Betriebsvereinbarung

betreffend

der Verarbeitung personenbezogener Arbeitnehmer_innen-Daten in IT-Anwendungen (kurz BV-IT)

abgeschlossen zwischen der

Akademie der bildenden Künste Wien
als Arbeitgeberin
vertreten durch
Rektor Dr. Johan F. Hartle

in der Folge kurz „Akademie" genannt,

sowie dem

Betriebsrat für das künstlerisch-wissenschaftliche Personal der Akademie der bildenden Künste Wien
vertreten durch die
Betriebsratsvorsitzende Dr^{in} Ruby Jana Sircar

und dem

Betriebsrat für das allgemeine Universitätspersonal der Akademie der bildenden Künste Wien
vertreten durch die
Betriebsratsvorsitzende Amtsrätin Dunja Reithner

beide gemeinsam in der Folge „Betriebsräte" genannt,

andererseits.

Inhalt

I. Allgemeines

1. Die Akademie setzt verschiedene automationsunterstützte IT-Anwendungen ein, mit Hilfe derer personenbezogene Daten von Arbeitnehmer_innen verarbeitet werden. Darunter fallen Systeme, die in hohem Umfang zur Optimierung der damit verbundenen Aktivitäten beitragen sollen und für die tägliche Arbeit unverzichtbar sind.

2. Die verwendeten IT-Systeme und IT-Anwendungen werden von der Akademie ausschließlich zur effizienten Abwicklung der Aufgaben, zur für den Betrieb notwendigen Arbeiten, zur Gewährleistung der Datensicherheit sowie zur internen und externen Datenkommunikation eingesetzt.

3. Die Akademie und die Betriebsräte stimmen darin überein, dass die von der Akademie eingesetzten Systeme für die jeweiligen Zwecke, insbesondere für eine effiziente Administration sowie für die Gewährleistung einer zeitgemäßen internen und externen Kommunikation notwendig sind. Einigkeit besteht auch dahingehend, dass elektronische Systeme aufgrund der rasant fortschreitenden technologischen Entwicklung ständig einem hohen Anpassungs- und Aktualisierungsbedarf unterliegen und dass die Akademie daher veranlasst ist, diesem dynamischen Wandel entsprechend Rechnung zu tragen.

4. Die Akademie erklärt, dass sie personenbezogenen Arbeitnehmer_innen-Daten nur im gesetzlich vorgeschriebenen und/oder betrieblich unbedingt notwendigen Ausmaß verarbeitet und/oder an Dritte übermittelt werden. Die Akademie verpflichtet sich zur äußerst sparsamen Verarbeitung und strikten Zweckbindung vorhandener personenbezogener Daten und zu einer Aufbewahrung bzw. Löschung aller Daten entsprechend der gesetzlichen Vorgaben und Fristen. Neben gesetzlichen Regelungen gelten die internen Vorgaben zur Aufbewahrung und Löschung (z.B. Archivierungsrichtlinie).

5. Die Betriebsvereinbarungsparteien halten fest, dass es der Akademie im Zusammenhang mit der Verarbeitung von personenbezogenen Arbeitnehmer_innen-Daten untersagt ist, diese für eine systematische, die Menschenwürde des Einzelnen berührende Kontrolle zu verwenden, unberechtigte Leistungs- und Verhaltenskontrollen durchzuführen, personenbezogene Profilings zu erstellen sowie personenbezogene Arbeitnehmer_innen-Daten unberechtigt zu speichern, zu übermitteln oder offen zu legen. Personenbezogene Auswertungen von Arbeitnehmer_innen-Daten sind nur im Rahmen der in dieser Betriebsvereinbarung bzw. darauf basierender Regelungen (Zusatz-Betriebsvereinbarungen) festgelegten Grundsätze zulässig.

II. Zielsetzung

1. Die Akademie als Arbeitgeberin ist datenschutzrechtlich verantwortlich und damit verpflichtet, die IT-Infrastruktur gegen Cyber-Angriffe zu schützen. Darüber hinaus sind aufgrund der rechtlichen Bestimmungen der Datenschutz-Grundverordnung (DSGVO) technische und organisatorische Maßnahmen (TOMs) zur Sicherheit der Verarbeitung zu treffen.

2. Mit dieser Betriebsvereinbarung soll sichergestellt werden, dass Arbeitnehmer_innen der Akademie vor einer technisch möglichen Überwachung ihrer Leistung und/oder ihres Verhaltens geschützt sind. Ziel ist dabei die Nachvollziehbarkeit und Überprüfung der personenbezogenen Verwaltung von Arbeitnehmer_innen für alle gegenwärtigen und in Zukunft verwendeten IT-Systeme und IT-Anwendungen zu ermöglichen und den Betriebsräten die ihnen gemäß der gesetzlichen Grundlagen zustehenden Rechte zu sichern.

3. Die Akademie und die Betriebsräte sind sich darüber einig, dass diese Betriebsvereinbarung dazu dient, die Umsetzung von rechtlichen Bestimmungen zur Verhinderung von Datenmissbrauch zu unterstützen.

4. Zum Schutz der lokal oder auf Cloudplattformen verarbeiteten Daten und Dokumente sind seitens der Akademie entsprechende Maßnahmen zu ergreifen. Daher werden zu diesem Zweck technische Systeme sowie Netzwerkanalysen zur IT-Datensicherheit eingesetzt (siehe Punkt X). Darüber hinaus werden Regelungen erlassen (Sicherheitsrichtlinie) und Schulungen umgesetzt, die den sorgsamen Umgang mit Daten sicherstellen sollen.

III. Geltungsbereich

1. Diese Betriebsvereinbarung regelt

a) die Einführung und Nutzung von Systemen und Anwendungen sowie die IT- und Datensicherheit
b) die Verarbeitung von personenbezogenen Daten der Arbeitnehmer_innen der Akademie.

Demnach regelt diese Betriebsvereinbarung sowohl die von der Akademie zur Verfügung gestellten Informations- und Kommunikationstechnologien wie z.B. Server, Netzwerkkomponenten, IT-Endgeräte, Internetzugang, Multifunktionsgeräte, elektronische Schließsysteme, samt der der damit in Zusammenhang stehenden Akademie-Dienste wie E-Mail, Laufwerke, Telefonie, Software as a Service, Cloudanbindungen, Big Data-Anwendungen und dergleichen sowie die damit allenfalls einhergehenden Kontrollen

als auch

die Verwendung von personenbezogenen Arbeitnehmer_innen-Daten in den bestehenden und zukünftigen IT-Anwendungen der Akademie wie sie gemäß Punkt VII.1 und im Verarbeitungsverzeichnis nach Art 30 DSGVO zu dokumentieren sind.

2. Alle gegenwärtigen und zukünftig vereinbarten IT-Anwendungen und IT-Systeme werden aus Gründen der Transparenz im Anhang wie folgt beschrieben:

- Anhang A: Übersicht der IT-Anwendungen und IT-Systeme, die personenbezogene Arbeitnehmer_innendaten verarbeiten und für die die Regelungen dieser BV-IT ausreichend sind.
- Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.
- Anhang C: IT-Anwendungen und IT-Systeme, die durch eine Zusatz-Betriebsvereinbarung geregelt sind.

3. Diese Betriebsvereinbarung gilt für alle Arbeitnehmer_innen, also sinngemäß auch für jene Beschäftigten an der Akademie, die nicht dem Kollektivvertag für Arbeitnehmerinnen und Arbeitnehmer der Universitäten (Uni-KV) unterliegen (z.B. Beamt_innen und Vertragsbedienstete) in Bezug auf die Verarbeitung von personenbezogenen Daten der Arbeitnehmer_innen.

4. Die Betriebsvereinbarung tritt am 13.07.2026 in Kraft und tritt an die Stelle der bisherigen Rahmenbetriebsvereinbarung betreffend automationsunterstützte Verwendung personenbezogener ArbeitnehmerInnendaten vom 02.04.2009. Sie gilt vorerst für achtzehn Monate. Während dieser Zeit besteht eine Phase der beiderseitigen Prüfung ihrer praktikablen Anwendbarkeit, binnen derer – über Wunsch einer Vertragsseite – auch ergänzende Gespräche mit dem Ziel einer einvernehmlichen Abänderung geführt werden

können. Sollte bis drei Monate vor Ablauf der achtzehnmonatigen Befristung keine Vertragsseite gegenüber der anderen Partei ausdrücklich und schriftlich (maßgeblich für die Rechtzeitigkeit ist, wie für alle der Schriftform bedürftigen Veranlassungen gemäß dieser Betriebsvereinbarung, das Einlangen bei der anderen Partei, wobei auch Übermittlung per E-Mail akzeptiert wird) auf einem Auslaufen der Betriebsvereinbarung mit Fristende bestehen, so verlängert sich diese Betriebsvereinbarung befristet um jeweils 24 Monate unter Beibehaltung des vorbeschriebenen Procederes für eine allfällige Nichtverlängerungserklärung. Weiters kann die Betriebsvereinbarung im Einvernehmen jederzeit, insbesondere nach erfolgter Evaluierung, geändert werden.

5. Mit Inkrafttreten dieser Betriebsvereinbarung tritt folgende Rahmenbetriebsvereinbarung einschließlich dazu abgeschlossener Zusatzdokumente vollinhaltlich außer Kraft:

- Rahmenbetriebsvereinbarung betreffend automationsunterstützte Verwendung personenbezogener ArbeitnehmerInnendaten

IV. Definitionen

Folgende Definitionen finden in dieser Betriebsvereinbarung Anwendung.

a. Daten werden nach der Daten-Governance-Verordnung der EU als „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen und Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material" beschrieben.
b. Personenbezogene Daten sind nach Art 4 Z 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."
c. Datenkategorisierung meint die Festlegung der berechtigten Datenverarbeitung entlang folgender Kategorien:
   Kategorie A: allgemeine Daten zur Person der_des Arbeitnehmer_in (Stammdaten). Diese Daten stehen zwar mit den einzelnen Arbeitnehmer_innen in Verbindung, gehören aber zu den notwendigen betrieblichen Kommunikationsdaten (Beispiele: Name, Organisationseinheit, Dienstadresse, Büroraum, dienstliche Nummer, E-Mail-Adresse, Benutzer_innen-Kennung, Berechtigungsrolle).
   Kategorie B: alle Daten, die im Zusammenhang mit der Abwicklung des Arbeitsverhältnisses stehen (Abwicklungsdaten) (Beispiele: Anwesenheiten, Abwesenheiten, notwendige Qualifikation, Privatadresse, private Telefonnummern).
   Kategorie C: umfasst besondere Kategorien personenbezogener Daten („sensible Daten"), d.h. alle Daten über die Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben sowie biometrische Daten (Art 4 Z 14 DSGVO) und genetische Daten (Art 9 DSGVO) und Daten über strafrechtliche Verurteilungen und Straftaten (Art 10 DSGVO).
   Kategorie D: alle Daten im Sinne von Geo-/Lokationsdaten, die Informationen zum aktuellen Standort von Arbeitnehmer_innen enthalten (Beispiele: Mobile Device Management-Systeme oder GPS-Trackingsysteme)
   Kategorie E: Bild-/Audiodateien, die Daten, die Bild-, Ton- oder Videoaufzeichnungen von Arbeitnehmer_innen enthalten (Beispiele: Lichtbilder, Telefon- oder

Videokonferenzen Live und Aufzeichnungen)
Kategorie F: Protokolldaten, im Sinne von Zugriffsdaten (z.B. Login-/Logoutdaten), Verkehrsdaten (z.B. Verbindungsdaten), Diagnosedaten und Auditdaten. Auditdaten sind Daten, die Zugriffe der Systemadministrator_innen auf personenbezogene Daten der Arbeitnehmer_innen dokumentieren.
Kategorie G: umfasst als Inhaltsdaten alle Inhalte, die von Arbeitnehmer_innen erzeugt werden. (Beispiele: Inhalte von E-Mail-Nachrichten, erstellte Dokumente, Chat-Nachrichten etc.)

d. Datenverarbeitung bezieht sich auf jede Verarbeitung von Daten im Sinne des Art 4 Z 2 DSGVO mit Ausnahme der Auswertungen. Für Auswertungen gelten die Bestimmungen des Punkts V.
e. IT-Anwendungen sind elektronische Datenverarbeitungssysteme, Programme und Applikationen, die im Verantwortungsbereich der Akademie als Arbeitsgeberin sind, in denen Daten automatisiert und nicht-automatisiert und unabhängig vom Speicherort verarbeitet werden.
f. Anwender_innen sind Personen, die die betreffenden IT-Anwendungen nutzen (ausgenommen Administrator_innen).
g. Systemadministrator_innen sind Arbeitnehmer_innen der Akademie, die nach ihrem Beschäftigungsverhältnis für die Planung, Installation, Konfiguration und Pflege von IT-Systemen und IT-Anwendungen an der Akademie zuständig sind.
h. Anwendungsaktualisierungen – Updates sind Aktualisierungen bestehender IT-Systeme und IT-Anwendungen
i. Bestehende Anwendungen sind IT-Systeme und IT-Anwendungen, die an der Akademie zum Zeitpunkt des Abschlusses dieser Betriebsvereinbarung in Betrieb sind bzw. vorrübergehend außer Betrieb genommen wurden.
j. Zukünftige Anwendungen sind Anwendungen, die an der Akademie zum Zeitpunkt des Abschlusses dieser Betriebsvereinbarung nicht in Betrieb sind, jedoch zu einem späteren Zeitpunkt in Betrieb genommen werden können.
k. Testbetrieb beschreibt den Betrieb einer IT-Anwendung zur Vorbereitung einer Anwendungsaktualisierung oder der Einführung einer zukünftigen Anwendung außerhalb des operativen Betriebs.
l. IT-Systeme meinen als Überbegriff die Ausgestaltung der IT-Umgebung in Zusammenspiel von Hardware, Software, Netzwerk-, Datenbank- und Sicherheitssysteme sowie mobile, cloudbasierte und webbasierte Systeme in der IT.
m. Außerbetriebnahme beschreibt die Deaktivierung/Deinstallation einer Anwendung unter Löschung der in dieser Anwendung erfassten Daten.
n. Gesetzliche Verpflichtungen meinen Verpflichtungen, die sich aus Gesetzen, Verordnungen und Gerichtsentscheidungen ergeben. Gleichgestellt sind Verpflichtungen auf kollektivvertraglicher Grundlage (Kollektivvertrag, Betriebsvereinbarung).
o. Sonstige rechtliche Verpflichtungen ergeben sich aus arbeitsvertraglichen Regelungen und/oder aus akademiespezifischen Regelungen.
p. TOMs beschreiben technische und organisatorische Maßnahmen, um die IT-Sicherheit der Verarbeitung von personenbezogenen Daten zu gewährleisten.

V. Grundsätze der Datenverarbeitung

1. Der Umgang mit personenbezogenen Daten und die diesbezüglichen Regelungen müssen den datenschutzrechtlichen Anforderungen der DSGVO entsprechen.

2. Der jeweilige Verarbeitungszweck sowie allfällige akademiespezifische TOMs sind in der Dokumentation der IT-Systeme und IT-Anwendungen gemäß Art 30 DSGVO und Punkt VII.1 festzuhalten.

3. Alle personenbezogenen Arbeitnehmer_innen-Daten sind nach der Zweckerfüllung und nach Ablauf der gesetzlichen oder sonstiger rechtlicher Aufbewahrungsfristen zu löschen oder zu anonymisieren. Diesbezügliche Aufbewahrungsfristen finden sich im jeweiligen Verzeichnis der Verarbeitungstätigkeiten gemäß Art 30 DSGVO.

4. Automationsgestützte Übermittlung von personenbezogenen Arbeitnehmer_innen-Daten an Dritte, die nicht der Verschwiegenheitspflicht unterliegen, darf ohne Zustimmung des_der betroffenen Mitarbeiter_in nur im Rahmen gesetzlicher, kollektivvertraglicher oder standesrechtlicher Verpflichtungen bzw. im Rahmen der Regelungen der vorliegenden Betriebsvereinbarung erfolgen.

5. Eine Übermittlung von personenbezogenen Arbeitnehmer_innen-Daten an Dritte ist möglich, wenn diese notwendig ist und gleichzeitig sichergestellt wird, dass diese Dritten der Verschwiegenheitspflicht unterliegen. Diese Notwenigkeit zur Datenweitergabe ist insbesondere bei Wirtschaftsprüfungen, externer Revision, Datenlieferung an Sozialversicherungen etc. gegeben. In diesbezügliche Auftragsverarbeitervereinbarungen ist dem Betriebsrat auf Anfrage Einsicht zu gewähren (zumindest die datenschutzrechtlichen Abschnitte).

6. Die Weitergabe von personenbezogenen Daten allgemein innerhalb der Akademie ist nur im Rahmen der dienstlichen Notwendigkeit, im unbedingt erforderlichen Ausmaß und nach Maßgabe datenschutzrechtlicher Vorgaben erlaubt. Eine Weitergabe von personenbezogenen Daten an Dritte ist mit Ausnahme der gesetzlichen Vorgaben und nach Maßgabe der datenschutzrechtlichen Bestimmungen generell untersagt.

V. Auswertung von Daten der Arbeitnehmer_innen

1. Daten der Arbeitnehmer_innen dürfen, soweit sich aus den nachfolgenden Bestimmungen nichts Abweichendes ergibt, nur in anonymisierter Form ausgewertet werden.

2. Daten der Arbeitnehmer_innen dürfen in den folgenden Fällen personenbezogen ausgewertet werden:

a. zur Erfüllung gesetzlicher Verpflichtungen sowie im Fall eines strafbehördlichen Auftrags. In diesen Fällen dürfen Arbeitnehmer_innen-Daten aller Datenkategorien ausgewertet werden. (Beispiele: Personalverrechnung, Urlaubsaufzeichnungen)
b. Arbeitnehmer_innen-Daten aller Kategorien mit Ausnahme der Kategorie D (Geo-/Lokationsdaten) und der Kategorie E (Bild-/Audiodaten) dürfen zur Erfüllung sonstiger rechtlicher Verpflichtungen ausgewertet werden.
c. Arbeitnehmer_innen-Daten aller Kategorien mit Ausnahme der Kategorie D (Geo-/Lokationsdaten) und der Kategorie E (Bild-/Audiodaten) dürfen bei Vorliegen eines konkreten begründeten Verdachts einer strafbaren Handlung durch den_die Arbeitnehmer_in unter Information des zuständigen Betriebsrates ausgewertet werden.
d. Daten der Kategorie D, E und F (Protokolldaten) und der Kategorie G (Inhaltsdaten) dürfen zur Gewährleistung der IT-Sicherheit ausgewertet werden.
e. Daten der Kategorie F (Protokolldaten) dürfen zur Gewährleistung der IT-Funktionalität ausgewertet werden.

3. Darüber hinaus dürfen Arbeitnehmer_innen-Daten nur dann personenbezogen ausgewertet werden, wenn dies in einer Zusatzregelung zu einer IT-Anwendungen

ausdrücklich genannt und im Umfang beschrieben ist oder der jeweils zuständige Betriebsrat einer Datenauswertung im Anlassfall zustimmt. In individuellen Auswertungen in Sonderfällen (z.B. Todesfall), die aus betrieblichen Gründen notwendig sind, wird die_der Datenschutzbeauftragte beigezogen.

4. Automatisierte Auswertung von Daten zur Feststellung der Dienstpflichtverletzung oder zur Leistungsfeststellung bzw. -beurteilung ist nicht zulässig.

VI. Datenschutzbeirat und Datenschutzbeauftragte_r

1. Zur Beratung aller Fragen, die sich im Zusammenhang mit der Einführung, dem Betrieb, der Auslegung und der Änderung von IT-Systemen und IT-Anwendungen ergeben, wird ein innerbetrieblicher Datenschutzbeirat gebildet. Die Beratungen, Ergebnisse und Erkenntnisse des Datenschutzbeirats dienen der Universitätsleitung und den Betriebsräten als Entscheidungsgrundlage. Die Entscheidungskompetenzen des Rektorats der Akademie als Leitungsorgan und die der Betriebsräte als Körperschaft gemäß ArbVG bleiben davon unberührt.

2. Der Datenschutzbeirat setzt sich zumindest aus folgenden Personen zusammen:

- zwei Vertreter_innen vom Rektorat nominiert
- zwei Vertreter_innen der Betriebsräte
- Datenschutzbeauftragte_r

Sowohl die Vertreter_innen des Rektorats und der Betriebsräte als auch die_der Datenschutzbeauftragte haben die Möglichkeit, bei Bedarf Fachpersonal ihrer Wahl zur Beratung beizuziehen. Allfällig anfallende Kosten trägt die Akademie. Die Tätigkeit im Datenschutzbeirat erfolgt während der bezahlten Arbeitszeit und es dürfen aus dieser Tätigkeit keine Nachteile entstehen. Dies gilt auch für hinzugezogenes Fachpersonal der Akademie. Der Datenschutzbeirat legt eine Geschäftsordnung fest.

3. Aufgabe des Datenschutzbeirats ist es unter anderem einen Interessensausgleich in Fragen des Einsatzes von IT-Systemen und IT-Anwendungen an der Akademie zwischen dem Rektorat und den Betriebsräten herbeizuführen. Die Tätigkeit des Datenschutzbeirats ist nicht mit einer Schlichtungsstelle gleichzusetzen. Die Rechte der Betriebsräte auf Anrufung einer gerichtlichen Schlichtungsstelle bleiben durch die Einrichtung und Tätigkeit des Datenschutzbeirats unberührt.

VII. Bestehende IT-Anwendungen

1. Die vorliegende Betriebsvereinbarung bildet die Grundlage für alle bestehenden IT-Anwendungen, die vom Geltungsbereich erfasst sind. Alle bestehenden IT-Anwendungen zum Zeitpunkt des Abschlusses dieser Betriebsvereinbarung, die in den Geltungsbereich fallen, sind in einer Dokumentation festgehalten, die zumindest folgende Angaben umfasst:

a) Name der Anwendung
b) Kurze Anwendungsbeschreibung
c) Betrieblich verantwortliche Organisationseinheit und Ansprechperson
d) Verarbeitete Datenkategorien
e) personenbezogene Auswertungen und Analysen
f) Übermittlung der erzeugten Daten in andere Systeme (Schnittstelle)
g) Verweis auf aktuelle Dokumentation aus dem Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO
h) Standort und Art der Datenerfassungsgeräte
i) Übermittlung an Dritte

j) Zugriffsberechtigungen (Funktion der Organisationseinheit und Ansprechperson)
k) Ort der Datenhaltung innerhalb/außerhalb des EWR
l) Akademie-spezifische TOMs

Diese Dokumentation ist nicht Teil dieser Betriebsvereinbarung. Sie ist dem Datenschutzbeirat und den Betriebsräten seitens des Rektorats zugänglich zu machen. Ergänzungen der jeweiligen Dokumentationen sind, soweit sie eine erweiterte Verarbeitung personenbezogener Daten betrifft, nur nach Einbeziehung des Datenschutzbeirates und der Bestimmungen dieser Vereinbarung gestattet.

2. Bestehende und zukünftig zum Einsatz kommende IT-Anwendungen weisen aufgrund der fortschreitenden technologischen Entwicklung einen laufenden Aktualisierungs- und Anpassungsbedarf auf. Vor der Inbetriebnahme von Anwendungsaktualisierungen, wenn

- Daten anderer als bisher eingemeldeter Datenkategorien verarbeitet werden,
- Daten zu einem anderen als dem bisher eingemeldeten Zweck verarbeitet werden,
- Anwender_innen-Daten über die bisher eingemeldeten Vorgänge ausgewertet werden (neue anwendungswirksame Verknüpfungsmöglichkeiten),

ist der Datenschutzbeirat mit diesen zu befassen und der jeweils zuständige Betriebsrat zu informieren bzw. gegebenenfalls dessen Zustimmung einzuholen.

3. Alle anderen Aktualisierungen sind als Aktualisierungen mit geringen Auswirkungen einzustufen und bedürfen keiner Befassung des Datenschutzbeirats sowie Information der Betriebsräte. Dies gilt insbesondere für Änderungen der Darstellungsformen (Benutzeroberfläche), Behebung von Sicherheitsmängeln und Veränderungen nicht-funktionaler Eigenschaften (Verfügbarkeit, Dienstqualität, Leistungsfähigkeit etc.).

VIII. Neue IT-Anwendungen

1.Die vorliegende Betriebsvereinbarung bildet auch die Grundlage für neue IT-Anwendungen. Die Betriebsräte und der Datenschutzbeirat sind über geplante Einführungen neuer IT-Anwendungen möglichst frühzeitig zu informieren. Die Betriebsräte können eine Regelung gemäß Punkt III 2 verlangen, wenn

- mit der geplanten Einführung eine Beurteilung von Arbeitnehmer_innen im Sinne des § 96a Abs. 1 Z 2 ArbVG erfolgt, oder
- die mit der Anwendung geplante Datenverarbeitung über die in der vorliegenden Betriebsvereinbarung geregelten Punkte hinausgeht.

2. Bestimmte neue IT-Anwendungen können ohne Einbindung der Betriebsräte und des Datenschutzbeirates eingeführt werden. Diese sind:

- neue Anwendungen mit denen ausschließlich Daten der Kategorie A, F und G verarbeitet werden und keine Verknüpfung mit anderen IT-Daten erfolgt, oder
- neue Anwendungen, die (auch) Daten anderer Kategorien verarbeiten, die Nutzung der Anwendung aber ausschließlich von dem_der Anwender_in entschieden wird.

3. Die vorliegende Betriebsvereinbarung bildet auch die Grundlage für Testbetriebe. Ein Testbetrieb ist immer zeitlich befristet und auf eine bestimmte Arbeitnehmer_innen-Anzahl/-Gruppe begrenzt.

IX. Zugriffsberechtigungen

1. Ein Zugriff auf IT-Systeme der Akademie und den damit verbundenen Diensten ist im Rahmen der dienstlichen Nutzung für die Arbeitnehmer_innen an der Akademie grundsätzlich jederzeit möglich, wobei explizit die Richtlinie zum mobilen Arbeiten sowie die etwaige weitere IT-Sicherheitsrichtlinien der Akademie zu beachten ist.

2. Vorgesetzte haben keine automatisch zugeordneten Zugriffsrechte auf die E-Mails oder Daten von ihnen zugeordneten Mitarbeiter_innen.

3. Systemadministrator_innen sind an die gesetzlichen Regelungen, insbesondere das Datenschutzgesetz und die DSGVO und an die Grundsätze dieser Betriebsvereinbarung gebunden. Die Akademie hat Systemadministrator_innen auf ihre diesbezügliche Verantwortlichkeit und ihre Verpflichtungen ausdrücklich hinzuweisen und diese entsprechend zu unterweisen.

4. Nach entsprechender Voranmeldung haben Systemadministrator_innen im Rahmen der Fernwartung Zugriffsrechte auf die IT-Endgeräte aller Mitarbeiter_innen. Beim Einsatz von Fernwartung ist dafür Sorge zu tragen, dass die in der vorliegenden Betriebsvereinbarung geregelten Rahmenbedingungen, insbesondere gemäß Punkt XII eingehalten werden.

5. Jeder Datenverkehr und Zugriff unterliegt zentral einer automatisierten Protokollierung, dem Logging. Die Logdateien dienen ausschließlich dazu, mögliche technische Schwachstellen und Gefährdungen aufzuzeigen und Probleme zu verhindern und zu beheben. Eine darüberhinausgehende Auswertung ist unzulässig. Protokolliert werden nur die Kommunikationsdaten (z.B. Sender, Empfänger, Zeit, Art, URL), nicht aber die Inhalte (z.B. E-Mail-Inhalte, Dokumente, Druckinformationen). Dateninhalte von Nachrichten werden durch automatische Systeme gelesen und auf enthaltene Gefährdungspotentiale untersucht (z.B. Virenscanner).

6. Die bei der Nutzung der IT-Systeme, IT-Anwendungen und Diensten der Akademie anfallenden personenbezogenen Arbeitnehmer_innen-Daten (Logdaten und Inhaltsdaten) dürfen nicht zur Leistungs- und Verhaltenskontrolle verwendet werden. Die Erstellung von personenbezogenen Verwendungsprofilen ist unzulässig.

7. Zugriff auf Logdateien haben ausschließlich Systemadministrator_innen. Im Rahmen des ISMS (Punkt X) können abweichende Regelungen, insbesondere in Hinblick auf SIEM und SOC, die den Grundsätzen der vorliegenden Betriebsvereinbarung nicht zuwiderlaufen dürfen, vereinbart werden.

X. Informationssicherheitsmanagement (ISMS)

1. Die Akademie evaluiert zur Sicherstellung der IT- und Datensicherheit regelmäßig die getroffenen Strategien, Konzepte sowie technischen und organisatorischen Maßnahmen (TOMs).

2. Dazu wird ein Informationssicherheitsmanagementsystem (ISMS) eingeführt, das sowohl interne als auch externe Maßnahmen sowie kooperative Maßnahmen im Sinne von universitätsübergreifenden Shared Services oder Shared Infrastructures umfassen kann. Das ISMS darf den Regelungen dieser Betriebsvereinbarung nicht zuwiderlaufen. Mit den Entscheidungen zur konkreten Ausgestaltung, Erweiterung oder Veränderung des ISMS sind der Datenschutzbeirat und gegebenenfalls die Betriebsräte zu befassen.

XI. Drittanbieter

1. Drittanbieter in der Form von Auftragsverarbeiter_innen im Sinne des Art 28 DSGVO, die im Auftrag der Akademie personenbezogenen Arbeitnehmer_innen-Daten verarbeiten und/oder auswerten, müssen ausreichend Gewähr für die rechtmäßige und sichere Datenverarbeitung leisten. Die Akademie kann zur Sicherstellung entsprechende Richtlinien und Regelungen erlassen, die nicht den Regelungen der vorliegenden Betriebsvereinbarung zuwiderlaufen dürfen.

2. Die nähere Ausgestaltung der Pflichten von Auftragsverarbeiter_innen sind jeweils in einem schriftlichen Vertrag (AVV) zwischen der Akademie und den jeweiligen Auftragsverarbeiter_innen festzuhalten.

3. Ein_e Auftragsverarbeiter_in darf personenbezogene Arbeitnehmer_innen-Daten nicht für eigene Zwecke verwenden.

XII. Fernwartung durch Externe und Remote-Zugriffe

1. Für Wartungs- und Servicezwecke kann externen Personen ein kontrollierter Zugang zu den IT-Systemen und IT-Anwendungen der Akademie gewährt werden. Der externe Zugang wird ausschließlich für Wartungszugänge eingerichtet.

2. Die Weitergabe der im Rahmen der Fernwartung und/oder Remote-Zugriffe erfassten personenbezogenen Daten darf ausschließlich in anonymisierter oder aggregierter Form erfolgen. Ist eine Weitergabe der personenbezogenen Daten unbedingt erforderlich, ist vor deren Verwendung die Zustimmung der_des jeweiligen Arbeiternehmer_in einzuholen, sowie der zuständige Betriebsrat und der Datenschutzbeirat zu informieren.

3. Remote-Zugriffe auf Endgeräte von Arbeitnehmer_innen sind ausschließlich für eine effiziente Unterstützung im Falle einer Problem- und/oder Fehlerbehebung sowie für die Erfassung der vorhandenen Hard- und Softwarekomponenten zulässig. Zur Aktivierung des Remote-Zugriffes ist vor jedem Zugriff von der_dem jeweiligen Mitarbeiter_in seine_ihre Zustimmung zur Verwendung einzuholen. Der_Die Mitarbeiter_in muss den Remote-Zugriff auf dem eigenen Bildschirm mitverfolgen können.

4.Die Akademie ist berechtigt eine gewissen Patch-Level voraussetzen und zu veranlassen, inklusive der Blockierung des Zugangs zum Netz bzw. zum vpn, falls ein gewisser Sicherheitslevel unterschritten und trotz mehrmaliger Aufforderung von den User_innen keine Maßnahmen eingeleitet wurden (z.B. Updates, Sicherheitspatches, Aufforderung des Endpoint-Managementsystems). Im Zuge dieser Prozesse können Neustarts von Endgeräten nach adäquater Vorwarnung erzwungen werden.

XIII. Beweismittel und -verwertungsverbot / Beweisverwertungsverzicht

1. Eine Verarbeitung von personenbezogenen Daten der Arbeitnehmer_innen, die unter Zuhilfenahme der durch diese Betriebsvereinbarung geregelten bestehenden und zukünftigen IT-Systeme und IT-Anwendungen in erlaubter oder unerlaubter Weise verarbeitet (erhoben, erfasst, ausgelesen, abgefragt, gespeichert, archiviert) wurden, zur Leistungs- und Verhaltenskontrolle oder zur wie auch immer gearteten Beurteilung von Arbeitnehmer_innen ist untersagt und damit rechtswidrig.

2. Es wird hiermit zur diesbezüglichen Bewehrung aus Gründen der rechtlichen Vorsicht gemäß Art 88 Abs 1 DSGVO ein entsprechendes außergerichtliches, gerichtliches und behördliches Beweismittel- und -verwertungsverbot vereinbart.

3. Erlangt die Akademie Kenntnis von derartigen Analysen Dritter, sind die betroffenen Arbeitnehmer_innen sowie der jeweils zuständige Betriebsrat zu informieren. Darüber hinaus hat die Akademie diese Dritten nachweislich zur Unterlassung aufzufordern und dies proaktiv dem jeweils zuständigen Betriebsrat zu kommunizieren.

XIV. Mitwirkungsrechte des Betriebsrats

1. Bei wesentlichen Änderungen der bestehenden IT-Systeme und IT-Anwendungen ist der zuständige Betriebsrat zu informieren, falls es dadurch zu einer wesentlichen Änderung bei der Ermittlung, Verarbeitung oder Übermittlung personenbezogener Arbeitnehmer_innen-Daten kommen könnte. Der zuständige Betriebsrat ist dabei vor der Implementierung, d.h. vor der Einführung bzw. Veränderung des Systems / der Anwendung, in Kenntnis zu setzen und auf Wunsch ist mit ihm hierüber zu beraten. In den gesetzlich vorgesehenen Fällen ist die Zustimmung der Betriebsräte zu erwirken.

2. Die Betriebsräte können Einsicht in die Dokumentation der IT-Systeme und Anwendungen gemäß Punkt VII.1 erlangen und Erläuterungen verlangen, die für die Wahrnehmung seiner nach dieser Betriebsvereinbarung und aufgrund anderer Rechtsgrundlage zustehenden Rechte erforderlich sind.

3. Der jeweils zuständige Betriebsrat hat das Recht, im Rahmen der ihm vom Gesetz her eingeräumten Befugnisse in Ausdrucke und Auswertungen von personenbezogenen Arbeitnehmer_innen-Daten Einsicht zu nehmen. Dabei ist jedoch insbesondere § 91 Abs 2 ArbVG zu beachten. Die Akademie verpflichtet sich, durch geeignete Maßnahmen die Kontrolle der Einhaltung dieser Betriebsvereinbarungen zu ermöglichen. Das Recht auf die Einräumung spezifischer Lizenzen ist damit nicht verbunden.

XV. Rechte und Pflichten der Arbeitnehmer_innen

1. Alle Arbeitnehmer_innen der Akademie sind über ihre Rechte und Pflichten in Bezug auf die Verarbeitung ihrer personenbezogenen Daten und über diese Betriebsvereinbarung zu informieren. Die einzelnen Informations-, Auskunfts-, Richtigstellung- und Löschungsrechte richten sich nach Art 15ff DSGVO. Insbesondere hat die Akademie als Arbeitgeberin den einzelnen Arbeitnehmer_innen die Informationen gemäß Art 12ff DSGVO zur Verfügung zu stellen.

2. Im Besonderen sind die Arbeitnehmer_innen verpflichtet:

- die datenschutzrechtlichen Bestimmungen einzuhalten, egal ob die Daten automatisiert, teil- oder nicht-automatisiert verarbeitet werden.
- Benutzerkennungen, Passwörter und sonstige Zugangsberechtigungen stets sorgfältig zu verwahren.
- betriebliche Anordnungen über die Verwendung personenbezogener Daten, insbesondere Übermittlungsanordnungen zu beachten.
- sämtliche Informationen über personenbezogene Daten zeitlich unbegrenzt auch über das Ende des Arbeitsverhältnisses hinaus vertraulich zu behandeln und geheim zu halten.

3. Des Weiteren ist es den Arbeitnehmer_innen untersagt, unbefugten Stellen/Dritten personenbezogene Daten zur Verfügung zu stellen oder diesen die Kenntnisnahme zu ermöglichen oder zur erleichtern.

4. Es wird vereinbart, dass die Akademie als Arbeitgeberin Schulungsmaßnahmen in Fragen der IT-Sicherheit und des Datenschutzes für die Arbeitnehmer_innen anbieten und bestimmte im Rahmen von Sicherheitsrichtlinien verbindlich stellen kann.

Wien, am 13.07.2026

Für die Akademie der bildenden Künste Wien:

.....

Dr. Johan F. Hartle
Rektor

Für den Betriebsrat für das künstlerisch-wissenschaftliche Personal:

.....

Dr^{in} Ruby Sircar
Vorsitzende

Für den Betriebsrat für das allgemeine Universitätspersonal:

.....

Amtsrätin Duhja Reithner
Vorsitzende

daspario Datenblatt Nr. 1

gemäß III. Geltungsbereich Absatz 2 der BV-IT zu Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.

	Dokumentation
Name der Anwendung	Daspario – digital art and science platform
Betrieblich verantwortliche Organisationseinheit	Vizerektorat für Infrastruktur und Nachhaltigkeit
Zweck der Datenverarbeitung	Leistungsdokumentation für Reporting gemäß Art. 6 Abs. 1 lit. e DSGVO iVm § 12 UG und damit verbundene Verordnungen (insbesondere WBV 2016)
(optional) Nichtziel	*Text einfügen*
Verarbeitete Datenkategorien	Betroffene Personen: Beschäftige und Studierende der Akademie der bildenden Künste Wien Personenbezogene Daten Name, Vorname, Aliasname Mailadresse Bidok Geburtstag (nur der Tag des Monats) Geschlecht durch Nutzer_innen eingetragene Leistungen entlang der vorgegebenen Kategorien der Wissensbilanz
vereinbarte personenbezogene Auswertungen und Analysen	Erstellung der Kennzahlen 3.B.1 und 3.B.2 der Wissensbilanz der Akademie, Erstellung des bibliographischen Nachweises der Akademie
Übermittlung von Daten von anderen/in andere Systeme (Beschreibung Schnittstelle)	Übermittlung der Daten in daspario erfolgt über eine Schnittstelle aus Akademie Online mit regelmäßiger Synchronisation der Nutzer_innen- bzw. Zugangsdaten Übermittlung der Kennzahlen der Wissensbilanz erfolgt über die Eingabe in ein elektronisches Tool des BMFWF
Verweis auf Art 30 DSGVO Dokumentation	datareg.brz.gv.at/app.html(view:home/verantwortlicher/68aebda5bd9e4e0c772041f6)

Rollen- und Berechtigungskonzept	Sys-Admin Org: Sperren von Accounts ORG-Admin: erfasste Leistungen von Nutzer_innen ausblenden, Leistungen löschen, Leistungen bearbeiten, Leistungen und Accounts auf „unsichtbar“ stellen Nutzer_innen: eigene Leistungen erfassen und bearbeiten, Mitwirkende hinzufügen, eigene Leistungen löschen
Übermittlung von Daten an Empfänger	Im Zuge der Wissensbilanz Daten der Kennzahlen 3.B.1 und 3.B.2 an das BMFWF Mit opt-in-Möglichkeit der Nutzer_innen: Übermittlung von Daten an Kulturpool
Verweis Akademie-spezifische TOMs	Die Liste der TOMs wird vom Vizerektorat für Infrastruktur und Nachhaltigkeit und der Abteilung Zentraler Informatikdienst gemeinsam verwaltet und wird dem Betriebsrat auf Anfrage jederzeit zu Verfügung gestellt.
(optional) organisatorische Regeln	
Anmerkungen	Bei daspario handelt es sich um eine Webapplikation zur Dokumentation und Präsentation von Leistungen der Universitätsangehörigen. Es ist ein Kooperationsprojekt von vier Universitäten.

Ort, Datum Wien, 13.7.26

.....

für das Rektorat

.....

für den Betriebsrat

Exchange Online Datenblatt Nr. 2

gemäß III. Geltungsbereich Absatz 2 der BV-IT zu Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.

	Dokumentation
Name der Anwendung	Exchange Online (Microsoft 365)
Betrieblich verantwortliche Organisationseinheit	ZID
Zweck der Datenverarbeitung	E-Mail-Kommunikation, Kalenderverwaltung, Kontaktverwaltung
(optional) Nichtziel	
Verarbeitete Datenkategorien	Stammdaten (Name, E-Mail-Adresse, Organisationszugehörigkeit); E-Mail-Inhalte inkl. Anhänge; Kalendereinträge (Termine, Teilnehmerlisten); Kontakte; Aufgaben; Archivpostfächer, technische Metadaten (IP-Adressen, Zeitstempel, Geräteinformationen)
vereinbarte personenbezogene Auswertungen und Analysen	Administrator_innen führen ausschließlich Mailflow-Abfragen im Rahmen von Troubleshooting durch (z.B. bei Sicherheitsvorfällen oder Synchronisationsproblemen). Kein direkter Zugriff auf Postfachinhalte.
Übermittlung von Daten von anderen/in andere Systeme (Beschreibung Schnittstelle)	Microsoft Entra ID (SSO, Identitätsverwaltung) mit Shibboleth/SAML2-Föderation (übermittelte Attribute: Name, E-Mail, Organisationszugehörigkeit); AD-Sync via Microsoft Entra Connect (Verzeichnisabgleich On-Premises AD ↔ Entra ID); Hybrid-Betrieb mit On-Premises Exchange (E-Mail-Routing, Verzeichnisreplikation); Zoom Kalender-Integration (teilweise in Verwendung).
Verweis auf Art 30 DSGVO Dokumentation	datareg.brz.gv.at/app.html(view:home/verantwortlicher/6a35468d7f85e51c25909ef7)#daten
Rollen- und Berechtigungskonzept	- globale Administrator_innen; - Adminstrator_innen mit eingeschränkten Rechten (Support-Team, für Troubleshooting)

Übermittlung von Daten an Empfänger	Microsoft Corporation (USA) als Auftragsverarbeiter auf Basis von Microsoft EDU-Campusvertrag; externe E-Mail-Empfänger_innen (regulärer E-Mail-Verkehr); automatische Weiterleitungen an externe E-Mail-Adressen durch einzelne Nutzer_innen konfiguriert.
Verweis Akademie-spezifische TOMs	Die Liste der TOMs wird vom Vizerektorat für Infrastruktur und Nachhaltigkeit und der Abteilung Zentraler Informatikdienst gemeinsam verwaltet und wird dem Betriebsrat auf Anfrage jederzeit zu Verfügung gestellt.
(optional) organisatorische Regeln	Privatnutzung ist nicht explizit geregelt.
Anmerkungen	DSFA gemäß Art. 35 DSGVO vorhanden (erstellt vor M365-Einführung).

Ort, Datum Wien, 13.7.26

.....

für das Rektorat

.....

für den Betriebsrat

ZOOM Datenblatt Nr. 3

gemäß III. Geltungsbereich Absatz 2 der BV-IT zu Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.

	Dokumentation
Name der Anwendung	ZOOM
Betrieblich verantwortliche Organisationseinheit	ZID
Zweck der Datenverarbeitung	Videokonferenzen
(optional) Nichtziel	
Verarbeitete Datenkategorien	Stammdaten (Name, E-Mail-Adresse, Organisationszugehörigkeit); technische Verbindungsdaten (IP-Adresse, Geräteinformationen, Client-Version); Nutzungsdaten (Teilnahme, Dauer, Zeitstempel); Meeting-Inhalte (Audio, Video, Bildschirmfreigaben); Chat-Inhalte; Aufzeichnungen (sofern erstellt)
vereinbarte personenbezogene Auswertungen und Analysen	Nutzungsstatistiken ausschließlich durch Administratoren zum Zweck der Lizenzverwaltung (Auslastung, Verlängerungsbedarf). Keine weitergehenden personenbezogenen Auswertungen vorgesehen.
Übermittlung von Daten von anderen/in andere Systeme (Beschreibung Schnittstelle)	SSO-Anbindung über Microsoft Entra ID und Shibboleth (übermittelte Daten: Name, E-Mail, Organisationszugehörigkeit). Kalender-Integration mit Microsoft Outlook/Exchange teilweise in Verwendung (übermittelte Daten: Meeting-Metadaten, Teilnehmerlisten, Meeting-Links).
Verweis auf Art 30 DSGVO Dokumentation	datareg.brz.gv.at/app.html(view:home/verantwortlicher/6a3547c67f85e51c25909f03)#daten
Rollen- und Berechtigungskonzept	Administrator_innen - mit Zugriff auf Nutzungsstatistiken und Lizenzverwaltung. Alle Nutzer_innen sind zur Aufzeichnung berechtigt, sofern alle Teilnehmenden zuvor eingewilligt haben.

Übermittlung von Daten an Empfänger	Zoom Video Communications, Inc. (USA) als Auftragsverarbeiter auf Basis von Standardvertragsklauseln (SCCs). Externe Meeting-Teilnehmer_innen erhalten im Rahmen der Meetingteilnahme Zugang zu personenbezogenen Daten interner Teilnehmender (Audio, Video, Anzeigename, Bildschirmfreigaben, Chat-Inhalte). Tritt regelmäßig auf; Empfänger_innen nicht im Voraus bestimmbar.
Verweis Akademie-spezifische TOMs	Die Liste der TOMs wird vom Vizerektorat für Infrastruktur und Nachhaltigkeit und der Abteilung Zentraler Informatikdienst gemeinsam verwaltet und wird dem Betriebsrat auf Anfrage jederzeit zu Verfügung gestellt.
(optional) organisatorische Regeln	Aufzeichnungen von Meetings sind nur mit vorheriger ausdrücklicher Einwilligung aller Teilnehmenden zulässig.
Anmerkungen	

Ort, Datum Wien, 13.07.26

.....

für das Rektorat

.....

für den Betriebsrat

SAP Datenblatt Nr. 4

gemäß III. Geltungsbereich Absatz 2 der BV-IT zu Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.

	Dokumentation
Name der Anwendung	SAP HR, SAP PM, Campus Online
Betrieblich verantwortliche Organisationseinheit	Leitung Finanzwesen, Personalverwaltung/Recht
Zweck der Datenverarbeitung	Verarbeitung und Übermittlung von Daten für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten. Verwendung und Evidenthaltung von personenbezogenen Daten von Bewerbern, wenn diese Daten vom Betroffenen angegeben wurden.
(optional) Nichtziel	
Verarbeitete Datenkategorien	Betroffene Personen: Beschäftigte, freie Dienstnehmer_innen, Lehrlinge, Volontär_innen, Praktikant_innen, ehemalige Beschäftigte, Angehörige, Honorarkräfte, Bewerber_innen Personenbezogene Daten: Name, Vorname, Aliasname, Geburtsort, Geschlecht, Personenstand, Geburtsdatum, Kinder und sonstige Familienangehörige, gesetzliche Vertretung, Staatsbürgerschaft, Bankverbindung, Abfertigungen, organisatorische Zuordnung, dienstliche Telefonnummer, Email, Wohnadresse, Kostenstelle, Sozialversicherungsnummer, Sozialversicherungsträger, Art des Anstellungsverhältnisses, MKV-Daten, Vordienstzeiten, Eintritt- und Austrittsdatum, Art der Beendigung des Dienstverhältnisses, Beschäftigungsbewilligungen, Bezeichnung der Tätigkeit, Daten zur Arbeitszeit, Daten zu Dienstverhinderung, Daten zu Entgelt, Daten nach dem Behinderteneinstellungsgesetz, Daten zu Sozialversicherung (E-Card), Daten zu Sachbezügen, Daten zu dienstlicher Reisetätigkeit und deren Abrechnungen, Gewerkschaftszugehörigkeit, Weiterbildungen und Schulungen, Ausbildungen und Qualifikationen, Nebenbeschäftigungen, Protokolle von Mitarbeiter_innen-Gesprächen,

vereinbarte personenbezogene Auswertungen und Analysen	Gesetzlich geregelte Personaladministration, Kennzahlen der Wissensbilanz, der Genderpay Gap Leistungstypen von Stipendien Betrag von Stipendien
Übermittlung von Daten von anderen/in andere Systeme (Beschreibung Schnittstelle)	Übermittlung von Daten zu Spenden und Stipendien an Transparenzdatenbank BMFWF Finanzberichte der §26 und §27 Projekte an FWF Kreditorenstammdaten an smartFix (free-com) Daten von Beamt_innen von BMFWF über BRZ an SAP Uploads: Bidok Upload an BMFWF laut Bildungsdokumentationsgesetz Daten der Personalverrechnung und -administration in ELDA zur Weiterleitung an BVAEB und BMF
Verweis auf Art 30 DSGVO Dokumentation	datareg.brz.gv.at/app.html(view:home/verantwortlicher/9ae728df-43c1-4a82-8074-9b5d5faf2c9f)#rechtmaessigkeit
Rollen- und Berechtigungskonzept	Berechtigungsvergabe durch Leitung des Finanzwesens Rollenkonzept: voneinander abgegrenzte Rollen einzelner Organisationseinheiten, sofern diese einen SAP-Zugang für ihre Verwaltungstätigkeit benötigen: • Institutsrollen • Beschaffungsrollen • Rektoratsrollen Zugänge werden unmittelbar bei Austritt gesperrt.
Übermittlung von Daten an Empfänger	Im Rahmen der Personaladministration und Lohnverrechnung notwendigen Daten laut Datenverarbeitungsverzeichnis
Verweis Akademie-spezifische TOMs	Die Liste der TOMs wird vom Vizerektorat für Infrastruktur und Nachhaltigkeit und der Abteilung Zentraler Informatikdienst gemeinsam verwaltet und wird dem Betriebsrat auf Anfrage jederzeit zu Verfügung gestellt.
(optional) organisatorische Regeln	
Anmerkungen	Bei SAP handelt es sich um das zentrale Personalverwaltungstool der Akademie der bildenden Künste Wien, das vom BRZ betrieben wird.

Wien, 13.7.2026

Ort, Datum

.....

für das Rektorat

.....

für den Betriebsrat

Telefonie Datenblatt Nr. 5

gemäß III. Geltungsbereich Absatz 2 der BV-IT zu Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.

	Dokumentation
Name der Anwendung	innovaphone VoIP-Telefonanlage
Betrieblich verantwortliche Organisationseinheit	ZID
Zweck der Datenverarbeitung	Interne und externe Telekommunikation
(optional) Nichtziel	
Verarbeitete Datenkategorien	Stammdaten (Name, Durchwahl — manuell angelegt); Verbindungsdaten (Datum, Uhrzeit, Dauer, angerufene Nummer) erfasst durch Telefonabrechnungssoftware; Voicemail-Inhalte (Sprachnachrichten)
vereinbarte personenbezogene Auswertungen und Analysen	Gesprächskosten werden durch Telefonabrechnungssoftware auf Kostenstellen aufgeteilt. Zugriff durch ZID-Administrator_innen. Jährliche Auswertung der Gesprächskosten pro Kostenstelle wird der Buchhaltung für die Kostenplanung übermittelt.
Übermittlung von Daten von anderen/in andere Systeme (Beschreibung Schnittstelle)	Telefonabrechnungssoftware: erhält Verbindungsdaten von der VoIP-Anlage sowie Durchwahlen und Kostenstellen via LDAP-Anbindung; SIP-Trunk zum Telefonie-Provider (öffentliches Telefonnetz). Kein Verzeichnisabgleich auf der VoIP-Anlage selbst.
Verweis auf Art 30 DSGVO Dokumentation	datareg.brz.gv.at/app.html(view:home/verantwortlicher/6a35452b7f85e51c25909eed)
Rollen- und Berechtigungskonzept	Administrator_innen (ZID) Vermittlungsplatz (Portier-SP) - hat erweiterte Rechte für eingehende Anrufe.
Übermittlung von Daten an Empfänger	Controlware (externer Wartungsdienstleister): Zugriff ausschließlich gemeinsam mit ZID-Administrator_innen (kein eigenständiger Fernzugriff); A1 als SIP-Provider (Verbindungsdaten für

	Gesprächsabwicklung über öffentliches Netz); Buchhaltung (jährlicher Kostenbericht pro Kostenstelle, intern).
Verweis Akademie-spezifische TOMs	Die Liste der TOMs wird vom Vizerektorat für Infrastruktur und Nachhaltigkeit und der Abteilung Zentraler Informatikdienst gemeinsam verwaltet und wird dem Betriebsrat auf Anfrage jederzeit zu Verfügung gestellt.
(optional) organisatorische Regeln	Gesprächsaufzeichnung ist technisch deaktiviert. Privatnutzung ist nicht explizit geregelt.
Anmerkungen	

Ort, Datum Wien, 13.07.26

.....

für das Rektorat

.....

für den Betriebsrat

Evasys Datenblatt Nr. 6

gemäß III. Geltungsbereich Absatz 2 der BV-IT zu Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.

	Dokumentation
Name der Anwendung	Evasys
Betrieblich verantwortliche Organisationseinheit	Abteilung Qualitätsentwicklung
Zweck der Datenverarbeitung	Durchführung von Befragungen, Verarbeitung von personenbezogenen Daten zur Kontaktaufnahme
(optional) Nichtziel	-
Verarbeitete Datenkategorien	Betroffene Personen: 1. Künstlerisch-wissenschaftliches Personal der Akademie der bildenden Künste Wien Personenbezogene Daten: · Vorname, Nachname · Mailadresse 2. Administratives Personal der Akademie der bildenden Künste Wien Personenbezogene Daten: Mailadresse 3. Studierende der Akademie der bildenden Künste Wien Personenbezogene Daten: Mailadresse 4. Absolvent_innen der Akademie der bildenden Künste Wien Personenbezogene Daten: Mailadresse aus den Daten der Alumni-Datenbank)
vereinbarte personenbezogene Auswertungen und Analysen	· Lehrveranstaltungsevaluation (= „LV-Feedback“) · Studienabschluss-Befragung · Absolvent_innen-Befragung

	· Weitere Befragungen im Rahmen der Qualitätsentwicklung der Akademie der bildenden Künste Wien
Übermittlung von Daten von anderen/in andere Systeme (Beschreibung Schnittstelle)	Die Mailadressen der Absolvent_innen stammen aus der Alumni-Datenbank der Akademie der bildenden Künste Wien. Diese Kontaktdaten beruhen auf einer freiwilligen Angabe der Absolvent_innen. Die Übermittlung der Daten in Evasys erfolgt über csv-Import.
Verweis auf Art 30 DSGVO Dokumentation	datareg.brz.gv.at/app.html(view:home/verantwortlicher/68ade1f7bd9e4e0c772041f2)
Rollen- und Berechtigungskonzept	Die Daten sehen allein die_der Administrator_in und die Teilbereichsadministrator_innen.
Übermittlung von Daten an Empfänger	Personenbezogenen Daten werden nicht übermittelt. Die Ergebnisse werden nur in aggregierter oder anonymisierter Form ausgewertet und übermittelt, sodass keine Rückschlüsse auf Einzelpersonen möglich sind.
Verweis Akademie-spezifische TOMs	Die Liste der TOMs wird vom Vizerektorat für Infrastruktur und Nachhaltigkeit und der Abteilung Zentraler Informatikdienst gemeinsam verwaltet und wird dem Betriebsrat auf Anfrage jederzeit zu Verfügung gestellt.
(optional) organisatorische Regeln	Anonymität und Datenschutz bei Umfragen der Abteilung Qualitätsentwicklung: https://www.akbild.ac.at/de/universitaet/qualitaetsentwicklung/selbstverstaendnis/anonymitaet-und-datenschutz-bei-umfragen-der-abteilung-qualitaetsentwicklung.pdf Mindest-Rücklaufgrenzen stellen Anonymität sicher: Ergebnisse werden erst ab einer zuvor definierten Mindestzahl an Rückmeldungen angezeigt. Befragungsantworten und personenbezogene Daten sind technisch vollständig getrennt.
Anmerkungen	Vgl.: Datenschutz und Informationssicherheit bei Evasys: https://evasys.de/datenschutz/#erfassung

Ort, Datum Wien, 13.7.26

.....

für das Rektorat

.....

für den Betriebsrat

Matomo Datenblatt Nr. 7

gemäß III. Geltungsbereich Absatz 2 der BV-IT zu Anhang B: IT-Anwendungen und IT-Systeme, die durch die Beifügung eines Datenblattes geregelt sind.

	Dokumentation
Name der Anwendung	Matomo
Betrieblich verantwortliche Organisationseinheit	ZID
Zweck der Datenverarbeitung	Webseitenanalyse und Nutzungsstatistiken der Akademie-Homepage
(optional) Nichtziel	
Verarbeitete Datenkategorien	Anonymisierte IP-Adresse (letztes Oktett entfernt); Browser-Typ und -Version; Betriebssystem; Bildschirmauflösung; Herkunftsland/-region; besuchte Seiten (URLs); Verweildauer; Referrer-URL;
vereinbarte personenbezogene Auswertungen und Analysen	Nutzungsstatistiken der Homepage durch ZID (Administration) und Öffentlichkeitsarbeit (nur Lesezugriff). KEINE personenbezogenen Auswertungen.
Übermittlung von Daten von anderen/in andere Systeme (Beschreibung Schnittstelle)	Keine Anbindung an externe Systeme. Tracking ausschließlich auf der Akademie-Homepage, KIOSK (kiosk.akbild.ac.at) und REPOSITORY (repository.akbild.ac.at).
Verweis auf Art 30 DSGVO Dokumentation	datareg.brz.gv.at/app.html(view:home/verantwortlicher/6a35443a7f85e51c25909ee1)
Rollen- und Berechtigungskonzept	Administrator_innen (ZID) User mit Lesezugriff (Büro für Öffentlichkeitsarbeit)

Übermittlung von Daten an Empfänger	Keine Übermittlung an Dritte. Self-hosted, Daten verbleiben auf eigener Infrastruktur.
Verweis Akademie-spezifische TOMs	Die Liste der TOMs wird vom Vizerektorat für Infrastruktur und Nachhaltigkeit und der Abteilung Zentraler Informatikdienst gemeinsam verwaltet und wird dem Betriebsrat auf Anfrage jederzeit zu Verfügung gestellt.
(optional) organisatorische Regeln	
Anmerkungen	IP-Anonymisierung aktiv.

Ort, Datum Wien, 13.7.26

.....

für das Rektorat

.....

für den Betriebsrat