

Whitepaper

Der Einsatz von Cloud-Diensten im Notariat

In Zusammenarbeit mit



LawX

Erbvertrag Scholz / 2023

21.04.2023

Sonderfall: Enterbung bei Auslandserbfolge
Notarvermerk mit Literaturhinweis

 Entwurf öffnen  Vermerk anzeigen

 3 Fälle gefunden

Vorgang  85%
Grundstückskaufvertrag

- 1  Abschrift versendet ...
- 2  Kostenberechnung erstellt ...
- 3  Eintrag in UVZ ...
- 4  Kaufpreiseingang bestätigt ...

 Grundschriftbestellung prüfen



Kapitel 1

Einleitung

LawX

Cloud-Dienste werden heute in nahezu allen Bereichen juristischer Tätigkeit eingesetzt, insbesondere in Anwalts- und Steuerkanzleien. Sie bilden längst den Standard für professionelle Bürokommunikation.

Für die Anwaltschaft hat der Deutsche Anwaltsverein in seinem jüngst veröffentlichten KI-Leitfaden klargestellt, dass die Nutzung von Cloud-Diensten unter Einhaltung bestimmter Vorgaben zulässig ist (Quelle: DAV, Stellungnahme 32/25, Juli 2025, insb. S. 5, 9 ff). Aus datenschutzrechtlicher Sicht sei vor allem die Implementierung adäquater technischer und organisatorischer Maßnahmen (sog. TOMs) maßgeblich, wie etwa die Verschlüsselung von Daten, differenzierte Zugriffskontrollen oder eine lückenlose Protokollierung. Aus berufsrechtlicher Sicht sei entscheidend, dass sich die Dienstleister zur besonderen Verschwiegenheit gemäß § 43e BRAO verpflichten (DAV, Stellungnahme 32/25, S. 9 ff., 14. Eine entsprechende Verschwiegenheitsverpflichtung für den notariellen Berufsstand findet sich in § 26a BNotO).

Für den notariellen Berufsstand hat die Bundesnotarkammer (BNotK) in ihrem aktuellen Rundschreiben (Nr. 1/2026) ebenfalls ausgeführt, dass die Cloud-Nutzung unter Beachtung des Datenschutzes und der Einhaltung berufsrechtlicher Vorgaben zulässig sei. So können auch zentrale Notarsoftwarelösungen in der Cloud betrieben werden, solange die (elektronische) Nebenakte regelmäßig (mindestens wöchentlich) in der Geschäftsstelle gespeichert wird und ein belastbarer Notfallplan für Cloud-Ausfälle vorhanden ist.

Für die Zukunftsfähigkeit des Notariats ist die berufsrechtliche Bewertung cloudbasierter IT-Infrastrukturen gleichermaßen zentral. In diesem Whitepaper zeigen wir auf, welche Gestaltungsmöglichkeiten der gegenwärtige rechtliche Rahmen bietet, wo die berufsrechtlichen Grenzen für deren Einsatz im Notariat verlaufen und wie Cloud Technologie die Arbeit im Büro nicht nur effizienter, sondern vor allem sicherer machen kann. Der Fokus liegt hierbei auf der für die Praxis besonders relevanten Führung der Nebenakten (§ 2 Nr. 5 NotAktVV), die derzeit in vielen Notariaten noch überwiegend papierbasiert erfolgt. Gerade hier bieten digitale Lösungen erhebliche und nachhaltige Effizienzgewinne: Prozesse werden beschleunigt, manuelle Doppelarbeit entfällt und Kosten sinken – etwa durch den Wegfall von Druck- und Papieraufwand. Gleichzeitig hebt sich die Datensicherheit auf ein neues Niveau.



Kapitel 2

Berufsrechtliche Einordnung

LawX

Die berufsrechtlichen Vorgaben für die Nutzung von Cloud-Diensten im Notariat sind vor allem in § 35 BNotO enthalten:

Gemäß § 35 Abs. 1 Satz 2 BNotO kann der Notar Akten und Verzeichnisse in Papierform oder elektronisch führen, soweit die Form nicht durch oder auf Grund eines Gesetzes vorgeschrieben ist. Zusätzlich darf er für die Aktenführung Hilfsmittel verwenden, deren Vertraulichkeit ebenfalls zu gewährleisten ist.

Eine gesetzliche Einschränkung für die elektronische Aktenführung regelt sodann § 35 Abs. 4 BNotO. Danach darf der Notar elektronische Akten und Verzeichnisse außerhalb der Geschäftsstelle nur im Elektronischen Urkundenarchiv oder im Elektronischen Notariatsaktenspeicher führen.

Vor diesem Hintergrund sind beim Cloud-Einsatz im Notariat zwei Bereiche zu unterscheiden:

1. Zulässigkeit der Nutzung cloudbasierter Hilfsmittel für die Aktenführung

Cloudbasierte Anwendungen können im notariellen Umfeld als Hilfsmittel im Sinne des § 35 Abs. 2 Satz 2 BNotO eingesetzt werden, z. B. zur Entwurfserstellung, Beteiligtenverwaltung oder digitalen Geschäftsstellenorganisation.

Eine solche Nutzung steht auch im Einklang mit den Vorgaben aus dem BNotK-Rundschreiben Nr.04/2021 und wird durch das jüngste BNotK -Rundschreiben Nr.1/2026 („Cloud-Nutzung im Notariat“ vom 2. Februar 2026) ausdrücklich klargestellt. Danach ist die Nutzung von Cloud-Diensten als „Hilfsmittel“ im Sinne des § 35 Abs. 2 Satz 2 BNotO zulässig, sofern Akten und Verzeichnisse weiterhin in der Geschäftsstelle geführt werden sowie die datenschutzrechtlichen und berufsrechtlichen Vorgaben, insbesondere zur berufsrechtlichen Verschwiegenheit, gewahrt sind. Der Cloud-Dienst selbst bzw. die dem Cloud-Dienst zugrunde liegende Software eines Software as a service-Anbieters (SaaS), wie z.B. von LawX, ist in diesen Fällen das Hilfsmittel.

Hilfsmittel dienen nicht der formalen Aktenführung, sondern ausschließlich vorbereitenden oder unterstützenden Tätigkeiten. Die insofern reduzierte Bedeutung des Hilfsmittels bei der Führung notarieller Akten und Verzeichnisse ist unter Verhältnismäßigkeitsgesichtspunkten besonders zu berücksichtigen. Zulässig ist der Einsatz von cloudbasierten Hilfsmitteln daher bereits heute unter folgenden Voraussetzungen:

- Die originäre Akte bzw. das originäre Verzeichnis wird im Fall der elektronischen Führung final in der Geschäftsstelle gespeichert (§ 35 Abs.4 BNotO).
- Datenschutz- und berufsrechtliche Anforderungen, insbesondere Abschluss eines Vertrags über Auftragsverarbeitung gemäß Art. 28 DS-GVO sowie einer besonderen berufsrechtlichen Verschwiegenheitsverpflichtung gemäß § 26a BNotO, sind technisch und vertraglich erfüllt.

- Der Zugriff auf den Cloud-Dienst ist ausschließlich dem Notar bzw. seinen Mitarbeitenden vorbehalten.

Die Einhaltung dieser Vorgaben lässt sich auch beim Einsatz von Microsoft grundsätzlich sicherstellen – einem der führenden Anbieter von Cloud-Diensten. Zu den bekanntesten Lösungen zählen Microsoft 365 (M365) und die Plattform Microsoft Azure. Beide werden bereits in der notariellen Praxis genutzt. Sie erfüllen die datenschutz- und berufsrechtlichen Anforderungen des juristischen Berufsstands – einschließlich des Notariats –, sofern Microsoft die besondere Verschwiegenheitsverpflichtung nach § 26a BNotO vertraglich übernimmt und die Softwareanwendung entsprechend der berufsrechtlichen Anforderungen konfiguriert wird.

Das BNotK-Rundschreiben Nr. 1/2026 nimmt wie folgt ausdrücklich zum Einsatz von M365 Stellung: Microsoft 365 kann – je nach Konfiguration – aus Sicht der BNotK nach aktuellem Stand in Konformität zu den berufsrechtlichen Anforderungen verwendet werden, soweit mit Microsoft die „Zusatzvereinbarung für Berufsgeheimnisträger“ abgeschlossen wird. Da sich die Inhalte der Zusatzvereinbarung ändern können, bleibt eine Einzelfallprüfung der Bedingungen auf Vereinbarkeit mit dem Berufsrecht unentbehrlich. Für die datenschutzrechtliche Bewertung von Cloud-Dienstleistern sind unter anderem zwei grundlegende Faktoren maßgeblich: der physische Serverstandort und der Sitz des Mutterunternehmens. Beide können rechtliche Risiken begründen, etwa im Hinblick auf Zugriffsrechte staatlicher Stellen oder die Anwendbarkeit ausländischen Rechts. Dies gilt insbesondere, soweit das Angebot eines US-Anbieters genutzt werden soll. Die Cloud-Dienstleistungen US-amerikanischer Anbieter können nach Ansicht der BNotK nach aktuellem Stand zwar datenschutzrechtlich zulässig genutzt werden, jedoch gibt es Unwägbarkeiten.

Microsoft als ein führender und sicherer Cloud-Dienstanbieter

M365

M365 ist das führende Software- und Servicepaket für Endnutzer, das vor allem Office-Anwendungen (Word, Excel, PowerPoint, Outlook, Teams) sowie Dienste wie OneDrive und Exchange Online umfasst. M365 wird in nahezu allen Industrien, darunter auch streng regulierte Industrien, eingesetzt. Etablierte Softwareanbieter wie DATEV oder RA Micro begleiten Kanzleien bereits heute bei der Einführung und dem Betrieb von M365. Auch in zahlreichen Notariaten befindet sich M365 bereits im Einsatz.

M365 unterzeichnet mit seinen Vertragspartnern in der Rechtsbranche (Kanzleien, Notariate und Legal Tech-Anbieter) regelmäßig besondere Verschwiegenheitsvereinbarungen entsprechend den berufsrechtlichen Vorgaben der § 43e BRAO bzw. § 26a BNotO. Hinsichtlich der Datensicherheit (Quelle: Microsoft, Hornet Security, Microsoft) erfüllt M365 als Teil der Microsoft-Gruppe ebenfalls die Anforderungen an angemessene TOMs auf höchstem Niveau:

- Datenverarbeitung in zertifizierten deutschen Rechenzentren (Frankfurt/Berlin) – mandantenbasiert konfigurierbar.
- Zertifizierungen nach ISO 27001, ISO 27018, SOC 1-3 und BSI C5 – letztere vom Bundesamt für Sicherheit in der Informationstechnik speziell für Cloudinfrastrukturen mit hoheitlichem Schutzbedarf entwickelt.
- Ende-zu-Ende-Verschlüsselung („at rest“ und „in transit“) und gestufte Schlüsselverwaltung, sodass selbst Microsoft keinen unmittelbaren Datenzugriff hat.
- Rollenbasierte Zugriffskontrolle (RBAC), vollständige Protokollierung und Multi-Faktor-Authentifizierung (MFA) gewährleisten umfassende Zugriffssicherheit.
- AV-Vertrag mit Microsoft Germany standardmäßig verfügbar.

M365 läuft in der Regel in der Azure-Cloud und speichert Daten ihrer Kunden mit Sitz in Deutschland standardmäßig in Microsoft-Rechenzentren in Deutschland (Quelle: Microsoft). Über Integrationen und Konnektoren (z. B. für Drittanbieter-Storage, ERP-Systeme, Fileserver) kann M365 aber auch mit Daten arbeiten, die in anderen deutschen Rechenzentren, d.h. außerhalb von Azure, gespeichert sind.

Azure-Cloud

Azure ist eine modulare Cloud-Plattform mit zertifizierten Rechenzentren in Deutschland, die hochverfügbare Rechen-, Speicher- und Sicherheitsdienste für verschiedenste Anwendungen – einschließlich, aber nicht beschränkt auf M365 – bereitstellt. Azure gilt als eine der weltweit führenden Infrastrukturen für Cloud Computing und kommuniziert aktiv, dass ihre Cloud-Dienste in Deutschland das C5-Testat erfüllen bzw. entsprechende Prüfberichte vorliegen, die die Einhaltung der C5-Kriterien nachweisen (Quelle: Microsoft). Microsoft stellt auf seiner offiziellen Seite dar, dass Azure, Azure Government und Azure Deutschland einen kombinierten Prüfbericht (C5, SOC 2 Typ 2, CSA STAR-Bescheinigung) von unabhängigen Prüfern unterhält, welcher die Erfüllung der Anforderungen des C5-Standards bestätigt. Damit erfüllt Azure die Anforderungen aus § 393 SGB V für Cloud-Dienste im Gesundheitswesen. Microsoft betont auch, dass die Compliance mit C5 als Grundlage für Kundenprogramme oder eigene Bescheinigungen genutzt werden kann.

2. Originäre Führung der elektronischen Nebenakte in der Cloud

Im Unterschied zum zulässigen Einsatz von cloudbasierten Hilfsmitteln legt § 35 Abs. 4 BNotO in seiner derzeitigen Fassung dem Berufsstand faktisch die Pflicht auf, die elektronisch geführte Nebenakte in der Geschäftsstelle zu speichern: Das elektronische Urkundenarchiv steht hierfür nicht zur Verfügung, der Elektronische Notariatsaktenspeicher wurde bis dato nicht eingerichtet. Eine ausschließliche Speicherung elektronisch geführter Akten und Verzeichnisse in der Cloud ist damit derzeit nicht zulässig.

a. Generelle Öffnung für eine sichere Cloud erfordert eine Novelle des § 35 Abs. 4 BNotO

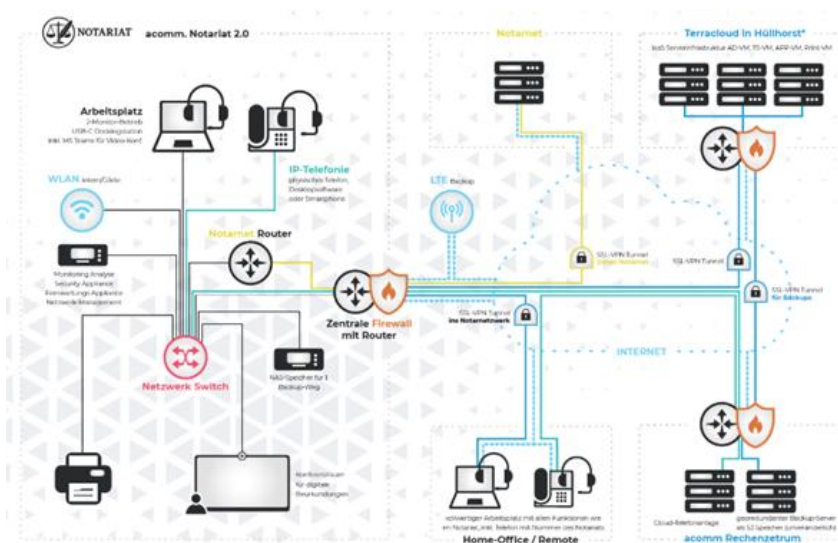
Nach Maßgabe heutiger IT-Sicherheitsstandards erscheint eine Öffnung – etwa durch eine Novelle des § 35 Abs. 4 BNotO oder durch die Einführung des Elektronischen Notariatsaktenspeichers – naheliegend. In bisherigen On-Premise-Setups (Serverstandort in der Geschäftsstelle) führen fehlende Standards bei Systemarchitektur und Administration, bedingt durch unterschiedliche IT-Dienstleister, oftmals zu Sicherheitslücken und einer ausgeprägten Systemheterogenität. Besonders betroffen sind Verfügbarkeit und Datensicherheit (vgl. Kapitel B).

b. Hybride Infrastruktur mit lokaler Sicherungskopie bereits heute möglich

In der Praxis existieren bereits erprobte Infrastrukturen, bei denen ausgewählte Komponenten in die Cloud ausgelagert werden. Entscheidend ist dabei aus regulatorischer Sicht, dass die Nebenakte abschließend in der Geschäftsstelle gespeichert wird – unabhängig davon, wo sie zwischenzeitlich verarbeitet oder zwischengespeichert wird. Hybride Infrastrukturen, die eine Cloudverarbeitung mit lokaler Sicherung kombinieren, erfüllen diese Voraussetzungen und werden heute bereits in Notariaten eingesetzt, insbesondere in Bayern.

Die Notariatssoftware wird dabei zentral über einen Cloud-Terminalserver oder VDI und daran angeschlossene Rechenzentren in Deutschland bereitgestellt. Mitarbeitende greifen über ihre lokalen Endgeräte auf diese Umgebung zu und arbeiten in einer gewohnten Windows-Oberfläche. Vor Ort im Büro sind keine klassischen Serverstrukturen erforderlich, was Ausfallsicherheit, Wartungsfreundlichkeit und IT-Sicherheit deutlich erhöht. Ergänzend erfolgt eine tägliche lokale Datensicherung (z. B. über NAS-Systeme in der Geschäftsstelle).

Ein Best-Practice-Beispiel ist der IT-Dienstleister acomm für Notariate aus Bayern und Baden-Württemberg, der vom Notarverein in Bayern empfohlen wird. In einem Schaubild wird das IT-Setup von mittlerweile über 26 Notariaten in Bayern (Stand: Januar 2026) dargestellt. Dieses Modell gilt heute als Referenz für eine moderne Notar-IT-Infrastruktur: Verfügbarkeit, Kosteneffizienz und IT-Sicherheit stehen im Zentrum des Designs. Durch die sukzessive Verlagerung zahlreicher Hardware-Komponenten und Services in das Rechenzentrum konnte die Anzahl möglicher Ausfallquellen im Notariat deutlich reduziert werden. Ergänzende Redundanzen in der verbleibenden lokalen Hardware erhöhen die Betriebssicherheit zusätzlich. Damit ist der Bedarf an kurzfristigen Vor-Ort-Einsätzen nahezu vollständig entfallen – Hardware-Ausfälle im Notariat selbst sind zur Ausnahme geworden.



Dieses Setup ermöglicht bereits heute moderne, skalierbare Arbeitsprozesse bei gleichzeitiger Wahrung der berufsrechtlichen Anforderungen.



Kapitel 3

Strukturelle Defizite von
On-Premise-Systemen,
die durch eine hybride
Infrastruktur überwunden
werden können

LawX

On-Premise-Systeme, bei denen sich sämtliche Hardware-Komponenten einschließlich der Server ausschließlich in der Geschäftsstelle befinden, sind in vielen Notariaten noch immer Standard. Ein solches Setup ist jedoch technisch überholt, organisatorisch schwerfällig und sicherheitstechnisch anfällig. Wartung und Betrieb hängen häufig von einzelnen IT-Dienstleistern ab, die jeweils unterschiedliche Standards setzen. Eine zentrale Überwachung fehlt, Sicherheitsupdates werden oft verzögert eingespielt, und bereits ein einzelner Hardwaredefekt kann den Betrieb vollständig lahmlegen. Hinzu kommen physische Risiken: ungesicherte Serverräume, unzureichende Klimatisierung und fehlende Alarmanlagen. Diese strukturellen Schwächen beeinträchtigen unmittelbar die Arbeitsfähigkeit und gefährden die Sicherheit sensibler Daten.

1. Verfügbarkeit – wenn der Alltag stillsteht

Ein einzelner Hardware-Defekt kann dazu führen, dass die gesamte Geschäftsstelle für Stunden oder gar Tage arbeitsunfähig wird. Das folgende Beispiel zeigt, wie schnell ein einzelner Defekt den gesamten Büroalltag zum Stillstand bringen kann:

Es ist ein Mittwochmorgen um 7:30 Uhr. Die Mitarbeiter eines Notariats wollen den Arbeitstag beginnen – doch statt der gewohnten Startmaske ihres Notar-Programms sehen sie nur einen schwarzen Bildschirm. Das System reagiert nicht. Kein Zugriff auf Urkundenentwürfe, keine E-Mails, kein Zugriff auf das Register – Stillstand. Da kein Monitoring-System existiert, wird der Ausfall erst in diesem Moment bemerkt – Stunden nach dem eigentlichen Eintritt des Fehlers.

Der zuständige IT-Dienstleister, ein Einzelunternehmer, ist telefonisch sofort erreichbar und versucht binnen 45 Minuten per Fernwartung zu helfen. Doch schnell stellt sich heraus: Der Server ist nicht mehr lauffähig, eine Remote-Wiederherstellung unmöglich. Erst drei Stunden später trifft der IT-Dienstleister vor Ort ein. Reparaturversuche scheitern – der Verdacht fällt auf einen gravierenden Hardware-Defekt am Mainboard.

Noch am selben Tag beginnt die Suche nach Ersatzhardware, die sich schwierig gestaltet. Mit etwas Glück kann ein passender Server am kommenden Vormittag bestellt werden, Expresslieferung inklusive. Gegen Mittag des Folgetags (Tag 3) trifft die Hardware ein. Nun beginnt die eigentliche Wiederherstellung: Das Aufsetzen des Systems und die Rücksicherung der virtuellen Maschinen nimmt weitere vier bis fünf Stunden in Anspruch. Ohne zusätzliche Herausforderungen können nach der Rücksicherung alle Arbeitsplätze wieder in Betrieb gehen.

Nach insgesamt rund 90 Stunden – fast vier volle Arbeitstage – ist das Notariat wieder arbeitsfähig. In diesem Szenario beschleunigte die schnelle Verfügbarkeit der Hardware den Prozess erheblich – was sehr oft nicht der Fall ist. Dennoch bedeutet ein solcher Ausfall nicht nur Stillstand, sondern auch den Verlust wertvoller Arbeitszeit, Fristenstress und erheblichen organisatorischen Mehraufwand.

In einer reinen On-Premise-Umgebung hängt die Arbeitsfähigkeit vollständig von lokaler Hardware ab. Fehlende Geo-Redundanz und ein nicht vorhandenes 24/7-Monitoring bedeuten, dass ein einzelner Defekt die gesamte Geschäftsstelle lahmlegen kann. Die Implementierung einer hybriden Infrastruktur mit lokaler Sicherungskopie kann hier Abhilfe schaffen: Die Verarbeitung erfolgt in der Cloud mit automatisierten Sicherheitsupdates und permanenter Überwachung, die finale Speicherung bleibt in der Geschäftsstelle. So bleibt die Geschäftsstelle auch bei Störungen arbeitsfähig.

2. Datenschutz und Datensicherheit – wenn die Speicherung in der Cloud überlegener ist

On-Premise-Systeme zeigen in der Praxis zudem einige Defizite bei der Datensicherheit und dem Datenschutz.

In kürzlich durchgeführten Audits eines erfahrenen IT-Anbieters wurden im Frühjahr 2025 in 19 von 22 Notariaten festgestellt, dass die Systemarchitektur datenschutzrechtliche Anforderungen nicht ausreichend erfüllt. Häufige Probleme sind insbesondere, dass Amtsräume in älteren Gebäuden nur selten die baulichen und technischen Maßnahmen erfüllen, die den Schutz personenbezogener Daten gemäß DS-GVO sicherstellen sollen (insb. Schutz vor Umwelteinflüssen oder fehlende Alarmanlagen), Server oft nicht vor physischen Zugriffen hinreichend geschützt waren und aufgrund der noch immer führenden Papierakte sensible Dokumente teilweise offen im Büro ausliegen.

Diese datenschutzrechtlichen und sicherheitstechnischen Defizite des On-Premise Setups lassen sich ebenfalls durch Cloud-Rechenzentren beheben. Letztere bieten durch eine höhere Standardisierung von Infrastruktur und Prozessen in der Regel ein deutlich höheres Sicherheitsniveau:

On-Premise

Meist Sicherheitsupdates manuell
Meist kein aktives Monitoring
Redundanz kostenintensiv
Single Tenant, häufig ungewartet
Geringer Schutz des Gebäudes / Serverraums
vor Umwelteinflüssen und Fremdzugriff

Cloud-Rechenzentrum

Echtzeit-Updates globaler Sicherheitslage
24/7 Threat Detection (Defender for Cloud)
Native Geo-Redundanz (z. B. Frankfurt <> Berlin)
Multi-Tenant mit garantierten Isolationsschichten
Sehr hohes Schutzniveau der Rechenzentren
vor Umwelteinflüssen und Fremdzugriff



Kapitel 4

Zusammenfassung und Ausblick

LawX

Die in diesem Whitepaper dargestellten Defizite klassischer On-Premise-Systeme – eingeschränkte Verfügbarkeit, hohe Ausfallrisiken, fehlendes Monitoring und bauliche Defizite – machen deutlich, wie groß der Handlungsdruck ist. Die Diskussion um den Einsatz von Cloud-Diensten im Notariat zeigt, dass moderne Technologien längst praxistauglich sind, sofern sie im Einklang mit den geltenden berufsrechtlichen Rahmenbedingungen genutzt werden. Der Einsatz cloudbasierter Hilfsmittel ist heute zulässig und auch hybride Infrastrukturen sind bereits erprobt.

LawX lässt sich als cloudbasiertes Hilfsmittel nahtlos in bestehende Microsoft-Umgebungen integrieren und funktioniert unabhängig von einer bestimmten Server- oder Hybrid-Infrastruktur. Damit können Notariate schon heute rechtssicher auf moderne, intuitive und workflow-optimierte, KI-gestützte Arbeitsweisen setzen. LawX bleibt dabei konsequent innerhalb des berufsrechtlichen Rahmens und macht digitale Arbeitsprozesse effizienter und sicherer – automatisiert wie nie, sicher wie immer.

acomm implementiert eine erprobte hybride Infrastruktur, bei der ausgewählte Systemkomponenten aus der Geschäftsstelle in einem zertifizierten Rechenzentrum betrieben werden. Dadurch wird die lokale Umgebung schlanker, Monitoring und Ausfallsicherheit werden erheblich verbessert und die Datensicherheit erreicht ein Niveau, das in vielen Geschäftsstellen praktisch nicht zu realisieren ist. Die Cloud verarbeitet, die lokale Sicherung bleibt in der Geschäftsstelle.

Das Notariat muss nicht auf regulatorische Änderungen warten: Wer die bestehenden Spielräume nutzt, kann sofort die Verfügbarkeit und Sicherheit erhöhen und zugleich den Grundstein für eine nachhaltige digitale Berufspraxis legen. Hybride Setups schaffen dabei eine klare Übergangslösung und bereiten die Geschäftsstelle darauf vor, künftige digitale Entwicklungen schnell und reibungslos umzusetzen. Für Notarinnen und Notare sowie ihre Mitarbeitenden bedeutet das: weniger Ausfallzeiten, weniger Papierprozesse und ein deutlich vereinfachter Arbeitsalltag. Automatisierung wirkt damit nicht nur in der IT, sondern unmittelbar in der täglichen Praxis. So sind Notariate nicht nur heute besser aufgestellt, sondern legen zugleich die Grundlage für eine zukunftsfähige, moderne Berufspraxis. Gerade in Zeiten knapper Personalressourcen gewinnen diese Effizienzgewinne zusätzlich an Bedeutung.



LawX

Über LawX

LawX ist das Betriebssystem der nächsten Generation für Notariate sowie kleine und mittelständische Kanzleien. Von der CD-ROM-Ära ins KI-Zeitalter – LawX macht Abläufe effizienter, intelligenter und einfacher. Mit KI-gestützten Workflows automatisiert LawX Routinen, reduziert Fehler und entlastet Teams spürbar. Gemeinsam mit Notarinnen, Notaren und ihren Mitarbeitenden entwickelt, ist die Lösung sofort produktiv und intuitiv zu bedienen. Sie erfüllt die hohen Anforderungen an Datenschutz, Datensicherheit und berufsrechtliche Vorgaben. So entsteht ein modernes Betriebssystem, das Effizienz und Praxisnähe verbindet und den Arbeitsalltag nachhaltig verbessert.

Dr. Norman Koschmieder
Geschäftsführer

Kontakt

Email: info@lawx.de
Website: www.lawx.de

Anschrift

LawX GmbH
% Mindspace
Hausvogteiplatz 12
10117 Berlin
Deutschland

Weitere Informationen auf
unsere Website
www.lawx.de