

Schweigepflicht und Cloud: § 203 StGB, Landeskrankenhausgesetze und Auftragsverarbeitung

§ 203 StGB

Schweigepflicht und Cloud

Wer mitwirken darf, wer unterschreiben muss – und wer im Rechenzentrum den Schlüssel hält

Drei Fragen, drei Rechtsgebiete

- ☐ Strafrecht: Darf der Dienstleister mitwirken?
- ☐ Datenschutz: Ist die Auftragsverarbeitung sauber geregelt?
- ☐ Landesrecht: Was sagt das Krankenhausgesetz Ihres Landes?



Die Cloud ist nicht das Problem. Die fehlende Unterschrift ist es.

Wissen

Alle Beiträge der Serie im Überblick:

› [Microsoft 365 im Krankenhaus](#)

Beratung

Verträge, Zugriffswege und Schlüssel prüfen:

› [Microsoft 365 Beratung für Krankenhäuser](#)

Schulung

Für IT, Datenschutz, ISB und Leitungsebene:

› [Microsoft 365 Schulung für Krankenhäuser](#)

Kaum ein Thema hält sich in Krankenhaus-Lenkungskreisen so hartnäckig wie die Schweigepflicht. Sie taucht zuverlässig dann auf, wenn eigentlich über etwas anderes gesprochen werden sollte: über das neue Intranet, über Teams für die Arzneimittelkommission, über Exchange Online. Irgendwann hebt jemand die Hand und sagt den Satz, der jede Projektplanung um sechs Wochen verlängert: „Und was ist mit § 203?“

Die gute Nachricht: Die Frage ist berechtigt, aber nicht unlösbar. Seit der Neuregelung im Jahr 2017 kennt das Strafgesetzbuch ausdrücklich die **mitwirkenden Personen** – also Dienstleister, die an der Tätigkeit von Ärzten und anderen Berufsheimnisträgern mitwirken, ohne selbst dazuzugehören. Die weniger gute Nachricht: Mit dem Strafrecht allein ist es nicht getan. Daneben stehen die Auftragsverarbeitung nach Datenschutzrecht, die Landeskrankenhausgesetze mit ihren sehr unterschiedlichen Regeln und für Cloud-Dienste zusätzlich das Sozialrecht. Drei Rechtsgebiete, drei Fragen, und keines beantwortet die Frage des anderen.

Dieser Beitrag sortiert die Fragen, zeigt, was das für Microsoft 365 konkret bedeutet – Vertrag, Verschwiegenheitsverpflichtung, Zugriffswege des Anbieters, Schlüsselverwaltung – und wo Sie mit Ihrer Rechtsberatung sprechen sollten. Er gehört zur Serie [Microsoft 365 im Krankenhaus](#) und richtet sich an IT-Leitung, Geschäftsführung, Datenschutz, Informationssicherheit und alle, die im Lenkungsreis gern die Hand heben.

Hinweis: keine Rechtsberatung

Dieser Beitrag beschreibt die Rechtslage aus Sicht der IT-Beratung, um Ihnen die richtigen Fragen an die Hand zu geben. Er ersetzt keine Rechtsberatung. Ob und wie Ihr Haus Microsoft 365 für bestimmte Daten einsetzen darf, hängt von Trägerschaft, Bundesland, Vertragslage und tatsächlicher Nutzung ab. Lassen Sie die Bewertung von Ihrem Justizariat, einer spezialisierten Kanzlei und Ihrem Datenschutzbeauftragten vornehmen. Gesetzestexte ändern sich – lesen Sie vor jeder Entscheidung die geltende Fassung.

Fakten auf einen Blick

- **§ 203 StGB:** Unbefugtes Offenbaren fremder Geheimnisse durch Berufsgeheimnisträger ist strafbar – Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.
- **Seit 2017:** Offenbaren an sonstige mitwirkende Personen ist erlaubt, soweit es für deren Tätigkeit erforderlich ist (Abs. 3).
- **Die Bedingung:** Wer mitwirkende Personen einbindet, muss dafür sorgen, dass sie zur Geheimhaltung verpflichtet werden – sonst droht eigene Strafbarkeit (Abs. 4).
- **Datenschutz:** Unabhängig davon braucht es einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO – im kirchlichen Bereich nach KDG oder DSG-EKD.
- **Landesrecht:** Die Landeskrankenhausgesetze regeln die Auftragsverarbeitung von Patientendaten teils zusätzlich und teils strenger.

§ 203 StGB nach der Neuregelung: Wer zum Kreis gehört

Fangen wir beim Strafrecht an, weil hier die meisten Missverständnisse wohnen. § 203 StGB bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Angehörigem bestimmter Berufe anvertraut oder sonst bekannt geworden ist. Geschützt ist nicht „der Datensatz“, sondern das Geheimnis: die Tatsache, dass jemand Patient ist, die Diagnose, der Befund, auch der Umstand, wer wann auf welcher Station lag.

Berufsgeheimnisträger – und warum das Krankenhaus selbst keiner ist

Absatz 1 zählt die Berufe auf. Für das Krankenhaus relevant sind vor allem Ärzte, Apotheker und Angehörige anderer Heilberufe mit staatlich geregelter Ausbildung – also auch Pflegekräfte, Therapeuten und viele Funktionsberufe. Schweigepflichtig ist der Mensch, nicht die Institution. Das Krankenhaus als Träger ist kein Berufsgeheimnisträger im Sinne des Absatzes 1, organisiert aber die Umgebung, in der Ärzte und Pflegekräfte ihre Schweigepflicht einhalten können oder eben nicht.

Für Häuser in öffentlicher Trägerschaft kommt Absatz 2 hinzu: Er erfasst Amtsträger und für den öffentlichen Dienst besonders Verpflichtete. Ob und für wen das in Ihrem kommunalen Haus oder Universitätsklinikum greift, ist eine Frage für das Justizariat – wer sich für die Parallelen in der Verwaltung interessiert, findet sie im Kompetenzbereich [Microsoft 365 in der öffentlichen Verwaltung](#).

Gehilfen und sonstige mitwirkende Personen

Absatz 3 ist das Herzstück der Neuregelung. Er unterscheidet zwei Gruppen:

- **Gehilfen und Auszubildende:** Die Personen, die beim Berufsgeheimnisträger berufsmäßig tätig sind – Stationssekretariat, Schreibdienst, Patientenaufnahme und in der Regel auch die

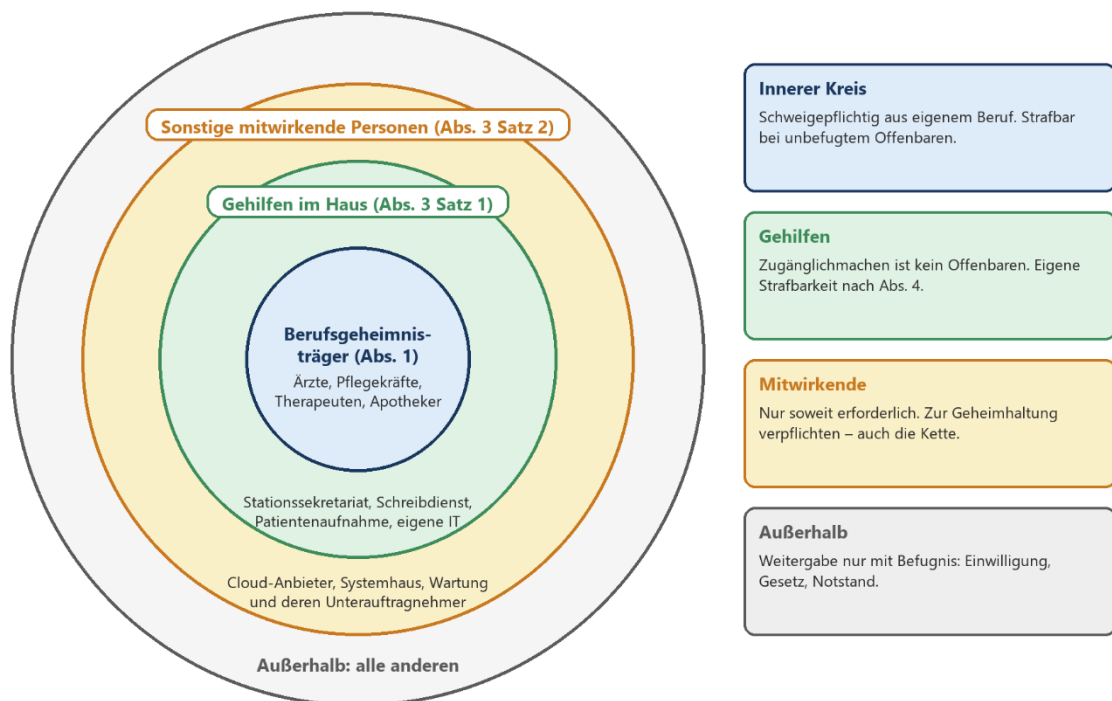
eigene IT-Abteilung. Wer ihnen Geheimnisse zugänglich macht, offenbart nach dem Gesetz nicht.

- **Sonstige mitwirkende Personen:** Externe, die an der beruflichen Tätigkeit mitwirken – das Systemhaus, der Wartungsdienstleister für das KIS, der Cloud-Anbieter. Ihnen gegenüber dürfen Geheimnisse offenbart werden, **soweit das für die Inanspruchnahme ihrer Tätigkeit erforderlich ist**. Dasselbe gilt, wenn diese Mitwirkenden ihrerseits weitere Personen hinzuziehen.

Damit ist die Kette ausdrücklich vorgesehen: Das Krankenhaus bindet Microsoft ein, Microsoft bindet Unterauftragnehmer ein. Das ist nicht per se ein Problem. Es ist aber auch keine Generalvollmacht, denn das Wort „erforderlich“ steht da nicht zur Zierde.

Der Kreis der Schweigepflicht im Krankenhaus

Vereinfachte Darstellung nach § 203 StGB – die Einordnung im Einzelfall prüft die Rechtsberatung



Vom inneren Kreis nach außen: Wer Geheimnisse kennt, wer sie kennen darf – und unter welcher Bedingung.

Die Sorgepflicht: Strafbar ist nicht die Cloud, sondern die fehlende Verpflichtung

Absatz 4 regelt die Kehrseite. Mitwirkende Personen, die ein Geheimnis unbefugt offenbaren, machen sich selbst strafbar. Und – das ist der Punkt, der Ärztliche Direktoren und Geschäftsführungen interessieren sollte – strafbar macht sich auch der Berufsgeheimnisträger, der nicht dafür gesorgt hat, dass eine mitwirkende Person zur Geheimhaltung verpflichtet wurde, wenn diese dann unbefugt offenbart. Dasselbe gilt eine Stufe weiter für Mitwirkende, die ihrerseits Dritte hinzuziehen. Ausgenommen sind Mitwirkende, die selbst Berufsgeheimnisträger sind.

Mit anderen Worten: Das Gesetz bestraft nicht den Einsatz eines Dienstleisters, sondern das Unterlassen der Verpflichtung. Galgenhumorig formuliert: Strafbar ist nicht die Cloud, sondern die fehlende Unterschrift – und zwar genau dann, wenn etwas passiert. Da im Krankenhaus nicht jeder Oberarzt einzeln Verträge mit Microsoft schließt, liegt die praktische Last beim Träger: Er schließt die Verträge und muss so organisieren, dass die Verpflichtung für alle Berufsgeheimnisträger im Haus wirkt.

Rolle im Krankenhaus	Stellung nach § 203 StGB	Was das Haus sicherstellen sollte
Ärzte, Pflegekräfte, Therapeuten	Berufsgeheimnisträger (Abs. 1)	Unterweisung, klare Regeln, welche Daten in welches System gehören
Stationssekretariat, Schreibdienst, Aufnahme	In der Regel Gehilfen (Abs. 3 Satz 1)	Verpflichtung im Arbeitsvertrag, regelmäßige Unterweisung
Eigene IT-Abteilung, Administratoren	In der Regel Gehilfen; Einordnung prüfen	Verpflichtung, Rollenkonzept, Protokollierung privilegierter Zugriffe
Systemhaus, Wartungsfirma, externer Support	Sonstige mitwirkende Personen (Abs. 3 Satz 2)	Schriftliche Verschwiegenheitsverpflichtung, Erforderlichkeit begründen
Cloud-Anbieter (z. B. Microsoft)	Sonstige mitwirkende Person	Vertragliche Verschwiegenheit, Regelung für Unterauftragnehmer, Zugriffswege prüfen
Unterauftragnehmer des Anbieters	Weitere mitwirkende Personen	Weitergabe der Verpflichtung in der Kette nachvollziehen

Warnung: „Erforderlich“ ist ein Prüfkriterium, kein Freibrief

Die Erlaubnis nach Absatz 3 reicht nur so weit, wie die Mitwirkung erforderlich ist. Ein E-Mail-Dienst ist für die Kommunikation des Hauses erforderlich – daraus folgt aber nicht, dass jede Excel-Liste mit Patientennamen, die jemand in einen Teams-Kanal lädt, vom Zweck gedeckt ist. Die ehrliche Frage lautet nicht „Darf Microsoft mitwirken?“, sondern „Wofür genau, und warum liegen diese Daten überhaupt dort?“

Schweigepflicht und Auftragsverarbeitung: zwei Schlösser an derselben Tür

Der zweite große Irrtum lautet: „Wir haben doch einen Auftragsverarbeitungsvertrag.“ Den haben Sie hoffentlich. Er beantwortet aber eine andere Frage.

Art. 28 DSGVO beantwortet die Datenschutzfrage

Die Auftragsverarbeitung nach Art. 28 DSGVO regelt, unter welchen Bedingungen ein Dienstleister personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen verarbeiten darf: Gegenstand und Dauer, Art der Daten, technische und organisatorische Maßnahmen, Unterauftragnehmer, Unterstützung bei Betroffenenrechten, Löschung am Ende. Für Gesundheitsdaten als besondere Kategorie nach Art. 9 DSGVO kommen die Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DSGVO mit entsprechend hohem Schutzbedarf hinzu.

Was Art. 28 DSGVO nicht regelt: ob die Weitergabe eines Geheimnisses an den Dienstleister strafrechtlich befugt ist. Das Bundesdatenschutzgesetz stellt in § 1 ausdrücklich klar, dass gesetzliche Geheimhaltungspflichten sowie Berufs- und besondere Amtsgeheimnisse unberührt bleiben. Datenschutzrecht und Schweigepflicht laufen also nebeneinander, nicht nacheinander.

Wo sich beides trifft

In der Praxis lassen sich beide Pflichten in einem Vertragswerk abbilden. Art. 28 DSGVO verlangt ohnehin, dass der Auftragsverarbeiter die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet. Diese datenschutzrechtliche Vertraulichkeit ist aber nicht automatisch die strafrechtlich gemeinte Verpflichtung zur Geheimhaltung nach § 203 Abs. 4 StGB. Der saubere Weg: eine Verschwiegenheitsklausel, die ausdrücklich auf § 203 StGB Bezug nimmt, über die Strafbarkeit belehrt und die Weitergabe an Unterauftragnehmer an deren Verpflichtung knüpft.



Strafrecht, Datenschutz, Landes- und Sozialrecht: Erst wenn alle drei Schlösser offen sind, ist die Tür offen.

Kirchliche Häuser: KDG und DSG-EKD statt DSGVO

Krankenhäuser in katholischer Trägerschaft wenden das Gesetz über den Kirchlichen Datenschutz (KDG) an, evangelische Häuser das Datenschutzgesetz der EKD (DSG-EKD). Beide regeln die Auftragsverarbeitung eigenständig und in der Grundstruktur ähnlich wie die DSGVO, mit eigenen Aufsichten und teils eigenen Anforderungen an Vertragsinhalte. In einzelnen Diözesen kommen zusätzlich eigene Regelungen zum Patientendatenschutz hinzu. Die Schweigepflicht nach § 203 StGB gilt dagegen für alle – das Strafgesetzbuch kennt keine Kirchenklausel. Was das für Microsoft 365 im Einzelnen bedeutet, behandelt der Beitrag [Microsoft 365 im kirchlichen Krankenhaus: KDG, DSG-EKD und die MAV am Tisch](#); den größeren Rahmen beschreibt der Kompetenzbereich [Microsoft 365 in Kirche, Diakonie und Caritas](#).

Die Rechtsquellen im Überblick

Die folgende Tabelle ordnet die Rechtsquellen, die für die Schweigepflicht in der Cloud zusammenspielen. Sie ist eine Landkarte, keine abschließende Prüfung.

Rechtsquelle	Gilt für	Zentrale Frage für Microsoft 365
§ 203 StGB	Ärzte, Pflegekräfte und andere Berufsheimnisträger; bei öffentlichen Häusern ggf. Amtsträger	Ist Microsoft als mitwirkende Person eingebunden, nur im erforderlichen Umfang, und wirksam zur Geheimhaltung verpflichtet – samt Unterauftragnehmern?
Art. 28 DSGVO	Krankenhäuser in öffentlicher und privater Trägerschaft (soweit kein	Ist der Auftragsverarbeitungsvertrag vollständig, sind Unterauftragnehmer,

Rechtsquelle	Gilt für	Zentrale Frage für Microsoft 365
	kirchliches Recht)	Weisungen und Löschung geregelt?
Art. 9 und 32 DSGVO, § 22 BDSG	Verarbeitung von Gesundheitsdaten	Ist das Schutzniveau dem Schutzbedarf angemessen – Verschlüsselung, Zugriffskontrolle, Protokollierung?
KDG bzw. DSG-EKD	Katholische bzw. evangelische Häuser	Erfüllt der Vertrag die kirchenrechtlichen Anforderungen, ist die kirchliche Aufsicht berücksichtigt?
Landeskrankenhausgesetz	Krankenhäuser im jeweiligen Land; Anwendungsbereich je Land prüfen	Erlaubt das Land die Auftragsverarbeitung von Patientendaten in dieser Form, mit welchen Zusatzaufgaben?
Landesdatenschutzgesetz	Öffentliche Stellen des Landes, je nach Land auch kommunale Häuser	Welche ergänzenden Regeln gelten für öffentliche Häuser?
§ 393 SGB V	Leistungserbringer, also auch zugelassene Krankenhäuser	Werden Sozial- oder Gesundheitsdaten in der Cloud verarbeitet – und liegt dann ein aktuelles C5-Typ-2-Testat oder gleichwertiger Nachweis vor?
§ 391 SGB V bzw. BSIG	Alle Krankenhäuser bzw. Betreiber kritischer Anlagen	Ist Microsoft 365 im ISMS und in der Risikoanalyse des Hauses abgebildet?

Zwei Zeilen dieser Tabelle haben eigene Beiträge in dieser Serie: Was § 393 SGB V verlangt, steht in [§ 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen](#). Die Sicherheitspflichten nach § 391 SGB V, NIS2 und dem B3S behandelt [NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten](#).

Landeskrankenhausgesetze: sechzehn Antworten auf eine Frage

Jetzt wird es föderal. Die datenschutzrechtliche Zulässigkeit der Verarbeitung von Patientendaten im Krankenhaus regeln die Länder, meist im Landeskrankenhausgesetz, teils in eigenen Gesundheitsdatenschutzgesetzen. Das Ergebnis ist ein Flickenteppich, dessen Muster sich alle paar Jahre ändert. Es gibt kein „normales“ Bundesland, an dem sich die anderen messen ließen – und die Fassung, die Ihr Projektordner von 2019 enthält, ist mit einiger Wahrscheinlichkeit nicht mehr die geltende.

Ein Beispiel mit Primärquelle: Bayern

Das Bayerische Krankenhausgesetz erlaubt in Art. 27 Abs. 4, dass sich das Krankenhaus zur Verarbeitung von Patientendaten anderer Personen oder Stellen bedient – sofern es sicherstellt, dass beim Auftragnehmer die besonderen Schutzmaßnahmen nach Art. 27 Abs. 6 eingehalten werden, und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der Patienten beeinträchtigt werden. Früher war die Auftragsverarbeitung in Bayern auf andere Krankenhäuser beschränkt; diese Beschränkung enthält die geltende Fassung nicht mehr. Das zeigt zweierlei:

Landesrecht bewegt sich, und eine Lockerung ist keine Freistellung – die Schutzmaßnahmen bleiben Pflicht.

Typische Regelungsmuster als Prüfpunkte

Für die übrigen Länder nennen wir an dieser Stelle bewusst keine Paragraphen, weil sich Nummerierung und Inhalt immer wieder ändern. Stattdessen die Muster, nach denen Sie Ihr Landesrecht durchsuchen sollten:

Regelungsmuster	Was es bedeutet	Prüffrage für Microsoft 365
Subsidiaritätsklausel	Auftragsverarbeitung nur, wenn sie für den Betrieb nötig oder deutlich wirtschaftlicher ist	Lässt sich die Notwendigkeit für den konkreten Dienst begründen und dokumentieren?
Ausdrücklicher Bezug zur Schweigepflicht	Das Haus muss sich vergewissern, dass beim Auftragnehmer die ärztliche Schweigepflicht gewahrt ist	Ist die Verschwiegenheitsverpflichtung nach § 203 StGB Teil des Vertragswerks?
Getrennte Speicherung	Patientendaten beim Auftragnehmer getrennt von Daten anderer Auftraggeber oder auf getrennten Datenträgern	Wie verhält sich eine solche Vorgabe zu einer mandantenfähigen Cloud? Rechtlich bewerten lassen.
Ortsvorgaben	Verarbeitung nur im Inland, in der EU oder in bestimmten Staaten	In welcher Datenregion liegt Ihr Tenant, welche Dienste verarbeiten außerhalb davon?
Anzeige- oder Zustimmungspflichten	Vorherige Information der Aufsicht oder Zustimmung des Trägers	Wer zeigt an, bis wann, mit welchen Unterlagen?
Beschränkter Anwendungsbereich	Gilt nur für bestimmte Träger, kirchliche Häuser teils ausgenommen	Welches Recht gilt für Ihren Träger an diesem Standort?

Tipp für Klinikverbünde über Ländergrenzen

Ein Verbund mit Standorten in zwei oder drei Ländern hat zwei oder drei Landeskrankenhausgesetze – aber oft nur einen Tenant. Bauen Sie die Prüfung deshalb je Standort auf und richten Sie die gemeinsamen Regeln am strengsten Landesrecht aus, statt am Sitz der Holding. Wie sich mehrere Häuser in einem Mandanten organisieren lassen, beschreibt

› [Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen](#)

Was das für Microsoft 365 praktisch heißt

Vorweg die Grundhaltung dieser Serie: Patientendaten gehören ins KIS und seine Subsysteme – LIS, RIS, PACS. Microsoft 365 ist das Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Wer das ernst nimmt, reduziert das Schweigepflicht-Problem erheblich. Ganz verschwinden wird es trotzdem nicht: Auch das Protokoll der

Morbiditätskonferenz, die E-Mail an den Zuweiser oder das Beschwerdemanagement berühren Geheimnisse im Sinne des § 203 StGB. Wo die Grenze verläuft, beschreibt der Beitrag [Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt](#).

Vertragswerk: Auftragsverarbeitung und Verschwiegenheit

Für Microsoft 365 besteht die datenschutzrechtliche Grundlage aus den Produktbedingungen und dem Data Protection Addendum von Microsoft, das die Auftragsverarbeitung regelt. Daneben bietet Microsoft für Kunden in Deutschland eine Zusatzvereinbarung für Berufsgeheimnisträger an, die auf § 203 StGB Bezug nimmt. Ob diese Vereinbarung Teil Ihres Vertrags ist, in welcher Fassung, über welchen Vertragskanal und für welche Dienste sie gilt, ist ein Prüfauftrag für Ihren Einkauf und Ihr Justizariat – nicht etwas, das man in einem Blogbeitrag pauschal beantworten kann.

- Liegt die Zusatzvereinbarung zur Schweigepflicht unterschrieben bzw. wirksam einbezogen vor – und wo ist sie abgelegt?
- Deckt sie alle Dienste ab, die Sie tatsächlich nutzen, auch neu hinzugekommene wie Copilot?
- Ist geregelt, dass Unterauftragnehmer ebenfalls zur Geheimhaltung verpflichtet werden?
- Gilt dasselbe für Ihr Systemhaus oder Ihren Lizenzpartner, sofern dieser administrativen Zugriff auf den Tenant hat?

Der letzte Punkt wird gern übersehen. Delegierte Administratorrechte von Partnern im Tenant sind ein Zugriffsweg wie jeder andere – und der Partner ist eine mitwirkende Person mit eigener Verpflichtungspflicht. Prüfen Sie in Entra ID, welche Partnerbeziehungen bestehen und welche Rollen sie gewähren; Hintergrund dazu im Kompetenzbereich [Microsoft Entra ID](#).

Verschwiegenheitsverpflichtung im eigenen Haus

Auch die eigene Belegschaft gehört in die Betrachtung. Mitarbeiterinnen und Mitarbeiter der IT sind in der Regel als Gehilfen einzuordnen und über Arbeitsvertrag oder Dienstanweisung zur Verschwiegenheit verpflichtet. Dass die Verpflichtung unterschrieben in der Personalakte liegt, ist das eine. Dass der Administrator weiß, warum er im Exchange-Admin-Center nicht „mal eben“ das Postfach des Chefarztes durchsucht, ist das andere. Unterweisungen für IT, Datenschutz und Leitungsebene gehören deshalb in jedes Einführungsprojekt – etwa im Rahmen einer [Microsoft 365 Schulung für Krankenhäuser](#).

Zugriffswege des Anbieters und Customer Lockbox

Die Schweigepflicht-Frage an die Cloud lautet im Kern: Wer beim Anbieter kann wann auf Inhalte zugreifen? Microsoft beschreibt den Betrieb von Microsoft 365 nach den Prinzipien „Least Privilege“ und „Just in Time“: Kein Microsoft-Personal hat dauerhaften Zugriff auf Kundeninhalte, Zugriffe für Betriebsaufgaben laufen über ein internes Genehmigungssystem namens Lockbox, bei dem eine zweite Person zustimmen muss.

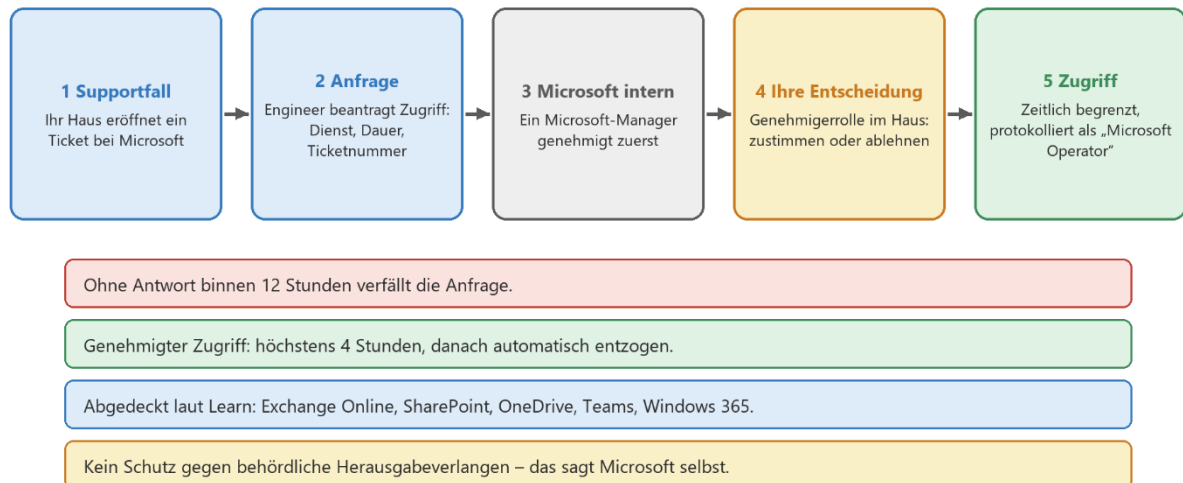
Customer Lockbox setzt auf diesen internen Prozess eine weitere Stufe: Wenn ein Microsoft-Engineer im Rahmen eines Supportfalls Zugriff auf Ihre Inhalte braucht, muss nach der internen Genehmigung auch Ihr Haus zustimmen. Laut Microsoft Learn gilt Folgendes:

- Abgedeckt sind Exchange Online, SharePoint, OneDrive, Teams und Windows 365; Interaktionen mit Microsoft 365 Copilot sind über Exchange Online erfasst.
- Genehmigen dürfen Personen mit der Rolle „Customer Lockbox access approver“ sowie globale Administratoren.
- Unbeantwortete Anfragen verfallen nach zwölf Stunden, ein genehmigter Zugriff ist auf höchstens vier Stunden begrenzt.

- Genehmigungen und Aktionen des Engineers werden im Überwachungsprotokoll erfasst, Letztere unter dem Benutzer „Microsoft Operator“.
- Customer Lockbox wird im Microsoft 365 Admin Center aktiviert und ist nicht von selbst eingeschaltet.

Customer Lockbox: Wer wann an Ihre Inhalte darf

Ablauf nach Microsoft Learn, vereinfacht – Stand der Dokumentation vor Einsatz prüfen



Customer Lockbox: Ohne Ihre Zustimmung kein Zugriff im Supportfall – mit Ablaufzeit und Protokoll.

Zur Lizenz: Nach der Dokumentation auf Microsoft Learn ist Customer Lockbox in Microsoft 365 E5 und Office 365 E5 enthalten und lässt sich anderen Plänen über Compliance-Add-ons hinzufügen. Lizenzmodelle ändern sich; prüfen Sie den aktuellen Stand in der Dokumentation zu [Customer Lockbox-Anforderungen auf Microsoft Learn](#) und in der Lizenzierungsübersicht für Sicherheit und Compliance, bevor Sie planen.

Was Customer Lockbox nicht leistet

Customer Lockbox regelt Zugriffe von Microsoft-Engineers im Supportfall. Es schützt nach Microsofts eigener Darstellung nicht vor Herausgabeverlangen von Behörden oder anderen Dritten. Es ersetzt weder die vertragliche Verschwiegenheitsverpflichtung noch die Frage, ob bestimmte Daten überhaupt in Microsoft 365 liegen sollten. Und es nützt nichts, wenn niemand im Haus die Benachrichtigungen liest: Legen Sie fest, wer genehmigt, wer vertritt – auch in der Rufbereitschaft am Wochenende – und nach welchen Kriterien.

Schlüsselverwaltung: Wer hält den Schlüssel?

Microsoft 365 verschlüsselt ruhende Daten standardmäßig, unter anderem mit BitLocker und dienstseitiger Verschlüsselung; die Schlüssel verwaltet Microsoft. Für Häuser, die mehr Kontrolle wollen, gibt es zwei weitere Stufen:

- **Customer Key:** Das Haus stellt eigene Stammschlüssel im Azure Key Vault bereit, mit denen Microsoft 365 Inhalte auf Anwendungsebene verschlüsselt – laut Learn für Exchange, SharePoint, OneDrive, Teams und weitere Arbeitslasten über Datenverschlüsselungsrichtlinien. Der Dienst nutzt die Schlüssel weiterhin, um Suche, eDiscovery oder Virenschutz zu ermöglichen. Der Gewinn liegt vor allem im Ausstieg: Werden

die Schlüssel widerrufen, führt das über den sogenannten Data Purge Path zur kryptografischen Löschung.

- **Double Key Encryption:** Ein Schlüssel bleibt beim Haus, der andere bei Microsoft. Ohne beide lassen sich geschützte Inhalte nicht öffnen – auch Microsoft kann sie nicht lesen. Der Preis: Dienste, die Inhalte verarbeiten müssen, sehen bei diesen Dokumenten nichts. Das eignet sich für wenige, gezielt ausgewählte Dokumente, nicht für den Alltag einer Station.

Schlüsselverwaltung: mehr Kontrolle, mehr Verantwortung

Je weiter rechts, desto mehr Kontrolle – und desto mehr kann im eigenen Haus schiefgehen



Mehr Kontrolle über die Schlüssel heißt auch: mehr Betrieb, mehr Notfallplanung, weniger Komfort.

Option	Kontrolle über Schlüssel	Auswirkung auf Funktionen	Für wen sinnvoll
Microsoft-verwaltet	Microsoft	Keine Einschränkung	Grundschatz für alle Inhalte
Customer Key	Haus stellt Stammschlüssel bereit, Dienst nutzt sie	Weitgehend keine Einschränkung, aber Betriebsaufwand für Key Vault und Notfallprozesse	Häuser mit hohem Kontrollanspruch und eigener Krypto-Kompetenz
Double Key Encryption	Ein Schlüssel ausschließlich im Haus	Inhalte für Suche, Vorschau und KI-Funktionen unsichtbar	Einzelne hochsensible Dokumente, nicht für die Fläche

Lizenzvoraussetzungen für Customer Key und Double Key Encryption sind an bestimmte Pläne bzw. Add-ons gebunden; prüfen Sie sie in der Purview-Dienstbeschreibung. Und eine nüchterne Anmerkung aus der Praxis: Wer die eigenen Schlüssel verwalten will, sollte vorher ehrlich prüfen, wie es um Schlüssel- und Zertifikatsverwaltung im eigenen Haus steht. Ein verlorener Schlüssel im Key Vault ist kein Datenschutzvorfall, sondern ein Verfügbarkeitsvorfall – und der fühlt sich im Krankenhaus nicht besser an. Mehr zu Verschlüsselung und Klassifizierung im Kompetenzbereich [Microsoft Purview](#).

Und die Excel-Liste mit Patientennamen?

Seien wir ehrlich: In vielen Häusern liegen in Teams und OneDrive Dinge, die dort nicht hingehören. Die Belegungsübersicht als Excel-Datei, das Foto vom Stationsboard im Chat, die OP-Planung als Anhang. Niemand hat das so beschlossen, es ist einfach passiert, meist aus guten Gründen wie Zeitdruck und einem KIS, das genau diese Ansicht nicht bietet. Das ist nicht der Normalfall, den man dokumentiert und absegt, sondern ein Befund, den man behandelt.

Warnung: Die gute Vertragslage heilt keine schlechte Ablage

Eine wirksame Verschwiegenheitsverpflichtung von Microsoft macht die Patientenliste im Teams-Kanal mit 300 Mitgliedern nicht zulässig. Das Problem ist dann nicht der Anbieter, sondern der Kreis der Personen im eigenen Haus, die Zugriff haben, ohne an der Behandlung beteiligt zu sein. Hier helfen Vertraulichkeitsbezeichnungen, Richtlinien zur Verhinderung von Datenverlust und vor allem klare Regeln, wofür Teams da ist.

Wie Teams im Krankenhaus sinnvoll für Gremien, Projekte und Kommissionen genutzt wird und wo es nichts zu suchen hat, beschreibt [Teams im Krankenhaus: Gremien, Projekte, Kommissionen und wo Teams nichts zu suchen hat](#). Besonders spürbar wird das Thema, sobald Copilot ins Spiel kommt – denn Copilot findet, was Berechtigungen hergeben. Dazu mehr in [Copilot im Krankenhaus: Oversharing, Patientenbezug und die Frage, wer ihn überhaupt bekommt](#).

Prüfliste für die Geschäftsführung

Prüfpunkt	Zuständig (Vorschlag)	Nachweis
Nutzung inventarisiert: Welche Dienste, welche Datenarten, wo Patientenbezug?	IT-Leitung mit Datenschutz	Verzeichnis der Verarbeitungstätigkeiten, Dienstliste
Auftragsverarbeitungsvertrag geprüft und abgelegt	Datenschutz, Einkauf	Vertragsakte, Prüfvermerk
Verschwiegenheitsverpflichtung nach § 203 StGB einbezogen, Kette geregelt	Justizariat	Zusatzvereinbarung, Prüfvermerk
Landesrecht je Standort geprüft, Anzeigepflichten erfüllt	Justizariat, Datenschutz	Stellungnahme je Land
Partnerzugriffe im Tenant geprüft, Systemhaus verpflichtet	IT-Leitung	Liste der Partnerbeziehungen, Verpflichtungserklärung
Customer Lockbox bewertet, Genehmiger und Vertretung benannt	IT-Leitung, ISB	Konfiguration, Verfahrensanweisung
Schlüsselverwaltung entschieden und begründet	ISB, IT-Leitung	Entscheidungsvorlage, Notfallkonzept
§ 393 SGB V geprüft, falls Gesundheitsdaten in der Cloud	ISB, Datenschutz	Testatprüfung, Kundenkriterien

Prüfpunkt	Zuständig (Vorschlag)	Nachweis
Belegschaft unterwiesen: Was gehört wohin?	Datenschutz, QM	Schulungsnachweise, Verfahrensanweisung

Wer diese Liste nicht allein abarbeiten möchte oder einen zweiten Blick auf Tenant, Partnerzugriffe und Schlüsselkonzept braucht, findet Unterstützung bei der [Microsoft 365 Beratung für Krankenhäuser](#). Für die technische Absicherung rund um Identitäten und Zugriffe lohnt der Blick in den Kompetenzbereich [Microsoft 365 Security](#).

Häufige Fragen

Ist Microsoft nach § 203 StGB eine mitwirkende Person?

Ein Cloud-Anbieter, der für das Krankenhaus Dienste betreibt, kommt als sonstige mitwirkende Person nach § 203 Abs. 3 StGB in Betracht. Voraussetzung ist, dass die Einbindung für dessen Tätigkeit erforderlich ist und das Haus für die Verpflichtung zur Geheimhaltung sorgt. Die Einordnung im Einzelfall gehört in die Rechtsberatung.

Reicht der Auftragsverarbeitungsvertrag für die Schweigepflicht?

Nein. Der Auftragsverarbeitungsvertrag nach Art. 28 DSGVO beantwortet die Datenschutzfrage. Die Verpflichtung zur Geheimhaltung nach § 203 Abs. 4 StGB ist eine eigene Anforderung, die ausdrücklich vereinbart werden sollte – idealerweise mit Bezug auf das Strafrecht und mit Regelung für Unterauftragnehmer.

Wer im Krankenhaus muss für die Verpflichtung sorgen?

Rechtlich trifft die Sorgepflicht den Berufsgeheimnisträger. Praktisch schließt der Träger die Verträge. Er sollte deshalb so organisieren, dass die Verpflichtung für alle Ärzte und Pflegekräfte im Haus wirkt, und das dokumentieren.

Brauchen wir Customer Lockbox?

Customer Lockbox gibt Ihrem Haus die Entscheidung über Supportzugriffe auf Inhalte zurück und protokolliert sie. Für Häuser, die Inhalte mit Bezug zur Schweigepflicht in Microsoft 365 verarbeiten, ist es ein starkes Argument in der Risikoabwägung. Die Lizenzvoraussetzungen prüfen Sie vorab auf Microsoft Learn.

Schützt Customer Key vor dem Zugriff durch Microsoft?

Nur eingeschränkt. Der Dienst nutzt die Schlüssel im laufenden Betrieb, damit Funktionen wie Suche weiterarbeiten. Der Hauptnutzen liegt in der Kontrolle über die Schlüssel und im kryptografischen Löschen beim Ausstieg. Wer Inhalte vor dem Anbieter verbergen will, braucht Double Key Encryption – mit allen funktionalen Einschränkungen.

Gilt das Landeskrankenhausgesetz auch für Verwaltungsdaten?

Die Regeln der Landeskrankenhausgesetze zielen auf Patientendaten. Reine Verwaltungsunterlagen ohne Patientenbezug fallen in der Regel nicht darunter, wohl aber unter das allgemeine Datenschutzrecht. Die Grenze ist im Alltag allerdings schmaler, als viele denken – ein Beschwerdebrief ist schnell ein Patientendatum.

Was ändert sich für kirchliche Krankenhäuser?

Statt der DSGVO gelten KDG oder DSG-EKD mit eigener Aufsicht. Die Schweigepflicht nach § 203 StGB und die Pflichten aus dem SGB V gelten unverändert. Ob und wie Landeskrankenhausgesetze auf kirchliche Häuser anwendbar sind, ist je Land zu prüfen.

Dürfen Arztbriefe per Exchange Online verschickt werden?

Das hängt von Vertragslage, Landesrecht, Schutzmaßnahmen und Empfänger ab. Für den Austausch mit anderen Leistungserbringern gibt es im Gesundheitswesen eigene, dafür vorgesehene Kommunikationswege. Klären Sie die Frage mit Datenschutz und Justizariat, bevor sich ein Gewohnheitsrecht bildet.

Fazit: Die Schweigepflicht verbietet die Cloud nicht – sie verlangt Ordnung

§ 203 StGB steht Microsoft 365 im Krankenhaus nicht grundsätzlich im Weg. Seit der Neuregelung dürfen Berufsgeheimnisträger Dienstleister einbinden, soweit das erforderlich ist und diese wirksam zur Geheimhaltung verpflichtet sind. Daneben stehen, unabhängig davon, die Auftragsverarbeitung nach DSGVO, KDG oder DSG-EKD, das Landeskrankenhausgesetz Ihres Standorts und für Gesundheitsdaten in der Cloud § 393 SGB V. Wer eines dieser Schlösser übersieht, steht vor einer verschlossenen Tür – egal, wie gut die anderen beiden geölt sind.

Technisch hat Microsoft 365 einiges zu bieten, um die Zugriffswege des Anbieters zu begrenzen und nachzuweisen: Customer Lockbox für Supportzugriffe, Customer Key und Double Key Encryption für die Schlüsselfrage. Das wirksamste Mittel bleibt aber organisatorisch: Patientendaten gehören ins KIS. Wer das durchhält, verwandelt die Schweigepflicht-Debatte im Lenkungskreis von einem Projektstopper in einen Tagesordnungspunkt. Und die Hand, die sich bei „Und was ist mit § 203?“ hebt, bekommt endlich eine Antwort, die länger hält als bis zur nächsten Sitzung.

Weiterlesen

- › [Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt](#)
- › [§ 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen](#)
- › [Microsoft 365 im kirchlichen Krankenhaus: KDG, DSG-EKD und die MAV am Tisch](#)
- › [Microsoft 365 Beratung für Krankenhäuser](#)