Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview

Es gibt einen Satz, den du in Diakonie und Caritas früher oder später hörst, und er klingt immer harmlos: „Ich hab das nur kurz in Excel gemacht, weil das Fachverfahren das nicht kann.“ Der Satz ist der Anfang einer Geschichte, die mit einer Belegungsliste beginnt, in der neben dem Namen die Diagnose steht, und die damit endet, dass diese Liste in einem Teams-Kanal mit vierzig Mitgliedern liegt, von denen zwölf im Fahrdienst arbeiten und drei seit einem halben Jahr nicht mehr im Haus sind.

Niemand hat dabei etwas Böses gewollt. Das ist das Unangenehme daran. Klientendaten wandern nicht aus Bosheit in Microsoft 365, sondern aus Hilfsbereitschaft, aus Zeitdruck und aus der sehr menschlichen Neigung, Werkzeuge zu benutzen, die funktionieren, statt solcher, die vorgesehen sind. Deine Aufgabe als IT-Leitung, Verwaltungsleitung, Geschäftsführung oder örtlich beauftragte Person für den Datenschutz besteht deshalb nicht darin, Menschen zu erziehen. Sie besteht darin, die Wege so zu bauen, dass der bequeme Weg auch der richtige ist — und dort, wo das nicht gelingt, wenigstens zu wissen, was passiert.

Dieser Beitrag sortiert drei Dinge: Erstens die Rechtslage, die bei Klientendaten anders ist als bei Personaldaten und deutlich anders als bei einem Gemeindebrief. Zweitens die Orte in Microsoft 365, an denen Klientendaten regelmäßig auftauchen, obwohl sie ins Fachverfahren gehören. Und drittens die Werkzeuge aus Microsoft Purview — mit einer ehrlichen Einschätzung, welche davon ein Träger mit rund 300 Beschäftigten tatsächlich betreiben kann und welche in der Praxis ein Papiertiger bleiben.

Die Einordnung, warum kirchliche und diakonische Träger technisch fast wie alle anderen arbeiten, rechtlich aber in einer eigenen Ordnung stehen, findest du im Überblick zu Microsoft 365 in Kirche, Diakonie und Caritas. Hier geht es um den Ausschnitt, der die meisten Nerven kostet: die Daten von Menschen, die zu dir kommen, weil sie Hilfe brauchen.

Drei Rechtskreise auf einem Schreibtisch

Die Verwirrung fängt damit an, dass bei Klientendaten in Diakonie und Caritas nicht ein Regelwerk gilt, sondern mindestens drei — und sie sind nicht deckungsgleich. Wer nur eines davon kennt, baut ein Konzept, das an der zweiten Frage der Aufsicht zerbricht.

Erster Kreis: kirchliches Datenschutzrecht

Auf evangelischer Seite gilt das EKD-Datenschutzgesetz, auf katholischer Seite das Kirchliche Datenschutzgesetz. Beide sind keine abgeschwächten Fassungen der Datenschutz-Grundverordnung, sondern eigenständige Gesetze mit eigener Aufsicht: dem Beauftragten für den Datenschutz der EKD einerseits, den Diözesandatenschutzbeauftragten beziehungsweise dem Katholischen Datenschutzzentrum andererseits. Wer Microsoft 365 in einem diakonischen Werk oder einem Caritasverband betreibt, hat es mit diesen Stellen zu tun, nicht mit der Landesdatenschutzbehörde.

Für Klientendaten ist die entscheidende Norm in beiden Gesetzen die zu den besonderen Kategorien personenbezogener Daten: § 13 DSG-EKD und § 11 KDG. Gesundheitsdaten, Daten über das Sexualleben, über religiöse Überzeugungen, über ethnische Herkunft — all das ist grundsätzlich verboten zu verarbeiten, mit eng umrissenen Ausnahmen. Eine dieser Ausnahmen ist die Versorgung und Behandlung im Gesundheits- oder Sozialbereich. Und beide Gesetze knüpfen diese Ausnahme an dieselbe Bedingung: Die Daten müssen von Fachpersonal oder unter dessen Verantwortung verarbeitet werden, und dieses Fachpersonal muss nach kirchlichem oder staatlichem Recht dem Berufsgeheimnis unterliegen. Wie das im jeweiligen Gesetz aufgebaut ist, führen die Beiträge zu DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet und KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche im Einzelnen aus.

Merk dir aus dieser Bedingung einen Satz, er trägt das halbe Konzept: Der Kreis der Personen, die an die Daten kommen, ist Teil der Rechtsgrundlage. Nicht ein Nebenaspekt, nicht eine technische Umsetzungsfrage — ein Tatbestandsmerkmal. Ein offener Teams-Kanal mit Diagnosen ist damit nicht bloß schlecht organisiert. Ihm fehlt die Erlaubnis.

Zweiter Kreis: Sozialdatenschutz

Das Sozialgeheimnis aus § 35 SGB I bindet zunächst die Leistungsträger — also Jugendamt, Sozialamt, Krankenkasse, Rentenversicherung. Ein freier Träger der Wohlfahrtspflege ist das nicht. Daraus wird gelegentlich der Schluss gezogen, der Sozialdatenschutz gehe die Diakonie und die Caritas nichts an. Dieser Schluss ist bequem und falsch.

Er ist falsch, weil § 78 SGB X den Spieß umdreht: Wer Sozialdaten von einem Leistungsträger übermittelt bekommt, darf sie nur für genau den Zweck verarbeiten, zu dem sie übermittelt wurden, und hat sie im selben Umfang geheim zu halten wie die übermittelnde Stelle. Sobald also das Jugendamt einem freien Träger den Hilfeplan schickt, sobald die Kommune einer Beratungsstelle einen Fall zuweist, sobald eine Pflegekasse Daten überträgt — ab diesem Moment hängt die Zweckbindung an den Daten wie ein Etikett, das sich nicht abziehen lässt. Und in der Kinder- und Jugendhilfe kommt hinzu, dass der besondere Vertrauensschutz für anvertraute Sozialdaten nach § 65 SGB VIII die Weitergabe auf wenige, ausdrücklich benannte Fälle beschränkt — im Kern auf die Einwilligung dessen, der die Daten anvertraut hat, und auf Konstellationen rund um die Gefährdung des Kindeswohls.

Für die IT bedeutet das etwas sehr Konkretes. Eine Datei, die aus einem übermittelten Hilfeplan entstanden ist, darf nicht deshalb in der allgemeinen Teamablage landen, weil dort gerade Platz ist. Die Zweckbindung ist mitgewandert.

Dritter Kreis: Berufsgeheimnis und § 203 StGB

Der dritte Kreis ist der, den Technikerinnen und Techniker am häufigsten übersehen, weil er nicht im Datenschutzrecht steht, sondern im Strafgesetzbuch. § 203 StGB stellt die Verletzung von Privatgeheimnissen unter Strafe, und die Liste der erfassten Berufe liest sich wie das Organigramm eines mittleren diakonischen Werks: Ärztinnen und Ärzte, Angehörige anderer Heilberufe, Berufspsychologen, staatlich anerkannte Sozialarbeiter und Sozialpädagogen sowie — nach Absatz 1 Nummer 4 — Ehe-, Familien-, Erziehungs- und Jugendberater ebenso wie Berater für Suchtfragen, sofern die Beratungsstelle von einer Behörde oder einer Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist.

Bemerkenswert ist, wer in dieser Aufzählung nicht ausdrücklich steht: die Schuldner- und Insolvenzberatung. Ihr Schutz läuft über den Sozialdatenschutz, über das kirchliche Datenschutzrecht und über vertragliche Verschwiegenheitsverpflichtungen, nicht über die Strafnorm. Das ist keine akademische Feinheit, sondern ein Unterschied im Risikoprofil, den du in der Schutzbedarfsfeststellung sauber abbilden solltest — statt alles pauschal auf die höchste Stufe zu heben und damit unglaubwürdig zu werden.

Fakten: Die Klausel, die deinen IT-Dienstleister betrifft

§ 203 StGB kennt seit der Neuregelung die Figur der „mitwirkenden Personen“. Nach Absatz 3 liegt kein Offenbaren vor, wenn ein Berufsgeheimnisträger Geheimnisse gegenüber solchen mitwirkenden Personen zugänglich macht, soweit das für die Inanspruchnahme ihrer Tätigkeit erforderlich ist.

Absatz 4 zieht die Rechnung: Mitwirkende Personen machen sich selbst strafbar, wenn sie ein ihnen bei der Tätigkeit bekannt gewordenes Geheimnis unbefugt offenbaren. Und strafbar macht sich auch, wer es unterlässt, die mitwirkenden Personen zur Verschwiegenheit zu verpflichten.

Übersetzt in den Alltag: Dein Systemhaus, dein Rechenzentrum und jeder externe Administrator mit Zugriff auf Postfächer oder SharePoint sind mitwirkende Personen. Die Verpflichtung gehört in den Vertrag, nicht in eine Mail. Wer das versäumt, riskiert keine Beanstandung, sondern eine Strafnorm.

Was daraus für die Abgrenzung zur Kommune folgt

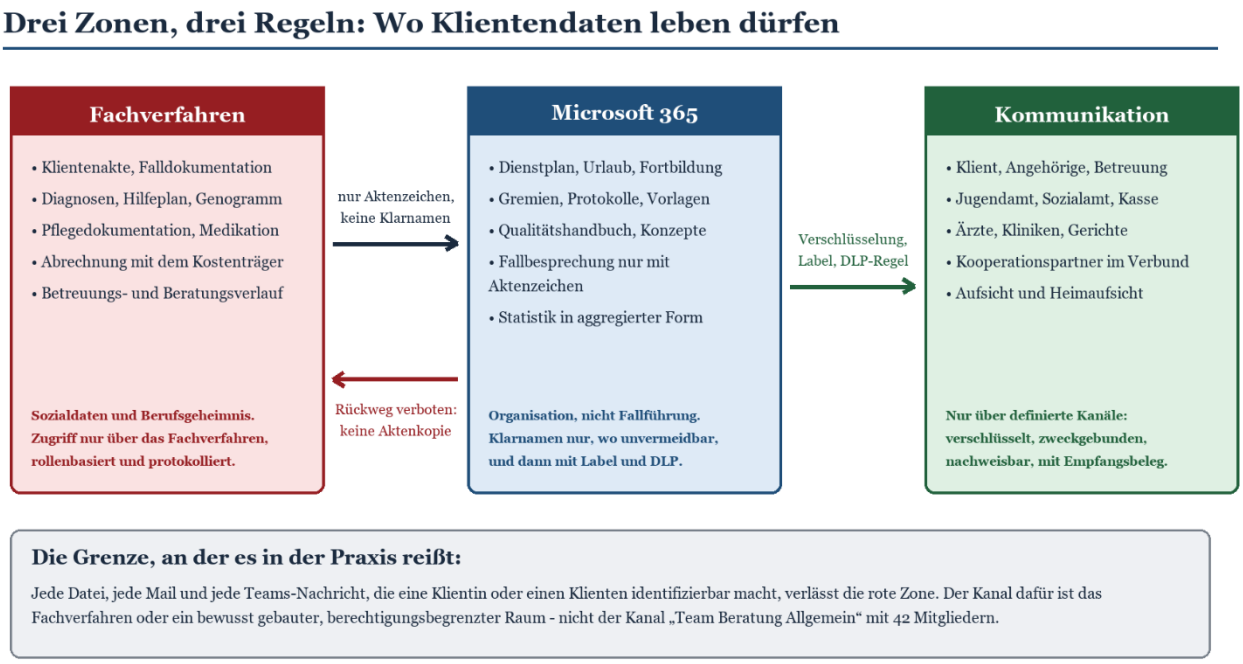
Die Kommune arbeitet unter Datenschutz-Grundverordnung und Landesdatenschutzgesetz, hat einen Personalrat und eine staatliche Aufsicht. Der kirchliche Träger arbeitet unter DSG-EKD oder KDG, hat eine Mitarbeitervertretung nach MVG-EKD oder MAVO und eine kirchliche Aufsicht. Diese Unterschiede sind real und haben Konsequenzen für Verträge, Meldewege und Beteiligung. Alles andere — Exchange, Teams, SharePoint, Conditional Access — ist ganz normales Microsoft 365, und es hilft niemandem, daraus eine Sonderwelt zu konstruieren. Die Sonderwelt liegt im Rechtsrahmen und im Schutzbedarf, nicht in der Technik.

Kriterium	Kommunale Einrichtung	Kirchlicher oder diakonischer Träger
Datenschutzrecht	DSGVO, Landesdatenschutzgesetz	DSG-EKD oder KDG als eigenständige Gesetze
Aufsicht	Landesbeauftragte für den Datenschutz	BfD EKD beziehungsweise Diözesandatenschutzbeauftragte oder Katholisches Datenschutzzentrum
Beteiligung der Beschäftigten	Personalrat nach Personalvertretungsgesetz	Mitarbeitervertretung nach MVG-EKD oder MAVO, Dienstvereinbarung
Arbeitsrechtlicher Rahmen	TVöD, Tarifverhandlungen	Dritter Weg, AVR, Dienstgemeinschaft
Entscheidungsgremium vor Ort	Rat, Ausschuss, Verwaltungsvorstand	Presbyterium, Kirchenvorstand, Pfarrgemeinderat, Verbandsvertretung, Aufsichtsrat des Trägers
Klientendaten	Sozialdaten beim Leistungsträger, § 35 SGB I unmittelbar	meist als Dritter nach § 78 SGB X gebunden, zusätzlich Berufsgeheimnis und kirchliches Recht
Microsoft-365-Technik	identisch	identisch

Wo der Unterschied wirklich liegt — und wo er nur behauptet wird.

Wo Klientendaten in Microsoft 365 auftauchen, obwohl sie ins Fachverfahren gehören

Die Grundordnung ist schnell erzählt und wird trotzdem selten eingehalten: Fallbezogene Daten gehören ins Fachverfahren. Dort sind sie rollenbasiert geschützt, protokolliert, mit Aufbewahrungslogik versehen und im Zweifel auch revisionsfest. Microsoft 365 ist die Umgebung für alles, was Organisation ist — Dienstplanung, Gremien, Konzepte, Qualitätsmanagement, Fortbildung, interne Kommunikation. Die Kommunikation nach außen ist eine dritte Zone mit eigenen Anforderungen an Verschlüsselung und Nachweis.



Skizze 1: Die drei Zonen und die Regeln an ihren Grenzen. Der Rückweg aus Microsoft 365 ins Fachverfahren ist erlaubt — der Rückweg der Daten in die Teamablage nicht.

Die sieben üblichen Fundorte

Wenn du in einem Träger mit 300 Beschäftigten eine ehrliche Bestandsaufnahme machst, findest du Klientendaten fast immer an denselben Stellen. Die Reihenfolge variiert, das Muster nicht.

- Das Postfach. Anhänge von Kostenträgern, Arztberichte als PDF, Weiterleitungen aus dem Fachverfahren an die eigene Adresse „zum Weiterarbeiten zu Hause“. Postfächer sind das größte inoffizielle Archiv jedes Trägers.
- Der Teams-Chat. Die schnelle Rückfrage zwischen Schichten: „Ist bei Frau M. die Verordnung durch?“ — mit vollem Namen, weil Tippen im Dienst schnell gehen muss. Chatverläufe sind dauerhaft, durchsuchbar und in Compliance-Verfahren greifbar.
- Der Kanal. Belegungslisten, Übergabeprotokolle, Fallübersichten als Excel-Datei in „Allgemein“, weil dort alle draufkommen. Genau das ist ja der Punkt.
- OneDrive. Die persönliche Kopie, die jemand erstellt hat, weil sie den Bericht in Ruhe fertig schreiben wollte. Sie liegt dort noch, wenn die Person längst in einem anderen Werk arbeitet.
- Der Kalender. Betreffzeilen wie „Hausbesuch Familie K., Verdacht Kindeswohlgefährdung“ in einem Kalender, der aus Vertretungsgründen für das halbe Team freigegeben ist.

- OneNote. Das Notizbuch der Fallbesprechung, angelegt in einem Team, gewachsen über zwei Jahre, von niemandem je aufgeräumt — inklusive der Notizen, die jemand nie schriftlich hätte festhalten sollen.
- Die Scanner-Ablage. Ein Multifunktionsgerät scannt in ein Sammelpostfach oder eine SharePoint-Bibliothek, auf die aus historischen Gründen die halbe Verwaltung Zugriff hat.

Warnung: Die Excel-Belegungsliste mit Diagnosen im Teams-Kanal

Der Klassiker, und er kommt in fast jeder Bestandsaufnahme vor. Eine Einrichtungsleitung pflegt eine Belegungsübersicht: Zimmernummer, Name, Aufnahmedatum, Pflegegrad — und in Spalte H, weil es praktisch ist, die Hauptdiagnose. Die Datei liegt im Kanal „Allgemein“ des Teams der Einrichtung, damit sie jeder in der Schicht öffnen kann.

Was daran rechtlich passiert: Gesundheitsdaten werden einem Personenkreis zugänglich gemacht, der über das Fachpersonal hinausgeht, das die Ausnahme in § 13 DSG-EKD beziehungsweise § 11 KDG überhaupt erst trägt. Wer im Team Küche, Haustechnik oder Fahrdienst Mitglied ist, hat Zugriff auf Diagnosen. Damit fehlt der Verarbeitung die Erlaubnis — nicht die Dokumentation, die Erlaubnis.

Was technisch dazukommt: Wer ein Team betritt, sieht rückwirkend den gesamten Inhalt des Standardkanals. Eine neue Aushilfe hat am ersten Tag Zugriff auf zwei Jahre Belegungsgeschichte. Und Suchfunktion, Copilot-Indizierung und Exportwerkzeuge machen keinen Unterschied zwischen „Ablage“ und „versehentlich abgelegt“.

Der Reflex, die Datei stillschweigend zu löschen, ist übrigens der falsche. Erst dokumentieren, Betroffenheit und Zugriffsverlauf bewerten, Meldepflicht prüfen, dann bereinigen. Eine gelöschte Datei ohne Protokoll ist bei der Aufsicht kein gelöstes Problem, sondern ein ungeklärtes.

Warum das passiert — und warum Schulung allein es nicht löst

Es wäre bequem, hier von mangelndem Bewusstsein zu sprechen. Die Wahrheit ist unbequemer: In den allermeisten Fällen weiß das Team ziemlich genau, dass die Liste dort nicht hingehört. Sie liegt dort trotzdem, weil das Fachverfahren keine brauchbare Übersicht ausgibt, weil es in der Nachtschicht auf dem Diensthandy nicht läuft, weil die Lizenz für den Modul-Zusatz nie gekauft wurde oder weil der Export nach Excel die einzige Möglichkeit ist, eine Frage der Geschäftsführung innerhalb eines Tages zu beantworten.

Daraus folgt eine unangenehme, aber sehr entlastende Einsicht: Ein Teil deines Klientendatenproblems in Microsoft 365 ist gar kein Microsoft-365-Problem. Es ist ein Fachverfahrensproblem, das sich in Microsoft 365 sichtbar macht. Purview kann das sichtbar halten und begrenzen. Lösen kann es nur, wer über Fachverfahren, Prozesse und Budgets entscheidet. Deshalb gehört das Ergebnis deiner Bestandsaufnahme nicht nur zur Datenschutzbeauftragten, sondern auf den Tisch der Geschäftsführung.

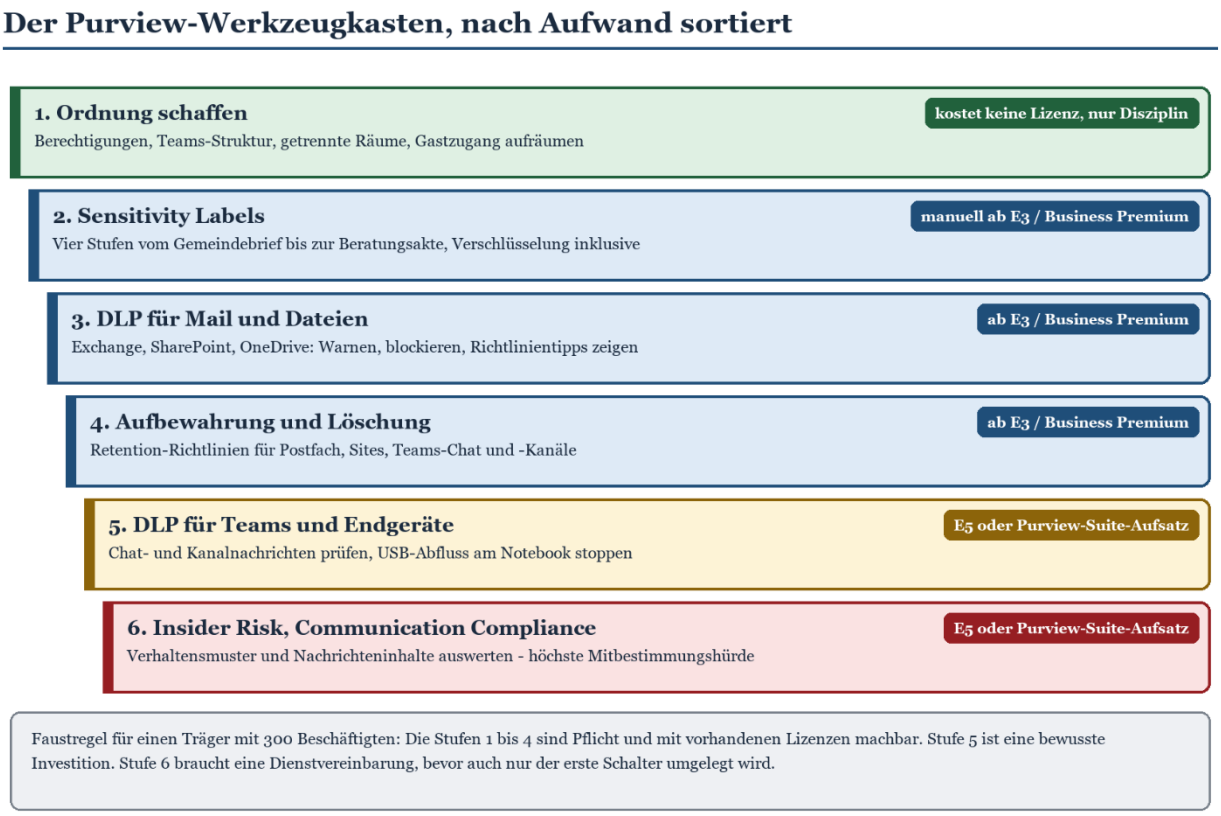
Tipp: Frag nicht nach Verstößen, frag nach Werkzeugen

Eine Bestandsaufnahme, die als Kontrolle daherkommt, produziert Schweigen. Eine, die fragt „Welche Auswertung brauchst du und bekommst du sie aus dem Fachverfahren?“, produziert eine Liste mit Lücken — und damit die Begründung für das Budget, das du ohnehin brauchst.

Praktisch bewährt: Ein diakonisches Werk in einer Großstadt hat die Frage in die bestehenden Leitungsrunden gegeben statt in einen Fragebogen. Nach sechs Wochen lag eine Liste mit elf wiederkehrenden Auswertungen vor, von denen sieben das Fachverfahren konnte — es wusste nur niemand. Vier blieben übrig und wurden zu einem Projektauftrag.

Die Purview-Werkzeuge, ehrlich einsortiert

Microsoft Purview ist kein Produkt, sondern eine Familie. Manche Mitglieder sind fleißig und anspruchslos, andere brauchen eine teure Lizenz und einen halben Personalstab. Die folgende Einordnung nimmt als Maßstab den Träger, um den es hier geht: rund 300 Beschäftigte, davon ein erheblicher Teil ohne festen Schreibtisch, eine IT mit zwei bis drei Köpfen, eine örtlich beauftragte Person für den Datenschutz mit einem Stellenanteil und eine MAV, die zu Recht genau hinschaut.



Skizze 2: Sechs Stufen, aufsteigend nach Aufwand und Lizenzbedarf. Die unteren vier sind der Pflichtteil.

Sensitivity Labels: die Sprache, in der alles andere spricht

Vertraulichkeitsbezeichnungen sind der Grundstein, weil sie die einzige Kennzeichnung sind, die an einem Dokument haftet, auch wenn es kopiert, umbenannt oder aus dem Tenant geschickt wird. Ein Label kann rein kennzeichnend wirken, es kann eine Wasserzeichen-Kopfzeile setzen, und es kann verschlüsseln — dann bleibt die Datei auch dann geschützt, wenn sie am falschen Ort landet.

Die lizenzrechtliche gute Nachricht: Manuelle Vertraulichkeitsbezeichnungen sind bereits in Microsoft 365 E3, in Business Premium und sogar in den Frontline-Plänen F1 und F3 enthalten. Automatische Klassifizierung auf Client- und Dienstseite setzt dagegen E5 oder den entsprechenden Information-Protection-Zusatz voraus. Für den Einstieg heißt das: Vier Stufen definieren, veröffentlichen, erklären — und die Automatik später nachrüsten, wenn sich die Stufen im Alltag bewährt haben. Wie ein solches Label-Konzept für kirchliche Träger konkret aussieht, gehört in ein eigenes Konzeptpapier; die Grundstruktur sieht in fast allen Häusern ähnlich aus.

Label	Typischer Inhalt	Technische Wirkung	Wer darf damit

			arbeiten
Öffentlich	Gemeindebrief, Pressemitteilung, Stellenausschreibung, Flyer der Beratungsstelle	keine Einschränkung, nur Kennzeichnung	alle
Intern	Protokolle ohne Personenbezug, Konzepte, Qualitätshandbuch, Dienstpläne	Kennzeichnung, Warnung beim externen Versand	alle Beschäftigten
Vertraulich	Personalangelegenheiten, Vergaben, Gremienvorlagen, pseudonymisierte Fallübersichten	Verschlüsselung, nur Tenant-intern, kein Weiterleiten nach außen	definierte Gruppen
Streng vertraulich — Klientenbezug	Das, was sich nachweislich nicht vermeiden ließ: Berichte, Hilfeplanauszüge, Gutachten	Verschlüsselung mit enger Gruppe, kein Drucken, kein Kopieren, kurze Aufbewahrung	namentlich benannte Fachkräfte

Vier Stufen reichen. Wer sieben baut, bekommt sieben falsch benutzte Stufen.

Wichtig: Ein Label ist kein Ersatz für die Zuständigkeitsfrage

Die verlockendste Fehlentscheidung lautet: „Wir machen ein Label für Klientendaten, dann dürfen sie in Microsoft 365 liegen." Das ist die Reihenfolge rückwärts.

Erst wird entschieden, was überhaupt nach Microsoft 365 darf. Dann wird das, was unvermeidbar dort landet, mit einem Label geschützt. Ein Label legitimiert keine Verarbeitung — es sichert eine ab, die schon aus anderen Gründen zulässig ist.

Data Loss Prevention: der Türsteher mit Augenmaß

DLP prüft Inhalte gegen Muster und greift ein: warnen, blockieren, protokollieren. Für Exchange Online, SharePoint Online und OneDrive ist DLP in E3 und in Business Premium enthalten. Die Ausweitung auf Teams-Chat und -Kanalnachrichten sowie auf Endgeräte über Endpoint DLP setzt dagegen E5, den Purview-Suite-Aufsatz oder eine Information-Protection-Lizenz voraus. Das ist für die Planung entscheidend, denn ausgerechnet der Teams-Chat ist der Ort, an dem Klientennamen am häufigsten auftauchen.

Der praktische Fallstrick liegt nicht in der Lizenz, sondern im Regelwerk. Die mitgelieferten Erkennungsmuster sind auf Kreditkartennummern und Ausweisdaten trainiert, nicht auf „Betreuungsverlauf Frau K.". Ein Träger mit 300 Beschäftigten kommt mit drei bis fünf eigenen, gut gewählten Mustern deutlich weiter als mit vierzig generischen — etwa dem Aktenzeichenformat des Fachverfahrens, der Struktur der Versichertennummer, einer Handvoll Schlüsselwörter aus dem Diagnosevokabular in Kombination mit einem Personennamen.

Und ein Verfahrenshinweis, der mehr Projekte rettet als jede Feinjustierung: Fang im Berichtsmodus an. Drei Monate mitlaufen lassen, ohne zu blockieren, ergibt eine belastbare Zahl über tatsächliche Treffer und Fehlalarme. Mit dieser Zahl gehst du in die MAV-Sitzung. Ohne sie diskutierst du über Gefühle.

Aufbewahrung und Löschung: die unterschätzte Pflicht

Aufbewahrungsrichtlinien in Purview sind in E3, E5 und Business Premium enthalten und decken Postfächer, SharePoint, OneDrive sowie Teams-Chats und -Kanäle ab. Bei Teams gilt eine Besonderheit, die man kennen sollte: Für einen Teil der günstigeren Pläne muss der Aufbewahrungs- oder Löschzeitraum länger als dreißig Tage sein.

Bei Klientendaten ist die Löschung wichtiger als die Aufbewahrung. Die Aufbewahrungsfristen aus dem Fachrecht gelten für die Akte im Fachverfahren, nicht für die Arbeitskopie in OneDrive. Eine Arbeitskopie mit Klientenbezug ist nach Abschluss des Vorgangs schlicht zu löschen — und weil sich niemand daran erinnern wird, gehört diese Löschung automatisiert. Wie sich kirchliche Fristenordnungen und Kassationsregelungen insgesamt in Purview abbilden lassen, ist ein Thema für sich; für Klientendaten reicht als Einstieg eine kurze, klar begründete Frist auf den Ablagen, in denen sie überhaupt vorkommen dürfen.

Insider Risk Management und Communication Compliance: mit sehr spitzen Fingern

Diese beiden Werkzeuge sind technisch beeindruckend und politisch heikel. Insider Risk Management bewertet Verhaltensmuster — massenhafte Downloads, Kopieren auf USB, Aktivität kurz vor dem Austritt. Communication Compliance prüft Nachrichteninhalte auf Richtlinienverstöße. Beide setzen Microsoft 365 E5, den Purview-Suite-Aufsatz oder eine entsprechende Zusatzlizenz voraus; Communication Compliance ist zusätzlich in Office 365 E5 enthalten.

Die Lizenz ist dabei die kleinere Hürde. Die größere heißt Mitbestimmung. Beide Werkzeuge erzeugen Auswertungen über das Verhalten einzelner Personen, und damit sind sie in der Sache genau das, was MVG-EKD und MAVO im Blick haben, wenn sie von technischen Einrichtungen sprechen, die zur Überwachung geeignet sind. Ohne Dienstvereinbarung ist das kein Projekt, sondern ein Konflikt mit Ansage. Was dabei zu regeln ist und in welcher Reihenfolge, behandelt der Beitrag Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung.

Meine Empfehlung für einen Träger dieser Größe ist unspektakulär: Lass die Finger davon, bis die Stufen eins bis vier sitzen. Ein Insider-Risk-Alarm, den niemand auswertet, ist schlechter als keiner — er dokumentiert, dass du hingesehen und nichts getan hast.

Werkzeug	Was es leistet	Ab welcher Lizenz	Realistisch bei 300 Beschäftigten?
Sensitivity Labels, manuell	Kennzeichnen, verschlüsseln, Weitergabe begrenzen	E3, Business Premium, F1/F3	Ja — der Einstieg schlechthin
Automatische Klassifizierung	Labels ohne Zutun der Beschäftigten setzen	E5 oder Information Protection	Später, wenn die Stufen stehen
DLP Exchange, SharePoint, OneDrive	Mail und Dateien prüfen, warnen, blockieren	E3, Business Premium	Ja — zuerst im Berichtsmodus
DLP für Teams-Chat und -Kanäle	Nachrichten mit sensiblen Inhalten abfangen	E5 oder Purview-Suite-Aufsatz	Wünschenswert, bewusst zu budgetieren
Endpoint DLP	Abfluss über USB, Cloud-	E5 oder Purview-Suite-	Nur mit gemanagten

	Upload, Druck am Gerät stoppen	Aufsatz	Geräten sinnvoll
Aufbewahrung und Löschung	Fristen und Kassation automatisiert durchsetzen	E3, Business Premium	Ja — und oft die wirksamste Maßnahme
Communication Compliance	Nachrichteninhalte auf Verstöße prüfen	E5, Purview Suite, Office 365 E5	Nur mit Dienstvereinbarung, selten nötig
Insider Risk Management	Riskante Verhaltensmuster erkennen	E5, Purview Suite, IRM-Zusatz	In der Regel nein — Betriebsaufwand zu hoch
eDiscovery und Audit	Vorgänge rekonstruieren, Auskunft belegen	Standard breit verfügbar, Premium ab E5	Ja, im Standardumfang — für Auskünfte und Datenpannen unverzichtbar

Der Purview-Werkzeugkasten gegen die Betriebsrealität eines mittleren Trägers gehalten.

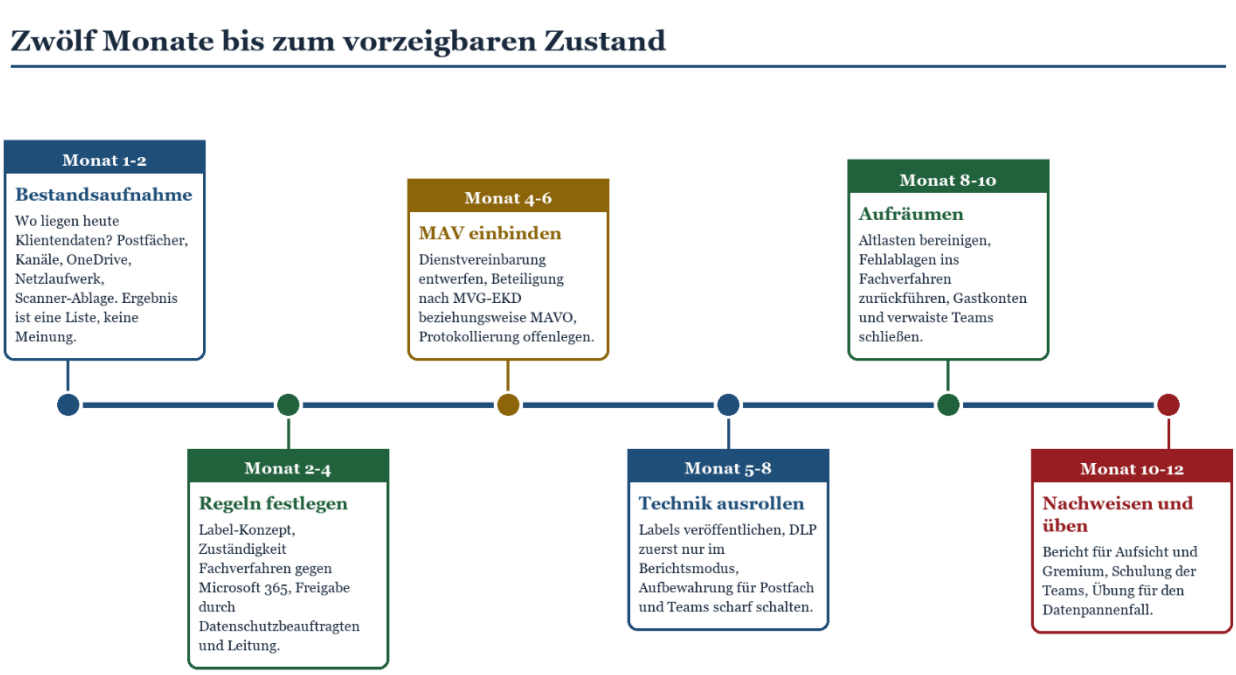
Fakten: Lizenznamen und was sich geändert hat

Microsoft hat den früheren E5-Compliance-Aufsatz in „Microsoft Purview Suite“ umbenannt; Funktionsumfang und Preis blieben davon unberührt. Für Häuser mit Microsoft 365 Business Premium als Basis gibt es die Suite als Zusatz — allerdings gedeckelt auf insgesamt 300 Plätze.

Für gemeinnützige Träger relevant: Der frühere Gratis-Grant über zehn Plätze Business Premium ist mit Wirkung zum 1. Juli 2025 ausgelaufen. Geblieben sind bis zu 300 gespendete Plätze Business Basic sowie Rabatte auf die kostenpflichtigen Pläne. Wer seine Purview-Planung auf den alten Grant gestützt hat, rechnet besser neu.

Ein realistischer Zuschnitt für einen Träger mit 300 Beschäftigten

Die Frage, die in jeder Leitungsrunde kommt, lautet: Was machen wir zuerst? Die Antwort enttäuscht regelmäßig, weil sie nicht mit Technik anfängt.



Skizze 3: Zwölf Monate, sechs Etappen. Der technische Rollout steht bewusst nicht am Anfang.

Zuerst: Zuständigkeiten, dann Schalter

Ohne eine schriftliche, von der Geschäftsführung getragene Festlegung, welche Datenart in welches System gehört, ist jede Purview-Konfiguration Ratespiel. Diese Festlegung ist kein Fünfzigseiter. In den Häusern, in denen sie funktioniert, passt sie auf zwei Seiten: eine Tabelle der Datenarten mit dem führenden System, ein Satz zur Ausnahmeregelung und die Benennung der Person, die Ausnahmen genehmigt. Genau diese Tabelle ist es, die deine örtlich beauftragte Person für den Datenschutz braucht, um überhaupt bewerten zu können — und die die Aufsicht als Erstes sehen will.

Datenart	Rechtsgrundlage und Schutzregime	Typischer Fundort in Microsoft 365	Schutzmaßnahme
Beratungsverlauf, Fallakte	§ 13 DSG-EKD / § 11 KDG; Berufsgeheimnis nach § 203 StGB	Postfach, OneDrive, OneNote im Team	Gehört ins Fachverfahren; in Microsoft 365 Fundstellen bereinigen, DLP-Regel auf Aktenzeichenformat
Gesundheits- und Pflegedaten, Diagnosen	besondere Kategorie; Verarbeitung nur durch Fachpersonal unter Berufsgeheimnis	Excel-Belegungslisten im Teams-Kanal, Mailanhänge	Fachverfahren; sonst eigener Raum, Label mit Verschlüsselung, enge Gruppe, kurze Frist
Von Kostenträgern übermittelte Sozialdaten	§ 78 SGB X: Zweckbindung und Geheimhaltung beim Dritten	Sammelpostfach, SharePoint-Eingangsbibliothek	Automatische Weitergabe ins Fachverfahren, Löschroutine auf dem Eingang
Anvertraute Daten in der Jugendhilfe	§ 65 SGB VIII: besonderer Vertrauensschutz	Teams-Chat der Fallgruppe, OneNote	Kein Chat mit Klarnamen; Fallbesprechung nur mit Aktenzeichen

Seelsorgeinhalte	§ 3 DSG-EKD; auf katholischer Seite Beicht- und Seelsorgegeheimnis	OneNote, Teams, Kalenderbetreff, Copilot-Verläufe	Gar keine digitale Ablage im Tenant; Konten und Postfächer aus der Indizierung heraushalten
Spender- und Kollektendaten	kirchliches Datenschutzrecht, Abgabenordnung für Zuwendungsbestätigungen	Excel in der Verwaltungsablage, Serienbrief-Listen	Führendes System Fundraising oder Finanzbuchhaltung; Label „Vertraulich“
Beschäftigtendaten, Personalakte	kirchliches Datenschutzrecht, AVR, Mitbestimmung nach MVG-EKD oder MAVO	Mailanhänge, Personal-Team in SharePoint	Eigene, berechtigungsbegrenzte Site; Label „Vertraulich“; keine Aufnahme in Copilot-Reichweite
Gemeindegliederdaten aus dem Meldewesen	kirchliches Meldewesen, eigenes Regelwerk der Landeskirche oder des Bistums	Exporte als Excel, Verteilerlisten	Bleibt im Meldewesen; nur aggregierte Auswertungen nach Microsoft 365

Die Tabelle, mit der jedes Klientendaten-Konzept anfängt. Spalte 3 füllst du nicht am Schreibtisch, sondern durch Hinsehen.

MAV, Gremien und der Weg zur Dienstvereinbarung

Purview-Funktionen erzeugen Protokolle, und Protokolle über Beschäftigte lösen Beteiligung aus. Das gilt für DLP-Treffer ebenso wie für Aktivitätsberichte, erst recht für alles auf Stufe sechs. Der Fehler, den Häuser machen, ist selten inhaltlicher Natur — er liegt im Zeitpunkt. Die MAV wird informiert, wenn die Konfiguration steht. Dann ist jede Nachfrage automatisch eine Bremse, und das Projekt bekommt einen Beigeschmack, den es nie wieder los wird.

Besser läuft es, wenn die MAV in der Phase mitliest, in der es noch nichts zu bewerten gibt: bei der Bestandsaufnahme. Ein Caritasverband auf Kreisebene hat die Auswertung der Fundstellen gemeinsam mit zwei MAV-Mitgliedern gelesen, bevor überhaupt über Werkzeuge gesprochen wurde. Die anschließende Dienstvereinbarung war in drei Sitzungen fertig, weil die gemeinsame Tatsachengrundlage nicht mehr strittig war. Der zusätzliche Nebeneffekt: Die MAV hatte ein eigenes Interesse daran, dass Klientendaten nicht im offenen Kanal liegen — dort hängt nämlich auch die Haftung derjenigen, die sie dort ablegen.

Tipp: Drei Sätze, die in jede Dienstvereinbarung gehören

Erstens: Wozu die Protokolle ausgewertet werden dürfen — und wozu ausdrücklich nicht. Eine Verhaltens- und Leistungskontrolle ist auszuschließen, sonst wird jede spätere Auswertung zum Streitfall.

Zweitens: Wer auswerten darf, nach welchem Vier-Augen-Prinzip und mit welcher Beteiligung der MAV im Einzelfall.

Drittens: Wie lange die Protokolle aufbewahrt werden und wann sie automatisch gelöscht sind. Eine Frist, die nicht technisch hinterlegt ist, existiert nicht.

Was die Aufsicht tatsächlich sehen will

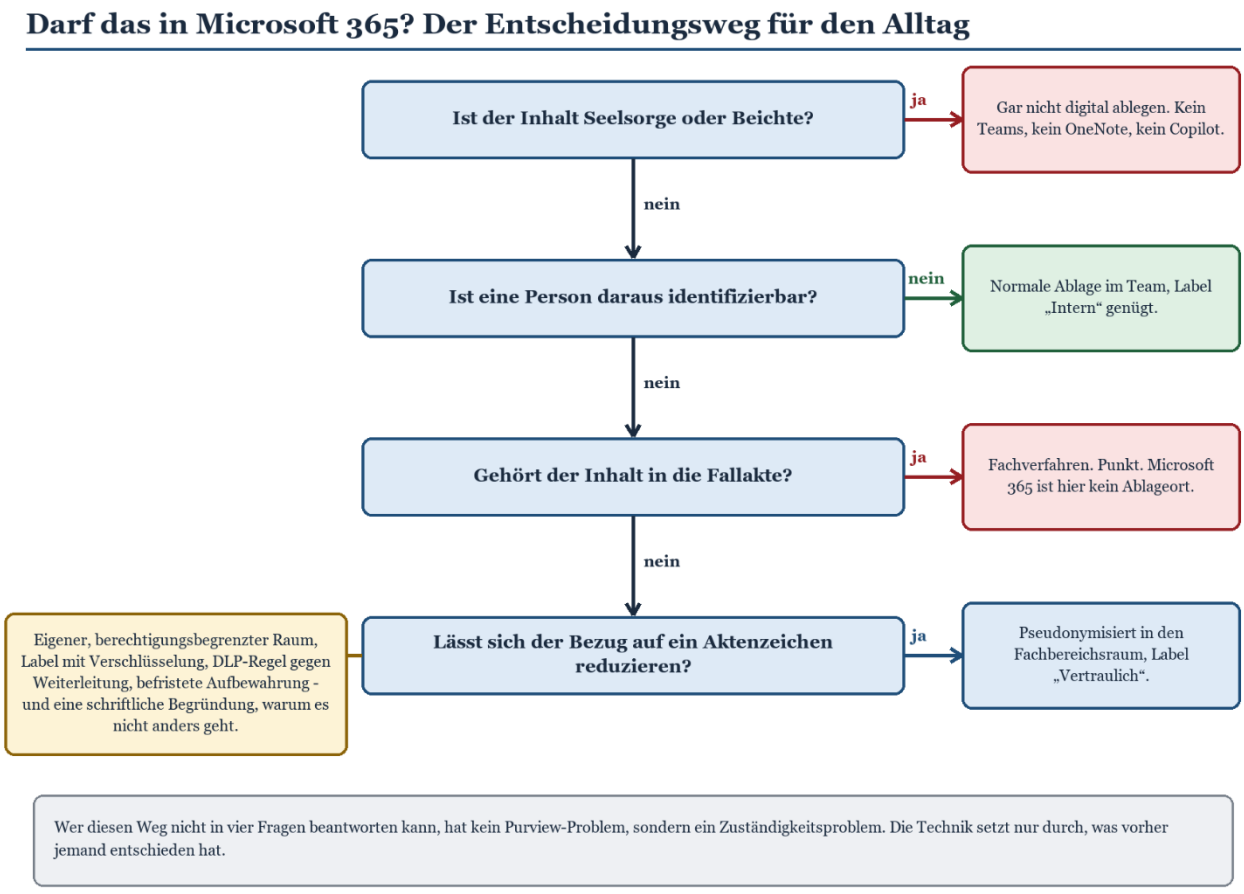
Weder der Beauftragte für den Datenschutz der EKD noch eine Diözesandatenschutzaufsicht erwartet, dass ein Träger mit 300 Beschäftigten sämtliche Purview-Funktionen betreibt. Was erwartet wird, ist Nachvollziehbarkeit: ein aktuelles Verzeichnis der Verarbeitungstätigkeiten, in

dem die Klientendatenverarbeitung realistisch beschrieben ist; eine Schutzbedarfsfeststellung, die zwischen Gemeindebrief und Beratungsakte unterscheidet; die Auftragsverarbeitungsvereinbarungen mit Microsoft, Systemhaus und Rechenzentrum samt der Verschwiegenheitsverpflichtung nach § 203 StGB; und für eine Verarbeitung dieser Sensibilität eine Datenschutz-Folgenabschätzung, die den Namen verdient.

Vor allem aber will die Aufsicht sehen, dass Abweichungen erkannt werden. Ein Träger, der sagt „bei uns gibt es keine Klientendaten in Teams“, wirkt in dem Moment unglaubwürdig, in dem die erste Suchabfrage das Gegenteil zeigt. Ein Träger, der eine Fundstellenliste vorlegt, einen Bereinigungsstand und ein laufendes Monitoring, steht wesentlich besser da — auch wenn die Zahl der Fundstellen unangenehm ist. Was die kirchlichen Aufsichten im Einzelnen abfragen, ist in Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten zusammengetragen.

Die Entscheidung im Alltag muss in vier Fragen passen

Ein Konzept, das nur die Datenschutzbeauftragte versteht, ändert nichts. Was das Team in der Beratungsstelle braucht, ist ein Weg, den man in einer Dienstbesprechung erklären und an die Pinnwand hängen kann.



Skizze 4: Vier Fragen, fünf mögliche Antworten. Mehr braucht der Alltag nicht.

Der linke, gelbe Ausgang ist dabei der wichtigste — und der, den die meisten Konzepte unterschlagen. Es gibt Fälle, in denen sich eine Verarbeitung in Microsoft 365 nicht vermeiden lässt: der Bericht, den das Fachverfahren nicht erzeugen kann, die Kooperationsstatistik für den Kostenträger, der Mailverkehr mit einem Gericht. Wer dafür keinen zulässigen Weg beschreibt,

bekommt keinen sauberen Zustand, sondern einen heimlichen. Der beschriebene Weg heißt: eigener Raum mit enger Gruppe, Label mit Verschlüsselung, DLP-Regel gegen Weiterleitung nach außen, kurze Aufbewahrungsfrist — und eine Zeile in einem Ausnahmeverzeichnis, damit später jemand nachsehen kann, ob die Ausnahme noch nötig ist.

Der Sonderfall, der keine Ausnahme kennt

Eine Kategorie fällt aus dieser ganzen Systematik heraus, und zwar vollständig: Seelsorge. Das Seelsorgegeheimnis auf evangelischer Seite und das Beicht- und Seelsorgegeheimnis auf katholischer Seite sind keine besonders hohe Schutzstufe, sondern eine andere Kategorie. Hier hilft kein Label, keine Verschlüsselung, kein berechtigungsbegrenzter Raum — hier hilft nur, dass die Inhalte gar nicht erst in den Tenant gelangen. Das betrifft auch Nebenwirkungen, an die im Projekt selten jemand denkt: Kalendereinträge, automatische Transkripte, die Indizierung durch Copilot. Ausführlich behandelt das der Beitrag Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf.

Die Abgrenzung ist in der Praxis unscharf, weil viele Fachkräfte beides tun — beraten und seelsorglich begleiten, manchmal im selben Gespräch. Für die Konfiguration heißt das: Die Trennung läuft nicht über die Person, sondern über den Kanal. Getrennte Postfächer, getrennte Geräte oder zumindest getrennte Ablagen, klar benannt und erklärt. Und bevor irgendwo Copilot ausgerollt wird, gehört geprüft, worauf der Dienst im Namen eines Nutzers zugreifen kann; das Thema Oversharing behandelt Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout im Detail.

Häufige Fragen

Dürfen Klientendaten überhaupt in Microsoft 365 verarbeitet werden?

Ja — es gibt kein Verbot, das an der Cloud als solcher hängt. Weder DSG-EKD noch KDG kennen eine Norm, die Microsoft 365 ausschließt. Was die beiden Gesetze verlangen, sind eine tragfähige Rechtsgrundlage, die Begrenzung auf Fachpersonal unter Berufsgeheimnis, angemessene technische und organisatorische Maßnahmen, eine saubere Auftragsverarbeitungsvereinbarung und bei dieser Sensibilität eine Datenschutz-Folgenabschätzung. Die ehrlichere Frage ist deshalb nicht, ob es zulässig wäre, sondern ob es sinnvoll ist. In den allermeisten Fällen lautet die Antwort: Die Fallakte gehört ins Fachverfahren, weil dort die Berechtigungs- und Protokollierungslogik schon eingebaut ist, die du in Microsoft 365 mühsam nachbauen müsstest.

Wir haben nur Business Premium. Reicht das für einen verantwortbaren Zustand?

Für den Pflichtteil ja. Manuelle Vertraulichkeitsbezeichnungen, DLP für Exchange, SharePoint und OneDrive sowie Aufbewahrungs- und Löschrichtlinien sind enthalten. Was fehlt, ist DLP für Teams-Chat und -Kanäle, Endpoint DLP und die automatische Klassifizierung. Das ist eine spürbare Lücke, aber keine, die einen verantwortbaren Betrieb verhindert — solange du sie kennst, benennst und organisatorisch kompensierst, etwa durch die klare Regel, dass im Teams-Chat keine Klarnamen von Klientinnen und Klienten vorkommen. Den Purview-Suite-Aufsatz gibt es zu Business Premium hinzu, gedeckelt auf 300 Plätze.

Reicht es, wenn alle Beschäftigten eine Verschwiegenheitserklärung unterschrieben haben?

Nein, aber sie ist notwendig. Die Verpflichtung auf das Datengeheimnis — im KDG ausdrücklich in § 5 geregelt, im DSG-EKD entsprechend vorgesehen — ist Pflicht und deckt den kirchlichen Rechtskreis ab. Sie ersetzt weder die technische Begrenzung des Zugriffs noch die gesonderte Verpflichtung mitwirkender Personen nach § 203 StGB. Und sie hilft in dem Moment nicht, in dem die Aufsicht fragt, warum der Fahrdienst technisch auf Diagnosen zugreifen konnte. Unterschriften begrenzen Befugnisse, keine Berechtigungen.

Ist der Teams-Chat rechtlich etwas anderes als eine Mail?

Rechtlich nein — beides sind Verarbeitungen personenbezogener Daten im Tenant. Praktisch verhalten sich Menschen aber völlig unterschiedlich: Chat fühlt sich flüchtig an, Mail nicht. Genau darin liegt die Gefahr, denn Chatnachrichten werden dauerhaft gespeichert, sind durchsuchbar, unterliegen Aufbewahrungsrichtlinien und tauchen in eDiscovery-Recherchen auf. Der Chat aus der Nachtschicht ist zwei Jahre später noch da. Die Regel „kein Klientenname im Chat“ ist deshalb keine Schikane, sondern die einzige Regel, die sich ohne E5-Lizenz durchsetzen lässt.

Was tun wir mit den Altlasten, die die Bestandsaufnahme zutage fördert?

Nicht heimlich löschen. Der saubere Ablauf lautet: Fundstellen dokumentieren, Zugriffsverlauf über das Audit-Protokoll prüfen, Betroffenheit bewerten, gemeinsam mit der datenschutzbeauftragten Person entscheiden, ob eine Meldung an die kirchliche Aufsicht erforderlich ist, danach bereinigen und die Bereinigung dokumentieren. Bei größeren Beständen empfiehlt sich ein Stichtag: Alles vor Datum X wird in einen gesperrten Bereich verschoben und nach Ablauf einer festgelegten Frist gelöscht, alles danach läuft nach den neuen Regeln. Das ist unelegant, aber es macht den Übergang prüfbar.

Brauchen wir für Purview eine eigene Datenschutz-Folgenabschätzung?

Für die Klientendatenverarbeitung in Microsoft 365 ja — eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten ist der Lehrbuchfall. Purview selbst ist dabei kein eigener Verarbeitungsvorgang, sondern eine Schutzmaßnahme, die in dieser Folgenabschätzung als solche beschrieben wird. Anders sieht es bei Insider Risk Management und Communication Compliance aus: Die richten sich auf das Verhalten von Beschäftigten und verdienen eine eigene Betrachtung — parallel zur Beteiligung der Mitarbeitervertretung.

Wie halten wir Auszubildende, Praktikanten und Ehrenamtliche aus den Klientendaten heraus?

Über Gruppen und Lizenzzuschnitt, nicht über Appelle. Praktisch bewährt hat sich, Teams mit Klientenbezug ausschließlich über eine eigene, gepflegte Sicherheitsgruppe zu besetzen, deren Mitgliedschaft an eine dokumentierte Einweisung und die Verschwiegenheitsverpflichtung gekoppelt ist. Gastkonten haben in solchen Teams nichts verloren. Und weil Ehrenamt in kirchlichen Trägern ein eigener, wertvoller und organisatorisch anstrengender Fall ist: Ehrenamtliche gehören in eigene Räume mit eigenem Zuschnitt, nicht in den Fachbereichsraum mit einer Berechtigung weniger.

Unser Fachverfahren kann die Auswertung nicht, die der Kostenträger verlangt. Was nun?

Dann beschreibst du den Ausnahmeweg, statt ihn zu verbieten: eigener Raum, enge Gruppe, Label mit Verschlüsselung, kurze Frist, Eintrag im Ausnahmeverzeichnis. Parallel gehört die Lücke auf die Liste für die nächste Fachverfahrensrunde. Wenn sich zeigt, dass viele solcher Auswertungen anfallen, ist eine strukturierte Lösung auf SharePoint-Listen oder Dataverse häufig besser als ein Wildwuchs aus Excel-Dateien — mit dem entscheidenden Vorteil, dass Berechtigungen und Protokollierung dort überhaupt erst existieren. Für den größeren Rahmen, in dem diese Entscheidungen stehen, lohnt der Blick in Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand.

Fazit

Klientendaten sind der Punkt, an dem sich entscheidet, ob eine Microsoft-365-Einführung in Diakonie und Caritas seriös war oder nur schnell. Bei Dienstplänen und Gremienprotokollen verzeiht die Umgebung viel. Bei einer Belegungsliste mit Diagnosen im offenen Kanal verzeiht sie nichts — weil dort nicht eine Regel verletzt wird, sondern die Grundlage entfällt, auf der die Verarbeitung überhaupt zulässig wäre.

Die gute Nachricht ist, dass der wirksamste Teil des Schutzes weder teuer noch kompliziert ist. Eine zweiseitige Festlegung, welche Datenart in welches System gehört. Vier Vertraulichkeitsbezeichnungen, die Menschen verstehen. Drei bis fünf DLP-Regeln, die zuerst nur berichten. Eine Löschroutine auf den Ablagen, in denen Klientendaten überhaupt vorkommen dürfen. Und ein beschriebener Ausnahmeweg für die Fälle, in denen es sich nicht vermeiden lässt. Das alles ist mit den Lizenzen machbar, die dein Haus mit hoher Wahrscheinlichkeit bereits hat.

Die schlechte Nachricht ist, dass dieser Teil nicht delegierbar ist. Insider Risk Management kann man kaufen. Die Entscheidung, dass die Fallakte ins Fachverfahren gehört und nicht in OneDrive, muss die Geschäftsführung treffen, die Datenschutzbeauftragte begleiten und die Mitarbeitervertretung mittragen. Purview setzt anschließend zuverlässig durch, was vorher jemand entschieden hat — und ebenso zuverlässig gar nichts, wenn niemand entschieden hat.

Fang deshalb nicht mit dem Purview-Portal an, sondern mit der Suche. Eine ehrliche Bestandsaufnahme dauert sechs Wochen, tut kurz weh und ist danach die belastbarste Grundlage, die du haben kannst — gegenüber der Leitung, gegenüber der MAV und gegenüber der Aufsicht.

Weiter im Thema

Wenn du an diesem Punkt Unterstützung brauchst — bei der Bestandsaufnahme, beim Label-Konzept oder bei der Abstimmung mit MAV und Aufsicht — findest du das passende Angebot hier:

› Microsoft 365 in Kirche, Diakonie und Caritas

› Kirche, Diakonie, Caritas: DSG-EKD, KDG und die Mitarbeitervertretung

› Microsoft-365-Schulungen für kirchliche Träger

› Microsoft-365-Beratung für kirchliche Träger