

## Datenschutz-Richtlinie

### Inhalt

<b>Erster Teil: Allgemeine Regelungen</b>	<b>2</b>
§ 1 Geltungsbereich .....	2
<b>Zweiter Teil: Datenschutzrechtliche Zuständigkeiten</b>	<b>2</b>
§ 2 Hochschulleitung .....	2
§ 3 CIO-Runde .....	2
§ 4 Fachsachgebiete und Zentrale Einrichtungen .....	2
§ 5 Behördliche Datenschutzbeauftragte bzw. Behördlicher Datenschutzbeauftragter.....	3
<b>Dritter Teil: Zusammenarbeit</b>	<b>3</b>
§ 6 Zusammenarbeit und gegenseitige Information .....	3
<b>Vierter Teil: Ablauforganisation</b>	<b>3</b>
<b>Abschnitt 1: Allgemeine Grundsätze zur Gewährleistung des Datenschutzes</b>	<b>3</b>
§ 7 Information der Beschäftigten .....	3
§ 8 Beteiligung der bzw. des behördlichen Datenschutzbeauftragten .	3
§ 9 Datenschutzbericht .....	3
§ 10 Gewährleistung der Richtigkeit und Vollständigkeit des Verarbeitungsverzeichnisses.....	4
<b>Abschnitt 2: Gewährleistung besonderer datenschutzrechtlicher Verpflichtungen</b>	<b>4</b>
§ 11 Verfahren bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO4	
§ 12 Auftragsverarbeitung .....	5
§ 13 Inkrafttreten .....	5

## Erster Teil: Allgemeine Regelungen

### § 1 Geltungsbereich

Die Richtlinie gilt für die Verarbeitung personenbezogener Daten durch alle Organisationseinheiten der Akademie der Bildenden Künste Nürnberg.

## Zweiter Teil: Datenschutzrechtliche Zuständigkeiten

### § 2 Hochschulleitung

- (1) Die Hochschulleitung stellt mit Unterstützung der nachfolgend genannten Beteiligten sicher, dass die Verarbeitung personenbezogener Daten im Einklang mit den datenschutzrechtlichen Bestimmungen erfolgt.
- (2) <sup>1</sup>Die Hochschulleitung benennt eine bzw. einen behördlichen Datenschutzbeauftragten und dessen Vertretung. <sup>2</sup>Für die Benennung ist die als Anlage 1 beigefügte Urkunde zu verwenden.
- (3) <sup>1</sup>Die Hochschulleitung erarbeitet im Benehmen mit der bzw. dem behördlichen Datenschutzbeauftragten und der CIO-Runde geeignete Datenschutzvorkehrungen nach Art. 24 Abs. 2 DSGVO. <sup>2</sup>Hierzu gehören insbesondere Datenschutz-Richtlinien und fachverfahrensspezifische Anweisungen an die Beschäftigten.

### § 3 CIO-Runde

Die CIO-Runde legt in Abstimmung mit den nach §§ 2 und 4 zuständigen Organisationseinheiten

- a) geeignete technische Maßnahmen zum Schutz der zu verarbeitenden Daten nach Art. 24 Abs. 1, Art. 25 und Art. 32 DSGVO,
- b) angemessene und spezifische Maßnahmen zum Schutz besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO, Art. 8 Abs. 2 BayDSG,

fest.

### § 4 Fachsachgebiete und Zentrale Einrichtungen

- (1) Die Fachsachgebiete und Zentralen Einrichtungen (hier im Weiteren als Organisationseinheiten bezeichnet) tragen für ihren Zuständigkeitsbereich die Verantwortung für die Beachtung der jeweils maßgeblichen datenschutzrechtlichen Vorschriften.
- (2) Im Benehmen mit dem behördlichen Datenschutzbeauftragten stellen die Organisationseinheiten für ihren Zuständigkeitsbereich sicher, dass die Rechte der betroffenen Personen nach Art. 12, Art. 15 bis Art. 22 DSGVO sowie die Informationspflichten nach Art. 13 und Art. 14 DSGVO erfüllt werden.
- (3) <sup>1</sup>Die Personalvertretung gilt als Fachsachgebiet. <sup>2</sup>Der besonderen Stellung der Personalvertretung ist Rechnung zu tragen.
- (4) Soweit nichts anderes bestimmt ist, führt das Organisationssachgebiet das Verarbeitungsverzeichnis nach Art. 30 DSGVO.

## **§ 5 Behördliche Datenschutzbeauftragte bzw. Behördlicher Datenschutzbeauftragter**

Ergänzend zu den durch Art. 39 Abs. 1 DSGVO sowie Art. 12 und 24 Abs. 5 BayDSG zugewiesenen Aufgaben in der Anlage 2 werden der bzw. dem behördlichen Datenschutzbeauftragten keine weiteren Aufgaben übertragen.

### **Dritter Teil: Zusammenarbeit**

#### **§ 6 Zusammenarbeit und gegenseitige Information**

- (1) <sup>1</sup>Die Organisationseinheiten, die CIO-Runde und die bzw. der behördliche Datenschutzbeauftragte arbeiten zur Gewährleistung des Datenschutzes vertrauensvoll zusammen und informieren sich gegenseitig. <sup>2</sup>Hierzu schaffen sie geeignete Verfahren der kontinuierlichen Zusammenarbeit. <sup>3</sup>Sie unterrichten die Hochschulleitung über alle wesentlichen Vorgänge.
- (2) <sup>1</sup>Jede bzw. jeder Beschäftigte meldet seiner bzw. seinem jeweiligen Vorgesetzten unverzüglich Verstöße gegen datenschutzrechtliche Bestimmungen. <sup>2</sup>Die Organisationseinheiten informieren die bzw. den behördlichen Datenschutzbeauftragten über den Verstoß.

### **Vierter Teil: Ablauforganisation**

#### **Abschnitt 1: Allgemeine Grundsätze zur Gewährleistung des Datenschutzes**

##### **§ 7 Information der Beschäftigten**

Die Beschäftigten sind durch Richtlinien zum Datenschutz und auf sonstige Art und Weise für den Umgang mit personenbezogenen Daten zu sensibilisieren.

##### **§ 8 Beteiligung der bzw. des behördlichen Datenschutzbeauftragten**

- (1) Die bzw. der behördliche Datenschutzbeauftragte wird frühzeitig in alle wesentlichen Datenschutzfragen eingebunden und vom Organisationseinheiten, der CIO-Runde und den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.
- (2) Ihr bzw. ihm ist vor dem erstmaligen Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden, Gelegenheit zur Stellungnahme zu geben.
- (3) <sup>1</sup>Vor dem Einsatz einer Videoüberwachung sind der bzw. dem behördlichen Datenschutzbeauftragten der Zweck, die räumliche Ausdehnung und die Dauer der Videoüberwachung, der betroffene Personenkreis, die Maßnahmen nach Art. 24 Abs. 2 BayDSG und die vorgesehenen Auswertungen mitzuteilen. <sup>2</sup>Ihr bzw. ihm ist Gelegenheit zur Stellungnahme zu geben.
- (4) <sup>1</sup>Die bzw. der behördliche Datenschutzbeauftragte ist im Vorfeld von Vergabeverfahren und neuer Fachverfahren sowie vor der Beschaffung von IT-Hard- und Software zu beteiligen, wenn datenschutzrechtlich bedeutsame Anschaffungen geplant werden.

##### **§ 9 Datenschutzbericht**

<sup>1</sup>Die bzw. der behördliche Datenschutzbeauftragte erstellt regelmäßig, mindestens alle zwei Jahre, einen Bericht zum Datenschutz. <sup>2</sup>In diesem

sind die in der Hochschule zur Gewährleistung des Datenschutzes eingesetzten technischen und organisatorischen Maßnahmen darzustellen sowie ggf. festgestellte Datenschutzverstöße und Schutzlücken aufzuführen.

<sup>3</sup>Der Bericht enthält eine Bewertung, ob die eingesetzten technischen und organisatorischen Maßnahmen ausreichend sind, dem Stand der Technik entsprechen und in welchem Umfang datenschutzrechtliche Risiken bestehen. <sup>4</sup>Die Ergebnisse des Berichts werden mit der Hochschulleitung und den zuständigen Organisationseinheiten erörtert und Verbesserungsmöglichkeiten geprüft. <sup>5</sup>Der Bericht wird nicht veröffentlicht.

#### **§ 10 Gewährleistung der Richtigkeit und Vollständigkeit des Verarbeitungsverzeichnisses**

- (1) Die Organisationseinheiten melden der für die Führung des Verarbeitungsverzeichnisses zuständigen Organisationseinheit unaufgefordert die neu aufgenommenen Verarbeitungstätigkeiten sowie wesentliche Änderungen bereits gemeldeter Verarbeitungstätigkeiten.
- (2) <sup>1</sup>Die für die Führung des Verarbeitungsverzeichnisses zuständige Organisationseinheit übersendet den Fachsachgebieten jährlich eine Liste der von diesen gemeldeten Verarbeitungstätigkeiten. <sup>2</sup>Die Fachsachgebiete prüfen die Liste auf Richtigkeit und Vollständigkeit, aktualisieren sie und leiten sie der für die Führung des Verarbeitungsverzeichnisses zuständigen Organisationseinheit zu.

### **Abschnitt 2: Gewährleistung besonderer datenschutzrechtlicher Verpflichtungen**

#### **§ 11 Verfahren bei Datenschutzverletzungen nach Art. 33 und Art. 34 DSGVO**

- (1) <sup>1</sup>Im Fall einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO informiert die jeweilige Organisationseinheit, der die Datenschutzverletzung bekannt geworden ist, unverzüglich das Vorfallteam hierüber. <sup>2</sup>Das Vorfallteam besteht aus der behördlichen Datenschutzbeauftragten bzw. dem behördlichen Datenschutzbeauftragten, der bzw. dem Informationssicherheitsbeauftragten, dem IT-Sachgebiet, der Kanzlerin bzw. dem Kanzler und ihrer/seiner Stellvertretung] sowie der Stabsstelle Datenschutzkoordination.
- (2) <sup>1</sup>Das Vorfallteam erfasst den Vorfall in der Vorfalldatenbank, prüft und bewertet den Vorfall. <sup>2</sup>Das Vorfallteam teilt der Hochschulleitung seine Einschätzung mit, ob eine Meldepflicht nach Art. 33 DSGVO oder eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. <sup>3</sup>Die Einschätzung ist schriftlich zu begründen.
- (3) <sup>1</sup>Die Hochschulleitung meldet im Einvernehmen mit dem Vorfallteam die Verletzung des Schutzes personenbezogener Daten unverzüglich dem Bayerischen Landesbeauftragten für den Datenschutz mit dem nach Art. 33 DSGVO vorgegebenen Mindestinhalt, möglichst innerhalb einer Frist von 72 Stunden. <sup>2</sup>Ist eine Meldung innerhalb von 72 Stunden nicht möglich, sind die Gründe hierfür zu dokumentieren und die Meldung unverzüglich nachzuholen. <sup>3</sup>Die Meldung unterbleibt, wenn das Vorfallteam nach Abs. 2 der Auffassung ist, dass die Voraussetzungen des Art. 33 DSGVO nicht vorliegen. <sup>4</sup>Die Gründe hierfür sind zu dokumentieren. <sup>5</sup>Wenn Daten von oder an die Verantwortliche bzw. den Verantwortlichen eines anderen Mitgliedstaates übermittelt wurden, sind im Anwendungsbereich der Art. 28 bis 37

BayDSG die Informationen nach Art. 33 Abs. 3 DSGVO unverzüglich auch an diese bzw. diesen zu melden.

- (4) <sup>1</sup>Die Hochschulleitung entscheidet auf der Grundlage der Einschätzung des Vorfallteams nach Abs. 2, ob eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat und somit eine Benachrichtigungspflicht nach Art. 34 DSGVO besteht. <sup>2</sup>Die Benachrichtigung der betroffenen Person erfolgt unverzüglich durch die Hochschulleitung. <sup>3</sup>Unterbleibt eine Benachrichtigung nach Art. 34 DSGVO, sind die Gründe hierfür zu dokumentieren.
- (5) Nach Bekanntwerden des Verstoßes leitet das Vorfallteam unverzüglich Abhilfemaßnahme ein.

## **§ 12 Auftragsverarbeitung**

- (1) <sup>1</sup>Die jeweilige Organisationseinheit prüft vor Abschluss eines Vertrages über die Auftragsverarbeitung, ob der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO und den zu ihrer Ergänzung erlassenen europäischen, bundes- und landesrechtlichen Regelungen erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. <sup>2</sup>Hierzu lässt sich die Organisationseinheit entsprechende Nachweise/Zertifikate vorlegen und holt die Stellungnahme der bzw. des behördlichen Datenschutzbeauftragten sowie der CIO-Runde ein.
- (2) Absatz 1 gilt entsprechend für Vereinbarungen gemäß Art. 26 DSGVO.

## **§ 13 Vertrauliche Meldung von Datenschutzverstößen nach Art. 36 BayDSG**

<sup>1</sup>Erlangt ein Mitarbeiter von einem Datenschutzverstoß Kenntnis, kann er sich jederzeit unmittelbar an die bzw. den behördlichen Datenschutzbeauftragten wenden. <sup>2</sup>Die bzw. der behördliche Datenschutzbeauftragte behandelt die Meldung vertraulich. <sup>3</sup>Er darf Tatsachen, die ihm in Ausübung seiner Funktion anvertraut wurden, und die Identität der mitteilenden Person nicht ohne dessen Einverständnis offenbaren.

## **§ 14 Inkrafttreten**

Diese Richtlinie tritt am 15.01.2024 in Kraft.