv/de/messages/vocations/documents/20260316-messaggio-vocazioni.html

Der Bischof von Limburg

Nr. 36 Aufruf der deutschen Bischofe zur Pfingstaktion Renovabis 2026

Liebe Schwestern und Brüder,

viele Länder in Mittel-, Ost- und Südosteuropa stehen vor großen Herausforderungen: Politische Polarisierung, wirtschaftliche Unsicherheit, soziale Spannungen sowie die Erfahrungen von Gewalt, Krieg und Flucht belasten den gesellschaftlichen Zusammenhalt. Vor diesem Hintergrund stellt Renovabis die diesjährige Pfingstaktion unter das Leitwort „zusammenwachsen, damit Europa menschlich bleibt".

Die Kirchen im Osten Europas sind in diesem Sinne engagiert. Durch soziale Hilfen, Bildungsangebote, Versöhnungsinitiativen und die Förderung des interreligiösen Dialogs bauen sie Brücken über Gräben und Grenzen hinweg.

Pfingsten erinnert uns daran, dass der Heilige Geist Menschen zusammenführt. Seine Gaben, um die wir heute besonders bitten, stiften Gemeinschaft. Die Welt braucht diesen Geist der Solidarität und der Ver-

bundenheit dringend. So bitten wir Sie herzlich: Unterstützen Sie die wichtige Arbeit von Renovabis durch Ihre großzügige Spende und Ihr Gebet.

Kollektenankündigung am Pfingstsonntag, 24. Mai 2026

Die heutige Kollekte ist für die Arbeit von Renovabis bestimmt. Dessen Projektpartner fördern durch soziale Hilfen, vielfältige Bildungsangebote sowie Dialog- und Versöhnungsinitiativen den gesellschaftlichen Zusammenhalt in den Ländern Mittel-, Ost- und Südosteuropas.

Herzlichen Dank für Ihre Unterstützung!

Würzburg, 26. Februar 2026 + Dr. Georg Bätzing
Für das Bistum Limburg Bischof von Limburg

Dieser Aufruf soll am Sonntag, 17. Mai 2026, in allen Gottesdiensten (auch am Vorabend) verlesen und den Gemeinden zudem in geeigneter anderer Weise bekannt gemacht werden. Die Kollekte am Pfingstsonntag, 24. Mai 2026, ist ausschließlich für die Solidaritätsaktion Renovabis bestimmt.

Limburg, 10. März 2026 Dr. Wolfgang Pax
Az.: 608B/47384/26/01/1 Generalvikar

Nr. 37 Aufruf der deutschen Bischöfe zum Sonntag der Weltmission 2026

Liebe Schwestern und Brüder,

„Sei mutig und stark" — dieses Wort aus dem Buch Josua (1,6) steht über dem Sonntag der Weltmission 2026. Es lenkt unseren Blick nach Madagaskar, wo viele Menschen jeden Tag mutig und stark um das Nötigste ringen müssen: um Nahrung, um medizinische Hilfe, um Bildung für die Kinder.

Die Kirche in Madagaskar unterstützt sie dabei. Besonders in den ländlichen Gebieten ist sie oft die einzige Institution, die soziale und medizinische Dienste oder Bildungsmöglichkeiten anbietet. Sie ermutigt die Menschen auch, selbst für eine bessere Zukunft ihres Landes zu kämpfen. Zugleich stärkt sie die Christen in ihrem Glauben.

Seit 100 Jahren erinnert uns der Sonntag der Weltmission daran, dass wir Christinnen und Christen weltweit zusammengehören. Das Hilfswerk Missio ist dieser globalen Solidarität verpflichtet. Bitte unterstützen Sie die wichtige Arbeit von Missio und seinen Projektpartnern. Helfen Sie mit, dass sich die Kirche in Madagaskar und in anderen Ländern dieser Welt für die Armen und Benachteiligten engagieren kann.

Kollektenankündigung am Sonntag der Weltmission 2026, 25. Oktober 2026

Die heutige Kollekte ist für die Arbeit von Missio bestimmt. Das Hilfswerk unterstützt die Kirche in Afrika, Asien und Ozeanien. Es geht dabei um pastorale und soziale Projekte, die insbesondere den Armen zugutekommen. Bitte beteiligen Sie sich an dieser weltweiten Solidaritätsaktion mit einer großzügigen Spende. Haben Sie herzlichen Dank!

Würzburg, 26. Februar 2026 + Dr. Georg Bätzing
Für das Bistum Limburg Bischof von Limburg

Dieser Aufruf am Sonntag, 18. Oktober 2026, in allen Gottesdiensten (auch am Vorabend) verlesen und den Gemeinden zudem in geeigneter anderer Weise bekannt gemacht werden. Die Kollekte am Weltmissionssonntag, 25. Oktober 2024, ist ausschließlich für die Päpstlichen Missio-Werke in Aachen und München bestimmt.

Limburg, 10. März 2026 Dr. Wolfgang Pax
Az.: :367J/16755/26/01/1 Generalvikar

Nr. 38 Aufruf der deutschen Bischöfe zum Diaspora-Sonntag 2026

Liebe Geschwister im Glauben,

„Geht hinaus in die ganze Welt und verkündet das Evangelium der ganzen Schöpfung!" (Mk 16,15). Dieser Sendungsauftrag Jesu gilt auch uns: Wir alle sind eingeladen, den christlichen Glauben in der heutigen Welt zu verkünden und zu bezeugen.

Das Bonifatiuswerk der deutschen Katholiken greift den Auftrag mit der diesjährigen Diaspora-Aktion auf. Sie steht unter dem Leitwort „Glauben bezeugen — Hoffnung teilen". Denn dort, wo wir über den Glauben sprechen und solidarisch handeln, machen wir die christliche Hoffnung erfahrbar. Dies ist ein Grundanliegen des Bonifatiuswerkes, das katholische Gläubige in Minderheitensituationen unterstützt. So fördert das Hilfswerk jährlich mehr als 1.000 Projekte in Nordeuropa, im Baltikum und in den katholischen Diaspora-Regionen Deutschlands.

Wir bitten Sie zum Diaspora-Sonntag am 15. November 2026 herzlich um Ihr Gebet und Ihre Spende für die Arbeit des Bonifatiuswerkes.

Kollektenankündigung am Diasporasonntag, 15. November 2026

Die heutige Kollekte ist für das Bonifatiuswerk der deutschen Katholiken bestimmt und dient der Unterstützung von kirchlichen Projekten in Nordeuropa, im Baltikum und in den katholischen Diaspora-Regionen Deutschlands. Bitte tragen Sie mit Ihrem Beitrag zur Kollekte dazu bei, dass die Kirche in der Diaspora die frohmachende Botschaft überzeugend verkünden kann. Herzlichen Dank!

Würzburg, 26. Februar 2026 + Dr. Georg Bätzing
Für das Bistum Limburg Bischof von Limburg

Dieser Aufruf soll am Sonntag, 8. November 2026, in allen Gottesdiensten (auch am Vorabend) verlesen oder den Gemeinden in geeigneter anderer Weise bekannt gemacht werden. Die Kollekte am Diaspora-Sonntag, 15. November 2026, ist ausschließlich für das Bonifatiuswerk der deutschen Katholiken bestimmt.

Limburg, 25. März 2024 Dr. Wolfgang Pax
Az.: 362A/38663/26/01/1 Generalvikar

Nr. 39 Beschluss der Regionalkommission Mitte am 18. Dezember 2025 in Mainz – Übernahme der beschlossenen mittleren Werte/abweichende Festsetzung der Arbeitszeit und des Erholungsurlaubs

Die Regionalkommission Mitte beschließt:

IV. Übernahme der beschlossenen mittleren Werte /abweichende Festsetzung der Arbeitszeit und des Erholungsurlaubs

1. Für den Bereich der Regionalkommission Mitte werden die mittleren Werte, die im Beschluss der Bundeskommission der Arbeitsrechtlichen Kommission vom 9. Oktober 2025 zur „AVR in der Fassung ab dem 1. Januar 2027 (AVR (2027))“ enthalten sind, in derselben Höhe und zu denselben Zeitpunkten als neue Werte festgesetzt. Es gelten folgende Abweichungen:
   a) Für Mitarbeiter in Krankenhäusern wird der Umfang der regelmäßigen Arbeitszeit gemäß § 15 Abs. 1 Satz 1 der ab 1. Januar 2027 geltenden Fassung der AVR im Zeitraum vom 1. Januar 2027 bis 31. Dezember 2028 auf durchschnittlich 39 Stunden wöchentlich festgesetzt. Damit gilt ab dem 1. Januar 2029 für Mitarbeiter in Krankenhäusern für den Umfang der regelmäßigen Arbeitszeit gemäß § 15 Abs. 1 Satz 1 AVR durchschnittlich 38,5 Stunden wöchentlich.

   b) In § 45 der ab 1. Januar 2027 geltenden Fassung der AVR wird folgender neuer Absatz 2a eingefügt:
   „(2a) (RK Mitte): [1]Mitarbeiter in Krankenhäusern erhalten zusätzlich zur Dauer des Erholungsurlaubs nach Absatz 1 in den Kalenderjahren 2027 und 2028 jeweils zwei weitere Arbeitstage Erholungsurlaub. [2]Infolgedessen erhöhen sich für sie die Höchsturlaubstage nach § 47 Abs. 7 Sätze 2 und 3 um zwei Arbeitstage.“

II. Inkrafttreten

Die Änderungen treten am 18. Dezember 2025 in Kraft.

Regelungsziel und wesentlicher Inhalt:

Der Beschluss beinhaltet im Wesentlichen die Übernahme des Beschlusses der Bundeskommission zur Neufassung der AVR-Caritas ab dem 1. Januar 2027. Damit werden die Höhe der Vergütungswerte, der Umfang der regelmäßigen Arbeitszeit und der Umfang des Erholungsurlaubs für den Geltungsbereich der Regionalkommission Mitte festgesetzt.

Hintergrund ist das geeinte Vorhaben der Regionalkommission Mitte, den Umfang der regelmäßigen Arbeitszeit für Mitarbeiter in Krankenhäusern auf durchschnittlich 39 Stunden wöchentlich festzusetzen. Die im Vergleich zum mittleren Wert erhöhte Festsetzung des zusätzlichen Erholungsurlaubs sind als Ausgleich für die erhöhte Arbeitszeit zu betrachten.

Die Regionalkommission ist für die Festlegung der Höhe aller Vergütungsbestandteile, des Umfangs der Arbeitszeit und des Umfangs des Erholungsurlaubs zuständig gemäß § 13 Abs. 3 Satz 1 AK-Ordnung.

Für das Bistum Limburg

Limburg, 25. Februar 2026 + Dr. Georg Bätzing
Az.: 359H/69659/26/01/4 Bischof von Limburg

Prof. Dr. Peter Platen, Kanzler der Kurie

Nr. 40 Beschluss der KODA vom 22. Januar 2026 – Anlage 15 zur AVO-Ordnung zur Fort- und Weiterbildung von Beschäftigten im Bistum Limburg

Die Fort- und Weiterbildungsordnung wird wie folgt neu gefasst:

Ordnung zur Fort- und Weiterbildung von Beschäftigten im Bistum Limburg

§ 1 Geltungsbereich

Diese Ordnung zur Fort- und Weiterbildung gilt für alle Beschäftigten im Sinne des § 2 Absatz 1 der Arbeitsvertragsordnung für die Beschäftigten im kirchlichen Dienst in der Diözese Limburg sowie für die Beschäftigten im Sinne des § 2 Absatz 1 AVO, die sich in der Elternzeit nach dem Bundeselterngeld- und Elternzeitgesetz oder im Sonderurlaub für Beschäftigte im kirchlichen Dienst des Bistums Limburg befinden.

§ 2 Begriffsbestimmungen

(1) Fortbildung dient der Erhaltung, Vertiefung und Verbesserung der zur Wahrnehmung im Aufgabenfeld erforderlichen Qualifikation. Sie macht folglich mit neueren Entwicklungen und Erkenntnissen vertraut und ergänzt und aktualisiert die in der praktischen Tätigkeit gesammelten Erfahrungen.

(2) Fortbildung als längerfristige und umfassende Vertiefung und Erweiterung der beruflichen Kompetenz setzen in der Regel eine mehrjährige Berufserfahrung nach Abschluss der Ausbildung voraus.

(3) Weiterbildung erfasst Bildungsveranstaltungen der allgemeinen, der theologischen, der politischen oder sonstiger Bildung, die nicht unmittelbar für das übertragene Aufgabenfeld geeignet sind.

(4) Abordnungen umfassen berufliche Qualifikationen, die für das übertragene Aufgabenfeld erforderlich sind[1].

§ 3 E-Learning/Blended-Learning

E-Learning und Blended-Learning sind präsentischen Qualifizierungsmaßnahmen gleichgestellt.

§ 4 Mindestbeschäftigungszeit

Der Anspruch auf Fort- und Weiterbildung entsteht grundsätzlich erstmals nach sechs Monaten nach Beginn des Arbeitsverhältnisses.

§ 5 Antragsverfahren

Anträge sind in der Regel spätestens sechs Wochen vor Beginn der Veranstaltung dem unmittelbaren Dienstvorgesetzten vorzulegen. Der unmittelbare Dienstvorgesetzte leitet den Antrag an die zuständige Stelle des Arbeitgebers weiter.

Der Arbeitgeber hat die Mitwirkung der MAV nach der Mitarbeitervertretungsordnung durchzuführen. Landesrechtliche Regelungen zu Bildungsveranstaltungen bleiben unberührt.

§ 6 Kostenbeteiligung und -abrechnung

Die Beteiligung des Arbeitgebers an den Kosten einer Fortbildung erfolgt im Rahmen der im Haushaltsplan zur Verfügung gestellten Mittel. Bei Bewilligung der Anträge werden diejenigen Beschäftigten vorrangig berücksichtigt, die in den vorhergehenden Jahren an keiner vom Arbeitgeber geförderten Veranstaltung teilgenommen haben. Für die Geltendmachung der Kostenerstattung gilt nach vollständigem Abschluss der Maßnahme eine Ausschlussfrist von sechs Monaten.

§ 7 Fortbildungsanspruch und Kostenerstattung

(1) Der Fortbildungsanspruch beträgt im Jahr fünf Tage. Wird regelmäßig an mehr als fünf Tagen in der Woche gearbeitet, beträgt der Anspruch sechs Tage. Die Zeit der Fortbildung einschließlich der Reisezeit gilt als Arbeitszeit.

(2) Dauert die Veranstaltung sechs oder mehr Unterrichtsstunden pro Tag, wird ein Tag auf den Fortbildungsanspruch angerechnet. Bei Veranstaltungen die weniger als sechs Unterrichtsstunden pro Tag dauern, werden 0,5 Tage auf den Fortbildungsanspruch angerechnet.

(3) Ob eine Aufnahme der Arbeit in der Betriebsstätte vor Beginn oder nach Ende der Veranstaltung ökonomisch sinnvoll ist, ist im Vorhinein zwischen Beschäftigtem und Dienstvorgesetzten zu klären. Ist dies nicht sinnvoll, wird die per-

[1] Artikel 5 Abs. 2 der Grundordnung vom 22. November 2022 sind als Abordnungen im Sinne § 2 Abs. 4 zu handhaben.

sönliche Sollzeit für diesen Tag als Arbeitszeit angerechnet.

(4) Der Fortbildungsanspruch aus dem Vorjahr kann in beiderseitigem Einvernehmen im laufenden Kalenderjahr genommen werden. Der Fortbildungstag wird im Krankheitsfall arbeitsrechtlich wie Erholungsurlaub behandelt.

(5) Den Beschäftigten werden die Bruttogesamtkosten einer Fortbildungsmaßnahme bis zu 500,00 € pro Kalenderjahr erstattet.

(6) Die Fahrtkosten zur in der Regel einmaligen An- und Abreise werden nach der Reisekostenordnung (RKO) erstattet.

§ 8 Dienstbefreiung und Kostenerstattung für längerfristige und umfassende Vertiefung und Erweiterung der beruflichen Kompetenz

(1) Voraussetzung für die Förderung einer solchen Maßnahme ist, dass die Antragstellerin/der Antragsteller sich bereit erklärt, die dadurch erworbenen Fähigkeiten in den kirchlichen Dienst einzubringen.

(2) Es soll ein Fortbildungsvertrag geschlossen werden.

(3) Dienstbefreiung und Kostenerstattung werden in der Regel zu zwei Dritteln vom Arbeitgeber und zu einem Drittel vom Antragsteller getragen.

§ 9 Dienstbefreiung für Weiterbildung

(1) Dienstbefreiung kann nur für eine Weiterbildungsveranstaltung pro Kalenderjahr geltend gemacht werden. Die Dienstbefreiung für Weiterbildung beträgt pro Jahr fünf Werktage. Wird regelmäßig an mehr als fünf Tagen in der Woche gearbeitet, so beträgt die Dienstbefreiung sechs Werktage.

(2) Für Weiterbildungen werden keine Kosten erstattet.

(3) Eine Übertragung der vorgesehenen Dienstbefreiung auf ein anderes Kalenderjahr ist nicht möglich. Der Weiterbildungstag wird im Krankheitsfall arbeitsrechtlich wie Erholungsurlaub behandelt.

§ 10 Abordnungen

(1) Abordnungen umfassen berufliche Qualifikationen, die für das übertragene Aufgabenfeld erforderlich sind. Dabei ist zu unterscheiden zwischen operativ und strategisch bedingten Abordnungen.

Operative Abordnungen beziehen sich auf bereits tatsächlich auf Beschäftigte übertragene Tätigkeiten und werden vom Dienstvorgesetzten angeordnet.

Strategische Abordnungen beziehen sich auf zukünftig auf Beschäftigte zu übertragene Tätigkeiten im Interesse des Arbeitgebers.

(2) Alle entstehenden Kosten werden übernommen. Die Teilnahme an Abordnungen gilt einschließlich der Reisezeiten als Arbeitszeit.

(3) Bei strategischen Abordnungen ist ein Vertrag mit Rückzahlungsklausel nach dem jeweils gültigen Muster der Anlage zu dieser Ordnung zu schließen.

§ 11 Anrechnungen

(1) Eine Freistellung als Weiterbildung wird auf Freistellungen für Fortbildung angerechnet, ebenso umgekehrt.

(2) Die Förderungsansprüche nach § 7 dieser Ordnung sind auf den Zeitraum und die Kosten nach § 8 anzurechnen und hierdurch abgegolten.

(3) Der gesetzliche Anspruch auf Bildungsurlaub ist bei Inanspruchnahme auf den Freistellungsanspruch für Weiterbildung anzurechnen. Der Anspruch auf Fortbildung bleibt hiervon unberührt.

Diese Ordnung tritt zum 1. März 2026 in Kraft und ersetzt die bisherige Ordnung vom 4. Mai 2005.

Limburg, 19. Februar 2026 + Dr. Georg Bätzing
Az.: 565AH/62656/26/03/1 Bischof von Limburg

Bischöfliches Ordinariat

Nr. 41 Hinweise zur Durchführung der Renovabis-Pfingstaktion 2026

Das Osteuropa-Hilfswerk Renovabis rückt in seiner Pfingstaktion 2026 unter dem Leitwort „zusammenwachsen“ damit Europa menschlich bleibt“ den gesellschaftlichen Zusammenhalt in den Fokus.

Renovabis unterstützt in 29 Ländern im Osten Europas zahlreiche Projekte – nicht zuletzt mit den Mitteln der Pfingstkollekte und mit Spenden. Gefördert werden pastorale und soziale Projekte von Partnern vor Ort. Diese eröffnen den Menschen und der Kirche Perspektiven und lindern Not. Auf diese Weise wird auch der Zusammenhalt in den Gesellschaften gestärkt.

Die bundesweite Eröffnung der Pfingstaktion ist am Sonntag, 10. Mai 2026, um 10:30 Uhr, mit Bischof Dr. Bertram Meier im Hohen Dom zu Augsburg (Livestream: domradio.de, Bibel-TV und EWTN). Der Abschlussgottesdienst am Sonntag, 24. Mai 2026, um 9:30 Uhr in Sankt Martin in Kaufbeuren wird als ZDF-Fernsehgottesdienst übertragen. Näheres unter: www.renovabis.de/pfingstaktion.

Von Montag, 27. April 2026, an sollen die Renovabis-Plakate ausgehängt, das Kompaktmagazin „Renovabis OST“ sowie Spendentüten in den Kirchen ausgelegt oder im Gottesdienst verteilt werden.

Die Pfingstnovene 2026 mit dem Titel „Komm Heil‘ger Geist, der uns verbindet und Leben schafft“ wurde von Abt Theodor Hausmann OSB (Abtei St. Stephan in Augsburg) verfasst. Das Neun-Tage-Gebet von Renovabis ist als Begleiter für die Tage auf das Pfingstfest gedacht. Renovabis-Bischof Dr. Heiner Koch empfiehlt sie für das Gebet und besonders als Gebetsbrücke in den Osten Europas.

Informationen und Impulse rund um das Thema der diesjährigen Pfingstaktion sind im Aktions-Themenheft und auf der Renovabis-Homepage zu finden. Gottesdienstbausteine und Predigtskizzen stehen ab Ende März bereit. Material zum Download unter: www.renovabis.de/material.

Am Wochenende vor Pfingsten, am 16./17. Mai 2026, soll in den Gemeinden der Aufruf der deutschen Bischöfe in allen Gottesdiensten verlesen werden. Ein Hinweis auf die Pfingstkollekte von Renovabis ist gewünscht. Bitte verteilen Sie die Spendentüten mit dem Hinweis, dass die Spende am Pfingstsonntag gesammelt wird, die Spende auch zum Pfarramt gebracht oder auf ein Renovabis-Spendenkonto überwiesen werden kann.

Am Pfingstsonntag, 24. Mai 2026, sowie in den Vorabendmessen am 23. Mai 2026 wird in allen katholischen Kirchen die Renovabis-Kollekte für Osteuropa gehalten. Bitte verlesen Sie dazu diese Ankündigung: „Die heutige Kollekte ist für die Arbeit von Renovabis bestimmt. Dessen Projektpartner fördern durch soziale Hilfen, vielfältige Bildungsangebote sowie Dialog- und Versöhnungsinitiativen den gesellschaftlichen Zusammenhalt in den Ländern Mittel-, Ost- und Südosteuropas. Herzlichen Dank für Ihre Unterstützung!“ Renovabis bittet auch, auf Überweisungsmöglichkeiten, die Abgabe von Barspenden in Spendentüten oder besonders gekennzeichneten Umschlägen hinzuweisen.

Auf Beschluss der deutschen Bischöfe ist die Renovabis-Kollekte ohne jeden Abzug gemäß Kollektenplan weiterzuleiten.

Individuelle Spenden oder Kollekten von Gruppen können direkt an Renovabis überwiesen werden: www.renovabis.de/pfingstspende oder per Bank an Renovabis e.V., LIGA Bank, DE24 7509 0300 0002 2117 77, GENODEF1M05.

Nr. 42 Hinweise zur Durchführung der Missio-Aktion 2026 (Missio Aachen)

Die Solidaritätsaktion zum Sonntag der Weltmission am 25. Oktober 2026 steht unter dem Leitwort „Sei mutig und stark“ (Jos 1,6) und lenkt den Blick auf Madagaskar, wo viele Menschen jeden Tag mutig und stark um das Nötigste ringen müssen. Die Kirche vor Ort unterstützt sie dabei – mit Bildung, medizinischer Versorgung, sozialen Diensten und Seelsorge. Der Weltmissionssonntag wird 2026 in besonderer Weise begangen. Seit 100 Jahren verbindet dieser Tag die Kirche weltweit in Gebet, Solidarität und Verantwortung füreinander. Christinnen und Christen sind über Grenzen hinweg miteinander verbunden und tragen gemeinsam Verantwortung für die Glaubensgeschwister weltweit.

In seiner Botschaft zum Weltmissionssonntag 2026 erinnert Papst Leo XIV. daran, dass missionarisches Handeln aus dem Glauben heraus Mut verlangt – Mut

zum Zeugnis, zur Hoffnung und zur tätigen Nächstenliebe.

Missio bittet darum, die Aktion im Monat der Weltmission aktiv zu unterstützen: Hängen Sie das Aktionsplakat gut sichtbar aus, legen Sie Spendentüten und Gebetskarten in der Kirche aus oder verteilen Sie diese über den Pfarrbrief bzw. an Haushalte. Auch Veranstaltungen vor Ort – etwa das Missio-Solidaritätsessen „Die Welt an einem Tisch" – können ein Zeichen weltkirchlicher Gemeinschaft setzen. Anregungen zur Gottesdienstgestaltung und Aktionsideen bietet das Aktionsheft mit liturgischen Bausteinen.

Die bundesweite Eröffnung der Aktion findet vom 25. bis 27. September 2026 im Bistum Aachen statt. In einem feierlichen Pontifikalamt eröffnet Bischof Dr. Helmut Dieser zusammen mit Msgr. Luc Olivier Razafitsimialona, Bischof von Tôlagnaro, und weiteren Gästen aus Madagaskar am Sonntag, 27. September, offiziell den Monat der Weltmission. Der Gottesdienst im Aachener Dom beginnt um 10:00 Uhr und wird live im domradio übertragen. Alle Informationen zur Eröffnung finden Sie unter www.missiohilft.de/wms.

Am 18. Oktober soll in allen katholischen Gottesdiensten der Aufruf der deutschen Bischöfe verlesen werden. Am 25. Oktober wird bundesweit die Missio-Kollekte gehalten. Die Spenden unterstützen kirchliche Projekte in Afrika, Asien und Ozeanien. Die Kollekte wird über die Bistumskassen ohne Abzüge an Missio Aachen weitergeleitet. Eine pfarreiinterne Verwendung ist nicht zulässig. Bitte verlesen Sie dazu die folgende Ankündigung: „Die heutige Kollekte ist für die Arbeit von Missio bestimmt. Das Hilfswerk unterstützt die Kirche in Afrika, Asien und Ozeanien. Es geht dabei um pastorale und soziale Projekte, die insbesondere den Armen zugutekommen. Bitte beteiligen Sie sich an dieser weltweiten Solidaritätsaktion mit einer großzügigen Spende. Haben Sie herzlichen Dank!" Weitere Materialien stehen ab Mitte August unter www.missio-hilft.de/wms bereit.

Bestellungen: bestellungen@missio-hilft.de oder unter 0241 7507-350. Rückfragen bitte an: post@missio-hilft.de oder 0241 7507-333.

Nr. 43 Hinweise zur Durchführung der Diaspora-Aktion 2026

Das Bonifatiuswerk unterstützt Katholikinnen und Katholiken dort, wo sie in einer extremen Minderheitensituation ihren Glauben leben. Das Werk fördert so die Seelsorge, sozial-karitative und missionarische Projekte in Deutschland, Nordeuropa, Estland und Lettland. Das Hilfswerk setzt sich für diejenigen ein, die in der Diaspora wertvolle Arbeit leisten – in Kinderheimen und Hospizdiensten, in Schulen und Jugendhilfeeinrichtungen, in Ortspfarreien und abgelegenen Regionen. Mit den vier Hilfsarten Bauhilfe, Kinder- und Jugendhilfe, Verkehrshilfe und Glaubenshilfe kommt die nötige Unterstützung dort an, wo sie gebraucht wird.

Die Diaspora-Kollekte wird am Sonntag, 15. November 2026, in allen Gottesdiensten einschließlich der Vorabendmessen gehalten. Die Kollekte ist zeitnah und ohne Abzüge weiterzuleiten, damit das Bischöfliche Ordinariat Limburg die Spenden an das Bonifatiuswerk weiterleiten kann. Die Verwendung der Kollekte ist ausschließlich für die Arbeit des Bonifatiuswerkes bestimmt.

Im September 2026 versenden wir die Aktionsmaterialien zum diesjährigen Diaspora-Sonntag, der unter dem Leitwort „Glauben bezeugen – Hoffnung teilen" steht. Das Materialangebot umfasst u. a. Gestaltungsideen für die Liturgie, Impulse zum Leitwort, Plakate, Pfarrbriefmäntel und Spendentüten. Bitte hängen Sie die Aktionsplakate gut sichtbar in Ihrer Gemeinde auf und machen Sie die Aktion über Ihre Medien (Pfarrbrief, Homepage) bekannt. Weitere Materialien können unter www.bonifatiuswerk.de/diaspora-aktion bestellt oder heruntergeladen werden.
Bitte verlesen Sie am Sonntag, 8. November 2026, sowie am Vorabend den Aufruf der deutschen Bischöfe zum Diaspora-Sonntag in allen Gottesdiensten und verteilen Sie die Spendentüten.

Bitte legen Sie am Diaspora-Sonntag, 14./15. November 2026, die restlichen Spendentüten aus und weisen Sie in allen Gottesdiensten auf die Diaspora-Kollekte hin. Verlesen Sie dazu folgende Ankündigung: „Die heutige Kollekte ist für das Bonifatiuswerk der deutschen Katholiken bestimmt und dient der Unterstützung von kirchlichen Projekten in Nordeuropa, im Baltikum und in den katholischen Diaspora-Regionen Deutschlands. Bitte tragen Sie mit Ihrem Beitrag zur Kollekte dazu bei, dass die Kirche in der Diaspora die frohmachende Botschaft überzeugend verkünden kann. Herzlichen Dank!"

Wir sind Ihnen dankbar, wenn Sie die Anliegen der Diaspora in Ihr Gebet und die Gestaltung der Gottesdienste aufnehmen. Bitte geben Sie am Wochenende 21./22. November 2026 das Kollektenergebnis-

bekannt und verbinden Sie dies mit einem Wort des Dankes an die ganze Gemeinde.

Bestellungen und Nachfragen richten Sie bitte per Mail an bestellungen@bonifatiuswerk.de, telefonisch an 05251 2996-94 oder per Fax an 05251 2996-88. Weitere Informationen zu den Projekten finden Sie auf unserer Homepage www.bonifatiuswerk.de.

Nr. 44 Cloud-Strategie und Cloud Policy

Erklärung der Bistumsleitung

Die Bistumsleitung trägt die Verantwortung für die wirtschaftliche und sichere Cloud-Nutzung (Cloud-Computing) sowie für die durch die Organisation in der Cloud gespeicherten und verarbeiteten Informationen. Dieser Verpflichtung ist sich die Bistumsleitung bewusst.

Neben den wirtschaftlichen und technischen Möglichkeiten durch die Nutzung von Cloud-Diensten ergeben sich neue Herausforderungen, insbesondere in Bezug auf den Datenschutz und die Informationssicherheit. Da Computerressourcen außerhalb der eigenen Bistumsräume liegen, hat das Bistum Limburg nicht die gleiche Kontrolle über die Betriebsmittel und Daten wie in einem eigenen Rechenzentrum.

Informationssicherheit ist eine Grundvoraussetzung für effiziente Prozesse im Bistum. Sie gewährleistet die drei primären Sicherheitsziele: Verfügbarkeit, Integrität und Vertraulichkeit von personenbezogenen Daten, Informationen und IT-Diensten über die physischen Bistumsgrenzen hinweg.

Das vorliegende Dokument – die Richtlinie zur Cloud-Nutzung des Bistums – bildet den Rahmen für technische und organisatorische Maßnahmen für eine wirtschaftliche und sichere Cloud-Nutzung.

Bestehende Vorgaben müssen an die hier festgelegten Regelungen angepasst werden.

Die Bistumsleitung erwartet von allen Mitarbeitenden ein durchgängiges Denken und Handeln im Sinne dieser Richtlinie.

Die Bistumsleitung wird unter Berücksichtigung der wirtschaftlichen Möglichkeiten und in Abwägung des Gesamtrisikos für das Bistum Limburg alle vertretbaren Schritte veranlassen, um die Sicherheitsziele zu erreichen. Entscheidungen gegen die Durchführung einer Maßnahme zur Steigerung der Informationssi

cherheit ist durch die Bistumsleitung schriftlich zu begründen und zu dokumentieren.

Durch diese Erklärung bekennt sich die Bistumsleitung zu den in diesem Dokument definierten Zielen.

Limburg, 20. November 2025

Diözesanökonom	Dirk von Juterzenka-Kuhn
Thomas Frings	Leiter Fachbereich IT
Leiter Ressourcen und Infrastruktur	

2 Dokumentinformation

Verteiler und Versionshistorie werden im Amtsblatt nicht veröffentlicht.

3 Einleitung

3.1 Motivation

Vor dem Hintergrund der zunehmenden Digitalisierung, aufgrund der gesteigerten regulatorischen Anforderungen und da Bistumsabläufe von einwandfrei funktionierenden Workloads[1] direkt abhängig sind, ist die sichere Nutzung von Cloud-Diensten ein zunehmender Erfolgsfaktor für das Bistum Limburg.

Informationssicherheit und Datenschutz bei der Bereitstellung oder Nutzung von Cloud-Diensten werden durch Umsetzung technischer und organisatorischer Maßnahmen erzielt. Diese Maßnahmen bestehen aus verbindlichen Vorgaben (Richtlinien), Empfehlungen aus der Praxis (Leitlinien), Verfahren (Prozesse), Organisationsstrukturen und geeigneter Informationstechnik (IT) für die Umsetzung.

Obwohl viele Gemeinsamkeiten zwischen einer traditionellen IT-Infrastruktur und dem Cloud-Computing vorhanden sind, existieren gravierende Unterschiede, die sich durch die Abstraktion, die durchgehende Automatisierung, Infrastruktur als Code und das Shared-Responsibility-Modell beim Cloud-Computing erklären lassen. Zwischen den Cloud-Service-Providern (CSP) kann es im Leistungsumfang, bei der Vertragsgestaltung und der Begrifflichkeit große Unterschiede geben.

Bei Verletzung von Vertraulichkeit, Verfügbarkeit oder

[1] Gem. Definition in Kapitel 4.1.

Integrität von personenbezogenen Daten, Informationen und IT-Diensten entstehen hohe Risiken, die eine direkte Auswirkung auf das Kerngeschäft des Bistums haben können. Das vorliegende Dokument legt das Ziel, die Strategie, die Anforderungen und die Organi sation für die sichere Nutzung von Cloud-Diensten im Bistum Limburg fest.

3.2 Ziel dieser Richtlinie

Diese Richtlinie hat das Ziel, die grundlegenden Anforderungen an eine sichere Nutzung von Cloud-Diensten zu formulieren. Die Richtlinie definiert die Ziele und die Anforderungen, zu deren Einhaltung alle Mitarbeitenden, Fachbereiche und verbundene Einrichtungen verpflichtet sind.

Das Bistum Limburg verfolgt eine Cloud-First-Strategie, das heißt, die Nutzung der Cloud ist bei sinnvollem Einsatz zu bevorzugen. Dies ist im Vorfeld zu bewerten. Die Entscheidung gegen den Einsatz einer Cloud-Lösung ist zu begründen und zu dokumentieren.

Es gibt keine Festlegung auf einen bevorzugten Cloud-Service-Provider (Multi-Vendor-Strategie). Die Einführung neuer Cloud-Dienste und Cloud-Service-Provider wird durch die IT-Abteilung entschieden.

Es gibt generell keine Beschränkung bei den Service-Modellen. Die Cloud-Nutzung als „Software as a Service“ (SaaS) soll priorisiert verwendet werden. Der Cloud-Architekt trifft die entsprechenden Entscheidungen.

Als Bereitstellungsmodell wird eine Hybrid-Cloud gestattet.

Diese Richtlinie richtet sich an die nachfolgenden Zielgruppen:

- Alle Mitarbeitende (i. S. v. Nutzer von Cloud-Services): Einhaltung der vorgegebenen Verhaltensregeln beim Umgang mit Cloud-Services.
- Verantwortliche Mitarbeitende/Führungskräfte (Prozesseigentümer; i. S. v. Verantwortung für einen spezifischen Cloud-Service): Beachtung und Einhaltung der vorgegebenen Verfahren zur Einführung, zum Betrieb und zur Kontrolle von Cloud-Services und Cloud-Service-Providern inkl. der Mitwirkungspflicht bei der Prüfung des Betriebs von Cloud-Services durch den Cloud Governance Officer.
- Bistumsleitung (Vertreten durch den Generalvikar) und erste Leitungsebene des Bistums: Wahrnehmung der Governance für Cloud-Services innerhalb des Bistum Limburgs zur Wahrung der Compliance mit geltenden Gesetzen und Regulatorien durch Zeichnung dieser Richtlinie, der aktiven Mitarbeit an der Weiterentwicklung dieser Richtlinie sowie der ggfs. notwendigen Delegation an und Einsetzung von entsprechenden Funktionen zur Wahrung der Cloud-Compliance in Übereinstimmung mit dieser Richtlinie.

3.3 Geltungsbereich

Der Geltungsbereich dieser Richtlinie erstreckt sich auf alle relevanten Workloads und Informationen des Bistums Limburg, die Cloud-Dienste verwenden oder bei einem Cloud-Service-Provider gespeichert werden. Allgemein kann ein Workload als in die Cloud ausgelagerter IT-gestützter Geschäftsprozess bezeichnet werden. Der Geltungsbereich umfasst alle Workloads, die sich in der Verantwortung des Bistums Limburg befinden. Hierzu gehören die an Cloud-Service-Provider ausgelagerten Informationen.

Im Zusammenhang mit der Nutzung von Cloud-Diensten und Workloads sind zum einen die Informationen als Wert anzusehen und zum anderen die in die Cloud ausgelagerten Aufgaben.

3.4 Gültigkeit

Diese Richtlinie tritt mit der Freigabe durch die Bistumsleitung in Kraft, entwickelt Wirksamkeit durch Veröffentlichung im Amtsblatt und ist gültig, bis sie durch eine neue Version abgelöst wird oder eine andere Regelung sie explizit ersetzt. Sämtliche Änderungen sind ebenfalls durch die Bistumsleitung zu verabschieden und werden über das Amtsblatt kommuniziert.

Alle vorhergehenden Versionen dieser Richtlinie verlieren mit Inkrafttreten dieser Version ihre Gültigkeit.

3.5 Verbindlichkeit

Diese Richtlinie ist für alle Mitarbeitenden und Externen, die die IT des Bistums nutzen oder deren Einsatz planen, in der jeweils gültigen Fassung verbindlich.
Sollte eine der Regelungen nicht umsetzbar sein oder in einem Konflikt zu anderen Regelungen stehen, ist zur Klärung der Cloud Governance Officer hinzuzuziehen.

Abweichungen von den Regelungen dieser Richtlinie sind durch die spezifischen Cloud-Service-Verantwortlichen (Prozesseigentümer) an den Cloud Governance Officer zu melden und werden in Abstimmung mit der Bistumsleitung oder einer von ihr eingesetzten Vertretung geklärt. Die verantwortliche Person erhält nach Klärung das Ergebnis mitgeteilt. Dies kann sowohl positiv als auch negativ ausfallen. Im letzten Fall steht der Cloud Governance Officer, der Cloud Architekt und die AG Informationssicherheit als Partner für die Erarbeitung von Lösungen oder Alternativen zur Verfügung.

Die Einhaltung der Richtlinie wird regelmäßig und in Stichproben durch den Informationssicherheitsbeauftragten überprüft.

Die jeweils gültige Version der Richtlinie wird für alle Mitarbeitenden zentral über die Rechtssammlung[2] bereitgestellt.

Die Umsetzung der vorliegenden Richtlinie hat unverzüglich zu beginnen und ist schnellstmöglich abzuschließen. Dies gilt insbesondere für Cloud-Services im Bestand. Sollte aufgrund bestehender Verträge oder Regularien eine unverzügliche Umsetzung nicht möglich sein, besteht eine erweiterte Umsetzungsfrist von 12 Monaten. Dies ist dem Cloud Governance Officer zwingend anzuzeigen.

Alle für einen Cloud-Service verantwortlichen Personen (Prozesseigentümer) sind verpflichtet, die von ihnen verantworteten Cloud-Services dem Cloud Governance Officer für die Bestandsaufnahme unverzüglich zu melden. Dies wird initial durch eine Revisionsabfrage begleitet. Der in Abschnitt 5 festgelegten Vorgabe für die Einführung neuer Cloud-Services bleiben davon unberührt.

Verstöße gegen diese Richtlinie können für die Mitarbeitenden Konsequenzen kirchenrechtlicher, arbeitsrechtlicher, zivilrechtlicher oder strafrechtlicher Art haben.

3.6 Pflege des Dokuments

Diese Richtlinie wird bei wesentlichen Veränderungen der Organisation und der Prozesse – jedoch mindestens jährlich – auf ihre Aktualität hin geprüft und bei Bedarf angepasst.

Zuständig für die Überprüfungen ist der Informationssicherheitsbeauftragte.

Inhaltliche Änderungen, die über redaktionelle Anpassungen hinausgehen, erfordern eine erneute Freigabe durch die Bistumsleitung.

Eine Version dieser Richtlinie ist revisionssicher aufzubewahren.

3.7 Begriffe

Für ein einheitliches Verständnis von Fachbegriffen aus der Informationssicherheit und der Cloud-Nutzung befinden sich im Anhang die Definitionen.

4 Festlegungen für Workloads

4.1 Definition

Als Workloads sind die IT-gestützten Verfahren zu verstehen, die in eine Cloud ausgelagert sind. Sie umfassen sowohl die verarbeiteten Informationen, die notwendigen Cloud-Dienste und die dazugehörigen Cloud-Ressourcen.

Fällt ein Workload aus oder liefert er falsche Ergebnisse, dann ist dieses in der traditionellen IT gleichzusetzen mit dem Ausfall eines oder mehrerer IT-gestützten Prozesse.

Die Workloads sind dabei in die beiden Kategorien kritische Workloads und unkritische Workloads aufgeteilt. Für beide sind die Anforderungen jeweils unterschiedlich zu sehen. Ziel dieser Unterscheidung ist es sicher zu stellen, dass alle Cloud-Dienste einen für den Zweck ausreichenden Schutz erhalten, aber auch die Nutzung von kleineren Diensten aus der Cloud möglich ist.

4.2 Kritische Workloads

Zu dieser Kategorie gehören alle Verfahren, die:
- Kerngeschäftsprozesse stützen
- vertrauliche Daten verarbeiten
- personenbezogene Daten verarbeiten

Für diese Kategorie sind die Anforderungen an die Planung, Betrieb und Außerbetriebnahme, die in dieser Richtlinie festgelegt sind, ohne Einschränkungen anzuwenden.

---

[2] https://rechtssammlung.bistumlimburg.de/

4.3 Unkritische Workloads

Zu dieser Kategorie gehören alle IT-Verfahren, die nicht zu den Kritischen Workloads zu rechnen sind. Es ist bei der Bewertung der Umsetzung der Anforderungen aus dieser Richtlinie für diese Workloads zu beachten, dass hier nur ein geringer Schutzbedarf vorliegt. Konkret bedeutet dies, dass alle Anforderungen die hier als MUSS gesetzt sind, als „SOLL" zu betrachten sind.

5 Strategie und Anforderungen zur Cloud-Nutzung

5.1 Cloud Strategie

5.1.1 Ziel der Cloud-Strategie

Die Cloud-Nutzung unterstützt und fördert das Erreichen von Geschäftszielen durch eine Effizienz- und/oder Effektivitätssteigerung insbesondere in der Zusammenarbeit und unter Berücksichtigung von Risiko und Compliance.

5.1.2 Anforderungen zur Umsetzung der Cloud-Strategie

Grundsätzlich sind die Anforderungen zur Umsetzung der Cloud-Strategie für alle Workloads (unabhängig des Geltungsbereichs[3]) anzuwenden.

- Der Kontext der Cloud-Nutzung muss die Ziele des Bistums unterstützen (Governance).
- Die Auswahl von Service- und Bereitstellungsmodellen sowie die Entscheidung für einen Cloud-Service-Provider muss zentral durch den Cloud-Architekten und IT-Abteilung erfolgen. Hierzu ist durch den Prozesseigentümer die Checkliste Cloud-Services auszufüllen. Diese ist beim Cloud Governance Officer abrufbar. Eine Nutzung von Cloud-Diensten ohne vorherige Genehmigung ist nicht zulässig, würde zu einer Schatten-IT führen und damit ein nicht vertretbares Risiko für die Organisation bedeuten (siehe Vergabe von Aufträgen).
- Bei Cloud-Betriebs- und Speicherorten außerhalb der Europäischen Union (EU) oder in einer Region, in der ein abweichender Rechtsraum gilt, muss eine Genehmigung zur Cloud-Nutzung durch die Bistumsleitung erfolgen.
- Anforderungen an den Datenschutz und an die Informationssicherheit müssen unter Einhaltung von gesetzlichen, regulatorischen und wirtschaftlichen Aspekten bei der Nutzung von Cloud-Diensten eingehalten werden (siehe Datenschutz und Informationssicherheit Cloud Security).
- Der Cloud Governance Officer, die AG Informationssicherheit und der Informationssicherheitsbeauftragte müssen bei Projekten zur Cloud-Nutzung frühzeitig eingebunden werden.
- Der betriebliche Datenschutzbeauftragte ist in allen Projekten mit einem Bezug zu personenbezogenen Daten – die es gemäß kirchlichem Datenschutzrecht erfordern – frühzeitig mit einzubinden.
- Die zuständige Mitarbeitervertretung ist in allen Cloud-Service-Projekten frühzeitig mit einzubinden.
- Für Workloads und Cloud-Anwendungen, die personenbezogene Daten, vertrauliche Informationen verarbeiten oder die eine hohe Verfügbarkeit erfordern, muss vor einer Freigabe des Produktivbetriebs eine formelle Information durch den Projektverantwortlichen durchgeführt und dokumentiert werden. Die Information hat die grundlegenden Aspekte zum Datenschutz und zur Informationssicherheit zu enthalten.
- Die Administration von im Bistum genutzten Cloud-Diensten – sowie die Überwachung von Workloads muss durch qualifiziertes Personal (vorzugsweise der jeweilige Cloud Services Manager) erfolgen.

5.2 Risikobetrachtung bei der Cloud-Nutzung

5.2.1 Ziel der Risikobetrachtung

Risiken und Chancen sind in jeder Organisation vorhanden. Die Beschäftigung mit diesen Risiken dient dem Erkennen und Bewerten sowie dem Erarbeiten von Steuerungsmaßnahmen und deren Umsetzung.

Viele IT-Risiken bekommen im Cloud-Computing eine andere Dimension, weil die Systeme, Applikationen oder Daten nicht unter eigener physischer Kontrolle sind, sondern außerhalb bei einem Provider liegen.

Risiken für die sichere Nutzung von Cloud-Diensten werden effektiv erkannt, bewertet und angemessen behandelt. Das Risikomanagement ist definiert, nachvollziehbar und wirksam.

[3] Kapitel 3.3.

5.2.2 Anforderungen an die Risikobetrachtung

- Neben den typischen IT-Risiken müssen insbesondere Cloud-spezifische Risiken berücksichtigt werden, die in der traditionellen IT-Umgebung nicht in dieser Form vorhanden sind[4].
- Durch die Steuerungsmaßnahmen müssen die Risiken bei der Nutzung von Cloud-Diensten auf akzeptable Restrisiken reduziert werden.
- Damit Risiken in der Informationsverarbeitung effektiv erkannt, bewertet und angemessen behandelt werden, muss ein geeignetes Risikomanagement definiert werden[5].

5.3 Vergabe von Aufträgen

5.3.1 Ziel der Vergabe von Aufträgen

Die Auslagerung von Leistungen (engl. outsourcing) oder einzelner Aufgaben (engl. outtasking) an einen Cloud-Service-Provider (CSP), gehören mittlerweile zum Alltagsgeschäft für IT-gestützte Geschäftsprozesse. Leistungen, Anforderungen und Zuständigkeiten sind vertraglich geregelt und im Einklang mit regulatorischen und gesetzlichen Bestimmungen.

5.3.2 Anforderungen an die Vergabe von Aufträgen

- Ein Cloud-Service-Provider muss sorgfältig gemäß den Anforderungen dieser Richtlinie ausgewählt werden und die gesetzlichen, regulatorischen, funktionalen und nicht-funktionalen Anforderungen des Bistums Limburg erfüllen.
- Da der unübersichtliche Markt an Cloud-Service-Providern weiter stark wächst, bedarf es einer klaren Auswahl- und Abgrenzungsstrategie in Bezug auf Marktreife, Angebotsumfang, Sicherheit und Kosten. Das Bistum Limburg verfolgt folgende Strategie bei der Auswahl der Anbieter:
  - Wenn das Unternehmen teilweise oder aufgrund der allgemeinen Geschäftsbedingungen (AGB) oder anderer Vertragsbedingungen das Recht an seinen Daten verliert, dann muss dieser Cloud-Service-Provider von einer Vergabe ausgeschlossen werden, da der Verlust des geistigen Eigentums droht.
  - Wenn der gerichtliche Standort für mögliche Rechtsstreitigkeiten der Organisation mit dem Cloud-Service-Provider in Ländern liegt, die für das Unternehmen als ungeeignet angesehen werden, dann muss dieser Cloud-Service-Provider von einer Vergabe ausgeschlossen werden.
  - Wenn der gerichtliche Standort für mögliche Rechtsstreitigkeiten der Organisation mit dem Cloud-Service-Provider in Ländern liegt, die für das Unternehmen als ungeeignet angesehen werden, dann muss dieser Cloud-Service-Provider von einer Vergabe ausgeschlossen werden.
  - Wenn der Cloud-Service-Provider keine Mandantentrennung auf Auftragsebene mit entsprechender Trennung der Daten von verschiedenen Mandanten anbietet und garantiert, dann muss dieser Cloud-Service-Provider von einer Vergabe ausgeschlossen werden.
  - Wenn der Cloud-Service-Provider per AGB oder gemäß anderen Vertragsbedingungen nicht verpflichtet ist, alle das Unternehmen betreffenden Sicherheitsvorfälle zeitnah und mit ausführlicher Information an das Unternehmen zu berichten, dann muss dieser Cloud-Service-Provider von einer Vergabe ausgeschlossen werden.
  - Wenn der Cloud-Service-Provider bei einem zuverlässigen CASB[6]-Anbieter als Hochrisikodienst gelistet ist, dann muss dieser Cloud-Service-Provider von einer Vergabe ausgeschlossen werden.
  - Wenn der Cloud-Service-Provider per AGB oder gemäß anderen Vertragsbedingungen berechtigt ist, das Vertragsverhältnis nach eigenem Ermessen, mit einer von der Organisation als ungenügend angesehenen Kündigungsfrist oder unter für die Organisation unzumutbaren Bedingungen zu beenden, dann muss dieser Cloud-Service-Provider von einer Vergabe ausgeschlossen werden.
  - Wenn die Datenhaltung des Cloud-Service-Providers außerhalb der EU nach nicht-EU-Standards erfolgt[7], es sich aber nicht um öffentliche Daten, sondern um besonders schützenswerte Daten[8] handelt , dann muss dieser Cloud-Service-Provider entweder disqualifiziert werden oder alternativ muss der

[4] Kapitel 7.3.

[5] Kapitel 7.2.

[6] Viele Cloud Access Security Broker führen eine CSP-Datenbank mit Risikobewertungen.

[7] Zum Beispiel nicht nach EU-DSGVO oder gleichwertigem Recht.

[8] Zum Beispiel um sensible persönlich identifizierende Informationen, PII.

besondere Schutzbedarf der Daten durch zusätzliche Maßnahmen[9] gewährleistet werden.
- Der Cloud-Service-Provider muss seine technischen und organisatorischen Datenschutz- und Sicherheitsmaßnahmen nachvollziehbar darlegen. Auf Basis dieser Informationen ist eine Risikobewertung durchzuführen. Alternativ hierzu muss ein Auditrecht vertraglich vereinbart werden.
- Der Cloud-Service-Provider muss einen aktuellen Nachweis über anerkannte Zertifizierungen vorweisen, die für das Bistum relevant sind. Mindestens muss dabei eine der nachfolgenden Zertifizierungen bzw. Nachweise bestehen:
  - Zertifizierung einer akkreditierten Zertifizierungsstelle nach ISO/IEC 27001 (Informationssicherheitsmanagementsystem) und ergänzend nach ISO/IEC 27017 (Informationssicherheit in Cloud Services) und optional zusätzlich ISO/IEC 27018 (Schutz personenbezogener Informationen in Cloud-Services)
  - Zertifizierung nach ISAE 3402 mit Schwerpunkt Cloud-Service-Provider durch eine anerkannte Wirtschaftsprüfungsgesellschaft/ Wirtschaftsprüfer.
- Es muss vor Abschluss eines Vertrages im Rahmen der „Shared Responsibility" geklärt sein, welche Zuständigkeiten beim Cloud-Service-Provider liegen und welche bei der Organisation.
- Es muss vor Abschluss eines Vertrages eine Vereinbarung zur Auftragsverarbeitung mit dem Cloud-Service-Provider abgeschlossen werden[10].

5.4 Datenschutz und Informationssicherheit

Durch das Bistum verarbeitete personenbezogene Daten, insbesondere der Mitarbeitenden, der Kunden und der Partner des Bistums der Bistumsleitung, stellen ebenso wichtige Werte wie Informationen über Geschäftsgeheimnisse dar.

5.4.1 Ziel von Datenschutz und Informationssicherheit

Bei der Auslagerung von personenbezogenen Daten und Geschäftsinformationen in die Cloud sowie bei der Nutzung von Cloud-Diensten sind alle erforderlichen Maßnahmen für den Datenschutz und zur Informationssicherheit umgesetzt und wirksam.

Aufzeichnungen von Videokonferenzen sind grundsätzlich nicht gestattet. Sofern alle Teilnehmer in der Konferenz informiert sind und die Möglichkeit haben, der Aufzeichnung zu entgehen, also zu ihrer Aufzeichnung freiwillig zustimmen können, ist eine Aufzeichnung möglich.
Die Verwendung KI-gestützter Dienste (z. B. Transkription, Übersetzung) ist in Übereinstimmung mit den organisationseigenen Regelungen zur Verwendung künstlicher Intelligenz zulässig. Dabei sind die datenschutzrechtlichen Vorgaben und zum Schutz der Informationen des Bistums verbindlich einzuhalten und zu berücksichtigen.

5.4.2 Anforderungen an den Datenschutz und die Informationssicherheit

- Ein angemessener Umgang mit personenbezogenen Daten und Informationen erfordert, dass sich die für den Geschäftsprozess verantwortliche Organisationseinheit, die für die Umsetzung und den Betrieb zuständigen beteiligten Fachbereiche und die Anwender der Sensibilität der Informationen, die sie nutzen und verarbeiten, bewusst sind. Dazu ist es notwendig, dass sie die Sensibilität der von ihnen erzeugten oder weitergegebenen Informationen kennen.
- Aufbewahrungsfristen sind für alle personenbezogenen Daten und für alle Belege nach HGB und GoBD und ggf. einer festgelegten organisationseigenen Aufbewahrungsfrist und der KAO definiert. Alle personenbezogenen Daten sind möglichst bald zu löschen, soweit nicht längere Aufbewahrungspflichten bestehen (z. B. bei GoBD und HGB 6 oder 10 Jahre). Für diese Daten sind in der Cloud Anwendung entsprechende Maßnahmen vorzusehen (z. B. Archivierung auf eigenen Systemen, per Labels und „Litigation Hold"), um die Archivierungs- und Lösch-Mechanismen der Cloud Anwendung zu nutzen.
- Neben Unterweisungen müssen Sensibilitäts- oder Schutzstufen definiert[11] und zum Beispiel über ein Cloud-Inventar den Workloads zugeordnet werden. Die Zuständigkeiten hierfür ergeben sich aus den Rollenbeschreibungen.
- Daten ohne Kennzeichnung sind grundsätzlich als „intern" zu behandeln.
- Es müssen geeignete technische und/oder organisatorische Maßnahmen zum Schutz der personenbezogenen Daten umgesetzt und wirksam

[9] Zum Beispiel Verschlüsselung mit ausschließlich eigener Schlüsselkontrolle.

[10] In der Regel ist dies Bestandteil eines Standardvertrages.

[11] Kapitel 7.2.

sein (siehe Cloud Security). Ziel dieser Maßnahmen muss es sein, dass vertrauliche Informationen oder personenbezogene Daten nicht an unbefugte Dritte gelangen und dass Inhalte bei der Datenübertragung nicht unbemerkt verändert werden können.
- Ein- und ausgehender Datenverkehr im Kontext des Cloud-Services soll automatisiert überprüft (Monitoring) werden, so dass ein unrechtmäßiger Abfluss von schützenswerten Daten aus den Workloads verhindert oder erkannt werden kann.
- Ende-zu-Ende-Verschlüsselung für die Übertragung von in der Cloud gelagerten Daten ist verpflichtend umzusetzen.

5.5 Identity und Access Management

In der Cloud ist die Identität oft der einzig verfügbare Perimeter und damit Schutz der Daten. Daher sind die Ziele des Identity und Access Managements besonders wichtig für den sicheren Betrieb von Cloud-Diensten.

5.5.1 Ziele des Identity und Access Management

Es ist sicherzustellen, dass nur berechtigte Personen und IT-Dienste ausschließlich Zugriff auf die Daten haben, die sie für ihre Arbeit benötigen.

5.5.2 Anforderungen an das Identity und Access Management

- Alle im Cloud-Service verwendeten Accounts sind aus einem zentralen Verzeichnis zu generieren.
- Berechtigungen sind über Rollen zu vergeben, die ihrerseits an eine Gruppe von Accounts gehängt sind (RBAC). Alternativ und sofern der Cloud Anbieter es unterstützt, kann auch ein „Policy Based Access Control“ (PBAC) die Berechtigungen der Accounts verwalten.
- Privilegierte Accounts sollten nicht synchronisiert werden, sondern Cloud-Nativ nur im Benutzerverzeichnis in der Cloud angelegt sein. Mindestens sind die Zuordnungen zu privilegierten Gruppen nur in der Cloud anzulegen.
- Berechtigungen, die nicht mehr benötigt werden, sind umgehend zu entziehen.
- Accounts, die nicht mehr benötigt werden, sind umgehend still zu legen.
- Stillgelegte Accounts dürfen erst gelöscht werden, wenn die Account-ID und der Inhaber, respektive die Verwendung, revisionssicher gespeichert wurden.
- Bei Anmeldungen von unüblichen Orten bzw. Endgeräten aus, oder über unübliche oder fremde Netze ist mindestens ein zweiter Faktor bei der Authentifizierung zu nutzen. Sollte der Service diese Möglichkeit nicht bieten, ist grundsätzlich ein zweiter Faktor bei der Authentifizierung zu nutzen.
- Für Accounts mit administrativen Berechtigungen oder besonderem Schutzbedürfnis ist grundsätzlich mindestens ein zweiter Faktor zu nutzen.

5.6 Cloud Security

Sicherheit bei der Bereitstellung oder Nutzung von Cloud-Diensten (kurz Cloud Security) dient dem Schutz von Informationen, personenbezogene Daten und Workloads vor einer Vielzahl von Bedrohungen.

Cloud Security wird beim Bistum Limburg definiert als Sicherung der:
- Vertraulichkeit: Gewährleistung des Zugangs zu Cloud-Diensten und Informationen für ausschließlich zugangsberechtigte Personen oder Kommunikationsinstanzen;
- Integrität: Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden in der Cloud;
- Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Cloud-Diensten und Informationen aus der Cloud für berechtigte Personen oder Kommunikationsinstanzen;

5.6.1 Ziel der Cloud Security

Workloads müssen nach aktuellem Stand der Technik gegen bekannte Bedrohungen geschützt sein.

5.6.2 Anforderungen an die Cloud Security

- Cloud Security muss die Aufrechterhaltung des Geschäftsbetriebs gewährleisten, geschäftsschädigende Einflüsse niedrig halten sowie die Investitionsrentabilität und die Geschäftschancen wahren.
- Es sind Prozesse zu implementieren, die die Ziele der IT-Sicherheit in der Cloud aufrechterhalten.
  - Bearbeitung der Benachrichtigungen über Sicherheits-Ereignisse bei den Anbietern
  - Regelmäßige Kontrolle der Sicherheits-Einstellungen und -Scores.
  - Bearbeitung von Vorfällen, inklusive Analyse und Nachverfolgung.

- Cloud Security muss unvorhergesehene, versehentliche und absichtlich herbeigeführte Sicherheitsereignisse verhindern oder zumindest in ihrer Auswirkung auf ein akzeptables Niveau (Restrisiko) für das Bistum Limburg reduzieren.
- Cloud Security muss die Zuverlässigkeit der Geschäftstätigkeit gewährleisten und darf ihr nicht entgegenwirken. Einschränkungen sind auf das Notwendige zu begrenzen. Im Zweifelsfall ist über eine Risikoabwägung zu entscheiden, ob eine Einschränkung umzusetzen ist.
- Cloud Security muss auf die Abwehr von Bedrohungen sowie die Erfüllung von gesetzlichen Anforderungen ausgerichtet sein und stellt eine Verpflichtung gegenüber Kunden, Mitarbeitern und Partnern des Bistums Limburg dar.
- Cloud Security muss dazu beitragen, die Qualität von Produkten und Dienstleistungen zu gewährleisten, sowie die Investitionsrentabilität und die Chancen für das Bistum Limburg zu wahren.
- Cloud Security muss den (privilegierten) Zugang zu Workloads oder Anwendungen sowie den Zugriff auf personenbezogene Daten und auf Informationen durch eine Zugangs- und Zugriffskontrolle auf die notwendigen berechtigten Personen und Dienste beschränken.
- Um Effizienz und Effektivität – also das Kosten- und Nutzen-Verhältnis – abzuschätzen, muss bei kritischen Workloads eine Business Impact Analyse (BIA) durchgeführt werden, die die mögliche Höhe eines Schadens für das Bistum unter Berücksichtigung des zuvor festgelegten Schutzbedarfs der Daten/Informationen/Workloads und die möglichen Auswirkungen von Schadensereignissen auf die betroffenen Kernprozesse verdeutlicht.
- Es ist zu beachten, dass nicht das technisch bestmögliche Schutzniveau umzusetzen ist. Es muss ein Kompromiss aus den technischen Möglichkeiten, einer praxisnahen Umsetzung und aus wirtschaftlichen Aspekten gefunden werden. Dieses entspricht dem Grundsatz der Verhältnismäßigkeit, so dass der Aufwand für Maßnahmen nicht außer Verhältnis zum Schadensausmaß steht.
- Es müssen technische und organisatorische Maßnahmen geplant und umgesetzt werden, die dem aktuellen Stand der Technik entsprechen. Beim Stand der Technik handelt es sich um Maßnahmen, die das Erreichen der vorgegebenen Sicherheitsziele sichern. Die Maßnahmen haben sich in der Praxis bewährt oder wurden mit Erfolg erprobt. Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität und Vertraulichkeit gesichert erscheinen lässt.
- Bei der Auswahl von geeigneten Maßnahmen müssen gängige Leitfäden aus der Praxis und aktuelle Marktanalysen genutzt werden.
- Insbesondere für die Anforderungen an die Cloud Security muss eine Fachrichtlinie (Cloud Security Baseline) oder ein technisches Sicherheitskonzept (Hardening-Guide) durch das Bistum Limburg erstellt und aktuell gehalten werden.
- Es sind für alle gemeinsam genutzten Daten des Bistums – die nur in der Cloud liegen – ausreichende Daten-Sicherungen anzulegen.
- Cloud Services müssen eine transportverschlüsselte Übertragung zur Verfügung stellen.
- Alle Cloud-Dienste und -Ressourcen sind in die Bestandsverwaltung des Bistum Limburgs aufzunehmen.
- Protokolldaten sollten gesammelt und mindestens 12 Monate vorgehalten werden.
- Zur stetigen Verbesserung muss die Informationssicherheit in technischer, organisatorischer, personeller und infrastruktureller Hinsicht regelmäßig geprüft und kontinuierlich optimiert werden (siehe Kontrolle und Verbesserung).

5.7 Kontinuität

5.7.1 Ziel der Kontinuität

Nach einem Notfall können bistumskritische Prozesse innerhalb einer vertretbaren Zeit bereitgestellt werden.

5.7.2 Anforderungen zur Kontinuität

- In unvorhergesehenen Situationen (Notfällen) muss es möglich sein, dass Workloads, Anwendungen und Informationen in der Cloud schnell wiederhergestellt werden.
- Es ist Vorsorge zu treffen, dass wichtige Informationen und Workloads nach einem Ausfall zeitnah verfügbar sind. Es muss klar geregelt sein, welche Maßnahmen durch den Cloud-Service-Provider ergriffen werden und welche das Bistum umzusetzen hat. Die Zuständigkeit ist vertraglich zu regeln (siehe Vergabe von Aufträgen).

- Verhaltensrichtlinien für den Notfall müssen in Sicherungs- und Notfallkonzepten dokumentiert sein und über das Business Continuity Management (BCM) gesteuert werden. Zuständig für die Sicherungs- und Notfallkonzepte sind die verantwortlichen Fachbereiche.
- Daten-Exporte müssen in einem gängigen und maschinenlesbaren Format bereitgestellt werden.

5.8 Sensibilisieren

Verständnis und Motivation aller Mitarbeitenden tragen entscheidend dazu bei, dass Vorgaben zur sicheren Cloud-Nutzung eingehalten werden.

Die Konfiguration, Administration und das Management von Diensten in der Cloud erfolgen teilweise anders als in der klassischen IT in einem eigenen Rechenzentrum. Auch wenn die Themen ähnlich sind, unterscheiden sich die Lösungsansätze, wie Virtualisierung (Abstraktion) und Automatisierung (Orchestrierung). Daher muss Personal, das sich in das Thema Cloud Computing einarbeitet, durch Schulungen unterstützt werden.

5.8.1 Ziel der Sensibilisierung

Cloud Manager, Cloud Administratoren und Cloud User sind über Sicherheitsverfahren und den richtigen Einsatz von Cloud-Diensten informiert oder geschult.

5.8.2 Anforderungen an das Sensibilisieren

- Cloud User müssen über Sicherheitsverfahren und den richtigen Gebrauch von Cloud-Diensten informiert werden, um Sicherheitsrisiken zu verringern.
- An alle Cloud User müssen mit der Freigabe der Cloud-Nutzung Leitlinien zur sicheren Nutzung von Cloud-Diensten in geeigneter Form zur Verfügung gestellt werden.
- Mitarbeitende, die für die Konfiguration, Administration und das Management von Cloud-Diensten zuständig sind, müssen regelmäßige Schulungen zu Cloud-Lösungen und zur Cloud Security erhalten.

5.9 Kontrolle und Verbesserung

Eine wesentliche Maßnahme, um Compliance-Anforderungen zu erfüllen, ist das proaktive Erkennen und die Analyse von technischen und organisatorischen Mängeln.

5.9.1 Ziel der Kontrolle und Verbesserung

Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit und Datenschutz werden in der Cloud erkannt und unterbunden.

5.9.2 Anforderungen an die Kontrolle und Verbesserung

- Die Wirksamkeit und Angemessenheit umgesetzter Maßnahmen zum Datenschutz und zur Informationssicherheit müssen regelmäßig oder anlassbezogen geprüft werden und sind an die aktuellen Anforderungen anzupassen.
- Sind Vor-Ort-Audits bei einem Cloud-Service-Provider nicht gestattet (was die Regel ist), dann müssen gültige Zertifikate und Testate, die durch eine anerkannte Prüfstelle (3rd-Party-Audit) ausgestellt werden, als Nachweis für eine Compliance Prüfung der zugrundeliegenden Cloud-Infrastruktur verwendet werden. Dieses Vorgehen wird pass-through audit bezeichnet.
- Für die selbstverwaltete virtuelle Umgebung in einer Cloud müssen Schwachstellen-Scan (nach Anmeldung beim CSP) durch das Bistum durchgeführt werden.
- Prüfungen und Maßnahmenplanung müssen zum Nachweis dokumentiert werden.

6 Organisation

Cloud Computing wirkt sich auf die Governance aus, da es entweder einen Cloud-Service-Provider in den Prozess einbezieht (im Falle von Public Cloud oder Hosted Private Cloud) oder bei Self-Hosting Private Cloud interne Governance-Strukturen verändert.

Der Cloud-Service-Provider ist für die Sicherheit der grundlegenden Infrastruktur seines Cloud-Angebotes verantwortlich und das Bistum Limburg (als Kunde) für die Sicherheit „innerhalb“ der genutzten Cloud-Dienste. Kunden behalten die Kontrolle darüber, welche Sicherheitsmaßnahmen sie zum Schutz ihrer eigenen Inhalte, der Plattform, der Anwendungen, Systeme und Netzwerke einsetzen – wie bei Anwendungen in einem lokalen Rechenzentrum.

6.1 Rollen und Zuständigkeit bei der Cloud-Nutzung

Für alle Workloads sind die Personen zu identifizieren, die die folgenden operativen Rollen wahrnehmen. Die organisatorischen Rollen sind zentral definiert.

Die generischen Rollen sind auf die Mitarbeitenden und Organisationseinheiten des Bistums Limburg anzuwenden und es ergeben sich die folgenden Zuordnungen:

6.1.1 Operative Rollen

Rolle	Beschreibung	Zuordnung
Prozesseigentümer	Person, die für einen Geschäftsprozess verantwortlich ist. Der Prozess umfasst häufig mehrere IT-Anwendungen. Der Prozesseigentümer ist gegenüber der Geschäftsleitung verantwortlich und trägt das operative Risiko. Er wird daher als Risikoeigentümer bezeichnet. In dieser Rolle kann er über die Handhabung von Risiken entscheiden und trägt persönlich gegenüber der Organisationsleitung die Verantwortung für akzeptierte Risiken. Bereits bei der Bedarfserhebung ist der Cloud Governance Officer einzubinden	Bereichsleitung
Cloud Service Manager	Person, die für einen oder mehrere Cloud-Dienste über den gesamten Life Cycle, das heißt von der Anforderungsanalyse über das On-Boarding bis zum Off-Boarding, für die Definition und Einhaltung der internen Anforderungen als Fachverantwortliche/r zuständig ist. Sie sorgt für die Einhaltung der Vorgaben des Cloud Governance Officers und arbeitet eng mit dem Cloud Service Administrator zusammen.	Wird vom Prozesseigentümer beauftragt
Cloud Service Administrator	Person, die für die Konfiguration und Administration eines Cloud Services im Sinne der Fachadministration zuständig ist.	Wird vom Cloud Service Manager und dem Prozesseigentümer beauftragt

6.1.2 Organisatorische Rollen

Rolle	Beschreibung	Zuordnung
Cloud Governance Officer	Person, die die grundlegenden Anforderungen an den Einsatz von Cloud Services im Bistum Limburg festlegt. Sie legt den Rahmen fest, in dem Cloud Services eingesetzt werden.	Bis zur abschließenden Festlegung der zentralen Steuerung von Digitalisierungsthemen übernimmt die AG Informationssicherheit diese Rolle
Cloud Architekt	Person, die den Aufbau und das Zusammenspiel der eingesetzten Cloud-Services und Cloud-Service-Provider koordiniert. Sie entscheidet gemeinsam mit der IT-Abteilung über die Einführung, Änderung und Abschaltung von Cloud Services.	Wird durch eine Person in der IT-Abteilung besetzt
Cloud Auditor	Ein Cloud-Auditor ist eine Partei, die eine unabhängige Prüfung von Cloud-Service-Kontrollen durchführen kann, um eine Stellungnahme dazu abzugeben. Es werden Audits durchgeführt, um die Einhaltung der Normen durch Überprüfung objektiver Beweise zu überprüfen. Ein Cloud-Auditor kann die von einem Cloud-Anbieter bereitgestellten Services in Bezug auf Sicherheitskontrollen, Datenschutzauswirkungen, Leistung usw. bewerten. Es hat eine Überprüfung von technischen und organisatorischen Maßnahmen zur Cloud Security zu erfolgen.	Unabhängige qualifizierte Person
Cloud User	Person, die eine Cloud-Anwendung oder einen Cloud-Dienst für die Arbeit nutzt. Entspricht einem IT-Anwender.	Alle Mitarbeitende
Cloud Service Provider	Der Cloud-Service-Provider ist der externe Cloud-Dienstleister mit dem ein Vertrag über die Nutzung von einem oder mehreren Cloud-Diensten (SaaS, PaaS, IaaS) abgeschlossen wird.	Extern
Cloud Customer	Die Organisation, die bei einem Cloud-Service-Provider einen oder mehrere Cloud-Dienste einkauft. Diese Rolle wird häufig als Cloud Consumer bezeichnet.	Bistum Limburg

Cloud Broker	Die Integration von Cloud Services kann für Cloud Customer zu komplex sein, um sie verwalten zu können. Ein Cloud-Customer kann Cloud-Services von einem Cloud-Broker anfordern, anstatt sich direkt an einen Cloud-Service-Provider zu wenden. Daher ist der Broker eine Einheit, die die Nutzung, Leistung und Bereitstellung von Cloud-Services verwaltet und Beziehungen zwischen Cloud-Service-Provider und Cloud Customer aushandelt.	Extern
Cloud Carrier	Ein Vermittler, der die Konnektivität und den Transport von Cloud-Services vom Cloud-Service-Provider zum Cloud Customer bereitstellt. Cloud Carrier bieten den Verbrauchern über Netzwerk-, Telekommunikations- und andere Zugangsgeräte den Zugang.	Extern
Organisationsleitung	Die Verantwortung für die Cloud-Nutzung des Bistums liegt und verbleibt bei Bistumsleitung. Ihre Aufgabe ist es, möglichen Schaden für die Organisation abzuwenden oder auf ein akzeptables Restrisiko zu reduzieren.	Bistumsleitung

7 Anlagen

7.1 Ansprechpartner

Rolle	Name	Kontaktdaten
Informationssicherheitsbeauftragter (ITSB)	Herr Jaenichen	Tel. 0152 099 349 78; J.Jaenichen@consulectra.de
Datenschutzbeauftragter (DSB)	Herr Lachenmann	Tel. 0221 204 63 884; lachenmann@BHO-Consulting.com
IT-Leitung	Herr v. Juterzenka-Kuhn	Tel. 06431 295 338; d.vonJuterzenka-kuhn@bistumlimburg.de
IT-Support (Helpdesk)		Tel. 06431 295 444; service-desk@it.bistumlimburg.de

7.2 Rahmen zur Klassifikation von Workloads

Ein Cloud-Inventar von bistumseigenen Workloads hilft sicherzustellen, dass Workloads effektiv geschützt werden. Die Erstellung eines Cloud-Inventars von Bistumseigenen Workloads ist eine wichtige Voraussetzung für das IT-Risikomanagement.

Für einen angemessenen Umgang mit Informationen müssen sich

- Informationseigentümer (zum Beispiel verantwortlicher Fachbereich),
- Informationstreuhänder (zum Beispiel für die Umsetzung zuständige IT-Abteilung) und
- Informationsnutzer (i. d. R. der Anwender) der Sensibilität der Informationen, die sie nutzten und verarbeiten, bewusst sein.

Dazu ist es notwendig, dass sie die Sensibilität der von ihnen erzeugten oder weitergegebenen Informationen kennen. In der Praxis werden zu diesem Zweck Sensibilitäts- oder Schutzstufen definiert und häufig in einem Inventar den Workloads zugeordnet.

7.2.1 Klassen

Die folgende Liste stellt ein Klassifizierungsschema für die Vertraulichkeit von Informationen dar.

öffentlich: Informationen sind öffentlich, wenn es sich um Informationen handelt, die frei zugänglich sind. Im Gegensatz zur Vertraulichkeit stehen die Integrität und die Verfügbarkeit von Informationen im Vordergrund.

Der Schutzbedarf ist hier normal.

Beispiele: öffentlich zugängliche Internetseiten.

intern: Informationen, die im Interesse der Cloud User oder der Organisation liegen und nicht öffentlich zugänglich sind. Dabei handelt es sich um Daten, deren Kenntnisnahme an ein berechtigtes Interesse des Einsichtsnehmenden gebunden ist (Zugangs- und Zugriffskontrolle). Es sind alle Informationen intern und dürfen nicht ohne eine Genehmigung veröffentlicht werden.

Der Schutzbedarf ist hier normal.

Beispiele: Organisationsrichtlinien, Besprechungsprotokolle, Urlaubspläne, Organigramm, Organisationsprozesse.

vertraulich: Wenn die Informationen nur einem eingeschränkten Personenkreis zur Einsicht zur Verfügung stehen dürfen oder die Preisgabe der Information die

Gefahr einer Schädigung der Interessen von Kunden, der Organisation und/oder der Mitarbeiter schaffen würde.

Der Schutzbedarf ist hier hoch bis sehr hoch.

Beispiele: Angebote, Einkaufskonditionen, IT-Dokumentation, Strategiepapiere.

personenbezogen: Datenschutzklasse III nach KDG-DVO: Daten, aus denen die rassische und ethnische Herkunft , politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (nicht: die bloße Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft) oder Daten über strafrechtliche Verurteilungen und Straftaten und Namens- und Adressangaben mit Sperrvermerken. Zudem Informationen, die dem Beicht- oder Seelsorgegeheimnis unterliegen.

Datenschutzklasse II nach KDG-DVO: Daten über Mietverhältnisse, Informationen zu Geschäftsbeziehungen, Kontaktdaten von Kooperationspartnern/deren Beschäftigten (z.B. Mitarbeiter*innen bei Dienstleistern oder anderen Stellen), Kommunikationsdaten (z. B. ausgetauschte Briefe/E-Mails; Telefonnotizen; Lebensläufe von beteiligten) und Geburts- und Jubiläumsdaten.

Datenschutzklasse I nach KDG-DVO: Namen- und Adressangaben (Personenstammdaten ohne Sperrvermerke); Berufs, Branchen- oder Geschäftsbezeichnungen.

Der Schutzbedarf ist hier hoch bis sehr hoch.

Personenbezogen-freigeben: Alle personenbezogenen Daten, die über ausreichend gesicherte Wege (z.B. Exchange Mail Security) mit externen Stellen geteilt werden dürfen.

NOCloud: Wenn die Preisgabe von Informationen die Gefahr einer erheblichen Schädigung der Interessen des Bistums Limburg bedeutet und eine reale Bedrohung besteht, die durch die Nutzung eines Cloud-Dienstes zu einem höheren oder nicht kontrollierbaren Risiko führt.

Beispiele: Geschäftsgeheimnisse, Entwicklungspläne oder sonstige Informationen, die vor Wirtschaftsspionage oder einer Offenlegung unbedingt zu schützen sind.

Die Erfassung, Speicherung, Verarbeitung, Verteilung oder Archivierung besonderer Kategorien personenbezogener Daten natürlicher Personen (nicht: die bloße Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft) in der Cloud ist untersagt (no-cloud). Dies gilt für personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Es gilt ein besonderer Schutz sensibler Daten für personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.

7.2.2 Schutzbedarf

Für den Schutzbedarf gilt:

normal: Bei einem normalen Schutzbedarf reichen Sicherheitsmaßnahmen aus, die generell für alle Cloud-Dienste gelten und ohne zusätzliche Kosten für einen Cloud Customer zur Verfügung stehen. Diese Sicherheitsmaßnahmen bilden die Grundlage eines Mindeststandards bei einem Cloud-Service-Provider.

Cloud-Dienste sind für einen hochverfügbaren Betrieb durch den Cloud-Service-Provider ausgelegt. Anders sieht es jedoch für die Anwendungen und Daten aus, die durch den Cloud Customer in die Cloud gebracht werden. Fällt eine Anwendung oder eine Datenbank aufgrund einer fehlerhaften Konfiguration oder eines Updates durch den Cloud Customer aus, so steht die gewünschte Funktion möglicherweise nicht mehr zur Verfügung. Hier ist der Cloud Customer selbst für eine Redundanz oder Ausfallsicherheit zuständig.

Der Mindeststandard der Cloud Security unterscheidet sich zwischen den unterschiedlichen Cloud-Service-Provider und Service Modellen. Diese sind daher jeweils zu prüfen. Ein Cloud-Service-Provider stellt viele Sicherheitsfunktionen als Cloud-Service zur Verfügung. Diese sind durch den Cloud Customer selbst

zu installieren und zu konfigurieren, damit der Schutz wirksam wird.

hoch: Hier reicht der Mindeststandard nicht mehr aus und es müssen zusätzliche Maßnahmen individuell getroffen werden. Es soll eine Einzelbetrachtung und eine IT-Risikoanalyse / Business Impact Analyse (BIA) zu den betroffenen Cloud Assets durchgeführt werden.

sehr hoch: Die Folgen bei einer Verletzung von Verfügbarkeit, Integrität, Vertraulichkeit oder Datenschutz können für Betroffene oder die Organisation erheblich sein. Es müssen spezielle Sicherheitsmaßnahmen getroffen werden. Eine Einzelbetrachtung, eine Business Impact Analyse (BIA) und eine IT-Risikoanalyse für Cloud Assets sind üblich. Je nach Risikobehandlung werden individuelle IT-Sicherheitsmaßnahmen umgesetzt und in einem dienstspezifischen Sicherheitskonzept beschrieben.

7.2.3 Beispiel für ein Cloud-Inventar

Das Cloud-Inventar soll darüber Auskunft geben können, bei welchem CSP ein Workload ausgeführt wird, wer in der Organisation die Risiko-Verantwortung hat, welchem Bistumszweck der Workload dient, welche Art von Informationen betroffen sind und welcher Schutzbedarf erforderlich ist.

Beispielsweise könnte ein Eintrag für einen IT-gestützten Prozess für die Auftragsverwaltung in der Cloud, wie folgt aussehen:

Bezeichnung	**Zweck**	**CSP**	**BPO**	**Art**	**Verantwortlich**	**Schutzbedarf**
Auftragsverwaltung	Elektronische Verwaltung von Kundenaufträgen.	MS Azure	FB-AV	Lieferdaten (personenbezogen)	<Fachbereich>	C=n, I=h, A=h

Für den Schutzbedarf gilt hier:

- Eine normale Vertraulichkeit (Confidentiality, C), da es zwar persönliche Ansprechpartner benannt werden, aber es sich nicht um sensible personenbezogene Daten handelt und mit keinem Schaden für die Betroffenen zu rechnen ist. Der Schutzbedarf richtet sich nach dem Wert der Informationen. Der höchste Wert bestimmt den Schutzbedarf (Maximum-Prinzip).
- Eine hohe Integrität (Integrity, I), da fehlerhafte Informationen einen wirtschaftlichen Schaden bedeuten.
- eine hohe Verfügbarkeit (Availability, A), da ohne die Informationen keine Aufträge ausgeführt werden und somit ein wirtschaftlicher Schaden entsteht.

7.3 Cloud-spezifischen Risiken

Die wichtigsten Klassen von Cloud-spezifischen Risiken sind:

7.3.1 Rechtliche Risiken

Es besteht das Risiko bei der Einführung von neuen Technologien, dass gesetzliche Pflichten nicht beachtet werden. Wie alle Kommunikation mit Kunden und Lieferanten unterliegt bspw. auch Mail und Chat den Aufbewahrungspflichten des HGB, der GoBD und ggf. einer festgelegten organisationseigenen Aufbewahrungsfrist oder der KAO.

7.3.2 Risiko des Verlustes der Entscheidungskompetenz (Governance)

Bei der Nutzung von Cloud-Infrastrukturen überlässt der Cloud Customer dem Cloud-Service-Provider notwendigerweise die Kontrolle über eine Reihe sicherheitsrelevanter Aspekte. Gleichzeitig ist es möglich, dass Service Level Agreements seitens des Cloud-Service-Provider keine Verpflichtung zur Bereitstellung solcher Dienste enthalten, was zu einer Lücke in den Sicherheitsvorkehrungen führt.

7.3.3 Lock-in Risiko

Derzeit gibt es keinen einheitlichen Standard für Verfahren oder Formate oder Service-Schnittstellen, die eine Portabilität von Daten, Anwendungen und Diensten gewährleisten. Dies kann es für den Cloud Customer schwierig machen, von einem Cloud-Service-Provider zu einem anderen Cloud-Service-Provider zu wechseln oder Daten und Dienstleistungen wieder in die eigene interne IT-Umgebung zu migrieren. Dies führt zu einer Abhängigkeit von einem bestimmten Cloud-Service-Provider, insbesondere wenn die Datenübertragbarkeit als grundlegendster Aspekt nicht gewährleistet ist.

7.3.4 Risiko von Isolationsfehlern

Mandantenfähigkeit und die Verwendung gemeinsamer Ressourcen prägen die Charakteristik des Cloud Computing. Diese Risikokategorie betrifft das Versagen von Mechanismen, die Storage, Memory, Routing und selbst Reputation zwischen verschiedenen Mandanten trennen (zum Beispiel durch sogenannte Guest-Shopping-Angriffe). Es ist jedoch zu berücksichtigen, dass Angriffe auf Ressourcenisolationsmechanismen (zum Beispiel gegen Hypervisor) in der Praxis selten und für einen Angreifer viel schwieriger zu realisieren sind als Angriffe auf traditionelle Betriebssysteme.

7.3.5 Compliance-Risiken

Investitionen in die Zertifizierung (zum Beispiel zum Nachweis von Industriestandards oder von regulatorischen Anforderungen) können durch die Migration in die Cloud gefährdet sein, wenn der Cloud-Service-Provider nicht nachweisen kann, dass er selbst die einschlägigen Anforderungen erfüllt oder wenn der Cloud-Service-Provider ein Audit durch den Cloud Customer nicht zulässt (was die Regel ist). In bestimmten Fällen bedeutet dies, dass durch die Nutzung einer Public Cloud Infrastruktur bestimmte Compliance-Anforderungen nicht erfüllt werden können.

7.3.6 Risiko einer Kompromittierung der Management-Schnittstelle

Kundenmanagement-Schnittstellen eines Public Cloud-Providers sind über das Internet zugänglich und ermöglichen den Zugriff auf umfangreichere Ressourcen (als herkömmliche Hosting-Provider) und stellen daher ein erhöhtes Risiko dar, insbesondere in Kombination mit Fernzugriff und Webbrowser-Schwachstellen.

7.3.7 Datenschutz-Risiko

Cloud Computing bedeutet mehrere Datenschutzrisiken für den Cloud Customer und Cloud-Service-Provider. In einigen Fällen kann es für den Cloud Customer (in seiner Rolle als Datenverantwortlicher) schwierig sein, die Datenverarbeitungspraktiken des Cloud Providers effektiv auf deren Rechtmäßigkeit zu überprüfen. Dieses Problem verschärft sich bei mehrfachen Datenübertragungen, zum Beispiel zwischen föderierten Clouds. Auf der anderen Seite geben einige Cloud-Anbieter Informationen über ihre Datenschutzpraktiken an. Einige bieten Zusammenfassungen der Zertifizierungen über ihre Datenverarbeitungs- und Datensicherheitsaktivitäten und die von ihnen durchgeführten Datenschutz-Audits an.

7.3.8 Unsichere oder unvollständige Datenlöschung

Wenn vom Cloud Customer eine Anforderung zum Löschen einer Cloud-Ressource an den Cloud-Service-Provider gestellt wird, führt dies nicht zwangsläufig zu einer sicheren Löschung der Daten. Eine angemessene oder rechtzeitige Datenlöschung kann auch unmöglich sein, entweder weil zusätzliche Kopien von Daten gespeichert werden oder weil die zu vernichtenden Datenträger auch Daten von anderen Kunden enthalten. Bei einer Cloud-Umgebung, die Hardware-Ressourcen (inkl. physischer Datenträger) für mehrere Mandanten teilt, besteht ein höheres Risiko für den Cloud Customer als bei dedizierter Hardware.

7.3.9 Risiko durch Insider

Obwohl in der Regel weniger wahrscheinlich, ist der Schaden, der durch Insider beim Cloud-Service-Provider verursacht werden kann, oft weitaus größer. Cloud-Architekturen erfordern bestimmte Rollen, die risikoreich sind. Beispiele sind Cloud-Service-Provider Systemadministratoren und Managed Security Service Provider.

7.3.10 Unzureichendes Identitäts-, Berechtigungs- und Zugriffsmanagement

Datenschutzverletzungen und die Möglichkeit von Angriffen können aufgrund des Fehlens skalierbarer Identitätszugriffsmanagementsysteme, der Nichtverwendung von Multifaktor-Authentifizierung, der schwachen Passwortverwendung und des Fehlens einer kontinuierlichen automatisierten Rotation von kryptografischen Schlüsseln, Passwörtern und Zertifikaten auftreten.

7.3.11 Unsichere Schnittstellen und APIs

Cloud Computing-Anbieter stellen eine Reihe von Software-Benutzeroberflächen (UIs) oder Anwendungsprogrammierschnittstellen (APIs) zur Verfügung, die Kunden zur Verwaltung und Interaktion mit Cloud Services verwenden. Bereitstellung, Management, Orchestrierung und Überwachung erfolgen über diese Schnittstellen. Die Sicherheit und Verfügbarkeit allgemeiner Cloud-Services hängen von der Sicherheit dieser grundlegenden APIs ab. Von der Authentifizierung und Zugangskontrolle bis hin zur Verschlüsselung und

Aktivitätsüberwachung müssen diese Schnittstellen so konzipiert sein, dass sie sowohl vor versehentlichen als auch vor böswilligen Versuchen zur Umgehung von Richtlinien schützen.

Darüber hinaus können Unternehmen und Dritte auf diesen Schnittstellen aufbauen, um ihren Kunden Mehrwertdienste anzubieten. Dies führt zur Komplexität der neuen mehrschichtigen API; es erhöht auch das Risiko, da Unternehmen möglicherweise gezwungen sein können, ihre Anmeldeinformationen an Dritte weiterzugeben, um ihren Account zu aktivieren.

APIs und Benutzeroberflächen sind im Allgemeinen die am stärksten gefährdeten Teile eines Systems, vielleicht das einzige Asset mit einer IP-Adresse, die außerhalb der vertrauenswürdigen Bistumsgrenze verfügbar ist. Diese Vermögenswerte werden das Ziel von Cyberangriffen sein, und angemessene Kontrollen, die sie vor den zu erwartenden Cyberangriffen schützen, sind die erste Verteidigungs- und Erkennungslinie.

7.3.12 System-Schwachstellen

System-Schwachstellen sind ausnutzbare Fehler in Programmen, mit denen Angreifer ein Computersystem infiltrieren können, um Daten zu stehlen, die Kontrolle über das System zu übernehmen oder den Dienstbetrieb zu unterbrechen. Schwachstellen innerhalb der Komponenten des Betriebssystems – Kernel, Systembibliotheken und Anwendungswerkzeuge – stellen ein erhebliches Risiko für die Sicherheit aller Dienste und Daten dar.

Diese Art von Bedrohung ist nichts Neues; Fehler sind seit der Erfindung von Computern ein Problem; sie wurden durch die Schaffung von Netzwerken aus der Ferne nutzbar. Mit dem Aufkommen der Mandantenfähigkeit im Cloud Computing werden Systeme verschiedener Unternehmen in unmittelbarer Nähe zueinander platziert und erhalten Zugriff auf gemeinsamen Speicher und Ressourcen, wodurch eine neue Angriffsfläche entsteht.

7.3.13 Account Hijacking

Account- oder Service-Hijacking ist nicht neu. Angriffsmethoden wie Phishing, Betrug und die Ausnutzung von Software-Schwachstellen führen immer noch zu Ergebnissen. Anmeldeinformationen und Passwörter werden oft wiederverwendet, was die Auswirkungen solcher Angriffe verstärkt. Cloud-Lösungen stellen eine neue Bedrohung für die Landschaft dar. Wenn ein Angreifer Zugriff auf Anmeldeinformationen erhält, kann er die Aktivitäten und Transaktionen abhören, Daten manipulieren, gefälschte Informationen zurückgeben und die Clients an illegale Websites weiterleiten. Die Instanzen eines Kontos oder Dienstes können zu einer neuen Basis für Angreifer werden. Von hier aus können sie die Reputation der Organisation nutzen, um nachfolgende Angriffe zu starten. Gelingt es einem Angreifer das Konto des Hauptadministrators für die Cloud zu übernehmen, hat er praktisch die Möglichkeit auf alle Ressourcen des Kontos zuzugreifen.

7.3.14 Fortgeschrittene persistente Bedrohungen

Advanced Persistent Threats (APTs) sind eine parasitäre Form von Cyberattacken, die Systeme infiltriert, um in der Computerinfrastruktur von Zielunternehmen Fuß zu fassen, aus denen sie Daten und geistiges Eigentum schmuggeln. Die APTs verfolgen ihre Ziele heimlich über einen längeren Zeitraum und passen sich oft an die Sicherheitsmaßnahmen an, die zur Verteidigung gegen sie bestimmt sind. Spear Phishing, die Bereitstellung von Angriffscode über USB-Geräte, die Penetration durch Partnernetzwerke und die Nutzung ungesicherter oder fremder Netzwerke sind häufige Einstiegspunkte für APTs. Einmal an Ort und Stelle, können sich APTs seitlich durch Rechenzentrumsnetze bewegen und sich in den normalen Netzwerkverkehr integrieren, um ihre Ziele zu erreichen.

7.3.15 Datenverlust

In der Cloud gespeicherte Daten können nicht nur aus bösartigen Gründen verloren gehen. Eine versehentliche Löschung durch den Cloud-Service-Provider oder schlimmer noch, eine physische Katastrophe wie ein Brand oder ein Erdbeben kann zum dauerhaften Verlust von Kundendaten führen, es sei denn, der Cloud-Service-Provider oder Cloud Customer ergreift geeignete Maßnahmen zur Datensicherung, unter Beachtung von Best Practices in Business Continuity und Disaster Recovery – sowie zur täglichen Datensicherung und möglicherweise zur externen Speicherung. Darüber hinaus liegt die Last der Vermeidung von Datenverlust nicht nur auf den Schultern des Anbieters. Wenn ein Cloud Customer seine Daten vor dem Hochladen in die Cloud verschlüsselt, aber den Schlüssel verliert, sind die Daten ebenfalls verloren.

7.3.16 Denial-of-Service

Denial-of-Service (DoS)-Angriffe sind Angriffe, die verhindern sollen, dass Nutzer eines Dienstes auf ihre Daten oder ihre Anwendungen zugreifen können. Indem der Angreifer oder die Angreifer, wie bei DDoS-Angriffen (Distributed Denial-of-Service), den betreffenden Cloud-Service zwingen, übermäßig viele Ressourcen wie Prozessorleistung, Speicher, Festplattenspeicher oder Netzwerkbandbreite zu verbrauchen, verursacht er eine nicht tolerierbare Systemverzögerung bis hin zum Systemausfall und hindert alle legitimen Service-Nutzer an der Verwendung des Dienstes.

7.3.17 Unzulängliche vertragliche Regelungen mit einem Cloud-Diensteanbieter

Aufgrund von unzulänglichen vertraglichen Regelungen mit einem Cloud-Diensteanbieter können viel-fältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Verantwortungsbereiche, Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, kann es passieren, dass der Cloud-Diensteanbieter unbeabsichtigt oder aufgrund fehlender Ressourcen Sicherheitsmaßnahmen nicht oder nur ungenügend umsetzt. Auch wenn Situationen eintreten, die nicht eindeutig vertraglich geregelt sind, können Nachteile für den Auftraggeber daraus resultieren. So nutzen Cloud-Diensteanbieter für ihre Services häufig die Dienste Dritter. Bestehen hier unzureichende vertragliche Vereinbarungen oder wurden die Abhängigkeiten zwischen dem Dienstleister und Dritten nicht offengelegt, kann sich dies auch negativ auf die Informationssicherheit und die Serviceleistung der Institution auswirken.

7.3.18 Mangelnde Planung der Migration zu Cloud-Diensten

Die Migration zu einem Cloud-Dienst ist fast immer eine kritische Phase. Durch mangelhafte Planungen können Fehler auftreten, die sich auf die Informationssicherheit innerhalb der Institution auswirken. Verzichtet eine Institution beispielsweise durch eine ungenügende Planungsphase leichtfertig auf eine stufenweise Migration, kann dies in der Praxis zu erheblichen Problemen führen. Gibt es im Vorfeld etwa keine Testphasen, Pilot-Benutzer oder einen zeitlich begrenzten Parallelbetrieb von bestehender Infrastruktur und Cloud-Diensten, können wichtige Daten verloren gehen oder Dienste komplett ausfallen.

7.3.19 Unzureichende Regelungen für das Ende eines Cloud-Nutzungs-Vorhabens

Unzureichende Regelungen für eine mögliche Kündigung des Vertragsverhältnisses können gravierende Folgen für die Institution haben. Das ist erfahrungsgemäß immer dann besonders problematisch, wenn ein aus Sicht der Institution kritischer Fall unerwartet eintritt, wie beispielsweise die Insolvenz, der Verkauf des Cloud-Diensteanbieters oder schwerwiegende Sicherheitsbedenken. Ohne eine ausreichende interne Vorsorge sowie genaue Vertragsregelungen kann sich die Institution nur schwer aus dem abgeschlossenen Vertrag mit dem Cloud-Diensteanbieter lösen. In diesem Fall ist es schwierig bis unmöglich, den ausgelagerten Cloud-Dienst zeitnah beispielsweise auf einen anderen Diensteanbieter zu übertragen oder ihn wieder in die eigene Institution einzugliedern. Auch kann eine unzureichend geregelte Datenlöschung nach Vertragsende dazu führen, dass unberechtigt auf die Informationen der Institution zugegriffen wird.

7.4 Abkürzungsverzeichnis

Abkürzung	Begriffsdefinition
API	Application Programming Interface (Programmschnittstelle)
APT	Advanced Persistent Threat
AWS	Amazon Web Services
Azure	Microsoft Azure Cloud
BCM	Business Continuity Management
BIA	Business Impact Analyse
BPO	Business Process Owner
BSI	Bundesamt für Sicherheit in der Informationstechnik
CapEx	Capital Expenditure (Investitionskosten)
CASB	Cloud Access Security Broker
CD	Continuous Deployment
CDN	Content Delivery Network
CI	Continuous Integration
CIAM	Customer Identity and Access Management
CISO	Chief Information Security Officer
CMP	Cloud Management Platform
CSA	Cloud Security Alliance
CSB	Cloud Service Broker
CSG	Cloud Security Gateway
CSP	Cloud-Service-Provider (gelegentlich auch: Cloud Solution Provider)
CWPP	Cloud Workload Protection Platform
DaaS	Desktop as a Service
DbaaS	Database as a Service
DLP	Data Loss Prevention

DR	Disaster Recovery
DraaS	Disaster Recovery as a Service
EC2	Elastic Cloud Computing (AWS Dienst)
ENISA	European Union Agency for Network and Information Security
EU-DSGVO	Datenschutz-Grundverordnung der Europäischen Union
FaaS	Function as a Service
FIM	Microsoft Forefront Identity Manager
GCP	Google Cloud Platform
HCMS	Hybrid Cloud Management Solution
HIPS	Host Intrusion Prevention System
HSM	Hardware Security Module (Schlüsselspeicher)
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IdaaS	Identity as a Service
ITSB	IT Sicherheitsbeauftragter
IP	Intellectual Property (geistiges Eigentum)
IPS	Intrusion Prevention System
ISO	International Standards Organization
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
MFA	Multi-Faktor-Authentifizierung
MSP	Managed Service Provider
MTA	Microsoft Technology Associate
M365	Microsoft 365
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology (Organisation)
OpEx	Operational Expenditure (Betriebskosten)
OWASP	Open Web Application Security Project
O365	Office 365
PaaS	Platform as a Service
PAM	Privileged Account Management (oft synonym zu PIM)
PBAC	Policy Based Access Control
PII	Personally Identifiable Information (personenbezogene Daten)
PIM	Privileged Identity Management (oft synonym zu PAM)
PoC	Proof-of-Concept (Machbarkeitsstudie)
PSM	Privileged Session Management
RBAC	Role Based Access Control
RZ	Rechenzentrum
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SSL	Secure Sockets Layer
SSO	Single Sign On
TCO	Total Cost of Ownership
TLS	Transport Layer Security
VM	Virtuelle Maschine
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall

Nr. 45 Totenmeldung

Am am 27. März 2026 verstarb Herr Pfarrer i. R. Karl-Heinz Diehl im Alter von 75 Jahren in Dernbach.

Karl-Heinz Diehl wurde am 29. November 1950 in Duisburg-Hamborn geboren. Dort und nach einem Umzug nach Lahr besuchte er die Hauptschule und wechselte danach an die gewerbliche Berufsfachschule in Limburg, die er im Jahr 1966 mit dem Berufsfachschulzeugnis abschloss. Es folgte eine Ausbildung zum Fernmeldehandwerker beim Fernmeldeamt der Deutschen Bundespost in Gießen. Nach erfolgreichem Abschluss der Ausbildung war er von August 1970 bis Juni 1971 Schüler der Berufsaufbauschule in Limburg und erwarb die Fachschulreife. Nach dem Besuch des Ketteler-Kollegs in Mainz erlangte er nach weiteren drei Jahren im Juni 1974 die Hochschulreife.

Zum Wintersemester 1974/1975 begann er das Studium der Philosophie und der Theologie an der Hochschule Sankt Georgen in Frankfurt. Für zwei Semester studierte er an der Universität München. Nach dem Abschluss des Studiums und dem Empfang der Diakonenweihe am 23. Februar 1980 wurde er Diakon in der Pfarrei St. Bernhard in Frankfurt.

Am 6. Dezember 1980 weihte ihn Bischof Dr. Wilhelm Kempf im Limburger Dom zum Priester.

Als Neupriester-Praktikant war er zunächst vom 1. Januar bis zum 31. Juli 1981 in der Pfarrei Maria Königin in Niedernhausen eingesetzt. Es folgten Kaplansstellen in Königstein-Falkenstein und Königstein-Schneidhain (1. August 1981 bis 31. August 1984) sowie in Elz (1. September 1984 bis 31. August 1988). Dort war die Stelle zugleich mit der Aufgabe des Spirituals für das Musische Internat der Domsingknaben in Hadamar verbunden. Diese seelsorgliche Tätigkeit bereitete ihm große Freude, nicht zuletzt deshalb, weil er dabei seine musikalische Begabung gut einbringen konnte. Zusätzlich war er vom 1. April 1986 bis zum 14. Juni 1986 Pfarrverwalter der Pfarrei St. Johannes der Täufer in Elz. Das Bistum ermöglichte ihm im Anschluss eine einjährige Teilnahme an einer Fortbildung in der kirchlichen Medienarbeit am Institut zur Förderung publizistischen Nachwuchses in München.

Mit der Fortbildung war ein fünfmonatiges Praktikum beim Deutschlandfunk in Köln verbunden.

Zum 1. September 1989 übertrug ihm der Bischof die Pfarrei St. Albert in Frankfurt. Von Juni bis Ende August 2005 war er zugleich Pfarrverwalter der Pfarrei St. Josef in Frankfurt-Eschersheim.

Zusätzlich zu seinen Diensten in der Pfarrei war Pfarrer Diehl Diözesanbeauftragter für die Hörfunkarbeit beim Hessischen Rundfunk und Leiter der Sendearbeitsgemeinschaft Rundfunk und Fernsehen beim Hessischen Rundfunk. In Zeiten von Programmreformen und Sparanstrengungen setzte er sich mit großem Engagement für das Anliegen des Konzils ein, das in der Verkündigung der Heilsbotschaft durch die Sozialen Kommunikationsmittel eine Pflicht sah. Die Umstände, wie er für die Verkündigung des Evangeliums eintreten konnte, reizten ihn sehr: Auf der einen Seite der Bertramstraße seine Pfarrei mit der Kirche St. Albert, auf der anderen Seite die Sendegebäude des Hessischen Rundfunks. Gleichwohl war diese Doppelaufgabe für ihn mit einer hohen Arbeitsbelastung verbunden.

Am 1. Juni 2006 wurde Pfarrer Diehl die Leitung der Pfarreien St. Anna – St. Raphael in Frankfurt-Hausen und Christ-König in Frankfurt-Praunheim anvertraut. Zum 1. Februar 2007 kamen die Leitung der Pfarrei St. Antonius in Frankfurt-Rödelheim und das Amt des priesterlichen Leiters des Pastoralen Raumes Nidda-Rödelheim hinzu. Darüber hinaus war er stets bereit, zusätzliche Pfarrverwaltungen zu übernehmen, so etwa für die Pfarreien St. Elisabeth und Frauenfrieden in Frankfurt im September 2014.

Zum 1. März 2015 nahm der Apostolische Administrator den Verzicht von Pfarrer Diehl auf die drei Frankfurter Pfarreien an und ernannte ihn zum Kooperator im Pastoralen Raum Frankfurt-West. Zum 1. Oktober 2015 trat Pfarrer Diehl in den Ruhestand und zog nach Montabaur in die Nähe eines Neffen. Hier übernahm er gerne Gottesdienste und half in der Pastoral mit. Seit einigen Jahren kämpfte Pfarrer Diehl mit einer Krebserkrankung. Als die Kräfte nachließen, übernahm er Gottesdienste bei den Schwestern in Dernbach. Seit Dezember 2025 zeichnete sich ab, dass die Erkrankung zunahm, so dass Pfarrer Diehl nicht mehr in seine Wohnung zurückkehren konnte und im Seniorenzentrum St. Josef und St. Agnes in Dernbach lebte und dort auch verstarb.

Pfarrer Diehl war in seinen verschiedenen Aufgaben ein geschätzter Seelsorger, der immer ein Ohr für die Anliegen der Menschen hatte. Seine Kommunikationsfreudigkeit eröffnete ihm viele Wege. Er verstand es Themen verständlich ins Wort zu bringen, Meinungen klar auszusprechen und dabei durchaus auch einmal zu irritieren. Für ihn stand die Botschaft von Jesus Christus im Mittelpunkt, sei es in Predigten, sei es in der Fortbildung und bei der Vorbereitung von Gottesdienstübertragungen. Träger der Verkündigung war für ihn neben dem Wort immer auch die Kunst, nicht zuletzt die Musik, die ihn auch durch schwierige Zeiten getragen hat. Mit der klaren Zuversicht auf die Auferstehung ist er – wie er selbst sagte – lebenssatt und in Dankbarkeit für alles Erlebte gestorben.

Wir danken Herrn Pfarrer Diehl für sein Wirken in unserem Bistum. Vertrauensvoll übergeben wir ihn in die Hände des barmherzigen Gottes und empfehlen den Verstorbenen dem Gebet der Mitbrüder und dem Gebet aller, mit denen er aus dem Glauben heraus gelebt und für die er gewirkt hat.

Auf Wunsch des Verstorbenen und aufgrund einer besonderen Verbundenheit wurden Requien im Kloster Helfta und in der Abtei Münsterschwarzach gefeiert.

Die Trauerfeier und Urnenbeisetzung fand auf dem Friedhof in Walbrunn-Lahr (Friedhofsweg).

Nr. 46 Dienstnachrichten

Priester

Mit Termin 1. März 2026 wird Father Alvin Nismal Vince CRUZ als Leiter der Seelsorge der philippinischen Katholiken in Frankfurt eingesetzt.

Mit Termin 31. März 2026 hat der Erste Rat der Europäischen Provinzleitung der Schönstatt-Patres den Gestellungsvertrag für Pater Michael CZYSCH ISch gekündigt.

Mit Termin 14. April 2026 scheidet Pater Roy CHETHIPUZHA Joseph OSS aufgrund Wahl zum Provinzial seiner Gemeinschaft aus dem Dienst des Bistums aus.
Mit Termin 1. Juli 2026 tritt Pfarrer Matthias OHLIG in den Ruhestand.

Mit Termin 1. August 2026 bis zur Wiederbesetzung der Pfarrei wird Pfarrer Robert GINTER zum Pfarr-

verwalter der Pfarrei St. Peter und Paul Wiesbaden ernannt.

Mit Termin 1. September 2026 wird Kaplan Moritz HEMSTEG zum Aufbaustudium im Bereich der Dogmatik in München freigestellt.

Mit Termin 1. September 2026 hat der Exarch für die katholischen Ukrainer des byzantinischen Ritus in Deutschland und Skandinavien Pfarrer Dr. Mykola DOBRA mit der Seelsorge an den Ukrainern auf dem Gebiet des Bistums Limburg beauftragt.

Nach Annahme der Bitte um die Versetzung in den Ruhestand durch den zuständigen Exarchen scheidet Pfarrer Roman LIRKA zum 1. November 2026 aus dem Dienst des Bistums aus.

Hauptamtliche Pastorale Mitarbeiterinnen und Mitarbeiter

Mit Termin 1. März 2026 wird Pastoralreferent Edwin BORG mit einem Beschäftigungsumfang von 50 % aus dem Schwerpunkt Familie im Fachteam Lebensphasenbegleitende Seelsorge in die Pfarrei St. Anna Biebertal versetzt.

Mit Termin 31. Mai 2026 tritt Pastoralreferentin Gabriela von MELLE in den Ruhestand.

Mit Termin 1. September 2026 wird Pastoralreferentin Caroline SCHNEIDER mit einem Beschäftigungsumfang von 75 % aus der Pfarrei St. Teresa am Main in die Pfarrei St. Franziskus Kelkheim versetzt.

Weitere Dienstnachrichten

Mit Termin 11. März 2026 wurde Frau Regionalleiterin Christina KUNKEL vom Vorsitz des Verwaltungsgremiums des Roncallihauses in Wiesbaden entpflichtet.

Mit Termin 11. März 2026 wurde Herr Regionalleiter Jürgen OTTO zum Vorsitzenden des Verwaltungsgremiums des Roncallihauses in Wiesbaden berufen.

Mit Termin 30. Juni 2026 scheidet Frau Christina KUNKEL, Regionalleiterin der Katholischen Region Wiesbaden – Rheingau-Taunus, aus dem Dienst des Bistums Limburg aus.

KATHOLISCHE
KIRCHE
BISTUM LIMBURG

Verlag des Bischöflichen Ordinariates Limburg, 65549 Limburg a. d. Lahn, E-Mail: verlag@bistumlimburg.de.
Herstellung: Druckerei Christof Heymann, Beselich. Bezugspreis: jährlich 23,- Euro.