Basis-Information zum Datenschutz an der HfMT Hamburg

Diese Basis-Information dient dazu, Grundlagen zum Thema Datenschutz zu vermitteln, um die Einhaltung der datenschutzrechtlichen Bestimmungen an der HfMT Hamburg zu gewährleisten.

Die datenschutzrechtliche Verantwortlichkeit für die Einhaltung der gesetzlichen Bestimmungen liegt beim Präsidium der HfMT Hamburg. Die Einhaltung dieser Bestimmungen ist aber auch Verpflichtung und Verantwortung aller Beschäftigten, Mitarbeitenden und Lehrenden (im Folgenden, unabhängig von ihrem Status, Hochschulangehörige genannt), sofern sie innerhalb ihres Aufgabenbereichs mit personenbezogenen Daten umgehen.

Gemäß § 3 Abs. 1 Hamburgisches Datenschutzgesetz (HmbDSG) ist es denjenigen Personen, die bei (…) öffentlichen Stellen (…) dienstlichen Zugang zu personenbezogenen Daten haben, untersagt, personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, insbesondere bekannt zu geben oder zugänglich zu machen. Dieses Verbot besteht auch nach Beendigung der Tätigkeit fort.

Häufig gibt es Unsicherheiten, wann und wie der Datenschutz zu berücksichtigen ist. Aus diesem Grunde werden im Folgenden einige Hilfestellungen zu verschiedenen Datenschutzbereichen gegeben.

Wann müssen Hochschulangehörige den Datenschutz berücksichtigen?

Die Datenschutzgrundverordnung (DSGVO) kommt ins Spiel, wenn in einem Arbeitsschritt oder Projekt personenbezogene Daten verarbeitet werden. Denn erst, wenn dies vorliegt, müssen auch datenschutzrechtliche Maßnahmen ergriffen werden. Erst dann haben die Betroffenen (Menschen, deren personenbezogene Daten verarbeitet werden) bestimmte Rechte und der Verantwortliche (in der Regel: die Hochschule) bestimmte Pflichten.

(1) Was sind personenbezogene Daten?

Darunter sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, Art. 4 Nr. 1 DSGVO. Zum Beispiel (keine abschließende Aufzählung):

- **Allgemeine Personendaten**, wie: Name, Alter, Geburtsdatum, Anschrift, Familienstand
- **Physische Merkmale**, wie: Geschlecht, Haut-, Haar- und Augenfarbe
- **Kennnummern**, wie: Matrikelnummer, Personalausweisnummer, Sozialversicherungsnummer
- **Bankdaten**, wie: Kreditkarte, Kontonummer, Einkommen, Kontostände
- **Onlinedaten**, wie: Standortdaten, IP-Adresse, E-Mail-Adresse, Chatprotokolle, Tracking-Daten
- **Gesundheitsinformationen**, wie: Krankendaten, Mitgliedschaft in einer Krankenversicherung

- **Bewerberdaten**, wie: Schul- und Arbeitszeugnisse, Abschlüsse im Ausland
- **Mediendaten**, wie: Bild-, Video- und Audiodateien

(2) Die Verarbeitung

Eine Verarbeitung ist ein Vorgang oder eine Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie z.B.:

- Das **Erfassen** von personenbezogenen Daten z. B. im Rahmen des Immatrikulationsprozesses und das **Speichern** dieser Daten
- Das **Ordnen und Strukturieren** von personenbezogenen Daten durch das Anlegen von digitalen Akten z. B. in der Personal- und Organisationsverwaltung oder durch Handakten
- Das **Weiterleiten** von personenbezogenen Daten an einen Dienstleister (z.B. externer Newsletter-Anbieter) oder aber auch an eine interne Stelle zur Weiterbearbeitung (z.B. Einkauf, Controlling etc.)
- **Verändern** von personenbezogenen Daten im Rahmen eines Forschungsprojektes (z.B. durch Auswertung, Pseudonymisierung von personenbezogenen Daten)
- Das **Löschen** von personenbezogenen Daten stellt auch eine Verarbeitung dar, z.B. beim Löschen von personenbezogenen Daten exmatrikulierter Studenten*innen oder auch von ausgeschiedenen Hochschulangehörigen.

Welche grundlegenden rechtlichen Verpflichtungen gibt es?

Die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten dürfen nur

a) auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) 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 („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Was heißt das konkret für Hochschulangehörige?

Hochschulangehörige dürfen die Verarbeitung in ihrem Aufgabenbereich nur durchführen, wenn (1) eine Rechtsgrundlage dafür vorhanden ist, (2) die entsprechenden Datenschutzerklärungen vorliegen und den Betroffenen zur Verfügung gestellt werden und (3) Einträge zur Verarbeitungstätigkeit in das Verarbeitungsverzeichnis (VVT) vorgenommen werden (Software privacy port). Ggf. sollten die Hochschulangehörigen (4) die Meldepflichten bei Datenpannen beachten und (5) ggf. Betroffenenanfragen bearbeiten oder an die Multiplikatoren*innen oder den/die Datenschutzkoordinator*in der HfMT Hamburg weiterleiten. In einzelnen Fällen kann es sein, dass die Hochschulangehörigen bei der Weiterleitung von personenbezogenen Daten an Externe anhand eines Musters (6) beim Abschluss eines Datenverarbeitungsvertrags mitwirken oder sich an der Erstellung einer (7) Datenschutz-Folgenabschätzung beteiligen. Den Hochschulangehörigen sollte bewusst sein, dass es (8) von Seiten der Aufsichtsbehörde Sanktionsmöglichkeiten bei Fehlverhalten im Datenschutzbereich geben kann. Deshalb sollten die Hochschulangehörigen der HfMT (9) grundsätzlich den/die Datenschutzkoordinator*in der HfMT Hamburg oder das Datenschutzteam des Multimedia Kontor Hamburg (MMKH) – ein Unternehmen der Hamburger Hochschulen – rechtzeitig einbinden.

(1) Rechtsgrundlage

Eine Verarbeitung personenbezogener Daten ist nur zulässig, wenn hierfür eine rechtliche Grundlage besteht – also eine Erlaubnis durch eine gesetzliche Regelung oder eine vorab erteilte Einwilligung der betroffenen Personen. Im Hochschulalltag werden diese Erlaubnisse häufig im Rahmen der Erfüllung von öffentlichen Aufgaben liegen, die bspw. im Hamburgischen Hochschulgesetz geregelt sind. Sollte jedoch keine Rechtsgrundlage z.B. in Form eines Gesetzes, einer Rechtsverordnung oder einer Hochschulsatzung vorliegen, kann von den Betroffenen eine freiwillige Einwilligung eingeholt werden.

Hinweis: Für eine solche Einwilligungserklärung finden die Hochschulangehörigen unter dem folgenden Link eine gut verständliche, kurze Anleitung, um eine vollständige und rechtmäßige Einwilligung nach neuem Recht verfassen zu können: **https://www.hh-datenschutz.de/infothek**

(2) Datenschutzerklärungen

Zum Zeitpunkt der Verarbeitung von Daten sind Betroffene entsprechend der Art. 12.ff der DSGVO zu informieren. Die Datenschutzerklärung einer Webseite hat zum Beispiel in erster Linie das Ziel, dieser Informationspflicht nachzukommen.

Muster für Datenschutzerklärungen können die Hochschulangehörigen unter **https://www.hh-datenschutz.de/infothek** finden. Die Hochschulangehörigen sollten bedenken, dass sie diese Muster von Datenschutzerklärungen mit den nur ihnen vorliegenden Informationen zu den Kategorien „personenbezogene Daten", „Verarbeitungstätigkeiten" und „Betroffene" ergänzen müssen.

(3) Verarbeitungsverzeichnis (VVT)

Die DSGVO verpflichtet den Verantwortlichen dazu, eine Dokumentation und Verfahrensübersicht über die Verarbeitung von personenbezogenen Daten, die an der Hochschule erfolgen, zu führen. Zur Erstellung dieses Verarbeitungsverzeichnisses nutzt die HfMT Hamburg die Software privacy port. Dort müssen alle wesentlichen Angaben über die Datenverarbeitung aufgeführt werden. Beispiele für eine dokumentationswürdige Verarbeitungstätigkeit an einer Hochschule können sein (keine abschließende Aufzählung!):

- Verwaltung von Studierendendaten
- Immatrikulationsprozess
- Prüfungsverwaltung
- Forschungsdatenerhebung
- Verwaltung von Daten der Ausleihenden für Geräte im Fachbereich ABC
- Verwaltung der Nutzerkonten der Hochschulbibliothek
- Absolventenverabschiedung
- Teilnehmende an einem Kurs/Veranstaltung (insbesondere Teilnehmerverwaltung, Zusendung von Teilnamebescheinigungen, Auswertung der Teilnahme etc.)
- Teilnehmende an einer Exkursion
- Personalaktenführung

(4) Datenpanne

Sollte es zu einer Datenpanne kommen, ist die Hochschule unter gewissen Umständen dazu verpflichtet, diese Panne der Datenschutzbehörde binnen 72 Stunden zu melden. Es kommt auch in Betracht, dass der Vorfall der betroffenen Person gemeldet werden muss, Art. 33, 34 DSGVO.

Beispiele für eine Datenpanne:

- ein verlorengegangener USB-Stick, unverschlüsselt
- versendete E-Mail mit falschem Anhang
- liegengelassener Dienstrechner (am Bahnhof/Flughafen/im Bus o.ä.)
- der Versand von E-Mails an einen größeren Empfängerkreis ohne Verwendung der BCC-Funktion
- Entsorgung von vertraulichen Unterlagen/Dokumenten im Papiermüll

Bei Vorliegen einer Datenpanne melden die Hochschulangehörigen oder die Multiplikatoren*innen der HfMT Hamburg die Datenpanne nach vorheriger Absprache mit dem/der Datenschutzkoordinator*in und dem Kanzler der HfMT Hamburg an den von der HfMT bestellten externen Datenschutzbeauftragten bei der datenschutz nord GmbH. Der externe Datenschutzbeauftragte meldet die Datenpanne in Absprache mit dem/der Datenschutzkoordinator*in und dem Kanzler der HfMT Hamburg der Aufsichtsbehörde.

Weiter ist es auch sinnvoll, dass die Hochschulangehörigen bei Kenntnis einer möglichen Datenpanne den entsprechenden Sachverhalt dokumentieren. Die Hochschulangehörigen, die auf die Datenpanne aufmerksam geworden sind, sollten sich innerhalb der Meldefrist von 72 Stunden (soweit wie möglich) verfügbar halten, damit bei etwaigen Rückfragen der Sachverhalt weiter ermittelt werden kann.

(5) Betroffenenanfragen

Bei Betroffenenanfragen handelt es sich in erster Linie um Datenauskünfte und Löschbegehren der Betroffenen. Die DSGVO sieht vor, dass Anfragen von Betroffenen binnen eines Monats ab Eingang bearbeitet werden müssen (Art. 12. Abs. 3 DSGVO).

Bei einer Datenauskunft möchte der*die Betroffene Auskunft, über die bei der HfMT Hamburg von ihm verarbeiteten personenbezogenen Daten haben. Die Hochschulangehörigen, bei denen aller Voraussicht nach die meisten personenbezogenen Daten des/der Betroffenen gespeichert werden, koordinieren die Erstellung der Datenauskunft (z.B. bei einem/einer Studenten*in wird dies wahrscheinlich die Studierendenverwaltung sein, bei sonstigen Hochschulangehörigen wird dies wahrscheinlich die Personalverwaltung sein). Dann wird eine solche Datenauskunft durch die Multiplikatoren*innen bzw. den/die Datenschutzkoordinator*in an der HfMT Hamburg abgenommen, bevor die personenbezogenen Daten dem/der Betroffenen mitgeteilt werden.

Bei einem Löschbegehren möchte der/die Betroffene, dass die HfMT Hamburg seine/ihre personenbezogenen Daten nicht mehr verarbeitet. Wenn die Hochschulangehörigen über eine Löschberechtigung verfügen, sollten sie die Löschung von **nicht mehr erforderlichen** personenbezogenen Daten selbst vornehmen. Ist eine vollständige Löschung der personenbezogenen Daten aus den Systemen der jeweiligen Hochschule durch die Hochschulangehörigen nicht möglich, sollte eine Löschung durch die IT-Abteilung erfolgen. Stehen der Löschung Aufbewahrungspflichten entgegen, sollte eine Sperrung der personenbezogenen Daten erfolgen. Dies kann z.B. bedeuten, dass nur ein zuständiges Mitglied oder ein/eine Angehörige/r der HfMT Hamburg Zugriff auf die personenbezogenen Daten des/der Betroffenen hat, bis die Daten nach Erlöschen der Aufbewahrungspflichten gelöscht werden müssen. Es sollte dem/der Betroffenen auf jeden Fall mitgeteilt werden, ob eine Löschung bzw. Sperrung erfolgt ist oder ob der Löschung Aufbewahrungspflichten entgegenstehen.

(6) Weitergabe von personenbezogenen Daten an Externe

Grundsätzlich ist die Weitergabe von personenbezogenen Daten an Externe verboten. Ausnahmsweise gilt: Sollten Hochschulangehörige daran beteiligt sein, mit Externen z. B. einen Vertrag abzuschließen, dessen Vertragsgegenstand in erster Linie aus der Verarbeitung von personenbezogenen Daten besteht, müssen diesem Vertrag Regelungen zum Datenschutz beigefügt werden. Es müsste dem Hauptvertrag also ein Datenverarbeitungsvertrag als Anlage beigefügt werden. Bei einem solchen Fall kontaktieren die Hochschulangehörigen bitte entweder den/die Datenschutzkoordinator*in der HfMT Hamburg oder das Datenschutzteam des MMKH.

(7) Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist vorzunehmen, wenn die Verarbeitung der personenbezogenen Daten zu einem datenschutzrechtlichen Risiko für die

Betroffenen führen kann. Dies kann z.B. bei der Verarbeitung von sensiblen Daten der Fall sein. In diesem Zusammenhang ist zu berücksichtigen, wie wahrscheinlich die Betroffenen beeinträchtigt werden können und welcher Schaden bei so einem Fall bei den Betroffenen eintreten würde. Die Frage, ob eine Datenschutz-Folgenabschätzung zu erfolgen hat, kann durch Nutzung der Software privacy port herausgefunden werden. Ist eine Datenschutz-Folgenabschätzung notwendig, muss nach Art. 35 Abs. 2 DSGVO der externe Datenschutzbeauftragte bei der datenschutz nord GmbH involviert werden.

(8) Konsequenzen

Bei Nicht-Einhaltung der datenschutzrechtlichen Erfordernisse drohen der HfMT Hamburg und unter Umständen auch der die Daten verarbeitenden Person selbst rechtliche Konsequenzen.

Ein Irrglaube der an den Hochschulen weit verbreitet ist: Öffentliche Stellen (und damit auch die Hochschulen) sind durch das Hamburgische Datenschutzgesetz von der Bußgeldandrohung der DSGVO zwar ausgenommen (§ 24 Abs. 3 HmbDSG), allerdings gibt es über das Bußgeld hinaus weitere Reaktionsmöglichkeiten, die der Aufsichtsbehörde gegenüber einer Hochschule zur Verfügung stehen und sogar kumulativ Anwendung finden können. Art. 58 Abs. 2 DSGVO nennt zehn Abhilfebefugnisse, unter anderem Warnungen, Verwarnungen, Anweisungen, Beschränkungen, Anordnungen bis hin zum Widerruf von Zertifizierungen. Die Abhilfebefugnisse variieren nach Schwere und Dauer des Verstoßes. Somit kann auch eine Hochschule, die zwar gegenüber dem Bußgeld privilegiert ist, vor enormen Problemen stehen, wenn etwa Datenverarbeitungen beschränkt oder ganz verboten werden.

(9) Frühes Einbinden der Multiplikatoren*innen, des/der Datenschutzkoordinators*in der HfMT Hamburg und/oder des Datenschutzteams des MMKH

Der/die Datenschutzkoordinator*in der HfMT Hamburg oder das Datenschutzteam des MMKH sind frühzeitig, d.h. bereits bei der Planung eines Einsatzes einer neuer Verarbeitungstätigkeit miteinzubeziehen. Dadurch können datenschutzrechtliche Aspekte von Anfang an berücksichtigt werden, wie z.B.

- bei der Verarbeitung "besonderer Kategorien" personenbezogener Daten lt. Art. 9 DSGVO (dies sind z.B. Gesundheitsdaten, Daten über politische Meinungen, ethnische Herkunft, biometrische Daten...)
- bei dem Umgang mit großen Mengen an personenbezogenen Daten oder
- wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bestehen könnte.

Damit das datenschutzrechtliche Anliegen der Hochschulangehörigen bearbeitet werden kann, ist es dienlich, wenn die Hochschulangehörigen der HfMT diese Informationen zusammentragen können:

WAS? Um welche Daten (Personen) handelt es sich?

WER? Wurden die Daten selbst erhoben oder sind sie von einer anderen Stelle weitergeleitet worden?

WARUM? Liegt gegebenenfalls eine Projektbeschreibung vor?

WOHIN? Werden die Daten weitergeleitet?

WIE LANGE? Bis wann werden die Daten benötigt?

Wo finden Hochschulangehörige weiterführende Informationen und an wen können sie sich bei Fragen wenden?

Die HfMT Hamburg arbeitet eng mit dem MMKH zusammen. Das MMKH bietet Informationen rund um das Thema „Datenschutz in der Hochschule" und unterstützt die HfMT Hamburg und weitere Hamburger Hochschulen bei allen Fragen rund um das Thema Datenschutz.

Vertiefende Hinweise und Informationen zum Thema Datenschutz an den Hamburger Hochschulen finden Hochschulangehörige unter: www.hh-datenschutz.de

- Allgemeine Fragen zum Thema Datenschutz, sei es projektbezogen oder nicht, richten Hochschulangehörige bitte an: datenschutz@hfmt-hamburg.de oder datenschutz@mmkh.de
- Schulungsanfragen richten Hochschulangehörige bitte an das MMKH: datenschutz@mmkh.de Gerne bietet das MMKH – neben allgemeinen Schulungen – auch spezielle Schulungen für einzelne Aufgabenfelder an.

Stand: 31.03.2022