DFN mitteilungen

Überall dabei

Die neuen Videokonferenzverträge im DFN

Gemeinsam gegen Cyberangriffe!
Mit MISP Threat Sharing

KI als Lehrkraft?
Das Projekt „Prof. Digital Twin“

9 770177 689001

Impressum

Herausgeber: Verein zur Förderung
eines Deutschen Forschungsnetzes e. V.

DFN-Verein
Alexanderplatz 1, 10178 Berlin
Tel.: 030 - 88 42 99 - 0
Fax: 030 - 88 42 99 - 370
Mail: presse@dfn.de
Web: www.dfn.de

ISSN 0177-6894

Redaktion: Maimona Id, Nina Bark
Lektorat: Angela Lenz
Gestaltung: Labor3 | www.labor3.com
Druck: ARNOLDprint service GmbH

Fotonachweis
Titel: lifeonwhite/magnific
Rückseite: j_markow/iStock

Peter Gietz
Geschäftsführer von DAASI International und Mitglied im Verwaltungsrat des DFN-Vereins

Noch bevor es das World Wide Web gab, faszinierte mich als junger Religionswissenschaftler und Indologe der scheinbar grenzenlose Zugriff auf Forschungsdaten und wissenschaftliche Ressourcen aus der ganzen Welt – damals noch über das File Transfer Protocol (FTP). Seitdem war mir klar, welche Bedeutung das Internet einmal haben würde und warum ich mich mit Internetprotokollen auskennen wollte.

In den frühen 90er-Jahren arbeitete ich als wissenschaftlicher Mitarbeiter am Zentrum für Datenverarbeitung der Universität Tübingen (ZDV) in den vom damaligen Bundesministerium für Bildung und Forschung (BMBF) geförderten DFN-Forschungsprojekten zu den Verzeichnisdiensten X.500 und LDAP, später als Projektleiter des DFN-Projekts „Aufbau eines Directory Competence Center (DCC)“. Aus diesem Projekt haben meine Frau Karin und ich die private Firma DAASI International als Open-Source-Firma ausgegründet, die sich auf Verzeichnisdienste und Identity und Access Management spezialisiert hat und deren Geschäftsführer ich seit nunmehr 26 Jahren bin. Zur richtigen Zeit am richtigen Ort: Der entscheidende Impuls für meinen Weg in die Selbstständigkeit kam vom DFN. Seitdem verbindet uns eine über Jahrzehnte gewachsene Partnerschaft, getragen von gegenseitigem Vertrauen – technisch übersetzt: Trust & Identity.

Wenn wir heute über digitale Souveränität sprechen – und in Europa wird sie intensiver denn je diskutiert –, führt kein Weg am Identitätsmanagement vorbei. Das DFN-Projekt DCC legte Ende der 90er-Jahre dafür eine wichtige Grundlage und trug maßgeblich zur Entwicklung föderierter Authentifizierungsinfrastrukturen (AAI) in Deutschland bei. Ich erinnere mich noch gut an das initiale Treffen zur DFN-AAI. In den rund 20 Jahren ihres Bestehens ist die DFN-AAI zu einem unverzichtbaren Teil digitaler Forschungsinfrastrukturen geworden. Wir wissen, dass sich die Einsatzmöglichkeiten digitaler Identitäten schnell weiterentwickeln werden. Hier müssen wir gemeinsam darauf achten, dass die informationelle Selbstbestimmung und digitale Souveränität als hohes Gut erhalten bleiben.

Dieses Jahr höre ich nicht nur als Geschäftsführer der DAASI International auf, sondern beende auch meine Arbeit im DFN-Verwaltungsrat, dessen Mitglied ich drei Jahre war. Dieses Engagement betrachte ich als krönenden Abschluss meiner Karriere. Ich freue mich, dass ich meine Erfahrungen und Kompetenzen im Bereich Federated Identity and Access Management (IAM) einbringen konnte. Denn damit schließt sich der Kreis eines gemeinschaftlichen, nachhaltigen und sinnstiftenden Engagements für die Wissenschaft. Ich wünsche dem DFN-Verein und seinen Mitgliedern viel Erfolg dabei, auch zukünftige Anforderungen weiterhin mit Bedacht und Engagement zu erfüllen, und Mut, den Weg zu digitaler Souveränität weiter konsequent zu verfolgen.

Ihr Peter Gietz

Inhalt

Gut vernetzt auf hoher See
Dr. Johannes Karstensen verrät, wie Forschungsschiffe mit dem Festland kommunizieren

Bye, Bye DFN-NetNews
Zum Jahresende 2026 wird der Social-Media-Pionier eingestellt

Preparation matters
TALON, Europe's first large-scale, cross-border crisis simulation for NRENS in Europe

Wissenschaftsnetzt

Gut aufgestellt – die neuen DFN-Rahmenverträge für Web- & Videokonferenzen
von Dirk Bei der Kellen **6**

Gut vernetzt auf hoher See
Interview von Maimona Id **10**

Von Grund auf neu gedacht – der DFN-Terminplaner 7
von Torsten Kersting **14**

Auf Herz und Nieren zertifiziert
von Michael Röder **16**

Bye, Bye DFN-NetNews – Abschied von einem geschätzten Wegbegleiter
von Vera Heinau **18**

Kurzmeldungen **21**

Sicherheit

Vertrauen schafft Sicherheit – das MISP Threat Sharing
von Christine Kahl **24**

Sicherheit aktuell **26**

Campus

Lehrkraft im Doppelpack: das Projekt „Professor Digital Twin"
von Matthias Baume **28**

NHR-Verbund stellt Datenspeichersysteme für die NFDI bereit
von Matthias S. Müller, Marius Politze und Philipp Wieder **32**

Taugt Backup als Archiv?
Thomas Eifert **35**

Open Source VDI für Forschung und Lehre
von Rafael Gieschke, Michael Scherle und Dirk von Suchodoletz **38**

International

International Newsflashes **41**

LesREN Launches – Building an Research and Education Network Focused on Community Impact
von Eric Gedenk **42**

TALON: Europe's First Cross-Border Crisis Exercise for NRENs
von Rosanna Norman **44**

Forschung

Exchanging Palm Oil Plantations for Designer Enzymes
von Eric Gedenk **46**

Digitale Souveränität im Fokus
das DFN-Diskussionsforum der Kanzlerinnen und Kanzler 2026

Recht

Alles begann mit einer Frage – die Forschungsstelle Recht im DFN
Interview von Maimona Id und Annette Rülke **49**

Anonym oder pseudonym? Alles ist möglich.
von Anna Maria Yang-Jacobi **52**

Mit digitalen Wasserzeichen zu klareren Informationsökosystemen?
von Paul Friedl **57**

DFN-Verein

Digitale Souveränität im Fokus – das DFN-Diskussionsforum der Kanzlerinnen und Kanzler 2026
von Nina Bark und Maimona Id **60**

DFN unterwegs **62**

DFN live **65**

Überblick DFN-Verein **68**

Die Mitgliedseinrichtungen **70**

Autorinnen und Autoren dieser Ausgabe im Überblick

1 Dr. Dirk Bei der Kellen, DFN-Verein (beiderkellen@dfn.de); **2** Maimona Id, DFN-Verein (id@dfn.de); **3** Torsten Kersting, DFN-Verein (kersting@dfn.de); **4** Michael Röder, DFN-Verein (roeder@dfn.de); **5** Vera Heinau, Freie Universität Berlin (vera.heinau@fu-berlin.de); **o. Abb.** Christine Kahl, DFN-CERT (kahl@dfn.de); **6** Dr. Matthias Baume, Technische Universität München (matthias.baume@tum.de); **7** Prof. Dr. Matthias S. Müller, RWTH Aachen (mueller@itc.rwth-aachen.de); **8** Dr. rer. nat. Marius Politze, RWTH Aachen (politze@itc.rwth-aachen.de); **9** Professor Dr. Philipp Wieder, GWDG (philipp.wieder@gwdg.de); **10** Dr. rer. nat. Thomas Eifert, RWTH Aachen (eifert@itc.rwth-aachen.de); **o. Abb.** Rafael Gieschke, Universität Freiburg (rafael.gieschke@rz.uni-freiburg.de); **o. Abb.** Michael Scherle, Universität Freiburg (michael.scherle@rz.uni-freiburg.de); **11** Dr. Dirk von Suchodoletz, Universität Freiburg (dirk.von.suchodoletz@rz.uni-freiburg.de); **12** Eric Gedenk, Impact Science Communication (info@impact-scicomm.com); **13** Rosanna Norman, GÉANT Association (rosanna.norman@geant.org); **o. Abb.** Annette Rülke, DFN-Verein (ruelke@dfn.de); **14** Anna Maria Yang-Jacobi, Forschungsstelle Recht im DFN (a.yang-jacobi@fu-berlin.de); **15** Dr. Paul Friedl, Forschungsstelle Recht im DFN (paul.friedl@hu-berlin.de); **16** Nina Bark, DFN-Verein (bark@dfn.de)

Gut aufgestellt – die neuen DFN-Rahmenverträge für Web- & Videokonferenzen

Die Auswahl an Web- und Videokonferenzsystemen wächst – und mit ihr die Anforderungen. Seit dem 1. März 2026 können teilnehmende Einrichtungen im Wissenschaftsnetz die neuen Rahmenverträge für cloudbasierte Web- und Videokonferenzdienste abrufen. Sie bieten Orientierung, stellen Einrichtungen aber auch vor strategische Entscheidungen. Ein Überblick über Anbieter, Unterschiede und Auswahlkriterien.

Text: **Dirk Bei der Kellen** (DFN-Verein)

In Forschung und Lehre sind cloudbasierte Web- und Videokonferenzsysteme längst zur Selbstverständlichkeit geworden – und die Rahmenverträge des DFN-Vereins mittlerweile ein Klassiker. Bereits 2021 reagierte der DFN-Verein mit einer ersten Ausschreibung auf die schlagartig gestiegene Nachfrage und die Erfahrungen aus der damaligen Umstellung auf digitale Arbeits- und Lehrformate. Was damals als schnelle Antwort auf eine akute Situation begann, hat sich inzwischen als dauerhafter Service für am Wissenschaftsnetz teilnehmende Einrichtungen verstetigt und ist fester Bestandteil des digitalen Arbeitsalltags.

Foto: L3/KI-gen.

Mit der erfolgreich abgeschlossenen europaweiten Neuausschreibung der Rahmenverträge stehen seit dem 1. März 2026 innovative Produkte und attraktive Angebote zur Verfügung, die den ungebrochen hohen Bedarf an hybriden Formaten, virtueller Projektarbeit und standortübergreifender Zusammenarbeit zuverlässig unterstützen. Mit den neuen Rahmenverträgen können DFN-Teilnehmer nun wieder bequem auf eine kuratierte Auswahl zugreifen, ohne selbst ausschreiben zu müssen. Darüber hinaus ist die Lizenzbestellung noch einfacher geworden: Das automatisierte Auswahl-Tool des

Videoconference & Collaboration Centers (VCC) im DFN-Verein hilft dabei, den umfangreichen und detaillierten Anforderungskatalog nach priorisierten Kategorien zu filtern.

Mit jetzt insgesamt zehn Providern konnte die Vielfalt an Produkten noch einmal vergrößert werden. Neben den vier bewährten Diensten Zoom X (Telekom Deutschland GmbH), Cisco Webex (Deutsche Telekom Business Solutions GmbH), Microsoft Teams (DrVis Software GmbH) und BigBlueButton (Infra.run Service GmbH) aus den vorherigen Rahmenverträgen, sind nun sechs Neuzugänge am Start – darunter auch Produkte europäischer Hersteller: alfaview (alfaview GmbH), edudip (edudip GmbH), fairmeeting (fairkom Gesellschaft), meedio (Meedio GmbH), Rainbow (PKE Mediacom GmbH) sowie visavid(Auctores GmbH).

Die Rahmenverträge haben eine Laufzeit von 24 Monaten und können über zwei Verlängerungsoptionen um jeweils zwölf Monate erweitert werden. Insgesamt ist so eine Vertragslaufzeit von bis zu 48 Monaten möglich.

Anforderungen und Unterschiede: worauf es bei der Auswahl ankommt

Aufgrund stetiger Neuentwicklungen im Bereich cloudbasierter Videosysteme – etwa bei Barrierefreiheit und KI-Integration – sowie aktueller gesetzlicher Änderungen erarbeitete das DFN-Cloud-Team die Anforderungen für die Neuausschreibung gemeinsam mit der Arbeitsgruppe VIKTAS (Videokommunikationstechnologien und ihre Anwendungsszenarien) der Deutschen Initiative für Netzwerkinformation e. V. (DINI) sowie dem Arbeitskreis Medienkonzepte und Technologien der Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V. (ZKI).

Mit der wachsenden Zahl an Rahmenverträgen wird die Auswahl für ein passendes Angebot außerdem zunehmend komplexer. Da alle Anbieter die definierten Mindestanforderungen erfüllen, reicht ein reiner Preisvergleich für eine belastbare Entscheidung nicht aus. Entscheidend sind die Unterschiede in Qualität, Funktionsumfang und strategischer Ausrichtung der Dienste.

RAHMENVERTRAGSPARTNER

- alfaview GmbH
- PKE Mediacom GmbH
- Infra.run Service GmbH
- DrVis Software GmbH
- edudip GmbH
- Auctores GmbH
- fairkom Gesellschaft
- Deutsche Telekom Business Solutions GmbH
- Meedio GmbH
- Telekom Deutschland GmbH

Als zentrale Orientierung dient der umfangreiche Anforderungskatalog der Ausschreibung, der insgesamt 129 Fragen umfasst. Aufbauend auf der ersten Ausschreibung wurden zusätzliche Themenfelder aufgenommen – darunter digitale Resilienz, KI, digitale Souveränität, hybride Raumtechnologien und weitergehende Anforderungen an die Barrierefreiheit. Letztere haben an Bedeutung gewonnen: Das merkt man besonders bei den Funktionen KI-gestützter Transkription, die für hör-eingeschränkte Personen einen deutlichen Mehrwert bieten.

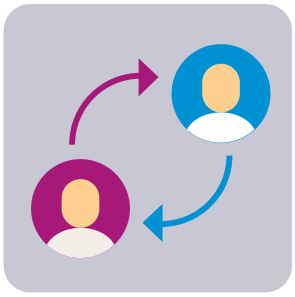
Einige Themenfelder lassen sich jedoch nicht ohne Weiteres in feste Standards übersetzen. Das zeigt sich insbesondere beim Thema digitale Souveränität. Hier geht es um transparente digitale Lieferketten, nachvollziehbare Datenverarbeitung, offene Schnittstellen und eine möglichst geringe Abhängigkeit von einzelnen Anbietern. Während einige Anbieter konsequent auf Open-Source-Modelle und nachvollziehbare

Entwicklungsprozesse setzen, verweisen andere stärker auf etablierte IT-Sicherheits- und Data-Compliance-Ansätze.

Auch digitale Resilienz spielt eine zunehmend wichtige Rolle. Dabei geht es nicht nur um technische Schutzmaßnahmen, sondern auch um organisatorische Vorkehrungen – etwa regelmäßige Notfallübungen für den Umgang mit Cyberangriffen. Die meisten Anbieter führen nach eigenen Angaben mindestens einmal jährlich entsprechende Übungen durch. Für Einrichtungen bedeutet das: Die Wahl eines Angebots ist nicht nur eine Preisfrage, sondern eine strategische Entscheidung – abhängig davon, welche Prioritäten gesetzt werden in puncto Integrationsfähigkeit, Barrierefreiheit, Sicherheitsniveau oder zusätzlicher Services.

Konkrete Beispiele aus den Rahmenverträgen

Die Unterschiede zwischen den Angeboten zeigen sich besonders deutlich, wenn man konkrete Umsetzungen betrachtet. So positioniert sich beispielsweise BigBlueButton klar im Open-Source-Umfeld. Der Anbieter argumentiert nicht allein mit dem Standort Deutschland, sondern verweist auf sein weltweites Engagement in der Open-Source-Community sowie auf einen vollständig offenen Hosting-Stack. Damit rückt weniger der geografische Standort als vielmehr die Transparenz und Offenheit der gesamten Software-Lieferkette in den Mittelpunkt.



In eine ähnliche Richtung argumentiert fairkom. Das Unternehmen setzt ebenfalls auf Open-Source-Software und betont darüber hinaus die Unterstützung föderierter Identitätsinfrastrukturen wie der DFN-AAI sowie deren Einbindung in internationale Föderationen im Umfeld der GÉANT Association, wodurch eine herstellerunabhängige und verteilte Anmeldung ermöglicht wird.

Anbieter proprietärer Plattformen verfolgen einen anderen Ansatz. So verweist beispielsweise DrVis Software GmbH – Anbieter von Microsoft Teams – auf die sogenannte EU Data Boundary, die eine Datenverarbeitung innerhalb der Europäischen Union ermöglichen soll. Dieser Ansatz adressiert zentrale Datenschutzanforderungen, trifft jedoch keine unmittelbaren Aussagen zur Offenheit von Software-Lieferketten oder zur langfristigen technologischen Unabhängigkeit.

Auch bei ergänzenden Services zeigen sich Unterschiede. So bietet die Telekom Deutschland GmbH neben der Bereitstellung der Plattform auch Dienstleistungen zur professionellen Produktion von Webinaren an – ein Angebot, das insbesondere für Einrichtungen mit starkem Fokus auf digitale Lehre interessant sein kann und interne Ressourcen entlastet.

Darüber hinaus kann auch die medientechnische Ausstattung ein entscheidender Faktor sein. Über das Portfolio der Deutschen Telekom Business Solutions GmbH besteht beispielsweise Zugang zu Hardware-Lösungen der Cisco Systems GmbH. Neben Netzwerkkomponenten bietet Cisco ein auf Videokonferenzplattformen abgestimmtes medientechnisches Ökosystem aus Mikrofonen, Lautsprechern und Displays an, das insbesondere für hybride Veranstaltungs- und Lehrszenarien relevant ist.

Innovation und Weiterentwicklung während der Laufzeit

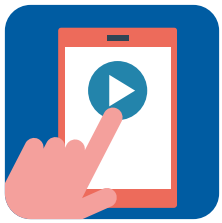
Ungeachtet der vergleichsweise langen Laufzeit von bis zu vier Jahren bleibt der Markt für cloudbasierte Kommunikationsdienste stark in Bewegung. Neue Funktionen, Sicherheitsanforderungen und Integrationsmöglichkeiten entstehen in kurzen Entwicklungszyklen. Deshalb ist ein kontinuierlicher Austausch zwischen Anbietern und dem DFN-Verein ein wichtiger Bestandteil der Zusammenarbeit. Regelmäßige Abstimmungen sorgen hier dafür, dass technische Neuerungen frühzeitig aufgegriffen werden und die eingesetzten Dienste auch während der Vertragslaufzeit auf dem aktuellen Stand bleiben.

So sichern die Rahmenverträge nicht nur rechtlich ab, sondern ermöglichen technologische Weiterentwicklung. Konkret profitieren Einrichtungen während der Laufzeit unter anderem durch:

- **SaaS-Modelle mit kontinuierlicher Weiterentwicklung:** Updates, neue Funktionen und Sicherheitsverbesserungen werden direkt in die bestehenden Dienste integriert – ohne dass eine neue Beschaffung erforderlich ist.
- **zukunftssichere Leistungskataloge:** Neue Module und Funktionen können innerhalb des vereinbarten Leistungsrahmens ergänzt werden.
- **aktualisierte Sicherheits- und Datenschutzstandards:** Anpassungen an regulatorische oder technische Anforderungen werden kontinuierlich berücksichtigt.
- **flexible Skalierung:** Nutzungsumfang und Kapazitäten lassen sich bedarfsgerecht anpassen.

Neue Vorgehensweise beim Bezug

Die größte Neuerung bei der Nutzung der neuen Rahmenverträge betrifft die Bestellgrundlage: Künftig erfolgt die Beauftragung auf Basis von EVB-IT Cloud.



Im Vergleich zu den zuvor genutzten EVB-IT-Systemen ist dieses Vertragswerk deutlich kompakter und damit einfacher zu handhaben. Die Vertragsunterlagen werden von den Anbietern in der Regel bereits vorausgefüllt bereitgestellt. Für Einrichtungen reduziert sich der Aufwand damit auf wenige Angaben – etwa zur Anzahl der Lizenzen, zur Laufzeit und zum Starttermin. Dennoch kann die Umstellung Anpassungen in den internen Beschaffungsprozessen der Einrichtungen erforderlich machen.

Neu ist außerdem eine automatische Verlängerungsoption: Sofern der Vertrag nicht spätestens drei Monate vor Ablauf gekündigt wird, verlängert er sich automatisch. Diese sogenannte „Auto-Renewal"-Regelung soll Planungssicherheit schaffen und Unterbrechungen in der Leistungserbringung vermeiden. Gleichzeitig erfordert sie jedoch, dass Einrichtungen Laufzeiten aktiv im Blick behalten – etwa durch ein bewusst gesetztes Enddatum oder entsprechende Erinnerungen.

Alternative Lizenzmodelle prüfen lohnt sich

Der Blick in die Preislisten zeigt: Ein direkter Vergleich der Angebote ist nicht immer einfach. Insbesondere Anbieter, die zunächst mit geringeren Abrufmengen rechnen, liegen in den kleineren Mengenstaffeln teilweise über den Preisen etablierter Anbieter. Gleichzeitig haben alle Rahmenvertragspartner angekündigt, flexible Lizenzmodelle anzubieten – darunter beispielsweise spezielle Education Bundles für Hochschulen und Forschungseinrichtungen.

Solche Modelle basieren häufig auf der Anzahl der Vollzeitäquivalente einer Einrichtung oder bieten statt Named-Host-Lizenzen auch Concurrent-Host-Modelle an. Gerade für größere Einrichtungen können diese Varianten deutlich wirtschaftlicher sein als die Standardpreise in den Preisblättern.

Hinzu kommt: Einige Anbieter haben bereits signalisiert, zu Beginn der Rahmenvertragslaufzeit mit besonderen Preisaktionen in den Markt zu gehen. Es kann sich daher lohnen, gezielt nach alternativen Lizenzmodellen oder aktuellen Aktionen zu fragen.

Für Einrichtungen, die einen Wechsel zwischen Anbietern in Betracht ziehen, eröffnen sich zusätzliche Einsparpotenziale, die ihren Haushalt entlasten können. Die angebotenen Systeme ähneln sich in Funktionsumfang und Bedienlogik häufig stark, sodass ein Wechsel in der Praxis meist mit überschaubarem Aufwand möglich ist.

Fazit

Die neuen Rahmenverträge bieten eine breite Auswahl leistungsfähiger Web- und Videokonferenzlösungen. Gleichzeitig zeigt sich: Die Wahl eines Systems ist heute mehr als eine reine Preisentscheidung. Unterschiede in Architektur,Interoperabilität, Integration, Nachnutzung, Sicherheit und ergänzenden Services machen eine bewusste, strategische Auswahl notwendig.

Ein wichtiger Schritt dabei ist der direkte Austausch mit den Anbietern. Alle Rahmenvertragspartner haben signalisiert, weiterführende Informationen bereitzustellen und individuelle Fragen beispielsweise in den vom DFN-Verein organisierten Provider-Webinaren zu beantworten. Zudem stehen Testzugänge zur Verfügung – eine gute Möglichkeit, Funktionen, Bedienbarkeit und Integration in der Praxis zu prüfen und die Auswahl belastbar zu begründen.

Außerdem gilt: Videokonferenzsysteme sind mittlerweile Alltagswerkzeuge geworden. Für übertriebene Markentreue gibt es wenig Anlass. Die hohe Beliebtheit eines Angebots in früheren Rahmenverträgen ist kein ausreichendes Auswahlkriterium. Entscheidend sind Qualität, Service und Verlässlichkeit über den gesamten Lebenszyklus hinweg.

Diese Qualitätsmaßstäbe gelten sowohl für die Funktionalität einer Software und für die Übertragungsgüte von Audio- und Videodaten als auch für die zeitnahe Bereitstellung relevanter Dokumente des Datenschutzes und die pünktliche Zuarbeit von Nutzungsberichten. Der gesamte Dienstlebenszyklus – von der vertrieblichen Unterstützung bei der Produktauswahl über die Inbetriebnahme in einer Einrichtung bis zum möglichen Providerwechsel – muss in diese Qualitätsbetrachtung einfließen.

Wer die Entscheidung aktiv gestaltet, Angebote kritisch vergleicht und Entwicklungen kontinuierlich verfolgt, legt damit die Grundlage für eine langfristig tragfähige und zukunftssichere Kommunikationslösung. ◆

AUF DEM NEUESTEN STAND BLEIBEN?

Tragen Sie sich in die Cloud-Video-Mailingliste ein:
https://www.listserv.dfn.de/sympa/info/cloudvideo

Weitere Informationen gibt es auf der DFN-Webseite unter:
https://www.dfn.de/dienste/cloud/

Beratung und Unterstützung bietet das Videoconference & Collaboration Center (VCC) an:
https://tu-dresden.de/zih/vcc

Gut vernetzt auf hoher See

Mit der METEOR IV wird das GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel im Frühjahr 2027 ein hochmodernes, weltweit einsetzbares Forschungsschiff mit Schwerpunkt Atlantik in Betrieb nehmen. Doch wie wird aus einem Forschungsschiff, das Tausende Kilometer vom nächsten Hafen entfernt ist, ein vernetzter Arbeitsplatz? Und wie funktioniert die Zusammenarbeit auf Distanz? Die Antworten hat Dr. Johannes Karstensen, Leiter der Abteilung Seegängige Technologien.

Als erfahrener Expeditionsleiter weiß Dr. Johannes Karstensen, worauf es bei der technischen Ausstattung eines Forschungsschiffes ankommt | *Foto: Janne Lene Pole/GEOMAR*

Forschung wird heute über Disziplinen und Standorte hinweg immer stärker vernetzt betrieben. Wie habe ich mir das auf einem Forschungsschiff auf hoher See vorzustellen?
Ein Forschungsschiff wirkt zwar nach außen wie eine eigene abgeschlossene Welt, tatsächlich ist es aber Teil eines größeren, vernetzten Systems. Einerseits werden vom Land aus gezielt Informationen abgerufen, um die Experimente auf See zu unterstützen. Andererseits wird die Forschung auf hoher See über Telepräsenz erlebbar – und sogar aktiv beeinflussbar. Die Vernetzung von Land und See gehört heute zum Forschungsalltag.

Telepräsenz findet auf unterschiedlichsten Ebenen statt: Das kann der Stream für die interessierte Öffentlichkeit sein oder der wissenschaftliche Diskurs von Forschenden via Videokonferenz. Hier nutzen wir übrigens verschiedene Anbieter aus den DFN-Rahmenverträgen. Der regelmäßige Datenaustausch zwischen dem Schiff, auf dem die Rohdaten gewonnen, und dem Rechenzentrum, in dem die Daten ausgewertet werden, ist Teil von Remote-Wissenschaft.

Remote-Wissenschaft hört sich spannend an. Wie können Forschende denn aus der Ferne aktiv an Experimenten beteiligt werden?
Zunächst erst einmal zu den Experimenten: Mit unseren Remote Operating Vehicles (ROVs) – das sind mit dem Schiff verbundene, aber ferngesteuerte Unterwasserfahrzeuge – untersuchen wir Phänomene wie die Black Smoker. Die schwarzen Rauchsäulen aus dem Meeresboden entstehen in Tausenden Metern Tiefe aufgrund vulkanischer Aktivität. Sie erreichen Temperaturen bis zu 400 °C und beherbergen wegen des mineralreichen Wassers ganz besondere Lebensformen. Mithilfe von ROVs ist es uns in Tiefen bis 6 000 Meter möglich, unterschiedliche Messungen zu machen und Proben zu nehmen.

Ein ROV kann man sich als einen riesigen, mehrere Tonnen schweren Kasten

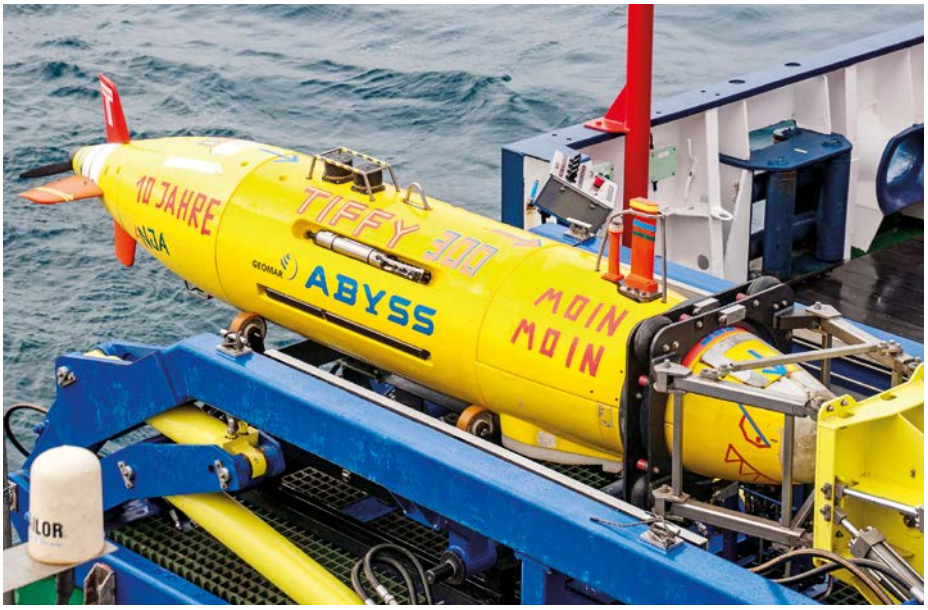
vorstellen – auf den ersten Blick eher unscheinbar, aber vollgepackt mit Technik. An Bord sind unterschiedliche Kameras, Lichtquellen und Sensoren, die kontinuierlich Daten wie Temperatur, Salz- und Sauerstoffgehalt sowie die Trübung des Wassers messen. Gesteuert wird das Fahrzeug von meist zwei Pilotinnen oder Piloten vom Schiff aus. Eine Person steuert das Vehikel, das sich mit Propellern über dem Meeresboden manövrieren lässt, die andere bedient die Greifarme. Aber nicht nur das: Als technische Spezialisten – etwa für Bildgebung, Optik, Netzwerke oder Hydraulik – müssen sie gleichzeitig eventuell auftretende Störungen im Blick haben und gegebenenfalls beheben. Diese Arbeit verlangt Konzentration, ist anstrengend und teils hektisch, sodass die Teams regelmäßig wechseln müssen.

> So können wir uns Forschende aus den unterschiedlichsten Disziplinen mit an Bord holen.

Mit in dem engen Kontrollraum an Bord des Schiffes sitzen auch die Wissenschaftlerinnen und Wissenschaftler, die anhand der Livebilder aus der Tiefe Anweisungen geben – etwa zur Navigation der ROVs oder zur gezielten Probenentnahme. Da nicht immer alle Fachleute an Bord eines Schiffes sein können, wird immer häufiger auch mit „Live"-Übertragungen per Videokonferenz experimentiert. Dort können weitere Expertinnen und Experten interaktiv an Versuchen teilnehmen und gegebenenfalls auch in das Geschehen eingreifen. So können wir uns Forschende aus den unterschiedlichsten Disziplinen mit an Bord holen. Auf diese Weise funktioniert verteiltes Arbeiten.

Dafür braucht es doch mit Sicherheit sehr gutes Internet. Welche Kommunikationswege werden auf See genutzt?

Die Kommunikation auf den Ozeanen erfolgt heute überwiegend über etablierte Satellitensysteme, die eine zuverlässige



Autonom im Einsatz: Das AUV Abyss (Spitzname Tiffy) kann eigenständig Messungen durchführen und damit den Meeresboden kartieren | *Foto: Emanuel Wenzlaff/GEOMAR*

Verbindung zu Bodenstationen etwa in Europa oder Nordamerika ermöglichen – und damit in terrestrische global verbundene Netze wie das Wissenschaftsnetz des DFN-Vereins.

Das sah früher anders aus: Als ich angefangen habe, auf einem Forschungsschiff zu arbeiten, gab es lediglich Seefunk. Pro Woche war maximal ein Gespräch mit der Außenwelt möglich, bei dem typischerweise alle an Bord mithörten. Dann wurden Anfang der 2000er-Jahre Iridium-Satellitentelefone bezahlbar. Dadurch wurde die Kommunikation wesentlich komfortabler und privater. Heute haben wir durchgehend Internet mit hoher Bandbreite. Dadurch können wir unsere Experimente beispielsweise live streamen – etwa über YouTube. So kann die Öffentlichkeit an unserer Forschung partizipieren.

Für stabile Kommunikationsverbindungen setzen Forschungsschiffe auf „Hybridkommunikation", einen Mix aus verschiedenen Kommunikationswegen. In Küstennähe erfolgt die Anbindung häufig über Mobilfunknetze, ähnlich wie an Land. Auf hoher See übernehmen dann Satellitenverbindungen. Je nach Position wechseln moderne Systeme automatisch in die jeweils beste verfügbare Verbindung.

Wo liegen die größten Herausforderungen in der Kommunikation?

Eine Herausforderung bei der Satellitenkommunikation sind die teils sehr hohen Latenzzeiten – bei Telefonaten oder Internetnutzung sind sie noch tolerierbar. Kritisch wird es, wenn vom Land aus aktiv in die Arbeitsabläufe an Bord eingegriffen werden soll. So gibt es etwa Überlegungen, ROVs auch aus der Ferne zu steuern – was allerdings sehr schnelle Reaktionszeiten erfordert. Da geht es teils um Sekunden. In der Wissenschaft im Automatisierungssektor wird Remote Operation gerade intensiv getestet. Zusätzlich wird geschaut, welche Satellitensysteme die geringsten Latenzzeiten haben.

Welche Unterschiede gibt es denn bei den Satellitensystemen?

Klassische Satellitensysteme arbeiten meist mit geostationären Satelliten, die in rund 36.000 Kilometern Höhe fest über einem Punkt der Erde stehen. Durch diese Entfernung ist zwar die Abdeckung recht gut, aber die Bandbreiten sind eher gering. LEO(Low Earth Orbit)-Systeme wie etwa die der kommerziellen Anbieter

OneWeb oder Starlink verfügen über viele kleine Satelliten, die untereinander gut vernetzt und darum unabhängiger von einzelnen Bodenstationen sind. Durch ihre niedrigen Umlaufbahnen etwa 160 bis 2000 Kilometer über der Erde ist die Bandbreite sehr viel höher, und die Latenzen sind niedriger.

Insbesondere für die Meeresbeobachtung sind Satelliten von großer Bedeutung: zum einen für die Kommunikation, zum anderen stellen uns Erdbeobachtungssatelliten detailreiche Informationen über die Ozeanoberfläche bereit, etwa die Temperatur, die Höhe des Meeresspiegels oder die Ozeanfarbe. Satelliten liefern durchgehend Daten und Berechnungen, die an Land generiert und aufgearbeitet werden und die wir an Bord über Webdienste abrufen. Sie liefern uns Erkenntnisse über das Meer, die wir mit bloßem Auge nicht sehen können. Auf diese Weise können wir unsere Experimente sehr viel gezielter planen und ausführen.

Das heißt, ein großer Teil der Forschung findet inzwischen gar nicht mehr nur an Bord statt?

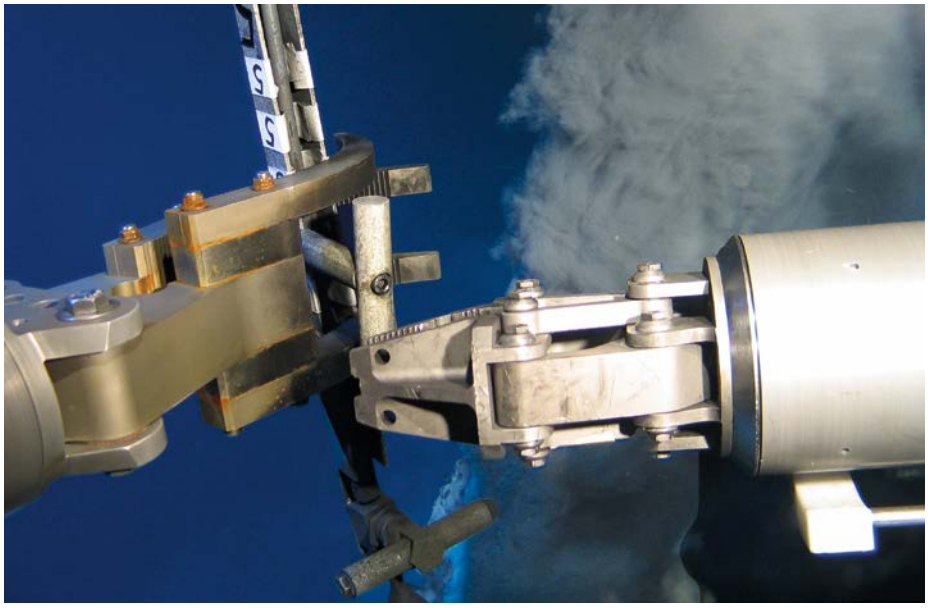
Die verschiedenen Messinstrumente, Sensoren und Kameras, die wir für unsere Experimente nutzen, sind zunehmend miteinander vernetzt – wie ein Schwarm. Das Schiff ist der Kontrollturm, in dem alle Informationen zusammengeführt werden und von dem aus der Schwarm ferngesteuert wird.

Darüber hinaus versuchen wir, unsere Apparaturen mit KI ein wenig schlauer zu machen: So sind Autonomous Underwater Vehicles (AUVs) – Roboter, die sich unter Wasser bewegen, ohne dass sie mit dem Schiff verbunden sind – mehr und mehr in der Lage, beispielsweise ihr Abtastverhalten eigenständig gezielter anzupassen, sodass Phänomene, an denen wir interessiert sind, viel besser vermessen werden können. Ein weiteres Beispiel sind die mit einem AUV aufgenommenen Fotos vom Meeresboden, die mithilfe von KI zu einem Mosaik zusammengeführt („gestitcht“) werden. Durch diese zielgenauen Einsätze können wir außerdem Energie sparen, denn wir sind in der Tiefe immer noch auf Akkus als Energiequelle angewiesen.

Bei den Experimenten auf See spielen auch digitale Zwillinge (Digital Twins) zunehmend eine Rolle: Sie bilden reale Umgebungen – etwa ozeanische Prozesse – als dynamische, digitale Modelle ab. Auf Basis von Messdaten lassen

Foto: Sarah Uphoff/GEOMAR

Dr. Johannes Karstensen | 1987 bis 1994 Studium der Physikalischen Ozeanographie an der Universität Hamburg | 1999 Promotion zum Dr. rer. nat. an der Universität Hamburg | 2000 bis 2002 Postdoktorand an der Columbia University (USA) | seit 2002 Wissenschaftler am GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel | 2010 Lehrtätigkeit an der King Abdullah University of Science and Technology (Saudi-Arabien) | 2016 bis 2019 Adjunct Professor an der Dalhousie University (Kanada) | seit 2025 Leiter Seagoing Technology am GEOMAR



Das ROV Kiel 6000 bei Probenahmen und Messungen am Black Smoker – heute noch vom Schiff aus gesteuert, in Zukunft möglicherweise von Land | *Foto: ROV-Team/GEOMAR*

sich so Entwicklungen simulieren und Vorhersagen treffen. Die dafür notwendigen Rechenleistungen sind jedoch enorm und können in der Regel nicht an Bord eines Forschungsschiffs erbracht werden. Stattdessen werden die Daten in leistungsfähigen Rechenzentren an Land verarbeitet. Die Ergebnisse fließen unvermittelt zurück an Bord und beeinflussen, wie Experimente fortgeführt werden – etwa welche Messreihen vertieft oder Parameter angepasst werden. So entsteht ein enger und schneller Austausch zwischen Forschung auf See und wissenschaftlicher Auswertung an Land.

Wie ist die METEOR IV beschaffen, um für diese Herausforderungen gerüstet zu sein?

Die METEOR IV ist wissenschaftlich sehr breit aufgestellt. Auf dem ganzen Schiff ist Glasfaser verbaut, um eine latenzfreie Umgebung zu garantieren. Außerdem

> „Das Schiff ist der Kontrollturm, in dem alle Informationen zusammengeführt werden."

sind Kühlräume für Hochleistungsrechner vorhanden. Insgesamt stehen der Wissenschaft rund 730 Quadratmeter Arbeitsfläche zur Verfügung – mit 17 spezialisierten Laboren, darunter Klimakammern und ein Labor für Atmosphärenchemie. So gibt es auch ausreichend Platz für Großgeräte wie ROVs oder AUVs. Einzigartig ist der Antrieb mit Voith-Schneider-Propellern. Damit können wir das Schiff sehr exakt auf Position halten – selbst bei Seegang –, was für viele Messungen und auch für den Umgang mit den Messrobotern entscheidend ist.

Dazu kommt eine hochmoderne technische Ausstattung: präzise Echolote, Forschungswinden für Einsätze bis in 12 000 Meter Tiefe und Systeme, die hochauflösende Videodaten in Echtzeit an Bord übertragen. Aber ein besonderes Anliegen ist es, auch jenseits aufwendig geplanter Experimente, Daten zu erheben. Die METEOR IV wird im Frühjahr 2027 in See stechen. In 2029 wird das Schiff die zentrale Beobachtungsplattform für die ein Jahr andauernde Forschungskampagne FUTURO vor der Westküste Afrikas sein.

GEOMAR

Mehr Infos zum neuen Forschungsschiff METEOR IV gibt es unter:

Foto: Marc Petrikowski

Warum ist es wichtig, zwischen den eigentlichen Experimenten zusätzlich Daten zu gewinnen?

Der Einsatz auf einem Forschungsschiff verursacht pro Tag Kosten im mittleren fünfstelligen Bereich. Es wird daher stets darauf geachtet, dass die Transitstrecken zwischen den Seegebieten, in denen geforscht wird, möglichst kurz sind. Gleichzeitig werden die unvermeidbaren Transitfahrten aber auch zur Datengewinnung genutzt: So wird etwa der Meeresboden kartiert und das Meerwasser mit Messgeräten analysiert.

Bei der Planung der METEOR IV war ich Teil eines Teams, das sich dafür eingesetzt hat, eine Messapparatur an Bord zu installieren, mit der auch während der Fahrt automatisiert Messungen zwischen der Meeresoberfläche und mehreren Hundert Metern Tiefe durchgeführt werden können. So entsteht ein „Profil" des Meeres entlang der zurückgelegten Strecke – ohne dass das Schiff dafür anhalten oder gezielt Messstationen anfahren muss.

Was fasziniert Sie an Ihrem Beruf?

Rund 70 Prozent der Erdoberfläche sind von Ozeanen bedeckt, die im Mittel knapp vier Kilometer tief sind. Da ist es nicht wirklich verwunderlich, dass wir über die Ozeane noch immer wenig wissen – und das meiste davon basiert auf sehr punktuellen Beprobungen.

Der Aspekt der ressourcenschonenden Ozeanbeobachtung fasziniert mich sehr: etwa der Einsatz von Messrobotern. Ein besonderer Reiz meiner Arbeit liegt darin, Forschungsschiffe so zu konzipieren, dass sie technologisch anschlussfähig bleiben – etwa im Hinblick auf zukünftige Entwicklungen bei Antriebssystemen. Für Forschungsschiffe sind die Anforderungen dabei oft komplexer als in der Handelsschifffahrt: Unsere Routen führen oft in abgelegene und logistisch schwer zugängliche Regionen, in denen die Versorgung mit alternativen Brennstoffen wie Methanol oder Ammoniak nicht zuverlässig sichergestellt werden kann.

Besonders motivierend ist für mich, Messdaten aufzuzeichnen, die dazu beitragen, das Meer als komplexes System besser zu verstehen. Ein System, das von ganz unglaublichen Lebewesen bewohnt wird und das einen riesigen Einfluss auf unser Leben an Land hat – besonders jetzt in Zeiten des menschengemachten Klimawandels.

Das Gespräch führte Maimona Id (DFN-Verein).

Von Grund auf neu gedacht – der DFN-Terminplaner 7

Seit über 15 Jahren unterstützt der DFN-Terminplaner die Wissenschaftscommunity dabei, Termine effizient zu koordinieren und abzustimmen – einfach, datenschutzkonform und ohne kommerzielle Hintergedanken. Mit Version 7, deren Fertigstellung für Sommer 2026 geplant ist, steht nun ein echter Generationenwechsel bevor – mit einem vollständig neuen Interface, modernen Webtechnologien im Unterbau und einem deutlich erweiterten Funktionsumfang.

Foto: rawpixel.com/Freepik

Text: **Torsten Kersting** (DFN-Verein)

Den optimalen Termin für das nächste Team-Meeting, die Videokonferenz oder Vorstandssitzung zu finden, kostet oft mehr Zeit als der Termin selbst. Genau hier setzt der DFN-Terminplaner an. Was 2009 als schlankes Koordinationswerkzeug begann, hat sich zu einem etablierten Dienst für Forschung, Lehre und Verwaltung entwickelt – mit monatlich Hunderttausenden Nutzerinnen und Nutzern. Version 7 soll diesen Weg nun konsequent weitergehen.

Drei Optionen, eine Entscheidung

Der Anstoß zur Überarbeitung kam von außen: Das Content-Management-System (CMS), auf dem der bisherige Terminplaner aufbaute, erreichte im vergangenen Jahr das Ende seines Lebenszyklus und wird nicht mehr gepflegt. Damit stand der DFN-Verein vor einer Weichenstellung. Drei Optionen lagen auf dem Tisch: die Anpassung des bestehenden Moduls an die CMS-Nachfolgeversion, die Migration auf einen Open-Source-Fork der bisherigen Systembasis – oder ein vollständiger Neuaufbau.

Die Wahl fiel auf die anspruchsvollste, aber zukunftsorientierteste Option. Ein Neuaufbau erlaubt es, alte Strukturen hinter sich zu lassen und den Dienst von Grund auf an aktuelle wie künftige Anforderungen anzupassen. Als technologische Basis dient das React-Framework – eine moderne, weitverbreitete Grundlage, die eine nachhaltige und skalierbare Weiterentwicklung des Dienstes sicherstellt.

Neu gedacht: Interface und mobile Nutzung

Sichtbarster Ausdruck des Wandels ist die Oberfläche. Das Interface wurde vollständig überarbeitet und konsequent nach dem Prinzip „Mobile First“ gestaltet. Abstimmungen sollen künftig am Smartphone ebenso flüssig funktionieren wie am Desktop. Besonderer Wert wurde dabei auf eine intuitive Bedienung gelegt. Damit trägt der Dienst dem flexiblen, ortsunabhängigen Arbeitsalltag in Wissenschaft und Forschung Rechnung.

Funktionale Erweiterungen im Überblick

Über die Optik hinaus bringt Version 7 eine Reihe von Neuerungen mit sich, die den Koordinationsalltag spürbar vereinfachen:

Integrierte Zeitzonenunterstützung:
Vorgeschlagene Termine werden automatisch an den jeweiligen Standort der Teilnehmenden angepasst – ein wichtiger Schritt für die zunehmend international vernetzte Forschungscommunity.

Sammelbearbeitungen:
Mehrere Termine lassen sich künftig durch die Auswahl im Kalender in einem Schritt anlegen und bearbeiten.

Verbesserte Auswertung:
Umfrageergebnisse können künftig analysiert und grafisch aufbereitet werden, um die Entscheidungsfindung zu beschleunigen.

Umfangreiche Erweiterungen bei Buchungslisten:

Mehrtägige Termine:
Erstmals lassen sich auch mehrtägige Veranstaltungen wie Konferenzen oder Workshops komfortabel abbilden.

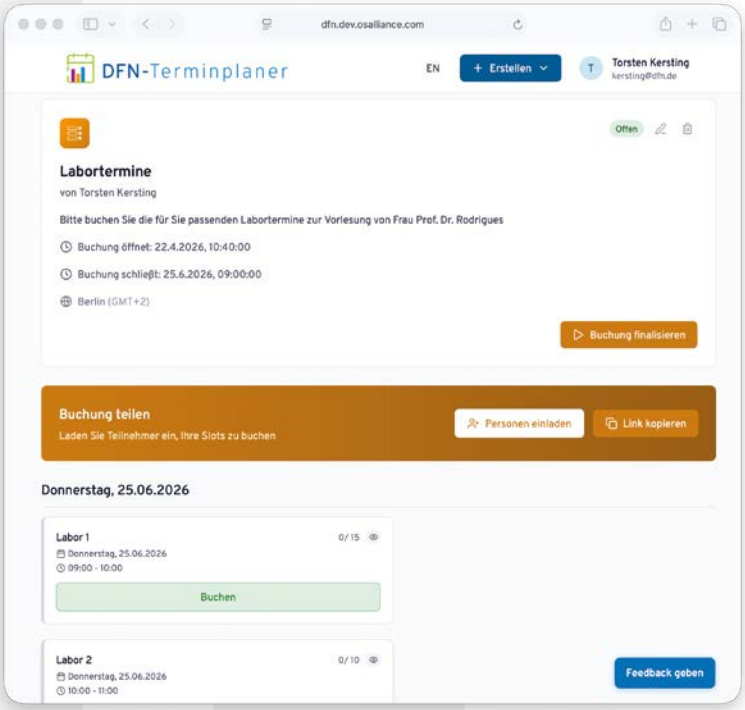
Verbesserte Limitierungsoptionen:
Bislang ließ sich nur ein einheitliches Gesamtlimit für alle Termine festlegen. Künftig kann für jede einzelne Buchungsoption ein eigenes Limit definiert werden – etwa 20 Plätze für Termin A, zehn für Termin B und fünf für Termin C.

Kombinationen aus Text und Datumsabfragen:
Terminabfragen und inhaltliche Fragen lassen sich künftig in einer einzigen Abstimmung kombinieren.

Mehr Dialog, gleicher Datenschutz

Neben den funktionalen Erweiterungen rückt Version 7 auch die Kommunikation stärker in den Vordergrund. Erweiterte Benachrichtigungs- und Kommentarfunktionen sollen den Austausch zwischen Erstellenden und Teilnehmenden direkter und transparenter machen – ohne den gewohnten Ablauf zu verkomplizieren.

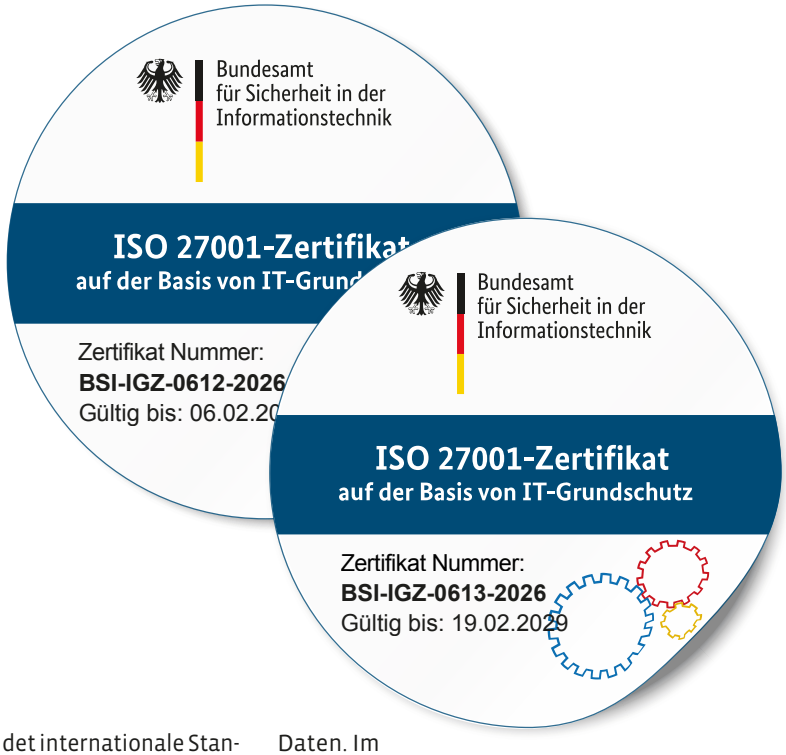
Was sich nicht ändert, ist das Fundament: Datenschutz bleibt oberstes Gebot. Eingaben werden weder an Dritte weitergegeben noch für andere Zwecke als die Ergebnisdarstellung verwendet. In einem Markt, in dem kommerzielle Dienste häufig auf Datenauswertung setzen, ist das ein entscheidender Vorteil – und ein Grund, warum der DFN-Terminplaner seit Jahren großes Vertrauen in der Wissenschaftscommunity genießt. ◆



Alle Collaboration Services des DFN-Vereins finden Sie unter:
https://www.dfn.de/dienste/collaboration-services/

Auf Herz und Nieren zertifiziert

Im Februar 2026 hat der DFN-Verein seine Informationsverbünde „RZ-Infrastruktur“ und „DFN-MailSupport“ erneut erfolgreich zertifizieren lassen. Der Blick hinter die Kulissen macht deutlich, wie viele technische, organisatorische und rechtliche Aspekte dabei zusammenspielen.



Text: **Michael Röder** (DFN-Verein)

Mit mehr als 40 Jahren im Einsatz bleibt die E-Mail das zentrale Kommunikationsmittel im Wissenschaftsnetz. Als Grundlage zahlreicher Prozesse in Forschung und Lehre muss sie zuverlässig und reibungslos funktionieren. Dabei geht es längst nicht nur um Technik: Die Verarbeitung von E-Mails berührt auch datenschutzrechtliche und mitunter strafrechtliche Fragestellungen. Entsprechend hoch sind die Anforderungen an eine vertrauenswürdige und rechtssichere Dienstleistung, die tief in die Kommunikationsinfrastruktur der Einrichtungen eingebunden ist.

Vor diesem Hintergrund haben sich die im DFN-Verein organisierten Einrichtungen für einen kooperativen Ansatz entschieden. Mit DFN-MailSupport stellt der DFN-Verein einen zentralen Dienst bereit, der die lokalen E-Mail-Systeme gezielt unterstützt und zugleich zum Sicherheitsniveau im Wissenschaftsnetz beiträgt. Eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz schafft dafür den notwendigen Nachweis: Sie verbindet internationale Standards mit konkreten Umsetzungsanforderungen und macht Informationssicherheit transparent und überprüfbar.

Warum der DFN-Verein auf ISO 27001 setzt

Im Zentrum jeder Zertifizierung steht eine grundlegende Frage: Was genau wird geprüft – und zu welchem Zweck?

DFN-MailSupport ist die zentrale Anti-Spam-Lösung im Wissenschaftsnetz und hat damit die Aufgabe, unerwünschte und schädliche Nachrichten – etwa Spam oder mit Malware infizierte E-Mails – bereits im Vorfeld zu erkennen und herauszufiltern. Dafür analysiert das System sämtliche eingehenden und – optional – auch ausgehenden Nachrichten. Als integraler Bestandteil der Kommunikation muss der Dienst höchsten Ansprüchen an Verfügbarkeit und Performance gerecht werden. Gleichzeitig beinhaltet E-Mail-Kommunikation in der Regel personenbezogene Daten. Im Ergebnis trifft die Zertifizierung Aussagen über den Reifegrad der Betriebsumgebung hinsichtlich Datenschutzes und IT-Sicherheit.

Das Zertifikat als gemeinsame Grundlage

Die vertragliche Basis für die Verarbeitung personenbezogener Daten ist eine Auftragsverarbeitungsvereinbarung (AVV), die zwischen dem DFN-Verein und den am Dienst teilnehmenden Einrichtungen geschlossen wird.

Die Datenschutz-Grundverordnung (DSGVO) schreibt vor, dass Auftraggebende einer AVV die Möglichkeit haben müssen, die Einhaltung datenschutzrechtlicher Vorgaben beim Auftragnehmer – und damit auch dessen Infrastruktur – zu überprüfen. Gleichzeitig sind Auftragnehmer der AVV verpflichtet, solche Prüfungen zuzulassen.

Damit nun nicht jede der mehr als 190 an DFN-MailSupport teilnehmenden Einrichtungen unter erheblichem Aufwand eigene Audits durchführen muss, gibt es eine etablierte Lösung: Ein unabhängiges Auditorentestat dient als gemeinsamer Nachweis. Genau diese Funktion erfüllt die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) – häufig ergänzt durch ein darauf aufbauendes Datenschutzaudit. Mit einem umfangreichen Maßnahmenkatalog trägt sie dazu bei, die entsprechenden Systeme und Prozesse in puncto Informationssicherheit zu überprüfen. Für die teilnehmenden Einrichtungen bedeutet das: Sie können sich auf einen standardisierten, anerkannten Nachweis verlassen – und lagern damit die eigenen Prüfaufwände komfortabel aus.

Zwei Verbünde, ein Ziel

Sind Zweck und Prüfinhalte definiert, folgt der nächste Schritt: die Bildung eines sogenannten Informationsverbundes (IV). Er beschreibt den konkreten Bereich, auf den sich die Zertifizierung bezieht, und definiert die dafür anzuwendenden Maßnahmen. Denn in der Praxis steht nur selten die gesamte Organisation im Fokus einer Zertifizierung – und das ist auch sinnvoll. Nicht alle Bereiche eines zertifizierten Unternehmens verarbeiten tatsächlich sensible oder personenbezogene Daten. Entsprechend werden gezielt diejenigen Teile betrachtet, für die die Anforderungen tatsächlich relevant sind.

Der DFN-Verein startete zunächst mit einem Informationsverbund: DFN-MailSupport. Weil aber die technische Infrastruktur, die die E-Mail-Inhalte verarbeitet, in den Rechenzentren der drei DFN-Teilnehmer Leibniz Universität Hannover, Technische Universität Berlin und Friedrich-Alexander-Universität Erlangen-Nürnberg untergebracht ist, unterscheiden sich auch die Anforderungen. Aus diesem Grund wurde neben DFN-MailSupport ein zweiter Informationsverbund geschaffen: RZ-Infrastruktur. Hier stehen andere Maßnahmen und Bausteine im Fokus, ergänzt durch ein eigenes Risikomanagement, das gemeinsam mit den beteiligten Rechenzentrumsstandorten entwickelt wird. Beide Informationsverbünde greifen ineinander und werden in einem Sicherheitskonzept dokumentiert.

Auf Herz und Nieren: das Audit als Härtetest

Irgendwann kommt der entscheidende Moment: die Prüfung durch unabhängige Auditorinnen und Auditoren. Sie haben die Aufgabe, Systeme, Prozesse und Rahmenbedingungen umfassend zu bewerten. Damit kontrollieren sie, ob das Sicherheitskonzept nicht nur auf dem Papier besteht, sondern auch in der Praxis umgesetzt wird. Diese externe Prüfung ist essenziell – denn ein Informationsverbund sollte sich nicht selbst kontrollieren.

Das Audit beginnt mit einer intensiven Analyse der Dokumentation. Darauf folgen stichprobenartige Begehungen der Standorte. Dabei wird die gesamte Bandbreite der Informationssicherheit betrachtet: von technischen und organisatorischen Maßnahmen über Betriebsprozesse bis hin zur physischen Sicherheit der Infrastruktur. Denn auch die Betriebssicherheit spielt eine zentrale Rolle – schließlich können Ausfälle ebenso sicherheitsrelevant sein. Entsprechend detailliert ist der Blick der Auditoren: Er reicht von der Trassenführung der Verkabelung im Rechenzentrum über Wartungs- und Prüfprotokolle von Notstrom- und Netzersatzanlagen bis hin zu baulichen Eigenschaften wie der Widerstandsfähigkeit der Gebäudehülle gegenüber Umwelteinflüssen.

Selbst bei bester Vorbereitung entgeht den Augen der Auditoren kaum etwas. Auch scheinbar kleine Details – etwa ein fehlendes Prüfsiegel an einem Feuerlöscher – werden mit Sicherheit erkannt. Und das ist überhaupt nicht schlimm – ganz im Gegenteil zeigt das Audit, wie es um die Umsetzungsreife des Informationsverbundes beschaffen ist und wo noch Verbesserungspotenzial besteht. Damit ist die Ortsbegehung ein wichtiger Impuls, um die Sicherheit weiter zu erhöhen. Bis zum krönenden Abschluss heißt es: abwarten.

Und wie geht es weiter nach dem IT-GS-Zertifikat?

Mit dem IT-GS-Zertifikat ist der Prüfprozess für DFN-MailSupport aber noch nicht abgeschlossen. Neben der Informationssicherheit sind im Rahmen der Auftragsverarbeitung auch datenschutzrechtliche Anforderungen von entscheidender Bedeutung. Die Zertifizierung ist daher nur einer von zwei wesentlichen Prüfbausteinen, denen der Dienst DFN-MailSupport gerecht werden muss. Aufbauend auf der IT-GS-Zertifizierung folgt im dritten Quartal 2026 ein Datenschutzaudit. Bis dahin behält das Auditorentestat aus dem Jahr 2023 seine Gültigkeit.

Erfolgreiche Zertifizierungen sind Teamarbeit!

An dieser Stelle gilt ein besonderer Dank den Mitarbeitenden an den Rechenzentrumsstandorten der X-WiN-Kernnetzknoten für die hervorragende Zusammenarbeit. Sie tragen dazu bei, dass die Audits bestens vorbereitet unter optimalen Bedingungen durchgeführt werden können – eine stabile Basis für künftige Prüfungen.

Eines ist sicher: Die dreijährige Laufzeit des IT-GS-Zertifikats vergeht schneller, als man denkt. Und dann beginnt der Zyklus von Neuem. Oder anders gesagt: Nach dem Audit ist vor dem Audit. ◆

Bye, bye DFN-NetNews – Abschied von einem geschätzten Wegbegleiter

Zum Jahresende 2026 schließt sich ein Kapitel Internetgeschichte im DFN: Der Dienst DFN-NetNews geht vom Netz. Was einst als offenes, internationales „Schwarzes Brett“ begann, war für viele das erste soziale Netzwerk der Wissenschaft – geprägt von Aufbruchsstimmung, schnellem Austausch und einer ungewöhnlich respektvollen Diskussionskultur. Vera Heinau von der FUB-IT, Zentrale IT-Services, der Freien Universität Berlin (FU Berlin) war von Beginn an dabei und wirft einen Blick zurück auf die Anfänge, die besondere Dynamik der NetNews-Community und die Gründe, warum dieses Kapitel nun zu Ende geht.

Text: **Vera Heinau** (Freie Universität Berlin)

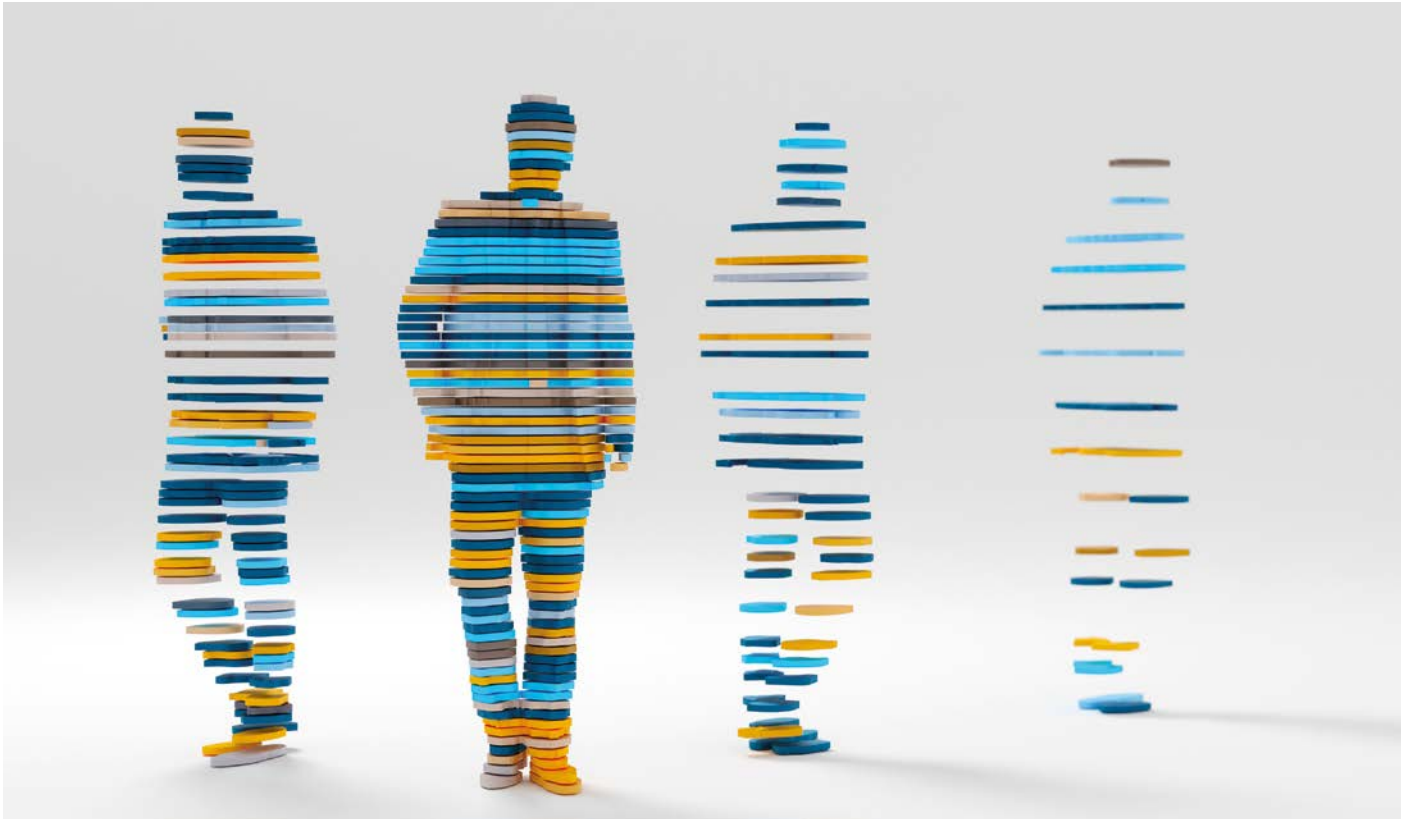


Illustration: piranka/iStock

Wenn Nerds einen Dienst erfinden und aufsetzen, so tun sie das in aller Regel, um erst einmal ihre eigenen Bedürfnisse zu befriedigen. In diesem Fall ging es darum, eine zentrale Plattform für Diskussionen und den fachlichen Austausch zu schaffen. Die ursprüngliche Idee von NetNews wuchs schnell über sich hinaus, und schon bald wurde nicht mehr nur über den Umgang mit einem bestimmten Betriebssystem diskutiert, sondern auch über andere technisch-wissenschaftliche Themen – aber ebenso über Dinge des täglichen Lebens wie Freizeit, Kultur und Gesellschaft.

Freier Meinungsaustausch über Ländergrenzen hinweg und anregende Diskussionen mit Menschen aus aller Welt: Als ich vor 40 Jahren den Dienst NetNews kennenlernte – das war etwa zwei Jahre nach Gründung des DFN-Vereins –, faszinierten mich die scheinbar unbegrenzten Möglichkeiten der modernen Kommunikation und des konstruktiven Miteinanders ungemein.

> Freier Meinungsaustausch über Ländergrenzen hinweg und anregende Diskussionen mit Menschen aus aller Welt

Eine besondere Aufbruchsstimmung prägte diese Zeit: Zum ersten Mal konnten auch Menschen außerhalb von Hochschulen oder Forschungseinrichtungen unmittelbar an der Entwicklung des Internets teilhaben. NetNews bot ihnen die Möglichkeit, mitzudiskutieren und damit die entstehende digitale Kultur mitzugestalten.

Klassiker der internationalen Diskussionssysteme

Das Netzwerk Usenet, die zugrunde liegende Infrastruktur für den Dienst NetNews, war eines der ersten verteilten Diskussionssysteme im Internet. Es wurde 1979 von Tom Truscott und Jim Ellis an der Duke University und der University of North Carolina at Chapel Hill als zivile Kommunikationsalternative zum Forschungsnetz ARPANET des US-Verteidigungsministeriums ins Leben gerufen. Die kostengünstige, offene Kommunikationslösung diente primär dazu, sich über technische Fragen der damals noch neuen Computer auszutauschen. In den folgenden Jahren mauserte sie sich zu einem weltumspannenden Medium für Hunderttausende Menschen, die eigene Beiträge leisteten oder auch nur mitlasen.

Karsten Leipold, Administrator für Domain-Dienste und Netzwerkinfrastruktur im DFN-Verein: „Das Aufsetzen und Konfigurieren des Newsservers gehörte Anfang der 90er-Jahre zu meinen ersten Aufgaben im DFN-Verein. Ich freue mich, dass ich damit einen Beitrag zur Verbreitung des Dienstes DFN-NetNews leisten konnte."

In seinen Spitzenzeiten – etwa Ende der 1990er- bis Mitte der 2000er-Jahre – war Usenet eines der größten verteilten Diskussionssysteme der Welt. Schätzungen gehen von weltweit mehreren Zehntausend Servern, rund Hunderttausend Newsgruppen, mehreren Millionen regelmäßigen Usern und einigen Hunderttausend Artikeln pro Tag aus.

Heiko Schlichting, Verantwortlicher für Software-Entwicklung und -Anpassung sowie Systemadministrator von DFN-NetNews an der Freien Universität Berlin: „Es war spannend und motivierend, an der Front der Entwicklung eines neuen Mediums zu stehen – eine Gelegenheit, die sich einem nicht oft im Leben bietet!"

Wegbereiter der Social-Media-Bewegung

Die Grundidee des Dienstes NetNews ist simpel: Man nehme ein virtuelles „Schwarzes Brett" mit definierten Kategorien (Hierarchien bzw. Newsgroups), das sich über viele Server hinweg spiegelt. Wenn jemand eine Notiz an das Schwarze Brett heftet – einen Beitrag postet –, wird dieser von Server zu Server weitergegeben und so im gesamten Netzwerk verbreitet. Mit diesem Konzept kann NetNews mit Fug und Recht als erster Vorgänger und Wegbereiter der heutigen mächtigen Social-Media-Plattformen und modernen Foren betrachtet werden. Anders als diese versteht es sich allerdings als nichtkommerzielle Graswurzelbewegung, basierend auf offenen Standards und kostenfreier Software.

Der NetNews-Zugang ist niederschwellig: Ein Internetanschluss und ein kostenfreier Client genügen, sodass der Dienst auch ohne umfangreiches technisches Know-how genutzt werden kann. Damit stand das Usenet – sowohl hinsichtlich der Themen als auch der Zugangsvoraussetzungen – einem breiten Publikum offen und wuchs mit der zunehmenden Verbreitung von PCs auch im privaten Bereich.

Die Einrichtung neuer Newsgruppen ist demokratisch organisiert. Alle Nutzenden können Vorschläge einbringen. Diese werden zunächst öffentlich diskutiert und anschließend im Voting, einem klar geregelten gemeinsam festgelegten Verfahren, abgestimmt.

So entstanden Newsgruppen mit eher „seriösen“ und sachlichen Bezeichnungen wie de.sci.chemie – aber auch solche mit flapsigen humorvollen Namen wie de.rec.mampf (de für deutschsprachig, sci für Science, rec für Recreation).

Die Atmosphäre in den Newsgroups war persönlich – fast schon familiär, die Hilfsbereitschaft überwältigend. Neulinge konnten jegliche Art von Fragen stellen, ohne herablassende oder abfällige Kommentare zu erhalten. Gepostet wurde unter dem eigenen Namen oder einem bekannten „Nickname“, und Beleidigungen („Flames“) oder gezielte Provokationen („Trolling“) waren verpönt. Der Umgang war geprägt von Neugier, Respekt und dem gemeinsamen Gefühl, an etwas großem Neuen teilzuhaben.

Bettina Fink, Newsmistress von DFN-NetNews: „Zwischen Austausch und Konflikt, zwischen Verbindungen schaffen und manchmal auch aushalten hast du mich 30 Jahre begleitet – und bleibst mir gerade deshalb in Erinnerung.“

Apropos: NetNews war aus meiner Sicht einer der ersten gelungenen Versuche, bei denen sich eine internationale Gemeinschaft von Nutzerinnen und Nutzern auf einen gemeinsamen allgemein anerkannten Verhaltenskodex verständigen konnte. Die Grundprinzipien der sogenannten Netiquette waren – mit kleinen Unterschieden je nach Region oder Organisation – weltweit ähnlich. Heutzutage würde man ein solches Werk wohl „Code of Conduct“ nennen und als große Errungenschaft herausstellen – damals war die Einhaltung für die allermeisten eine Selbstverständlichkeit.

Ein neuer Dienst im Wissenschaftsnetz: DFN NetNews

Recht schnell erkannten auch Hochschulen und Forschungseinrichtungen in Deutschland die innovativen Informations- und Kommunikationsmöglichkeiten. Bereits in den frühen 90er-Jahren betrieb der DFN-Verein einen eigenen Newsserver für NetNews – genau wie die Freie Universität Berlin (FU Berlin). Beide Admin-Teams pflegten einen intensiven, partnerschaftlichen Austausch. Später entwickelte die FU Berlin aufgrund ihrer langjährigen Erfahrung und Expertise im Auftrag des DFN-Vereins den Pilotdienst News.CIS.DFN.DE und übernahm die Administration und Wartung. Der Dienst ging 2003 unter dem Namen DFN NetNews in den Produktivbetrieb über. Damit wollte der DFN-Verein der Wissenschaftscommunity in Deutschland einen einfachen Zugang zum Usenet – und damit zu einem weltweiten Netz von Newsgroups – ermöglichen und die technischen Hürden für einzelne Einrichtungen vermeiden. Zahlreiche Einrichtungen im Wissenschaftsnetz nahmen das Angebot wahr – sowohl kleinere, die sich so das Aufsetzen eines eigenen Servers ersparen konnten, als auch große, die mit dem Dienst ihr eigenes Dienstportfolio ergänzten.

Wind of Change

Wie so oft: Nicht nur die Revolution frisst ihre Kinder, sondern auch der Erfolg die erste Generation von Idealisten. Entgegen dem Gemeinschaftssinn gab es immer mehr Nutzende, die das Usenet nur als Mittel für ihre Zwecke betrachteten. Spam, bösartige Links, „Flame Wars“, Hassrede und Propaganda breiteten sich zunehmend aus. Technische Maßnahmen halfen zwar bei der Eindämmung, aber das sichere Gefühl des geschützten, familiären Raums war endgültig dahin.

> Spam, bösartige Links, „Flame Wars“, Hassrede und Propaganda breiteten sich zunehmend aus.

Nicht wenige, die das Usenet gezielt zum Austausch spezifischer fachlicher Themen genutzt hatten, waren genervt vom Missbrauch in „ihren“ Gruppen und zogen in passende Webforen um – dort ging es meist zivilisierter zu. Dieser Effekt zeigte sich überproportional im akademischen Umfeld, in dem viele die neuen Foren mittlerweile als deutlich angenehmer und effizienter empfanden – was sich letztendlich daran zeigte, dass DFN-NetNews immer weniger genutzt wurde. Dieser Aderlass traf die Qualität einiger Newsgruppen empfindlich. Denn dadurch wurde ihnen ein Teil des qualifizierten Know-hows entzogen, was sie wiederum für Neulinge weniger attraktiv gestaltete.

Andreas M. Kirchwitz, „Hüter“ der Netiquette für die deutschsprachigen Newsgruppen de: „Die elementare Kernbotschaft der Netiquette ist längst allgemeingültiger Ratschlag und Mahnung für alle elektronischen Medien der heutigen Zeit: Vergiss niemals, dass auf der anderen Seite ein Mensch sitzt!“

Gleichzeitig schritt die Entwicklung des Web 2.0 sowie der sozialen Medien rasant voran. Getrieben von großen Firmen oder Konsortien zeigten sich die Plattformen nun in einem Layout, das insbesondere jüngere Generationen ansprach, und mit fortwährend neuen interaktiven Features. Die Möglichkeit, Grafiken

und Bilder in Posts einzubinden – im textorientierten Usenet nicht vorgesehen bzw. nicht akzeptiert –, war ein sehnsüchtig erwartetes Feature und damit einer der großen Gamechanger. Das eher an klassischen E-Mail-Clients orientierte textbasierte Layout und die Funktionalität der Newsreader konnten da schlicht und ergreifend nicht mithalten.

Ein weiterer Grund dafür, dass die Nutzungszahlen drastisch in den Keller gingen, lag im Selbstverständnis der NetNews-Community: Werbung war nur in eigens gekennzeichneten Gruppen erlaubt. Für viele Unternehmen war der Dienst damit unattraktiv – auch weil sie auf kritische oder unerwünschte Beiträge keinen Einfluss nehmen konnten. Stattdessen setzten sie zunehmend auf eigene Plattformen wie Foren oder Wikis. So stellte etwa Microsoft 2010 den Support über Newsgruppen ein. Über die Jahre nahmen viele Betreiber ihre NetNews-Server vom Netz.

Ist NetNews nun endgültig tot?

Der Dienst DFN-NetNews wird ohne Zweifel am 31. Dezember 2026 ersatzlos eingestellt. Es wird nach wie vor enthusiastische Menschen geben, die privat Newsserver betreiben und sich mit anderen vernetzen. Und es wird sicherlich auch weiterhin Szenarien geben, für die diese Kommunikationstechnik geeignet ist, oder Einsatzgebiete, bei denen es sich nicht mehr lohnt, auf andere Systeme umzusteigen.

Auch wenn DFN-NetNews nun endet, bleibt vor allem die Erinnerung an eine Zeit, in der Austausch im Netz noch persönlicher und respektvoller war. Der Dienst war für mich mehr als ein Werkzeug – es war ein Ort der Begegnung. Ich habe ihn gerne genutzt und dabei viele kluge, hilfsbereite und nette Menschen kennengelernt. ◆

Wer weiterhin im Usenet unterwegs sein möchte, findet auf folgender Webseite eine Liste von Usenet-Anbietern im deutschsprachigen Raum: **https://th-h.de/net/usenet/faqs/newsserverliste/**

Einen Artikel zu den Anfängen von NetNews im DFN-Verein finden Sie in Ausgabe 28 der DFN-Mitteilungen: **https://www.dfn.de/wp-content/uploads/2023/11/DFN-Mitteilungen-28.pdf**

Kurzmeldungen

Neu in der DFN-Cloud: barrierefreie Videos mit Melvin erstellen

Von teilnehmenden Einrichtungen für teilnehmende Einrichtungen: Als Neuzugang in den föderierten Diensten der DFN-Cloud bietet das datenschutzkonforme Tool Melvin seit 1. März 2026 eine integrierte Open-Source-Lösung, um barrierefreie Videos zu erstellen. Melvin funktioniert intuitiv. Ohne zusätzliche Software, direkt im Browser, können Beiträge hochgeladen, automatisch untertitelt und anschließend über einen barrierefreien Player inklusive Transkript bereitgestellt werden. Anschließend lassen sich die Untertitel sowohl einzeln als auch im Team überarbeiten und optimieren.

Melvin wurde im Rahmen des Projekts „SHUFFLE – Hochschulinitiative digitale Barrierefreiheit für Alle“ entwickelt. Ziel des Projekts zur Verbesserung digitaler Barrierefreiheit war es, Maßnahmen auf technischer, struktureller und didaktischer Ebene zu entwickeln, zu erproben und dauerhaft als Open-Source-Lösungen bereitzustellen. Projektpartner waren die Hochschule der Medien Stuttgart, die Universität Bielefeld, die Pädagogische Hochschule Heidelberg und die Pädagogische Hochschule Freiburg. Das Projekt endete im Dezember 2025 mit einer Reihe unterschiedlicher Anwendungen – unter anderem dem SHUFFLE-Reifegradmodell, das wir in der aktuellen Ausgabe der DFN-Mitteilungen vorstellen.

Die föderierten Dienste der DFN-Cloud werden von teilnehmenden Einrichtungen im Wissenschaftsnetz bereitgestellt. Dazu zählen unter anderem Sync-&-Share-Funktionen, Virtualisierungsumgebungen sowie Tools für Kollaboration, E-Teaching und E-Learning. ◆

Weitere Angebote der DFN-Cloud finden Sie unter: **https://www.dfn.de/dienste/cloud/**

Kurzmeldungen

Mehr Resilienz im X-WiN: direktes Peering mit NORDUnet in Betrieb

Redundante Anbindungen zur Erhöhung der Resilienz zählen zu den zentralen Strategien im Wissenschaftsnetz. Aus diesem Grund plant der DFN-Verein vermehrt direkte Peerings mit benachbarten Forschungsnetzen. Nach dem Peering mit dem polnischen Forschungsnetz PCSS im September 2025 hat der DFN-Verein nun gemeinsam mit dem nordischen regionalen Forschungsnetzverbund NORDUnet – einem Zusammenschluss der Forschungsnetze DeiC (Dänemark), Funet/CSC (Finnland), RHnet (Island), Sikt (Norwegen) und Sunet (Schweden) – eine weitere direkte Peering-Verbindung erfolgreich in Betrieb genommen. Mit einer Anschlussbandbreite von 100 Gbit/s werden die Netzinfrastrukturen am X-WiN-Kernnetzknoten in Hamburg zusammengeführt.

Blick auf die Elbphilharmonie in Hamburg | *Foto: ceo-21/magnific*

Private Network Interconnections (PNIs) bezeichnen die direkte Kopplung von Routern zweier Peering-Partner und schaffen damit dedizierte, vom öffentlichen Internet unabhängige Verbindungen. Ziel ist es, den Datenverkehr effizienter zu leiten, Latenzen zu reduzieren und Paketverluste zu minimieren. Durch diese direkten Peerings lassen sich insbesondere Verfügbarkeit und Antwortzeiten signifikant verbessern.

Gleichzeitig erhöhen PNIs die Resilienz der Netzarchitektur: Durch zusätzliche, voneinander unabhängige Übergabepunkte entstehen redundante Leitungen, über die der Verkehr bei Störungen automatisch umgeleitet werden kann. Für teilnehmende Einrichtungen im X-WiN bedeutet das eine höhere Verfügbarkeit und stabile Antwortzeiten – auch bei Ausfällen im Netz.

Die neue Anbindung an NORDUnet ergänzt den bestehenden Übergang zum europäischen Forschungsnetz GÉANT. Dieses verbindet die nationalen Forschungsnetze (National Research and Education Networks, NRENs) in Europa miteinander und schafft die Anbindung an weltweite Forschungsnetze. Neben den bestehenden GÉANT-Anschlüssen des X-WiN mit einer Gesamtkapazität von 800 Gbit/s steht nun ein zusätzlicher Übertragungsweg bereit. ◆

DFN-Fernsprechen: neue Rahmenverträge für Mobilfunk

Das Vergabeverfahren für die neuen Mobilfunkrahmenverträge wurde erfolgreich abgeschlossen. Der DFN-Verein erteilte gleich drei Netzbetreibern den Zuschlag und stärkt damit Vielfalt und Wettbewerb. So stehen teilnehmenden Einrichtungen am Dienst DFN-Fernsprechen seit dem 1. März 2026 Rahmenverträge mit der Telekom, Vodafone und Telefónica zur Verfügung. Für Hochschulen und Forschungseinrichtungen ergeben sich daraus attraktive Konditionen. Darüber hinaus können sie künftig das Mobilfunkangebot wählen, das optimal zu ihren organisatorischen und wirtschaftlichen Anforderungen passt, und damit komfortabel und sicher Sprach-, Nachrichten- und Datenübertragung nutzen.

Der Dienst DFN-Fernsprechen bietet neben den Mobilfunkrahmenverträgen auch Voice-over-IP (kurz VoIP)-basierte Anschlussarten, die in das Wissenschaftsnetz X-WiN integriert und auf die Anforderungen von Wissenschaft und Forschung abgestimmt sind. Dank seiner redundanten Anbindung an das X-WiN weist der Dienst eine sehr hohe Verfügbarkeit auf. ◆

Mehr Informationen zu DFN-Fernsprechen finden Sie unter: **https://www.dfn.de/dienste/collaboration-services/dfnfernsprechen/**

GÉANT TNC26: drei DFN-Talente im Finale des FTP

Der DFN-Verein schickte in diesem Jahr drei Nachwuchstalente zur Finalrunde des Future Talent Programme (FTP) nach Helsinki. Anna Maria Yang-Jacobi, Felix Jahn und Jan-Frederik Rieckers konnten sich im internationalen Auswahlverfahren durchsetzen und präsentierten ihre innovativen Projekte auf der TNC26.

Die TNC ist die weltweit größte und wichtigste Konferenz für Forschungs- und Bildungsnetzwerke. Sie wird jährlich vom europäischen Forschungsnetzverbund GÉANT organisiert und zieht regelmäßig über 900 Teilnehmende aus mehr als 70 Ländern an. Das Publikum reicht dabei von Entscheidungsträgern bis hin zu Spezialisten für Cybersicherheit und Identitätsmanagement.

Die diesjährige Konferenz fand vom 8. bis 12. Juni in Helsinki unter dem Motto „Digital Sisu“ – das finnische Wort steht für innere Stärke, Ausdauer und Mut – statt. In diesem hochkarätigen Umfeld ist das Future Talent Programme fest verankert: Es bietet Studierenden und jungen Fachkräften die Bühne, um ihre Ideen vor der globalen Community sichtbar zu machen und die digitale Souveränität der Wissenschaft aktiv mitzugestalten.

Für die drei DFN-Teilnehmenden markierte die Konferenz den feierlichen Höhepunkt eines mehrmonatigen Entwicklungsprozesses. Im Vorfeld durchlaufen alle Finalisten ein professionelles Präsentationstraining durch das GÉANT Learning and Development Team (GLAD). In Workshops und Einzelcoachings lernen sie, komplexe technische oder rechtliche Themen prägnant für ein internationales Fachpublikum aufzubereiten. ◆

Mehr Informationen zu der Veranstaltung, der Finalistin und den zwei Finalisten finden Sie unter:
https://www.dfn.de/future-talent-programme-tnc26/

Jan-Frederik Rieckers
DFN-Verein
Projekt: „eduroam Login Made Simple: How Passkeys Can Help“
Jan-Frederik Rieckers widmet sich der Modernisierung des weltweiten eduroam-Zugangs. Er untersucht, wie passwortfreie Passkeys (FIDO-2) den Konfigurationsaufwand für Nutzende drastisch reduzieren und gleichzeitig die Resilienz des Systems gegen Phishing-Angriffe stärken können.

Anna Maria Yang-Jacobi
Forschungsstelle Recht im DFN
Projekt: „Time for Transformation: How New Media Can Help to Explain (Legal) Change“
Anna Maria Yang-Jacobi zeigt auf, wie man das Medium Podcast nutzen kann, um komplexe Schnittstellen zwischen Recht und Technologie – wie die neue europäische „Digital Omnibus“-Verordnung – verständlich zu vermitteln. Ziel ist es, sperrige juristische Zusammenhänge und die Kritik an Anpassungen von Rechtsakten wie der DSGVO für die Forschungsgemeinschaft greifbar aufzuschlüsseln.

Felix Jahn
Hochschulforum Digitalisierung
Projekt: „Curating Collaboration: From ‚Can‘ to ‚Want‘“
Felix Jahn hinterfragt primär technologiegetriebene Innovationen in Hochschulen. Er stellt das PST-Framework (Pedagogy, Space, Technology) vor, um aufzuzeigen, dass hybride Zusammenarbeit ganzheitlich mit pädagogischen und räumlichen Komponenten gedacht und gestaltet werden muss.

Vertrauen schafft Sicherheit – das MISP Threat Sharing

Das DFN-CERT entwickelt den Austausch von Bedrohungsinformationen stetig weiter: Teilnehmende Einrichtungen am Wissenschaftsnetz erhalten aus der MISP-Threat-Sharing-Plattform des DFN-CERT künftig nicht nur aufbereitete Daten, sondern auch direkten Zugriff auf ausgewählte Rohdaten. Dafür werden aktuell zwei Zugangswege vorbereitet.

Text: **Christine Kahl** (DFN-CERT)

Vertrauen schafft Sicherheit: Wenn es um die erfolgreiche Abwehr von Cyberangriffen geht, trifft dieser Leitspruch genau ins Schwarze. IT-Sicherheitsvorfälle erfolgen nicht nur weitaus häufiger, sondern werden auch immer professioneller. Um der gestiegenen Frequenz und Varianz zu begegnen, sind sowohl Informationen zu den Angriffen als auch zu den Angreifenden notwendig, die Sicherheitsexpertinnen und Sicherheitsexperten weltweit zusammentragen. Um diese auszutauschen, hat sich die MISP-Threat-Sharing-Plattform mittlerweile als De-facto-Standard etabliert und wird seit mehreren Jahren auch erfolgreich vom DFN-CERT eingesetzt. Jetzt steht der nächste Schritt an, das Teilen der Rohdaten.

Welche Daten enthält MISP?

Die Grundsteinlegung für das MISP Threat Sharing erfolgte 2011, um den Austausch von Kompromittierungsindikatoren (Indicators of Compromise, IOCs) zu strukturieren und zu vereinfachen. Die ursprüngliche Bezeichnung von MISP als Malware Information Sharing Platform greift mittlerweile zu kurz: Neben dem Austausch, der Speicherung und der Korrelation von Indikatoren für Kompromittierungen verarbeitet MISP zusätzlich umfangreiche Bedrohungsdaten – etwa zu Angreifenden, Finanzbetrug und weiteren Aspekten der Cyberkriminalität.

Warum ist Threat Sharing so wichtig? Cyberkriminelle arbeiten längst hochgradig vernetzt: Für Angriffe gibt es Playbooks und Software zu kaufen oder zu mieten. Fachleute für Cybersicherheit müssen es ihnen gleichtun, um im Wettlauf mit ihnen eine Chance zu haben. Der große Vorteil von MISP liegt im kollektiven Wissen. Das als Open-Source-Plattform entwickelte MISP ist extrem flexibel und unterstützt eine Vielzahl von Attributen, unter anderem:

- IP-Adressen, Domains, URLs
- Hashes (MD5, SHA1, SHA256)
- Malware-Samples
- Daten über Phishing-Kampagnen

Illustration: Nuthawut Somsuk/iStock

- TTPs (Tactics, Techniques & Procedures beschreiben charakteristische Angriffsmuster und geben Einblicke in das Vorgehen von Angreifern.)
- MITRE ATT&CK-Zuordnungen (MITRE ATT&CK oder ATT&CK ist eine Wissensdatenbank der MITRE Corporation zur Klassifizierung und Beschreibung von Cyberbedrohungen.)

Diese Informationen werden in sogenannten Events – einer Art Akte, die alle zu einem Angriff zugehörigen Informationen enthält – zusammengefasst, die zusätzlich Metadaten wie Bedrohungslevel, Vertraulichkeit (Traffic Light Protocol, TLP) und zeitliche Gültigkeit enthalten.

Was eine Organisation jetzt entdeckt, kann gleich andere schützen

Durch gemeinsames Sammeln von Daten lassen sich:

- Angriffe früher erkennen
- False Positives reduzieren
- Reaktionszeiten massiv verkürzen
- Ressourcen effizienter einsetzen

Da die in MISP enthaltenen Informationen nicht nur der manuellen Auswertung dienen, können die Daten über APIs und Feeds sowohl automatisch importiert als auch exportiert und in anderen Systemen wie Firewalls, SIEM (Security Information and Event Management) oder EDR (Endpoint Detection and Response) weiterverwendet werden.

Warum braucht es Vertrauen und Vertraulichkeit?

Threat Sharing basiert auf Vertrauen. Wenn eine Organisation Bedrohungsdaten aus MISP einsetzt, um zum Beispiel Kommunikationsverbindungen zu blockieren, dann muss sie sich sicher sein, dass diese Daten aus einer vertrauenswürdigen Quelle stammen und damit aller Wahrscheinlichkeit nach korrekt sind. Auch andersherum braucht es Vertrauen: IOC-Daten, zum Beispiel IP-Adressen von Command-und-Control-Servern (C2-Servern), sind nur dann wertvoll, wenn Angreifende nicht wissen, dass diese bereits bekannt sind. Sobald Cyberkriminelle davon Kenntnis erhalten, werden IOC-Daten in der Regel geändert, und das Spiel beginnt von Neuem. Das bedeutet, wenn Informationen geteilt werden, steht höchste Vertraulichkeit an erster Stelle. Nur so wird sichergestellt, dass die wertvollen Erkenntnisse nicht in die falschen Hände geraten. MISP trägt diesen Anforderungen Rechnung durch:

- granulare Sharing-Gruppen
- TLP-Kennzeichnungen
- Community- und Organisationsmodelle

So besteht jederzeit Kontrolle darüber, wer welche Daten sehen darf.

Warum besitzt nicht jede Einrichtung eine MISP-Instanz?

Trotz aller Vorteile ist der Einsatz von MISP kein Selbstgänger. Wer ein eigenes System aufsetzen möchte, muss es nicht nur pflegen, sondern sich auch Gedanken über den Bezug der Daten und deren Weiterverwendung machen. Es braucht Prozesse, klare Verantwortlichkeiten und insbesondere Zeit.

Das DFN-CERT hat bereits vor mehreren Jahren begonnen, in MISP zu investieren. Seither bezieht es Daten aus verschiedenen vertrauenswürdigen Quellen und pflegt zudem eigene Informationen in das System ein. Diese selbst eingebrachten Daten werden unter anderem zur Erstellung der DNS-RPZ (Domain Name System Response Policy Zone) genutzt, die das DFN-CERT teilnehmenden Einrichtungen im Rahmen des Dienstes DFN-Security zur Verfügung stellt. DNS-RPZ als aktive Abwehrkomponente ermöglicht es bei der Namensauflösung durch rekursive DNS-Resolver mittels eigener Richtlinien einzugreifen, dadurch letztlich den Zugriff auf bestimmte Domains zu unterbinden und insbesondere Phishing-Angriffe zu verhindern.

Teilnehmende Einrichtungen haben bislang vor allem indirekt von den in MISP verfügbaren Daten profitiert – etwa über Warnmeldungen oder RPZ. Künftig sollen diese Informationen auch in Form von „Rohdaten“ bereitgestellt werden. Dafür werden derzeit zwei Wege vorbereitet: Zum einen entsteht eine MISP-Instanz, auf der DFN-Teilnehmer eigene Accounts erhalten können. Zum anderen wird die Synchronisation mit anderen MISP-Instanzen aufgebaut, um den Austausch von Daten weiter zu erleichtern. Damit wird der Austausch von Bedrohungsinformationen innerhalb der DFN-Community deutlich erweitert.

Die Nutzung von MISP – sei es über eigene Accounts oder durch Synchronisation – erfordert eine gründliche Einarbeitung. Deshalb begleitet das DFN-CERT seit Februar 2026 den Einstieg mit Informationsveranstaltungen. Teilnehmende erhalten dabei einen ersten Einblick in das System, seinen Nutzen, aber auch in die damit verbundene Komplexität. Ziel ist es, Einrichtungen eine fundierte Grundlage zu vermitteln, damit sie bei Verfügbarkeit der Zugänge die für sie passende Form der Nutzung wählen können. ◆

Bei Fragen zu MISP oder zum Dienst DFN-Security stehen wir Ihnen gerne zur Verfügung unter: **dfn-security@dfn.de**

Die Standarddefinitionen und Anwendungshinweise (Version 2.0) zum Traffic Light Protocol (TLP) finden Sie unter: **https://www.first.org/tlp/**

Sicherheit aktuell

eduVPN: zwei Nutzungsszenarien und ihre Herausforderungen

Der Dienst eduVPN ist ein weltweit verfügbarer VPN-Dienst für Studierende, Forschende und Lehrende. Er ermöglicht sowohl den sicheren Zugang zu Ressourcen der eigenen Einrichtung als auch geschützte Verbindungen in wissenschaftliche Netze.

Im Wesentlichen unterstützt eduVPN zwei Anwendungsszenarien: „Institute Access“ und „Secure Internet“. Beim „Institute Access“ erfolgt die Verbindung zum eduVPN-Server der eigenen Einrichtung in der Regel über föderierte Zugänge. Aktuell bieten rund 44 Einrichtungen dieses Szenario an. Das Szenario „Secure Internet“ ermöglicht hingegen Verbindungen zu eduVPN-Diensten in derzeit 20 unterschiedlichen NRENs und wird von etwa 55 000 Nutzenden im DFN-Kontext verwendet.

Im DFN befindet sich eduVPN derzeit im Pilotbetrieb für einen sicheren VPN-Zugang (Secure Internet Access) zum X-WiN. Die Teilnahme wird über den jeweiligen Identity Provider der Einrichtungen innerhalb der DFN-AAI konfiguriert. Der zugehörige Service Provider ist über das eduVPN-Portal erreichbar.

Voraussetzung für die Anmeldung ist die samlPairwiseID, ein dauerhaftes Attribut, das nicht neu vergeben werden darf. Perspektivisch soll sie das funktional vergleichbare, jedoch als veraltet geltende Attribut eduPersonTargetedID sowie die SAML2 persistent NameID in der DFN-AAI ersetzen.

„Secure Internet“ kommt insbesondere dann zum Einsatz, wenn kein Zugang zum VPN der eigenen Einrichtung besteht – etwa während eines Auslandsaufenthalts oder für bestimmte Forschungsszenarien. In der Praxis zeigt sich jedoch eine Herausforderung: Nutzende, die eigentlich den „Institute Access“ verwenden möchten, gelangen teilweise stattdessen in das Szenario „Secure Internet“.

Für den Umgang mit dieser Situation werden derzeit verschiedene Ansätze diskutiert. Dazu zählen unter anderem ein Opt-in-Verfahren, das jedoch bestehende Nutzende unmittelbar ausschließen würde, konfigurationsseitige Anpassungen auf Ebene der eduVPN-Server einzelner Einrichtungen sowie eine veränderte Darstellung des „Secure Internet“-Szenarios innerhalb der App, beispielsweise in den Einstellungen. ◆

DFN-PKI: Änderungen am Zeitstempeldienst

Im Rahmen der DFN-PKI wird ein Zeitstempeldienst betrieben. Zweck dieses Dienstes ist es, einen Nachweis über die Existenz eines Dokumentes oder anderer Daten zu einem bestimmten Zeitpunkt durch eine Trusted Third Party (hier: den DFN-Verein) zu erstellen.

Das technische Funktionsprinzip ist einfach: Ein Client erstellt zunächst einen Hash – das ist ein digitaler Fingerabdruck – über die Daten, die mit einem Zeitstempel versehen werden sollen. Der Hash wird an den Dienst gesendet, der ihn mit einem Datum kombiniert und signiert. Die entstehende Datenstruktur wird Zeitstempel genannt und kann dann vom Client zusammen mit den Originaldaten archiviert werden.

Nun steht eine turnusmäßige Änderung an, auf die teilnehmende Einrichtungen am Wissenschaftsnetz gegebenenfalls reagieren müssen: Das Zertifikat, mit dem der Dienst die Zeitstempel signiert, muss ausgetauscht werden. Das neue Zertifikat stammt aus der DFN-Verein Community-PKI. Durchgeführt wird der Zertifikatswechsel zum 23. Juni 2026. Das bedeutet, dass Nutzende die DFN-Verein Community-PKI in ihren Systemen hinterlegen müssen, um die ausgestellten Zeitstempel weiterhin prüfen zu können. ◆

Die Dokumentation des Dienstes ist abrufbar unter:
https://doku.tid.dfn.de/de:dfnpki:zeitstempeldienst

Hinweise zum Zertifikatswechsel finden Sie in den FAQ zum Zeitstempeldienst:
https://doku.tid.dfn.de/de:dfnpki:zeitstempeldienst:faq

Neu in easyroam: Gast- und Maschinen-Accounts möglich

Der eduroam-Zugang mit easyroam wird um ein neues Feature erweitert: Künftig können lokale Gast-Accounts sowie lokale Maschinen-Accounts genutzt werden. Mit der Gast-Authentifizierung können Einrichtungen temporäre Zugänge für Personen bereitstellen, die über keinen eduroam-Account verfügen und nur für einen begrenzten Zeitraum auf Netzwerkressourcen zugreifen müssen. Den Gast-Accounts können dabei mehrere Profile mit unterschiedlichen Seriennummern zugeordnet werden, sodass sich verschiedene Geräte auch zeitlich befristet authentifizieren und unterscheiden lassen.

Mit der Erweiterung reagiert easyroam auf typische Anforderungen aus dem Betrieb vor Ort und schafft zusätzliche Flexibilität bei der Verwaltung von Zugängen – etwa für Gäste oder Geräte wie Infotafeln und Smartboards.

Die Diensterweiterung easyroam ermöglicht über die DFN-AAI einen vereinfachten und sicheren Zugang zum weltweiten WLAN-Zugangsdienst eduroam. easyroam verzichtet dabei auf passwortbasierte Authentifizierung und setzt ausschließlich auf zertifikatsbasierte Verfahren über EAP-TLS. Aktuell nutzen über 130 Einrichtungen mit knapp 400 000 Anwenderinnen und Anwendern easyroam. ◆

Weitere Informationen zu easyroam finden Sie unter:
https://doku.tid.dfn.de/de:eduroam:easyroam

GÉANT TCS: einfacher Bezug von S/MIME-Zertifikaten per DFN-AAI-Login

Seit Mitte 2025 steht im GÉANT Trusted Certificate Service (TCS) eine Methode zur Verfügung, mit der User ohne weiteren manuellen Eingriff vonseiten der Administration S/MIME-Zertifikate beziehen können, die ihren Namen und ihre Organisationszugehörigkeit enthalten.

Um das Verfahren zu aktivieren, müssen teilnehmende Einrichtungen gegenüber dem TCS-Anbieter HARICA (Hellenic Academic and Research Institutions Certification Authority) einmalig eine Zusicherung über die Korrektheit der Daten in der DFN-AAI abgeben und die AAI-Attributfreigaben konfigurieren. User können sich dann über die DFN-AAI bei HARICA einloggen und ein entsprechendes Zertifikat beziehen, ohne dass Mitarbeitende der Einrichtung noch einmal Identifizierungsdaten oder Zugehörigkeiten bestätigen müssen. ◆

Eine ausführliche Dokumentation finden Sie unter:
https://doku.tid.dfn.de/de:dfnpki:tcs:2025:usercerts

KONTAKT
Wenn Sie Fragen oder Kommentare zum Thema „Sicherheit im DFN“ haben, schicken Sie bitte eine E-Mail an **sicherheit@dfn.de**

Mitarbeit an dieser Ausgabe Sicherheit aktuell:
Heike Ausserfeld, Jürgen Brauckmann, Ralf Paffrath

Lehrkraft im Doppelpack: das Projekt „Professor Digital Twin“

Jederzeit verfügbar und immer gut gelaunt? Inwieweit digitale Zwillinge von Professorinnen oder Professoren die Lehre sinnvoll unterstützen können, untersucht derzeit die Technische Universität München in ihrem Projekt „Professor Digital Twin“. Ziel ist es unter anderem, herauszufinden, welche Lehr- und Lernsituationen sich für den Einsatz eignen. Die spannende Frage bleibt jedoch: Wie reagieren die Studierenden auf eine virtuelle Lehrkraft?

Text: **Matthias Baume** (Technische Universität München, TUM)

Original und Avatar im direkten Vergleich: Dr. Matthias Baume von der Technischen Universität München (TUM) untersucht, wie Lehrende von ihren virtuellen KI-Abbildern bei Vorlesungen, Prüfungen und bei der Betreuung von Studierenden unterstützt werden können | *Foto: TUM*

Die Technische Universität München (TUM) ist eine der größten Präsenzuniversitäten in Deutschland, mit rund 52 000 Studierenden und etwa 13 000 Beschäftigten – davon um die 700 Professorinnen und Professoren. Das bedeutet: Im Schnitt betreut jede Professorin bzw. jeder Professor etwa 75 Studierende. Insbesondere in großen Grundvorlesungen mit teils mehr als 1 000 Teilnehmenden ist das Betreuungsverhältnis dementsprechend weitaus ungünstiger.

Hochschullehrende sind in vielen Rollen gleichzeitig gefragt und bewältigen täglich eine Vielzahl an Aufgaben: Zusätzlich zur Lehre und Betreuung von Studierenden betreiben sie Forschung, präsentieren ihre Ergebnisse auf Konferenzen und bilden Promovierende aus. Darüber hinaus engagieren sie sich in Gremien und vieles mehr. Gleichzeitig wünschen sich Studierende, ihre Dozentinnen und Dozenten wären einfacher und häufiger ansprechbar – außerdem bei Bedarf eine Unterstützung in der Lerngruppe und Hilfe bei der Prüfungsvorbereitung. Gerade in großen

Lehrveranstaltungen ist das jedoch kaum leistbar. Die Erwartungen sind hoch – die verfügbare Zeit begrenzt.

Prof. Dr.-Ing. Gerhard Müller, Geschäftsführender Vizepräsident für Studium und Lehre an der TUM: „Das Projekt ‚Professor Digital Twin' ist für uns ein weiterer, besonders spannender Baustein in unserer Arbeit an neuen Perspektiven für die Weiterentwicklung von Studium und Lehre. Dabei geht es uns nicht nur um die Erprobung des Einsatzes virtueller Professorinnen und Professoren, sondern zugleich um die systematische Untersuchung im Hinblick auf deren Wirkung auf Studierende. Die TUM Future Learning Initiative 2025 schafft hierfür einen geeigneten Rahmen: Sie eröffnet Freiräume für experimentelle Ansätze und unterstützt die Entwicklung tragfähiger Konzepte für die Lehre der Zukunft."

Um Lösungen für diese Problematik zu entwickeln, hat die TUM das Projekt „Professor Digital Twin" ins Leben gerufen. Das Projekt zählt zu den Gewinnern der internen „TUM Future Learning Initiative 2025" (TFLI 2025), die innovative Ansätze für die Lehre der Zukunft fördert. Innerhalb von zwölf Monaten erstellen verschiedene Professorinnen und Professoren digitale Abbilder ihrer selbst – sogenannte digitale Zwillinge – und erproben diese in unterschiedlichen Hochschulszenarien. Ziel ist es, herauszufinden, in welchen Lehr- und Lernsituationen sich digitale Zwillinge sinnvoll einsetzen lassen und wie Studierende diese wahrnehmen. Können ihre virtuellen Abbilder die Studierenden möglicherweise stärker zum Lernen motivieren als ein Chatbot oder ein abstrakter Avatar?

Was ist ein digitaler Zwilling?

In den vergangenen Jahren hat sich das Konzept des digitalen Zwillings (Digital Twin) in der Wirtschaft und in der Wissenschaft, aber auch im Bildungs- und Hochschulbereich zunehmend etabliert. Dahinter steht die Idee, ein virtuelles Abbild realer Gegenstände oder Artefakte zu entwickeln, um damit schneller und einfacher analysieren, planen, entwickeln oder forschen zu können. In der Praxis kommen digitale Zwillinge in unterschiedlichsten Szenarien zum Einsatz: Sie simulieren reale Bedingungen – etwa ein virtuelles Flugzeug im Windkanal – oder helfen, Eigenschaften und Entwürfe zu optimieren, beispielsweise die Belastbarkeit einer Brückenkonstruktion. Typische Anwendungsfelder reichen von einzelnen Maschinen über komplexe Infrastrukturen bis hin zu ganzen Städten, deren Planung und Betrieb so verbessert werden sollen. Dabei bildet ein digitaler Zwilling je nach Anwendungsfall sehr viele relevante Eigenschaften seines realen Gegenstücks möglichst präzise ab.

Der persönliche digitale Zwilling

Kombiniert man das Konzept des digitalen Zwillings mit den heutigen großen Sprachmodellen, so lässt sich daraus ein persönlicher digitaler Zwilling (Personal Digital Twin) entwickeln. Diese digitale Repräsentation einer realen Person wird mithilfe spezieller Software dreidimensional generiert und erhält dadurch ein mit der Originalperson vergleichbares Aussehen, eine ähnliche Stimme sowie weitere charakteristische Eigenschaften.

Zusätzlich kann der persönliche digitale Zwilling mit individuellen Inhalten sowie Interaktionen, etwa in Form von Gesprächen, trainiert werden. Auf diese Weise lässt sich auch das Fachwissen der realen Person abbilden. Diese kann über eine entsprechende Nutzerschnittstelle einfach neue Inhalte bereitstellen oder den persönlichen Digital Twin für andere Personen freischalten. Wie wäre es, wenn der persönliche digitale Zwilling Alltagsaufgaben wie Terminvereinbarungen oder Telefonate übernehmen oder bei Abwesenheit wichtige Informationen weitergeben könnte? Denkbar wäre auch, Charakter und Erscheinungsbild der realen Person auf diese Weise für die Nachwelt zu erhalten.

Aufgrund seiner digitalen Natur lässt sich der persönliche digitale Zwilling problemlos vervielfältigen und in parallelen Settings gleichzeitig einsetzen. Dadurch können mehrere Instanzen desselben Zwillings gleichzeitig Anfragen bearbeiten oder Personen beraten – ohne dass sich die reale Person „zerteilen" muss. Das ist bei Weitem nicht vergleichbar mit irgendeinem Chatbot als Ansprechpartner oder einer Telefonwarteschleife. Vielmehr entsteht der Eindruck einer persönlichen Interaktion und Unterstützung.

Das Projekt „Professor Digital Twin"

Digitale Zwillinge von Lehrenden bieten das Potenzial, bestehende Lehrformate gezielt zu ergänzen und die Betreuung von Studierenden skalierbarer zu machen. Dazu wird der digitale Zwilling einer Professorin oder eines Professors mit fachlichen Inhalten trainiert und in unterschiedliche Lehr- und Lernszenarien integriert. Seine Stärke liegt in der parallelen Einsetzbarkeit: Der digitale Zwilling ist jederzeit erreichbar und kann unabhängig von Zeit und Ort Fragen beantworten, Inhalte erläutern und Studierende individuell unterstützen.

In der Vorlesung:
Individuelle Rückfragen lassen sich parallel zur laufenden Lehrveranstaltung vom digitalen Zwilling klären, ohne dass die reale Lehrkraft ihre Vorlesung unterbrechen muss.

Während persönlicher Lernphasen und in der Lerngruppe:
Der digitale Zwilling kann als zusätzlicher fachlicher, kontinuierlich verfügbarer Ansprechpartner eingebunden werden, um Verständnisfragen zu klären oder Inhalte zu vertiefen. Auch beim individuellen Lernen steht er als kontinuierlich verfügbarer Ansprechpartner zur Verfügung und unterstützt beim Verständnis und der Vertiefung von Lehrstoff.

In der Prüfungsvorbereitung:
Durch Abfragen von Lehrinhalten, wiederholte Erklärungen und strukturierte Aufbereitung von Lehrstoff kann der digitale Zwilling Studierende gezielt auf Prüfungen vorbereiten.

Perspektivisch in Prüfungsszenarien:
Langfristig könnten digitale Zwillinge auch in Prüfungsprozesse eingebunden werden, etwa zur Unterstützung bei mündlichen Prüfungen in großen Kohorten. Bislang waren derartige Prüfungsszenarien nur mit immensem Aufwand und einer Mindestanzahl an unterschiedlichen Prüfenden umsetzbar. Dieser Ansatz eröffnet zwar organisatorische Spielräume, wirft jedoch didaktische und rechtliche Fragen auf.

Prof. Dr. Hanna Hottenrott, Professorin für Innovationsökonomik an der TUM: „Im laufenden Semester betreue ich eine große Vorlesung mit ca. 1000 Studierenden. Da ist die Unterstützung von einzelnen Teilnehmenden nicht ganz einfach. Wenn mein Digital Twin beispielsweise bei der Beantwortung von Fragen zur Vorlesung oder bei der Prüfungsvorbereitung mithilft, wäre das auf jeden Fall eine Entlastung. Im Moment glaube ich aber nicht, dass ein Digital Twin eine echte Lehrkraft wirklich ersetzen könnte."

Das Projekt „Professor Digital Twin" untersucht den Einsatz von digitalen Zwillingen mithilfe von grundlegenden Fragestellungen und entsprechenden Forschungsmethoden.

Die übergeordneten wissenschaftlichen Fragestellungen sind:

- Wie nehmen Studierende den Digital Twin wahr? Inwiefern unterscheidet sich das Lernen mit dem Digital Twin vom Austausch mit einer echten Lehrkraft?
- Welche Vor- und Nachteile hat der Einsatz eines Professor Digital Twin?
- In welchen praktischen Anwendungsfeldern eignen sich Digital Twins zur Unterstützung der Studierenden?

Die teilnehmenden Studierenden füllen nach den jeweiligen Szenarien einen Fragebogen aus und können dort ihre Sichtweise und Wahrnehmung detailliert einbringen. Ergänzend werden bei Bedarf Einzelinterviews mit Studierenden und Dozierenden geführt.

Welche Potenziale und Risiken sind zu berücksichtigen?

Digitale Zwillinge lassen sich in der Lehre nahtlos einsetzen: Damit können sie Lehr- und Lernszenarien gezielt ergänzen, ohne bestehende Strukturen grundlegend zu verändern. Sie ermöglichen eine flexiblere und individuellere Unterstützung der Studierenden, etwa durch zusätzliche Erklärangebote und eine zeitunabhängige Verfügbarkeit. Gleichzeitig können sie Lehrende entlasten, indem sie wiederkehrende Fragen übernehmen oder Inhalte ergänzend vermitteln. Dadurch entstehen Freiräume für andere Aufgaben in Forschung, Lehre und Betreuung.

Risiken und offene Fragen
Mit dem Einsatz digitaler Zwillinge sind jedoch auch Risiken verbunden. Digitale Zwillinge lassen sich aus unterschiedlichen Quellen erzeugen. Das kann prinzipiell öffentlich verfügbares Bild- und Videomaterial sein. Es stellt sich die Frage nach der Authentizität: Wie lässt sich sicherstellen, dass ein digitaler Zwilling tatsächlich vom realen Vorbild autorisiert ist und verlässliche Inhalte vermittelt?

Hinzu kommen Herausforderungen im Umgang mit Inhalten: Digitale Zwillinge können

Prof. Dr. Felix Ehrlenspiel, Leitung des Arbeitsbereiches Sportpsychologie an der TUM: „Ich finde es spannend, mit KI neue Erfahrungen in der Lehre zu sammeln. Ob ein Digital Twin von mir in der Praxis besser angenommen wird als andere KI-Lösungen, wird sich zeigen, aber ich könnte mir vorstellen, dass unsere Studierenden dem gegenüber sehr aufgeschlossen sind. Im laufenden Semester habe ich mehrere verschieden große Lehrveranstaltungen, die sich gut für den Einsatz eignen. Und wenn mir mein Digital Twin dann am Ende etwas Unterstützungsarbeit abnimmt – umso besser!"

nur auf Basis der ihnen verfügbaren Informationen agieren. Es bleibt daher zu klären, wie mit möglichen Wissenslücken oder fehlerhaften Antworten sowie allgemein mit Diskrepanzen zwischen digitalem Zwilling und der realen Lehrperson umgegangen wird.

Auch für den Prüfungsbereich ergeben sich offene Fragen, etwa hinsichtlich rechtlicher Rahmenbedingungen, Verlässlichkeit und Fairness. Der Einsatz in prüfungsrelevanten Situationen erfordert daher besondere Sorgfalt und klare Regeln.

Fazit

Es wird deutlich, dass im Projekt „Professor Digital Twin“ noch zahlreiche Fragen offen sind, die sich heute nur begrenzt beantworten lassen. Gleichzeitig entwickeln sich Sprachmodelle und Avatar-Technologien mit hoher Dynamik weiter und finden bereits zunehmend Anwendung in Wirtschaft und Gesellschaft. Gerade vor diesem Hintergrund ist das Projekt für die Technische Universität München von besonderer Relevanz.

Entscheidend wird sein, wie Studierende den Einsatz digitaler Zwillinge tatsächlich bewerten und ob sie diese als sinnvolle Unterstützung im Lernprozess annehmen. Die Ergebnisse des Projekts werden in den kommenden Monaten vorliegen und veröffentlicht. Sie dürften eine wichtige Grundlage dafür liefern, wie sich digitale Zwillinge künftig in der Hochschullehre einordnen lassen – und ob sie den Weg vom Experiment in den Alltag finden. ◆

SOFTWARE UND HARDWARE

Software für die Erstellung digitaler Zwillinge
Für die Erstellung persönlicher digitaler Zwillinge kommt spezialisierte Software zum Einsatz. Im Projekt „Professor Digital Twin“ wird dafür die Plattform mindbank.ai genutzt. Darüber hinaus existieren weitere Software-Lösungen, die ähnliche Funktionen bieten.

Hardware für den Einsatz im Hörsaal
Im Projekt ist vorgesehen, digitale Zwillinge auch in Präsenz direkt in Lehrveranstaltungen einzubinden. Perspektivisch könnten sie Teile von Vorlesungen übernehmen und vor Ort im sozialen Rahmen der Hochschule dargestellt werden. Für eine möglichst realitätsnahe Darstellung bietet sich der Einsatz einer sogenannten Holobox an, anstelle eines Beamers. Diese ist etwa so groß wie eine klassische Telefonzelle und ermöglicht die quasiholografische, dreidimensionale Darstellung von Personen. Über integrierte Mikrofone und Lautsprecher kann sie zudem mit der Umgebung interagieren.

INFORMATIONEN ZUM PROJEKT

Publikation zum Projekt:
M. Baume: „Professor Digital Twin“ – A (R)Evolution in Teaching!? Proceedings of INTED2026 Conference, Valencia, Spain 2026, Article: 1729, ISBN: 978-84-09-82385-7, doi: 10.21125/inted.2026.1729.

Infos zur TUM Future Learning Initiative:
https://www.tum.de/studium/im-studium/tum-future-learning-initiative

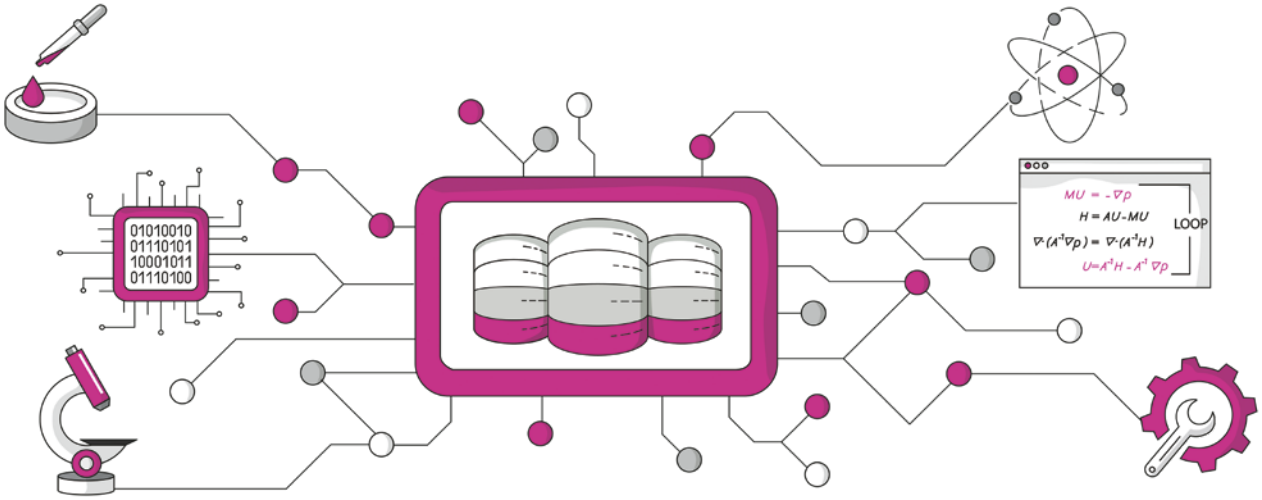
Video-Kurzfassung des Projekts:
https://www.youtube.com/watch?v=ArDeVf-7ao8

Die Webseite zum Projekt:
https://www.prolehre.tum.de/prolehre/angebote/forschung-und-innovation/projekte/professor-digital-twin/

NHR-Verbund stellt Datenspeichersysteme für die NFDI bereit

Der Verein für Nationales Hochleistungsrechnen (NHR-Verein) entwickelt leistungsfähige Datenspeicher für die Nationale Forschungsdateninfrastruktur (NFDI-Verein).Die geplante Infrastruktur wird sowohl Komponenten für die längerfristige Speicherung als auch für hochperformante, eng mit den HPC-Rechensystemen verbundene Speicherlösungen enthalten. Das Zugriffsmanagement für diese Ressourcen wird im Rahmen des IAM4NFDI-Projekts realisiert, das die RWTH Aachen und der DFN-Verein gemeinsam koordinieren.

Text: **Matthias S. Müller**, **Marius Politze** (RWTH Aachen), **Philipp Wieder** (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen, GWDG)



In einer konzertierten Aktion und in enger Abstimmung mit Bund und Ländern hat die Deutsche Forschungsgemeinschaft (DFG) im vergangenen Jahr eine Ausschreibung zur Unterstützung von Investitionen in Datenspeichersysteme für die Nationale Forschungsdateninfrastruktur (NFDI) durchgeführt. Von den neun erfolgreichen Anträgen stammen sechs aus dem Verbund für Nationales Hochleistungsrechnen (NHR). Die sieben an den Anträgen beteiligten NHR-Zentren bauen ihr untereinander abgestimmtes Angebot auf dieser Basis nun so aus, dass die NFDI-Konsortien disziplinspezifische Forschungsdatenservices implementieren können.

Der Aufbau der Speichersysteme basiert auf der etablierten Expertise und den Kompetenzen des NHR-Verbunds bei der Bereitstellung überregionaler, universitätsübergreifender und hochskalierbarer IT-Infrastrukturen. Dennoch gibt es spezifische Anforderungen bei der Versorgung der NFDI-Konsortien mit Speicher für Forschungsdatenservices, die der NHR-Verbund gezielt berücksichtigen muss. Zudem sollen die Ressourcen mit den existierenden

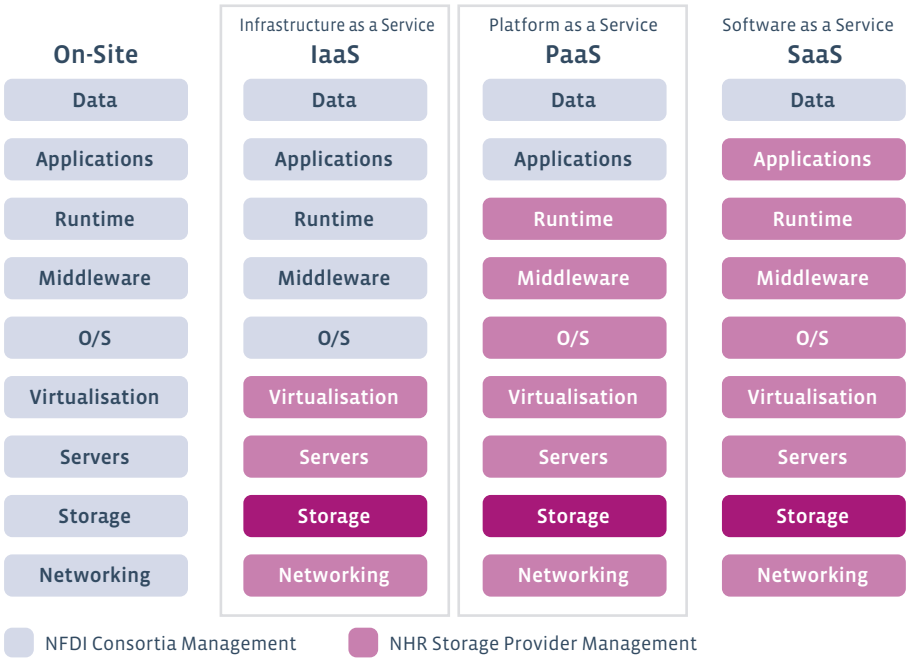


Abbildung 1: Stufen des Cloud-Modells. Ein Großteil der Services wird auf der Infrastruktur- oder Plattformebene zwischen den NHR-Zentren und den NFDI-Konsortien übergeben.

HPC-Systemen verbunden werden, sodass Forschungsdaten für die Analysen der datengetriebenen Forschung – beispielsweise für KI-Training und KI-Inferenz – zugänglich sind.

Gleichzeitig müssen Mechanismen etabliert werden, um Speicherkapazitäten zwischen den NFDI-Konsortien aufteilen zu können. Das geschieht einerseits über die Anbindung an das föderierte Identitätsmanagement für die NFDI, das im Rahmen des von der RWTH und dem DFN-Verein gemeinsam koordinierten IAM4NFDI-Projekts aufgebaut wird. Andererseits müssen in diesem Zusammenhang auch Richtlinien der noch im Aufbau befindlichen EOSC-Föderation beachtet und eingehalten werden.

Strukturierung des Speicherangebots

Die Wahl der richtigen Technologien, Leistungs- und Redundanzklassen kann nur disziplinspezifisch durch die NFDI-Konsortien und für ihre jeweiligen Services getroffen werden. In Absprache mit diesen baut der NHR-Verbund die Speichersysteme daher so aus, dass ein möglichst breites Spektrum an Disziplinen abgedeckt werden kann. Hinzu kommen Virtualisierungsschichten für Protokollübersetzungen, Datenabfragen oder Zugriffsmanagement, die sich auf HPC-Systemen nicht wirtschaftlich ausführen lassen.

Cloud-Anbieter definieren (technische) Übergabepunkte für das Verhältnis von Dienstnehmern und -gebern. Dieses Modell lässt sich auch auf NHR-Zentren und NFDI-Konsortien übertragen. Im Fall der Speicherinfrastrukturen soll die Übergabe auf der Ebene von Infrastruktur- oder Plattformservices stattfinden,[1] sodass die NFDI-Konsortien ihre Services auf diesem Angebot aufbauen können. Eine Übergabe auf Ebene der Software-Services (SaaS) ist hingegen nur sinnvoll, wenn NHR-Zentren bereits Forschungsdatenservices anbieten, die den Anforderungen der NFDI-Konsortien entsprechen (vgl. Abbildung 1).

Integration in eine (inter-)nationale Gesamtarchitektur

Die NFDI-Konsortien sind dafür verantwortlich, einen Forschungsdatenlebenszyklus zu etablieren und die Forschungsdatendienste für ihre jeweilige Community aufzubauen und zu betreiben. Daraus ergibt sich eine Governance mit zwei Übergabepunkten: zwischen dem NHR-Zentrum und

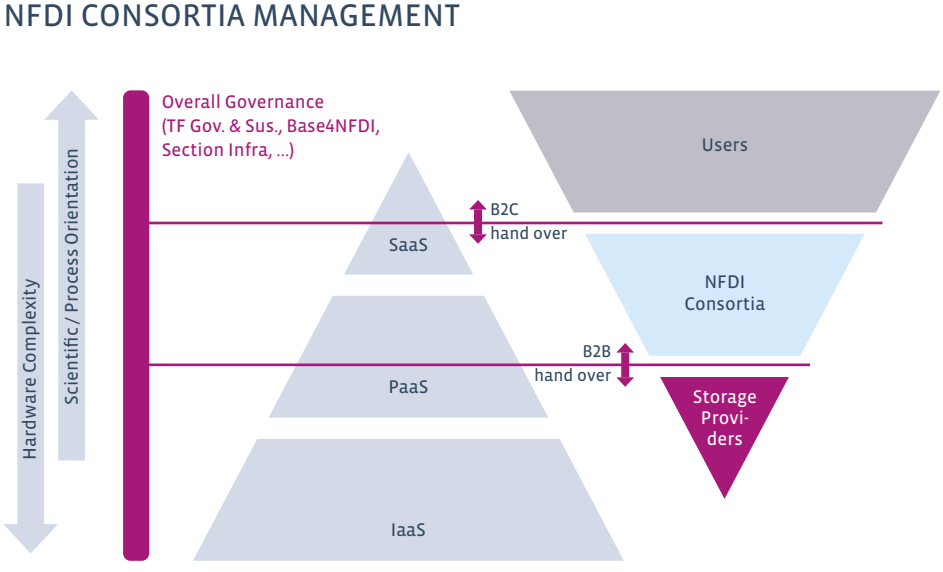


Abbildung 2: Das Übergabemodell illustriert die verschiedenen Dienstleisterrollen von Speicheranbietern und NFDI-Konsortien.

1 vgl. https://doi.org/10.6028/nist.sp.800-145, IaaS, PaaS

Die Speichersysteme werden zentrenübergreifend in verschiedene Leistungsklassen eingeteilt:

- **Hot:** Speicher für hochfrequent geänderte Daten mit schnellem, wahlfreiem Lese- und Schreibzugriff über ein Dateisystem.
- **Warm:** Speicher für Daten, die sich weniger häufig ändern, aber regelmäßigen Zugriff erfordern.
- **Cold:** Speicher für Daten, die einmal geschrieben nicht erneut modifiziert werden und auf die nur selten zugegriffen wird.

Zudem ist der Schutz vor Datenverlust durch technische Fehlfunktionen, Schadensereignisse oder Naturkatastrophen eine weitere Dimension:

- **Local:** Eine einzelne Kopie der Daten wird im Speichersystem vorgehalten.
- **Local Redundant:** Eine weitere Kopie oder mehrere Versionen werden direkt auf oder in unmittelbarer Nähe des Speichersystems vorgehalten.
- **Geo Redundant:** Daten werden über mindestens zwei örtlich getrennte Rechenzentren verteilt, sodass eine Resilienz gegenüber lokal begrenzten Katastrophen gewährleistet wird.

dem NFDI-Konsortium (engl. Business-to-Business, B2B) sowie zwischen dem NFDI-Konsortium und den Forschenden in der jeweiligen Community (engl. Business-to-Community, B2C).

Es entsteht ein Übergabemodell, das ebenfalls in der Arbeitsgruppe Overall Architecture der NFDI-Sektion Common Infrastructures für die Zusammenarbeit zwischen Dienstleistern und der Forschungscommunity identifiziert wurde (vgl. Abbildung 2). Eine weitere Konkretisierung ist das Schichtenmodell, das den Aufbau technischer Dienste näher spezifiziert.[2] Neben den traditionellen Dateisystemen werden dort vor allem Objektspeicher gefordert, da diese sich einfacher und kostengünstiger in die Services der NFDI-Konsortien integrieren lassen.

Auf diese Weise werden eine grundlegende Interoperabilität sowie konkrete Verantwortlichkeiten zwischen den Akteuren geschaffen. Damit entstehen die notwendigen technischen Strukturen, auf deren Basis die NFDI ihre Rolle als „EOSC German National Node“ einnehmen kann. Ein wesentlicher Bestandteil auf diesem Weg ist die Implementierung des oben genannten föderierten Identitätsmanagements. Sowohl der NHR-Verbund als auch die NFDI nutzen dabei bestehende Infrastrukturen wie die DFN-AAI und implementieren allgemein anerkannte Standards wie die AARC Blueprint Architecture[3] sowie weitere Richtlinien der AARC-Community. So sind sie bereits heute konzeptionell und auch technisch interoperabel.

Forschungsdaten für datengetriebene Forschung und KI

Die aktuellen Speichersysteme der NHR-Zentren sind eng mit den HPC-spezifischen Abläufen und Werkzeugen verknüpft. Die Ausweitung auf Forschungsdaten aus den NFDI-Konsortien sowie die Ergänzung des dateisystembasierten Zugriffs um beispielsweise Objektspeicher-Schnittstellen stellen einen klaren Vorteil dar. Forschende können mit denselben Bibliotheken und Arbeitsabläufen auf Datensätze zugreifen, wie sie es von kommerziellen Cloud-Anbietern gewohnt sind. Die Co-Location von Daten und Rechenleistung bietet einen weiteren Vorteil für KI und datengetriebene Experimente. Forschungsdaten können direkt oder mit minimalen Datentransferzeiten auf HPC-Systemen genutzt werden. Dadurch werden Hochdurchsatz-Experimente ermöglicht, wie das Tuning von KI-Modellen oder die KI-Inferenz mit kuratierten Referenzdaten (engl. Ground Truth).

Fazit

Die NHR-Zentren positionieren sich als Dienstleister für die NFDI-Konsortien mit einem Angebot, das verschiedene Technologie-, Leistungs- und Redundanzklassen abbildet. Die Integration von Datenspeichern in HPC-Zentren unterstützt dabei besonders datengetriebene Forschung und KI. Über definierte Übergabepunkte werden Verantwortlichkeiten für die Diensterbringung klar aufgeteilt, um disziplinspezifische Communities mit hochwertigen Forschungsdatenservices zu versorgen. ◆

Der Beitrag entstand in Zusammenarbeit mit weiteren Expertinnen und Experten aus dem NHR-Verbund:
Thomas Eifert (RWTH Aachen), Andreas Wolf (TU Darmstadt), Andreas Petzold (KIT), Matthias Lieber (TU Dresden), Theresa Höhne (ZIB), Holger Nitsche (Universität Paderborn), Jens Simon (Universität Paderborn), Ann-Kathrin Häfner (Goethe-Universität Frankfurt)

Weitere Informationen zum NHR-Verein finden Sie unter: **https://www.nhr-verein.de/**
Informationen zum Projekt IAM4NFDI gibt es unter: **https://base4nfdi.de/projects/iam4nfdi**

2 https://doi.org/10.5281/zenodo.18755450

3 https://aarc-community.org/architecture/

Taugt Backup als Archiv?

Die Trennung von Backup und Archiv gehört zu den bekannten Grundprinzipien in der IT – in der Praxis wird sie häufig nicht konsequent umgesetzt. Warum es sich lohnt, diesen Ansatz neu zu betrachten, zeigt die RWTH Aachen University. Sie macht deutlich, wie sich Datenbestände gezielter steuern, Wiederherstellungen beschleunigen und Anforderungen aus Verwaltung, Forschung und IT sauber voneinander trennen lassen.

Text: **Thomas Eifert** (RWTH Aachen)

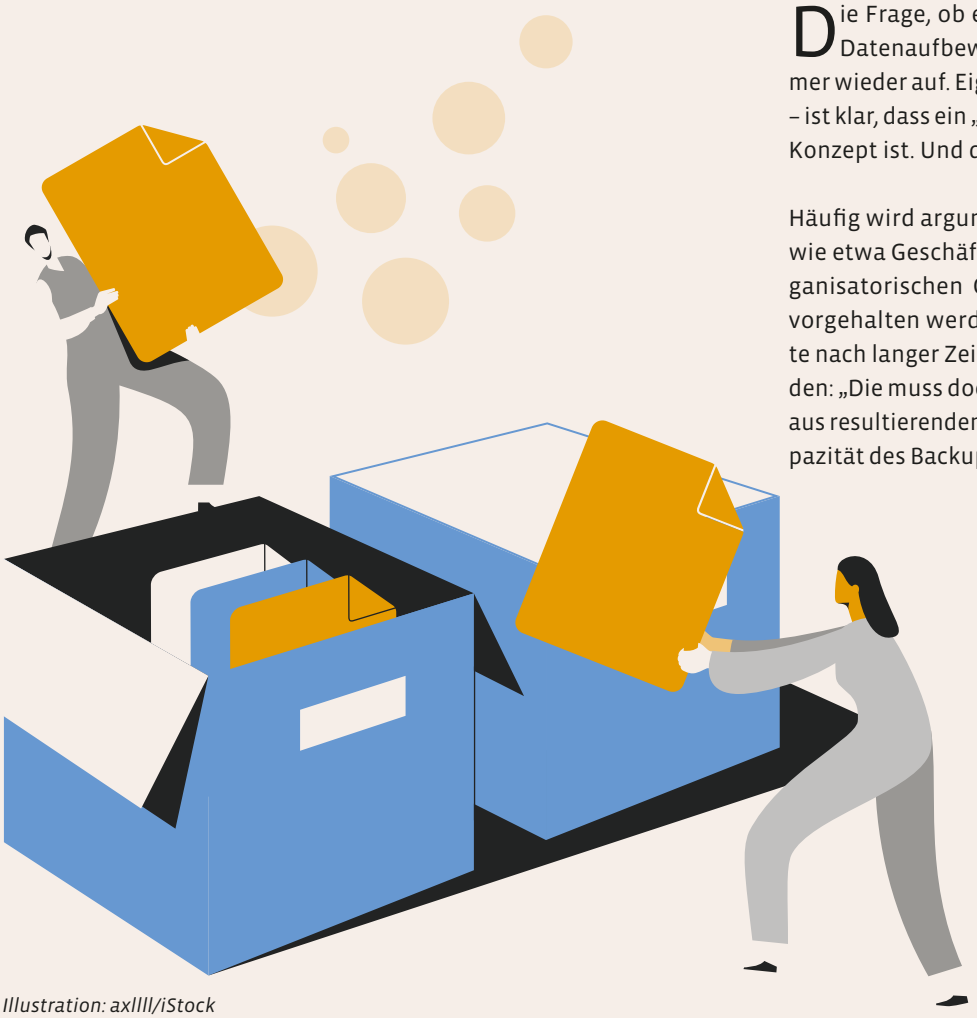


Illustration: axllll/iStock

Die Frage, ob ein Backup auch als langfristige Datenaufbewahrung dienen kann, taucht immer wieder auf. Eigentlich – zumindest theoretisch – ist klar, dass ein „Langzeit-Backup“ ein überholtes Konzept ist. Und dann holt uns die Realität ein …

Häufig wird argumentiert, dass bestimmte Daten wie etwa Geschäftsdaten aus rechtlichen oder organisatorischen Gründen über lange Zeiträume vorgehalten werden müssen. Oder jemand möchte nach langer Zeit eine vermisste Datei wiederfinden: „Die muss doch noch im Backup sein!“ Die daraus resultierenden hohen Anforderungen an die Kapazität des Backup-Systems führen dann häufig zu

der Unterscheidung in „heiße“ und „kalte“ Daten und zu der Lösung, letztere auszulagern, um unterschiedliche Zugriffshäufigkeiten und Aufbewahrungszeiten abzubilden. Auf den ersten Blick wirkt dieser Ansatz plausibel. Bei genauerer Betrachtung zeigt sich jedoch, dass dadurch eine Reihe von Problemen entsteht. Aus diesem Grund hat sich das IT-Center der RWTH Aachen University dafür entschieden, unterschiedliche Lösungen für die Aufbewahrung von Daten (möglichst) strikt zu trennen.

Der Zweck eines Backups ist eigentlich klar definiert: Es dient dazu, den letzten bekannten guten Zustand eines Systems zu sichern. Ziel ist es, im Falle eines Fehlers, eines Unfalls oder eines Angriffs – beispielsweise durch Schad-Software – einen Datenverlust zu vermeiden und das System

> In jedem Fall enthält das Backup-System den oder die (wenigen) Zustände, aus denen im Ernstfall die IT wiederhergestellt werden kann.

möglichst schnell wieder in einen funktionsfähigen Zustand zu versetzen. Es handelt sich also um einen systemgetriebenen Ansatz. Im Mittelpunkt stehen das IT-System und seine Wiederherstellbarkeit.

Was macht Backup?

Backup-Systeme arbeiten in der Regel mit periodischen Sicherungen. Wenn ein Langzeit-Backup erstellt wird, werden zusätzliche, termingebundene Sicherungen zu bestimmten Anlässen durchgeführt. Zwischen diesen Sicherungsarten entstehen komplexe Abhängigkeiten, die für Anwender meist unsichtbar bleiben, weil sie tief im Innern der Backup-Software verborgen sind. Dennoch bestimmen sie maßgeblich, wie Daten gesichert werden und wie eine Wiederherstellung funktioniert.

Ein weiterer wichtiger Punkt ist, dass eine Sicherung immer zum Zustand des Systems im Moment der Sicherung passt. Das bedeutet: Das Backup bildet ein konkretes System inklusive dessen Struktur, dessen Konfiguration und dessen Daten zu einem bestimmten Zeitpunkt ab. Genau darin liegt auch ein Zielkonflikt. Einerseits möchte man für die langfristige Speicherung eine möglichst generische Sicherung, die viele verschiedene Anforderungen erfüllt. Andererseits soll das Backup effizient sein – sowohl bei der Sicherung als auch bei der Wiederherstellung. In manchen Fällen ist es sogar notwendig, nicht nur die Daten, sondern auch die Anwendung selbst mitzusichern, um später wieder auf einen konsistenten Zustand zurückkehren zu können.

„Wie lange habe ich denn nun Backup?“

Die Aufbewahrungszeit von Backups richtet sich nicht primär nach organisatorischen oder rechtlichen Anforderungen, sondern eher nach technischen Überlegungen. Ein Beispiel dafür ist die Frage, wie lange eine mögliche Malware unentdeckt in einem System verbleiben kann. Daraus ergibt sich eine heuristische Entscheidung darüber, wie lange Sicherungen verfügbar bleiben sollten, um im Ernstfall auf einen Zustand zurückgreifen zu können, der noch nicht kompromittiert war. Gleichzeitig ist die Maximalzeit dadurch beschränkt, wie lange sich mit einer solchen systemseitigen Sicherung sinnvoll noch etwas anfangen lässt. In jedem Fall enthält das Backup-System den oder die (wenigen) Zustände, aus denen im Ernstfall die IT wiederhergestellt werden kann.

Ganz anders sieht es bei einer Wiederherstellung sehr alter Daten aus, etwa alter Buchungsdaten. Aus betrieblicher Sicht ist es meist nicht sinnvoll, solche Daten aus einem Backup in das Primärsystem wiederherzustellen, sondern, sie beispielsweise für eine Revision bereitzustellen. Damit gehört diese Aufgabe nicht zum eigentlichen Zweck eines Backups, sondern in den Bereich einer geordneten Datenaufbewahrung im Rahmen von Geschäftsprozessen. Wenn Daten über lange Zeiträume vorgehalten werden müssen, geschieht dies aus Gründen der Dokumentation, der Nachvollziehbarkeit oder aufgrund gesetzlicher Anforderungen – nicht weil das unterliegende IT-System sie in einer Sicherung gespeichert hat. Überdies kann – je nach Aufbewahrungsfrist – das IT-System in der Zwischenzeit erneuert oder ersetzt worden sein, was die Verwendbarkeit einer solchen systembezogenen Sicherung infrage stellt.

Damit wird deutlich: Diese Form der Aufbewahrung von Daten passt nicht wirklich zu einem Backup. Die Notwendigkeit ergibt sich aus dem jeweiligen Geschäftsprozess und nicht aus dem IT-System selbst. Daraus folgt die logische Konsequenz, systemgetriebene und prozessgetriebene Aufbewahrung voneinander zu trennen. Diese Trennung führt zu den komplementären Ansätzen Backup und Datenarchiv.

Für eine Einrichtung wie die RWTH Aachen ergibt sich daraus ein klarer Lösungsansatz. Statt zu versuchen, ein einziges System für alle Zwecke zu nutzen, werden separate Lösungen für Backup und Archivierung eingesetzt. Das Backup übernimmt die Sicherung von Systemzuständen und dient der schnellen Wiederherstellung im Störfall. Das Archiv hingegen kümmert sich um die langfristige und strukturierte Aufbewahrung von Daten, deren Haltezeiten durch organisatorische, wissenschaftliche oder gesetzliche Anforderungen bestimmt werden.

Innerhalb des Archivs selbst ist eine weitere Differenzierung sinnvoll. Ein Bereich betrifft Dokumentenmanagementsysteme und Verwaltungsarchive. Hier werden Haltezeiten in erster Linie durch Geschäftsprozesse festgelegt sowie durch Compliance-Anforderungen oder gesetzliche Regelungen. Ein anderer Bereich betrifft Forschungsdaten. Für diese gelten in der Regel andere Kriterien. Oft orientiert sich die Aufbewahrungsdauer an den Regeln guter wissenschaftlicher Praxis, die beispielsweise eine Mindestaufbewahrung von zehn Jahren vorsehen können. Darüber hinaus kann es Forschungsdaten geben, die einen dauerhaften wissenschaftlichen Wert besitzen und deshalb in eine langfristige Datenhaltung oder Langzeitverfügbarkeit überführt werden sollten. Eine entsprechende Infrastruktur haben wir in die Landesinitiative für Forschungsdatenmanagement – fdm.nrw integriert. Hier existiert ein von mehreren NRW-Hochschulen kollaborativ erbrachter Service für alle Forscherinnen und Forscher an NRW-Hochschulen.

Schließlich gibt es noch einen dritten Bereich: Die „digitalen Reste“ sind Daten, die keinem klar definierten Prozess zugeordnet sind oder deren zukünftige Bedeutung unklar ist – die aber dennoch zumindest

> Ein wichtiger Punkt ist die Verlagerung von Single-Item-Recovery-Funktionen auf die Ebene des primären datenhaltenden Systems.

vorläufig aufgehoben werden sollen. Auch für diese Daten muss eine Lösung gefunden werden, allerdings nicht unbedingt innerhalb eines klassischen Backup-Systems.

„Single-Purpose“-Systeme mit klar definierten Aufgaben

Ein weiterer wichtiger Punkt in diesem Konzept ist die Verlagerung von Single-Item-Recovery-Funktionen auf die Ebene des primären datenhaltenden Systems. Ein typisches Beispiel hierfür ist ein E-Mail-System wie Exchange. Wenn einzelne Objekte – etwa eine E-Mail, ein Kalendereintrag oder ein Dokument – wiederhergestellt werden sollen, ist es wesentlich effizienter, dies direkt innerhalb des Systems zu tun, das diese Daten verwaltet. Das Backup dient hier „nur“ der Wiederherstellung nach einem großen Datenverlust.

Der Vorteil dieses Ansatzes liegt darin, dass wir zwar mehrere unterschiedliche Systeme betreiben müssen, jedes dieser Systeme jedoch klar auf einen bestimmten Zweck ausgerichtet ist, sodass nur „Single-Purpose“-Systeme mit klar definierten Aufgaben vorhanden sind. Diese Spezialisierung führt zu einer deutlichen Reduktion von Abhängigkeiten und Komplexität. Backup-Systeme müssen sich nicht mehr um langfristige Archivierungsanforderungen kümmern, und Archivsysteme müssen nicht die Anforderungen an schnelle Systemwiederherstellung erfüllen. Beide Bereiche können unabhängig voneinander optimiert werden.

Darüber hinaus ermöglicht die Trennung Optimierungen auf der Prozess- und der Kostenseite: Durch den geschäftsprozessgetriebenen Ansatz ist klar, welche Daten für welchen Zweck aufbewahrt werden. Darauf folgt unmittelbar, für welche Daten dies nicht der Fall ist, sodass diese aus der langfristigen Speicherung herausgehalten werden können – eine Unterscheidung, die auf Systemebene nicht möglich ist. Überdies ist damit auch ein wichtiger Aspekt des Business Continuity Management (BCM) adressiert, dass nämlich die geschäftskritischen Datenbestände hier bereits klar identifiziert sind.

Auf der technischen Ebene sorgt diese Trennung für den großen Gewinn: Zum Beispiel ist im Fall einer Erneuerung klar definiert, welche Datenbestände nach einer begrenzten Haltezeit obsolet sind und für welche Teile eine oft aufwendige Migration gestellt werden muss.

Fazit

Selbstverständlich war die Umsetzung dieses Trennungsansatzes auch mit einem gewissen Aufwand verbunden, insbesondere bei der Einführung auf Prozessebene. In vielen Einrichtungen existieren bereits große Mengen an Daten, die über Jahre hinweg in unterschiedlichsten Strukturen abgelegt wurden. Um die Trennung zwischen Backup und Archiv sauber umzusetzen, ist es unumgänglich, grundlegend aufzuräumen. Alternativ kann ein Stichtag definiert werden, ab dem neue Regeln gelten.

Eine pragmatische Lösung besteht darin, einen „Daten-Dachboden“ einzurichten. Dabei handelt es sich um einen Bereich, in dem unsortierte oder schwer einzuordnende Daten abgelegt werden können. Diese Daten sind zwar weiterhin verfügbar, werden jedoch nicht mehr aktiv in operative Prozesse integriert. Auf diese Weise lässt sich vermeiden, dass wertvolle Informationen verloren gehen, während gleichzeitig eine klare Struktur für neue Daten geschaffen wird.

Langfristig ermöglicht die Trennung von Backup und Archiv eine deutlich verbesserte Steuerung der Datenhaltung. Systeme bleiben übersichtlich, Wiederherstellungen werden effizienter, und die Anforderungen aus Verwaltung, Forschung und IT lassen sich klar voneinander abgrenzen. Genau darin liegt der eigentliche Vorteil eines solchen Ansatzes: Er schafft Klarheit darüber, wofür welche Systeme zuständig sind – und verhindert, dass ein Backup-System zu einer universellen, aber letztlich ungeeigneten Lösung für alle Formen der Datenaufbewahrung wird. ◆

Open Source VDI für Forschung und Lehre

Virtuelle Desktops sind längst im Hochschulalltag angekommen – doch steigende Kosten und proprietäre Abhängigkeiten stellen viele Einrichtungen vor neue Herausforderungen. Die VDI-Arbeitsgruppe der Abteilung eScience am Rechenzentrum der Albert-Ludwigs-Universität Freiburg geht deshalb neue Wege und entwickelt eine offene VDI-Plattform, die auf Flexibilität, Skalierbarkeit und digitale Souveränität setzt.

Text: **Rafael Gieschke, Michael Scherle, Dirk von Suchodoletz** (Albert-Ludwigs-Universität Freiburg)

Bei Virtual Desktop Infrastructures (VDI) – teilweise auch als Desktop as a Service bezeichnet – handelt es sich eigentlich um ein eher gut abgehangenes Thema, welches seit mehr als 30 Jahren eine Rolle bei der Ausgestaltung typischer IT-Stacks spielt. Die Vorteile sind hinlänglich bekannt: VDI bietet eine attraktive Alternative zur aufwendigen, dezentralen Bereitstellung und Pflege einzelner Rechner mit unterschiedlichen Software-Umgebungen. Gleichzeitig vereinfacht sie die Administration, bietet eine verbesserte Zugriffskontrolle und erhöht die Sicherheit. Darüber hinaus ermöglicht die Plattform eine effizientere und flexiblere Nutzung von Hard- und Software – und unterstützt nicht zuletzt Green-IT-Bestrebungen. Herausforderungen wie die zunehmende Nutzung von 3D-Grafik, schnelles Rendering und effizienter Remote-Transport wurden dabei gemeistert.

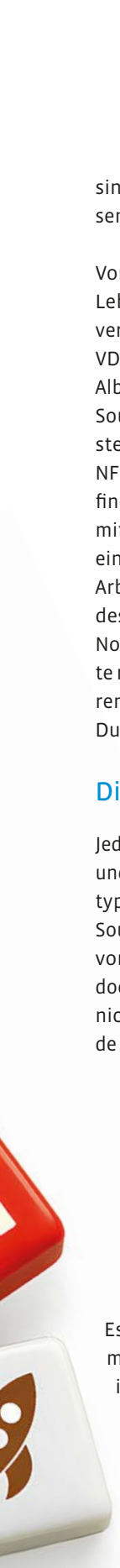
Obwohl der Bedarf durch flexiblere Arbeitsmodelle und komplexere wissenschaftliche Workflows insbesondere in Forschungseinrichtungen deutlich ansteigt, sind vor allem die (langfristigen) Kosten eine größere Herausforderung: Mit VMware hat Broadcom ein deutliches Signal gesetzt, und Citrix folgte im selben Kielwasser mit ebenfalls erhöhten Preisen. Der Markt wird derzeit von eher kommerziellen, teuren und proprietären Lösungen beherrscht, obwohl sehr viele Bausteine bereits im Open-Source-Umfeld vorhanden

sind – leider bisher zu verteilt, zu unvollständig oder mit diversen Unzulänglichkeiten behaftet.

Vor dem Hintergrund neuer Anforderungen aus Forschung und Lehre hinsichtlich einer langfristig tragfähigen und digital souveränen Lösung für unterschiedliche Use Cases identifizierte die VDI-Arbeitsgruppe der Abteilung eScience am Rechenzentrum der Albert-Ludwigs-Universität Freiburg bereits 2021 die für eine Open Source Virtual Desktop Infrastructure (OSVDI) notwendigen Bausteine in parallelen aufeinander aufbauenden Projekten (PePP, NFDI4BIOIMAGE, bwCloud 3). Die sich nun in der Entwicklung befindliche OSVDI verfolgt das Ziel, die typische Grafik-Workstation mit vollständig offenen und frei verfügbaren Software-Stacks auf einen Hypervisor oder in die Cloud zu verlagern. Dadurch können Arbeitsumgebungen mit einer Vielzahl grafischer Anwendungen des lokalen (Windows-)PCs konsolidiert werden. So entfällt die Notwendigkeit, große oder sensible Daten an entfernte Standorte mit potenziell schlecht zu schützenden Umgebungen zu kopieren. Das erleichtert das Datenmanagement, da das Kopieren und Duplizieren von Datensätzen vermieden wird.

Die technische Umsetzung

Jede VDI-Lösung erfordert das Zusammenspiel mehrerer Hardware- und Software-Komponenten. Kommerzielle Anbieter bündeln diese typischerweise zu einem vermarkteten Gesamtprodukt. Im Open-Source-Bereich gibt es kein direktes Äquivalent, jedoch eine Reihe von Komponenten, die sich kombinieren lassen. Häufig fehlt jedoch eine nahtlose Integration, oder es gibt einzelne Bausteine, die nicht optimal zusammenpassen. OSVDI zielt darauf ab, bestehende Ansätze weiterzuentwickeln und fehlende Module zu ergänzen.



> Dadurch können Arbeitsumgebungen mit einer Vielzahl grafischer Anwendungen des lokalen (Windows-)PCs konsolidiert werden.

Es gibt eine Reihe von klar abgrenzbaren Bereichen, die implementiert und in die verschiedenen Virtualisierungsumgebungen integriert werden sollten. Für den zentralisierten Desktop-Betrieb bilden serverbasierte Graphics Processing Units (GPUs) die Grundlage. Diese ermöglichen hardwarebeschleunigtes Rendering für virtuelle Maschinen (VMs), etwa für 3D-Anwendungen oder flüssige Videowiedergabe auf flexibel partitionierter Host-Hardware.

Zum Einsatz kommen dabei spezielle Grafikkarten, die sich in mehrere virtuelle Einheiten aufteilen lassen. Aktuell stehen hier vor allem Modelle wie die Data Center Intel Flex 140 und 170 (ATS-M) sowie die neueren Intel ARC B50/60/70 zur Auswahl, die eine gute Treiberunterstützung bieten. Lösungen von NVIDIA sind aufgrund hoher Kosten und proprietärer Treiber derzeit ebenso unattraktiv wie Optionen von AMD, da entsprechende Karten (Radeon Pro) schwer verfügbar sind und die Treiberlage uneinheitlich ist.

Zusätzlich wird ein Zugangs-Gateway zu den VDI-Ressourcen benötigt, ein zentraler Einstiegspunkt für die Nutzenden. Dieses lässt sich über OIDC (einen Standard für Web-Login-Verfahren) mit Keycloak an die bestehende AAI (Authentifizierungs- und Autorisierungsinfrastruktur) anbinden. Für eine flüssige Nutzung müssen die Bildschirminhalte der virtuellen Maschinen effizient erfasst („Framegrabbing“) und möglichst verzögerungsarm übertragen werden, idealerweise mit Hardware-Beschleunigung. Aktuell kommt dafür das ursprünglich von Red Hat entwickelte Remote-Desktop-Protokoll SPICE zum Einsatz, das auf GStreamer-Encoding basiert

OSVDI-EINSATZSZENARIEN

OSVDI erlaubt Forschenden, Studierenden und Verwaltungsmitarbeitenden den ortsunabhängigen Zugriff auf eine vertraute Desktop-Umgebung – auch auf spezialisierter oder optimierter Hardware. Egal ob altes PC-Modell, Thin Client, privates Laptop, Mobiltelefon, Tablet oder Smart TV – die auf den lokalen Client gestreamte Desktop-Umgebung entspricht exakt dem lokalen Pendant in Form des Büro- oder Pool-PCs oder der leistungsfähigen Spezial-Workstation für Arbeits- und Lernumgebungen.

Auch grafikintensive Anwendungen und hochauflösende Darstellungen laufen performant. Gleichzeitig bleibt der Bandbreitenbedarf moderat (ca. 10 Mbit/s für Full HD, unter 100 Mbit/s für höhere Auflösungen). VDI-Lösungen erlauben den direkten Zugriff auf große oder sensible Daten nahe ihrer Quelle. Das vereinfacht sowohl das Datenmanagement als auch die Absicherung von Infrastruktur und Daten.

Beispiel: Das Konsortium NFDI4BIOIMAGE innerhalb der Nationalen Forschungsdateninfrastruktur (NFDI) entwickelt neue Dateiformate, Metadatenstandards, nachnutzbare Analyseverfahren sowie integrierte Speicher- und Verarbeitungsumgebungen. Ergänzend dazu werden Fernzugriffslösungen wie OSVDI erprobt, die eine interaktive, hochauflösende Bearbeitung von Bilddaten in gewohnten Desktop-Umgebungen ermöglichen. Ziel ist es, Angebote von Imaging Facilities zu erweitern und ortsunabhängig zugänglich zu machen.

und auch Funktionen wie Audio in beide Richtungen, Drucken oder USB-Weiterleitung unterstützt. Aufgrund von Einschränkungen, vor allem bei der Verzögerung zwischen Eingabe und Bildanzeige (Round-Trip Time), wird derzeit geprüft, ob sich für den Videostream leichtere und leistungsfähigere Alternativen einsetzen lassen.

Insbesondere bei stark schwankendem Bedarf an nichtpersistenten Ad-hoc-Ressourcen, wie sie in der Lehre in vielfältiger Form benötigt werden, bietet der Cloud-Betrieb Vorteile gegenüber den eher statischen Modellen klassischer Virtualisierungsumgebungen. VDI ist letztlich ein weiterer Anwendungsfall für Ressourcenteilung, da viele Maschinen sehr ähnliche Arbeitslasten ausführen und während der Sitzungen häufig Leerlaufzeiten haben. Dafür ist in OpenStack eine langfristige Ressourcenplanung für großskalige interaktive Use Cases erforderlich.

Die nächsten Schritte

Parallel zur bestehenden Projektförderung von NFDI4BIOIMAGE und bwCloud 3 sollen die aktuellen Entwicklungen im OSVDI-Projekt stärker sichtbar gemacht werden, um sowohl Anwenderinnen und Anwender als auch weitere Mitstreitende zu gewinnen. Gleichzeitig ist es das Ziel, ein nachhaltiges Finanzierungs- und Betriebskonzept zu etablieren, um sich perspektivisch unabhängig von Projektmitteln zu machen.

Für Open-Source-Projekte gibt es verschiedene Ausgestaltungs- und Betriebsmodelle, die die VDI-Arbeitsgruppe gemeinsam mit den Einrichtungen entwickeln möchte. Hierzu arbeitet sie an Beteiligungsmodellen für eine gemeinsame Steuerung, die unter anderem auf die langjährigen Erfahrungen in bwLehrpool zurückgreifen. Eine stärkere Beteiligung

> Für Open-Source-Projekte gibt es verschiedene Ausgestaltungs- und Betriebsmodelle.

von Hochschulen und Forschungseinrichtungen bei der Erstellung und Betreuung von strategischen Open-Source-IT-Bausteinen kommt nicht nur diesen selbst zugute, sondern fördert die digitale Souveränität. Hiervon können sowohl öffentliche Einrichtungen wie Schulen und Verwaltungen als auch Unternehmen profitieren. Denn diese müssen zunehmend große Summen für ihre IT-Bedarfe ausgeben, oft ohne einen Einfluss auf die verwendeten Software-Pakete zu haben. Um Bedarfe und Angebote besser zusammenzubringen, sind geeignete Marktplätze erforderlich – ein Thema, das auf der zweiten DFN-Unkonferenz zu Cloud-Diensten in Augsburg diskutiert wurde.

Für eher statisch konfigurierte Use Cases lässt sich bereits eine Demo in der eigenen Einrichtung umsetzen; die Integration in OpenStack und Proxmox VE sind weitere Meilensteine für dieses und das kommende Jahr.

Nach einer erfolgreichen Präsentation eines größeren Setups mit drei Servern und bis zu 24-GPU-unterstützten Clients auf den Chemnitzer Linux-Tagen Ende März wird auf der DFN-Betriebstagung im Herbst ein bis dahin hoffentlich weiter poliertes erstes Basisprodukt gezeigt werden. Dabei ist die Einbindung in die DFN-AAI bereits vorgesehen. ◆

ÖFFENTLICH VERFÜGBARE DEMO UND CODE

Die Demo wird am Rechenzentrum der Universität Freiburg gehostet und durch NFDI4BIOIMAGE (TA 2.4) sowie das Service-Entwicklungsprojekt bwCloud 3 gefördert.

Die öffentlich zugängliche Demo mit Log-in via DFN-AAI gibt es unter:
https://demo.osvdi.uni-freiburg.de/

Code zum Download, Wege zur Interaktion und Beiträge finden Sie unter:
https://gitlab.uni-freiburg.de/opensourcevdi/

Die Dokumentation gibt es unter:
https://gitlab.uni-freiburg.de/opensourcevdi/

Bei Interesse oder Fragen zur Open Source Virtual Desktop Infrastructure (OSVDI) wenden Sie sich gerne an Dr. Dirk von Suchodoletz unter:
dirk.von.suchodoletz@rz.uni-freiburg.de

International Newsflashes

GÉANT Establishes NREN Humanitarian Support Group

This year, the broader GÉANT community began its Humanitarian Support Group for NRENs. The program coordinates support for European NRENs that are facing war, infrastructure failure, large-scale environmental or other societal upheaval, or other sustained crises. The effort was born out of GÉANT's support of URAN, the Ukrainian NREN, which was been challenged by that country's war with Russia.

The group is focused on supporting NRENs with financial assistance; equipment and infrastructure needed to operate an NREN during times of crisis, such as emergency generators or networking equipment; technical expertise for operations, engineering, and organizational matters; and broad community solidarity aimed at strengthening professional networks. ◆

For more information about the support group, please visit the group's webpage: **https://community.geant.org/humanitarian-support-group**

For more information about the initiative, please visit the GÉANT website: **https://connect.geant.org/2026/03/05/the-geant-community-establishes-the-humanitarian-support-group-for-nrens**

Network eAcademy Offers New AI Training Programme

As the artificial intelligence boom continues, scientists, engineers, and educators have had to suddenly learn a host of new skills that can improve productivity and improve insights in research endeavors. To this end, the Network eAcademy recently started a new course program dedicated to AI training. The eAcademy is a community-driven service that supports academic and research organizations in advancing their staffs capabilities in network technologies and services.

The program has modules dedicated to AI as a technology generally as well as how it can be used for network management. The units focus on major AI-related topics at the moment, including predictive AI, generative AI, classical machine learning, natural language processing, and transparent and explainable AI systems. Accessing the courses is free of charge for those who have access to the Network eAcademy portal. ◆

For more information, please visit the GÉANT website: **https://connect.geant.org/2026/04/07/new-ai-training-programme-in-the-network-eacademy**

GÉANT Selected as EOSC Federation Candidate Node

During an April 2026 meeting of the European Open Science Cloud (EOSC) federation, the organization's Tripartite Governance selected GÉANT as a candidate node in the EOSC, building on GÉANT's contribution to delivering the EOSC EU node. The second round of nodes showcases continued progress in connecting Europe's various national research and education networks (NRENs) in a federated, interoperable ecosystem that efficiently connects network services and researchers across the continent. ◆

For more information, please visit the GÉANT website: **https://connect.geant.org/2026/05/01/geant-selected-as-candidate-node-in-the-eosc-federation**

Collaboration on this Newsflash: Eric Gedenk

You can find more international community news under: **https://connect.geant.org/community-news**

Starke Partner weltweit

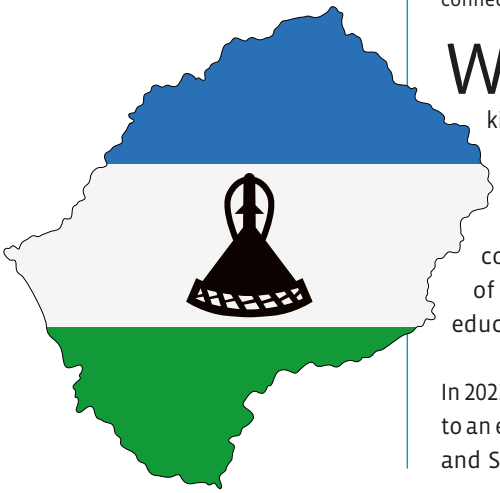
Konnektivität fördern, Zukunft gestalten, Herausforderungen gemeinsam meistern: Nationale Forschungsnetze rund um den Globus betreiben leistungsfähige Infrastrukturen für Wissenschaft, Forschung und Lehre. Ein Blick in die Welt der NREN-Community.

LesREN Launches – Building a Research and Education Network Focused on Community Impact

Lesotho's national research and education network (LesREN) is one of the newest NRENs in the Southern African Development Community (SADC). After joining the Ubuntunet Alliance last year, the organization focuses on expanding affordable, reliable high-speed internet infrastructure to students at all levels.

Text: **Eric Gedenk** (Impact Science Communication)

LesREN helps support research and education, including the National University of Lesotho, with connectivity and digital services | *Photo: K. Kendal /Wikimedia Commons/CC BY 2.0*



With just over 2 million people and a land area of around 30,000 square kilometres, Lesotho is one of the smallest countries in southern Africa. Despite its small size, Lesotho puts a large emphasis on education, with the country investing almost seven percent of its annual gross domestic product on education.

In 2022, as the COVID-19 pandemic was coming to an end, Mr. Letsatsi Lekhooa, CEO of LesREN and Systems Librarian at the National University of Lesotho, participated in a research and education roundtable put on the 16th CHPC National Conference at the Council for Scientific and Industrial Research (CSIR) South Africa. He saw a panel discussing the role of national research and education networks (NRENs) in other countries in the region and saw the need to advance internet and communication technology (ICT) infrastructure at home.

The following year, Lekhooa, government officials, and representatives from the region-

Letsatsi Lekhooa, CEO of LesREN, championed efforts to strengthen digital infrastructure in Lesotho | *Photo: UbuntuNet Alliance*

al Ubuntunet Alliance let by Prof Madara Ogot met in the capital Maseru to develop a roadmap for establishing LesREN. All parties agreed that expanding the access to high-speed internet in the country's research and education facilities was a key step to raising Lesotho's burgeoning research profile and ensure that the brightest young minds and talented researchers would have reliable, secure internet connectivity to collaborate with researchers around the world. LesREN was officially registered and brought online in the country in April 2025, making it one of the newest NRENs in the world.

Forging regional bonds for stronger research and economic outcomes

Officials understood that LesREN's primary goal was bringing different stakeholders together in the country and beyond to improve research and education outcomes in Lesotho. To that end, Lekhooa and other LesREN collaborators have focused on bringing together educational institutions with private-sector organizations to simplify access to the best-possible network solutions for educators and students from primary education to graduate programs at universities.

The organization works closely with network and information technology (IT) experts and librarians at Lesotho's academic organizations to ensure they are aware of how they can connect to LesREN's services and contribute to bolstering the organization. They are particularly focused on ensuring that students at universities and other institutions for higher education not only see improved access to high-speed networks, but also can access more science, technology, engineering, and math (STEM) education at that level, ultimately helping to bolster the number of students that pursue these fields at the university or post-graduate levels.

Further, LesREN was inspired by the Ubuntunet Alliance, and, accordingly, became part of the alliance as soon as the NREN was formally established last year. The alliance brings together students, researchers, and educators from 22 countries in southern and eastern Africa. It not only helps its 16 member NRENs with building out infrastructure and network capacity throughout their respective countries, but also offers cloud and storage services, cybersecurity support, trust and identity services, and serves as a central location for NREN staff members to learn about training and funding opportunities in the region and beyond.

Building capacities, expanding opportunities

Still in its infancy, LesREN spent its first year of existence primarily forging connections to academic institutions across the country and working closely with Lesotho's three primary internet providers to close the digital gap between home or institution-based internet connectivity — roughly 53 percent of households have home internet in Lesotho, compared with 97 percent of people having access to mobile networks.

Further, LesREN is intending to work closely with universities to establish institutional repositories to both save and organize scientists' and engineers' research, and to ensure their research can be more easily found and shared with the international research community. Lekhooa indicated that most of the internet capacity is centered in the capital, and LesREN is focused on building out internet speed and reliability to organizations in more rural parts of the country.

LesREN is also focused on bridging the knowledge gap in cybersecurity. The growth of mobile networks and mobile device usage skyrocketed during the pandemic, and Lekhooa indicated that LesREN was prioritizing campaigns about cybersecurity across the country so those with relatively little experience online would be better prepared to avoid scams, privacy invasions, and the other risks that can proliferate online.

While the organization is small — there are 10 people that are part of LesREN's governing body — they are highly motivated to identify collaborators at Lesotho's various education organizations that can both bring LesREN services to those organizations and \support LesREN's activities on a national scale. There are 17 institutions in the country currently working with LesREN, and Lekhooa indicated that as the organization continues to grow, it continues to seek both manpower and funding sources to increase its training and education opportunities, further grow its core staff, and continue to expand improved internet access across Lesotho. ◆

For more information about LesREN, please visit:
www.lesren.org.ls

For more information about the Ubuntunet Alliance, please visit:
https://ubuntunet.net/

TALON: Europe's First Cross-Border Crisis Exercise for NRENs

In March 2026, staff from European national research and education networks (NRENs) came together for TALON 2026, a GÉANT initiative and the first large-scale, cross-border crisis simulation of its kind in Europe. Building on the legacy of the CLAW crisis management events, the exercise offered participating organisations a unique opportunity to test their crisis preparedness and contingency plans in a realistic, fast-moving scenario.

Text: **Rosanna Norman** (GÉANT)

Coordinating responses, assessing situations, making decisions under pressure: TALON trained NRENs to respond collectively to cyber incidents. The photo shows a similar training scenario during a CLAW workshop at Poznan Supercomputing and Networking Center (PSNC) in Poznan | *Photo: Maciej Rutkowski (PSNC)*

On the morning of 19 March, ten organisations – ACOnet (Austria), Asiera (Ireland), BelWü (Germany), CYNET (Cyprus), DeiC (Denmark), GÉANT, Jisc (UK), RESTENA (Luxembourg), SURF (the Netherlands) and SWITCH (Switzerland) – knew a crisis was coming, but not what form it would take. With a sense of anticipation in the air, teams began their day as usual, waiting for the first signs of disruption. When the scenario unfolded, that quiet tension quickly gave way to a fast-moving and demanding situation.

Within this broader exercise, TALON specifically set out to test how effectively NRENs communicate in the early stages of a crisis. From a communications perspective, the focus was not only on speed, but also on clarity, consistency and empathy, ensuring organisations can reassure stakeholders that "we know, we do, we care."

The exercise assessed whether NRENs could deliver timely and coordinated information, maintain trust, and operate clear communication structures under pressure. It also explored how well teams manage social media noise, misinformation, and high volumes of incoming requests, while encouraging alignment of key messages across organisations.

As Davina Luyten, communications lead for the exercise, noted: "TALON showed that NRENs are able to respond quickly and responsibly under pressure, but it also highlighted how critical coordination and internal information flow are to maintaining consistent, trusted communication during a crisis."

A realistic and demanding simulation

TALON created a highly immersive media environment. A central communications team simulated social media activity, news coverage and public reactions, while exercise leaders played the roles of internal stakeholders and policymakers.

Reflecting on the exercise, TALON exercise leader Charlie van Genuchten commented: "A crisis can hit at any time, and when it does, you feel the impact immediately. There's no opportunity to rewind or rethink your setup, you must rely on the preparation, structures and decisions already in place."

A dedicated team of journalists added further pressure, engaging NRENs with increasingly complex questions as the scenario escalated from local to international media. This allowed participants to demonstrate responsiveness, clarity and their ability to handle sensitive enquiries.

High intensity, valuable learning

Once the scenario began, events escalated rapidly, requiring teams to manage multiple tasks simultaneously. Clear roles and responsibilities proved essential, and the overall experience was intense, engaging and highly instructive.

Strong performance with clear lessons

Overall, NRENs performed well. Most organisations were responsive and accessible, and many issued initial social media statements within 30 minutes. Spokespersons generally engaged openly, even when faced with difficult questions.

However, the exercise also highlighted areas for improvement. In some cases, spokespersons lacked sufficient information, pointing to gaps in internal communication between technical and communications teams. Differences in organisational maturity were also evident.

Key areas for improvement

Message alignment across NRENs remains a key challenge. Limited coordination sometimes led to inconsistent messaging, underlining the need for stronger collaboration mechanisms.

Further priorities include ensuring dedicated, well-trained spokespersons and preparing pre-approved materials such as Q&As and holding statements to support faster, more consistent responses.

A strong foundation for the future

TALON demonstrated both the strengths of the NREN community and the importance of continued improvement. The exercise provided valuable insights that will help strengthen coordination and ensure more effective communication in future crises. ◆

For more information, please visit the GÉANT website: **https://security.geant.org/talon-2026/**

THE FIELD

National research & education networks (NRENs) all over the world working together. With our powerful communication infrastructures we enable access to knowledge & resources, connect people, foster collaboration. In this series our participating institutions share their inspiring stories and achievements.

Exchanging Palm Oil Plantations for Designer Enzymes

Researchers at the Goethe University Frankfurt and the Dalian Institute of Chemical Physics at the Chinese Academy of Sciences are creating synthetic fatty acids as part of the "green chemistry" revolution. In time, these compounds could replace land-intensive palm oil and coconut oil production.

Text: **Eric Gedenk** (Impact Science Communication)

Members of the Grininger lab have been developing ways to create fatty acid synthase in laboratory conditions, then share their work with chemical engineers in China to scale the production of these enzymes | *Photo: Goethe-Universität Frankfurt am Main*

Fatty acids give your Nutella its luscious texture. They help make degreasers and other cleaners, get used in cosmetics, and are being investigated for their use in certain pharmaceuticals. Because they are so widely used across many industries, farms in the Global South have increased the production of palm oil and coconut oil to serve some of the most common uses of fatty acids. While these forms of fatty acids are economically cheap to produce, they have a significant environmental cost as more forests and jungles are destroyed to make more room for plantations.

Aerial view of the palm grove in Borneo, Indonesia | *Photo: Naya Nurindra/iStock*

Recently, researchers at the Goethe University Frankfurt have been collaborating with scientists at China's Dalian Institute of Chemical Physics in how to design synthetic fatty acids with variable molecular chain lengths that they can produce with a lower environmental footprint. Specifically, the team focuses on an enzyme called fatty acid synthase (FAS), which builds various fatty acid chains in an organism.

"Previous research showed us that we can regulate FAS to influence the length of fatty acid chains, and with that in mind, we realized we should be able to tune this phenomenon to be able to produce different chain lengths at larger scales," said Prof. Martin Grininger, researcher at Goethe University Frankfurt and lead on the project. "While this work did not begin focused on food chemistry or cosmetics, the research has developed and evolved in a way that supports advancements in these areas."

As a research group at Goethe University Frankfurt, Grininger and his colleagues rely on the security, speed, and reliability of the German Research Network's (DFN's) network infrastructure to not only expedite their research at home, but also to work with collaborators on the other side of the globe in pursuit of further developing these sustainable production methods.

Enzymes support engineered fatty acids

Almost all fatty acids contain a single chain of carbon atoms. Their properties are largely based on these chain lengths—shorter chains are more water soluble, for instance. "If you want to ensure that your chocolate cream has the right consistency to spread on bread, you want to use something like palm oil with its longer fatty acids, but if you are designing a soap that needs to lather correctly in the shower, you want to make the soap out of medium-chain fatty acids," Grininger said.

While FAS usually produces fatty acids that have 16 carbon atoms as part of their chains, many commercial and industrial applications need fatty acids with carbon chains between 6 and 14 atoms long, driving the need for sources like palm oil. In its previous research, the Grininger team identified two enzyme subunits of FAS that directly regulate fatty acid chain lengths—ketosynthase, which continues to lengthen a fatty acid's carbon chain, and thioesterase, which ends a fatty acid carbon atom chain.

The team began to investigate how these two subunits could be manipulated to design fatty acids with specific chain lengths. Damian Ludig, doctoral student and researcher on the team, spearheaded the research and was able to produce short-chain and medium-chain fatty acids in laboratory conditions. While the team showed that it could use these subunits to adjust lengths, it needed to develop a cost-effective, scalable method to produce larger volumes of these fatty acids.

International collaboration accelerates innovation

While Grininger noted that the team could create boutique fatty acid chains in these smaller, more specific contexts, he knew they had to look for collaborators that could scale this chemical engineering work in such a way that it could support the various industries' demands for fatty acids. He turned to a long-time colleague, Yongjin Zhou, professor at the Dalian Institute of Chemical Physics in China.

The Goethe University Frankfurt researchers shared DNA-level information with scientists at the Dalian Insitute of Chemical Physics. In time, this international collaboration's work could replace land-intensive palm oil plantations | *Photo: Goethe-Universität Frankfurt am Main*

"We have long collaborated with my friend Yongjin Zhou, both in his roles in Europe and in China," Grininger said. "In our collaborations, we were glad to see that we could engineer and change chain lengths in fatty acids in a laboratory setting, but we know it is too energy intensive to have to purify the enzyme at a practical scale," Grininger said. "We needed to find a way to make this change happen inside the cell, so we took our DNA-level information and shared it with Yongjin and his colleagues in Dalian."

Zhou's team took the protein-level information that was provided by the German team and began to seek out a microbial host strain that could produce variable fatty acid chains cheaply and sustainably. The team identified Ogataea polymorpha, a species of yeast that can grow on cheap carbon sources like methanol and produce fatty acids.

Having a proof of concept on using this yeast, the team is now exploring how to improve the efficiency of the conversion—currently, the team can only produce roughly a gram of a specific short- and medium-chain fatty acids per liter of yeast culture mix, while the standard-length fatty acids produced the same way create 30 to 40 grams per liter. The reduced yield is attributed to the toxicity of these shortened fatty acids, which are non-native to the yeast and harm cellular function.

However, despite their research challenges, Grininger and Zhou are optimistic that their large-scale collaboration will ultimately be able to produce fatty acids at scale to reduce the need for palm and coconut oil in the years to come. "I believe that in five years, we will have solved many of the current challenges and made significant progress toward practical applications," Grininger said.

Grininger emphasized that without having access to DFN networks, the team would not be able to keep up the continual, iterative process involved in this collaboration. "One of the best arguments I can make for the initiatives and infrastructure provided by DFN is just how easy it is to forget about it," he said. "Everything works so smoothly in our day-to-day work that you don't have to think about how to navigate network issues at your home institution. 25 years ago, I was dealing with a lot of data, and transferring and sharing data was always an issue. While we are not sharing large amounts of data in this work, we are regularly collaborating with our colleagues in China, and we do not have to consider how to keep up that collaboration." ◆

For more details on the research, read the team's recently published scientific papers in *Nature Chemical Biology* **https://www.nature.com/articles/s41589-025-02105-w** and *Angewandte Chemie* **https://onlinelibrary.wiley.com/doi/10.1002/anie.202511726**.

.in THE FIELD

Find more exciting research stories from all over the world on In The Field blog:
www.inthefieldstories.net

Alles begann mit einer Frage – die Forschungsstelle Recht im DFN

Nach rund 28 Jahren an der Universität Münster ist die am Institut für Informations-, Telekommunikations- und Medienrecht (ITM) aufgebaute Forschungsstelle Recht im DFN Anfang 2026 vollständig an die Humboldt-Universität zu Berlin gewechselt. Zum Abschied blickt der langjährige Projektleiter Prof. Dr. Thomas Hoeren zurück auf die Anfänge und Besonderheiten dieser einzigartigen Einrichtung im Wissenschaftsnetz.

Wenn Sie die Forschungsstelle Recht mit drei Wörtern beschreiben müssten, welche wären das?

Spontan kommt mir in den Sinn: chaotisch, bunt und spannend. Chaotisch im besten Sinne des Wortes. Es kamen vor allem in der Gründungsphase so viele juristische Fragestellungen aus den unterschiedlichsten Themenfeldern – ob Telekommunikationsrecht, Rundfunkrecht, Urheberrecht oder Datenschutzrecht, Medienrecht oder Jugendschutz. Jeder Tag war völlig anders. Wir haben teils Lösungen ausarbeiten müssen, für die es noch gar keine rechtlichen Vorlagen gab.

Außerdem fällt mir noch der Begriff jung ein, weil die Forschungsstelle Recht vor allem von den wissenschaftlichen Mitarbeitenden getragen wird, die mit Elan und Herzblut pragmatische gut verständliche Lösungen formulieren, die auch Nichtjuristinnen und -juristen nachvollziehen können.

Wie entstand die Forschungsstelle Recht im DFN?

Eigentlich begann alles mit den Worten: „Sie haben doch Ahnung vom IT-Recht – ich hätte

Von Herzen: Im Namen des DFN-Vereins verabschiedet Annette Rülke, die die Forschungsstelle Recht im DFN mitkoordiniert, Prof. Dr. Thomas Hoeren nach 23 Jahren der vertrauensvollen und erfolgreichen Zusammenarbeit | *Foto: Maimona Id/DFN*

da mal eine Frage.“ Bei einer Sitzung des Rechenzentrums der Heinrich-Heine-Universität Düsseldorf sprach mich der damalige Geschäftsführer des DFN-Vereins, Dr. Klaus-Eckart Maas, an. Offenbar war meine Antwort überzeugend, denn es blieb nicht bei dieser einen Frage. Im Gegenteil: Es wurden immer mehr – so viele, dass ich sie allein nicht mehr bewältigen konnte. Kurzerhand entstand daraus die Idee, mit zwei Mitarbeitenden eine kleine Forschungsstelle Recht im DFN-Verein aufzubauen. 1998 war damit ihre Geburtsstunde. Zunächst in Düsseldorf angesiedelt, später an der Universität Münster. Damit sollten die Mitgliedseinrichtungen im DFN-Verein beim damals noch recht jungen Thema Rechtssicherheit im Umgang mit elektronischen Informations- und Kommunikationssystemen bestmöglich unterstützt werden.

Gab es Themen, mit denen Sie zu Beginn hauptsächlich zu tun hatten?

Es gab zwei große Themenbereiche, die die Mitarbeitenden der Forschungsstelle besonders beschäftigt haben: Das eine ist das Thema Datenschutzrecht und das andere das Immaterialgüterrecht, hier insbesondere das Urheberrecht. Zu Letzterem gab es vor allem in den Anfängen grundlegende Fragen und auch so manches Missverständnis.

In diesem Zusammenhang wurde häufig das Zitat „Information wants to be free“ bemüht, das John Perry Barlow bekannt gemacht hat – als Argument für eine völlig freie Nutzung von Inhalten. Natürlich ist Informationsfreiheit ein Grundsatz, der gerade in der Wissenschaft, im Hochschul- und im Forschungsbereich eine große Berechtigung hat. Tatsächlich lautet das Zitat aber vollständig: „Information wants to be free. Information also wants to be expensive.“ Barlow – der sich in der frühen Tech- und Hacker-Szene bewegte und Songwriter der Punkband Grateful Dead war – beschreibt damit ein Spannungsverhältnis, das auch für das Urheberrecht zentral ist: Informationen sollen zugänglich sein, haben aber zugleich einen wirtschaftlichen Wert.

Zwischen Technik und Recht: Im Gespräch erinnern sich Annette Rülke und Prof. Dr. Thomas Hoeren an die rasanten Entwicklungen im Wissenschaftsnetz, die sie für die DFN-Mitgliedseinrichtungen juristisch eingeordnet und praxisnah vermittelt haben | *Foto: Maimona Id/DFN*

Und jetzt bekommt das Urheberrecht in Hinblick auf Künstliche Intelligenz wieder neue Brisanz. Dieses Thema ist in einer Gesellschaft, in der Informationen ein äußerst kostbares Gut sind, weiter virulent.

Wie stehen Sie zu Künstlicher Intelligenz?

Mich erinnert die ganze Diskussion an die Zeit, als in Schulen noch erhitzt darüber gestritten wurde, ob Kinder durch die Nutzung von Taschenrechnern das Rechnen verlernen. Künstliche Intelligenz entwickelt sich seit Jahrzehnten, gewinnt aber aktuell durch generative Verfahren stark an Bedeutung. Sie wird bereits in vielen Bereichen selbstverständlich eingesetzt, auch in der Wissenschaft. Damit rücken rechtliche Fragen stärker in den Fokus – etwa zur Nutzung von Trainingsdaten, zum Urheberrecht an KI-Ergebnissen oder zur Verantwortlichkeit. KI wird bleiben, deshalb brauchen wir klare Rahmenbedingungen, die Innovation ermöglichen und zugleich Rechte schützen.

Sie erwähnten eben Datenschutzrecht als zweites großes Thema. Wie hat sich das entwickelt?

Obwohl es zu Beginn noch eine vergleichsweise geringe Rolle spielte, gewann das Datenschutzrecht jedoch mit zunehmender Digitalisierung stetig an Bedeutung und rückte insbesondere mit der Datenschutz-Grundverordnung ab 2016 in den Fokus. Im Vergleich zur vorherigen Rechtslage in Deutschland brachte die Verordnung in einzelnen Bereichen mehr Flexibilität, insgesamt aber vor allem deutlich strengere und einheitlichere Vorgaben. Entsprechend hatte sich die Forschungsstelle Recht mit zahlreichen Einzelfragen zu befassen. Bis heute bestehen in manchen Punkten Unsicherheiten – auch, weil Aufsichtsbehörden teils unterschiedliche Auffassungen vertreten.

Außerdem bewegen wir uns bei vielen Themen der Forschungsstelle Recht im europäischen Rechtsrahmen. Die Fülle an

Prof. Dr. Thomas Hoeren | 1980 Studium der Katholischen Theologie und Rechtswissenschaften in Münster, Tübingen und London | 1995 bis 1997 Universitätsprofessor an der Juristischen Fakultät der Heinrich-Heine-Universität Düsseldorf (Professur für Bürgerliches Recht und internationales Wirtschaftsrecht) | 1996 bis 2011 Richter am OLG Düsseldorf (20. Zivilsenat, zuständig u. a. für Urheber- und Wettbewerbsrecht) | 1998 bis 2026 Leiter des DFN-Projekts „Rechtsfragen im Deutschen Forschungsnetz“ | seit April 1997 Universitätsprofessor an der Juristischen Fakultät der Westfälischen Wilhelms-Universität Münster, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) | 2012 bis 2014 Dekan der Rechtswissenschaftlichen Fakultät der Universität Münster

Foto: Maimona Id/DFN

Regelungen ist nicht leicht zu durchblicken. Immerhin soll es im Datenrecht durch den sogenannten „Digitalen Omnibus“ noch einmal zu einer Fokussierung kommen. Was uns immer mehr beschäftigt, sind Fragen, die sich mit Cybersicherheit beschäftigen. Vor diesem Hintergrund und auch vor dem der politischen Situation in den USA ist auch die digitale Souveränität ein Schwerpunkt. Das sind alles Themen, die die Forschungsstelle Recht in Vorträgen, Infobriefen und dem Podcast „Weggeforscht“ aufarbeitet.

Lassen Sie uns über das Thema Zusammenarbeit sprechen: Den Mitarbeitenden der Forschungsstelle Recht standen ja hauptsächlich Mitarbeitende aus den Rechenzentren gegenüber. Wie funktioniert das?
Das ist tatsächlich spannend. Es reicht nicht, Menschen mit so gegensätzlichem Background einfach in einen Raum zu setzen – gute Zusammenarbeit entsteht erst durch gegenseitiges Zuhören. Im DFN-Verein waren dafür die Voraussetzungen schon immer sehr gut. Dabei zeigte sich, dass die scheinbar gegensätzlichen Blickwinkel oft zu überraschend ähnlichen Ergebnissen geführt haben. Und selbst wenn das nicht der Fall war, führte es zu äußerst produktiven Diskussionen. Genau daraus ist eine sehr gute und nachhaltige Zusammenarbeit entstanden.

Einen wichtigen Beitrag leistet auch der DFN-Ausschuss für Recht und Sicherheit, in dem unterschiedliche Perspektiven vertreten sind. Diese geben neue Impulse und tragen dazu bei, den Blick auf zentrale Fragen zu schärfen.

Sie haben über 30 Jahre Pionierarbeit in der Forschungsstelle Recht geleistet. Mit welchem Gefühl beenden Sie die Arbeit?
Ein wenig Wehmut ist schon dabei. Gleichzeitig gibt es ein großes Projekt, das mich schon länger begleitet. Es wird immer wichtiger, internationaler zu denken. Deshalb habe ich unter dem Label LDE – Law of the Digital Economy – begonnen, Vorlesungen zum europäischen Recht auf Englisch anzubieten – mit der Perspektive, daraus einen internationalen Studiengang zu entwickeln. Ziel ist es, Studierende aus verschiedenen Ländern zusammenzubringen und den Austausch zu fördern. Daran möchte ich auch nach meiner Pensionierung weiterarbeiten.

Was wünschen Sie der Forschungsstelle Recht für die Zukunft?
Ich wünsche der Forschungsstelle Recht, dass sie auch künftig engagierte, kluge wissenschaftliche Mitarbeitende gewinnt, die die Themen mit Elan und Neugier voranbringen. Ebenso wichtig ist, dass sie weiterhin mit Mut und Weitblick neue Entwicklungen frühzeitig aufgreift und den Diskurs weiterhin aktiv mitgestaltet. Ich weiß das Projekt bei meiner Nachfolgerin Prof. Dr. Katharina de la Durantaye in außerordentlich guten Händen und freue mich schon darauf, wie sich die Forschungsstelle Recht weiterentwickeln wird.

Das Gespräch führten Annette Rülke und Maimona Id (DFN-Verein). ◆

Anonym oder pseudonym? Alles ist möglich.

Der Europäische Gerichtshof hat zum Verständnis des Begriffs „personenbezogene Daten“ entschieden

Was sind „personenbezogene Daten“ nach europäischem Datenschutzrecht? Diese Frage beantwortete der Europäische Gerichtshof (EuGH) im September 2025.[1] Somit herrscht in einem langjährigen Streit endlich Rechtsklarheit.[2] Viele anschließende Fragen bleiben jedoch offen. Auch Hochschulen und Forschungseinrichtungen sollten sich mit dem Urteil befassen. Das Urteil kann viele Auswirkungen haben. So könnte sich dadurch eine Chance für Forschungsprojekte und das Training von Künstlicher Intelligenz (KI) bieten.

Text: **Anna Maria Yang-Jacobi** (Forschungsstelle Recht im DFN)

I. Generell: personenbezogene Daten vs. anonyme Daten

Nach Art. 1 Abs. 1 der Datenschutz-Grundverordnung (DSGVO)[3] schützen die Vorschriften der DSGVO natürliche Personen bei der Verarbeitung personenbezogener Daten und den freien Verkehr solcher Daten. Die Regelungen der DSGVO sind also grundsätzlich nur anwendbar, wenn es sich um personenbezogene Daten natürlicher Personen handelt. Daten, die keinen Personenbezug aufweisen, sind entsprechend nicht vom Anwendungsbereich der DSGVO umfasst. In vielen Fällen ist es leicht zu beantworten, ob Daten

1 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P.
2 Zur Entscheidung der Vorinstanz und der Unterscheidung des relativen und absoluten Verständnisses bereits ausführlich Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.
3 Verordnung (EU) 2016/679.

einen Personenbezug haben. Sogenannte direkte Identifikationsmerkmale wie der Name, die Anschrift, das Geburtsdatum oder auch äußerliche Merkmale wie Geschlecht, Augenfarbe, Größe und Gewicht sind eindeutig personenbezogene Daten.[4] Daten können allerdings auch pseudonymisiert und sogar anonymisiert werden.

1. Pseudonymisierung

Die Pseudonymisierung ist eine technische Maßnahme zum Schutz personenbezogener Daten. Die betroffene Person selbst, ein Dritter oder auch ein Verantwortlicher können personenbezogene Daten so umwandeln, dass die betroffene Person nur über weitere Informationen identifizierbar ist. Es gibt verschiedene technische Möglichkeiten, um direkte Identifikationsmerkmale zum Beispiel durch einen Code, Ziffern, Zahlenabfolgen oder andere Pseudonyme zu ersetzen. In einem weiteren Schritt müssen die Daten organisatorisch durch angemessene Schutzmaßnahmen gesichert werden. Sofern eine Daten verarbeitende Stelle allerdings über die zusätzlichen Informationen verfügt, kann sie den Personenbezug problemlos wiederherstellen und eine Re-Identifizierung durchführen. In solchen Fällen ändert sich der Personenbezug der Daten folglich nicht. Die Daten bleiben trotz Pseudonymisierung weiterhin personenbezogene Daten, was auch Erwägungsgrund (ErwGr) 26 Satz 2 DSGVO aufzeigt. Art. 4 Nr. 5 DSGVO enthält eine Legaldefinition der „Pseudonymisierung".

2. Anonymisierung

Im Gegensatz dazu enthält die DSGVO weder eine Definition der „Anonymisierung" noch Ausführungen zu speziellen Anonymisierungsverfahren. Anonyme Informationen bzw. Daten werden nur in ErwGr 26 Satz 5 und 6 DSGVO erwähnt. Allgemein beschreibt die Anonymisierung im Rahmen des Datenschutzrechts einen Vorgang, der den Personenbezug so von den Daten trennt, dass nach dem datenschutzrechtlichen Verständnis für den Verantwortlichen kein verhältnismäßiges Mittel zur Verfügung steht,[5] diese Daten eindeutig einer individuell bestimmbaren Person zuzuordnen. Anonyme Daten weisen entsprechend keinen Personenbezug auf. Die DSGVO findet nach ErwGr 26 Satz 6 DSGVO bei anonymen Daten keine Anwendung. Aus technischer Sicht gibt es verschiedene Verfahren der Anonymisierung, die auch kombiniert werden können.[6] Gerade mit Blick auf technische Weiterentwicklungen ändern sich auch die Anforderungen, die an eine Anonymisierung zu stellen sind.[7] Dabei ist eine vollständige Anonymisierung von personenbezogenen Daten aus technischer Sicht anzuzweifeln.[8]

II. SRB-Urteil des EuGH

Hintergrund des Rechtsstreits vor dem EuGH waren Datenverarbeitungen bei der Abwicklung einer spanischen Bank. Finanzbehörden wickeln ein Finanzinstitut ab, wenn es ausfällt oder ein Ausfall wahrscheinlich ist und die Stabilität des Finanzsektors gewährleistet werden soll. Ein Ausfall liegt beispielsweise vor, wenn eine Bank ihre Schulden nicht mehr begleichen kann oder die Bank die gesetzlichen Zulassungsanforderungen nicht mehr erfüllt. Bei großen europäischen Finanzinstituten ist eine europäische Behörde für die ordnungsgemäße Abwicklung zuständig: der sogenannte Einheitliche Abwicklungsausschuss (engl.: Single Resolution Board, kurz: SRB). 2018 erhob der SRB in einem ersten Verfahrensschritt persönliche Daten von Anteilshabenden und Kreditgebenden (nachfolgend: betroffene Personen/Betroffenen) der ausfallenden spanischen Bank. Der SRB veröffentlichte auf seiner Webseite eine Datenschutzerklärung, um über die Datenverarbeitung zu informieren. In einem zweiten Schritt sollten die Betroffenen Stellungnahmen abgeben. Der SRB verarbeitete die persönlichen Daten und die Stellungnahmen getrennt voneinander. Um eine spätere interne Zuordnung zu ermöglichen, erhielten die Stellungnahmen eine 33-stellige, zufällig generierte Identifikationsnummer. Diese Stellungnahmen inklusive Identifikationsnummer übermittelte der SRB zur weiteren Bewertung an die Wirtschaftsprüfungsgesellschaft Deloitte. Über diese mögliche Übermittlung an Deloitte informierte der SRB die Betroffenen in seiner Datenschutzerklärung nicht. Der Datenempfänger, Deloitte, hatte zu keinem Zeitpunkt Zugang zu den persönlichen Daten des ersten Schritts.[9] 2019 erreichten den Europäischen Datenschutzbeauftragten (EDSB) Beschwerden von Betroffenen. Der EDSB entschied daraufhin, dass es sich bei den vom SRB übermittelten Daten um personenbezogene

4 Vgl. die Aufzählung von Schild, in: BeckOK Datenschutzrecht, 53. Edition, Stand: 1.8.2025, DSGVO Art. 4 Rn. 3 sowie Rn. 16.
5 Vgl. EuGH, Urt. v. 19.10.2016, Rs. C-582/14 – Breyer, Rn. 41–46.
6 Zu den genauen technischen Möglichkeiten siehe IT-Planungsrat, Becker, Handreichung Anonymisierung, 28.4.2024, S. 27–40, https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/schwerpunktthemen/2025_04_22_Handreichung_Anonymisierung_final.pdf (alle Links dieses Beitrags wurden zuletzt am 15.12.2025 abgerufen).
7 Ernst, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, DSGVO Art. 4 Rn. 50.
8 So zum Beispiel in diesem Bericht über eine Studie aus dem Jahr 2019: https://netzpolitik.org/2019/weitere-studie-belegt-luege-anonymer-daten/.
9 Zum Sachverhalt siehe EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 9–28.

Daten handelte und der SRB gegen das europäische Datenschutzrecht verstoßen habe. Die Betroffenen hätten darüber informiert werden müssen, dass ihre personenbezogenen Daten an Dritte übermittelt werden. Nach einem erfolglosen Überprüfungsverfahren klagte der SRB vor dem Europäischen Gericht (EuG).[10] Nachdem das EuG zugunsten des SRB urteilte, wandte sich der EDSB in der nächsten Instanz an den EuGH.

Für Stellen der EU gilt bei der Verarbeitung personenbezogener Daten gemäß Art. 2 Abs. 3 DSGVO nicht die DSGVO, sondern besondere Vorschriften. Diese sind seit 2018 in einer separaten Datenschutzverordnung (DSVO)[11] festgelegt. Für den SRB als EU-Behörde gilt entsprechend die DSVO, sodass das Urteil die datenschutzrechtlichen Fragen anhand dieser DSVO behandelt. Der Begriff der „personenbezogenen Daten" ist jedoch im europäischen Datenschutzrecht identisch auszulegen,[12] sodass im Folgenden die Vorschriften der für Hochschulen und Forschungseinrichtungen relevanten DSGVO verwendet werden.

1. Personenbezogene Daten – was bedeutet Identifizierbarkeit?

Im Urteil werden zentrale Fragen des europäischen Datenschutzrechts behandelt. Im Mittelpunkt steht der Begriff der „personenbezogenen Daten". Nach Art. 4 Nr. 1 DSGVO sind dies „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Der EuGH entschied zu mehreren Bestandteilen dieser Definition. Zunächst ging es um die Frage, ob die Stellungnahmen als „Informationen" i. S. d. Art. 4 Nr. 1 DSGVO zu klassifizieren seien. Der EuGH bestätigte eine weite Auslegung von „Informationen" und verwies auf seine frühere Rechtsprechung. Stellungnahmen, die Informationen „über" eine Person und persönliche Meinungen oder Sichtweisen enthalten, sind personenbezogene Daten i. S. d. Art. 4 Nr. 1 DSGVO.[13]

Folgenreicher sind jedoch die grundlegenden Aussagen des EuGH zur „Identifizierbarkeit" einer natürlichen Person. Insbesondere lehnte der Gerichtshof ein absolutes Verständnis[14] des Personenbezugs deutlich ab. Für die Identifizierbarkeit ist es nicht ausreichend, wenn die Daten von „irgendeiner Stelle" zugeordnet werden können. Vielmehr bedarf es immer einer Einzelfallprüfung, ob die betroffene Person identifiziert oder identifizierbar ist oder die Daten anonym sind.[15] So stellte der EuGH fest, dass pseudonymisierte Daten „[…] nicht in jedem Fall und für jede Person als personenbezogene Daten betrachtet werden [müssen]. Denn die Pseudonymisierung kann – je nach Umständen des Einzelfalls – andere Personen als den Verantwortlichen tatsächlich an einer Identifizierung der betroffenen Person hindern, [sodass] letztere für sie nicht oder nicht mehr identifizierbar ist."[16] Der Begriff der „personenbezogenen Daten" ist zwar weit zu verstehen, aber gerade nicht unbegrenzt.[17]

Der EuGH begründet diese Entscheidung wie folgt: Erstens ist die Pseudonymisierung kein Element der Definition von „personenbezogene[n] Daten" in Art. 4 Nr. 1 DSGVO, sondern nur eine technische und organisatorische Umsetzung von Maßnahmen, die das Risiko einer Identifizierung vermindern sollen.[18] Wenn geeignete Maßnahmen getroffen werden, um eine Identifizierung zu verhindern, kann dies auch Auswirkungen auf den Personenbezug der Daten haben.[19] Zweitens zeigt eine Auslegung des ErwGr 26 Satz 3 und Satz 4, dass „alle Mittel" und „alle objektiven Faktoren", „die nach allgemeinem Ermessen wahrscheinlich genutzt werden", bei der Beurteilung der Identifizierbarkeit berücksichtigt werden sollen.[20] Somit begründet das bloße Vorliegen von zusätzlichen Informationen noch nicht, dass personenbezogene Daten vorliegen, stattdessen bedarf es einer genaueren Prüfung.[21] Drittens bestätigte der EuGH seine Rechtsprechung, wonach sich der Personenbezug von Daten ändern kann.[22] So können an sich nicht personenbezogene Daten (zum Beispiel IP-Adressen) doch

10 Dazu ausführlich Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.
11 Verordnung (EU) 2018/1725.
12 So auch der EuGH im Urteil, EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 52.
13 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 54, 60. Das EuG hatte noch eine eingehende Prüfung von Inhalt, Zweck und Auswirkungen der Stellungnahmen vorgesehen: EuG, Urt. v. 26.4.2023, Rs. T-557/20, Rn. 73 f.
14 Zu diesem relativen bzw. absoluten Verständnis siehe auch bereits Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.
15 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 69, 86.
16 Ibid., Rn. 86.
17 Ibid., Rn. 88.
18 Ibid., Rn. 72.
19 Ibid., Rn. 75.
20 Ibid., Rn. 79 f.
21 Ibid., Rn. 82.
22 Ibid., Rn. 83 f. mit Verweis auf die Rs. Breyer, Urt. v. 19.10.2016, Rs. C-582/14 und Rs. Gesamtverband Autoteile-Handel, Urt. v. 9.11.2023, Rs. C-319/22. Zu diesen Entscheidungen auch bereits Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 1/2024.

personenbezogen sein, wenn die rechtliche Möglichkeit besteht, die zusätzlichen Informationen zur Re-Identifizierung zu erhalten,[23] oder auch, sofern die Daten anderen Personen überlassen werden, die über Mittel zur Re-Identifizierung verfügen.[24] Die Re-Identifizierungsmöglichkeiten sind somit auf eine konkrete Stelle bezogen. Sobald nicht ausgeschlossen werden kann, dass ein Datenempfänger die Daten doch zuordnen kann, liegen sowohl bei der Übermittlung als auch bezüglich einer späteren Verarbeitung personenbezogene Daten vor, und die DSGVO ist weiterhin anwendbar (sogenannter indirekter Personenbezug).[25]

Im vorliegenden Fall konnte der SRB die Stellungnahmen und die zusätzlichen Informationen den jeweiligen Betroffenen jederzeit zuordnen. Die Daten wurden zwar pseudonymisiert, waren aber für den SRB weiterhin personenbezogene Daten.[26] Für den Datenempfänger, Deloitte, könnten die pseudonymisierten Stellungnahmen anonym sein, sofern Deloitte die Maßnahmen zur Pseudonymisierung nicht aufheben kann und eine Zuordnung in keinem Fall möglich ist.[27]

2. Gilt die Informationspflicht nach Art. 13 DSGVO, wenn die Daten für den Empfänger anonym sind?

Zusätzlich entschied der EuGH auch darüber, wie mit den Informationspflichten bei Erhebung von personenbezogenen Daten bei der betroffenen Person nach Art. 13 DSGVO umzugehen ist, wenn die pseudonymisierten Daten für den Datenempfänger anonym sind. Art. 13 Abs. 1 DSGVO legt als zeitliches Element der Informationspflicht den „Zeitpunkt der Erhebung dieser Daten“ fest. Der EuGH verwies entsprechend dem Wortlaut somit zunächst auf seine Rechtsprechung, wonach die Betroffenen sofort (bei Datenerhebung) zu informieren sind.[28] Die Identifizierbarkeit ist dabei aus Sicht des Verantwortlichen zu bestimmen.[29] Folglich spielt es für die Informationspflicht nach Art. 13 DSGVO keine Rolle, ob der Empfänger die Daten zuordnen kann oder ob sie für ihn anonym wären.[30] Der EuGH argumentiert dabei mit dem Sinn der Informationspflicht nach Art. 13 DSGVO. Danach sollen betroffene Personen durch die Informationen die Möglichkeit haben, mit voller Kenntnis der Sachlage über ihre personenbezogenen Daten bei der Datenerhebung zu entscheiden.[31] Zur vollen Sachlage gehören auch die potenziellen Empfänger. Somit müssen selbst Empfänger, für die die Daten anonym wären, vom Verantwortlichen genannt werden. Vorliegend entschied der EuGH, dass der SRB die betroffenen Personen über Deloitte als möglichen Empfänger der personenbezogenen Daten hätte informieren müssen.

III. Folgen des SRB-Urteils

Das SRB-Urteil hat in Fachkreisen zu vielen Diskussionen geführt. Insbesondere stellen sich nach diesem Urteil datenschutzrechtliche Folgefragen. Dies betrifft vor allem Situationen, in denen Daten ausgetauscht werden oder mehr als eine Stelle Daten verarbeitet und die Identifizierbarkeit der Daten auseinanderfällt.

1. Gemeinsame Verantwortung, Art. 26 DSGVO

Als Erstes stellt sich bereits die Frage, wie Konstellationen von zwei oder mehr Verantwortlichen[32] zu behandeln sind, wenn dieselben Daten von einem Verantwortlichen mithilfe von zusätzlichen Informationen zugeordnet werden können, also personenbezogen sind, und für einen anderen Verantwortlichen wiederum keine tatsächlichen oder rechtlichen Möglichkeiten einer Zuordnung bestehen. Wenn zwei Stellen gemeinsame Entscheidungen über Zwecke und Mittel einer Verarbeitung treffen, spricht dies in der Regel für eine gemeinsame Verantwortlichkeit i. S. d. Art. 26 DSGVO. Wenn die Daten für eine der Stellen jedoch anonym sind, ist fraglich, ob die DSGVO für diese Stelle überhaupt Anwendung findet. Gerade dann sind jedoch umfangreiche Vorkehrungen zu treffen, um im Zweifel beweisen zu können, dass die Daten für die Stelle tatsächlich und dauerhaft anonym sind und auch bleiben.

23 EuGH, Urt. v. 4.9.2025, Rs. C-413/23 P, Rn. 83.
24 Ibid., Rn. 84.
25 Ibid., Rn. 85.
26 Ibid., Rn. 76.
27 Ibid., Rn. 77.
28 Ibid., Rn. 102.
29 Ibid., Rn. 111.
30 Ibid., Rn. 112.
31 Ibid., Rn. 108.
32 Allgemein zur gemeinsamen Verantwortung siehe Geiselmann, Gemeinsam sind wir verantwortlich!, DFN-Infobrief Recht 1/2024 sowie zur EuGH-Rechtsprechung Tech, Die Heiligen Drei der gemeinsamen Verantwortlichkeit, DFN-Infobrief Recht 12/2025.

2. Auftragsverarbeitung, Art. 28 DSGVO

Außerdem ist fraglich, wie mit der Auftragsverarbeitung nach Art. 28 DSGVO künftig umzugehen ist, wenn (wie in der Konstellation bei SRB und Deloitte) der Verantwortliche die Daten pseudonymisiert an einen Dienstleister übermittelt, für den die Daten anonym sind. Liegt dann noch eine Auftragsverarbeitung i. S. d. Art. 28 DSGVO vor, und bedarf es einer Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DSGVO? Immerhin definiert Art. 4 Nr. 8 DSGVO den Auftragsverarbeiter als eine Person, die „personenbezogene Daten im Auftrag des Verantwortlichen" verarbeitet. Dabei sind verschiedene Konstellationen und Szenarien zu unterscheiden, die jeweils genau durchgeprüft werden müssen. In diesem Zusammenhang könnte sich der Verantwortliche zumindest insofern zusätzlich absichern, indem er vertraglich mit dem Dienstleister vereinbart, dass eine Re-Identifizierung verboten ist.[33]

3. Datenübermittlungen, Art. 44 ff. DSGVO

Zuletzt verbleibt nach dem SRB-Urteil des EuGH die Frage, ob eine Rechtsgrundlage für die Weitergabe der Daten oder gerade auch im Kontext von Drittlandtransfers nach Art. 44 ff. DSGVO erforderlich ist und wessen Perspektive dafür heranzuziehen ist. Auch hier gilt es, die Situationen genaustens zu prüfen und Nachweise zu sammeln.

4. Digitaler-Omnibus-Verordnungsentwurf

Mitte November 2025 veröffentlichte die EU-Kommission den Verordnungsentwurf zu einem digitalen Omnibus zur Änderung von Datengesetzen.[34] Dieser enthält – gerade im Datenschutzrecht – einige Anpassungen.[35] So will der Gesetzgeber die Rechtsprechung des EuGH gesetzlich verankern, indem er die Definition der „personenbezogenen Daten" in der DSGVO anpasst. Die Datenschutzkonferenz (DSK) sah die vorgeschlagenen Änderungen der DSGVO jedoch kritisch und will sich gerade bezüglich der Definition von „personenbezogenen Daten" noch ausführlich äußern.[36]

IV. Bedeutung für Hochschulen und Forschungseinrichtungen

Das SRB-Urteil ist auch für Hochschulen und Forschungseinrichtungen interessant. Zum einen betont das Urteil, dass datenschutzrechtliche Informationspflichten einzuhalten sind. Dies sollten auch Hochschulen und Forschungseinrichtungen als Verantwortliche nicht vernachlässigen. Zum anderen gilt auch für Hochschulen und Forschungseinrichtungen als Verantwortliche, dass künftig eine noch sorgfältigere Prüfung bei einer Weitergabe von pseudonymisierten Daten erfolgen muss. Das Urteil kann jedoch auch eine Chance für die Forschung sein. Bestimmte Forschungsprojekte und gerade das Training von KI-Modellen sind einfacher durchzuführen, wenn anonyme Daten verwendet werden. Sofern also beispielsweise personenbezogene Daten bei einer anderen Stelle verarbeitet und so pseudonymisiert an Hochschulen und Forschungseinrichtungen übermittelt werden, sodass diese keine Möglichkeit einer Re-Identifizierung haben, wären die Daten für die Hochschule oder Forschungseinrichtung anonym. Die tatsächlichen Folgen des SRB-Urteils könnten somit in vielerlei Hinsicht weitreichend sein. ◆

33 So zum Beispiel auch Nebel, CR 2025, 711, 716 Rn. 37.

34 COM (2025) 837 final, 19.11.2025, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

35 Zu den Reformvorschlägen der DSGVO ausführlich in dieser Infobrief-Ausgabe: Müller-Westphal, Alles bleibt anders, DFN-Infobrief Recht 2/2026.

36 Pressemitteilung vom 12.12.2025, S. 1 f., https://datenschutzkonferenz-online.de/media/pm/DSK_PM_110_DSK.pdf.

Mit digitalen Wasserzeichen zu klareren Informationsökosystemen?

Wie die EU KI-generierte Inhalte erkennbar machen will

Katzenvideos, Forschungsdaten, Fotobeweise für Kriegsverbrechen: Seit Kurzem lässt sich all das täuschend echt von Künstlicher Intelligenz (KI) generieren. Jetzt verabschiedet die EU einen „Verhaltenskodex für die Kennzeichnung von KI-generierten Inhalten“.[1] Können die Vorgaben zu KI-Wasserzeichen und anderen technischen Lösungen Abhilfe schaffen?

Text: **Paul Friedl** (Forschungsstelle Recht im DFN)

I. „Slop“ und Co.: KI-generierte Gesellschaftsherausforderungen

Jedes Jahr im Dezember kürt das bekannte englische Wörterbuch Merriam-Webster ein Wort des Jahres. 2020 war das „pandemic“, passend zum grassierenden Corona-Virus, 2022 „gaslighting“, ein Modebegriff zur Bezeichnung psychischer Manipulationsstrategien, und 2024 „polarization“, wenig überraschend im US-amerikanischen Wahljahr. Letztes Jahr kürte die Jury nun „slop“ zum Gewinner. Damit werden nach der hauseigenen Definition „geringwertige digitale Inhalte, die für gewöhnlich in großen Mengen durch Künstliche Intelligenz produziert werden“, bezeichnet.[2] Darunter fallen etwa Videos von alten Frauen, die angeblich ihren hundertzwanzigsten Geburtstag feiern, oder Bilder eines aus Shrimps bestehenden Jesus.[3] Auf Deutsch lässt sich „slop“ wörtlich mit „Pampe“ oder „Mansch“ übersetzen. Durchaus passend also, denn es steht zu befürchten, dass von generativer KI produzierter „slop“ unsere ohnehin schon angeschlagenen Informationsökosysteme vertrübt, im schlimmsten Fall sogar verseucht. Was echt und was falsch ist, lässt sich schließlich immer schlechter unterscheiden.

II. Abhilfe durch Nachverfolgbarkeit und Transparenz?

Schon länger wird debattiert, diesen Problemen mit einer Transparenzoffensive zu begegnen: KI-generierte Inhalte müssten als solche gelabelt und Nutzer:innen diese Informationen zugänglich präsentiert werden. Dadurch solle sichergestellt werden, dass KI-generierte Inhalte nachverfolgt und potenziell auch moderiert werden können. Endnutzer:innen würden befähigt, Inhalte richtig einzuschätzen und darauf aufbauend ihr Verhalten anzupassen. Um solche Nachvollziehbarkeit bzw. Transparenz zu erreichen, stehen verschiedene technologische Mittel zur Verfügung. Die technische Identifikation eines Inhalts als KI-generiert kann beispielsweise über Metadaten erfolgen, in denen der künstliche Ursprung einer Datei, klassischerweise einer Audio-, Video- oder Bilddatei, an die Hauptdatei angehängt und im Datentransfer an jede:n Empfänger:in (beispielsweise eine Social-Media-Plattform oder ein:en Social-Media-Nutzer:in) mitübermittelt wird. Derartige Metadaten lassen sich aber technisch leicht entfernen und können die Nachverfolgbarkeit des künstlichen Ursprungs eines Inhalts deshalb nur begrenzt sicherstellen. Deswegen gewinnen seit einigen Jahren auch sogenannte

1 So die eigenartige, KI-generierte deutsche Übersetzung des im englischen Original als „Code of Practice on Marking and Labelling of AI-generated content“ betitelten Dokuments, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-second-draft-code-practice-marking-and-labelling-ai-generated-content, alle Links dieses Beitrages wurden zuletzt abgerufen am: 18.03.2026.

2 Merriam-Webster, „slop“, Bedeutung 1.a, https://www.merriam-webster.com/dictionary/slop.

3 Beide Beispiele sind besonders weit verbreitet und deswegen bekannt, siehe https://www.theguardian.com/technology/2025/dec/27/from-shrimp-jesus-to-erotic-tractors-how-viral-ai-slop-took-over-the-internet.

digitale Wasserzeichen an Beliebtheit. Bei diesen wird die Struktur der generierten Datei noch im Erstellungsvorgang selbst so verändert, dass mit spezifisch dafür entwickelten Programmen der künstliche Ursprung der Datei ausgelesen werden kann, ohne dass dies für das menschliche Auge oder Ohr erkennbar wäre. Technisch wird dies beispielsweise durch „unsichtbare" Veränderungen der Pixelstruktur eines Bildes oder Videos erreicht. Auch Wasserzeichen bieten allerdings keinen hundertprozentigen Schutz; auch sie können – teils ohne größeren technischen Aufwand – überschrieben oder zerstört werden und sind insbesondere bei künstlich generierten Texten schwer zu bewerkstelligen und fehleranfällig.

Neben diesen Mitteln, die die technische Erkennbarkeit von KI-Inhalten gewährleisten können, bedarf es aber auch Techniken, die die Erkennbarkeit von KI-Inhalten gegenüber Menschen bewirken können. Hier kommen in erster Linie sichtbare Wasserzeichen, beispielsweise in Gestalt kleiner Logos, in Betracht, die auf das Medium „aufgedruckt" werden. KI-Systeme wie OpenAIs Sora oder Googles Gemini verwenden derartige sichtbare Wasserzeichen schon heute in der Bild- und Videogeneration.

III. Das Regelungskonzept der KI-VO

Auch die 2024 verabschiedete KI-Verordnung (KI-VO)[4] der EU sieht Regelungen vor, die die Nachvollziehbarkeit und Erkennbarkeit von KI-generierten Inhalten garantieren oder zumindest erhöhen sollen. Konkret sieht Art. 50 KI-VO Transparenzpflichten für zwei Arten von Akteuren vor: Nach Art. 50 Abs. 2 KI-VO müssen Anbieter[5] von KI-Systemen, die „synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen", sicherstellen, dass die „Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind". Diese Mittel müssen weiter möglichst „wirksam, interoperabel, belastbar und zuverlässig" sein. Praktisch bedeutet dies, dass GenAI-Anbieter wie Google, Meta oder OpenAI dafür sorgen müssen, dass die mit ihren Systemen generierten Inhalte (wirksam, interoperabel etc.) als solche erkannt werden können. Daneben sieht Art. 50 Abs. 4 KI-VO vor, dass Betreiber[6] eines KI-Systems offenlegen müssen, dass Inhalte „künstlich erzeugt oder manipuliert wurden", wenn es sich entweder um a) „Deepfakes"[7] oder b) „Text, der … die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse informieren" soll, handelt, wobei in beiden Fällen gewisse Ausnahmen bestehen. Praktisch bedeutet dies, dass etwa OpenAI sicherstellen muss, dass mit ChatGPT erzeugte Deepfakes als solche erkennbar sind. Gleiches gilt nach der zweiten Alternative für Online-Magazine, die KI-generierte Artikel veröffentlichen wollen, sofern diese nicht „einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden". Wie genau diese Pflichten aber erfüllt werden sollen, lässt sich aus dem doch sehr abstrakten Normtext nicht ableiten.

IV. Ein bisschen konkreter: der neue Praxisleitfaden

Zur Konkretisierung der abstrakten Pflichten sieht die KI-Verordnung deshalb auch die Ausarbeitung eines Praxisleitfadens (engl.: Code of Practice) vor. Solche Praxisleitfäden können von der Europäischen Kommission als rechtsverbindliche Konkretisierungen der genannten gesetzlichen Pflichten anerkannt werden. Kommt es zu dieser Anerkennung, reicht die Einhaltung der Vorgaben des Praxisleitfadens auch zur Einhaltung des Gesetzes aus. Aus diesem Grund kommt den Praxisleitfäden erhebliche Bedeutung zu, nicht zuletzt, weil derzeit alle beteiligten Akteure von einer Annahme durch die Kommission auszugehen scheinen.

Die Ausarbeitung des Praxisleitfadens zur Kennzeichnung von KI-generierten Inhalten (engl.: Code of Practice on Marking and Labelling of AI-generated content) stieß das Büro für Künstliche Intelligenz der EU im September 2025 an: KI-Entwickler, Nutzende, Forschende und Vertreter der Zivilgesellschaft (u. a.) wurden in einem Konsultationsverfahren dazu aufgerufen, Input zu verschiedenen offenen Fragen bezüglich Regelungsbereich und -inhalt der genannten Pflichten zu liefern. Ausgehend von diesen Einreichungen haben von der Kommission ausgewählte wissenschaftliche Expert:innen in Zusammenarbeit mit den eingeladenen Stakeholdern bisher zwei Entwürfe des Praxisleitfadens veröffentlicht.

4 Verordnung (EU) 2024/1689.

5 „Anbieter" sind in Art. 3 Nr. 4 KI-Verordnung definiert als „natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich".

6 „Betreiber" sind in Art. 3 Nr. 4 KI-Verordnung definiert als „natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet".

7 „Deepfakes" sind in Art. 3 Nr. 60 KI-VO definiert als ein „durch KI erzeugter oder manipulierter Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde". Im Hochschulkontext ist an die Transparenzpflichten für Betreiber nach Art. 50 Abs. 4 KI-VO beispielsweise bei der Erstellung von Lehrmaterial zu denken. Siehe dazu Schöbel, Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2/2025, S. 4.

Im ersten Entwurf dieses Praxisleitfadens wurden bereits erste große Weichenstellungen getroffen. Was die Pflichten für Anbieter von generativen KI-Systemen angeht, einigte man sich darauf, dass diese nicht auf eine einzige Kennzeichnungstechnologie setzen dürften, sondern vielmehr einen „multilayered approach", d. h. eine Kombination an Methoden, verfolgen sollten, da keine Technologie zu 100 % sicher sei. Zu diesen Technologien gehörten zumindest 1) für das menschliche Auge unsichtbare, für dazu spezialisierte Systeme aber erkennbare „Wasserzeichen", 2) Metadaten-Tags und 3) sogenanntes Fingerprinting. Bei Letzterem wird für jedes erstellte Medium (beispielsweise ein Bild) ein digitaler Kurzschlüssel erstellt und gespeichert, mit dem in der Folge nachgewiesen werden kann, dass das betroffene Medium mit dem jeweiligen KI-System erstellt wurde. Außerdem sollten Hersteller ein Interface bereitstellen, mit dem Dritte kostenlos überprüfen lassen könnten, ob ein bestimmtes Medium aus dem betroffenen KI-System stammt, und generell zur Entwicklung zuverlässigerer KI-Detektionssysteme beitragen. Betreiber von KI-Systemen wiederum müssten eine einheitliche Taxonomie zur Identifizierung von Deepfakes und KI-generierten Texten anwenden und derartige Inhalte mit einem leicht erkennbaren und barrierefreien Icon versehen. Zudem müssten Feedbackkanäle bereitgestellt werden, über die Dritte nicht oder falsch gelabelte Deepfakes oder KI-Texte melden könnten; Betreiber müssten Fehler in der Folge auch kategorisieren.

Im Anfang März veröffentlichten zweiten Entwurf des Praxisleitfadens wurde dann bestimmt, dass Hersteller von generativen KI-Systemen mindestens zwei Identifizierungsschichten verwenden müssten (Metadaten und unsichtbare Wasserzeichen). Außerdem sollten Identifizierungsmarker in einem von der EU noch zu entwickelnden, öffentlichen Verzeichnis bereitgestellt und hier gespeichert werden, um interoperable Identifizierungstechniken zu ermöglichen. Was die Pflichten für Betreiber betrifft, wurde klargestellt, dass die Verwendung eines von der EU noch zu entwickelnden Kennzeichnungs-Icons freiwillig bleiben würde. Zusätzlich wurde für die Entwicklung dieses Icons die Einsetzung einer EU-Taskforce in den Raum gestellt.

V. Potenzial des Leitfadens und Ausblick

Bei dem Leitfaden handelt es sich um einen ambitionierten Vorschlag, der dem „Problem" KI-generierter Inhalte mit einem umfangreichen und ausgefeilten Lösungsarsenal beikommen will und dabei auch auf die zentralen technologischen Herausforderungen eingeht, die zur Herstellung von Nachverfolgbarkeit und Transparenz bewältigt werden müssen. Die Technologieoffenheit, die dem Leitfaden an wichtigen Stellen eingeschrieben ist, und auch die vorgeschlagenen Kooperationsmechanismen zwischen KI-Herstellern, KI-Betreibern und Aufsichtseinrichtungen überzeugen.

Der Praxisleitfaden bietet also eine gute Lösung. Als Außenstehender fragt man sich allerdings auch: Für welches Problem eigentlich? Wie eingangs schon erwähnt wurde, spielen KI-generierte Inhalte in vielen Bereichen eine Rolle. Einige der problematischsten, etwa der Einsatz für Desinformationskampagnen oder Betrugsmaschen, zeichnen sich durch Aspekte aus, die in dem Leitfaden wenig bis gar nicht adressiert werden. Insbesondere müssen hier nämlich Akteure eingefangen werden, die die Identifikation ihrer Inhalte als KI-generiert aktiv verhindern wollen und aus diesem Grund auch auf (außereuropäische) Anbieter zurückgreifen, die sich nicht an die Regeln der EU halten. Im Übrigen scheint der bisherige Entwurf zu wenig Augenmerk auf die Verbreitung KI-generierter Inhalte und die Akteure dieser Verbreitung, primär Social-Media-Plattformen, zu legen. Entscheidend ist in erster Linie nicht, dass Deepfakes oder andere (schädliche) KI-Inhalte nicht generiert werden, sondern, dass sie nicht oder nur mit adäquatem Kontext verbreitet werden. Um das zu erreichen, müssen Content-Verbreiter womöglich nicht nur befähigt, sondern auch verpflichtet werden, risikobehaftete Inhalte zu markieren oder zu verhindern. Auch wenn solche Pflichten potenziell auch aus dem Digital Services Act abgeleitet werden können, wäre eine stärkere Einbindung dieser Akteure auch in das Regelungsgefüge des Art. 50 KI-VO und den hier besprochenen Praxisleitfaden sicherlich wünschenswert. Bleibt zu hoffen, dass dies in der finalen, für den Juni angekündigten Version des Praxisleitfadens berücksichtigt wird. Denn aller Voraussicht nach treten die Transparenzpflichten des Art. 50 KI-VO schon im August dieses Jahres in Kraft.

Das kann durchaus auch für Hochschulen oder dort Beschäftigte relevant werden. Treten diese nämlich als Betreiber eines KI-Systems auf – so etwa die Universität, die ihren Studierenden eine eigens getrimmte generative KI bereitstellt, oder die Lehrperson, die eine solche zur Erstellung von Vorlesungsmaterialien nutzt –, sind sie es, die das Einhalten der Kennzeichnungspflichten bezüglich Deepfakes und Texten von öffentlichem Interesse einhalten müssen. ◆

Digitale Souveränität im Fokus – das DFN-Diskussionsforum der Kanzlerinnen und Kanzler 2026

Wissenschaftsfreiheit braucht Sicherheit: Beim DFN-Diskussionsforum der Kanzlerinnen und Kanzler in Berlin diskutierten Hochschulleitungen, wie digitale Souveränität gelingen kann. Klar wurde: Nur mit gemeinsamen Strategien, zuverlässigen Infrastrukturen und hochschulübergreifender Zusammenarbeit lassen sich Forschung und Innovation wirksam schützen.

Text: **Nina Bark, Maimona Id** (DFN-Verein)

Eindringliches Plädoyer für ein gemeinsames Sicherheitsverständnis: Mit ihrer Erfahrung in Spionageabwehr und Krisenmanagement zeichnete Friederike Dahns, Abteilungsleiterin für Cyber- und Informationssicherheit im BMI, in ihrer Keynote ein präzises Bild der aktuellen Bedrohungslage | *Foto: Jürgen Aloisius Morgenroth/DFN-Verein*

Am Montag und Dienstag, 27. und 28. April 2026, kamen in Berlin Hochschulleitungen aus ganz Deutschland beim DFN-Diskussionsforum der Kanzlerinnen und Kanzler zusammen, um gemeinsam aktuelle Herausforderungen und Entwicklungen der Digitalisierung in Bildung und Forschung zu diskutieren.

Nach einer herzlichen Begrüßung der Teilnehmenden durch die DFN-Vorstandsmitglieder Prof. Dr.-Ing. Stefan Wesner und Christian Zens eröffnete Friederike Dahns, Abteilungsleiterin für Cyber- und Informationssicherheit im Bundesministerium des Innern die Veranstaltung mit ihrer Keynote „Wissen schützen: Wissenschaft im Zeitalter von Cybersicherheit und digitaler Souveränität“. Damit setzte sie den thematischen Schwerpunkt des diesjährigen Treffens. Sie verdeutlichte, dass sicheres Handeln im digitalen Raum ein Kernaspekt digitaler Souveränität ist. Für Hochschulen und Forschungseinrichtungen bedeute dies, ihre IT-Infrastruktur so abzusichern, dass innovative Erkenntnisse und hochwertige Forschungsdaten vor Ausspähung und Manipulation geschützt sind. Sicherheit sei damit kein Gegensatz zur Freiheit der Wissenschaft, sondern eine Voraussetzung.

Daran knüpfte Prof. Dr. Wolfgang Hommel, leitender Direktor des Forschungsinstituts Cyber Defence der Universität der Bundeswehr München, am zweiten Tag der Veranstaltung an: Er mahnte, dass das hohe Gut der Freiheit von Forschung und Lehre mit Verantwortung einhergehe – und sowohl hochschulweite als auch hochschulübergreifende Strategien, Prioritäten und Ressourcen erfordere. Digitale Souveränität bedeute auch, Wissen und Kompetenzen in den eigenen Einrichtungen nicht systematisch zugunsten kommerzieller Dienstleistungen abzugeben.

Im Anschluss betrachteten DFN-Vorstandsmitglied Prof. Dr. Helmut Reiser und Dr. Christian Grimm, Geschäftsführer des DFN-Vereins, die Resilienz von Infrastrukturen und Diensten im Verein. Am Beispiel DFN-Security erläuterten sie, wie der DFN-Verein die Einrichtungen bei der Erhöhung ihres IT-Sicherheitsniveaus unterstützt. Ergänzend hoben sie die Bedeutung kooperativer Ansätze hervor, um gerade auch kleine Einrichtungen vor der Bedrohung durch Cyberangriffe besser zu schützen.

Dr. jur. Jan K. Köcher, Prokurist der DFN-CERT Services GmbH, beleuchtete die gesetzlichen Anforderungen an die Cybersicherheit im Hochschulbereich und beschrieb das Spannungsfeld zwischen föderaler Regulierung und technischer Realität. Die juristische Einordnung von digitaler Souveränität lieferte die Forschungsstelle Recht im DFN: In der nachfolgenden Session gingen die wissenschaftlichen Mitarbeitenden Anna Maria Yang-Jacobi und Philipp Schöbel auf die Themen digitale Hochschulzeugnisse, die europäische KI-Regulierung sowie die Reform des europäischen Datenrechts ein.

Ein herzlicher Dank geht an alle Vortragenden, die die Veranstaltung mit ihrer Expertise und fundierten Einblicken bereichert haben, sowie an die zahlreichen Teilnehmenden für die konstruktiven Diskussionen, den Austausch und die wertvollen Impulse. Diese tragen dazu bei, dass wir unser Netz und unsere Dienste noch besser auf die Bedarfe der teilnehmenden Einrichtungen am Wissenschaftsnetz weiterentwickeln können. Wir freuen uns auf ein Wiedersehen in zwei Jahren! ◆

Das nächste DFN-Diskussionsforum der Kanzlerinnen und Kanzler findet 2028 statt. Informationen zur Veranstaltung finden Sie rechtzeitig unter:
https://www.dfn.de/news/veranstaltungen/

Gut vernetzt: Die gelungene Veranstaltung brachte nicht nur wertvolle Erkenntnisse, sondern lebte vor allem vom intensiven Erfahrungsaustausch untereinander | *Fotos: Jürgen Aloisius Morgenroth/DFN-Verein*

DFN unterwegs

Der Begriff Netz ist schon Teil unseres Namens. Und gut vernetzt sind auch unsere Mitarbeiterinnen und Mitarbeiter – weit über die Grenzen unserer technischen Infrastruktur hinaus. Wo wir überall unterwegs sind, zeigen wir hier.

Als Gruppenleiter beim DFN-CERT entwickelt Eugene Brin mit NeMo die technische DDoS-Resilienz des Forschungsnetzes aktiv weiter. Ausgestattet mit dem Hut des Programme Committee Chairs war er für das inhaltlich hochaktuelle Programm der …

… GÉANT Security Days 2026 mitverantwortlich, die vom 7. bis 9. April 2026 in Utrecht stattfanden.

Schon nach der ersten Kaffeepause zeigt sich oft, wie eine Veranstaltung wird. Bei den GÉANT Security Days war recht früh klar: Hier passt einfach alles zusammen – Themen, Teilnehmende und Impulse. Die Stimmung war offen, lebendig und konzentriert. Mit 167 registrierten Teilnehmenden war die Tagung gut besucht. Einige zusätzlich vor Ort ausgestellte Badges für Kurzentschlossene zeigten das große Interesse an der Veranstaltung. Vielleicht lag das auch ein Stück weit an der Location: Das Jaarbeurs, das fast futuristisch anmutende große Messe- und Kongresszentrum direkt am Hauptbahnhof von Utrecht, war der passende Rahmen für ein Event, das sich auch mit der Zukunft der IT-Sicherheit auseinandersetzt.

Für mich war die Tagung in diesem Jahr in doppelter Hinsicht besonders. Zum einen durfte ich nicht nur das Programmkomitee leiten, sondern auch den DDoS-Track mit dem Workshop „Protecting Research and Education Networks from DDoS – What's Working, What's Not" – später habe ich auch das DDoS-Sidemeeting moderiert. Gerade deshalb habe ich mich unheimlich gefreut, dass das Programm nicht nur auf dem Papier stimmig aussah, sondern vor Ort auch wirklich getragen hat. Die Mischung aus Keynotes, fachlichen Sessions, Lightning Talks, praktischen Workshops, Capture-The-Flag(CTF)-Format und informellen Gesprächen ist genau das, was diese Tagung so stark macht. Man kommt mit einer Idee rein und fährt mit zehn neuen wieder nach Hause.

Die Opening Plenary gab gleich einen Vorgeschmack auf die kommenden Tage. In seiner Keynote „The bumpy road ahead – IT security challenges of the next years" stellte Frank Rieger, Internetaktivist und ehemaliger Sprecher des Chaos Computer Clubs, die sehr reale Frage, was KI-gestützte Cyberangriffe und Verteidigung für unsere Arbeit in der Cybersicherheit bedeuten. Spannend war dabei, wie nah er an der Praxis blieb, inklusive der ganz handfesten Empfehlung, auch mal selbst ein paar Euro in die Hand zu nehmen, um zu verstehen, welchen Fortschritt Frontier-Modelle in den vergangenen Monaten gemacht haben.

Im Anschluss schärfte Valerie Aurora, Expertin für Systemarchitektur und Autorin, den Blick für das Thema Internet Resilience und sprach über die unangenehme, aber notwendige Frage, wie wir mit Ausfällen und Störungen umgehen, wenn Infrastruktur nicht einfach so verfügbar ist. Einer der einprägsamsten Takeaways ihrer Keynote: LoRa-Mesh-Netze – dezentrale Funknetze, die auch ohne zentrale Infrastruktur funktionieren – aus der

GÉANT Security Days 2026: Unter dem Motto „Securing Tomorrow Together“ kamen Fachleute aus ganz Europa zusammen, um gemeinsam Lösungsansätze rund um Cybersicherheit in Forschung und Lehre zu diskutieren | *Fotos: Nabeel Ashraf/GÉANT und Michel Gerdes/DFN-CERT*

Community sind günstig, überraschend resilient, und das Mitmachen kann viel Spaß bringen.

Am zweiten Tag hielt Nancy Beers, Gamification-Expertin mit über 25 Jahren Erfahrung in der Informations- und Kommunikationstechnik, ein Plädoyer für mehr Spiel, Neugier und Beweglichkeit. Damit sorgte sie nicht nur für frische Perspektiven, sondern auch für eine lockere Atmosphäre und viel gute Laune. Im Abschlussplenum erinnerte Alexandre Dulaunoy, Leiter des Computer Incident Response Centers Luxembourg (CIRCL), daran, warum Open Source, offene Communities und vertrauensvolle Zusammenarbeit in offenen Netzen kein Beiwerk sind, sondern ein sehr handfester Sicherheitsfaktor und letztlich auch ein gesellschaftlicher Wert.

Besonders beeindruckt hat mich, wie gut die Krisen- und Resilienzthemen ineinandergriffen. Die Beiträge rund um TALON, die erste europäische Krisenübung für nationale Forschungs- und Bildungsnetze (NRENs), und das Thema

Ob Hands-on-Training, interaktiver Workshop oder Capture-the-Flag-Session: Die GÉANT Security Days 2026 setzten auf viel Praxis und direkt anwendbares Wissen | *Fotos: Nabeel Ashraf/GÉANT und Michel Gerdes/DFN-CERT*

Krisenvorbereitung waren stark. Die praktische Crisis Session war für mich sogar eines der Highlights der Tagung. Sie war interaktiv, lebendig und konkret. Genau so etwas bleibt nachhaltig hängen: nicht nur abstrakt und theoretisch über Krisen zu reden, sondern gemeinsam darüber nachzudenken, wie eine sinnvolle Vorbereitung tatsächlich aussieht, wo es hakt und was im Ernstfall wirklich hilft.

Keine Fragen, kein Schnickschnack, reiner Inhalt: Als geballte Ladung von spannenden Kurzvorträgen in nur je 300 Sekunden waren die Lightning Talks ein weiteres Highlight. Dieses Format funktioniert erstaunlich gut. Sehr eindrucksvoll war, dass mein Kollege Andrej Zieger vom DFN-CERT dabei sein Talent als Märchenerzähler unter Beweis stellen konnte, als er von einer wundervollen Spielwiese für sagenhafte Forschende im GÉANT Security Innovation Lab berichtete und dafür reichlich Applaus erntete.

Auch der DDoS-Track am zweiten Tag hat aus meiner Sicht einen nachhaltigen Eindruck hinterlassen. Die drei Vorträge boten aufschlussreiche Einblicke, aktuelle Entwicklungen und operative Relevanz – genug Stoff für lebhafte Gespräche in der Mittagspause. Mindestens genauso wichtig war mir aber das DDoS-Sidemeeting am letzten Tag. Nach drei weiteren Präsentationen entwickelte sich dort eine sehr dynamische Diskussion im Round-Table-Format. Genau dieser Teil war für mich ausgesprochen wertvoll. Denn dort wurde nicht nur präsentiert, sondern wirklich diskutiert: über Positionen, Schmerzpunkte und sehr konkrete Herausforderungen, mit denen die europäische NREN-Community im DDoS-Umfeld aktuell ringt. Solche Foren sind schwer in Folien zu gießen, aber oft der eigentliche Mehrwert einer Veranstaltung.

Abseits der Sessions hatte Utrecht genau die richtige Atmosphäre für so ein Treffen. Professionell, freundlich und fokussiert, aber nicht steif. Man konnte sich morgens über Botnet-Infrastruktur, Supply Chains, Detektion und Krisenvorbereitung austauschen und ein paar Stunden später mit Stroopwafels beim Abendprogramm genau an diese Gespräche wieder anknüpfen. Diese Mischung aus Fachlichkeit und Community ist schwer zu planen, aber leicht zu erkennen, wenn sie aufgeht. Und in Utrecht war sie deutlich spürbar.

Mein Fazit: Die GÉANT Security Days 2026 waren inhaltlich stark, organisatorisch rund und vor allem ein exzellentes Beispiel dafür, warum solche Community-Formate wichtig sind. Sie bringen Leute zusammen, die ähnliche Probleme haben, aber oft in unterschiedlichen Kontexten arbeiten. Genau daraus entstehen Impulse und Verbindungen, die man später mit nach Hause nimmt. Für mich persönlich waren es drei intensive, sehr gelungene Tage mit vielen guten Begegnungen, klugen Beiträgen und dem schönen Gefühl, dass in unserer Community nicht nur viel Expertise vorhanden ist, sondern auch echtes Interesse am Miteinander. ◆

DFN live: Wissen teilen, Erfahrungen weitergeben

Der DFN-Verein lebt von der Expertise und Erfahrung seiner Mitglieder und Teilnehmer am Deutschen Forschungsnetz. Mit zahlreichen Veranstaltungen, Tutorien, Tagungen und Workshops bietet der DFN-Verein ein Forum für lebendigen Dialog und Wissenstransfer.

91. DFN-Mitgliederversammlung

Am Mittwoch, 3. Dezember 2025, fand die 91. DFN-Mitgliederversammlung im Wissenschaftszentrum Bonn statt. Zweimal im Jahr treffen sich die Delegierten der mehr als 350 DFN-Mitgliedseinrichtungen aus Forschung und Lehre, um gemeinsam die Zukunft des DFN-Vereins zu gestalten. Auf der Tagesordnung standen neben den Berichten über die Aktivitäten des DFN-Vereins im ersten Halbjahr 2025 verschiedene Vorträge zum Stand des Wissenschaftsnetzes und der Dienste.

Ein besonderes Highlight der Vorabendveranstaltung war der Vortrag „Noch mehr Daten! Wie datengetriebene Modelle die Wetter- und Klimavorhersagen revolutionieren“ von Prof. Dr. Martin Schultz vom Forschungszentrum Jülich. In seiner Präsentation zeigte der Co-Leiter der Abteilung Large Scale Data Science am Jülich Supercomputing Centre (JSC), dass datengetriebene Modelle, etwa auf Basis von KI, die Wettervorhersage grundlegend verändern, weil sie große Datenmengen effizient auswerten und teils sehr präzise Prognosen liefern. Für Klimaprojektionen seien Kombinationen aus datengetriebenen und physikalischen Ansätzen besonders vielversprechend, da sie Mustererkennung mit physikalischem Verständnis verbinden und so verlässlichere Aussagen ermöglichen. ◆

Gemeinsam gestalten: Basierend auf dem Mandat der Mitgliedseinrichtungen wird das Wissenschaftsnetz zukunftssicher weiterentwickelt | *Foto: DFN*

TERMIN

Die 92. Mitgliederversammlung findet am **Dienstag, 16. Juni 2026**, statt.

84. DFN-Betriebstagung

Am 17. und 18. März 2026 fand die 84. DFN-Betriebstagung im Leonardo Royal Hotel Berlin Alexanderplatz statt. Zwei Tage lang diskutierten 320 Teilnehmende vor Ort in neun Foren aktuelle Herausforderungen und Innovationen rund um Kommunikationsinfrastrukturen, IT-Sicherheit und kollaborative Dienste im Wissenschaftsnetz. Zusätzlich verfolgten 169 weitere Teilnehmende das Plenum im Livestream.

Am ersten Tag berichteten die Leiter der DFN-Bereiche Security, Trust and Identity Services, Collaboration Services sowie Network and Communication Services im Plenum über aktuelle Fortschritte und Neuigkeiten. Dabei ging es unter anderem um die DFN-CERT- sowie BSI-Lageberichte für Teilnehmer an DFN-Security; die aktuellen Rahmenverträge für cloudbasierte Videokonferenzdienste sowie DFN-Fernsprechen, die seit 1. März 2026 gelten; die neuen Außenanbindungen und Peering-Knoten im X-WiN und vieles mehr.

Auch die gut besuchten Foren hatten viele spannende Themen im Programm: zum Beispiel der Gemeinschaftsbeitrag von der Technischen Universität Berlin und der Freien Universität Berlin „Identity as a Service an Hochschulen – SSI, eIDAS und die EUDI Wallet“. ◆

Der persönliche Austausch zählt: Als Präsenzveranstaltung bietet die DFN-Betriebstagung viel Raum für Gespräche und Begegnungen | *Foto: Iven Jurk/DFN*

TERMIN

Die 85. DFN-Betriebstagung findet am **Dienstag und Mittwoch, 6. und 7. Oktober 2026**, statt.

Neben dem Vortragsprogramm bot die Ausstellung praxisnahe Einblicke in aktuelle Technik – von Datenbrillen bis hin zu KI-gestützten Kameralösungen | *Foto: Dirk Bei der Kellen/DFN*

TERMIN

Der 29. Workshop Videokonferenzen im Wissenschaftsnetz findet am **Dienstag und Mittwoch, 10. und 11. November 2026**, statt.

28. Workshop Videokonferenzen im Wissenschaftsnetz

Am Dienstag und Mittwoch, 4. und 5. November 2025, fand in Dresden der 28. Workshop Videokonferenzen im Wissenschaftsnetz statt. Dabei zeigte sich wieder einmal, wie vielfältig die Einsatzmöglichkeiten von Medientechnik in den Einrichtungen des Wissenschaftsnetzes sind. Themen wie Augmented Reality, die audiovisuelle Ausstattung des Forschungsschiffes „Polarstern“ oder Echtzeitübersetzungen von Vorlesungen sorgten für intensive Diskussionen. Ergänzt wurde das Vortragsprogramm durch eine Ausstellung mit Technik zum Ausprobieren – darunter Datenbrillen, AV-Technik und eine KI-gesteuerte Kamera. Zudem informierte der DFN-Verein über aktuelle Entwicklungen im Bereich Collaboration Services.

Auf Einladung des Videoconference & Collaboration Centers (VCC) treffen sich jedes Jahr Fachleute für audiovisuelle Kommunikation und Medientechnik im Klemperer-Saal der Sächsischen Landesbibliothek – Staats- und Universitätsbibliothek Dresden (SLUB), um sich über neue Entwicklungen in Forschung und Lehre auszutauschen. ◆

12. DFN-Konferenz „Datenschutz“

Die 12. DFN-Konferenz „Datenschutz“ fand am Dienstag und Mittwoch, 9. und 10. Dezember 2025, im Hotel Hafen Hamburg an den Landungsbrücken statt. Vertretende von Datenschutzaufsichtsbehörden sowie Expertinnen und Experten aus Hochschulen und Forschungseinrichtungen diskutierten viele spannende Themen – von Data Act, KI-VO, NIS-2 bis DDtrust-Scale. Ein Highlight war die Keynote „Der Data Act ist da: Neue Chancen für die Forschung“ von Thomas Fuchs, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit.

Seit 2012 veranstaltet das DFN-CERT im Auftrag des DFN-Vereins jedes Jahr die DFN-Konferenz „Datenschutz“. Die Konferenz richtet sich an Datenschutzverantwortliche aus Forschung, Bildung und Behörden und dient dem Austausch über die praktische Umsetzung des Datenschutzes. ◆

Dauerbrenner Datenschutz: Mit Fachvorträgen und Diskussionen zu aktuellen Entwicklungen und rechtlichen Rahmenbedingungen unterstützt die jährliche Konferenz Datenschutzverantwortliche aus Forschung und Bildung | *Foto: Jean Neuwald/DFN*

TERMIN

Die 13. DFN-Konferenz „Datenschutz“ findet am **Dienstag und Mittwoch, 24. und 25. November 2026**, statt.

IT-Sicherheit in allen Facetten: Die große Vielfalt an Themen macht die DFN-Konferenz „Sicherheit in vernetzten Systemen“ zu einem zentralen Treffpunkt für Fachpublikum rund um Cybersecurity | *Foto: Nina Bark/DFN*

TERMIN

Die 34. DFN-Konferenz „Sicherheit in vernetzten Systemen“ findet am **Dienstag und Mittwoch, 23. und 24. Februar 2027**, statt.

33. DFN-Konferenz „Sicherheit in vernetzten Systemen“

Die 33. DFN-Konferenz „Sicherheit in vernetzten Systemen“ fand am Dienstag und Mittwoch, 27. und 28. Januar 2026, im Grand Elysée Hotel Hamburg statt und wurde vom DFN-CERT im Auftrag des DFN-Vereins veranstaltet. Das Programm bot hochkarätige Beiträge zu aktuellen Entwicklungen und Herausforderungen der Informationssicherheit – vom Einsatz von KI zur Verbesserung der IT-Sicherheit bis zum Aufbau eines Ethical-Hacking-Labors. In ihrer Keynote „Shift Happens: Wie sich Cybercrime und IR in fünf Jahren verändert haben“ zogen Leonard Rapp und Jasper Bongertz (G Data Advanced Analytics GmbH) unter anderem das Fazit, dass IT-Sicherheit kein technisches, sondern ein organisatorisches, wirtschaftliches Problem ist.

Mit ihrer explizit technischen und wissenschaftlichen Ausrichtung, einer großen Vielfalt an Beiträgen und Diskussionen hat sich die DFN-Konferenz als eine der größten deutschen Tagungen für Informationssicherheit etabliert. ◆

Alle Veranstaltungen des DFN-Vereins finden Sie hier:
https://www.dfn.de/news/veranstaltungen/

Überblick DFN-Verein

(Stand: 06/2026)

Foto: jackijack / fotolia

Laut Satzung fördert der DFN-Verein die Schaffung der Voraussetzungen für die Errichtung, den Betrieb und die Nutzung eines rechnergestützten Informations- und Kommunikationssystems für die öffentlich geförderte und gemeinnützige Forschung in der Bundesrepublik Deutschland. Der Satzungszweck wird insbesondere verwirklicht durch Vergabe von Forschungsaufträgen und Organisation von Dienstleistungen zur Nutzung des Deutschen Forschungsnetzes.

Als Mitglieder werden juristische Personen aufgenommen, von denen ein wesentlicher Beitrag zum Vereinszweck zu erwarten ist oder die dem Bereich der institutionell oder sonst aus öffentlichen Mitteln geförderten Forschung zuzurechnen sind. Sitz des Vereins ist Berlin.

Die Geschäftsstelle

Standort Berlin (Sitz des Vereins)
DFN-Verein e. V.
Alexanderplatz 1
10178 Berlin
Telefon: +49 30 884299-0

Standort Stuttgart
DFN-Verein e. V.
Schloßstraße 70
70176 Stuttgart
Telefon: +49 711 63314-0

Die Organe

Mitgliederversammlung
Die Mitgliederversammlung ist u. a. zuständig für die Wahl der Mitglieder des Verwaltungsrates, für die Genehmigung des Jahreswirtschaftsplanes, für die Entlastung des Vorstandes und für die Festlegung der Mitgliedsbeiträge. Derzeitiger Vorsitzender der Mitgliederversammlung ist Dr. Rainer Bockholt, Universität Bonn.

Verwaltungsrat
Der Verwaltungsrat beschließt alle wesentlichen Aktivitäten des Vereins, insbesondere die technisch-wissenschaftlichen Arbeiten, und berät den Jahreswirtschaftsplan. Für die 14. Wahlperiode sind Mitglieder des Verwaltungsrates:

Kerstin Bein
(Universität Mannheim)

PD Dr. Wolfgang zu Castell
(GFZ Helmholtz-Zentrum für Geoforschung)

Peter Gietz
(DAASI International GmbH)

Ilona Glaser
(Deutscher Wetterdienst)

Prof. Dr. Frank Jenko
(Technische Universität München)

Dr. Lars Köller
(Technische Hochschule Ostwestfalen-Lippe)

Dieter Lehmann
(Universität Leipzig)

Dr. Holger Marten
(Christian-Albrechts-Universität zu Kiel)

Dr. Hartmut Plehn
(Otto-Friedrich-Universität Bamberg)

Prof. Dr. Helmut Reiser
(LRZ der Bayerischen Akademie der Wissenschaften)

Prof. Dr.-Ing. Günter Schäfer
(Technische Universität Ilmenau)

Prof. Dr.-Ing. Stefan Wesner
(Universität zu Köln)

Christian Zens
(Friedrich-Alexander-Universität Erlangen-Nürnberg)

Der Verwaltungsrat hat als ständige Gäste

eine Vertreterin der Hochschulrektorenkonferenz:
Prof. Dr. rer. nat. Ulrike Tippe
(Technische Hochschule Wildau)

einen Vertreter der Hochschulkanzlerinnen und -kanzler:
Dietmar Smyrek
(Hauptberuflicher Vizepräsident für Personal, Finanzen und Hochschulbau der Technischen Universität Braunschweig)

einen Vertreter der Kultusministerkonferenz:
Jürgen Grothe
(SMWK Dresden)

den Vorsitzenden der jeweils letzten Mitgliederversammlung:
Dr. Rainer Bockholt
(Universität Bonn)

den Vorsitzenden des ZKI:
Torsten Prill
(Freie Universität Berlin)

Vorstand
Der Vorstand des DFN-Vereins im Sinne des Gesetzes wird aus dem Vorsitzenden und den beiden stellvertretenden Vorsitzenden des Verwaltungsrates gebildet. Derzeit sind dies:

Prof. Dr.-Ing. Stefan Wesner
Vorsitz

Prof. Dr. Helmut Reiser
Stellv. Vorsitzender

Christian Zens
Stellv. Vorsitzender

Der Vorstand wird beraten vom Strategischen Beirat, einem Betriebsausschuss (BA) und einem Ausschuss für Recht und Sicherheit (ARuS).

Der Vorstand bedient sich zur Erledigung laufender Aufgaben einer Geschäftsstelle mit Standorten in Berlin und Stuttgart. Sie wird von einer Geschäftsführung geleitet. Als Geschäftsführung wurden vom Vorstand Dr. Christian Grimm und Alina Hain bestellt.

Die Mitgliedseinrichtungen

Aachen	Fachhochschule Aachen - Technik und Wirtschaft
	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH)
Aalen	Hochschule Aalen
Albstadt	Hochschule Albstadt-Sigmaringen
Amberg	Ostbayerische Technische Hochschule Amberg-Weiden
Ansbach	Hochschule für angewandte Wissenschaften, Fachhochschule Ansbach
Aschaffenburg	Technische Hochschule Aschaffenburg
Augsburg	Technische Hochschule Augsburg
	Universität Augsburg
Bad Homburg	NTT Germany AG & Co. KG
Bamberg	Otto-Friedrich-Universität Bamberg
Bayreuth	Universität Bayreuth
Berlin	Alice Salomon Hochschule Berlin
	Berlin-Brandenburgische Akademie der Wissenschaften
	Berliner Institut für Gesundheitsforschung/Berlin Institute of Health
	Berliner Hochschule für Technik (BHT)
	Bundesamt für Verbraucherschutz und Lebensmittelsicherheit
	Bundesanstalt für Materialforschung und -prüfung
	Bundesinstitut für Risikobewertung
	Deutsche Telekom AG Laboratories
	Deutsche Telekom IT GmbH
	Deutsches Institut für Normung e. V. (DIN)
	Deutsches Institut für Wirtschaftsforschung e. V. (DIW)
	European School of Management and Technology GmbH (ESMT)
	Evangelische Hochschule Berlin
	Forschungsverbund Berlin e. V.
	Freie Universität Berlin
	Helmholtz-Zentrum Berlin für Materialien und Energie GmbH
	Hertie School gGmbH
	Hochschule für Technik und Wirtschaft Berlin
	Hochschule für Wirtschaft und Recht Berlin
	Humboldt-Universität zu Berlin
	International Psychoanalytic University Berlin gGmbH
	IT-Dienstleistungszentrum Berlin
	Leibniz-Gemeinschaft e. V.
	Museum für Naturkunde – Leibniz-Institut für Evolutions- und Biodiversitätsforschung
	NOW GmbH – Nationale Organisation für den Wandel in der Mobilität
	Robert Koch-Institut
	Stanford University in Berlin
	Stiftung Deutsches Historisches Museum
	Stiftung Preußischer Kulturbesitz
	Technische Universität Berlin (TUB)
	Umweltbundesamt
	Universität der Künste Berlin
	Wissenschaftskolleg zu Berlin
	Wissenschaftszentrum Berlin für Sozialforschung gGmbH
	Zuse-Institut Berlin (ZIB)
Biberach	Hochschule Biberach
Bielefeld	Hochschule Bielefeld
	Universität Bielefeld
Bingen	Technische Hochschule Bingen
Bochum	ELFI Gesellschaft für Forschungsdienstleistungen mbH
	Evangelische Hochschule Rheinland-Westfalen-Lippe
	Hochschule Bochum
	Ruhr-Universität Bochum
	Technische Hochschule Georg Agricola
Bonn	Bundesinstitut für Arzneimittel und Medizinprodukte
	Bundesministerium des Innern
	Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit
	Deutsche Forschungsgemeinschaft
	Deutscher Akademischer Austauschdienst e. V.
	Deutsches Zentrum für Luft- und Raumfahrt e. V.
	Deutsches Zentrum für Neurodegenerative Erkrankungen e. V.
	Helmholtz-Gemeinschaft Deutscher Forschungszentren e. V.
	Rheinische Friedrich-Wilhelms-Universität Bonn
Borstel	Forschungszentrum Borstel – Leibniz Lungenzentrum
Brandenburg	Technische Hochschule Brandenburg
Braunschweig	Leibniz-Institut DSMZ – Deutsche Sammlung von Mikroorganismen und Zellkulturen GmbH
	Helmholtz-Zentrum für Infektionsforschung GmbH
	Hochschule für Bildende Künste Braunschweig
	Johann Heinrich von Thünen-Institut, Bundesforschungs-institut für Ländliche Räume, Wald und Fischerei
	Julius Kühn-Institut, Bundesforschungsinstitut für Kulturpflanzen
	Niedersächsische Landesmuseen Braunschweig
	Physikalisch-Technische Bundesanstalt
	Technische Universität Braunschweig
Bremen	Constructor University Bremen gGmbH
	Hochschule Bremen
	Hochschule für Künste Bremen
	Universität Bremen
Bremerhaven	Alfred-Wegener-Institut, Helmholtz-Zentrum für Polar- und Meeresforschung
	Hochschule Bremerhaven
Buxtehude	hochschule 21 gemeinnützige GmbH
Chemnitz	Technische Universität Chemnitz
Clausthal	Technische Universität Clausthal
Coburg	Hochschule für angewandte Wissenschaften, Fachhochschule Coburg
Cottbus	Brandenburgische Technische Universität Cottbus-Senftenberg
	Medizinische Universität Lausitz – Carl Thiem

Darmstadt	Deutsche Telekom IT GmbH
	European Space Agency (ESA)
	Evangelische Hochschule Hessen
	GSI Helmholtzzentrum für Schwerionenforschung GmbH
	Hochschule Darmstadt
	Technische Universität Darmstadt
Deggendorf	Technische Hochschule Deggendorf
Diepolz	Private Hochschule für Wirtschaft und Technik gGmbH
Dortmund	Fachhochschule Dortmund
	Technische Universität Dortmund
Dresden	Evangelische Hochschule Dresden
	Helmholtz-Zentrum Dresden-Rossendorf e. V.
	Hannah-Arendt-Institut für Totalitarismusforschung e. V.
	Hochschule für Bildende Künste Dresden
	Hochschule für Technik und Wirtschaft Dresden
	Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden e. V.
	Leibniz-Institut für Polymerforschung Dresden e. V.
	Sächsische Landesbibliothek – Staats- und Universitätsbibliothek
	Technische Universität Dresden
Dummerstorf	Forschungsinstitut für Nutztierbiologie (FBN)
Düsseldorf	Heinrich-Heine-Universität Düsseldorf
	Hochschule Düsseldorf
	Hochschul-IT-Services.nrw KöR
	Information und Technik Nordrhein-Westfalen (IT.NRW)
	Kunstakademie Düsseldorf
	Robert Schumann Hochschule Düsseldorf
Eichstätt	Katholische Universität Eichstätt-Ingolstadt
Emden	Hochschule Emden/Leer
Erfurt	Fachhochschule Erfurt
	Universität Erfurt
Erlangen	Friedrich-Alexander-Universität Erlangen-Nürnberg
Essen	Folkwang Universität der Künste
	RWI – Leibniz-Institut für Wirtschaftsforschung e. V.
	Universität Duisburg-Essen
Esslingen	Hochschule Esslingen
Flensburg	Europa-Universität Flensburg
	Hochschule Flensburg
Forchheim	Institut für Nanotechnologie und korrelative Mikroskopie gGmbH
Frankfurt/M.	Bundesamt für Kartographie und Geodäsie
	Deutsche Nationalbibliothek
	DIPF | Leibniz-Institut für Bildungsforschung und Bildungsinformation
	Frankfurt School of Finance & Management gGmbH
	Frankfurt University of Applied Sciences
	Johann Wolfgang Goethe-Universität Frankfurt am Main
	Philosophisch-Theologische Hochschule St. Georgen e. V.
	Senckenberg Gesellschaft für Naturforschung
Frankfurt/O.	IHP GmbH – Institut für innovative Mikroelektronik
	Stiftung Europa-Universität Viadrina
Freiberg	Technische Universität Bergakademie Freiberg
Freiburg	Albert-Ludwigs-Universität Freiburg
	Evangelische Hochschule Freiburg
	Katholische Hochschule Freiburg
Freising	Hochschule Weihenstephan-Triesdorf
Friedrichshafen	Zeppelin Universität gGmbH
Fulda	Hochschule Fulda
Furtwangen	Hochschule Furtwangen
Garching	European Southern Observatory (ESO)
	Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH
	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
Gatersleben	Leibniz-Institut für Pflanzengenetik und Kulturpflanzenforschung (IPK)
Geesthacht	Helmholtz-Zentrum hereon GmbH
Gelsenkirchen	Westfälische Hochschule
Gießen	Technische Hochschule Mittelhessen
	Justus-Liebig-Universität Gießen
Görlitz	Deutsches Zentrum für Astrophysik gGmbH (DZA)
Göttingen	Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GWDG)
	Verbundzentrale des Gemeinsamen Bibliotheksverbundes
Greifswald	Universität Greifswald
	Friedrich-Loeffler-Institut, Bundesforschungsinstitut für Tiergesundheit
Hagen	Fachhochschule Südwestfalen
	FernUniversität in Hagen
Halle/Saale	Agentur für Innovation in der Cybersicherheit GmbH
	Leibniz-Institut für Wirtschaftsforschung Halle e. V.
	Martin-Luther-Universität Halle-Wittenberg
	Burg Giebichenstein Kunsthochschule Halle
Hamburg	Berufliche Hochschule Hamburg (BHH)
	Bundesamt für Seeschifffahrt und Hydrographie
	Deutsches Elektronen-Synchrotron DESY
	Deutsches Klimarechenzentrum GmbH (DKRZ)
	DFN – CERT Services GmbH
	HafenCity Universität Hamburg
	Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg
	Hochschule für Angewandte Wissenschaften Hamburg
	Hochschule für bildende Künste Hamburg
	Hochschule für Musik und Theater Hamburg
	Technische Universität Hamburg
	Universität Hamburg

Hameln	Hochschule Weserbergland
Hamm	Hochschule Hamm-Lippstadt
Hannover	Bundesanstalt für Geowissenschaften und Rohstoffe
	Hochschule Hannover
	Gottfried Wilhelm Leibniz Bibliothek – Niedersächsische Landesbibliothek
	Gottfried Wilhelm Leibniz Universität Hannover
	HIS Hochschul-Informations-System eG
	Hochschule für Musik, Theater und Medien Hannover
	Landesamt für Bergbau, Energie und Geologie
	Medizinische Hochschule Hannover
	Technische Informationsbibliothek
	Stiftung Tierärztliche Hochschule Hannover
Heide	Fachhochschule Westküste
Heidelberg	Deutsches Krebsforschungszentrum (DKFZ)
	European Molecular Biology Laboratory (EMBL)
	NEC Laboratories Europe GmbH
	Universität Heidelberg
Heilbronn	Hochschule Heilbronn
	MOLIT Institut gGmbH
Hildesheim	Hochschule für angewandte Wissenschaft und Kunst Hildesheim/Holzminden/Göttingen
	Stiftung Universität Hildesheim
Hof	Hochschule für angewandte Wissenschaften Hof
Idstein	Hochschule Fresenius gemeinnützige Trägergesellschaft mbH
Ilmenau	Technische Universität Ilmenau
Ingolstadt	BayZiel - Bayerisches Zentrum für Innovative Lehre
	Technische Hochschule Ingolstadt
Jena	Ernst-Abbe-Hochschule Jena
	Friedrich-Schiller-Universität Jena
	Leibniz-Institut für Photonische Technologien e. V.
	Leibniz-Institut für Alternsforschung – Fritz-Lipmann-Institut e. V. (FLI)
Jülich	Forschungszentrum Jülich GmbH
Kaiserslautern	Hochschule Kaiserslautern
	Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau
Karlsruhe	Bundesanstalt für Wasserbau
	FIZ Karlsruhe - Leibniz-Institut für Informationsinfrastruktur GmbH
	FZI Forschungszentrum Informatik
	Hochschule Karlsruhe
	Karlshochschule International University
	Karlsruher Institut für Technologie – Universität des Landes Baden-Württemberg und nationales Forschungszentrum in der Helmholtz-Gemeinschaft (KIT)
	Staatliche Akademie der Bildenden Künste Karlsruhe
	Zentrum für Kunst und Medien Karlsruhe
Kassel	Universität Kassel
Kehl	Hochschule für öffentliche Verwaltung Kehl
Kempten	Hochschule für angewandte Wissenschaften, Fachhochschule Kempten
Kiel	Christian-Albrechts-Universität zu Kiel
	Hochschule für Angewandte Wissenschaften Kiel (HAW Kiel)
	Helmholtz-Zentrum für Ozeanforschung Kiel (GEOMAR)
	IPN Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik
	Kiel Institut für Weltwirtschaft
	ZBW – Deutsche Zentralbibliothek für Wirtschaftswissenschaften – Leibniz-Informationszentrum Wirtschaft
Koblenz	Hochschule Koblenz
Köln	Deutsche Sporthochschule Köln
	GESIS – Leibniz-Institut für Sozialwissenschaften e. V.
	Hochschulbibliothekszentrum des Landes NRW
	Katholische Hochschule Nordrhein-Westfalen
	Kunsthochschule für Medien Köln
	Rheinische Hochschule Köln gGmbH
	Technische Hochschule Köln
	Universität zu Köln
Konstanz	Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)
	Universität Konstanz
Köthen	Hochschule Anhalt
Krefeld	Hochschule Niederrhein
Kühlungsborn	Leibniz-Institut für Atmosphärenphysik e. V.
Landshut	Hochschule Landshut – Hochschule für angewandte Wissenschaften
Leipzig	Helmholtz-Zentrum für Umweltforschung GmbH – UFZ
	Hochschule für Grafik und Buchkunst Leipzig
	Hochschule für Musik und Theater „Felix Mendelssohn Bartholdy“
	Hochschule für Technik, Wirtschaft und Kultur Leipzig
	Leibniz-Institut für Troposphärenforschung e. V.
	Mitteldeutscher Rundfunk
	Universität Leipzig
Lemgo	Technische Hochschule Ostwestfalen-Lippe
Lübeck	Technische Hochschule Lübeck
	Universität zu Lübeck
Ludwigsburg	Evangelische Hochschule Ludwigsburg
Ludwigshafen	Hochschule für Wirtschaft und Gesellschaft Ludwigshafen
Lüneburg	Leuphana Universität Lüneburg
Magdeburg	Hochschule Magdeburg-Stendal
	Leibniz-Institut für Neurobiologie Magdeburg
	Universität Magdeburg
Mainz	Hochschule Mainz
	Johannes Gutenberg-Universität Mainz
	Katholische Hochschule Mainz
Mannheim	Technische Hochschule Mannheim
	Universität Mannheim
	ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung GmbH

Marbach a. N.	Deutsche Schillergesellschaft e. V. Deutsches Literaturarchiv Marbach
Marburg	Philipps-Universität Marburg
Meißen	Hochschule Meißen (FH) und Fortbildungszentrum
Merseburg	Hochschule Merseburg
Mittweida	Hochschule Mittweida
Mülheim an der Ruhr	Hochschule Ruhr West
Müncheberg	Leibniz-Zentrum für Agrarlandschaftsforschung (ZALF) e. V.
München	Bayerische Staatsbibliothek
	Hochschule für angewandte Wissenschaften München
	Hochschule für Philosophie München
	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
	Helmholtz Zentrum München Deutsches Forschungszentrum für Gesundheit und Umwelt GmbH
	ifo Institut – Leibniz-Institut für Wirtschaftsforschung e. V.
	Katholische Stiftungshochschule München
	Ludwig-Maximilians-Universität München
	Max-Planck-Gesellschaft zur Förderung der Wissenschaften e. V.
	Technische Universität München
	Universität der Bundeswehr München
Münster	FH Münster University of Applied Sciences
	Universität Münster
Neubrandenburg	Hochschule Neubrandenburg
Neuruppin	Medizinische Hochschule Brandenburg Campus gGmbH
Neu-Ulm	Hochschule für Angewandte Wissenschaften Neu-Ulm
Nordhausen	Hochschule Nordhausen
Nürnberg	Kommunikationsnetz Franken e. V.
	Technische Hochschule Nürnberg Georg Simon Ohm
	Technische Universität Nürnberg
Nürtingen	Hochschule für Wirtschaft und Umwelt Nürtingen-Geislingen
Nuthetal	Deutsches Institut für Ernährungsforschung Potsdam-Rehbrücke
Oberwolfach	Mathematisches Forschungsinstitut Oberwolfach gGmbH
Offenbach/M.	Deutscher Wetterdienst
	Hochschule für Gestaltung Offenbach
Offenburg	Hochschule Offenburg
Oldenburg	Carl von Ossietzky Universität Oldenburg
	IBS IT & Business School Oldenburg
	Landesbibliothek Oldenburg
Osnabrück	Hochschule Osnabrück
	Universität Osnabrück
Paderborn	Fachhochschule der Wirtschaft Paderborn
	Universität Paderborn
Passau	Universität Passau
Peine	Bundesgesellschaft für Endlagerung mbH (BGE)
Pforzheim	Hochschule Pforzheim – Gestaltung, Technik, Wirtschaft und Recht
Potsdam	Fachhochschule Potsdam
	Filmuniversität Babelsberg KONRAD WOLF
	GFZ Helmholtz-Zentrum für Geoforschung
	Potsdam-Institut für Klimafolgenforschung (PIK) e. V.
	Universität Potsdam
Regensburg	Ostbayerische Technische Hochschule Regensburg
	Universität Regensburg
Reutlingen	Hochschule Reutlingen
Rosenheim	Technische Hochschule Rosenheim
Rostock	Leibniz-Institut für Ostseeforschung Warnemünde
	Universität Rostock
Saarbrücken	CISPA – Helmholtz-Zentrum für Informationssicherheit gGmbH
	Universität des Saarlandes
Salzgitter	Bundesamt für Strahlenschutz
Sankt Augustin	Hochschule Bonn-Rhein-Sieg
Schenefeld	European X-Ray Free-Electron Laser Facility GmbH
Schmalkalden	Hochschule Schmalkalden
Schwäbisch Gmünd	Pädagogische Hochschule Schwäbisch Gmünd
Schwerin	Landesamt für Kultur und Denkmalpflege Mecklenburg-Vorpommern
Siegen	Universität Siegen
Speyer	Deutsche Universität für Verwaltungswissenschaften Speyer
Straelen	GasLINE Telekommunikationsnetzgesellschaft deutscher Gasversorgungsunternehmen mbH & Co. Kommanditgesellschaft
Stralsund	Hochschule Stralsund
Stuttgart	Cisco Systems GmbH
	Duale Hochschule Baden-Württemberg
	Hochschule der Medien Stuttgart
	Hochschule für Technik Stuttgart
	Universität Hohenheim
	Universität Stuttgart
Tautenburg	Thüringer Landessternwarte Tautenburg
Trier	Hochschule Trier
	Universität Trier
Tübingen	Eberhard Karls Universität Tübingen
	Stiftung "Medien in der Bildung" – Leibniz-Institut für Wissensmedien
Ulm	Technische Hochschule Ulm
	Universität Ulm
Vallendar	Vinzenz Palotti University gGmbH
Vechta	Universität Vechta
Wadern	Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH
Weimar	Bauhaus-Universität Weimar
	Hochschule für Musik FRANZ LISZT Weimar
Weingarten	Hochschule Ravensburg-Weingarten
	Pädagogische Hochschule Weingarten

Wernigerode	Hochschule Harz
Wiesbaden	Hochschule RheinMain
	Statistisches Bundesamt
Wildau	Technische Hochschule Wildau
Wilhelmshaven	Jade Hochschule Wilhelmshaven/Oldenburg/Elsfleth
Wismar	Hochschule Wismar
Witten	Private Universität Witten/Herdecke gGmbH
Wolfenbüttel	Ostfalia Hochschule für angewandte Wissenschaften
	Herzog August Bibliothek
Worms	Hochschule Worms
Wuppertal	Bergische Universität Wuppertal
Würzburg	Julius-Maximilians-Universität Würzburg
	Technische Hochschule Würzburg-Schweinfurt
	Universitätsklinikum Würzburg
Zittau	Hochschule Zittau/Görlitz
Zwickau	Westsächsische Hochschule Zwickau

DFN-Mitteilungen
bieten Hintergrundwissen zu Themen aus der Welt der Kommunikationsnetze und des DFN-Vereins

DFN-Infobrief Recht
informiert über aktuelle Entwicklungen und Fragen des Medien- und Informationsrechts

DFN-Newsletter
liefert neueste Informationen rund um das Deutsche Forschungsnetz

Podcast Forschungsstelle Recht im DFN
„Weggeforscht“ beschäftigt sich mit aktuellen juristischen Fragestellungen aus dem digitalen Umfeld

DFN auf Mastodon
trötet & teilt spannende News rund um das Deutsche Forschungsnetz

DFN auf LinkedIn
postet aktuelle Nachrichten zum Deutschen Forschungsnetz

Alle Publikationen können Sie hier abonnieren:
https://www.dfn.de/publikationen/