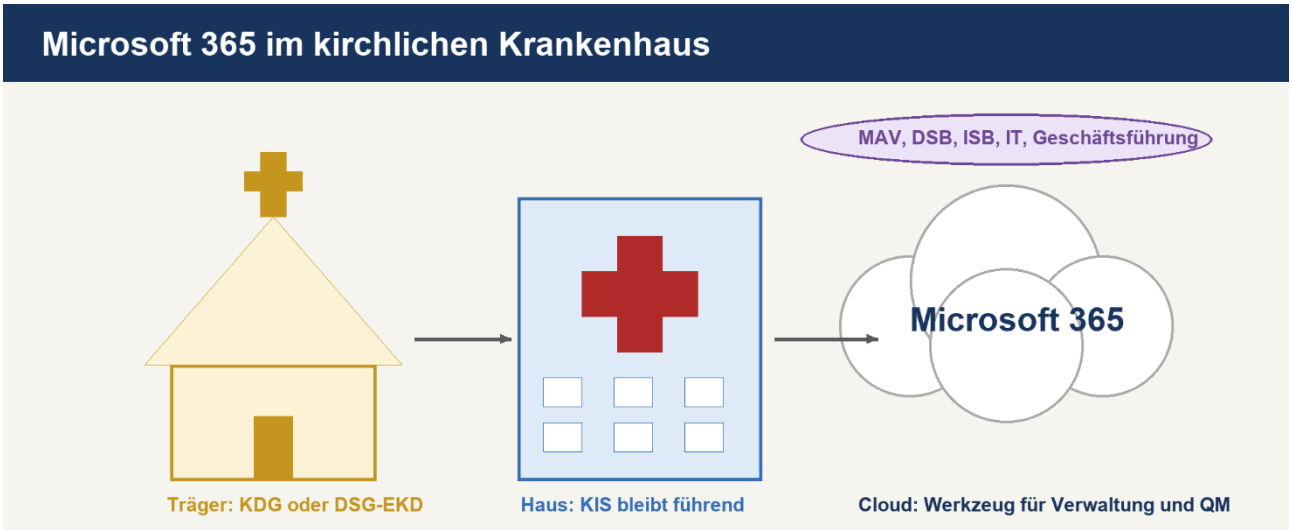
Microsoft 365 im kirchlichen Krankenhaus: KDG, DSG-EKD und die MAV am Tisch



Wissen

Der Überblick zur ganzen Serie: Recht, Technik und Organisation in der Klinik.

› **Microsoft 365 im Krankenhaus**

Beratung

Konzept, Mandantenzuschnitt und Vorlage für Geschäftsführung und MAV.

› **Microsoft-365-Beratung für Krankenhäuser**

Schulung

Admins, Key-User und Gremien fit machen – vom Stationsrechner bis zum QM.

› **Microsoft-365-Schulung für Krankenhäuser**

Es gibt diese eine Folie, die in fast jedem Projekt-Kick-off eines freigemeinnützigen Trägers auftaucht. Links das Logo von Microsoft, rechts das Kreuz, dazwischen ein Fragezeichen von der Größe einer Notaufnahme. Und irgendwer aus der Geschäftsführung sagt dann den Satz: „Wir sind doch nicht anders als die Uniklinik nebenan." Doch, sind Sie. Nicht bei der Technik, aber beim Recht, bei der Aufsicht und bei der Frage, wer am Tisch sitzt, wenn über Teams, SharePoint und Exchange Online entschieden wird.

Ein großer Teil der deutschen Krankenhäuser steht in freigemeinnütziger, sehr oft kirchlicher Trägerschaft. Für diese Häuser gilt nicht die DSGVO pur, sondern kirchliches Datenschutzrecht: das **Gesetz über den Kirchlichen Datenschutz (KDG)** im katholischen Bereich und das **EKD-Datenschutzgesetz (DSG-EKD)** im evangelischen. Statt Betriebsrat oder Personalrat verhandelt die **Mitarbeitervertretung (MAV)**. Und das Krankenhaus ist oft nur eine Gesellschaft unter vielen in einer Trägerholding, zu der auch Altenhilfe, Jugendhilfe und Verwaltung gehören. Wer Microsoft 365 hier einführt, plant also nicht für ein Haus, sondern für ein kleines Kirchenkonzern-Ökosystem mit eigener Gerichtsbarkeit.

Dieser Beitrag gehört zur Serie „Microsoft 365 im Krankenhaus", deren Überblick Sie über die Kachel „Wissen" oben erreichen, und schaut mit Krankenhausbrille auf die kirchlichen Besonderheiten: Auftragsverarbeitung nach kirchlichem Recht, Datenschutz-Folgenabschätzung, Meldewege bei Datenpannen und den Mandantenzuschnitt in der Holding. Die Grundhaltung bleibt dieselbe wie in der ganzen Serie: Patientendaten gehören ins KIS und seine Subsysteme. Microsoft 365 ist das Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit.

Weiter: Der kirchliche Blick ohne Krankenhausbrille

Wer die Grundlagen für Bistum, Landeskirche, Caritas und Diakonie insgesamt sucht – Kirchengemeinden, Kitas, Beratungsstellen, Verwaltungszentren –, findet sie im Kompetenzbereich. Dieser Artikel wiederholt das nicht, sondern ergänzt den Klinikblick.

› Microsoft 365 in Kirche, Diakonie und Caritas

Hinweis: Keine Rechtsberatung

Dieser Beitrag ordnet Rechtsnormen aus Sicht der IT-Praxis ein. Er ersetzt keine Rechtsberatung. Verbindlich sind die amtlichen Fassungen im Amtsblatt Ihrer (Erz-)Diözese oder Ihrer Landeskirche und die Auskünfte Ihres Datenschutzbeauftragten und der zuständigen kirchlichen Aufsicht.

Kirchlich heißt nicht weniger Recht, sondern anderes Recht

Die DSGVO erlaubt es Kirchen in Artikel 91, eigene umfassende Datenschutzregeln weiter anzuwenden, sofern diese mit der Verordnung in Einklang gebracht sind und eine unabhängige Aufsicht besteht. Genau das haben katholische und evangelische Kirche getan. Für Ihr Krankenhaus bedeutet das: Die Paragrafen haben andere Nummern, die Aufsicht hat eine andere Anschrift, die Grundgedanken sind weitgehend die der DSGVO. Wer „KDG“ hört und an ein Sonderrecht für Weihrauch denkt, liegt daneben. Wer glaubt, man könne es ignorieren, liegt noch weiter daneben.

Wichtig für die Klinik-IT: Das kirchliche Datenschutzrecht verdrängt nur das allgemeine staatliche Datenschutzrecht. Krankenhausspezifisches staatliches Recht gilt weiter, gleichgültig, wer der Träger ist. Dazu gehören die IT-Sicherheitspflichten nach § 391 SGB V, für Betreiber kritischer Anlagen stattdessen die Pflichten des BSIG, die Testatpflicht für Cloud-Dienste nach § 393 SGB V, die Schweigepflicht nach § 203 StGB und das Landeskrankenhausrecht. Die Landeskrankenhausgesetze unterscheiden sich von Land zu Land deutlich, gerade bei Datenschutzregeln und bei der Frage, wie sie mit kirchlichen Trägern umgehen. Prüfen Sie Ihr Bundesland einzeln und übertragen Sie keine Antwort aus dem Nachbarland.

KDG und DSG-EKD in Kurzform

Fakten: Stand der kirchlichen Datenschutzgesetze

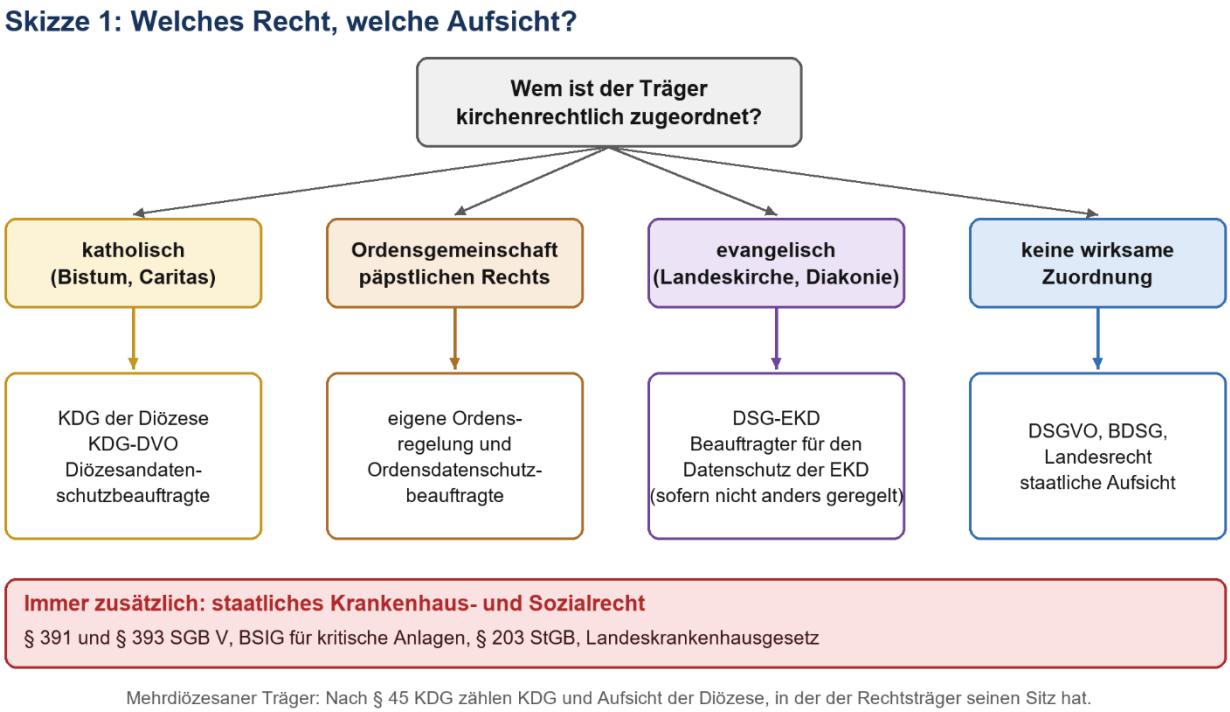
- **KDG:** Die Vollversammlung des Verbands der Diözesen Deutschlands hat die Neufassung von KDG und KDG-Durchführungsverordnung (KDG-DVO) am 24. November 2025 beschlossen. Die Diözesanbischöfe setzen sie jeweils für ihre (Erz-)Diözese in Kraft; vorgesehen war der 1. März 2026. Maßgeblich ist die Fassung im Amtsblatt Ihrer Diözese.
- **Was bleibt:** Nach der Arbeitshilfe der Konferenz der Diözesandatenschutzbeauftragten gelten die Regeln zu Auftragsverarbeitung, Datenschutz-Folgenabschätzung und Meldung von Datenschutzverletzungen unverändert fort.
- **DSG-EKD:** In Kraft seit 24. Mai 2018, von der EKD-Synode im November 2024 evaluiert. Die Änderungen gelten seit 1. Mai 2025. Gestrichen wurde dabei die viel kritisierte „Unterwerfungsklausel“ für nicht-kirchliche Auftragsverarbeiter.
- **Neu im DSG-EKD:** § 30a zu zentralen Verfahren, an denen mehrere verantwortliche Stellen beteiligt sind.
- **Neu in der KDG-DVO:** § 18 regelt die Nutzung von Cloud-Diensten mit einem Prüfkatalog

und verlangt eine Exit-Strategie; § 25 erklärt die Übermittlung personenbezogener Daten per Fax grundsätzlich für unzulässig.

Wer ist eigentlich Ihre Aufsicht?

Die Frage klingt banal und wird in Workshops erstaunlich oft mit Schulterzucken beantwortet. Katholische Einrichtungen unterliegen der Diözesandatenschutzbeauftragten oder dem Diözesandatenschutzbeauftragten ihrer Diözese; mehrere Diözesen haben dafür gemeinsame Datenschutzzentren eingerichtet. Ordensgemeinschaften päpstlichen Rechts haben eine eigene Regelung und eine eigene Ordensaufsicht – das betrifft in der Praxis gar nicht wenige Krankenhäuser mit Ordenstradition. Evangelische und diakonische Einrichtungen melden sich beim Beauftragten für den Datenschutz der EKD, sofern ihre Landeskirche nichts Abweichendes geregelt hat; dessen Meldeformular fragt deshalb ausdrücklich nach Landeskirche oder diakonischem Landesverband.

Für Klinikverbünde, deren Häuser über Diözesangrenzen verstreut liegen, ist § 45 KDG entscheidend: Bei einem über- oder mehrdiözesanen Rechtsträger gilt das KDG der Diözese, in der der Rechtsträger seinen Sitz hat, und dort sitzt auch die zuständige Aufsicht. Das gilt ebenso für rechtlich unselbstständige Einrichtungen in anderen Diözesen. Für die IT heißt das: ein Ansprechpartner für den ganzen Rechtsträger – aber nur, wenn die Häuser tatsächlich zu diesem Rechtsträger gehören und nicht eigene gGmbHs sind.



Skizze 1: Die Zuordnung des Trägers entscheidet über Gesetz und Aufsicht – das staatliche Krankenhausrecht gilt immer zusätzlich.

Katholisch, evangelisch und was das für Microsoft 365 heißt

Thema	Katholisch (KDG, KDG-DVO)	Evangelisch (DSG-EKD)	Folge für Microsoft 365
Auftragsverarbeitung	§ 29 KDG: Vertrag nach kirchlichem, staatlichem oder europäischem Recht; Schriftform, Ersatz durch	§ 30 DSG-EKD: Auftrag in Textform; bei nicht-kirchlichen Auftragsverarbeitern	Der Standard-Datenschutzanhang von Microsoft ist Ausgangspunkt;

Thema	Katholisch (KDG, KDG-DVO)	Evangelisch (DSG-EKD)	Folge für Microsoft 365
	elektronische Form oder Textform nach staatlichen Regeln	dürfen sich die Inhalte an Art. 28 DSGVO orientieren	prüfen und dokumentieren Sie, ob er die kirchlichen Pflichtinhalte abdeckt
Kontrolle des Dienstleisters	§ 9 Abs. 7 KDG-DVO: vom Schutzniveau überzeugen, etwa durch Vorlage von Nachweisen	§ 30 Abs. 3 DSG-EKD: vor Beginn und dann regelmäßig von den TOM überzeugen, Ergebnis dokumentieren	Prüfberichte und Testate aus dem Service Trust Portal ziehen, bewerten, ablegen – und das jährlich wiederholen
Cloud-Nutzung	§ 18 KDG-DVO: Risikokatalog (u. a. Speicherort, Admin-Zugänge, Portabilität) und Exit-Strategie	Keine eigene Cloud-Norm; Bewertung über TOM, Risiko und DSFA	Exit-Strategie für Exchange, SharePoint und Teams schriftlich festhalten, nicht nur „wir könnten ja exportieren“
Verzeichnis der Verarbeitungstätigkeiten	§ 31 KDG	§ 31 DSG-EKD	Ein Eintrag je Workload und Zweck, nicht ein Eintrag „Microsoft 365“
Datenschutz-Folgenabschätzung	§ 35 KDG	§ 34 DSG-EKD	Pflicht wird bei Gesundheits- und Personaldaten im Klinikumfeld regelmäßig ausgelöst
Meldung von Datenpannen	§ 33 KDG: unverzüglich; nach 72 Stunden nur mit Begründung der Verzögerung	§ 32 DSG-EKD: unverzüglich bei voraussichtlich nicht unerheblichem Risiko	Meldeprozess, Formulare und Rufbereitschaft vorab festlegen
Datenschutzbeauftragter	§ 36 KDG: betrieblicher DSB; für Gesundheitseinrichtungen nach Arbeitshilfe regelmäßig Pflicht	§§ 36 ff. DSG-EKD: örtlich Beauftragte	DSB von Anfang an in Konzept, DSFA und Mandantenentscheidung einbinden
Mitbestimmung	Mitarbeitervertretungsordnung (MAVO) des Bistums	Mitarbeitervertretungsgesetz (MVG-EKD bzw. landeskirchliches Recht)	Dienstvereinbarung statt Betriebsvereinbarung; Zuständigkeit Einzel-MAV oder Gesamt-MAV klären

Auftragsverarbeitung mit Microsoft nach kirchlichem Recht

Microsoft ist Auftragsverarbeiter, Ihr Krankenhaus ist Verantwortlicher. So weit, so DSGVO. Der kirchliche Teil beginnt bei der Frage, auf welcher Rechtsgrundlage der Vertrag steht. Erfahrungsgemäß verhandelt ein Hyperscaler seinen Standardvertrag nicht pro Krankenhaus neu, auch nicht für fromme Kunden. Microsoft legt den **Datenschutzanhang für Produkte und**

Services (DPA) vor, der auf der DSGVO beruht. Die gute Nachricht: Beide kirchlichen Gesetze haben dafür inzwischen eine Tür.

Katholisch: Vertrag nach kirchlichem, staatlichem oder europäischem Recht

§ 29 Abs. 3 KDG lässt ausdrücklich einen Vertrag „nach dem kirchlichen, dem staatlichen oder dem europäischen Recht“ zu. Ein Vertrag auf Grundlage der DSGVO ist damit nicht von vornherein ungeeignet. Ihre Aufgabe ist der Abgleich: Sind Gegenstand, Dauer, Art und Zweck, Datenarten und Kategorien betroffener Personen beschrieben? Sind Weisungsbindung, Vertraulichkeit, Unterauftragsverarbeiter, Unterstützungspflichten, Löschung und Kontrollrechte geregelt? Die Formfrage regelt § 29 Abs. 9 KDG: Schriftform, wobei für deren Ersatz durch elektronische Form oder Textform die staatlichen Regelungen maßgeblich sind. Klären Sie mit Ihrem betrieblichen Datenschutzbeauftragten, wie Ihr Haus den elektronischen Vertragsabschluss im Lizenzportal dokumentiert.

Die KDG-DVO legt nach. Sie ordnet personenbezogene Daten in drei Datenschutzklassen ein. Gesundheitsdaten und Daten über arbeitsrechtliche Rechtsverhältnisse gehören nach § 13 KDG-DVO in Klasse III – und ohne Einordnung gilt nach § 9 Abs. 5 KDG-DVO automatisch Klasse III. Das ist für ein Krankenhaus keine Überraschung, für die Personalabteilung aber oft schon: Die Dienstplanliste mit Krankmeldungen in einem Teams-Kanal ist kein Kavaliersdelikt, sondern Datenschutzklasse III. Bei Auftragsverarbeitung müssen Sie sich nach § 9 Abs. 7 KDG-DVO vom passenden Schutzniveau überzeugen, etwa durch Vorlage von Nachweisen.

Evangelisch: Textform und die gestrichene Unterwerfungsklausel

Im evangelischen Bereich war jahrelang die „Unterwerfungsklausel“ der Stolperstein: Nichtkirchliche Auftragsverarbeiter sollten sich der kirchlichen Datenschutzaufsicht unterwerfen. Kein Hyperscaler hat das je unterschrieben, und viele Diakonie-Einrichtungen haben mit Zusatzvereinbarungen und Bauchschmerzen gelebt. Mit der Evaluierung des DSG-EKD ist die Klausel gestrichen. Seit 1. Mai 2025 gilt: Der Auftrag ist in Textform zu erteilen, und wenn kirchliches Datenschutzrecht auf den Auftragsverarbeiter keine Anwendung findet, dürfen sich die Vertragsinhalte an Artikel 28 DSGVO orientieren (§ 30 Abs. 5 DSG-EKD).

Was bleibt, ist die Kontrollpflicht. Nach § 30 Abs. 3 DSG-EKD überzeugen Sie sich vor Beginn der Verarbeitung und danach regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentieren das Ergebnis. „Regelmäßig“ heißt nicht „beim nächsten Audit, wenn jemand fragt“. Und § 30 Abs. 6 DSG-EKD erinnert daran, dass auch Fernwartung mit möglichem Zugriff auf personenbezogene Daten Auftragsverarbeitung ist – ein Punkt, der in der Medizintechnik gern vergessen wird.

Tipp: Die Nachweismappe für die Auftragsverarbeitung

Legen Sie für Microsoft 365 eine Nachweismappe an, die Datenschutzbeauftragter, Informationssicherheitsbeauftragter und QMB gemeinsam pflegen:

- aktueller Datenschutzanhang und Produktbedingungen mit Abrufdatum,
- Abgleich gegen § 29 KDG bzw. § 30 DSG-EKD als Tabelle mit Fundstellen,
- Liste der Unterauftragsverarbeiter mit Abrufdatum und Ihr Verfahren für Änderungsmitteilungen,
- Prüfberichte und Testate aus dem Service Trust Portal mit Bewertungsvermerk,
- Konfigurationsnachweis für den Datenstandort und die EU-Datengrenze,
- Exit-Strategie (für katholische Träger nach § 18 Abs. 3 KDG-DVO ausdrücklich gefordert).

Das ist im Zertifizierungsaudit nach KTQ oder ISO 9001 auch dann hilfreich, wenn der Auditor nur fragt, „wie Sie Dienstleister steuern“.

§ 393 SGB V gilt auch unter dem Kreuz

Kirchliches Datenschutzrecht befreit nicht von staatlichem Sozialrecht. Wer Sozial- oder Gesundheitsdaten in Cloud-Diensten verarbeitet, braucht nach § 393 SGB V seit 1. Juli 2025 ein aktuelles C5-Typ-2-Testat des Anbieters für die eingesetzten Cloud-Systeme oder ein gleichwertiges Testat bzw. Zertifikat nach der dort vorgesehenen Verordnung, und die im Prüfbericht genannten Kundenkriterien müssen umgesetzt sein. Welche Microsoft-Dienste von welchem C5-Testat welchen Typs erfasst sind, ist ein **Prüfauftrag**: Laden Sie den aktuellen Bericht im Service Trust Portal herunter und gleichen Sie den Geltungsbereich mit den Diensten ab, die Sie tatsächlich nutzen. Die Details stehen im Beitrag § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen.

Für den Datenstandort hilft die EU-Datengrenze: Nach Microsofts eigener Dokumentation sind Microsoft-365-Mandanten mit Registrierungsland in der EU oder der EFTA im Geltungsbereich, Kunden mit Multi-Geo-Funktionen dagegen nicht. Microsoft nennt dort auch die verbleibenden Ausnahmen, in denen Daten die Grenze verlassen. Lesen Sie diese Ausnahmen, bevor jemand in der Gremiensitzung „alles bleibt in Europa“ verspricht – die Beschreibung finden Sie unter EU-Datengrenze bei Microsoft Learn. Für Drittlandübermittlungen gelten §§ 39 bis 41 KDG bzw. § 10 DSG-EKD.

Warnung: Die Cloud-Frage ist nicht nur eine Datenschutzfrage

Ob Patientenbezug in Microsoft 365 überhaupt zulässig ist, entscheidet sich nicht allein am KDG oder DSG-EKD, sondern auch an § 203 StGB und am jeweiligen Landeskrankenhausgesetz. Manche Landesgesetze sind bei der Verarbeitung von Patientendaten durch Dritte deutlich strenger als andere. Vertiefung: Schweigepflicht und Cloud: § 203 StGB, Landeskrankenhausgesetze und Auftragsverarbeitung.

Datenschutz-Folgenabschätzung: Die Excel-Liste mit Patientennamen ist kein Randfall

Eine Datenschutz-Folgenabschätzung ist nach § 35 KDG und § 34 DSG-EKD fällig, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen hat; die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten ist das klassische Beispiel. Ein Krankenhaus kann sich mit „wir machen in Microsoft 365 nur Verwaltung“ nicht so leicht herausreden, wie es gern möchte. Die Verwaltung eines Krankenhauses ist voller Gesundheitsbezug: Abrechnungsklärung, Beschwerdemanagement, Arbeitsmedizin, Betriebliches Eingliederungsmanagement, Hygienemeldungen, Haftpflichtfälle.

Und dann ist da die Realität, die jede IT-Leitung kennt: die Belegungsübersicht als Excel-Datei im Teams-Kanal der Station, die Liste „Patienten mit Isolationspflicht“ im OneDrive der Hygienefachkraft, der Screenshot aus dem KIS im Chat. Das ist kein Normalfall, und es darf auch keiner werden. Aber eine ehrliche DSFA verschweigt es nicht, sondern beschreibt es als Risiko, legt Maßnahmen fest und bietet einen besseren Weg an. Wie die Grenze zwischen KIS und Office sauber gezogen wird, steht in Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt.

Skizze 2: Was gehört wohin? Datenkategorien im kirchlichen Krankenhaus



Skizze 2: Drei Kategorien, drei Orte. Die mittlere Zeile ist die, über die in der DSFA am längsten diskutiert wird.

Was in die DSFA eines kirchlichen Krankenhauses gehört

Baustein	Inhalt im Klinikkontext	Wer liefert zu
Beschreibung der Verarbeitung	Workloads (Exchange Online, SharePoint, Teams, OneDrive), Zwecke, Nutzergruppen von der Verwaltung bis zur Station	IT-Leitung
Abgrenzung zum KIS	Welche Daten ausdrücklich nicht in Microsoft 365 gehören und wie das technisch unterstützt wird	IT, Ärztlicher Direktor, Pflegedirektion
Datenschutzklassen	Einordnung nach KDG-DVO bzw. Schutzbedarf nach DSG-EKD; Personal- und Gesundheitsdaten gesondert	Datenschutzbeauftragter
Risiken	Fehlfreigaben, Gastzugriffe, Schatten-Excel, Kontoübernahme, Protokollauswertung zur Leistungskontrolle	ISB, MAV
Maßnahmen	Vertraulichkeitsbezeichnungen, Verhinderung von Datenverlust, bedingter Zugriff, Gastrichtlinie, Aufbewahrung, Schulung	IT, ISB, QMB
Rest-Risiko und Entscheidung	Begründete Freigabe durch die Geschäftsführung, Wiedervorlage bei neuen Funktionen	Geschäftsführung

Technisch landen viele dieser Maßnahmen in Microsoft Purview (Vertraulichkeitsbezeichnungen, Verhinderung von Datenverlust, Aufbewahrung) und in Microsoft Entra ID (bedingter Zugriff, Gastkonten, Administratorrollen). Was davon in welcher Lizenz enthalten ist, ändert sich regelmäßig – prüfen Sie es vor der DSFA gegen die aktuelle Lizenzbeschreibung, nicht gegen den Foliensatz vom letzten Jahr.

Wichtig: Neue Funktionen sind neue Verarbeitungen

Eine DSFA für Microsoft 365 ist kein Dokument, das man einmal schreibt und dann im QM-Handbuch einbalsamiert. Copilot, neue Teams-Funktionen oder Auswertungen im Admin Center können die Bewertung ändern. Legen Sie fest, wer neue Funktionen sichtet und wann die DSFA wieder auf den Tisch kommt. Die Arbeitshilfe zur KDG-Novelle empfiehlt ausdrücklich, vorhandene Folgenabschätzungen auf geänderte Rechtsgrundlagen zu prüfen.

Fax, ein kirchlicher Sonderfall mit Sprengkraft

Ein Detail, das in katholischen Häusern für Gesprächsstoff sorgt: § 25 KDG-DVO erklärt die Übermittlung personenbezogener Daten per Fax grundsätzlich für unzulässig; Ausnahmen und Übergangsregeln sind über spezifische Bestimmungen möglich. In einem Krankenhaus, in dem das Fax zwischen Station, Labor, Hausarztpraxis und Kostenträger noch immer mehr Arbeit erledigt als mancher Server, ist das keine Fußnote. Auch wer den Fax-Weg technisch modernisiert, etwa mit Fax mit Microsoft Teams, sollte vorher mit dem betrieblichen Datenschutzbeauftragten klären, welche Übermittlungen davon betroffen sind und welche Alternative an ihre Stelle tritt. Ob es für Ihre Diözese eine Übergangsregel gibt, steht im Amtsblatt, nicht in diesem Artikel.

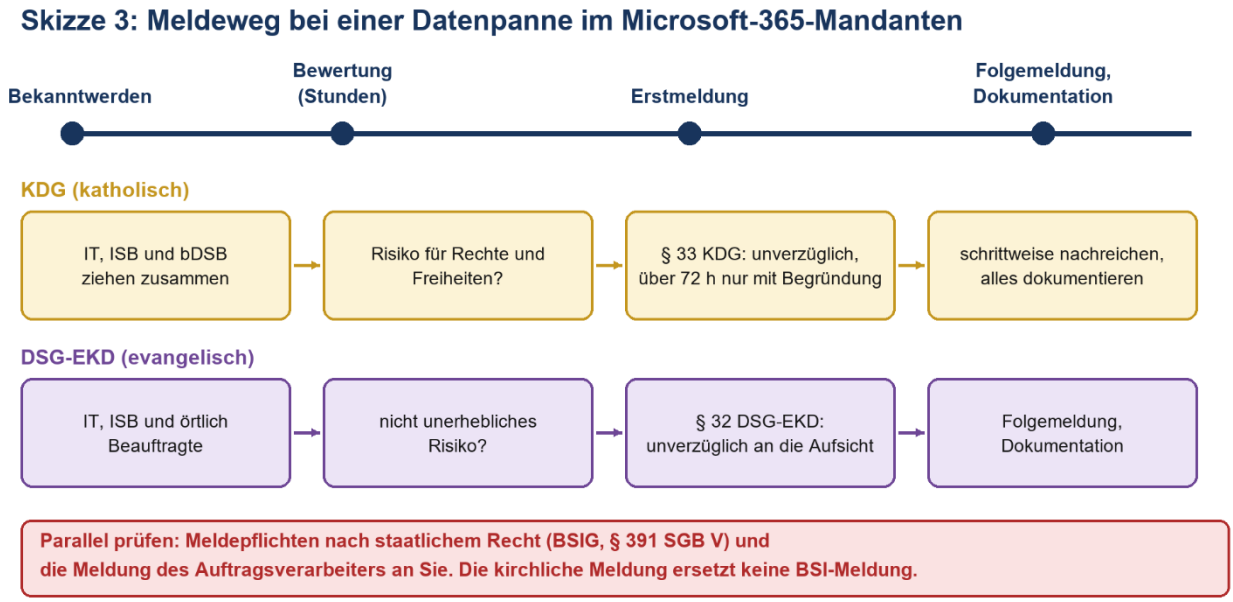
Datenpanne: Meldewege an die kirchliche Aufsicht

Freitagabend, 22:40 Uhr, Rufbereitschaft. Ein Konto aus der Personalabteilung verschickt Phishing-Mails an das halbe Haus, und im OneDrive liegen Bewerbungsunterlagen und BEM-Protokolle. Jetzt ist nicht der Moment, um herauszufinden, ob Ihr Haus nach KDG oder nach DSG-EKD meldet, wer das Formular ausfüllen darf und wo es überhaupt liegt.

Die Fristen im Vergleich

Nach § 33 KDG meldet der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich an die Datenschutzaufsicht, wenn sie ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. Erfolgt die Meldung nicht binnen 72 Stunden nach Bekanntwerden, ist eine Begründung für die Verzögerung beizufügen. Fehlende Angaben dürfen schrittweise nachgereicht werden. Das Katholische Datenschutzzentrum betreibt dafür ein Online-Formular; die Meldung gibt eine vom Verantwortlichen berechtigte Person ab.

Das DSG-EKD formuliert in § 32 anders: Die verantwortliche Stelle meldet unverzüglich, wenn die Verletzung voraussichtlich zu einem „nicht unerheblichen Risiko“ für die Rechte natürlicher Personen führt. Eine feste Stundenzahl nennt der Paragraf nicht; „unverzüglich“ heißt ohne schuldhaftes Zögern, und das ist bei einem Krankenhaus am Wochenende kein Freibrief bis Montag. Der Beauftragte für den Datenschutz der EKD bietet ebenfalls ein Online-Formular an und nimmt Folgemeldungen entgegen. Bei hohem Risiko sind zusätzlich die betroffenen Personen zu benachrichtigen (§ 34 KDG bzw. § 33 DSG-EKD).



Skizze 3: Zwei kirchliche Meldewege – und daneben die staatlichen Pflichten, die nicht wegfallen.

Frage	KDG	DSG-EKD
Schwelle	Risiko für Rechte und Freiheiten	voraussichtlich nicht unerhebliches Risiko
Frist	unverzüglich; nach 72 Stunden Begründung beifügen	unverzüglich
Adressat	zuständige Diözesan- bzw. Ordensdatenschutzaufsicht	Beauftragter für den Datenschutz der EKD bzw. landeskirchlich bestimmte Aufsicht
Auftragsverarbeiter	meldet unverzüglich an den Verantwortlichen	meldet unverzüglich an die verantwortliche Stelle
Dokumentation	alle Verletzungen, auch nicht meldepflichtige	alle Verletzungen, auch nicht meldepflichtige

Was die IT vorbereiten muss

- Ein Meldeprozess als Verfahrensanweisung im QM-Handbuch, der beide Fragen beantwortet: Datenschutzverletzung ja oder nein, Sicherheitsvorfall nach staatlichem Recht ja oder nein.
- Erreichbarkeit des Datenschutzbeauftragten oder seiner Vertretung außerhalb der Bürozeiten, mindestens über die Rufbereitschaft der IT.
- Protokolle, die eine Bewertung überhaupt erst möglich machen: Anmeldeprotokolle, Überwachungsprotokoll, Freigabeberichte. Ohne sie bleibt nur Raten – und Raten ist kein Risikobewertungsverfahren.
- Ein Weg, Meldungen von Microsoft zu erkennen: Wer das Message Center und den Dienststatus nicht liest, erfährt von einem Vorfall beim Dienstleister aus der Zeitung.
- Eine Vorlage für die Benachrichtigung von Patienten und Mitarbeiterinnen und Mitarbeitern in klarer, einfacher Sprache.

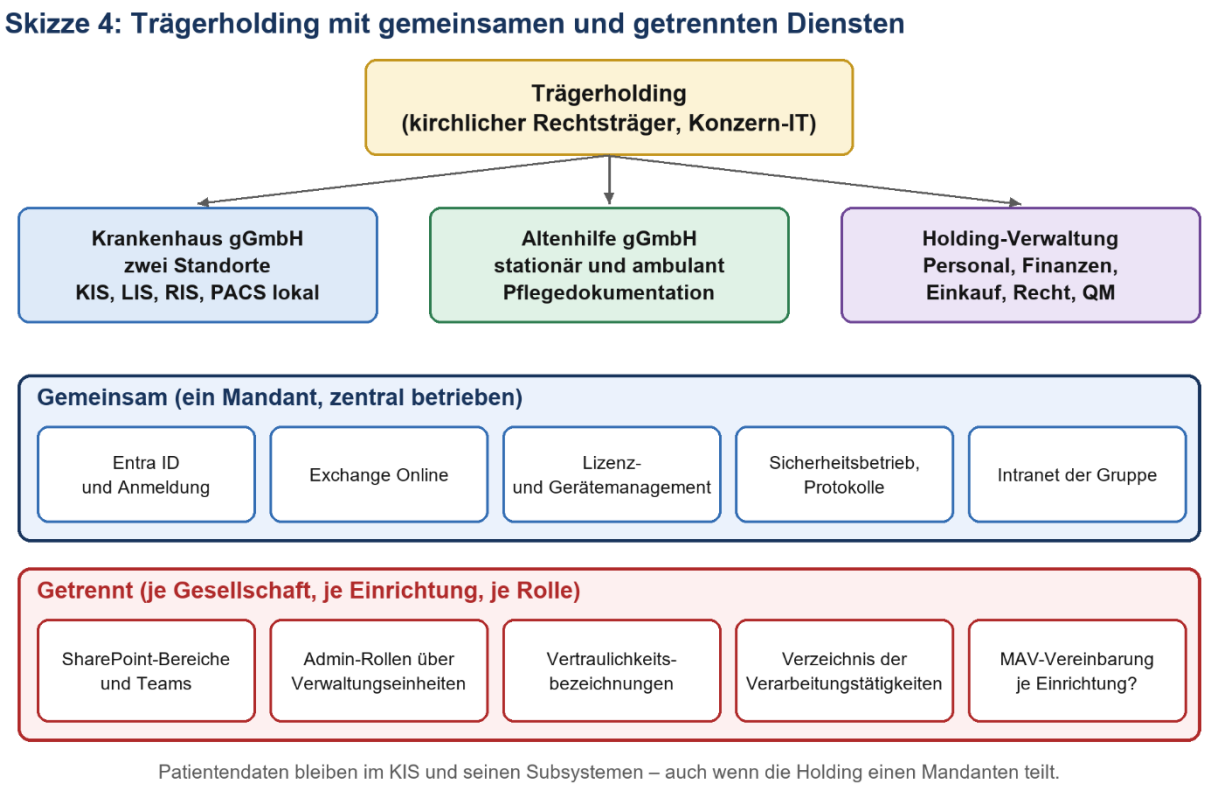
Warnung: Zwei Rechtskreise, zwei Meldungen

Die Meldung an die kirchliche Datenschutzaufsicht ersetzt keine Meldung nach staatlichem IT-Sicherheitsrecht. Ein Krankenhaus, das als Betreiber einer kritischen Anlage oder als Einrichtung nach dem BSIG gilt, hat eigene Meldepflichten gegenüber dem BSI. Welche Pflichten Ihr Haus konkret trifft, ist ein Prüfauftrag – Hintergrund im Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten.

Wie man das Ganze technisch so absichert, dass die Rufbereitschaft am Freitagabend gar nicht erst klingelt, gehört in den Bereich Microsoft 365 Security. Kurz gesagt: phishingresistente Anmeldung für privilegierte Konten, bedingter Zugriff, saubere Administratorrollen und ein Sicherheitsbetrieb, der Warnungen auch liest.

Mandantenzuschnitt in der Trägerholding und die MAV am Tisch

Die typische kirchliche Trägerstruktur ist eine Holding mit mehreren gemeinnützigen Gesellschaften: ein oder mehrere Krankenhäuser, Altenhilfe, manchmal Jugendhilfe, Bildungseinrichtungen und eine zentrale Verwaltung mit Personal, Finanzen und Einkauf. Häufig gibt es eine Konzern-IT, die alle versorgt. Damit stellt sich die Frage, die in jedem Grobkonzept bei kirchlichen Trägern früher oder später auftaucht: ein Microsoft-365-Mandant für alle oder mehrere?



Skizze 4: Gemeinsame Dienste zentral, Inhalte und Rechte getrennt – die häufigste tragfähige Variante.

Ein Mandant oder mehrere?

Variante	Stärken	Schwächen	Passt, wenn …
Ein Mandant für die ganze Holding	Ein Verzeichnis, gemeinsame Zusammenarbeit, ein Sicherheitsbetrieb, ein Lizenzpool	Trennung muss über Rollen, Verwaltungseinheiten, Bezeichnungen und Berechtigungen gebaut werden; Fehler wirken gruppenweit	die Konzern-IT zentral administriert und die Gesellschaften eng zusammenarbeiten
Ein Mandant je Gesellschaft	Klare Grenze für Daten, Rollen und Verantwortlichkeit; einfache Zuordnung zum Verantwortlichen	Mehrfacher Betrieb, Gastkonten zwischen Schwestergesellschaften, getrennte Kalender und Adressbücher	Gesellschaften rechtlich und organisatorisch weit auseinander liegen oder verkauft werden könnten
Mischform: Krankenhaus eigener Mandant, Rest gemeinsam	Krankenhaus mit seinen Sicherheitspflichten sauber abgegrenzt	Zwei Betriebsmodelle, Doppelaufwand bei Identitäten	das Krankenhaus deutlich höhere Sicherheitsanforderungen hat oder einen eigenen Betreiberstatus nach BSIG

Datenschutzrechtlich ist entscheidend, wer Verantwortlicher ist. Jede gGmbH ist in der Regel eine eigene verantwortliche Stelle mit eigenem Verzeichnis der Verarbeitungstätigkeiten, auch wenn alle im selben Mandanten sitzen. Betreibt die Holding-IT den Mandanten für die Gesellschaften, liegt zwischen Holding und Gesellschaft meist selbst eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit vor – das muss geregelt werden, bevor der erste Benutzer angelegt

ist, nicht danach. Im evangelischen Bereich eröffnet § 30a DSG-EKD die Möglichkeit, dass kirchliches Recht für zentrale Verfahren die Aufgaben zwischen den beteiligten Stellen abweichend verteilt. Ob es für Ihre Landeskirche oder Ihren diakonischen Verbund eine solche Regelung gibt, ist zu prüfen; als Generalschlüssel für jede Holding taugt die Norm nicht.

Die eigentliche Komplexität entsteht aber, wenn Konfessionen gemischt sind: ein katholisches Krankenhaus und eine evangelische Altenhilfe im selben Verbund, ökumenische Trägerschaften, kommunale Beteiligungen. Dann gelten innerhalb eines Mandanten unterschiedliche Gesetze und unterschiedliche Aufsichten. Technisch ändert das wenig, organisatorisch viel: getrennte Verzeichnisse, getrennte Meldewege, möglicherweise getrennte Dienstvereinbarungen. Wie Verbünde mit mehreren Häusern ihren Mandanten schneiden, behandelt die Serie an anderer Stelle ausführlich; die kirchliche Schicht kommt als zusätzliche Dimension obendrauf. Gewachsene Strukturen kennen wir aus der langjährigen Begleitung eines Krankenhausverbunds mit mehreren Standorten: Vertrauensstellungen zwischen Domänen, Exchange Hybrid, eine PKI, die erst gehärtet werden musste. Der Mandant erbt diese Geschichte, ob man will oder nicht.

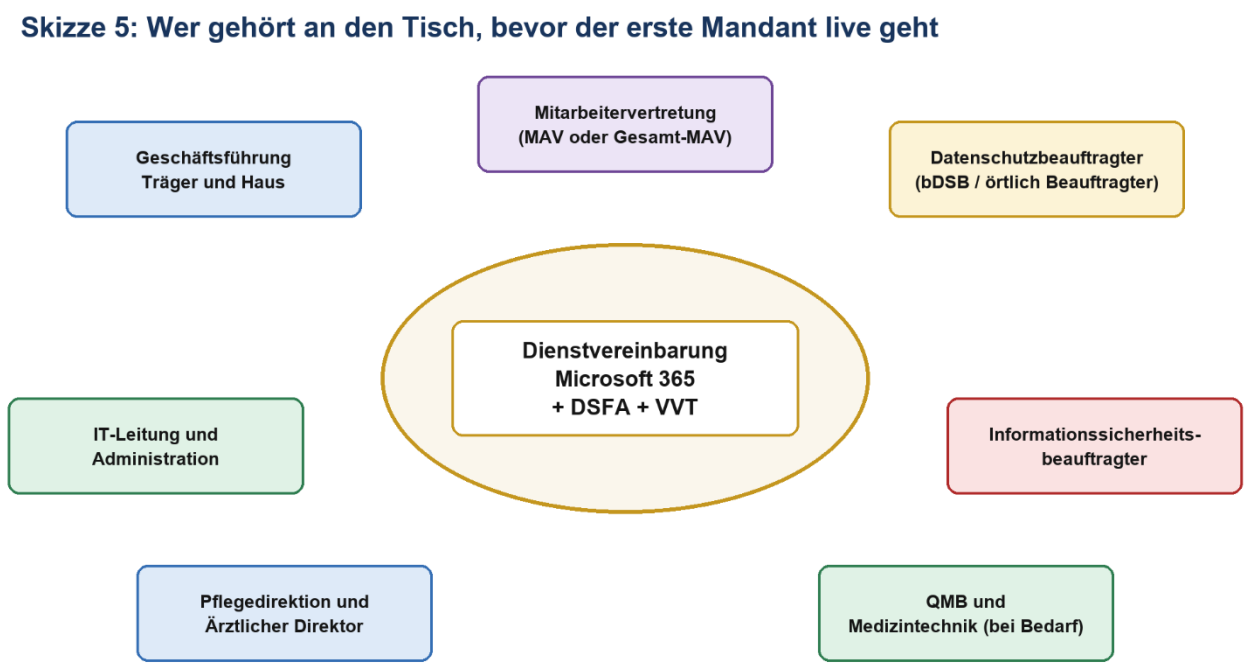
Tipp: Trennung technisch abbilden

- **Verwaltungseinheiten in Entra ID** für Administratorrollen je Gesellschaft oder Standort, damit die Altenhilfe-IT nicht die Konten der Intensivstation zurücksetzt.
- **Vertraulichkeitsbezeichnungen** mit Gesellschaftsbezug für Personal, MAV und Geschäftsführung.
- **SharePoint-Bereiche und Teams je Gesellschaft** mit eindeutigem Besitzer; Gruppen-Intranet nur für wirklich gemeinsame Inhalte.
- **Informationsbarrieren** nur, wenn es einen echten Grund gibt – sie lösen kein Berechtigungschaos, sie verstecken es.

Die MAV: Mitbestimmung nach MAVO und MVG

Das Betriebsverfassungsgesetz gilt für Religionsgemeinschaften und ihre karitativen und erzieherischen Einrichtungen nicht. An seine Stelle treten die Mitarbeitervertretungsordnung im katholischen und das Mitarbeitervertretungsgesetz im evangelischen Bereich. Beide kennen einen Mitbestimmungstatbestand für technische Einrichtungen, mit denen Verhalten oder Leistung der Mitarbeiterinnen und Mitarbeiter überwacht werden können. Microsoft 365 erfüllt diesen Tatbestand praktisch immer, weil Anmelde-, Nutzungs- und Überwachungsprotokolle anfallen, ob man sie auswertet oder nicht. Streitigkeiten landen nicht beim staatlichen Arbeitsgericht, sondern bei kirchlichen Gerichten. Die Unterschiede zwischen Betriebsrat, Personalrat und MAV, inklusive der Fundstellen, stehen im Beitrag Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

In einer Holding kommt die Zuständigkeitsfrage hinzu. Viele Träger haben neben den örtlichen Mitarbeitervertretungen eine Gesamtmitarbeitervertretung gebildet. Ob eine Dienstvereinbarung zu Microsoft 365 mit der Gesamt-MAV oder mit jeder einzelnen MAV zu schließen ist, hängt von der jeweiligen Ordnung und den Vereinbarungen im Verbund ab. Klären Sie das am Anfang – eine Vereinbarung mit dem falschen Gremium ist nur ein sehr gründlich formatiertes Gesprächsprotokoll.



Skizze 5: Der Tisch, an dem Microsoft 365 im kirchlichen Krankenhaus entschieden wird.

Regelungspunkt der Dienstvereinbarung	Warum es im Krankenhaus zählt
Zweckbindung der Protokolle	Anmeldeprotokolle dienen der Sicherheit, nicht der Kontrolle, wer im Nachtdienst wie lange am Stationsrechner war
Auswertungen und Berichte	Nutzungsberichte im Admin Center anonymisieren oder abschalten; Ausnahmen für Sicherheitsvorfälle mit Verfahren regeln
Status und Anwesenheit in Teams	Kein Rückschluss auf Leistung im Schichtdienst; klare Aussage zur Nutzung des Status
Copilot und neue Funktionen	Beteiligung der MAV vor der Freischaltung, nicht nach der ersten Beschwerde
Schulung	Wer Werkzeuge nutzen muss, wird geschult, auch Pflegekräfte im Schichtdienst – in der Arbeitszeit
Rollen der Administration	Wer darf Postfächer und Protokolle einsehen, unter welchem Vier-Augen-Prinzip

Tipp: Die MAV früh und ernsthaft einbinden

In den Workshops und Grobkonzepten bei kirchlichen Trägern hat sich bewährt, die MAV schon in die Konzeptphase zu holen – mit eigenem Termin, echter Demo und den Protokollansichten im Admin Center. Misstrauen entsteht selten an dem, was man zeigt, sondern an dem, was man weglässt. Unterstützung bei Konzept und Vorlage bietet die Microsoft-365-Beratung für Krankenhäuser; für Administratoren und Key-User die Microsoft-365-Schulung für Krankenhäuser.

Und wo bleibt das QM?

Im kirchlichen Krankenhaus ist das Qualitätsmanagement häufig der Bereich, der Microsoft 365 am schnellsten sinnvoll nutzt: QM-Handbuch, Verfahrensanweisungen, Standards, Hygieneplan, Protokolle der Ethikkomitees und Kommissionen. Diese Inhalte haben in der Regel keinen Patientenbezug und sind damit der risikoärmste Einstieg. Erfahrungen aus einem QM-Handbuch mit SharePoint für ein Krankenhaus zeigen: Wenn Lenkung, Freigabe und Auffindbarkeit stimmen, wird das Intranet auch ohne Patientendaten zum wichtigsten Werkzeug auf Station. Das kirchliche Profil – Leitbild, Seelsorge, Ethikberatung – passt dort übrigens bestens hin. Warum die Klinik insgesamt anders tickt als Verwaltung und Mittelstand, beschreibt Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand.

FAQ: Microsoft 365 im kirchlichen Krankenhaus

Dürfen kirchliche Krankenhäuser Microsoft 365 überhaupt nutzen?

Weder das KDG noch das DSG-EKD verbieten Cloud-Dienste. Sie verlangen eine tragfähige Auftragsverarbeitung, angemessene technische und organisatorische Maßnahmen, bei hohem Risiko eine Datenschutz-Folgenabschätzung und, im katholischen Bereich, die Prüfung nach § 18 KDG-DVO einschließlich Exit-Strategie. Zusätzlich gelten § 393 SGB V, § 203 StGB und das Landeskrankenhausrecht.

Reicht der Standard-Datenschutzanhang von Microsoft für das kirchliche Recht?

Das KDG lässt Verträge nach staatlichem oder europäischem Recht ausdrücklich zu, das DSG-EKD erlaubt bei nicht-kirchlichen Auftragsverarbeitern eine Orientierung an Artikel 28 DSGVO. Ob der konkrete Anhang alle Pflichtinhalte abdeckt, müssen Sie mit Ihrem Datenschutzbeauftragten prüfen und dokumentieren. Eine pauschale Freigabe ersetzt diese Prüfung nicht.

Muss sich Microsoft noch der kirchlichen Datenschutzaufsicht unterwerfen?

Im evangelischen Bereich nicht mehr: Die sogenannte Unterwerfungsklausel wurde bei der Evaluierung des DSG-EKD gestrichen, die Änderungen gelten seit 1. Mai 2025. Die Aufsicht über Ihre Einrichtung als Verantwortliche bleibt selbstverständlich bei der kirchlichen Aufsicht.

Welche Frist gilt bei einer Datenpanne?

Nach § 33 KDG unverzüglich; wer später als 72 Stunden nach Bekanntwerden meldet, muss die Verzögerung begründen. Nach § 32 DSG-EKD unverzüglich, ohne feste Stundenzahl. Staatliche Meldepflichten nach IT-Sicherheitsrecht können parallel bestehen.

Wer ist bei einem Klinikverbund über mehrere Diözesen zuständig?

Für einen über- oder mehrdiözesanen katholischen Rechtsträger gilt nach § 45 KDG das KDG der Diözese, in der der Rechtsträger seinen Sitz hat, und die dortige Aufsicht. Sind die Häuser eigene Gesellschaften, kann jede ihren eigenen Sitz und damit ihre eigene Zuständigkeit haben.

Braucht ein kirchliches Krankenhaus einen eigenen Datenschutzbeauftragten?

Im katholischen Bereich ist nach der Arbeitshilfe zur KDG-Novelle für Gesundheitseinrichtungen weiterhin regelmäßig ein betrieblicher Datenschutzbeauftragter zu benennen, unabhängig von der neuen Schwelle von 20 Personen. Im evangelischen Bereich regeln die §§ 36 ff. DSG-EKD die örtlich Beauftragten. Für die Microsoft-365-Einführung gehört diese Person von Beginn an ins Projekt.

Ist eine Dienstvereinbarung mit der MAV Pflicht?

Mitbestimmungspflichtig ist die Einführung technischer Einrichtungen, die Verhalten oder Leistung überwachen können – das trifft auf Microsoft 365 praktisch immer zu. Ob die Mitbestimmung über eine Dienstvereinbarung oder anders ausgeübt wird, richtet sich nach MAVO bzw. MVG und Ihrer Praxis. Ohne Beteiligung der MAV sollte kein Mandant produktiv gehen.

Dürfen Patientendaten in Teams?

Die Grundregel dieser Serie lautet: Patientendaten gehören ins KIS und seine Subsysteme. Wo es dennoch Patientenbezug in Microsoft 365 gibt, braucht es eine begründete Ausnahme mit DSFA, Prüfung nach § 393 SGB V, Landeskrankenhausrecht und § 203 StGB – und keinen Kanal namens „Station 4 Liste“.

Fazit: Andere Paragrafen, gleiche Sorgfalt, mehr Stühle am Tisch

Ein kirchliches Krankenhaus braucht für Microsoft 365 keine andere Technik als ein kommunales oder privates Haus. Es braucht aber den richtigen Rechtsrahmen im Kopf: KDG und KDG-DVO oder DSG-EKD statt DSGVO und BDSG, die kirchliche Aufsicht als Adressat der Datenpannenmeldung, die MAV als Verhandlungspartner und eine Trägerholding, deren Mandantenzuschnitt zur rechtlichen Struktur passt. Darüber liegt unverändert das staatliche Krankenhausrecht mit § 391 und § 393 SGB V, Landeskrankenhausgesetz und Schweigepflicht.

Die gute Nachricht: Beide Kirchen haben ihr Datenschutzrecht in den letzten Jahren modernisiert. Die Unterwerfungsklausel ist im evangelischen Bereich Geschichte, das KDG akzeptiert Verträge nach europäischem Recht, und die KDG-DVO sagt erstmals ausdrücklich, was bei Cloud-Diensten zu prüfen ist. Die schlechte Nachricht: Das macht die Arbeit nicht kleiner, nur klarer. Wer Auftragsverarbeitung, DSFA, Meldeweg und Dienstvereinbarung vor dem ersten produktiven Postfach erledigt, hat später weniger zu beichten.

Weiter: Passende Beiträge und Kompetenzbereiche

› Microsoft 365 in Kirche, Diakonie und Caritas
› Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft
› § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen
› Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt
› Microsoft-365-Beratung für Krankenhäuser