HfMDK

Datenschutzkonzept der Hochschule für Musik und Darstellende Kunst Frankfurt am Main

Amtliche Bekanntmachungen
der Hochschule für Musik und Darstellende Kunst
Frankfurt am Main

Veröffentlichungsnummer: 126/2023 In Kraft getreten am: 04.07.2023

Datenschutzkonzept der Hochschule für Musik und Darstellende Kunst Frankfurt am Main

(Stand Juni 2023)

Die Hochschule für Musik und darstellende Kunst Frankfurt am Main (Hochschule) ist als juristische Person des öffentlichen Rechts zur Einhaltung der Datenschutzvorschriften des Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG) zuletzt geändert am 12. September 2018, der Datenschutzgrundverordnung (DSGVO) vom 27. April 2016 sowie anderer Rechtsvorschriften über den Datenschutz verpflichtet.

In Erfüllung dieser Verpflichtung verabschiedet das Präsidium der Hochschule folgendes Datenschutzkonzept:

I. Allgemeiner Teil

§ 1 Ziele des Datenschutzkonzepts

Das Datenschutzkonzept der Hochschule ist eine Hilfestellung bei der Umsetzung der gesetzlichen Anforderungen des Datenschutzes. Insbesondere dient es den Mitarbeitenden als Nachschlagewerk. Das im Rahmen von Schulungen und Sensibilisierungsmaßnahmen erworbene Wissen, kann im Datenschutzkonzept nachgeschaut werden. Auch soll neuen Mitarbeitenden dieses Konzept als Information für den Umgang mit personenbezogenen Daten an die Hand gegeben werden. Es ist Ausdruck der Wahrnehmung der Verantwortung der Hochschulleitung für die Einhaltung und Umsetzung der gesetzlichen Vorgaben für den Datenschutz.

§ 2 Geltungsbereich des Datenschutzkonzepts

Dieses Datenschutzkonzept gilt für die gesamte Hochschule. Hierzu zählen die Fachbereiche, die Verwaltung, das Präsidium sowie alle sonstigen Einrichtungen der Hochschule. Es gilt für alle an der Hochschule Beschäftigten. Hierzu zählen neben den festangestellten auch die gast- oder nebenberuflich tätigen Personen sowie studentische Hilfskräfte.

§ 3 Begriffsbestimmungen

Entsprechend den Begriffsbestimmungen der DSGVO bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene 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;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
3. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;
4. „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
5. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

II. Grundsätze der Datenverarbeitung

§ 4 Bei der Verarbeitung von personenbezogenen Daten müssen die folgenden Grundsätze Berücksichtigung finden:

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst sind. Der Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie die Auskunft darüber, welche sie betreffenden personenbezogene Daten verarbeitet werden.

2. Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

3. Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dazu zählt auch, dass durch technische Voreinstellungen sichergestellt wird, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

4. Richtigkeit

Personenbezogene Daten müssen sachlich richtig erfasst sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

5. Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher werden die Löschfristen in dem Verzeichnis der Verarbeitungstätigkeiten erfasst und regelmäßig überprüft. Eine längere Speicherung ist vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen für ausschließlich im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig.

6. Integrität und Vertraulichkeit

Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll insbesondere auch gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können. Hierzu zählt beispielweise auch das Abschließen von Türen und Schränken sowie das Sperren des Arbeitscomputers, sobald dieser verlassen wird.

§ 5 Rechtsgrundlagen

Bei der Verarbeitung personenbezogener Daten sind insbesondere die DSGVO, das HDSIG sowie datenschutzrechtliche Vorschriften im Hessischen Hochschulgesetz (HessHG) zu beachten. Daneben gibt es datenschutzrechtliche Spezialvorschriften in verschiedenen Gesetzen, die unter Umständen bei konkreten Verarbeitungstätigkeiten zu beachtenden sind.
Darüber hinaus können sich datenschutzrechtliche Anforderungen aus Dienstvereinbarungen zwischen dem Präsidium und dem Personalrat ergeben.

§ 6 Verantwortlichkeiten

(1) Die Verantwortung für die Einhaltung und Umsetzung der gesetzlichen Vorgaben für den Datenschutz an der HfMDK trägt der*die Präsident*in. Für die konkrete Umsetzung der gesetzlichen Anforderungen in den einzelnen Einheiten (Fachbereiche, zentrale Verwaltung, Betriebseinheiten und sonstige Einrichtungen) sind deren jeweilige Leiter*innen verantwortlich.

(2) Jede Führungskraft ist verpflichtet, die ihr zugeordneten Mitarbeitenden im Laufe ihrer Tätigkeit für die HfMDK für die datenschutzrechtlichen Aspekte der jeweiligen Aufgabe zu sensibilisieren.

(3) Alle Mitarbeitenden werden bei Aufnahme ihrer Tätigkeit über die zu beachtenden Anforderungen des Datenschutzes durch die Personalabteilung informiert. Um die Kenntnisse während der Tätigkeit in dem jeweils erforderlichen Umfang zu aktualisieren, sollen Mitarbeitende alle zwei Jahre ein Schulungsangebot der*des behördlichen Datenschutzbeauftragten wahrnehmen oder die erforderlichen Informationen und Unterlagen über die*den behördliche*n Datenschutzbeauftragte*n anfragen und selbstständig erarbeiten.

§ 7 Behördliche*r Datenschutzbeauftragte*r

(1) Die HfMDK bestellt gem. Art. 37 Abs. 1 lit. a) DSGVO, § 5 HDSIG eine*n behördliche*n Datenschutzbeauftragte*n sowie ihre*seine Stellvertretung. Die Datenschutzbeauftragen sind bei der Wahrnehmung ihrer Aufgaben ausschließlich an die Vorgaben des HDSIG sowie der DSGVO gebunden. Sie unterliegen keiner Weisung der*des Vorgesetzten. Organisatorisch sind sie der*dem Kanzler*in zugeordnet. Die*Der Datenschutzbeauftragte berichtet dem Präsidium bei Bedarf, mindestens aber einmal im Semester über die aktuellen datenschutzrechtlich relevanten Entwicklungen und Themen der Hochschule.

(2) Die*Der Datenschutzbeauftragte berät die Abteilungen und Mitarbeitenden der HfMDK in allen datenschutzrechtlichen Fragen. Auf Anfrage begleitet sie*er bei der Einführung neuer Verarbeitungstätigkeiten sowie bei Datenschutzfolgeabschätzungen (Art. 35 DSGVO). Soweit sich Betroffene zur Wahrnehmung Ihrer Rechte (z.B. des Auskunftsrechts nach Art. 15 DSGVO oder des Rechts auf Löschung nach Art. 17 DSGVO) an die HfMDK wenden, koordiniert die*der Datenschutzbeauftragte die Bearbeitung der entsprechenden Anfragen. Außerdem ist die*der Datenschutzbeauftragte Anlaufstelle für die Aufsichtsbehörde, den Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI).

(3) Die*Der Datenschutzbeauftragte überwacht die Einhaltung und Umsetzung der datenschutzrechtlichen Vorschriften an der HfMDK. Sie*Er hat in diesem Zusammenhang soweit dies zur Erfüllung ihrer*seiner Aufgabe erforderlich ist ein Recht auf Einsicht in sämtliche Akten, Datenbestände, IT-Systeme und sonstige Informationsquellen, ein Recht gegenüber allen Mitarbeitenden der

HfMDK auf Information und Auskunft sowie nach Ankündigung oder bei Gefahr im Verzug ein Recht auf Zugang zu allen dienstlichen Einrichtungen. Der*Dem Datenschutzbeauftragten sind alle Informationen, die zu ihrer*seiner Aufgabenwahrnehmung erforderlich sind, unaufgefordert zur Verfügung zu stellen. Die*Der Datenschutzbeauftragte ist jedoch nicht befugt, gegenüber den Mitarbeitenden der HfMDK Weisungen zu erteilen. Die*Der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität von betroffenen Personen sowie über Umstände, die Rückschlüsse auf betroffene Personen zulassen, verpflichtet, soweit sie*er nicht durch die betroffenen Personen hiervon befreit ist.

(4) Die*Der Datenschutzbeauftragte dokumentiert ihre*seine Aufgaben und berichtet dem Präsidium in Form eines Halbjahresberichts (vgl. Abs. 1).

(5) Die*Der Datenschutzbeauftragte sowie die Stellvertretung besuchen bei Bedarf, mindestens aber einmal im Semester eine Fortbildung, um das nach Art. 37 Abs. 5 DSGVO erforderliche Fachwissen zu erwerben und zu aktualisieren. Sie vernetzen sich mit den Hochschul-Datenschutzbeauftragten und sollen die jährlich stattfindenden Tagungen besuchen.

III. Umsetzung des Datenschutzes an der HfMDK

§ 8 Technische und organisatorische Maßnahmen

(1) Die HfMDK trifft abhängig von der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos von Datenschutzverletzungen (Art. 32 Abs. 1 DSGVO) geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
(2) Zu diesen technischen und organisatorischen Maßnahmen gehören in Anlehnung an das Standard-Datenschutzmodell der „Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder“ insbesondere:

Maßnahmen zur Gewährleistung der Verfügbarkeit von personenbezogenen Daten
- Anfertigung von Sicherheitskopien von Daten und Prozesszuständen
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Redundanz von Hard- und Software sowie Infrastruktur, soweit notwendig
- Vertretungsregelung für abwesende Beschäftigte

Maßnahmen zur Gewährleistung der Integrität von personenbezogenen Daten
- Löschen oder Berichtigen falscher Daten
- Prozesse zur Aufrechterhaltung der Aktualität von Daten
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

Maßnahmen zur Gewährleistung der Vertraulichkeit von personenbezogenen Daten

- Festlegung eines Rechte- und Rollen-Konzepts (z.B. für Zugriffe auf den Aktenplan)
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen, insbesondere Kommunikationskanäle
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen

§ 9 Schulung von Mitarbeitenden

Die*Der Datenschutzbeauftragte bietet regelmäßig, mindestens jedoch alle zwei Jahre, als auch auf Nachfrage, Schulungen für Mitarbeitende an. Die Schulungen behandeln Grundlagen des Datenschutzes sowie allgemeine datenschutzrechtliche Fragestellungen. Bei Bedarf können Schulungen auf besondere datenschutzrechtliche Themen ausgerichtet werden. Mitarbeitenden der Hochschule können themenspezifische Schulungen bei der*dem Datenschutzbeauftragten anfragen.

§ 10 Datenschutzrechtlich relevante Dokumente/Muster

Soweit erforderlich stellt die*der Datenschutzbeauftragte Muster für Datenschutzerklärungen, Einwilligungserklärungen durch die Betroffenen zur Verfügung. Soweit eine Auftragsverarbeitung stattfindet, sind Vereinbarungen für Auftragsverarbeitungen (Art. 28 DSGVO) und Vereinbarungen für gemeinsam Verantwortliche (Art. 26 DSGVO) von den Vertragspartnern der Hochschule anzufordern.

§ 11 Verzeichnis von Verarbeitungstätigkeiten

(1) Die Mitarbeitenden der Hochschule erfassen in ihrem Zuständigkeitsbereich solche Verarbeitungstätigkeiten, die personenbezogene Daten beinhalten, in dem gesetzlich vorgeschriebenen Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO). Sie sind gehalten, das Verzeichnis für die in ihrem Zuständigkeitsbereich erfassten Verarbeitungstätigkeiten bei Bedarf zu aktualisieren. Die*Der Datenschutzbeauftragte hat Zugriff auf alle in dem Verzeichnis erfassten Verarbeitungstätigkeiten. Sie*Er berät bei der Aufnahme einer neuen Verarbeitungstätigkeit.

(2) Für die Erfassung des Verzeichnisses von Verarbeitungstätigkeiten stellt die HfMDK eine Vorlage zur Verfügung, die alle Mitarbeitenden einsehen können. Sie dient als Ausfüllhilfe. Die in ihrem Zuständigkeitsbereich erfolgenden Verarbeitungstätigkeiten sind ausschließlich in diesem Verzeichnis zu erfassen. Ausnahmen sind mit der*dem Datenschutzbeauftragten abzustimmen.

§ 12 Datenschutz-Folgenabschätzung

Sollten besonders sensible Daten (z.B. Gesundheitsdaten) verarbeitet werden oder soll eine Form der Verarbeitung implementiert werden, die aufgrund der Verwendung neuer Technologien oder der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist vor Aufnahme der Verarbeitungstätigkeit eine Abschätzung ihrer Folgen vorzunehmen (Art. 35 Abs. 1 DSGVO). Jede*r Mitarbeitende, unter dessen Leitung eine Verarbeitung personenbezogener Daten durchgeführt wird, ist gehalten, vor Aufnahme der Verarbeitungstätigkeit die*den Datenschutzbeauftragte*n zu kontaktieren.

§ 13 Löschung von Daten

(1) Personenbezogene Daten sind grundsätzlich dann zu löschen, wenn sie für die Zwecke, für die sie erhoben worden oder auf sonstige Weise verarbeitet worden sind, nicht mehr notwendig sind (Art. 17 Abs. 1 DSGVO).

(2) Alle Mitarbeitenden der HfMDK sind gehalten, sich mit den Löschfristen bezogen auf ihre Verarbeitungstätigkeit auseinanderzusetzen und so frühzeitig wie möglich eine Frist für die Löschung der personenbezogenen Daten des betreffenden Verarbeitungsvorgangs festzulegen (Löschkonzept). Bei Bedarf erstellt die Abteilungsleitung für ihren Zuständigkeitsbereich allgemeine Löschkonzepte. Für Dokumente der zentralen Verwaltung gilt insoweit die Liste der Aufbewahrungsfristen des Arbeitskreises der Hochschularchive in Hessen in der jeweils aktuellen Fassung (Anlage 1).

§ 14 Vorgehen bei Datenschutzvorfällen

(1) Verletzungen des Schutzes personenbezogener Daten sind unverzüglich und möglichst innerhalb von 72 Stunden nach Kenntnis der*dem Hessischen Datenschutzbeauftragten zu melden (§ 60 Abs. 1 HDSIG). Eine Verletzung des Schutzes personenbezogener Daten ist gem. Art. 4 Ziff. 12 DSGVO jede „Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

(2) An der HfMDK ist im Falle des Verdachts einer Verletzung des Schutzes personenbezogener Daten dieser Verdacht unverzüglich zunächst der*dem Datenschutzbeauftragten zu melden, die*der eine Einschätzung vornimmt, ob tatsächlich eine Datenschutzverletzung vorliegt und wie hoch das Risiko für die Betroffenen voraussichtlich ist. Die*Der Datenschutzbeauftragte legt anschließend das Ergebnis ihrer*seiner Prüfung der*dem Kanzler*in und der*dem Präsident*in vor, die einvernehmlich darüber entscheiden, ob eine Meldung an den Hessischen Datenschutzbeauftragten erfolgt und ob die Betroffenen von der Verletzung benachrichtigt werden.

(3) Die*Der Datenschutzbeauftragte legt ggf. im Nachgang zu einem Datenschutzvorfall der*dem Präsident*in und der*dem Kanzler*in Vorschläge für technische und/oder organisatorische Maßnahmen vor, um vergleichbare Datenschutzvorfälle für die Zukunft nach Möglichkeit zu verhindern.

§ 15 Inkrafttreten

Dieses Konzept tritt am Tag nach der Veröffentlichung in den Amtlichen Bekanntmachungen auf der Webseite der Hochschule in Kraft.

26.06.2023, Frankfurt am Main

gez. Prof. Elmar Fulda, Präsident