Hochschule Düsseldorf
University of Applied Sciences
HSD

Campus IT
Campus IT
CIT

Hochschule Düsseldorf, Münsterstraße 156, 40476 Düsseldorf

Henning Mohren
CIO und Leiter der Campus IT/
CIO and Head of the Campus IT

Münsterstraße 156
Gebäude 1a, Raum 01.1.101
40476 Düsseldorf

T +49 211 4351-9100

campus-it
@hs-duesseldorf.de
www.hs-duesseldorf.de

Betreff:
Nachvollziehbarkeit von Kommunikationsvorgängen
21.07.2026

Nachvollziehbarkeit von Kommunikationsvorgängen Leistungsumfang und Grenzen

Regelung zur Bearbeitung von Nachfragen zu Kommunikations- und Kollaborationsvorgängen durch die Campus IT

Die Campus IT der Hochschule Düsseldorf (HSD) betreibt die zentrale Kommunikations- und Kollaborations-Infrastruktur für alle Beschäftigten sowie Studierenden. Zur Gewährleistung der IT-Sicherheit, zur Abwehr von Schadsoftware und zur Aufrechterhaltung des ordnungsgemäßen Systembetriebs werden temporär Verbindungs- und Protokolldaten (Logfiles) erfasst.

Zu den Kommunikationsservices gehören u.a.:

- E-Mail
- Kalender
- Teams-Chat
- Teams-Kanäle
- Telefonie
- Crestron

Zu den Kollaborationsservices gehören u.a.:

- M365
- Teams
- SharePoint (online und on-premises)
- OneDrive
- Sciebo
- Ticketsystem
- Aufgabenverwaltung
- gemeinsame Dokumentenablagen

Die Aufzählung ist nicht abschließend und umfasst sämtliche, ggf. auch nicht explizit benannte und durch die Campus IT betriebenen Kommunikations- und Kollaborationsservices.
Aufgrund datenschutzrechtlicher Vorgaben sowie weiterer kommunikationsbezogener Schutzrechte bedarf jede Einsichtnahme, Analyse oder Auswertung dieser Protokoll- und Nutzungsdaten einer klaren Rechtsgrundlage und eines standardisierten, transparenten Verfahrens. Dieses Verfahren wurde für die gesamte Kommunikations- und Kollaborations-Infrastruktur entsprechend der Vorgaben des DISM-Prozesses an der HSD festgelegt und dort dokumentiert.
Dieses Dokument beschreibt den Leistungsumfang der Campus IT bei Anfragen zur Nachvollziehbarkeit von Kommunikations- und Kollaborationsvorgängen sowie die hierfür geltenden Zuständigkeiten und Rahmenbedingungen.

Grundsatz

Die Campus IT gewährleistet den ordnungsgemäßen Betrieb der Kommunikations- und Kollaborationsservices der Hochschule. Die Rekonstruktion individueller Kommunikationsvorgänge gehört grundsätzlich nicht zum Leistungsumfang der Services. Ein Anspruch auf Nachverfolgung einzelner Kommunikations- oder Kollaborationsvorgänge besteht nicht.
Die Campus IT speichert keine Kommunikationsdaten mit dem Ziel einer späteren Rekonstruktion individueller Kommunikationsvorgänge. Protokollierungen erfolgen ausschließlich zum Betrieb der Services, zur Gewährleistung der Informationssicherheit sowie zur Fehleranalyse.
Im Rahmen jedwedes Auskunftsersuchen nimmt die Campus IT als Betreiberin der technischen Infrastruktur keine Entscheidungen über rechtliche, disziplinarische, prüfungsrechtliche oder arbeitsrechtliche Fragestellungen vor.
Im Zweifel hat der Schutz der Vertraulichkeit von Kommunikations- und Kollaborationsvorgängen Vorrang vor dem Interesse an der Rekonstruktion individueller Vorgänge.

Ziel des Dokuments

Das Dokument stellt die Rahmenbedingungen für Nachforschungen anhand von Betriebs-, Verbindungs- und Protokolldaten dar.
Zugriffe auf Inhaltsdaten von Kommunikations- oder Kollaborationsservices sind grundsätzlich ausgeschlossen und bedürfen einer gesonderten rechtlichen Prüfung.

Kategorisierung der Anfragen:

Kategorie	Definition/ Beispiel	Zulässigkeit/ Regelung
A: Systemstörungen & IT-Sicherheit	Serverausfall, aktive Phishing-Welle, Spam-Abwehr, begründeter Verdacht auf kompromittierte Konten.	**Zulässig**. Fällt in den regulären Betrieb und die gesetzliche Pflicht zur Gewährleistung der IT-Sicherheit.
B: Individuelle Nachforschung (Nutzer selbst)	Beschäftigte/ Studierende vermissen eine bestimmte Nachricht, Datei oder einen anderen Kommunikations- bzw. Kollaborationsvorgang	**Nicht Bestandteil des Regelservices**. Individuelle Nachforschungen zu einzelnen Kommunikationsvorgängen sind grundsätzlich nicht Bestandteil des Serviceangebots. Die Campus IT prüft grundsätzlich lediglich die Betriebsfähigkeit des betroffenen Kommunikations- oder Kollaborationsservice im fraglichen Zeitraum. Dabei wird insbesondere festgestellt, • ob Störungen oder Einschränkungen des Service bekannt waren, • ob technische Vorfälle dokumentiert wurden, • ob Hinweise auf einen systemischen Fehler vorliegen. Die Campus IT beantwortet damit ausschließlich die Frage, ob im fraglichen Zeitraum Hinweise auf eine technische Beeinträchtigung des betroffenen Service‘ vorlagen.
C: Nachweise für Verwaltungsverfahren	Verwaltungs-, Prüfungs-, Disziplinar- oder Rechtsverfahren	**Nur über offiziellen Dienstweg**. Keine direkte Auskunft an Studierende oder Sachbearbeiter ohne formalisierte Anforderung der zuständigen Stelle und Einbeziehung der Datenschutzbeauftragten sowie der Rechtsabteilung.
D: Verhaltens- und Leistungskontrolle	Prüfung von Kommunikations- oder Kollaborationsaktivitäten, Antwortzeiten, Dokumentenzugriffen oder vergleichbaren Nutzungsmerkmalen von Beschäftigten	**Strikt unzulässig**. Eine Nutzung der System-Logs zu Zwecken der Verhaltens- oder Leistungskontrolle ist ausgeschlossen.
E: Forschung, Statistik, Audit	Nutzungszahlen, Kapazitätsplanung, Sicherheitsanalysen	**Zulässig**. Auswertungen erfolgen ausschließlich aggregiert und anonymisiert bzw. pseudonymisiert; keine personenbezogene Auswertung

Rechtliche Grundlagen und Rahmenbedingungen (Auszug)

- **Fernmeldegeheimnis (TDDDG)**: Die Auswertung von Kommunikations- und Protokolldaten berührt datenschutzrechtliche und telekommunikationsrechtliche Schutzrechte der Betroffenen. Deshalb erfolgen Einsichtnahmen und Auswertungen ausschließlich auf Grundlage eines dokumentierten und rechtlich zulässigen Verfahrens.
- **Datenschutz (DSGVO & DSG NRW)**: Protokolldaten sind personenbezogene Daten. Sie unterliegen einer strengen Zweckbindung (IT-Sicherheit und Systemerhalt) und dürfen nicht zweckentfremdet ausgewertet werden.
- **Verhaltens- und Leistungskontrolle (LPVG NRW)**: Maßnahmen, die eine Überwachung des Verhaltens oder der Leistung von Beschäftigten ermöglichen, unterliegen der Mitbestimmung des Personalrats.

Technische Schutzmaßnahmen & Speicherfristen

Um das Risiko eines unberechtigten Datenzugriffs zu minimieren, gelten folgende systemseitige Vorgaben:

1. **Verbindungsprotokolle**: Verbindungsprotokolle werden entsprechend der jeweils gültigen technischen Betriebs- und Löschkonzepte gespeichert und anschließend automatisiert gelöscht. Nach Ablauf der Aufbewahrungsfrist stehen entsprechende technische Informationen für eine Bewertung der Betriebsfähigkeit nicht mehr zur Verfügung.
2. **Inhaltsprotokollierung**: Es findet keine standardmäßige Protokollierung oder gesonderte Speicherung von Inhaltsdaten aus Kommunikations- oder Kollaborationsservices außerhalb der jeweiligen Produktivsysteme statt.
3. **Berechtigungskonzept**: Der Zugriff auf Betriebs-, Verbindungs- und Sicherheitsprotokolle ist auf eine namentlich definierte Gruppe autorisierter Administratorinnen und Administratoren beschränkt. Jeder administrative Zugriff auf Log-Dateien wird systemseitig revisionssicher protokolliert.

Sonderverfahren für formalisierte Anfragen (Kategorie C)

Behauptet eine Person, einen fristrelevanten Kommunikations- oder Kollaborationsvorgang durchgeführt zu haben, dessen Eingang oder Vorliegen von einer Hochschulstelle bestritten wird, gilt folgendes Verfahren:

1. Die Campus IT trifft keine Aussage zur rechtlichen Bewertung von Zugang, Fristwahrung oder Wirksamkeit elektronischer Erklärungen.
2. Direkte Nachforschungsanfragen an die Campus IT werden grundsätzlich abgelehnt.
3. Eine Überprüfung vorhandener Betriebs-, Verbindungs- und Protokolldaten erfolgt ausschließlich auf schriftliche Anforderung der zuständigen Stelle (z.B. Dezernat für Studium und

Lehre) oder eines Prüfungsausschusses im Rahmen offizieller Verwaltungsverfahren.

4. Die Anfrage muss innerhalb der jeweils geltenden technischen Aufbewahrungsfristen eingehen. Nach Ablauf der Frist kann seitens der Campus IT lediglich eine allgemeine Aussage über die Systemverfügbarkeit zum fraglichen Zeitpunkt getroffen werden.

Henning Mohren
CIO und Leiter Campus IT