

Microsoft 365 im kirchlichen Krankenhaus: Büro-IT, Zusammenarbeit und Telefonie – das KIS bleibt das KIS

Es gibt eine Sorte Besprechung, die in kirchlichen Krankenhäusern erstaunlich zuverlässig stattfindet. Jemand aus der Geschäftsführung hat gehört, dass man mit Microsoft 365 „endlich alles digital“ machen könne. Jemand aus der IT weiß, dass das Krankenhausinformationssystem seit Jahren mit drei Schnittstellen und einem Wartungsvertrag zusammengehalten wird. Und jemand aus dem Datenschutz sitzt daneben und rechnet im Kopf aus, wie viele Gesetze gleichzeitig verletzt würden, wenn die Vorstellung aus der ersten Reihe wahr würde. Am Ende geht man auseinander, ohne etwas entschieden zu haben. Das ist immerhin besser als die Alternative.

Dieser Beitrag räumt genau diese Besprechung auf. Er zieht die Linie, die in kirchlichen Häusern zu selten schriftlich existiert: Microsoft 365 ist ein hervorragendes Werkzeug für Verwaltung, Leitung, Gremienarbeit, Projektarbeit, Qualitätsmanagement und Bürotelefonie. Es ist kein Primärsystem. Es wird kein Krankenhausinformationssystem, kein Patientendatenmanagementsystem, kein Bildarchiv und ganz sicher keine Alarmierungsanlage. Wer diese Linie einmal sauber zieht, spart sich die nächsten fünf Jahre Diskussion – und vermutlich eine Meldung an die kirchliche Datenschutzaufsicht.

Und ja, ein kirchliches Krankenhaus hat gegenüber einem kommunalen Haus eine zusätzliche Ebene. Nicht eine schlimmere, aber eine weitere. Zum Patientendatenschutz, zu den IT-Sicherheitsanforderungen des Sozialgesetzbuchs, zu KRITIS und zu den Auflagen aus der Krankenzukunftsförderung kommt das kirchliche Datenschutzrecht: auf evangelischer Seite das DSG-EKD, auf katholischer Seite das KDG. Mit eigener Aufsicht, eigener Rechtsordnung und eigener Systematik. Wer aus der kommunalen Welt kommt und glaubt, er könne sein DSGVO-Konzept eins zu eins übernehmen, merkt das spätestens beim ersten Gespräch mit dem Diözesandatenschutzbeauftragten oder dem Beauftragten für den Datenschutz der EKD.

Dieser Beitrag ist Teil der Serie [Microsoft 365 in Kirche, Diakonie und Caritas](#). Dort findest du die Gesamteinordnung, von der Kirchengemeinde bis zum diakonischen Großträger. Wenn dein Haus kommunal ist und du hier nur zufällig gelandet bist: Für öffentliche Träger gilt der Kompetenzbereich [Microsoft 365 in der öffentlichen Verwaltung](#) – die technischen Fragen sind dieselben, die Rechtsgrundlagen nicht.

FAKTEN – Der Regelwerksstapel, verifiziert

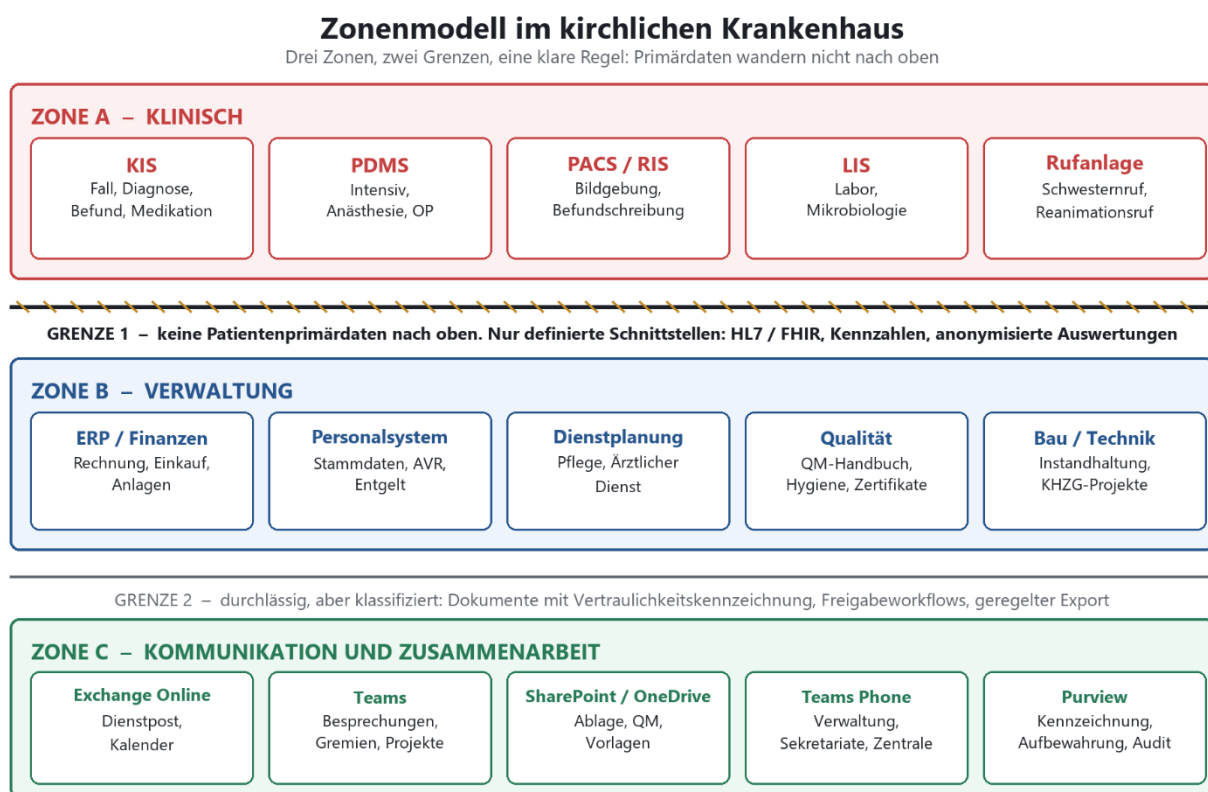
Ein kirchliches Krankenhaus arbeitet Stand heute unter mindestens vier Ebenen gleichzeitig. Diese Eckdaten sind gegen Primärquellen geprüft:

- Die IT-Sicherheitspflicht für Krankenhäuser steht seit dem Digital-Gesetz in § 391 SGB V; die Norm ist am 26. März 2024 in Kraft getreten und hat den früheren § 75c SGB V abgelöst. Sie gilt für Häuser jeder Größe, unabhängig von KRITIS.
- Als kritische Infrastruktur gilt ein zugelassenes Krankenhaus, das den Schwellenwert von 30.000 vollstationären Fällen im Jahr erreicht. Die Selbstprüfung erfolgt jährlich zum 31. März.
- Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz ist am 6. Dezember 2025 in Kraft getreten. Die Registrierungsfrist beim BSI lief zum 6. März 2026; das BSI hat eine Nachfrist bis zum 31. Juli 2026 gesetzt.
- Aus der Krankenzukunftsförderung stammt der Fördertatbestand IT-Sicherheit; mindestens 15 Prozent der Fördermittel müssen dorthin fließen, Umsetzungsfrist ist der 31. Dezember 2026.

- Auf katholischer Seite ist das KDG novelliert: Die Vollversammlung des Verbands der Diözesen Deutschlands hat die Novelle am 24. November 2025 beschlossen, in Kraft in den Diözesen seit dem 1. März 2026. Konzepte, die noch die alte Fassung zitieren, sind Altpapier.

Drei Zonen, zwei Grenzen: das Ordnungsmodell, das alles trägt

Bevor irgendjemand über Lizenzen, Tenants oder Migrationswellen redet, braucht dein Haus ein Zonenmodell. Es ist ein Blatt Papier, es kostet einen Nachmittag, und es beendet ungefähr achtzig Prozent aller späteren Grundsatzdiskussionen. Die Idee ist simpel: Du teilst die Systemlandschaft in drei Zonen und legst fest, was zwischen ihnen fließen darf.



Skizze 1: Zonenmodell. Zone A bleibt bei den Primärsystemen, Zone C ist Microsoft 365, Zone B liegt dazwischen und ist der eigentliche Verhandlungsraum.

Zone A: klinisch – hier hat Microsoft 365 nichts zu suchen

In Zone A liegt alles, was direkt der Behandlung dient. Das Krankenhausinformationssystem mit Fall, Diagnose, Befund und Medikation. Das Patientendatenmanagementsystem auf Intensiv, in der Anästhesie und im OP. Das Bildarchiv und das radiologische Informationssystem. Das Laborsystem. Und die Rufanlage, die nach DIN VDE 0834 geplant, betrieben und geprüft wird und über die im Zweifel ein Reanimationsruf läuft.

Diese Systeme sind nicht deshalb tabu, weil Microsoft 365 schlecht wäre. Sie sind tabu, weil sie andere Eigenschaften haben müssen. Ein Befund muss über Jahrzehnte revisionssicher auffindbar sein, in einem System, dessen Datenmodell ein Medizincontroller versteht. Ein Alarm muss innerhalb von Sekunden ankommen, und zwar auch dann, wenn die Internetanbindung des Hauses gerade von einem Bagger neu sortiert wurde. Beides ist kein Anwendungsfall für einen

Zusammenarbeitsdienst, der seine Stärke im Umgang mit Dokumenten, Terminen und Gesprächen hat.

Zone B: Verwaltung – der eigentliche Verhandlungsraum

Zone B ist die Zone, in der die interessanten Gespräche stattfinden. Hier liegen ERP, Personalsystem, Dienstplanung, Qualitätsmanagement und die technische Gebäudeverwaltung. Diese Systeme bleiben Primärsysteme für ihre Kerndaten – aber alles, was um sie herum passiert, ist Zusammenarbeit. Der Freigabeworkflow für eine Investition, die Abstimmung zum Hygieneplan, die Vorbereitung der Begehung, die Projektdokumentation der Fördermaßnahme. Genau dort ist Microsoft 365 stark.

Die Kunst besteht darin, nicht in die Falle der Doppelführung zu laufen. Sobald dieselbe Information in einer SharePoint-Liste und im ERP gepflegt wird, hast du keine Digitalisierung gebaut, sondern eine zweite Wahrheitsquelle. In sechs Monaten weiß niemand mehr, welche stimmt. Faustregel: Das Fachsystem führt die Daten, Microsoft 365 führt den Vorgang.

Zone C: Kommunikation und Zusammenarbeit – das ist der Tenant

Zone C ist Microsoft 365 im engeren Sinne: Dienstpost und Kalender, Besprechungen, Gremienarbeit, Ablage, Vorlagen, Bürotelefonie und die dazugehörige Verwaltung von Kennzeichnung, Aufbewahrung und Protokollierung. Das ist kein Trostpreis. In einem Haus mit tausend Beschäftigten ist die Verwaltung der größte einzelne Dokumentenproduzent, und sie arbeitet in vielen Häusern immer noch mit Dateiablagen, deren Ordnerstruktur aus der Zeit vor dem letzten Trägerwechsel stammt.

Die Zuordnungstabelle, die du ausdrucken und aufhängen solltest

Die folgende Tabelle ist der Kern dieses Beitrags. Sie beantwortet für jeden Bereich vier Fragen: Ist Microsoft 365 geeignet? Welches Primärsystem bleibt? Und was fließt an der Schnittstelle tatsächlich? Nimm sie als Vorlage, streiche, was bei dir anders heißt, und lasse sie von Geschäftsführung, IT-Leitung und Datenschutz gemeinsam abzeichnen.

Bereich	Microsoft 365 geeignet	Primärsystem bleibt	Schnittstelle
Patientenakte, Diagnose, Befund, Medikation	Nein	KIS	Keine Kopie in den Tenant; Zugriff ausschließlich im KIS-Kontext
Intensiv-, Anästhesie- und OP-Dokumentation	Nein	PDMS	Keine; Datenübergabe nur KIS-seitig
Bildgebung und Befundung	Nein	PACS und RIS	Keine; Befundwege über die medizinischen Kanäle
Labor und Mikrobiologie	Nein	LIS	Keine; Ergebnisse gehen ins KIS, nicht ins Postfach
Schwesternruf, Reanimations- und Notfallalarmierung	Nein, unter keinen Umständen	Rufanlage, Alarmserver, DECT	Keine; technisch und organisatorisch getrennt
Dienst- und Schichtplanung Pflege	Nur als Anzeige	Dienstplansystem	Einbahn-Export in den Kalender oder in Schichten; keine Planung im Tenant
Personalakte und Entgelt	Nein für die Akte	Personalsystem	Dokumentenübergabe, Signaturprozess, Bewerbungskommunikation
Finanzen, Einkauf, Rechnungsprüfung	Ja für Vorgang und Freigabe	ERP	Freigabeworkflow, Belegablage, Zahlungsfreigabe bleibt im ERP
Qualitätsmanagement und	Ja	ggf. QM-Fachsystem	Ablage, Versionierung, Lenkung

Hygiene			von Dokumenten
Gremien: Aufsichtsrat, Trägerkonferenz, MAV	Ja	entfällt	entfällt
Bau-, Technik- und Förderprojekte	Ja	entfällt	entfällt; Nachweise gehören in eine geordnete Projektablage
Fortbildung, Einarbeitung, Unterweisung	Ja	ggf. Lernplattform	Verlinkung und Nachweisführung
Bürotelefonie Verwaltung, Sekretariate, Zentrale	Ja	TK-Anlage für klinische Bereiche	Rufnummernplan, Session Border Controller
Kommunikation mit Einweisern und Praxen	Eingeschränkt	Dienste der Telematikinfrastruktur	Keine Patientendaten über die Dienstpost

WARNUNG – Der häufigste Einzelfehler in kirchlichen Häusern

Nicht die große Architekturentscheidung geht schief, sondern der kleine Alltag. Ein Chefarztsekretariat legt eine Teams-Besprechung für die Tumorkonferenz an und lädt den Befund als Anlage hoch, weil das schneller geht als der Weg über das KIS. Eine Pflegedienstleitung schickt eine Belegungsliste mit Namen und Diagnosekürzeln per Dienstpost an sieben Stationsleitungen. Ein Arztbrief wird „nur kurz“ in OneDrive zwischengespeichert, weil der Rechner im Arztzimmer wieder langsam ist.

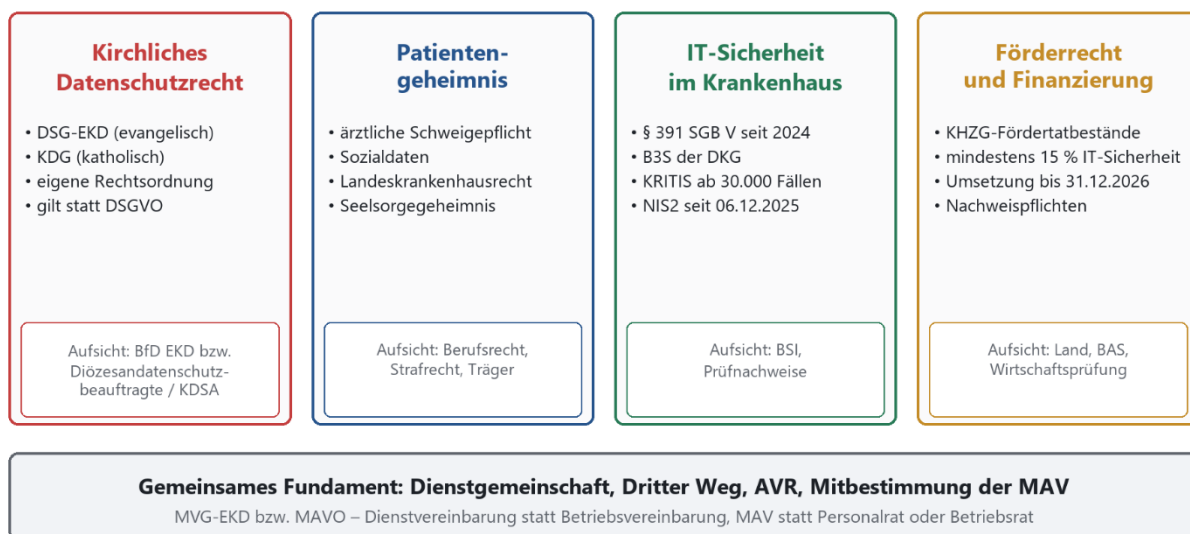
Jeder dieser Vorgänge ist eine Verarbeitung von Gesundheitsdaten außerhalb des dafür vorgesehenen Systems. Nach kirchlichem Datenschutzrecht ist das genauso meldepflichtig wie nach staatlichem – nur bei einer anderen Aufsicht. Und im Unterschied zur großen Architekturfrage merkt es niemand, bis jemand danach sucht.

Die zusätzliche Ebene: DSG-EKD und KDG neben allem anderen

Jetzt zum Teil, der ein kirchliches Krankenhaus tatsächlich von einem kommunalen unterscheidet. Nicht die Technik. Nicht die Patientensicherheit. Sondern die Rechtsordnung, unter der dein Haus steht, und die Aufsicht, die dich kontrolliert.

Vier Regelwerke liegen gleichzeitig auf demselben Haus

Das kirchliche Datenschutzrecht kommt zu allem hinzu, was ein Krankenhaus ohnehin trifft



Ergebnis für den Tenant: eine Konfiguration muss allen vier Ebenen gleichzeitig standhalten.

Wer nur eine Ebene betrachtet, baut zuverlässig an mindestens drei anderen vorbei.

Skizze 2: Vier Regelwerke liegen gleichzeitig auf demselben Haus. Der Tenant muss allen vier gleichzeitig standhalten.

Warum die Kirchen ein eigenes Datenschutzrecht haben – und was das praktisch heißt

Die Kirchen regeln ihre eigenen Angelegenheiten selbst. Das ist keine Marotte, sondern verfassungsrechtlich abgesichertes kirchliches Selbstbestimmungsrecht, und die Datenschutz-Grundverordnung erkennt eigene Datenschutzregelungen der Religionsgemeinschaften ausdrücklich an, sofern sie mit ihr in Einklang gebracht werden. Deshalb gilt für dein Haus nicht die DSGVO, sondern das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland oder das Gesetz über den Kirchlichen Datenschutz der katholischen Kirche.

Für die Praxis bedeutet das drei Dinge. Erstens: Deine Rechtsgrundlagen heißen anders und stehen an anderer Stelle. Zweitens: Deine Aufsicht ist eine andere – der Beauftragte für den Datenschutz der EKD beziehungsweise die Diözesandatenschutzbeauftragten und die kirchlichen Datenschutzzentren. Die Landesdatenschutzbehörde ist für dich nicht zuständig, auch wenn sie freundlich antwortet, wenn du dort anrufst. Drittens: Der Rechtsweg führt über kirchliche Gerichte, auf katholischer Seite über das Interdiözesane Datenschutzgericht und das Datenschutzgericht der Deutschen Bischofskonferenz.

Die Details beider Gesetze sind jeweils einen eigenen Beitrag wert: [DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet](#) und [KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#). Was die Aufsichten im Gespräch tatsächlich sehen wollen, steht in [Kirchliche Datenschutzaufsicht in der Praxis](#). Hier geht es um das, was speziell im Krankenhaus dazukommt.

Was im Krankenhaus zusätzlich obendrauf liegt

Das kirchliche Datenschutzrecht ersetzt nichts von dem, was ein Krankenhaus ohnehin trifft. Es kommt hinzu. Die ärztliche Schweigepflicht ist strafbewehrt und interessiert sich nicht für die Konfession des Trägers. Die landesrechtlichen Krankenhausgesetze gelten weiter. Sozialdatenschutz gilt weiter. Und die IT-Sicherheitspflicht aus dem Sozialgesetzbuch gilt für jedes zugelassene Krankenhaus, egal wie groß.

Dazu kommt eine kirchliche Besonderheit, die im Krankenhaus eine eigene Schärfe hat: das Seelsorgegeheimnis. Was ein Patient der Krankenhauseelsorge anvertraut, unterliegt einem Schutz, der noch enger ist als die ärztliche Schweigepflicht, und er ist kirchenrechtlich eigenständig geregelt. Praktisch heißt das: Seelsorgedokumentation gehört in keinen Teams-Kanal, in kein OneNote-Notizbuch, in keine geteilte Ablage und erst recht in keinen Index, den ein KI-Assistent durchsuchen kann. Die technische Umsetzung ist nicht trivial und hat einen eigenen Beitrag verdient.

Wie du das technisch absicherst, steht in [Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365](#). Für die Klientendaten in angeschlossenen Beratungs- und Pflegeangeboten gilt Vergleichbares, beschrieben in [Klientendaten in Diakonie und Caritas](#).

Die Regelwerkstabelle für deinen Aktenordner

Regelwerk	Gilt für	Aufsicht bzw. Prüfinstanz	Konsequenz für den Tenant
DSG-EKD	evangelische und diakonische Träger und Einrichtungen	Beauftragter für den Datenschutz der EKD	eigene Rechtsgrundlagen, eigene Meldewege, eigene Vertragsformen für Auftragsverarbeitung
KDG in der Fassung seit 1. März 2026	katholische Träger, Caritas, katholische Krankenhäuser	Diözesandatenschutzbeauftragte, katholische Datenschutzzentren	novellierte Fassung ist maßgeblich; alte Konzepte und Musterverträge sind zu prüfen
Ärztliche Schweigepflicht, Landeskrankenhausrecht	jedes Krankenhaus	Berufsrecht, Strafrecht, Träger	Behandlungsdaten verlassen die klinische Zone nicht
§ 391 SGB V, in Kraft seit 26. März 2024	jedes zugelassene Krankenhaus, unabhängig von der Größe	Nachweisführung gegenüber Kostenträgern und Aufsicht	Stand der Technik, Sensibilisierung der Belegschaft ist ausdrücklich Pflichtbestandteil
KRITIS ab 30.000 vollstationären Fällen	große Häuser und Verbünde	BSI	Nachweise alle zwei Jahre, Meldepflichten, branchenspezifischer Sicherheitsstandard der DKG
NIS2-Umsetzungsgesetz, in Kraft seit 6. Dezember 2025	je nach Einstufung auch mittlere Häuser	BSI	Registrierung, Risikomanagement, Meldewege, Verantwortung der Leitung
Krankenhauszukunftsförderung	geförderte Häuser	Land, Bundesamt für Soziale Sicherung, Wirtschaftsprüfung	mindestens 15 Prozent für IT-Sicherheit, Umsetzung bis 31. Dezember 2026, Nachweispflicht
MVG-EKD bzw. MAVO	alle kirchlichen Dienstverhältnisse	MAV, Schlichtungsstelle, kirchliche Arbeitsgerichte	Dienstvereinbarung vor dem Rollout,

	e		nicht danach
--	---	--	--------------

Die MAV ist kein Hindernis, sondern eine Abkürzung

In kirchlichen Häusern gibt es keinen Betriebsrat und keinen Personalrat, sondern die Mitarbeitervertretung. Ihre Rechte ergeben sich auf evangelischer Seite aus dem Mitarbeitervertretungsgesetz der EKD, auf katholischer Seite aus der Mitarbeitervertretungsordnung. Und dort steht, was du schon aus der weltlichen Welt kennst: Die Einführung und Anwendung technischer Einrichtungen, die dazu geeignet sind, Verhalten oder Leistung zu überwachen, ist mitbestimmungspflichtig. Nach der MAVO steht das in § 36 Absatz 1 Nummer 9. Die Dienstvereinbarung nach MVG-EKD ist in § 36 MVG-EKD geregelt.

Das Wort „geeignet“ ist dabei entscheidend. Es kommt nicht darauf an, ob du überwachen willst. Es kommt darauf an, ob das System es könnte. Bei Microsoft 365 lautet die Antwort: selbstverständlich. Anwesenheitsanzeige, Anrufstatistik in der Telefonie, Nutzungsberichte, Protokollierung in Purview, Auswertungen über die Zusammenarbeit – das ist sämtlich mitbestimmungsrelevant, und zwar bevor es eingeschaltet wird.

Der praktische Rat aus vielen Projekten: Hol die MAV in dem Moment an den Tisch, in dem das Zonenmodell entsteht, nicht wenn der Migrationsplan steht. Eine MAV, die den Unterschied zwischen Verwaltungsablage und Patientenakte verstanden hat, ist der beste Verbündete gegen die Kollegin, die den Arztbrief doch in OneDrive legen will. Eine MAV, die drei Wochen vor dem Rollout ein fertiges Konzept auf den Tisch gelegt bekommt, ist es nicht.

Wie eine tragfähige Dienstvereinbarung für Teams, Protokollierung und KI-Assistenz aussieht, steht in [Mitarbeitervertretung und Microsoft 365](#).

WICHTIG – Die Frage, die dir in jeder Aufsichtsprüfung gestellt wird

Sie lautet nicht „Wird Microsoft 365 genutzt?“ – das ist längst geklärt. Sie lautet: Welche Kategorien personenbezogener Daten werden in welchem Dienst verarbeitet, auf welcher Rechtsgrundlage, mit welcher Aufbewahrung, und wodurch ist sichergestellt, dass besonders geschützte Daten dort nicht landen?

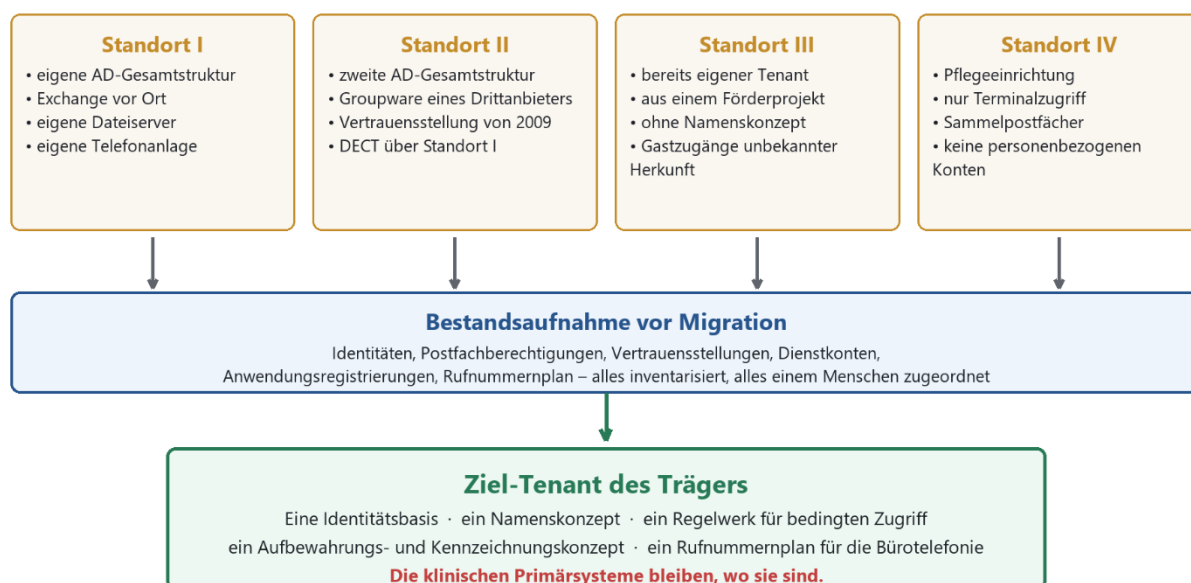
Wenn du auf diese Frage mit einem Zonenmodell, einer Zuordnungstabelle, einem Kennzeichnungskonzept und einer Datenschutz-Folgenabschätzung antworten kannst, ist das Gespräch kurz. Wenn du mit „wir haben die Standardeinstellungen belassen“ antwortest, wird es lang.

Ein Träger, viele Standorte, historisch getrennte IT

Kirchliche Krankenhausträger sind selten am Reißbrett entstanden. Sie sind gewachsen: Ein Haus eines Ordens wurde einer Stiftung übertragen, zwei Häuser eines Kirchenkreises haben fusioniert, ein diakonisches Werk hat eine Pflegeeinrichtung übernommen, ein Bistum hat seine Häuser in einer Trägergesellschaft gebündelt. Auf dem Papier ist das ein Träger. In der IT sind es vier Verzeichnisdienste, drei Mailsysteme, zwei Groupware-Produkte und ein Tenant, den vor Jahren jemand für ein Förderprojekt angelegt hat und dessen Administrator inzwischen in Rente ist.

Ein Träger, vier Standorte, vier Geschichten

Fusionen erzeugen keine gemeinsame IT. Sie erzeugen eine gemeinsame Bilanz und vier Verzeichnisdienste.



Die Konsolidierung ist ein Identitätsprojekt mit angehängter Postfachmigration – nicht umgekehrt.

Skizze 3: Die typische Ausgangslage eines gewachsenen Trägers und der Weg zum gemeinsamen Tenant. Die Bestandsaufnahme ist der Schritt, den alle überspringen wollen.

Warum Migration das falsche erste Wort ist

Die Versuchung ist groß, direkt loszulegen. Postfächer kann man migrieren, Dateiablagen kann man kopieren, es gibt Werkzeuge dafür, und es fühlt sich nach Fortschritt an. Das Problem: Du migrierst nicht nur Daten. Du migrierst Berechtigungen. Und in einer über zwanzig Jahre gewachsenen Landschaft sind Berechtigungen kein Konzept, sondern eine Sedimentschicht.

Konkret heißt das: Vollzugriffsrechte auf Postfächer, die jemand 2011 für eine Urlaubsvertretung vergeben hat. Stellvertreterrechte auf Kalender, deren Inhaber das Haus verlassen hat. Sammelpostfächer, in denen fünfzig Personen mit demselben Kennwort arbeiten. Dienstkonten, die auf Nachnamen lauten, damit sie in der Benutzerliste unauffällig wirken. Vertrauensstellungen zwischen Gesamtstrukturen, die nach einer Trägerumstrukturierung niemand zurückgebaut hat. Wenn du das unverändert in einen gemeinsamen Tenant hebst, hast du den Wildwuchs nicht beseitigt, sondern zentralisiert und mit einem Internetzugang versehen.

AUS DER PRAXIS — Ein katholischer Krankenhausverbund mit mehreren Standorten

Aus der forensischen Arbeit, anonymisiert und ohne Details zum Vorfall selbst: Im Zuge einer Untersuchung wurde die Postfachlandschaft eines Verbunds mit mehreren Standorten ausgewertet. Dabei fiel ein Zugriffsmuster auf ein Verwaltungspostfach auf, das über einen längeren Zeitraum regelmäßig stattfand – technisch einwandfrei berechtigt, protokolliert, unauffällig.

Niemand im Haus konnte sagen, wem dieser Zugriff gehörte. Nicht die IT-Leitung, nicht die Standortadministration, nicht der örtlich Beauftragte für den Datenschutz. Die Berechtigung stammte aus der Zeit vor einer Zusammenführung, war bei der Migration mitgenommen worden und hatte seitdem keine Prüfung mehr gesehen. Die Berechtigungsdokumentation, die es gab, beschrieb einen Zustand, der seit zwei Reorganisationen nicht mehr existierte.

Drei Lehren, die sich in fast jedem gewachsenen Träger wiederholen. Erstens: Ein Zugriff, den niemand zuordnen kann, ist unabhängig von seiner Herkunft ein Befund – gegenüber der kirchlichen Aufsicht musst du ihn bewerten und gegebenenfalls melden, und dafür brauchst du Protokolldaten,

die weit genug zurückreichen. Zweitens: Die Standardaufbewahrung der Protokollierung in Microsoft Purview beträgt in der Basisstufe 180 Tage; wer forensisch arbeiten will, muss die Aufbewahrung vorher verlängert haben, nicht hinterher. Drittens: Die Bestandsaufnahme der Berechtigungen gehört vor die Migration, nicht danach – hinterher weiß niemand mehr, was Altlast war und was du selbst gebaut hast.

Was du inventarisieren musst, bevor irgendetwas umzieht

Die Bestandsaufnahme ist unspektakulär und wird deshalb gern übersprungen. Sie ist trotzdem der Punkt, an dem Projekte gewonnen oder verloren werden. Die folgende Tabelle zeigt, was in einem Träger mit mehreren Standorten typischerweise zu entscheiden ist.

Artefakt aus der Altlandschaft	Typischer Befund	Entscheidung vor der Migration
Postfachberechtigungen und Stellvertretungen	Vollzugriffe ohne Anlass, Inhaber teils nicht mehr im Haus	vollständig auslesen, jedem Eintrag eine verantwortliche Person zuordnen, Rest entfernen
Sammel- und Funktionspostfächer	geteilte Kennwörter, keine personenbezogene Nachvollziehbarkeit	in gemeinsame Postfächer mit personenbezogenem Zugriff überführen
Dienst- und Anwendungskonten	lauten auf Personennamen, Zweck unbekannt, kein Eigentümer	Zweck dokumentieren, Eigentümer benennen, auf moderne Authentifizierung umstellen
Vertrauensstellungen zwischen Gesamtstrukturen	aus früheren Fusionen, wechselseitig, ungeprüft	Abhängigkeiten klären, Rückbauplan mit Termin, nicht mitmigrieren
Vorhandene Tenants einzelner Standorte	aus Förder- oder Pilotprojekten, ohne Namenskonzept	Zieltenant festlegen, Domänen konsolidieren, Altmandanten geordnet stilllegen
Gastzugänge und externe Freigaben	Herkunft unklar, Dienstleister von damals noch berechtigt	Bestand prüfen, Ablaufdatum erzwingen, Freigaberegeln zentral setzen
Dateiablagen der Verwaltung	Ordnerstruktur aus der Zeit vor dem Trägerwechsel, Berechtigungen vererbt	Informationsarchitektur neu entwerfen, nicht eins zu eins kopieren
Rufnummernplan und TK-Anlagen	pro Standort eigene Anlage, Durchwahlbereiche überschneiden sich	gemeinsamen Nummernplan definieren, klinische Bereiche ausdrücklich ausklammern

Die Frage, ob ein Träger einen oder mehrere Tenants betreibt, ist eine Grundsatzentscheidung mit erheblichen Folgen. Sie ist in [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#) ausführlich behandelt. Für die Identitätsseite – Landeskirche, Verband, Träger, Einrichtung – hilft [Entra ID für kirchliche Träger](#). Und wenn dein Haus weiter Anwendungen vor Ort betreibt, die über die Windows-Anmeldung angebunden sind, lohnt ein Blick auf den Kompetenzbereich [Microsoft Kerberos](#) – gerade in Krankenhäusern hängt an dieser Stelle mehr, als die Projektplanung vermuten lässt.

TIPP – Die Reihenfolge, die sich in gewachsenen Trägern bewährt hat

Erst das Zonenmodell, dann die Identitäten, dann die Berechtigungen, dann die Sicherheitsregeln, dann erst die Daten. Wer in dieser Reihenfolge arbeitet, bekommt Migrationswellen, die langweilig verlaufen – und langweilig ist im Krankenhausbetrieb das höchste Lob, das eine IT-Abteilung bekommen kann.

- Bestandsaufnahme in Zahlen ausdrücken: wie viele Postfächer, wie viele Fremdzugriffe, wie viele Konten ohne Eigentümer. Das überzeugt Gremien besser als jede Präsentation.
- Aufbewahrung der Protokollierung erhöhen, bevor du migrierst – nicht, wenn du sie brauchst.
- Jede entfernte Altberechtigung dokumentieren. Das ist gleichzeitig der Nachweis für die Aufsicht und für die Förderprüfung.
- Standort für Standort, nicht alles gleichzeitig. Ein Haus im Regelbetrieb verträgt keine vier parallelen Umstellungen.

Zusammenarbeit und Bürotelefonie: wo Microsoft 365 wirklich liefert

Genug der Abgrenzung. Reden wir darüber, was Microsoft 365 in einem Krankenhaus tatsächlich besser macht – denn das ist erheblich, es betrifft nur eben nicht die Patientenversorgung im engeren Sinne.

Verwaltung, Leitung und Gremien

Die Gremienarbeit eines kirchlichen Trägers ist dokumentenintensiv und terminkritisch. Aufsichtsrat, Trägerkonferenz, Direktorium, Wirtschaftsausschuss, MAV-Sitzungen, die Abstimmung mit dem Landeskirchenamt oder dem Generalvikariat. Das läuft in vielen Häusern immer noch über Papiermappen, die drei Tage vorher per Boten gefahren werden, und über Mailanhänge, deren Versionsstand niemand rekonstruieren kann.

Für diese Arbeit ist Microsoft 365 gebaut: eine strukturierte Ablage pro Gremium, Tagesordnung und Unterlagen an einem Ort, Versionsführung, kontrollierter Zugriff für Mitglieder, geregelte Aufbewahrung nach der Kassationsordnung deines Trägers. Der Unterschied zu einer kommunalen Verwaltung ist dabei weniger technisch als organisatorisch: Kirchliche Gremien haben oft ehrenamtliche Mitglieder, und für die brauchst du eine Antwort, die weder „jeder bekommt ein Vollkonto“ noch „wir schicken es halt per Mail“ lautet.

Für die Ablagestruktur hilft [SharePoint-Informationsarchitektur für Kirchengemeinde und Kirchenkreis](#), für die Gremienarbeit selbst [Gremienarbeit in Microsoft Teams](#), und für die Frage der ehrenamtlichen Zugänge [Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?](#).

Pflegedienstleitung: der Schreibtischanteil, nicht die Station

Eine Pflegedienstleitung hat zwei Arbeitsplätze. Der eine ist die Station, dort wird dokumentiert, dort wird koordiniert, dort läuft alles über die Fachsysteme. Der andere ist der Schreibtisch: Personalgespräche vorbereiten, Fortbildungsplanung, Budgetabstimmung, Hygienebegehung, Kommunikation mit der Geschäftsführung, Zusammenarbeit mit anderen Standorten. Der zweite Arbeitsplatz ist vollständig Microsoft-365-Terrain.

Die häufigste Fehlannahme lautet, man könne auch gleich die Dienstplanung in Teams abbilden. Kann man technisch, sollte man nicht. Dienstplanung in einem kirchlichen Krankenhaus hängt an den Arbeitsvertragsrichtlinien, an Zuschlagsregeln, an Arbeitszeitgesetz und an einer Dienstvereinbarung. Das Fachsystem kennt diese Regeln. Teams kennt sie nicht. Was du sinnvoll machen kannst: die Anzeige des fertigen Plans in die Schichtenfunktion oder den Kalender spiegeln, damit die Belegschaft ihn auf dem Mobilgerät sieht. Geführt wird er woanders.

Für Beschäftigte ohne festen Schreibtisch – Pflege, Service, Technik – gibt es eigene Lizenz- und Gerätemodelle. Beschrieben in [Kita, Pflege, Jugendhilfe: Frontline-Arbeitsplätze in Microsoft 365 für Menschen ohne Schreibtisch](#).

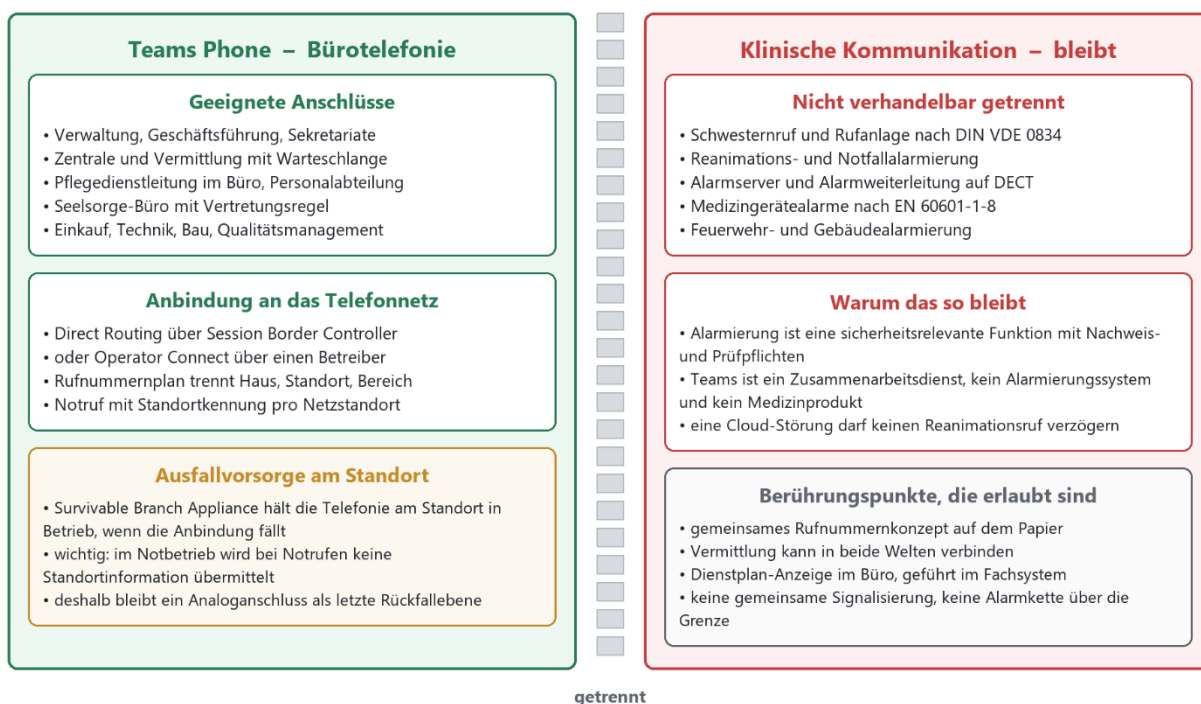
Bürotelefonie ja, Alarmierung niemals

Die Telefonie ist der Bereich, in dem die Abgrenzung am klarsten und gleichzeitig am häufigsten missverstanden wird. Teams Phone ist eine ausgereifte Telefonanlage. Für Verwaltung, Sekretariate, Zentrale, Einkauf, Technik und Leitungsfunktionen ist sie ein echter Gewinn: eine Rufnummer über alle Geräte, Vertretungsregeln, die die Belegschaft selbst pflegt, Warteschlangen für die Zentrale, standortübergreifende Vermittlung ohne Querverbindungen zwischen alten Anlagen.

Und dann hört es auf. Der Schwesternruf ist keine Telefonie. Die Reanimationsalarmierung ist keine Telefonie. Die Weiterleitung eines Medizingerätealarms auf ein DECT-Gerät ist keine Telefonie. Das sind sicherheitsrelevante Funktionen mit Planungs-, Betriebs- und Prüfpflichten nach eigenen Normen – Rufanlagen nach DIN VDE 0834, Alarmsysteme im Umfeld medizinischer elektrischer Geräte nach der zugehörigen Gerätenorm. Teams ist ein Zusammenarbeitssdienst. Es ist kein Alarmierungssystem und kein Medizinprodukt, und kein Vertriebsgespräch der Welt ändert daran etwas.

Bürotelefonie und klinische Kommunikation sind zwei Systeme

Die Trennlinie ist keine Geschmacksfrage, sondern eine Frage der Haftung



Merksatz für die Geschäftsführung: Wer telefoniert, darf in die Cloud. Wer alarmiert, nicht.

Skizze 4: Bürotelefonie und klinische Kommunikation bleiben zwei Systeme. Berührungspunkte auf der Ebene des Nummernplans sind erlaubt, gemeinsame Alarmketten nicht.

Ein Detail, das in Krankenhausprojekten regelmäßig zu spät auffällt: Für den Fall, dass die Anbindung eines Standorts ausfällt, gibt es die Survivable Branch Appliance. Sie hält die Telefonie am Standort in Betrieb, wenn der Weg in die Cloud unterbrochen ist – Anrufe ins Telefonnetz gehen weiter. Aber: Im Notbetrieb wird bei Notrufen keine Standortinformation mitgegeben, und Richtlinien für die Notrufführung greifen dort nicht. Für ein Krankenhaus mit mehreren Gebäuden auf einem Gelände ist das kein Randthema. Die Konsequenz ist unspektakulär und wirksam: Es bleibt eine analoge oder anderweitig unabhängige Rückfallebene, und die Pforte weiß, wo das Gerät steht.

Szenario	Teams Phone	Bleibt bei TK oder	Begründung
----------	-------------	--------------------	------------

		Fachsystem	
Verwaltung, Geschäftsführung, Sekretariate	Ja	—	klassische Bürotelefonie mit Vertretungsbedarf
Zentrale und Vermittlung	Ja	—	Warteschlangen und Weiterleitung sind Kernfunktionen
Pflegedienstleitung im Büro	Ja	—	Schreibtischanteil, keine Alarmfunktion
Krankenhausseelsorge im Büro	Ja, mit strenger Vertretungsregel	—	Erreichbarkeit ja, Gesprächsinhalte werden nirgends dokumentiert
Station und Funktionsbereiche	Nein	DECT und Stationsapparate	Ausfallsicherheit und Kopplung an die Rufanlage
Schwesternruf	Nein	Rufanlage nach DIN VDE 0834	eigenes Normenregime mit Prüf- und Betriebspflichten
Reanimations- und Notfallruf	Nein	Alarmierungssystem des Hauses	sicherheitsrelevant, keine Abhängigkeit von einer Cloud-Anbindung
Medizingerätealarme	Nein	Alarmserver und DECT	Anforderungen an verteilte Alarmsysteme
Notruf aus Verwaltungsbereichen	Ja, mit Standortkennung je Netzstandort	analoge Rückfallebene bleibt	im Notbetrieb der Standortapplianz wird keine Standortinformation übermittelt
Externe Erreichbarkeit des Hauses	Ja	—	gemeinsamer Rufnummernplan über alle Standorte

Kennzeichnung und Aufbewahrung: die zwei Stellschrauben, die wirklich wirken

Wenn du in einem kirchlichen Krankenhaus nur zwei Dinge in Microsoft Purview richtig machen kannst, dann diese: ein schlankes Kennzeichnungskonzept und eine Aufbewahrung, die zur Kassationsordnung deines Trägers passt.

Beim Kennzeichnungskonzept ist der häufigste Fehler die Überkomplexität. Vierzehn Stufen mit Untervarianten sehen im Konzeptpapier beeindruckend aus und werden in der Praxis von niemandem verwendet. Vier bis fünf Stufen reichen: offen, intern, vertraulich, streng vertraulich – und eine gesonderte Stufe für die Bereiche mit besonderem Schutzbedarf, also Seelsorge und Beratung. Entscheidend ist nicht die Anzahl, sondern dass die Stufen mit technischen Folgen hinterlegt sind: Verschlüsselung, eingeschränkte Weitergabe, Ausschluss aus Indizes.

Bei der Aufbewahrung ist die Besonderheit kirchlicher Träger, dass es eben nicht nur staatliche Fristen gibt. Kirchliche Archivgesetze und Kassationsordnungen regeln, was aufzubewahren, was anzubieten und was zu vernichten ist – und sie unterscheiden sich zwischen den Gliedkirchen und zwischen den Diözesen. Das lässt sich in Purview abbilden, aber nur, wenn jemand die Ordnung vorher gelesen hat.

Ein praxistaugliches Label-Konzept beschreibt [Sensitivity Labels für kirchliche Träger](#), die Fristenseite [Kirchliche Aufbewahrungsfristen, Kassationsordnungen und Archivgesetze in Microsoft Purview abbilden](#).

FAKTEN – Datenstandort – die ehrliche Fassung

Microsoft hat die EU-Datengrenze im Februar 2025 abgeschlossen. Mit der letzten Phase werden auch die Daten aus dem technischen Support – vom Kunden übermittelte Protokolle ebenso wie von

Microsoft erzeugte Fallnotizen – in der EU und der EFTA gespeichert. Das ist ein echter Fortschritt und in Gesprächen mit der kirchlichen Aufsicht ein belastbares Argument.

Es ist aber kein Freibrief. Die Aufsichten sehen nach wie vor die Fragen der Nutzung von Daten zu eigenen Zwecken des Anbieters, der Transparenz und der Ausgestaltung der Auftragsverarbeitung. Genau deshalb ist eine Datenschutz-Folgenabschätzung für dein Haus kein Formular, sondern Arbeit – und genau deshalb ist das Zonenmodell so wertvoll: Es beantwortet die schwierigste Frage der Folgenabschätzung, nämlich welche Datenkategorien überhaupt in Reichweite des Dienstes kommen.

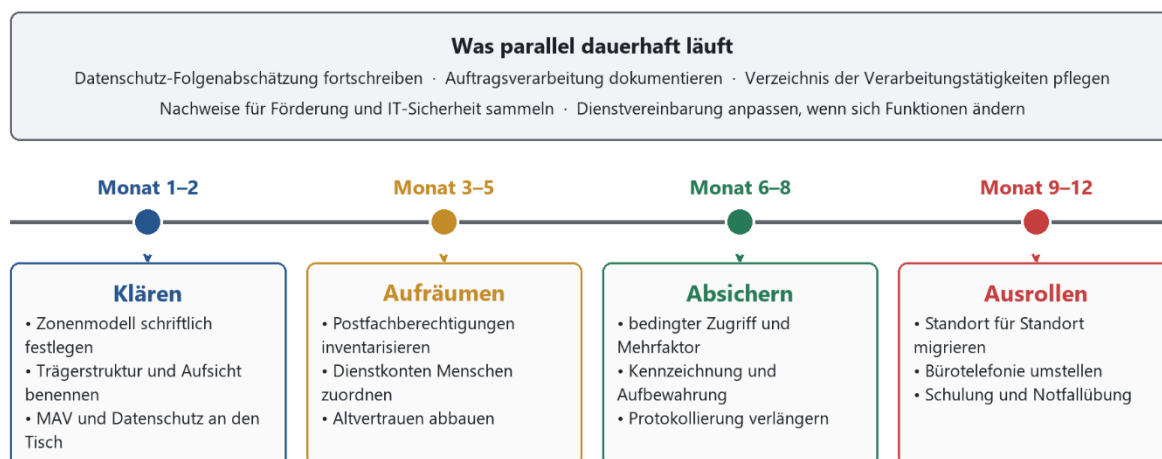
Die Debatte über kirchliche Rechenzentren und Datenstandorte ist in [Die Cloud-Frage in der Kirche](#) ausführlich geführt. Das Vorgehen für eine belastbare Folgenabschätzung steht in [Microsoft 365 für kirchliche Träger: DSG-EKD und KDG](#).

Der Fahrplan: in welcher Reihenfolge du das anfasst

Krankenhäuser haben eine unangenehme Eigenschaft: Sie laufen weiter. Es gibt kein Wochenende, an dem man den Betrieb anhält und die IT neu baut. Jede Umstellung findet im laufenden Betrieb statt, neben Notaufnahme, OP-Programm und Visite. Das diszipliniert die Planung.

Fahrplan für die ersten zwölf Monate

Reihenfolge schlägt Geschwindigkeit. Wer mit der Migration beginnt, migriert seine Altlasten mit.



Skizze 5: Zwölf Monate in vier Phasen. Die Querschnittsaufgaben laufen durchgehend mit und sind der Teil, der später geprüft wird.

Was in welcher Phase passiert

Phase	Ergebnis am Ende der Phase	Wer muss beteiligt sein	Typische Stolperstelle
Monat 1–2: Klären	Zonenmodell und Zuordnungstabelle, von der Geschäftsführung abgezeichnet	Geschäftsführung, IT-Leitung, Ärztliche und Pflegedirektion, örtlich Beauftragter für den Datenschutz, MAV	die Runde wird zu klein besetzt und muss später wiederholt werden
Monat 3–5: Aufräumen	vollständige Inventur von Identitäten, Berechtigungen, Dienstkonten und Rufnummern	IT der Standorte, Datenschutz, gegebenenfalls externe Unterstützung	man beginnt zu migrieren, bevor die Inventur fertig ist
Monat 6–8: Absichern	bedingter Zugriff, Mehrfaktor, Kennzeichnung, Aufbewahrung, verlängerte	IT-Sicherheit, Datenschutz, MAV für alles Auswertbare	Regeln werden für die Verwaltung gebaut und sperren dann den

	Protokollierung		Bereitschaftsdienst aus
Monat 9–12: Ausrollen	Standorte migriert, Bürotelefonie umgestellt, Belegschaft geschult, Notfallübung durchgeführt	alle, plus Kommunikation nach innen	die Schulung wird gestrichen, weil das Budget in der Technik aufgebraucht wurde

Bedingter Zugriff im Krankenhaus ist kein Bürothema

Ein Punkt, der ein Krankenhaus von einer Verwaltung wirklich unterscheidet: Die Regeln für den bedingten Zugriff müssen den Nachtdienst überstehen. Ein Regelwerk, das am Dienstagmorgen in der Verwaltung wunderbar funktioniert, kann am Sonntag um drei Uhr den Hintergrunddienststarzt aussperren, der von zu Hause aus auf ein Dokument zugreifen muss. Die Antwort ist nicht, die Regeln aufzuweichen, sondern sie für Rollen zu entwerfen und die Ausnahmen bewusst und dokumentiert zu setzen – inklusive eines Notfallzugangs, der protokolliert wird und dessen Nutzung jemand am Montagmorgen anschaut.

Ein Regelwerk, das Pfarrbüro, Pflegedienst, Verwaltung und Ehrenamt gleichzeitig abdeckt, ist beschrieben in [Conditional Access und MFA in Kirche und Diakonie](#).

Die Schulung ist kein Beiwerk, sondern Pflichtbestandteil

Dass die Sensibilisierung der Belegschaft im Krankenhaus nicht optional ist, steht inzwischen ausdrücklich im Gesetz: Die IT-Sicherheitsvorschrift für Krankenhäuser nennt verpflichtende Maßnahmen zur Steigerung des Sicherheitsbewusstseins der Beschäftigten ausdrücklich als Teil der zu treffenden Vorkehrungen. Das war in der Vorgängerregelung nicht so deutlich formuliert.

In der Praxis ist das ohnehin der Punkt mit dem besten Verhältnis von Aufwand und Wirkung. Die teuerste Sicherheitsarchitektur scheitert an einer Stationsleitung, die den Arztbrief „nur schnell“ per Dienstpost schickt, weil ihr nie jemand erklärt hat, warum das ein Problem ist. Eine halbe Stunde am richtigen Punkt in der Einarbeitung ersetzt erstaunlich viel Technik.

Häufige Fragen

Dürfen wir als kirchliches Krankenhaus Microsoft 365 überhaupt einsetzen?

Ja. Weder das DSGVO noch das KDG verbieten Microsoft 365. Beide Gesetze stellen Anforderungen – an Rechtsgrundlage, Auftragsverarbeitung, technische und organisatorische Maßnahmen, Dokumentation und in vielen Konstellationen an eine Datenschutz-Folgenabschätzung. Die kirchlichen Aufsichtsbehörden haben in der Vergangenheit deutliche Kritik an Standardkonfigurationen geäußert, insbesondere zur Nutzung von Daten für eigene Zwecke des Anbieters und zur Transparenz. Der praktische Weg besteht darin, den Einsatzbereich sauber abzugrenzen und die Konfiguration zu dokumentieren, statt auf eine pauschale Freigabe zu warten, die es nicht geben wird.

Können wir das KIS nicht doch ablösen und alles in Microsoft 365 machen?

Nein, und zwar nicht aus Bequemlichkeit, sondern aus Architekturgründen. Ein Krankenhausinformationssystem bildet Fall- und Behandlungslogik ab, ist an Abrechnung, Medizincontrolling, Kodierung und gesetzliche Dokumentationspflichten gekoppelt und muss über sehr lange Zeiträume revisionssicher auskunftsfähig sein. Microsoft 365 ist eine Plattform für Kommunikation, Dokumente und Vorgänge. Beides zu vermischen erzeugt eine Landschaft, in der weder die Behandlungsdokumentation noch die Zusammenarbeit funktioniert.

Was ist mit Teams für Tumorkonferenzen und Fallbesprechungen?

Die Besprechung selbst kann in Teams stattfinden – gerade bei mehreren Standorten ist das ein erheblicher Gewinn. Die Falldaten gehören aber nicht in die Besprechung, sondern bleiben im KIS und werden dort gezeigt. Konkret heißt das: keine Befunde als Anlage, keine Patientennamen in Titel oder Chat, keine Aufzeichnung, keine automatische Transkription. Wer hier unsauber arbeitet, erzeugt eine Zweitdokumentation von Gesundheitsdaten in einem System, das dafür nicht vorgesehen ist – mit allen Folgen für Auskunft, Löschung und Meldepflicht.

Wir sind unter dem Schwellenwert für kritische Infrastrukturen. Sind wir damit raus?

Aus KRITIS vielleicht, aus der Pflicht nicht. Die IT-Sicherheitspflicht für Krankenhäuser im Sozialgesetzbuch gilt für jedes zugelassene Krankenhaus, unabhängig von der Größe und unabhängig von der KRITIS-Einstufung. Hinzu kommt die Einstufung nach dem NIS2-Umsetzungsgesetz, die eigenen Kriterien folgt und auch mittlere Einrichtungen erfassen kann. Und das kirchliche Datenschutzrecht kennt ohnehin keine Schwellenwerte.

Die Aufsicht für unser Haus – wer ist das eigentlich genau?

Auf evangelischer Seite der Beauftragte für den Datenschutz der EKD, zuständig für die Einrichtungen im Bereich der EKD und der Diakonie, mit regionalen Strukturen. Auf katholischer Seite die Diözesandatenschutzbeauftragten, organisiert in den katholischen Datenschutzzentren, deren Zuständigkeitsbereiche mehrere Bistümer umfassen. Welches Zentrum für dein Haus zuständig ist, hängt an der Diözese des Trägers, nicht am Standort der Klinik. Bei Trägern mit Häusern in mehreren Bistümern ist das eine Frage, die man vorher klärt und nicht im Meldefall.

Wir haben mehrere Standorte mit eigenen Tenants. Zusammenlegen oder lassen?

In den allermeisten Fällen zusammenlegen – ein Träger, eine Identitätsbasis, ein Regelwerk. Getrennte Tenants sind nur dort sinnvoll, wo tatsächlich getrennte Verantwortlichkeiten im datenschutzrechtlichen Sinne bestehen, und das ist bei Standorten desselben Trägers meist nicht der Fall. Wichtiger als die Entscheidung selbst ist der Weg dorthin: erst inventarisieren, dann Zieltenant festlegen, dann Altmandanten geordnet stilllegen. Ein Tenant, den man einfach stehen lässt, ist ein Zugriffsweg, den niemand mehr beobachtet.

Braucht jede Einstellung eine Dienstvereinbarung?

Nicht jede, aber jede, die Verhalten oder Leistung auswertbar macht. Die MAVO nennt die Einführung und Anwendung technischer Einrichtungen, die zur Überwachung von Verhalten oder Leistung geeignet sind, in § 36 Absatz 1 Nummer 9 ausdrücklich als mitbestimmungspflichtig; das MVG-EKD sieht die Dienstvereinbarung als Instrument in § 36 vor. In der Praxis empfiehlt sich eine Rahmenvereinbarung für die Plattform mit Anlagen für einzelne Funktionen. Dann musst du nicht das Gesamtwerk neu verhandeln, wenn eine Funktion hinzukommt – und bei Microsoft 365 kommt regelmäßig etwas hinzu.

Wie lange müssen wir Protokolldaten aufbewahren?

Das hängt an deinem Schutzbedarf, nicht an einer einzelnen Vorschrift. Wichtig ist die technische Ausgangslage: Die Basisstufe der Protokollierung in Microsoft Purview bewahrt Einträge standardmäßig 180 Tage auf, und der maximale Suchzeitraum entspricht dieser Spanne. Für ein Krankenhaus, das im Ernstfall gegenüber der kirchlichen Aufsicht bewerten muss, ob und wie lange ein unberechtigter Zugriff bestand, ist das häufig zu kurz. Die Aufbewahrung lässt sich erhöhen – aber nur mit Wirkung für die Zukunft. Das ist eine Entscheidung, die du am Anfang triffst, nicht im Vorfall.

Was sagen wir dem Anbieter, der uns Alarmierung über Teams verkaufen will?

Dass Teams kein Alarmierungssystem ist. Rufanlagen in Krankenhäusern und Pflegeeinrichtungen werden nach DIN VDE 0834 geplant, errichtet, betrieben und geprüft, und das Zusammenspiel mit verteilten Alarmsystemen folgt der zugehörigen Norm für medizinische elektrische Geräte. Diese Anforderungen erfüllt ein allgemeiner Zusammenarbeitsdienst nicht, unabhängig davon, wie zuverlässig er im Alltag wirkt. Was es gibt, sind spezialisierte Alarmierungslösungen mit eigener Zulassung – die kann man prüfen. Nur sind das keine Microsoft-365-Produkte.

Unser Haus ist kommunal, nicht kirchlich. Gilt das hier trotzdem?

Das Zonenmodell, die Zuordnungstabelle, die Telefonieabgrenzung und der Fahrplan: ja, unverändert. Die Rechtsebene: nein. Für kommunale Häuser gelten DSGVO, Landesdatenschutzgesetz und die jeweilige Landesdatenschutzaufsicht, statt der MAV gibt es einen Personalrat, und statt Dienstvereinbarungen nach kirchlichem Recht gelten die Personalvertretungsgesetze. Der passende Einstieg dafür ist der Kompetenzbereich zur öffentlichen Verwaltung.

Fazit

Microsoft 365 ist für ein kirchliches Krankenhaus eine ausgezeichnete Plattform – für Verwaltung, Leitung, Gremienarbeit, Projektarbeit, Qualitätsmanagement und Bürotelefonie. Es ist keine Plattform für Behandlungsdaten, nicht für das Krankenhausinformationssystem, nicht für die Intensivdokumentation und unter keinen Umständen für Alarmierung. Diese Grenze zu ziehen ist kein Eingeständnis von Schwäche, sondern die Voraussetzung dafür, dass die Plattform dort, wo sie passt, wirklich gut funktioniert.

Die Besonderheit gegenüber einem kommunalen Haus liegt nicht in der Technik. Sie liegt in der zusätzlichen Rechtsebene: DSG-EKD oder KDG mit eigener Aufsicht und eigener Rechtsordnung, dazu das Seelsorgegeheimnis, die Mitbestimmung über MVG-EKD oder MAVO und die Strukturen eines Trägers, der aus mehreren Häusern gewachsen ist. Nichts davon ist ein Ausschlusskriterium. Alles davon will vor dem Rollout geklärt sein, nicht danach.

Und wenn du aus diesem Beitrag nur eine Sache mitnimmst, dann diese: Bevor du migrierst, inventarisierst. Die Berechtigung, die niemand mehr zuordnen kann, gibt es nicht nur in dem einen Verbund, dessen Fall hier beschrieben ist. Es gibt sie in fast jedem gewachsenen Träger. Der Unterschied liegt allein darin, ob jemand nachgesehen hat, bevor es jemand anderes tut.

WEITERLESEN

- › [Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand](#)
- › [Microsoft 365 Einführungskonzept für kirchliche Träger: Die Kirchnedition zum Festpreis](#)
- › [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#)
- › [Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Frage, wer überhaupt berechtigt ist](#)
- › [Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout](#)
- › [Microsoft 365 Beratung für Verwaltungen](#)
- › [Schulungen für kirchliche Träger](#)

Wenn dein Träger die Abgrenzung schriftlich festhalten und den Tenant darauf ausrichten will, ist das ein überschaubares Vorhaben mit klarem Ergebnis. Ausgangspunkt ist die [Microsoft 365 Beratung für kirchliche Träger](#).