Bundesnotarkammer | Anton-Wilhelm-Amo-Straße 34 | 10117 Berlin

An alle Notarkammern

GESCHÄFTSFÜHRUNG

Nachrichtlich an:
das Präsidium der Bundesnotarkammer
die Notarkasse
die Ländernotarkasse
das Deutsche Notarinstitut

Rundschreiben Nr. 1/2026
Cloud-Nutzung im Notariat

2. Februar 2026
Unser Zeichen: 151/2

Dr. Milan Bayram

Bundesnotarkammer K.d.ö.R.
Anton-Wilhelm-Amo-Straße 34
10117 Berlin

T. +49 30 383866-0
F. +49 30 383866-66
E. bnotk@bnotk.de

www.bnotk.de

Sehr geehrte Damen und Herren Kolleginnen und Kollegen,

bereits mit dem Rundschreiben Nr. 04/2021 haben wir darüber informiert, unter welchen Voraussetzungen eine Cloud-Nutzung im Notariat nach Ansicht der Bundesnotarkammer zulässig ist.

Inzwischen erreichen die Geschäftsstelle der Bundesnotarkammer wieder vermehrt Anfragen zur Zulässigkeit und den Grenzen einer Cloud-Nutzung im Notariat. Dieses Rundschreiben dient insbesondere der Klarstellung hinsichtlich der Nutzung von Cloud-Diensten im Notariat und soll darüber hinaus als Orientierungshilfe sowie zur Konkretisierung weiterführender Fragestellungen beitragen.

Unter „Cloud“ (abgeleitet von „Cloud Computing“) werden hier durch Cloud-Anbieter über das Internet zur Verfügung gestellte IT-Ressourcen wie z. B. Rechenleistung, Anwendungen oder Speicher, die meist durch ein vernetztes System aus Rechenzentren angeboten werden, verstanden.[1] Im Gegensatz zu klassischen On-Premise-Modellen, bei denen Nutzerinnen und Nutzer diese Ressourcen z. B. in Form von Festplatten, Computern oder Software erwerben und regelmäßig selbst intern installieren und betreiben,[2] verlassen die zu verarbeitenden Daten beim Cloud Computing die im Büro befindliche IT-Infrastruktur der Nutzerinnen und Nutzer und werden in die Infrastruktur der Cloud-Anbieter übertragen und ggf. auch dort gespeichert.[3]

[1] „Cloud Computing Grundlagen“, BSI, abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html.
[2] „Nutzung von cloudbasierten Dienstleistungen in Kritischen Infrastrukturen – eine Hilfestellung des UP KRITIS“, BSI, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-cloudbasierte-dienstleistungen.pdf?__blob=publicationFile&v=12.
[3] „Cloud Computing Grundlagen“, BSI, abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html.

Durch die Nutzung von Clouds können IT-Ressourcen – abhängig von der konkreten Systemarchitektur – flexibel, skalierbar und effizient bereitgestellt und Investitionskosten in laufende Kosten überführt werden.[4] Das bedeutet, dass der Umfang der Dienstleistungen auf den aktuellen Nutzerbedarf ausgerichtet und durch den hohen Grad an Automatisierung und Standardisierung einer großen Anzahl von Nutzerinnen und Nutzern gleichzeitig angeboten werden kann.[5]

Zusammengefasst steht das notarielle Berufsrecht, insbesondere § 35 Abs. 4 BNotO, einer Cloud-Nutzung nicht grundsätzlich entgegen. Zwar müssen elektronische Akten und Verzeichnisse in der Geschäftsstelle bzw. den Systemen der Bundesnotarkammer gespeichert sein, damit deren Verfügbarkeit auch für nachfolgende Verwahrstellen sichergestellt ist. Andere – u. U. auch inhaltsgleiche – Speicherungen (zur konkreten Ausgestaltung siehe A.) unterliegen jedoch als Hilfsmittel im Sinne des § 35 Abs. 2 Satz 2 BNotO nicht den spezifischen Einschränkungen des § 35 Abs. 4 BNotO. Für Hilfsmittel kommt eine Cloud-Nutzung daher in Frage, sofern der Datenschutz und die Verschwiegenheit gewahrt sind (s. dazu B.).

Die Auswahl des jeweiligen Cloud-Anbieters liegt in der Verantwortung der jeweiligen Notarin bzw. des jeweiligen Notars. Angesichts der zentralen Bedeutung von Cloud-Technologien für die Datensouveränität, die Sicherheit sowie die wirtschaftliche und technologische Unabhängigkeit Europas ist bei der Auswahl von Cloud-Lösungen eine systematische und regelmäßig wiederkehrende Prüfung europäischer Angebote vorzunehmen. Dabei ist fortlaufend zu bewerten, ob europäische Cloud-Lösungen in Bezug auf Leistungsfähigkeit, Sicherheit, Verfügbarkeit und Wirtschaftlichkeit den jeweiligen Anforderungen entsprechen. Sofern dies der Fall ist, sollten sie – insbesondere in sensiblen Anwendungsbereichen – gegenüber außereuropäischen Angeboten bevorzugt berücksichtigt werden.

A. Berufsrechtliche Vorgaben zum Speicherort

Entscheidend ist aus berufsrechtlicher Sicht die Unterscheidung zwischen Akten und Verzeichnissen einerseits und Hilfsmitteln andererseits.

Nebenakten, Generalakten und Sammelakten können wahlweise papiergebunden oder elektronisch geführt werden (§§ 43 ff. NotAktVV). Nach § 35 Abs. 4 BNotO dürfen Notarinnen und Notare elektronische Akten und Verzeichnisse nur in der Geschäftsstelle oder im künftigen Elektronischen Notaraktenspeicher (§ 78k BNotO) führen. Eine Cloud-Speicherung ist für Akten und Verzeichnisse also unzulässig.

Für Hilfsmittel ist eine Cloud-Speicherung dagegen zulässig, sofern der Datenschutz sowie die Verschwiegenheit gewahrt sind. Hilfsmittel im Sinne von § 35 Abs. 2 Satz 2 BNotO sind technische oder

[4] *Mell/Grance*, „The NIST Definition of Cloud Computing“, National Institute of Standards and Technology (NIST), S. 6, abrufbar unter https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
[5] *Mell/Grance*, „The NIST Definition of Cloud Computing“, National Institute of Standards and Technology (NIST), S. 6, abrufbar unter https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

organisatorische Mittel, die nicht selbst Akten oder Verzeichnisse darstellen, aber unmittelbar deren Erstellung, Bearbeitung oder Sicherung dienen.

Es steht im Ermessen der Notarin oder des Notars, ob die Akten in Papierform, elektronisch oder hybrid geführt werden. Falls etwa die Nebenakten in Papierform geführt werden, können elektronische Dateien (z. B. Entwurfsdateien) von vornherein nur Hilfsmittel sein. Als Hilfsmittel dürfen sie unter Einhaltung der datenschutzrechtlichen und berufsrechtlichen Pflichten grundsätzlich in einer Cloud gespeichert werden.

Falls Notarinnen oder Notare die Nebenakte bereits elektronisch führen, müssen sie die zur Nebenakte gehörenden Daten in der elektronischen Nebenakte in der Geschäftsstelle speichern (vgl. § 35 Abs. 4 BNotO). Damit werden die Daten zum Bestandteil der Nebenakten. Sie sind gewissermaßen das digitale Äquivalent des physischen Ausdrucks für die Nebenakte. Daneben können Notarinnen und Notare die Daten – als Hilfsmittel – ohne Einschränkung aufgrund § 35 Abs. 4 BNotO an zusätzlichen Orten speichern und dabei auch Cloud-Lösungen nutzen.

Konkret bedeutet dies, dass Daten durchaus in der Cloud liegen dürfen, solange die führende elektronische Nebenakte an dem für Nebenakten bestimmten Speicherort in der Geschäftsstelle gespeichert ist. Praktisch kann das System zum Beispiel so gestaltet werden, dass die elektronischen Akten in regelmäßigen Abständen (beispielsweise einmal pro Arbeitstag, mindestens aber einmal pro Woche) in der Geschäftsstelle gespeichert werden, während im Alltagsbetrieb zusätzliche Speicherungen außerhalb der Geschäftsstelle (also in der Cloud) genutzt werden, die dann als Hilfsmittel einzuordnen sind.

Diese Anforderung regelmäßiger Speicherungen von im Alltagsbetrieb verwendeten Daten in der Geschäftsstelle ist letztlich Ausfluss des Gesetzeszwecks des § 35 Abs. 4 BNotO: Dadurch, dass die Notarin oder der Notar elektronische Akten und Verzeichnisse außerhalb der Geschäftsstelle nur im Elektronischen Urkundenarchiv oder im Elektronischen Notariatsaktenspeicher führen darf, soll neben der Wahrung der notariellen Verschwiegenheitspflicht insbesondere die erforderliche Verfügbarkeit von Daten sichergestellt werden.[6] Die erforderliche Verfügbarkeit von Daten setzt voraus, dass Notarinnen und Notare selbst im Fall eines vollständigen Zugriffsverlusts auf Hilfsmittel in der Cloud unmittelbar arbeitsfähig bleiben und es in der Konsequenz nicht zu einem Datenverlust kommt, der im laufenden Betrieb nicht mehr ausgeglichen werden kann. Eine Datenverfügbarkeit nach diesen Maßstäben ist aus Sicht der Bundesnotarkammer gewahrt, falls die in der Cloud liegenden Hilfsmittel mindestens einmal pro Woche auf einem Server oder anderem Speichermedium in der Geschäftsstelle gespeichert werden, auf dessen Grundlage die Fortsetzung des Alltagsbetriebs jederzeit möglich wäre.

Vor diesem Hintergrund dürfen Notarsoftwarelösungen und sonstige Anwendungen auch ausschließlich in Clouds installiert und betrieben werden, solange die vorgenannten berufsrechtlichen Anforderungen sowie die gesetzlichen Vorgaben an Datenschutz und Verschwiegenheit gewahrt sind. Die Auswirkungen eines Ausfalls von Cloud-Diensten können je nach Art der Notarsoftwarelösung unterschiedlich gravierend sein. Der Ausfall eines Hilfstools – etwa zur Grundbuch-Analyse – wäre in der Regel deutlich weniger kritisch als der Ausfall der zentralen Notarsoftware eines

[6] BT-Drucks. 18/10607, S. 55.

Notarbüros, in der etwa die Entwurfsvorbereitung und elektronische Aktenführung stattfindet. Notarinnen und Notare sollten daher darauf achten, dass Anbieter cloudbasierter zentraler Notarsoftwarelösungen einen belastbaren Notfallplan bereithalten, der eine Aufrechterhaltung des Alltagsbetriebs eines Notarbüros auch im Fall eines vollständigen Zugriffsverlusts auf Cloud-Dienste ermöglicht.

Ebenso ist eine standortübergreifende Servernutzung durch mehrere Anwaltsnotarinnen und Anwaltsnotare möglich und zwar unabhängig davon, ob sich der gemeinsam genutzte Server in den Räumen einer der Geschäftsstellen oder in einem externen Rechenzentrum befindet. Daten dürfen zur Verwendung als Hilfsmittel im Sinne von § 35 Abs. 2 Satz 2 BNotO auf solchen gemeinsam genutzten Servern gespeichert werden. Allerdings müssen die Akten und Verzeichnisse – entsprechend der obigen Ausführungen – auch hier stets in der Geschäftsstelle der (jeweiligen) Notarin bzw. des Notars geführt werden.

I. Aktive Bearbeitung vor Speicherung in der Akte

Es ist berufsrechtlich unbedenklich, wenn eine Datei (z. B. ein Urkundsentwurf) in einer Cloudlösung erstellt, bearbeitet und gespeichert wird, solange sie anschließend und fortlaufend – spätestens innerhalb einer Woche – in die (elektronische oder papiergebundene) Akte übernommen wird.

Die Cloudfassung bleibt in diesem Fall ein Hilfsmittel und wird nicht Bestandteil der Akte. Dies gilt auch für:

- eine Online-Textverarbeitung,
- die fortlaufende Synchronisation von Dokumenten,
- eine Nutzung mobiler Endgeräte zur Erstellung von Akteninhalten,
- das langfristige Speichern von Sicherungskopien in der Cloudlösung.

II. Hybride Nutzungsszenarien

Zulässig sind auch Konstellationen, in denen:

- eine Datei hochgeladen und in der Cloud bearbeitet und
- anschließend
  - ausgedruckt und in die Papierakte genommen oder
  - innerhalb einer Woche lokal im Notarbüro gespeichert wird (bei elektronischer Aktenführung).

B. Anforderungen an Datenschutz und Verschwiegenheit

Zusammengefasst setzen Datenschutz und Verschwiegenheitspflicht in der derzeitigen Rechtslage voraus:

- Gewährung eines Zugangs zu der Verschwiegenheitspflicht unterliegenden Tatsachen nur, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist (§ 26a Abs. 1 Satz 1 BNotO),
- eine sorgfältige Auswahl und Überwachung des Anbieters (§ 26a Abs. 2 BNotO; Art. 28 Abs. 1 DSGVO), eine Verschwiegenheitsvereinbarung in Textform[7] (§ 26a Abs. 3 BNotO),
- eine Auftragsverarbeitungsvereinbarung[8] (Art. 28 Abs. 3 DSGVO),
- eine Aufnahme der Empfänger oder Kategorien von Empfängern in die Datenschutzinformationen[9] (Art. 13 Abs. 1 lit. e) DSGVO) und das Verarbeitungsverzeichnis[10] (Art. 30 Abs. 1 lit. d) DSGVO),
- die Vornahme technischer und organisatorischer Maßnahmen, um die Sicherheit der Datenverarbeitung zu gewährleisten[11] (Art. 32 DSGVO),
- ggf. eine Datenschutz-Folgenabschätzung, soweit eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat[12] (Art. 35 DSGVO).

I. Notarielle Verschwiegenheitspflicht

Bei der Nutzung von Cloud-Angeboten im Notariat ist die Pflicht zur Verschwiegenheit nach § 18 Abs. 1 Satz 1 BNotO zu beachten. Grundsätzlich ist danach der Zugriff auf die Cloudlösung ausschließlich Notarinnen und Notaren bzw. ihren Mitarbeitenden vorbehalten. Nur nach Maßgabe des § 26a BNotO dürfen Notarinnen und Notare Dienstleistern den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung zur Verschwiegenheit gemäß § 18 BNotO bezieht.[13]

Der Maßstab der Erforderlichkeit in § 26a Abs. 1 Satz 1 BNotO ist nicht auf das „Ob" der Inanspruchnahme bezogen.[14] Der Gesetzgeber geht vielmehr davon aus, dass die Inanspruchnahme externer

---

[7] Ein Muster einer Verschwiegenheitsvereinbarung mit einem Dienstleister nach § 26a BNotO ist abrufbar im internen Bereich unter https://www.bnotk.de/intern/vordrucke/verschwiegenheitsvereinbarung-nach-26a-bnoto.

[8] Näher hierzu auch https://www.bnotk.de/intern/datenschutz/auftragsverarbeitungsvereinbarungen.

[9] In der Musterdatenschutzerklärung der Bundesnotarkammer wäre dies unter *„4. An wen gebe ich Daten weiter?"* zu erwähnen. Die Musterdatenschutzerklärung ist abrufbar im internen Bereich unter https://www.bnotk.de/intern/vordrucke/datenschutzerklaerung-nach-dsgvo-2.

[10] Die im internen Bereich der Homepage verfügbaren Musterverarbeitungsverzeichnisse der Bundesnotarkammer sehen ein entsprechendes Datenfeld vor (*„Empfänger oder Kategorien von Empfängern, denen die Daten offengelegt sind oder werden"*). Der Cloud-Dienstleister muss darin nur der Kategorie nach verzeichnet werden (etwa als „Notarsoftware-Anbieter"). Die Musterverarbeitungsverzeichnisse sind im internen Bereich aus dem Notarnetz abrufbar unter https://www.bnotk.de/intern/vordrucke/verzeichnisse-von-verarbeitungstaetigkeiten.

[11] Ein Muster für die Dokumentation technischer und organisatorischer Maßnahmen ist im internen Bereich abrufbar unter https://www.bnotk.de/intern/vordrucke/toms-dokumentationen.

[12] Näher hierzu *Hessel/Ziegler-Kiefer/Schneider*, K&R 2025, 755 (760).

[13] Umfassend hierzu Rundschreiben Nr. 4/2018 vom 17.04.2018 und Rundschreiben Nr. 4/2021 vom 23.04.2021.

[14] Diehn/*Diehn*, BNotO, 3. Aufl. 2025, § 26a Rn. 10.

Dienstleistungen grundsätzlich statthaft ist und räumt dem Notar ein Organisationsermessen ein.[15] Die Erforderlichkeit ist vielmehr auf das „Wie" der Inanspruchnahme der konkreten Dienstleistung bezogen: Die Offenbarung eines Geheimnisses ist erforderlich, wenn es keinen genauso effektiven Weg für die Inanspruchnahme der jeweiligen Dienstleistung gibt, der das Geheimnis weniger beeinträchtigt, wobei zu bedenken ist, dass der Tatbestand der Offenbarung eines Geheimnisses schon durch die bloße Möglichkeit der Kenntniserlangung erfüllt ist.[16]

II. Datenschutzrecht

Bei der Nutzung von Cloud-Diensten liegt regelmäßig eine Auftragsverarbeitung nach Art. 4 Nr. 8, Art. 28 DSGVO vor. Neben einer sorgfältigen Anbieterauswahl ist daher ein Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO erforderlich. Entsprechende Vereinbarungen stellen viele Anbieter zum Download bereit (Textform genügt, vgl. Art. 28 Abs. 9 DSGVO). Darüber hinaus sind die Empfänger oder Kategorien von Empfängern in die Datenschutzinformationen nach Art. 13 Abs. 1 lit. e) DSGVO und das Verarbeitungsverzeichnis nach Art. 30 Abs. 1 lit. d) DSGVO aufzunehmen. Schließlich sind technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO erforderlich, um die Sicherheit der Datenverarbeitung zu gewährleisten.

Herausfordernder ist die Einhaltung des Datenschutzrechts indes bei einer Datenübermittlung in ein Drittland außerhalb des EWR, da hierfür besondere Erlaubnistatbestände nach Art. 44 ff. DSGVO erfüllt sein müssen.[17] Praxisrelevant ist vor allem eine Datenübermittlung in die USA (siehe Ziffer B. III.).

III. Organisatorische Verantwortung und Auswahl von Cloudanbietern

Die Verantwortung für die ordnungsgemäße Umsetzung der geschilderten Anforderungen liegt bei der jeweiligen Notarin bzw. beim jeweiligen Notar. Wichtig ist dabei, dass eine Cloud-Lösung nicht per se sicherer oder unsicherer als die Installation und das Betreiben von Software innerhalb der eigenen IT-Infrastruktur im Notarbüro (On-Premise-Lösung) ist.

In der Cloud betriebene Lösungen bestehen meist aus einer Vielzahl technischer Komponenten wie z. B. Infrastrukturkomponenten, Systemsoftware, Datenbanken und schließlich Anwendungssoftware. Die Sicherheit jeder einzelnen Komponente ist dabei nicht nur von ihrer Qualität, sondern auch von der korrekten Konfiguration der Komponente abhängig. Die Sicherheit der gesamten Cloud-Lösung bemisst sich letztlich an der Sicherheit ihrer jeweils schwächsten Komponente. Daher

---

[15] Diehn/*Diehn*, BNotO, 3. Aufl. 2025, § 26a Rn. 10. Im Ergebnis ebenso BeckOK BNotO/*Hushahn*, 12. Ed. 1.8.2025, § 26a BNotO Rn. 7; Schönenberg-Wessel/Plottek/Sikora/*Tykwer,* BNotO, § 26a Rn. 10. In der Gesetzesbegründung zu § 26a BNotO wird auf die Ausführungen zu § 43e BRAO verwiesen, BT-Drs. 18/11936, S. 38. Hier heißt es zum Begriff der Erforderlichkeit „Allerdings muss der Rechtsanwältin und dem Rechtsanwalt auch ein Spielraum für verantwortliche unternehmerische Entscheidungen eröffnet werden. Die Erforderlichkeit einer Auslagerung ist nicht deshalb zu verneinen, weil auch die Möglichkeit bestünde, Dienstleister in der Kanzlei anzustellen.", BT-Drs. 18/11936, S. 34. Ein entsprechendes Organisationsermessen wird daher auch im anwaltlichen Bereich angenommen. Siehe hierzu „Initiativ-Stellungnahme des Deutschen Anwaltsvereins zum Einsatz von KI in der Anwaltschaft", S. 12, abrufbar unter https://anwaltverein.de/newsroom/sn-32-25-einsatz-von-ki-in-der-anwaltschaft.

[16] Diehn/*Diehn*, BNotO, 3. Aufl. 2025, § 26a Rn. 11.

[17] Zusätzlich muss der Notar die Absicht, die personenbezogenen Daten an ein Drittland zu übermitteln, in seine Datenschutzerklärung nach Art. 13 Abs. 1 lit. f DSGVO aufnehmen und sich darin ausführlich zur Rechtsgrundlage äußern. Schließlich bedarf die Übermittlung von personenbezogenen Daten an ein Drittland nach Art. 30 Abs. 1 Satz 2 lit. e DSGVO einer gesonderten Aufnahme in das Verarbeitungsverzeichnis. Näher hierzu Rundschreiben Nr. 04/2021 vom 23.04.2021.

ist die Sicherheit einer Cloud-Lösung neben der Auswahl eines geeigneten Cloud- und Software-Anbieters insbesondere auch von der korrekten Konfiguration der Cloud-Lösung durch den jeweiligen IT-Dienstleister abhängig.

Es existieren eine Vielzahl unterschiedlicher Testate und Zertifizierungen von Cloud-Lösungen, die durch verschiedene Stellen und Organisationen vergeben werden. Beispielsweise ist der BSI Cloud Computing Compliance Criteria Catalogue (kurz: BSI C5) ein Kriterienkatalog, der Mindestanforderungen an die Informationssicherheit für Cloud-Dienste enthält, die aus Sicht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nicht unterschritten werden sollten.[18] Ziel des Kataloges ist ausweislich des BSI die transparente Darstellung der Informationssicherheit eines Cloud-Dienstes auf Basis einer standardisierten Prüfung.

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 aktuellem Stand zwar datenschutzrechtlich zulässig genutzt werden, jedoch gibt es Unwägbarkeiten. Daher wird nach Möglichkeit zu europäischen Angeboten geraten.

1. Zugriffsrecht des Drittstaats

Cloud-Anbieter mit Sitz und Datenverarbeitung ausschließlich im Europäischen Wirtschaftsraum (EWR), die nicht Teil eines Konzerns mit Sitz in einem Drittstaat sind, sind allein der DSGVO und ggf. mitgliedstaatlichen Datenschutzvorschriften, aber keinem außereuropäischen Rechtsregime, unterworfen und können – Einhaltung dieser Vorschriften vorausgesetzt – beauftragt werden.

Komplexer verhält es sich bei Anbietern, die oder deren Konzernmutter außerhalb des EWR ansässig sind. Auch bei EU-Serverstandorten kann durch konzerninterne Weisungsrechte ein faktischer Zugriff der Drittstaatenmutter auf personenbezogene Daten entstehen. Dies ist insbesondere relevant, wenn das Mutterunternehmen dem Recht eines Staates mit extraterritorialer Zugriffsbefugnis unterliegt – etwa dem US-Cloud Act (Clarifying Lawful Overseas Use of Data Act). Der US-Cloud Act aus dem Jahr 2018 verpflichtet US-Dienstleister, u.a. bei einem gültigen Gerichtsbeschluss oder Durchsuchungsbefehl Daten an US-Behörden herauszugeben – auch dann, wenn die Daten auf Servern außerhalb der USA liegen. Das betrifft nach derzeitigem Stand also auch Daten, die etwa von AWS, Microsoft oder Google in Deutschland gehostet werden.

2. Rechtsgrundlage für die Zulässigkeit der Datenverarbeitung in den USA

Wenn ein US-Anbieter EU-US Data Privacy Framework (DPF)-zertifiziert ist, ist ein DSGVO-konformer Einsatz nach Art. 44 ff. DSGVO grundsätzlich möglich. Ob eine entsprechende Zertifizierung

[18] BSI, C5 Einführung, abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/C5_Einfuehrung_node.html.

eines bestimmten US-Unternehmens besteht, kann auf der Website der „International Trade Administration“, einer Behörde des US-Handelsministeriums, eingesehen werden.[19]

Der für die Zulässigkeit der Datenverarbeitung in den USA erforderliche Angemessenheitsbeschluss nach Art. 45 DSGVO basiert u.a. auf verschiedenen US-amerikanischen Datenschutz-Kontrollinstitutionen, die per Präsidialerlass des seinerzeitigen US-Präsidenten etabliert wurden. Derartige Präsidialerlasse sind allerdings jederzeit widerruflich.

Die Basis für den Angemessenheitsbeschluss (Art. 45 DSGVO) wurde in der Vergangenheit zudem bereits zweimal (Safe Harbour[20] und Privacy Shield[21]) durch den EuGH für unwirksam erklärt („Schrems I und II“). Zwar wurde die Wirksamkeit des Angemessenheitsbeschlusses auf Grundlage des DPF jüngst durch das EuG bestätigt.[22] Allerdings bezieht sich die Entscheidung des EuG auf das Jahr 2023 und es hat zugleich klargestellt, dass die EU-Kommission fortlaufend prüfen müsse, ob ein äquivalentes Datenschutzniveau auf Grundlage des DPF nach wie vor gewährleistet sei.[23] Es besteht insoweit das nicht auszuschließende Risiko, dass auch der aktuelle Angemessenheitsbeschluss vom EuGH als unzureichend eingestuft werden könnte.[24] Die Urteile des EuGH zu den vorangegangenen Angemessenheitsbeschlüssen lassen befürchten, dass auch alternative Rechtsgrundlagen wie die Standardvertragsklauseln der US-Cloud-Anbieter wegen der bestehenden Zugriffsrechte von US-Behörden über den Cloud Act kurzfristig einer Überprüfung eines ausreichenden Schutzniveaus für eine zulässige Datenübermittlung durch den EuGH möglicherweise nicht standhalten werden. Jede Art von Datentransfer in die USA fände im Falle einer Entscheidung des EuGH gegen den Angemessenheitsbeschluss *ex nunc* ohne Rechtsgrundlage statt.[25]

Neben diese datenschutzrechtlichen Aspekte tritt die sich zunehmend verändernde geopolitische Lage. In der Vergangenheit sind bereits temporär Services von Drittstaatenanbietern in Europa – auch kurzfristig – gesperrt worden.[26]

3. Auswahl von Cloudanbietern

Neben US-amerikanischen und sonstigen drittstaatlichen Cloud-Anbietern stehen auch Cloud-Dienstleistungen solcher Unternehmen zur Verfügung, die ihren Sitz im EWR haben, nicht durch einen drittstaatlichen Konzern kontrolliert werden und die Datenverarbeitung ausschließlich im EWR vornehmen. Bei Beauftragung solcher Unternehmen ergeben sich die beschriebenen

[19] International Trade Administration, Data Privacy Framework List, abrufbar unter https://www.dataprivacyframework.gov/list. Hier sind derzeit z. B. Amazon, Google und Microsoft aufgeführt.
[20] EuGH, Urteil vom 6.10.2015 - C-362/14.
[21] EuGH, Urteil vom 16.7.2020 – C-311/18.
[22] EuG, Urteil vom 3.9.2025 – T-553/23.
[23] „EU-Gericht weist Klage gegen Abkommen mit den USA ab“, Tagesschau, abrufbar unter https://www.tagesschau.de/ausland/europa/eu-datenschutz-urteil-100.html.
[24] *Hessel/Ziegler-Kiefer/Schneider*, K&R 2025, 755 (756).
[25] *Hessel/Ziegler-Kiefer/Schneider*, K&R 2025, 755 (756).
[26] „Microsoft steckt in der Trump-Falle“, WirtschaftsWoche vom 25.05.2025, abrufbar unter https://www.wiwo.de/technologie/digitale-welt/sanktionen-gegen-internationalen-gerichtshof-microsoft-steckt-in-der-trump-falle/100129647.html; „Diese E-Mail ist unzustellbar“, Die Zeit vom 23. Juli 2025, abrufbar unter https://www.zeit.de/digital/internet/2025-07/microsoft-email-sperre-karim-khan-donald-trump-istgh; „Internationaler Strafgerichtshof will Bürosoftware von Microsoft durch deutsches Produkt ersetzen“, Deutschlandfunk vom 31. Oktober 2025, abrufbar unter https://www.deutschlandfunk.de/internationaler-strafgerichtshof-will-buerosoftware-von-microsoft-durch-deutsches-produkt-ersetzen-102.html.

datenschutzrechtlichen Unsicherheiten nicht. Cloud-Technologien haben eine strategische Bedeutung für die Datensouveränität, Sicherheit und wirtschaftliche Unabhängigkeit Europas. Vor diesem Hintergrund sollten bei der Auswahl von Cloud-Lösungen europäische Angebote systematisch berücksichtigt und – sofern leistungsfähig und verfügbar – bevorzugt werden. Dies gilt insbesondere für sensible Bereiche.

Anbieter sogenannter „souveräner Cloud-Angebote" versprechen einen selbstbestimmten Einsatz US-amerikanischer Cloud-Technologie, indem sie diese als selbstständige Unternehmen mit Sitz im EWR auf Grundlage von Vereinbarungen mit den US-amerikanischen Unternehmen anbieten und eine Datenverarbeitung ausschließlich im EWR vornehmen.[27] Allerdings werden diese Angebote wegen ihrer technologischen Abhängigkeit von US-Unternehmen teilweise kritisch gesehen.[28] Gleichwohl können sie eine Lösung sein, falls es zwar im Einzelfall zwingend US-amerikanischer Cloud-Technologie bedarf, aber ein europäischer Cloud-Dienstleister beauftragt werden soll, der Eigentümer der Cloud-Infrastruktur und Betreiber der Cloud-Plattform ist.[29]

Hinsichtlich der Fragen, welcher Cloud-Dienstleister und welche Cloud-Services in Anspruch genommen werden, sollten Notarinnen und Notare Rücksprache mit ihrem IT-Dienstleister und Notarsoftwareanbieter halten.

C. Microsoft 365 für Notarkanzleien

Mit Microsoft Office 2024 wurde im September 2024 eine neue Version der Microsoft Office Suite veröffentlicht, die wie gewohnt lokal installiert und vollständig offline genutzt werden kann.[30] Für die Zukunft hat Microsoft zudem die Arbeit an einer weiteren lokalen Office Version über dieses Release hinaus bestätigt.[31] Gleichzeitig bewirbt der Microsoft-Konzern stark seinen Abonnement-Dienst „Microsoft 365".[32] Beispielsweise erhält diese Abo-Anwendung im Vergleich zur klassischen Office-Suite bevorzugt Features wie z. B. eine KI-Unterstützung. Dabei wird Microsoft 365 derzeit zwingend in der „Azure-Cloud" von Microsoft betrieben. Damit gehen die bereits geschilderten Risiken von „US-Clouds" einher (vgl. vorstehend Ziffer B.III.).

Verschiedene Datenschutzbeauftragte auf Bund-, Länder- und EU-Ebene sehen strukturelle Probleme bei Microsoft 365, insbesondere hinsichtlich Transparenz und Datentransfer in die USA (vgl.

---

[27] Siehe auch die Regierungsdefinition des Begriffs souveräne Cloud, BT-Drs. 20/15138, S. 6.

[28] „Schein-Lösungen stoppen: Souveränitäts-Washing von Big Tech gefährdet Sondervermögen", Gesellschaft für Informatik, abrufbar unter https://gi.de/themen/beitrag/kritik-zu-souveraenitaets-washing-von-big-tech.

[29] Vgl. „Finale Verträge für die souveräne Cloud sind unterzeichnet", eGovernment vom 25.09.2024, abrufbar unter https://www.egovernment.de/finale-vertraege-fuer-die-souveraene-cloud-sind-unterzeichnet-a-828ef87cbbf0326ed3f19cda97f04d1b/; „Delos Cloud: Das kostet die digitale Souveränität", Computerwoche vom 26.02.2025, abrufbar unter https://www.computerwoche.de/article/3833699/delos-cloud-das-kostet-die-digitale-souveranitat.html.

[30] Sicherheitsempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zur Konfiguration von Microsoft Office 2021 und 2024 durch Unternehmen sind abrufbar unter https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_135.pdf?__blob=publicationFile&v=9.

[31] Häufig gestellte Fragen zu Office 2024 und Office LTSC 2024, Frage „Wird es darüber hinaus lokale Versionen von Office geben?", Antwort „Wir freuen uns, unsere Verpflichtung zu einer weiteren Version der lokalen Version von Office in Zukunft über dieses Release hinaus bestätigen zu können.", abrufbar unter https://support.microsoft.com/de-de/office/h%C3%A4ufig-gestellte-fragen-zu-office-2024-und-office-ltsc-2024-1c454a7d-3d0a-4139-b1bd-c61725ea436c.

[32] „Was ist der Unterschied zwischen Microsoft 365 und Office 2024?", abrufbar unter https://support.microsoft.com/de-de/office/was-ist-der-unterschied-zwischen-microsoft-365-und-office-2024-ed447ebf-6060-46f9-9e90-a239bd27eb96.

bereits Ziffer B. III.).[33] Da in Microsoft Word typischerweise stark schützenswerte Daten verarbeitet werden, sind die Auswirkungen theoretisch möglicher Datenabflüsse potenziell erheblich. Angesichts jüngster politischer Konflikte zwischen den USA und der EU erscheint zudem nicht ausgeschlossen, dass digitale Dienste von Microsoft erneut als Druckmittel eingesetzt werden.[34]

Mindestens muss auf die richtigen Vertragskonditionen, die richtige technische Konfiguration und die richtige Dokumentation (Datenschutz-Folgenabschätzung, Art. 35 DSGVO) geachtet werden.[35] Ein DSGVO-konformer Einsatz ist damit derzeit grundsätzlich möglich.[36]

Was die notarielle Verschwiegenheitspflicht anbelangt, bietet Microsoft 365 eine Reihe von Konfigurationsmöglichkeiten. Die Standardeinstellungen der Anwendung sind für eine maximale Funktionalität optimiert, aber nicht auf vertrauliches Arbeiten ausgerichtet und müssen daher angepasst werden.[37] Tatsächlich kann jeder Patch der Software seitens Microsoft Konfigurationsänderungen erfordern oder den Umgang mit Daten ohne mögliche Korrektur verändern.

Microsoft 365 kann – je nach Konfiguration – aus Sicht der Bundesnotarkammer nach aktuellem Stand in Konformität zu den berufsrechtlichen Anforderungen des § 35 BNotO und des § 26a BNotO verwendet werden, soweit mit Microsoft die „Zusatzvereinbarung für Berufsgeheimnisträger“ abgeschlossen wird, da die Software bei Beachtung der unter Ziffer A. dargelegten Maßgaben grundsätzlich als „Hilfsmittel“ im Sinne von § 35 Abs. 2 Satz 2 BNotO zu bewerten ist. So dürfen Akten und Verzeichnisse nicht vollständig in Microsoft 365 ausgelagert werden. Da sich die Inhalte der „Zusatzvereinbarung für Berufsgeheimnisträger“ in Zukunft ändern können, bleibt eine Einzelfallprüfung der Vertragsbedingungen mit Microsoft auf Vereinbarkeit mit § 35 BNotO und § 26a BNotO unentbehrlich.

Notarinnen und Notare sollten für sich prüfen, ob der Einsatz der erweiterten Funktionen von Microsoft 365 unter Berücksichtigung möglicher datenschutzrechtlicher Unsicherheiten und des damit verbundenen Aufwands zur Wahrung der notariellen Verschwiegenheitspflicht sinnvoll ist –

[33] „DSK: Warum Verantwortliche Microsoft 365 nicht datenschutzkonform nutzen können“, Datenschutz PRAXIS vom 07.12.2022, abrufbar unter https://www.datenschutz-praxis.de/verarbeitungstaetigkeiten/warum-sie-microsoft-365-nicht-datenschutzkonform-nutzen-koennen/; „Hier klemmt es in NRW beim Datenschutz“, WDR vom 08.07.2024, abrufbar unter https://www1.wdr.de/nachrichten/landespolitik/bericht-datenschutzbeauftragte-nrw-100.html; „Während Den Haag aussteigt: Bayern schließt Milliarden-Deal mit Microsoft“, Frankfurter Rundschau vom 10.11.2025, abrufbar unter https://www.fr.de/wirtschaft/bayern-und-microsoft-besiegeln-milliardendeal-den-haag-wechselt-anbieter-zr-94028610.html. Kritisch dagegen *Hessel/Ziegler-Kiefer/Schneider*, K&R 2025, 755 (757 ff.).

[34] „Digitale Erpressbarkeit: Europa hängt stark von US-Firmen ab“, Handelsblatt vom 09.01.2026, abrufbar unter https://www.handelsblatt.com/dpa/trump-und-europaeer-digitale-erpressbarkeit-europa-haengt-stark-von-us-firmen-ab/100190075.html; „Internationaler Strafgerichtshof plant Wechsel von Microsoft zu deutschem Officepaket“, Der Spiegel vom 30.10.2025, abrufbar unter https://www.spiegel.de/netzwelt/internationaler-strafgerichtshof-wechsel-zu-deutschem-officepaket-nach-us-sanktionen-a-6ddfddcd-8871-4955-898a-2a325ae7fe06.

[35] *Hessel/Ziegler-Kiefer/Schneider*, K&R 2025, 755 (760).

[36] „Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft 365“ vom 15. November 2025, abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2025-11/hbdi_bericht_m365_2025_11_15.pdf; *Hessel/Ziegler-Kiefer/Schneider*, K&R 2025, 755 (760).

[37] Näher hierzu und zu weiteren Handlungsempfehlungen für Verantwortliche: „Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft 365“ vom 15. November 2025, S. 76 ff., abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2025-11/hbdi_bericht_m365_2025_11_15.pdf. Siehe auch *Hessel/Ziegler-Kiefer/Schneider*, K&R 2025, 755.

oder ob im konkreten Fall der Verbleib bei einer klassischen Office-Suite weiterhin ausreichend erscheint.

Mit freundlichen kollegialen Grüßen

Dr. Milan Bayram
Hauptgeschäftsführer