Hochschule für Schauspielkunst
Ernst Busch

Busch – Blatt
5 / 2026

vom 13. Juli 2026

Herausgegeben

im Auftrag der Präsidentin
der Hochschule für Schauspielkunst Ernst Busch Berlin

Zinnowitzer Straße 11
10115 Berlin
Telefon: 030/75 54 17 - 0
Telefax: 030/75 54 17 - 175

Inhalt:

Dienstvereinbarung über digitale Telefonie

an der Hochschule für Schauspielkunst Ernst Busch Berlin (HfS)

Präambel

Die Hochschule für Schauspielkunst Ernst Busch Berlin nutzt zur dienstlichen Kommunikation digitale Telefonie einschließlich app-basierter Kommunikationsfunktionen. Der technische Betrieb erfolgt durch das Service-Center IT (SC-IT) als gemeinsame Einrichtung der Hochschule für Musik Hanns Eisler Berlin, der Hochschule für Schauspielkunst Ernst Busch Berlin und der Weißensee Kunsthochschule Berlin. Die Vertragsparteien verfolgen das Ziel, die Nutzung der digitalen Telefonie datenschutzgerecht, transparent und beschäftigtenfreundlich zu gestalten sowie den Anforderungen der modernen Arbeitswelt gerecht zu werden. Gleichzeitig soll ein sicherer und effizienter Betrieb der Systeme gewährleistet werden. Die digitale Telefonie dient der Kommunikation und Zusammenarbeit. Sie darf nicht zur Leistungs- oder Verhaltenskontrolle von Beschäftigten eingesetzt werden. Um die damit einhergehenden Fragen einvernehmlich zu regeln, schließen die Hochschule und der Personalrat folgende Dienstvereinbarung über digitale Telefonie ab.

§ 1 Gegenstand und Geltungsbereich

(1) Diese Dienstvereinbarung regelt die Einführung und Nutzung der digitalen Telefonie einschließlich mobiler und app-basierter Kommunikationsfunktionen.

(2) Sie gilt für alle Beschäftigten der Hochschule, soweit sie vom Personalrat vertreten werden.

(3) Der technische Betrieb erfolgt durch das SC-IT. Die datenschutzrechtlichen und personalvertretungsrechtlichen Verantwortlichkeiten der Hochschule bleiben hiervon unberührt.

§ 2 Grundsätze der Datenverarbeitung

(1) Es dürfen ausschließlich diejenigen personenbezogenen Daten verarbeitet werden, die für

- die Bereitstellung der Dienste,
- die Durchführung der Kommunikation,
- die IT-Sicherheit,
- die Administration,
- die Fehleranalyse sowie
- die Erfüllung gesetzlicher Verpflichtungen

erforderlich sind.

(2) Art und Umfang der verarbeiteten Daten werden in einer gesonderten technischen Dokumentation beschrieben und der Hochschulleitung und dem Personalrat zugänglich gemacht.

(3) Die Verarbeitung erfolgt nach den Grundsätzen der Erforderlichkeit, Zweckbindung und Datenminimierung.

§ 3 Schutz vor Leistungs- und Verhaltenskontrolle

(1) Die mit dem System erhobenen Daten dürfen weder unmittelbar noch mittelbar zur Leistungs- oder Verhaltenskontrolle von Beschäftigten verwendet werden.

(2) Insbesondere dürfen Verbindungs-, Status-, Diagnose- oder Protokolldaten nicht zur Erstellung von Leistungsprofilen, Anwesenheitsprofilen oder Verhaltensbewertungen genutzt werden.

(3) Eine automatisierte Bewertung von Beschäftigten findet nicht statt.

§ 4 Erreichbarkeit und Arbeitszeit

(1) Eine Verpflichtung zur dienstlichen Erreichbarkeit besteht ausschließlich im Rahmen der jeweils geltenden Arbeitszeitregelungen.

(2) Außerhalb der Arbeitszeit besteht keine Verpflichtung zur Nutzung der Anwendung oder zur Reaktion auf eingehende Nachrichten oder Anrufe.

(3) Arbeitszeitrechtliche Vorschriften, insbesondere zu Ruhezeiten, bleiben unberührt.

(4) Die Beschäftigten können die Statusanzeige in der Anwendung individuell einstellen. Die Nutzung der Statusanzeige ist ausschließlich freiwillig. Hieraus dürfen den Beschäftigten keine Nachteile entstehen.

§ 5 Nutzung privater Endgeräte

(1) Die Nutzung privater Endgeräte für dienstliche Zwecke erfolgt freiwillig.

(2) Beschäftigten dürfen aus der Ablehnung oder Beendigung einer solchen Nutzung keine Nachteile entstehen.

(3) Ein Zugriff auf private Inhalte der Geräte ist unzulässig.

(4) Für Schäden, die durch eine dienstliche Nutzung der App auf privaten Endgeräten entstehen, gelten die gesetzlichen und tariflichen Grundsätze; ein pauschaler Haftungsausschluss des Dienstgebers ist ausgeschlossen.

(5) Entstehen im Zusammenhang mit einer zugelassenen dienstlichen Nutzung der Anwendung auf privaten Geräten Kosten, bspw. im Zuge einer Auslands-Dienstreise, sind diese nach den geltenden Regelungen zu erstatten oder in anderer geeigneter Weise auszugleichen.

(6) Bei Beendigung der dienstlichen Nutzung oder des Arbeitsverhältnisses sind die dienstlichen Anwendungsdaten von privaten Endgeräten zu entfernen und die App ist zu deinstallieren.

§ 6 IT-Sicherheit und Systembetrieb

(1) Das SC-IT trifft die erforderlichen technischen und organisatorischen Maßnahmen zum sicheren Betrieb des Systems auf den Anlagen, die in der Hochschule betrieben werden und den Dienstgeräten, die vollständig vom SC-IT administriert werden.

(2) Administrations- und Sonderrechte werden dokumentiert und auf das erforderliche Maß beschränkt.

(3) Sicherheitsrelevante Protokollierungen sind nur zulässig, soweit sie für Betrieb, Fehleranalyse und IT-Sicherheit erforderlich sind.

(4) Private Geräte, auf denen die App genutzt wird, sind durch die Nutzenden sicherheitstechnisch auf einem aktuellen Stand zu halten.

§ 7 Auswertungen in Ausnahmefällen

(1) Personenbezogene Auswertungen sind nur zulässig

- zur Aufklärung konkreter Sicherheitsvorfälle,
- zur Abwehr erheblicher Gefahren für den IT-Betrieb,
- bei konkretem Verdacht eines schwerwiegenden Missbrauchs der digitalen Telefonie oder
- aufgrund gesetzlicher Verpflichtungen.

(2) Anlass, Umfang und Ergebnis einer solchen Auswertung sind zu dokumentieren.

(3) Der Personalrat wird unter Beachtung der gesetzlichen Vorgaben beteiligt.

(4) Inhaltsdaten von Gesprächen oder Nachrichten werden nicht ausgewertet.

§ 8 Löschung, Speicherfristen und Mittschnittverbot

(1) Personenbezogene Daten werden gelöscht, sobald sie für ihren Zweck nicht mehr erforderlich sind.

(2) Die konkreten Speicher- und Löschfristen werden in einem Löschkonzept dokumentiert.

(3) Das Löschkonzept wird dem Personalrat zur Verfügung gestellt.

(4) Gesprächs- oder Videomitschnitte sind unzulässig.

§ 9 Beteiligung des Personalrats

(1) Der Personalrat wird rechtzeitig über wesentliche Änderungen oder wesentliche Erweiterungen des Systems, die das SC-IT vornimmt oder die dem SC-IT bekannt werden, informiert.

(2) Die gesetzlichen Mitbestimmungsrechte des Personalrats bleiben unberührt.

(3) Der Personalrat erhält Zugang zu den für die Wahrnehmung seiner Aufgaben erforderlichen Unterlagen, insbesondere in

- Rollen- und Berechtigungskonzepte,
- Löschkonzepte,
- Datenschutzdokumentationen,
- Beschreibungen wesentlicher Funktionen (Handbücher oder Vergleichbares).

§ 10 Schlussbestimmungen

(1) Gesetzliche, tarifliche und datenschutzrechtliche Bestimmungen bleiben unberührt.

(2) Sollten einzelne Bestimmungen dieser Dienstvereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, unverzüglich eine wirksame Regelung zu vereinbaren, die dem Schutzzweck der unwirksamen Regelung möglichst nahekommt.

(3) Diese Dienstvereinbarung wird auf unbestimmte Zeit geschlossen; sie tritt mit Inbetriebnahme des Systems in Kraft und ersetzt bislang bestehende Dienstvereinbarungen oder Regelungen zur Telefonie. Sie gilt bis zum Abschluss einer neuen Dienstvereinbarung fort. Die Dienstvereinbarung kann jederzeit im beiderseitigen Einvernehmen geändert werden; sie kann mit einer Frist von sechs Wochen zum Jahresende gekündigt werden.

(4) Folgende Anlagen sind Bestandteile der Dienstvereinbarung. Anlage 2 und 4 können seitens der Hochschule fortgeschrieben werden, solange dadurch keine neuen personenbezogenen Daten verarbeitet oder neue Auswertungsmöglichkeiten geschaffen werden.

- Anlage 1 – Verarbeitete Datenkategorien
- Anlage 2 – Rollen- und Berechtigungskonzept
- Anlage 3 – Lösch- und Speicherfristen
- Anlage 4 – Technische und organisatorische Maßnahmen im SC-IT (TOM)

Berlin, 09.07.2026

gez. Dr. Anna Luise Kiss	gez. Christiane Linsel	gez. Sebastian Auerbach
Präsidentin	Kanzlerin	Vorsitzender des Personalrats

Anlage 1

Verarbeitete Datenkategorien

Im Rahmen der digitalen Telefonie dürfen ausschließlich die nachfolgend aufgeführten personenbezogenen Daten verarbeitet werden, soweit dies für die jeweiligen Zwecke erforderlich ist.

Stammdaten (werden aus Verzeichnisdienst im SC-IT übertragen)

- Vor- und Nachname
- persönliche dienstliche E-Mailadresse
- dienstliche Rufnummer
- organisatorische Zuordnung (Organisationseinheit)
- Anschrift der Organisation
- Position/Information zur beruflichen Funktion
- Benutzerkennung (E-Mailadresse = Benutzername, Passwort)

Kommunikationsdaten

- Zeitpunkt eines Anrufes
- Dauer eines Anrufes
- beteiligte Rufnummern bzw. Teilnehmerkennungen
- Zeitpunkt der Zustellung von Nachrichten
- technische Zustellinformationen

Statusdaten

- Verfügbarkeitsstatus (wird durch die Beschäftigten gesetzt)
- Anmeldezustand der Anwendung

Technische Daten

- Gerätekennung
- Betriebssystemversion
- Versionsstand der Anwendung
- technische Fehler- und Diagnosedaten

Administrationsdaten

- Rollen und Berechtigungen
- Änderungs- und Administrationsprotokolle

Nicht zulässig

Nicht verarbeitet oder ausgewertet werden dürfen insbesondere:

- Gesprächsinhalte
- Inhalte von Nachrichten
- Audioaufzeichnungen
- Videoaufzeichnungen
- Bewegungs- oder Standortprofile
- Leistungs- oder Verhaltensprofile

Soweit technische Funktionen solche Daten erzeugen können, sind sie zu deaktivieren oder organisatorisch von einer Nutzung auszuschließen. Die Anwendung erfolgt nicht zur Arbeitszeiterfassung. Arbeitszeiten werden ausschließlich in den dafür vorgesehenen Systemen dokumentiert.

Anlage 2

Rollen- und Berechtigungskonzept

Grundsatz

Berechtigungen werden ausschließlich nach dem Erforderlichkeitsprinzip vergeben. Jede Person erhält nur die Rechte, die zur Erfüllung ihrer dienstlichen Aufgaben erforderlich sind.

Rollen/Berechtigungen

Nutzende Beschäftigte:

- Führen und Empfangen von Anrufen
- Nutzung freigegebener Kommunikationsfunktionen
- Verwaltung persönlicher Einstellungen

Lokale Telefonanlagen Systemadministration (SC-IT, NTT):

- Benutzer*innenverwaltung (SC-IT)
- Zuordnung von Rufnummern (SC-IT)
- Verwaltung organisatorischer Einstellungen
- kein Zugriff auf Gesprächsinhalte oder Nachrichteninhalte
- technischer Betrieb
- Fehleranalyse
- Sicherheitsmaßnahmen
- Systempflege

Rainbow Administration (SC-IT):

- Benutzer*innenverwaltung
- Zuordnung von Rufnummern
- Verwaltung organisatorischer Einstellungen
- kein Zugriff auf Gesprächsinhalte oder Nachrichteninhalte

Rainbow Systemadministration (NTT, Alcatel-Lucent):

- kein Zugriff auf Gesprächsinhalte oder Nachrichteninhalte
- technischer Betrieb (Alcatel-Lucent)
- Fehleranalyse
- Sicherheitsmaßnahmen
- Systempflege (Alcatel-Lucent)

Zugriffe erfolgen ausschließlich im erforderlichen Umfang durch NTT nach Freigabe durch das SC-IT.

Dokumentation

Administrationsrechte sind zu dokumentieren. Berechtigungen werden mindestens einmal jährlich durch das SC-IT überprüft. Nicht mehr benötigte Rechte sind unverzüglich zu entziehen.

Anlage 3

Lösch- und Speicherkonzept

Kommunikationsdaten: Verbindungsdaten werden nur so lange gespeichert, wie dies für den sicheren Betrieb, die Fehleranalyse oder gesetzliche Verpflichtungen erforderlich ist.

Regelfrist: 6 Monate (https://www.ismslite.de/blog/loeschkonzept-dsgvo - Löschklasse 7).

- Lokale Telefonanlage – 1 Jahr
- Rainbow – 1 Jahr

Sicherheitsprotokolle: Sicherheits- und Fehlerprotokolle werden grundsätzlich nach 6 Monaten (https://www.ismslite.de/blog/loeschkonzept-dsgvo - Löschklasse 7) gelöscht. Soweit sie für die Bearbeitung eines laufenden Sicherheitsvorfalls benötigt werden, können sie bis zum Abschluss des Vorgangs aufbewahrt werden.

- Lokale Telefonanlage – 1 Jahr
- Rainbow – 1 Jahr

Administrationsprotokolle: Administrations- und Zugriffsprotokolle werden nach sechs Monaten gelöscht (https://www.ismslite.de/blog/loeschkonzept-dsgvo - Löschklasse 7).

- Lokale Telefonanlage – 1 Jahr
- Rainbow – 1 Jahr

Benutzerkonten: Bei Ausscheiden von Beschäftigten werden Benutzerkonten deaktiviert. Nicht mehr benötigte personenbezogene Daten werden entsprechend den gesetzlichen Vorgaben gelöscht.

- Lokale Telefonanlage – Auf Anforderung, werden Personennamen aus TK-Anlage entfernt.
- Rainbow – 10 Tage (erst Deaktivierung und dann Löschung)

Regelmäßige Überprüfung

Das Löschkonzept wird mindestens einmal jährlich durch das SC-IT überprüft und bei Bedarf angepasst. Der Personalrat wird über wesentliche Änderungen informiert.

Anlage 4

Technische und organisatorische Maßnahmen im SC-IT (TOM)

Zur Gewährleistung der Sicherheit der Verarbeitung werden insbesondere folgende Maßnahmen umgesetzt:

Zugriffsschutz

- personengebundene Benutzerkonten
- passwortgestützte Authentifizierungsverfahren
- rollenbasierte Berechtigungsvergabe

Datensicherheit

- verschlüsselte Datenübertragung
- regelmäßige Sicherheitsupdates
- regelmäßige Anwendungsupdates

Betriebssicherheit

- regelmäßige Datensicherungen der Server und Dateien (NICHT Client)
- Notfall- und Wiederanlaufverfahren
- Überwachung der Systemverfügbarkeit

Datenschutz

- Protokollierung aller Zugriffe
- regelmäßige Überprüfung von Berechtigungen
- Umsetzung des Grundsatzes der Datensparsamkeit

Organisation

Das SC-IT dokumentiert die technischen und organisatorischen Maßnahmen und aktualisiert diese bei wesentlichen technischen Änderungen.

Der Personalrat kann Einsicht in die jeweils aktuelle Dokumentation nehmen, soweit dies zur Wahrnehmung seiner gesetzlichen Aufgaben erforderlich ist.