Technische Universität Braunschweig

Cloud-Strategie der TU Braunschweig

1. Einleitung

Die Digitalisierung stellt Hochschulen vor grundlegende technologische, organisatorische und ökonomische Herausforderungen.

Cloud-Dienste beschreiben als Sammelbegriff unterschiedliche Arten der Nutzung von Hard- und Software über ein Netzwerk, vor allem das Internet. Dabei kann nach Umfang der Leistung („Schichtenmodell“) oder Art des Angebotes („Bereitstellungsmodell“) unterschieden werden. Das vorliegende Dokument fokussiert sich auf die Bereitstellungsmodelle Private Cloud, Community Cloud und Public Cloud (nähere Erläuterung siehe Glossar).

In Niedersachsen wird diese Entwicklung durch das Landesprogramm Hochschule.digital Niedersachsen neu strukturiert: IT-Dienste sollen künftig nicht mehr primär lokal an jeder Hochschule betrieben werden, sondern arbeitsteilig durch wenige, leistungsfähige Rechenzentren für alle Hochschulen des Landes bereitgestellt werden. Dies betrifft sowohl klassische On-Premises[1]-Dienste als auch den koordinierenden, verantwortungsvollen Einsatz externer Cloud-Angebote.

Vor diesem Hintergrund verfolgt die TU Braunschweig das Ziel, ihre eigene Cloud-Strategie so auszurichten, dass sie sowohl die landesweite Servicearchitektur unterstützt als auch ihre eigene institutionelle Verantwortung für Datenschutz, Informationssicherheit und nachhaltige IT-Entwicklung wahrnimmt. Cloud-Dienste sollen im Zusammenspiel mit den landesweiten Strukturen genutzt werden, wobei Risiken transparent bewertet und Synergien konsequent ausgeschöpft werden.

Diese Strategie baut auf den technologischen Grundlagen des Cloud-Computing, den bewährten Konzepten anderer Hochschulen sowie den sicherheitsorientierten Leitlinien und Risikoanalysen der TU9 ITSB/CISO-Gruppe auf, berücksichtigt jedoch darüber hinaus die neuen Rahmenbedingungen einer kooperativen und arbeitsteiligen Hochschul-IT-Landschaft für Niedersachsen.

[1] Siehe Glossar

2. Vision und Leitidee der Cloud-Nutzung im Kontext eines landesweiten IT-Verbundes

Im Rahmen von Hochschule.digital Niedersachsen entsteht derzeit ein hochschulübergreifend gestaltetes Ökosystem von digitalen Services, in der Hochschulen nicht mehr isoliert handeln, sondern abgestimmt und arbeitsteilig. IT-Dienste sollen dort erbracht werden, wo Kompetenzen, Ressourcen und Spezialisierungen dies am effizientesten und sichersten ermöglichen.

Wesentliche Elemente dieser Cloud-Strategie sind daher:

1. Die TU Braunschweig agiert primär als Anbieterin hochqualitativer IT-Dienste für andere niedersächsische Hochschulen.
2. Die Universität ist ebenso Nutzerin von Diensten, die durch andere Hochschulen oder zentrale Landesstrukturen bereitgestellt werden.
3. Die IT-bezogenen Gremien erstellen abgestimmte Empfehlungen für Entscheidungen durch das Präsidium (und bei strategisch relevanten Entscheidungen zusätzlich durch den Senat).
4. Cloud-Technologien werden dort genutzt, wo sie funktional, sicher, wirtschaftlich und organisatorisch sinnvoll sind.
5. Datenhoheit, Datenschutz und Informationssicherheit werden nicht nur an der TU Braunschweig, sondern auch im arbeitsteiligen Verbund gewahrt.
6. Innovationspotentiale externer Cloud-Anbieter werden gezielt erschlossen, aber stets im Einklang mit den lokalen und HdN-bezogenen Governance-Strukturen.
7. Die TU Braunschweig unterstützt und gestaltet aktiv eine vereinheitlichte, interoperable, mehr-instanzfähige IT-Servicearchitektur in Niedersachsen.

Cloud-Nutzung ist damit nicht mehr allein eine institutionelle Entscheidung, sondern ein Baustein eines koordinierten hochschulübergreifenden Digitalökosystems.

3. Strategische Grundsätze im landesweiten Kontext

3.1 Arbeitsteilige Bereitstellung und Nutzung von IT-Diensten

Durch Hochschule.digital Niedersachsen wird das Prinzip der föderierten, aber arbeitsteiligen IT verbindlich. Diese Struktur beeinflusst die Cloud-Strategie in mehrfacher Hinsicht:

- Die TU Braunschweig betreibt künftig nicht mehr jeden benötigten IT-Dienst selbständig, sondern übernimmt gezielt Verantwortungen für bestimmte Dienste, für die sie Kompetenz und Kapazität besitzt. In der Auswahl der selbst betriebenen Dienste bleibt die

TU Braunschweig grundsätzlich autonom, allerdings strebt sie an, sich an dem Verteilungsmodell der HdN zu orientieren.

- Gleichzeitig nutzt sie zentral bereitgestellte Dienste anderer Hochschulen, einschließlich Community-Cloud- oder externer Cloud-Lösungen, die hochschulübergreifend abgeschlossene Verträge nutzen.
- Vor Einführung neuer Cloud-Dienste an der TU Braunschweig erfolgt eine Abstimmung mit dem LANIT sowie dem Leitungsausschuss HdN der IT-Allianz. Die Einführung neuer Cloud-Dienste erfolgt nicht mehr isoliert auf der Ebene einzelner Organisationseinheiten der TU Braunschweig.

Damit wird die Universität Teil einer landesweiten serviceorientierten IT-Governance, die Doppelstrukturen reduziert, Synergien schafft und Sicherheitsstandards harmonisiert.

3.2 Innovation und Kompetenz weiterentwickeln

Im arbeitsteiligen Modell gewinnt die Spezialisierung an Bedeutung. Die TU Braunschweig verpflichtet sich daher:

- eigene Cloud-Kompetenzen gezielt auszubauen, insbesondere in Bereichen, in denen sie landesweite Dienste erbringt,
- gemeinsam mit anderen Hochschulen standortübergreifende Kompetenzzentren zu entwickeln,
- moderne Cloud-Technologien in Forschung und Lehre zugänglich zu machen – unabhängig davon, ob diese lokal, landesweit oder extern betrieben werden,
- sich aktiv in die Definition landesweiter Cloud-Standards einzubringen.

Innovationen werden damit gleichzeitig lokal gestärkt und landesweit skaliert.

3.3 Wirtschaftlichkeit im Verbundmodell

Wirtschaftlichkeit wird im Rahmen von Hochschule.digital Niedersachsen neu bewertet:

- Entscheidungen über Cloud-Einsatz berücksichtigen nicht nur lokale Kosten, sondern auch Synergieeffekte und Skaleneffekte des Landesverbundes.
- Dauerlasten werden bevorzugt landesweit gebündelt und technisch entweder als Private- oder Community-Cloud bereitgestellt.
- Die TU Braunschweig berücksichtigt bei Investitionen die Rollenverteilung im Verbund:
    - Betreibt sie einen Dienst selbst?

    - Oder wird sie ihn künftig beziehen?
- Externe Cloud-Dienste werden vorrangig standortübergreifend beschafft, um Verhandlungsmacht zu bündeln, Kosten zu reduzieren und den rechtlichen Aufwand zu minimieren.

So entsteht ein wirtschaftlich tragfähigeres Gesamtmodell, bei dem redundante Infrastrukturen reduziert und gemeinsame Investitionen gestärkt werden.

3.4 Datenschutz und Informationssicherheit im föderierten Betrieb

Durch die arbeitsteilige Bereitstellung entstehen neue Anforderungen:

- Daten können in der Verantwortung einer Hochschule liegen, aber auf Systemen einer anderen Hochschule verarbeitet werden.
- Die TU Braunschweig muss daher sowohl als verantwortliche Stelle als auch als Dienstanbieterin agieren können.
- Datenschutz und Informationssicherheit sollen sukzessive landesweit harmonisiert werden, indem gemeinsame Standards, Prüfschemata und Risikoanalysen entwickelt werden (u. a. auf Basis der TU9-Leitlinien).
- Verträge, Auftragsverarbeitungsverträge und Betriebsvereinbarungen sollen nach Möglichkeit standortübergreifend abgestimmt werden, um Mehrfachverhandlungen zu vermeiden.

Besonders relevant ist der Umgang mit externen Cloud-Anbietern:

- Diese werden möglichst über den Landesverbund zentral beschafft, damit Datenschutzprüfung, TOM[2]-Kontrolle und Vertragsgestaltung einheitlich erfolgen.
- Die Risiken durch extraterritoriale Gesetzgebung (z. B. CLOUD Act[3]) werden nach Möglichkeit gemeinsam bewertet und abgestimmt adressiert.

Damit entsteht ein kohärentes Sicherheitsniveau, das institutionelle Unterschiede überbrückt.

[2] Technisch-Organisatorische Maßnahmen
[3] https://de.wikipedia.org/wiki/CLOUD_Act

4. Governancemodell: Entscheidungsprozesse im Verbund

Die Rolle des CIO-Boards der TU Braunschweig verändert sich.

Es bleibt zuständig für die Bewertung von Cloud-Diensten für die eigene Hochschule, berücksichtigt dabei zukünftig darüber hinaus die übergeordnete landesweite IT-Governance.

Ein Dienst kann daher erst eingeführt oder betrieben werden, wenn:

1. das CIO-Board der TU Braunschweig basierend auf den Rückmeldungen des / der Datenschutzbeauftragten, des Datenschutzmanagements sowie des CISO-Teams eine positive Empfehlung ausspricht, welche im Nachgang vom Präsidium (und bei strategisch relevanten Entscheidungen zusätzlich durch den Senat) beschlossen wird,
2. seine Einführung grundsätzlich mit den Strategien der Hochschule.digital Niedersachsen kompatibel ist,
3. Synergiepotenziale geprüft wurden (z. B. „Kann/soll dieser Dienst landesweit bereitgestellt werden?“),
4. existierende landesweite Dienste nicht über den tatsächlichen Bedarf hinaus dupliziert werden.

Damit wird verhindert, dass sich neue Insellösungen etablieren.

Als Kriterien gelten:

- für externe Cloud-Dienste muss sichergestellt werden, dass spezifiziert wurde, welche Daten gemäß der *Richtlinie Klassifizierung und Handhabung von Informationen* mit dem jeweiligen Dienst bearbeitet bzw. auf der externen Plattform gespeichert werden dürfen,
- Risikoanalyse (Sicherheit, Datenschutz, Betrieb),
- Wirtschaftlichkeit für die TU Braunschweig und auf Landesebene,
- technische Integrationsfähigkeit in die IT-Landschaft der TU Braunschweig und des Verbundes,
- Nachhaltigkeit und Skalierbarkeit.

Die Entscheidung über Cloud-Dienste wird damit nicht nur universitätsbezogen, sondern darüber hinaus strategisch standortübergreifend gedacht und getroffen.

5. Priorisierte Betriebsmodelle in Niedersachsen

Die Priorisierung bleibt grundsätzlich erhalten, wird jedoch an die neue Verbundlogik angepasst.

5.1 Landesweite Private Clouds und Verbundplattformen

Für sensible Daten (gemäß der Definition in der *Richtlinie Klassifizierung und Handhabung von Informationen*) und hochkritische Dienste sind typischerweise lokale, zentrale Plattformen vorgesehen; weniger kritische Daten können auf gemeinsam betriebenen Plattformen an verschiedenen Hochschulen gehostet, aber landesweit genutzt werden.

Die TU Braunschweig kann sowohl Betreiberin solcher Dienste sein als auch Nutzerin vergleichbarer Angebote anderer Hochschulen.

5.2 Community Clouds im Landesverbund

Community Clouds – z. B. DFN, NHR oder hochschulübergreifende Kooperationen – werden explizit als bevorzugtes Modell präferiert.

Im Rahmen von Hochschule.digital Niedersachsen wird dieses Modell gestärkt, da mehrere Hochschulen dadurch gemeinsam

- Dienste betreiben,
- Sicherheitsstandards definieren,
- Supportstrukturen aufbauen sowie
- redundante Angebote eliminieren.

Die TU Braunschweig beteiligt sich aktiv am Aufbau und Betrieb dieser Dienste.

5.3 Public Clouds: kontrolliert, koordiniert, strategisch

Public Clouds bleiben ein wichtiges Werkzeug, sollen jedoch künftig:

- zentral lizenziert,
- standardisiert geprüft,
- landesweit für entsprechend geteilte Dienste für die nutzenden Hochschulen bereitgestellt und

- durch eine gemeinsame Governance abgesichert werden.

Damit entfällt die Notwendigkeit individueller Prüfprozesse auf Ebene individueller Hochschulen; stattdessen wird ein einheitlicher Qualitätsstandard geschaffen. Dies bedeutet gemeinsame Sicherheits- und Rechtsstandards für die Hochschulen in Niedersachsen insbesondere bei der Nutzung der Public Clouds großer Anbieter (Microsoft, Google u.a.).

6. Rollen und Verantwortlichkeiten im föderierten Modell

Die Rollen erweitern sich wie folgt:

6.1 TU Braunschweig als Dienstanbieterin

- übernimmt Verantwortung für Sicherheit, Betrieb und Support definierter landesweiter Dienste,
- implementiert hohe Sicherheits- und Qualitätsstandards,
- betreibt eigene Infrastrukturen cloudfähig und multi-tenancy-ready[4].

6.2 TU Braunschweig als Nutzerin

- bezieht Dienste anderer Hochschulen oder landesweiter Strukturen,
- integriert diese in ihre lokale Architektur,
- gewährleistet sichere Nutzung und klare Serviceprozesse.

6.3 Landesweite Steuerungsstrukturen

- IT-Lenkungsausschuss der HdN
- AG Digitalisierung der LHK
- LHK Plenum

[4] Multi-tenancy-ready bedeutet, dass eine Software so konzipiert ist, dass eine einzige Instanz mehrere Kunden (Mandanten) effizient und sicher bedienen kann, wobei die Daten jedes Mandanten streng getrennt und isoliert bleiben

7. Technische Leitlinien in einer föderierten IT-Landschaft

Im Verbund müssen Cloud-Dienste:

- mandantenfähig (Multi-Tenancy[5]) sein,
- standardisierte Schnittstellen zum landesweiten Identitätsverbund[6] unterstützen (z. B. DFN-AAI, Shibboleth, OIDC),
- interoperabel mit landesweiten Logging-, Monitoring- und Ticketingsystemen sein,
- Compliance-Anforderungen einheitlich umsetzen,
- zentrale Exit-Strategien unterstützen (z. B. hochschulübergreifende Datenmigration).

Auch externe Cloud-Dienste müssen landesweit integriert werden können, etwa:

- zentrale Identity-Federation[7],
- gemeinsame Kostenmodelle,
- abgestimmte Datennutzungsrichtlinien.

8. Weiterentwicklung und Evaluierung

Diese Cloud-Strategie wird regelmäßig angepasst:

- an die Entwicklungen innerhalb des Verbundes Hochschule.digital Niedersachsen,
- an neue landesweite Dienste,
- an gemeinsame Sicherheitsstandards,
- an Erfahrungen im Verbundbetrieb sowie
- an technologische Entwicklungen externer Cloud-Anbieter.

Die TU Braunschweig versteht sich dabei als aktiver Mitgestalter dieser neuen IT-Landschaft. Verantwortlich für den Change-Management Prozess dieser Strategie ist der*die fachlich zuständige Vizepräsident*in für Digitalisierung und Nachhaltigkeit, der*die notwendige Aktualisierungen bei geänderten Rahmenbedingungen mit den IT-Gremien (IT-User Board, Multiprojekt-Management Board und CIO-Board) für die Entscheidungsgremien (Präsidium und Senat) erarbeitet bzw. vorschlägt.

---

[5] Ein Tenant (zu Deutsch „Mieter“), bezieht sich im IT-Kontext auf eine eigenständige und isolierte Instanz (z.B. für eine Hochschule) innerhalb einer gemeinsam genutzten Infrastruktur. Multi-Tenancy beschreibt damit die Fähigkeit eines Dienstes, getrennte Instanzen für unterschiedliche Institutionen (z.B. Hochschulen) implementieren zu können.
[6] Damit wird sichergestellt, dass sich Nutzende von unterschiedlichen Hochschulen bei dem Dienst anmelden können.
[7] https://de.wikipedia.org/wiki/F%C3%B6derierte_Identit%C3%A4t

9. Glossar[8]

Ein **Service Level Agreement (SLA)** bezeichnet eine **Dienstgütevereinbarung** zwischen dem Auftraggeber (der Hochschule) und dem Auftragnehmer (einer diensterbringenden Stelle). Hierbei kann es sich um einen externen Dienstleister oder das Hochschulrechenzentrum handeln. In der Vereinbarung werden Kennzahlen (**Key Performance Indicators, KPI**) z.B. zur Verfügbarkeit von Daten und Diensten definiert, welche verpflichtend einzuhalten sind. Insbesondere bei externen Anbietern können Vertragsstrafen bei Nichteinhaltung vereinbart werden. Werden Dienste ohne vertragliche Verpflichtungen „so gut wie möglich" erbracht, spricht man vom „**Best Effort**"-Ansatz.

Arten von Cloud-Diensten und ihre Bewertung aus Sicht der Informationssicherheit

Die Nutzung von Cloud-Diensten ist mit Gefahren verbunden, welche je nach seiner Ausprägung variieren. Um einschätzen zu können, ob die Risiken der Nutzung eines solchen Dienstes für einen konkreten Anwendungsfall vertretbar sind oder nicht, sind die verschiedenen Ausprägungen von Cloud-Diensten zu untersuchen und deren Einsatz abzuwägen. In Einzelfällen sind auch Mischformen denkbar, diese werden hier nicht weiter betrachtet.

1. Private-Cloud-Dienste („On-Premises")

Cloud-Services, welche durch die eigene Hochschule auf ihrer eigenen Infrastruktur betrieben werden, werden als „Private-Cloud-" oder „On-Premises"-Dienste bezeichnet.

Eigenschaften

On-Premises-Dienste zeichnen sich u.a. durch die im Folgenden beschriebenen Eigenschaften aus:

- Die Daten werden in der eigenen Hochschule gespeichert und verarbeitet.
- Der Betrieb erfordert eigene (ggf. virtualisierte) Hardware für Betrieb und Speicherplatz.
- Der Betrieb erfolgt oft nur an einem Standort oder an zwei Standorten in räumlicher Nähe.
- Es werden Backups in der eigenen Hochschule angeboten und verwaltet.
- Der Aufwand für den technischen Betrieb des jeweiligen Angebots entsteht in der eigenen Hochschule.
- Die Betreuung der Nutzenden erfolgt vollständig in der eigenen Hochschule.
- Die konkrete Ausgestaltung des jeweiligen Dienstes erfolgt in der eigenen Hochschule.

[8] Zitiert aus Empfehlung der TU9 ITSB/CISO vom 18.11.2021

Genaue Anpassung an lokale Anforderungen/Optimierungen sind (einfacher) möglich.
- Die Rechtevergabe und Zugriffsverwaltung für die Nutzenden werden hochschulintern geregelt.
- Dienstgütevereinbarungen können bilateral zwischen Dienststelle und Rechenzentrum bzw. dem internen Diensterbringer geregelt werden.
- Es ist nur der für die eigene Hochschule gültige Rechtsrahmen zu berücksichtigen.
- Gespeicherte Daten werden nicht (durch Dritte) zu kommerziellen Zwecken verwertet.

2. Hochschulübergreifende kooperative Cloud-Dienste (auch „Community-Cloud“)

Hierbei handelt es sich um Cloud-Dienste, die durch andere deutsche Hochschulen oder Einrichtungen im Hochschulumfeld außerhalb der eigenen Hochschule betrieben werden und explizit Mitgliedern der eigenen Hochschule zur Nutzung angeboten werden. Ein solcher Dienst ist beispielsweise der DFN-Videokonferenzdienst.

Eigenschaften

Solche Dienste zeichnen sich u.a. durch die im Folgenden beschriebenen Eigenschaften aus:

- Die Daten werden in der jeweils anbietenden Hochschule oder Einrichtung (z.B. dem DFN-Verein) verarbeitet.
- Der Betrieb eigener (virtualisierter) Hardware (Rechen- und Speicherkapazität) entfällt.
- Der Betrieb erfolgt häufig an einem oder an zwei Standorten. Es gibt wenige hochschulübergreifende Betriebsmodelle.
- Es werden keine Backups in der eigenen Hochschule angeboten und verwaltet.
- Der Aufwand für den technischen Betrieb des jeweiligen Angebots entfällt.
- Die Verantwortung für die Betreuung der Nutzenden muss geregelt werden und es müssen entsprechende Schnittstellen abgestimmt und bereitgestellt werden. Oft verbleibt die Verantwortung für den First-Level-Support in der nutzenden Hochschule.
- Die konkrete Ausgestaltung des jeweiligen Dienstes obliegt der anbietenden Hochschule oder einem (hochschulübergreifenden) Lenkungsgremium. Eine genaue Anpassung (aus der Sicht der Nutzenden) an lokale Anforderungen bzw. die lokale Vornahme von Optimierungen ist nur in begrenztem Rahmen möglich.
- Die Rechtevergabe und Zugriffsverwaltung für die Nutzenden muss hochschulübergreifend technisch und organisatorisch geregelt werden.
- Dienstgütevereinbarungen sind ggf. möglich, bedürfen aber der Abstimmung aller beteiligten Hochschulen. Die zur Einhaltung solcher Vereinbarungen erforderlichen personellen und

finanziellen Ressourcen müssen ggf. auf alle Nutzenden umgelegt werden. Für unkritische Dienste sind „Best Effort“-Ansätze denkbar.
- Es gilt deutsches Recht, in einigen Bereichen, z.B. dem Datenschutz sind aber die verschiedenen Rechtsauslegungen der einzelnen Bundesländer zu beachten.
- Gespeicherte Daten werden nicht (durch Dritte) zu kommerziellen Zwecken verwertet.

3. Public-Cloud-Dienste („Off-Premises”)

Als „Public-Cloud“ oder „Off-Premises“-Dienste werden Cloud-Dienste bezeichnet, die auf der Infrastruktur eines externen Anbieters betrieben und über das Internet den Nutzenden der Hochschule angeboten werden.

Eigenschaften

Off-Premises-Dienste zeichnen sich u.a. durch die im Folgenden beschriebenen Eigenschaften aus:

- Die Serviceerbringung einschließlich der Datenhaltung erfolgt durch einen externen Anbieter, in fast allen Fällen mit Sitz außerhalb Deutschlands, meistens in den USA.
- Der Betrieb erfolgt in Rechenzentren der Dienstanbieter oder von diesen beauftragten (Cloud-)Anbietern (z.B. AWS, Azure) und erfordert keine (oder nur sehr wenig) eigene Hardware.
- Im Allgemeinen werden sie weltweit verteilt redundant betrieben.
- Backups werden in der Regel nicht oder nur gegen Aufpreis bereitgestellt. Lokale Sicherungen seitens der Hochschule gestalten sich aufgrund fehlender Schnittstellen meist schwierig.
- Es fällt kein Aufwand für den technischen Betrieb des Angebots an, jedoch u.U. zur Anbindung und Integration lokaler Systeme in der eigenen Hochschule, insbesondere zur Authentifizierung
- Support und Dokumentation erfolgen weitgehend durch den externen Anbieter, eine zusätzliche lokale Anlaufstelle für „kleine“ Probleme ist aber weiterhin im Sinne der Nutzendenzufriedenheit anzuraten. Sofern kein 1st-Level-Support durch den Anbieter geleistet wird, ist Support durch den Auftraggeber (die Hochschule) zu leisten, auch wenn dabei durch die Support-Mitarbeitenden der 2nd-Level-Support des Anbieters genutzt wird.
- Die Nutzenden bzw. die Hochschulen begeben sich in die Abhängigkeit des Anbieters. Die konkrete Ausgestaltung des Dienstes obliegt dem Anbieter und ist i. A. nicht verhandelbar. Eine Anpassung an lokale Bedürfnisse ist nicht möglich. Kurzfristige einseitige funktionelle Änderungen durch den Anbieter oder Lizenzbedingungen sind stets möglich.
- Die Rechtevergabe und Zugriffsverwaltung sind von den gegebenen Möglichkeiten des Angebots abhängig.

- Es gibt verschiedene Ausprägungen von Dienstgütevereinbarungen in Abhängigkeit des finanziellen Einsatzes, z.B. bzgl. Verfügbarkeit oder Datensicherheit. Je nach Dienstgütevereinbarung wird z.B. die Datensicherung durch den Provider garantiert oder auch nicht. Bei „kostenlosen“ Diensten ist dies meist nicht der Fall.
- Anbieter mit Firmensitz im außereuropäischen Ausland unterliegen auch in deren europäischen Firmensitzen i.A. der Rechtsprechung des Landes, in dem die Konzernmutter ihren Sitz hat.
- Insbesondere bei (vermeintlich) kostenlosen Diensten räumen sich Anbieter u.U. großzügige Nutzungsrechte an den gespeicherten Daten ein, was sie damit kostenpflichtig macht: Nutzende zahlen mit der erzwungenen Überlassung der Nutzungsrechte an ihren Daten. Eine derartige Überlassung der Nutzungsrechte kann auch bei (monetär) kostenpflichtigen Diensten vorkommen, meist dann in kleinerem Umfang.

Präsidiumsbeschluss vom 17. Dezember 2025, Senatsbeschluss vom 21. Januar 2026