Datenschutzmanagement der Hochschule für Angewandte Wissenschaften Hamburg (HAW Hamburg)

Kontakt:

Datenschutzkoordinatorin der HAW Hamburg
Ann Kristin Spreen
+49 40 428 75 9042
datenschutz@haw-hamburg.de

Datenschutzmanagement an der Hochschule für Angewandte Wissenschaften Hamburg (HAW Hamburg)

Die HAW Hamburg verarbeitet personenbezogene Daten im Rahmen von Forschung, Lehre, Studium und Weiterbildung sowie den dazu erforderlichen Verwaltungsaufgaben. Es werden insbesondere Daten von Bewerber*innen, Studierenden, Absolvent*innen sowie der Beschäftigten und Vertragspartner*innen verarbeitet. Die HAW Hamburg unterliegt als Körperschaft des öffentlichen Rechts und Einrichtung der Freien und Hansestadt Hamburg der Datenschutzgrundverordnung (DSGVO) sowie den einschlägigen landesrechtlichen Vorschriften, insbesondere dem Hamburgischen Datenschutzgesetz (HmbDSG) und dem Hamburgischen Hochschulgesetz (HmbHG).

Die HAW Hamburg ist im Rahmen der geltenden Vorschriften verpflichtet, besonders sorgsam mit personenbezogenen Daten umzugehen. Die Beschäftigten der HAW Hamburg sind zur Einhaltung der im folgenden beschriebenen Grundsätze verpflichtet.

Die HAW Hamburg trägt Sorge dafür, dass die Vorgaben der DSGVO erfüllt werden und die Hochschule dies im Rahmen ihrer gesetzlich obliegenden Rechenschaftspflichten dokumentiert (vgl. Art. 5 Abs. 2 DSGVO).

Das vorliegende Dokument stellt einheitlich und verbindlich dar, wie an der HAW Hamburg den datenschutzrechtlichen Anforderungen strukturell und inhaltlich entsprochen wird. Auf dieser Basis erfolgt im Einzelnen die technische und organisatorische Umsetzung und Gewährleistung der ausgewählten Maßnahmen. Deren Darstellung ist nicht Aufgabe dieses Dokuments.

Um dem Datenschutz im Hochschulalltag nachzukommen, sind folgende datenschutzrechtliche Grundsätze innerhalb der HAW Hamburg zu beachten:

Inhaltsverzeichnis

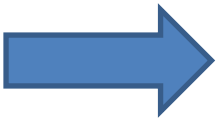
1. Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

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 HmbHG geregelt sind.

Mögliche Rechtsgrundlagen für die Verarbeitung sensibler Daten sind in Art. 9 Abs. 2 DSGVO aufgeführt. Sensible Daten sind u. a. Gesundheits- und Sozialversicherungsdaten. Diese dürfen z. B. gem. Art. 9 Abs. 2 a) DSGVO nur verarbeitet werden, wenn die Betroffenen dem im Rahmen der Einwilligungserklärung explizit zugestimmt haben, wenn dies im Rahmen des Arbeitsrechts gem. Art. 9 Abs. 2 b) DSGVO oder für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin (Art. 9 Abs. 2 h) DSGVO) erforderlich ist. Weitere typische Rechtsgrundlagen finden sich in Anlage 1.

Bei einer Einwilligung erklären sich die Betroffenen mit der Datenverarbeitung durch die HAW Hamburg einverstanden. Im Rahmen der Einwilligung müssen die Betroffenen darauf hingewiesen werden, dass ihre Einwilligung freiwillig ist. Die Betroffenen müssen auch Kenntnis davon haben, dass sie diese Einwilligung jederzeit ohne Angabe von Gründen widerrufen können. Die Abgabe der Einwilligungserklärung durch die Betroffenen muss dokumentiert werden, damit die HAW Hamburg nachweisen kann, dass sie von den Betroffenen eine Einwilligung eingeholt hat. Eine Mustereinwilligungserklärung wird zur Verfügung gestellt. Diese ist allerdings aufgrund der unterschiedlichen Fallkonstellationen im Einzelfall anzupassen. Eine Einwilligung ist nur dann als Rechtsgrundlage erforderlich, wenn keine gesetzliche Rechtsgrundlage vorliegt.

Neben dem Grundsatz, dass eine Verarbeitung personenbezogener Daten nur bei Vorliegen einer Rechtsgrundlage erlaubt ist, enthält die DSGVO weitere Grundsätze, die u. a. eine rechtskonforme Verarbeitung personenbezogener Daten ermöglichen sollen. Die folgenden Grundsätze müssen bei jeder Datenverarbeitung eingehalten werden. Sie sind bei jedem Vorgang erneut zu prüfen und zu hinterfragen:



Grundsätze

Transparenz

- Die informationelle Selbstbestimmung der Betroffenen muss gewahrt bleiben und Betroffene müssen ihre Rechte (vgl. Nr. 4) nach Art. 12 DSGVO ff. ausüben können.
- Werden Betroffene in Datenschutzhinweise über die Datenverarbeitung und ihre Rechte informiert?
- Art. 12 ff. DSGVO

Zweckbindung

- Zwecke der Datenverarbeitung sind die Gründe, aus denen Daten verarbeitet werden sollen. Der Zweck muss bei Erhebung bereits festgelegt, eindeutig und legitim sein. Wissen Sie, wozu Sie die Daten brauchen?
- Eine Weiterverarbeitung zu anderen Zwecken ist nur in Ausnahmen zulässig. Bspw. wenn die Weiterverarbeitung mit den ursprünglichen Erhebungszwecken vereinbar ist.

Datenminimierung

- Arbeiten Sie nur mit so vielen Angaben, wie sie zwingend dazu benötigen, um ihren Zweck zu erfüllen. Brauchen Sie die Daten wirklich?

Richtigkeit der Daten

- Daten über Menschen sollen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.
- Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, sollen unverzüglich gelöscht oder berichtigt werden. Wie ist Ihr aktueller Stand?
- Art. 16, Art. 17 DSGVO

Speicherbegrenzung

- Sobald die erhobenen Daten für den Verarbeitungszweck nicht mehr erforderlich sind, müssen sie gelöscht werden. Sind alte Daten gelöscht?
- Ausnahmen davon ergeben sich bspw. nach gesetzlichen Aufbewahrungspflichten, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke oder zur Abwehr von Rechtsansprüchen.
- Art. 17 DSGVO, Art. 5 DSGVO

Integrität und Vertraulichkeit

- Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor
- unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung
- oder Schädigung der personenbezogenen Daten.
- Sind Ihre Daten geschützt, insbesondere sensible Daten?
- Art. 32 DSGVO

Die für die jeweiligen Datenverarbeitungen inhaltlich verantwortlichen Organisationseinheiten der der Hochschule müssen vor der Entscheidung über die Verarbeitung personenbezogener

Daten prüfen,

- nach welcher Rechtsgrundlage die Verarbeitung zulässig ist,
- ob die weiteren datenschutzrechtlichen Grundsätze eingehalten werden,
- ob eine Verarbeitung nach Treu und Glauben erfolgt, d.h. von der betroffenen Person als fair empfunden werden dürfte und
- ob eine Datenschutz-Folgenabschätzung (siehe unter 2) erforderlich ist und diese gegebenenfalls durchführen.

2. Datenschutz-Folgenabschätzung

Die für die Datenverarbeitung inhaltlich verantwortlichen Organisationseinheiten analysieren bei der Einführung neuer Verarbeitungsvorgänge oder bei einer wesentlichen Änderung eines bestehenden Verarbeitungsvorganges, insbesondere durch die Verwendung neuer Technologien, ob diese Verarbeitung ein hohes Risiko für die Privatsphäre der Betroffenen darstellt. Dabei sind Art, Umfang, Kontext und Zweck der Datenverarbeitung zu berücksichtigen. Die vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit herausgegebene Liste von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung erforderlich ist, ist zu beachten (https://datenschutz-hamburg.de/assets/pdf/Liste_Art_35-4_DSGVO_HmbBfDI-oeffentlicher_Bereich_v2.0a.pdf). Im Rahmen einer Risikoanlayse nach Art. 35 DSGVO führt der verantwortliche Organisationsbereich eine Bewertung der Auswirkungen der geplanten Verarbeitungen auf den Schutz personenbezogener Daten durch. Die sogenannte Datenschutz-Folgenabschätzung hat stets vor der Datenverarbeitung zu erfolgen. Bei der Beschaffung neuer Systeme ist die Datenschutz-Folgenabschätzung bereits vor der Beschaffung des Systems vorzunehmen

*VVT: Die Frage, ob eine Datenschutz-Folgenabschätzung zu erfolgen hat, kann durch Nutzung des Tools privacy port beantwortet werden. Beim Anlegen eines Verarbeitungsprozesses sind die Angaben zur Datenschutz-Folgenabschätzung zu beantworten. Werden mehrere Fragen mit „Ja" beantwortet, ist der*die Datenschutzkoordinator*in umgehend zu kontaktieren. Ist eine Datenschutz-Folgenabschätzung notwendig, muss nach Art. 35 Abs. 2 DSGVO die datenschutz nord GmbH als behördlicher Datenschutzbeauftragter der HAW Hamburg involviert werden.*

3. Die Dokumentation

Die DSGVO sieht „zum Nachweis der Einhaltung dieser Verordnung"[1] u.a. ein Verzeichnis der Verarbeitungstätigkeiten (VVT) und ein Löschkonzept vor. Es handelt sich um eine spezielle und explizite Dokumentationspflicht, die der HAW Hamburg gemäß Art. 5 Abs. 2 DSGVO obliegt. Prozesse der HAW Hamburg sind herauszuarbeiten, um die relevanten Verarbeitungstätigkeiten im VVT abzubilden. Daran schließt sich ein Konzept an, welches die Löschung bzw. Vernichtung der erhobenen Daten aus den einzelnen Tätigkeiten regelt.

[1] ErwG. 82 DSGVO.

3.1 Informationen

Der transparente Umgang mit personenbezogenen Daten von Betroffenen ist eine zentrale Vorgabe der DSGVO. Im Zeitpunkt einer Datenerhebung sind die Betroffenen grundsätzlich darüber zu informieren, was mit Ihren Angaben geschieht (=Datenschutzerklärung). Dies gilt ebenfalls bei einzuholenden Einwilligungen, entsprechend Art. 7 DSGVO. Die Unterrichtung von Betroffenen muss umfänglich erfolgen, soll leicht verständlich sein und mit Angaben versehen werden, wer, wie und in welchem Umfang Auskünfte erteilt. Über die Zweckbindung muss informiert werden. Ob und wann eine Löschung erfolgt, ist ebenfalls mitzuteilen. Konkret hat eine Datenschutzerklärung folgendes zu beinhalten nach Art. 13 DSGVO: Name und Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten (bitte zwei verschiedene Kontaktwege nennen), die Zwecke der Datenverarbeitung, mögliche Empfänger der personenbezogenen Daten, Drittländer (=Nicht-EU-Länder), an welche personenbezogene Daten übermittelt werden, die Speicherdauer, die Betroffenenrechte und die Rechtsgrundlage. Bei einer Einwilligung erfolgt zusätzlich der Hinweis, dass ein Widerruf jederzeit mit Wirkung für die Zukunft möglich ist. Hierzu ist ein Kontakt anzugeben.

Die datenschutzrechtlichen Informationen werden durch den für die Verarbeitung jeweils zuständigen Bereich erstellt. Auch sei darauf hingewiesen, dass Datenschutzerklärungen aufgrund von Änderungen rechtlicher Vorgaben von Zeit zu Zeit aktualisiert werden müssen.

Das von der HAW Hamburg zur Verfügung gestellte Muster ist zu beachten.

VVT: Aktuelle Versionen von Datenschutzerklärungen und Einwilligungstexten sind zu kopieren bzw. zu speichern und im VVT zu hinterlegen. Gleiches gilt bis zum Ablauf der Aufbewahrungsfrist für vorherige Versionen. Die HAW Hamburg kommt damit den ihr obliegenden Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO nach. Zu Websites & Social Media hat dies unter „Webseiten/ Social Media" zu erfolgen. Bei allen anderen Themen sollen die Dokumente im entsprechenden Verarbeitungsprozess hinterlegt werden.

3.2 Verarbeitungsverzeichnis (VVT) mit „privacy-port"

Das VVT soll eine prozessorientierte Übersicht aller Verarbeitungen darstellen. Mithilfe des VVTs kann die HAW Hamburg gegenüber der Aufsichtsbehörde nachweisen, dass die Grundsätze der Verarbeitung von personenbezogenen Daten (siehe 2.1.1) eingehalten werden, im Sinne des Art. 5 Abs. 2 DSGVO, Art. 30 Abs. 3 DSGVO.

Intern wird das VVT dazu verwendet, technische sowie rechtliche Lücken bei der Datenverarbeitung zu erkennen und diese rechtzeitig z.B. mit dem Datenschutz- und IT-Team und dem Informationssicherheitsbeauftragten zu schließen. Das VVT hilft ebenfalls dabei, Datenströme zu erkennen. Einen schnellen Überblick zu erhalten, woher Daten stammen und an wen sie fließen, ist für die Beantwortung von Betroffenenanfragen, wie bspw. Löschung oder

Auskunft, hilfreich.

Die HAW Hamburg nutzt zurzeit die SaaS-Anwendung „privacy port“ der privacy central GmbH für die Dokumentationen im Rahmen des VVT. Zuständig für die Erstellung der einzelnen VVTs sind die für den Prozess/das Verfahren verantwortlichen Organisationseinheiten. Den dort benannten Mitarbeiter*innen der verschiedenen Organisationseinheiten der HAW Hamburg wurden Zugangsdaten zur Verfügung gestellt. Sie legen die Verarbeitungstätigkeiten in „privacy port“ an und leiten diese (per Deeplink Funktion) an den*die zuständige Fach-Verfahrensverantwortliche*n zum Befüllen weiter.

Verarbeitungsprozesse sind in „privacy port“ unter der Eingabemaske „Verarbeitungstätigkeiten + Datenschutz-Folgenabschätzung“ anzulegen. Einem Prozess sind - sofern vorhanden - insbesondere nachstehende Dokumente beizufügen:

- abgeschlossener Auftragsverarbeitungsvertrag mit Partner
- Kopie der aktuellen Datenschutzhinweise bzgl. Einwilligungserklärungen
- Art der Daten und spezifische Löschfristen
- Angaben zu den spezifischen Technischen und Organisatorische Maßnahmen (TOMs) des Verarbeitungsprozesses (entweder durch Beantwortung der abgefragten Punkte oder Anlage eines Dokuments)
- Beantwortung der Fragen bzgl. einer Datenschutz-Folgenabschätzung
- Eintrag der Rechtsgrundlage/n

In Einzelfällen verlangt „privacy port“ weitere Ergänzungen. Diese sollen in separate Eingabemasken eingetragen werden. Welche das sind, ist der folgenden Übersicht zu entnehmen, nebst den passenden Eingabemasken (gekennzeichnet mit: „“):

- Verarbeitung von Daten im Auftrag eines Dritten: „Verarbeitungstätigkeit als Auftragsverarbeiter“
- Einbindung von Videoüberwachung: „Videoüberwachung“
- Zusammenarbeit mit Partnern aus Drittstaaten: „Datenübermittlung an Dritte außerhalb der EU“
- Teilnahme an Kooperationen etc.: „Gemeinsame Verantwortlichkeit/ Joint Controller“
- Allgemeine Technische und Organisatorische Maßnahmen sowie spezielle für einzelne Projekte, wie Websites, Repositorien, Umfragen etc.: „Technische und Organisatorische Maßnahmen“
- Projekte bzgl. Websites bzw. Social Media: „Webseiten/ Social Media“
- Bei Anfragen der Betroffenen: „Anfragen von Betroffenen“
- Bei Datenschutzverletzungen und IT-/Informationssicherheitsvorfällen: „Vorfälle“
- Hausinterne Schulungen, Workshops etc.: „Schulungen“
- Sonstiges: „Einzelprojekte“
- Speichern von allgemeinen Dokumenten, wie Organigramm, Satzungen und Ordnungen: „Dokumente“

Die zuständigen Mitarbeiter*innen werden durch das Multimediakontor Hamburg (MMKH) (siehe auch unter 9.6) bei der Erstellung der einzelnen VVTs in rechtlichen Fragestellungen unterstützt. Schulungen zur Anwendung von „privacy port“ erfolgen ebenfalls durch das MMKH.

3.3 Löschkonzepte

Die strengen Vorgaben der DSGVO beinhalten, dass die HAW Hamburg personenbezogene Daten nur so lange aufbewahrt, wie sie zwingend benötigt werden oder eine Aufbewahrung gesetzlich vorgeschrieben ist. Die Angabe der geltenden Löschfristen erfolgt im VVT mit „privacy port“. Nach Ablauf der Löschfrist sind die Daten umgehend zu löschen. Die Löschung ist mittels eines sogenannten Löschkonzeptes zu regeln und zu dokumentieren (gemeint ist hier, wie die Löschung von der IT-Seite her erfolgt und wie dies dann auch dokumentiert wird). Hintergrund ist, dass den Betroffenen das sog. Recht auf Vergessenwerden zusteht. Dabei sind Besonderheiten, wie bspw. des Prüfungswesens, des Bewerbungsprozesses sowie des Beschäftigtendatenschutzes gesondert zu berücksichtigen. In dieser Hinsicht sind die Aktenordnung der HAW Hamburg sowie das Personalaktenrecht, als auch gesetzliche Vorgaben zu beachten. Ein gesondertes Löschkonzept, das in das VVT aufgenommen wird, wird erarbeitet.

VVT: Bei den einzelnen Verarbeitungsprozessen sind die Aufbewahrungs-/Löschfristen den Datenkategorien zuzuordnen. Ist für die Löschung eine besondere technische oder organisatorische Maßnahme erforderlich, ist diese als Teil der TOMs zu dokumentieren.

3.4 Technische und organisatorische Maßnahmen (TOMs)

Die TOMs beinhalten Vorgaben zur Datensicherheit nach Art. 32 DSGVO. Technische Maßnahmen, die die Systeme und personenbezogenen Daten an der HAW Hamburg vor dem Zugriff Unbefugter schützen, werden von der Informationssicherheit vorgegeben. Organisatorische Maßnahmen sind beispielsweise Schulungen der Mitarbeitenden. Die HAW Hamburg hat ihre TOMs zu dokumentieren. Dabei wird zwischen internen und externen TOMs unterschieden. So kann es vorkommen, dass die HAW Hamburg als Auftraggeberin fungiert und in dieser Rolle von externen Auftragnehmern die Übersendung einer Übersicht ihrer TOMs verlangt. Diese Übersicht ist wesentlicher Bestandteil des Vertrages nach Art. 28 DSGVO. Die HAW Hamburg kommt damit ihren gesetzlich obliegenden Rechenschaftspflichten im Sinne des Art. 5 Abs. 2 DSGVO nach.

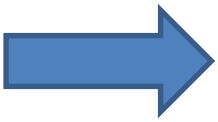
Auch die HAW Hamburg kann in Einzelfällen als Auftragsverarbeiterin tätig werden. Auch in diesem Fall ist ein entsprechender Vertrag zu schließen.

VVT: Die HAW Hamburg hat die geltenden TOMs im VVT zu hinterlegen. Die speziellen TOMs sind im jeweiligen Verarbeitungsprozess zu dokumentieren. Werden bei Projekten eigene TOMs benötigt, wie bspw. bei Websites, in der Forschung oder für Tools etc., sind diese projektbezogen unter „Technische und Organisatorische Maßnahmen“ zu hinterlegen.

4. Umgang mit Betroffenenrechten

Betroffenenrechte beschreiben die Rechte jener Personen, die von einer Datenverarbeitung umfasst sind. Betroffenenrechte schützen die informationelle Selbstbestimmung und sorgen dafür, dass die Menschen über die Verarbeitung ihrer Daten informiert sind. Mit der DSGVO haben die Betroffenen die Möglichkeit erhalten, Ihre Daten besser zu steuern und zu kontrollieren. Welche Betroffenenrechte die DSGVO kennt, zeigt die folgende Übersicht.

Betroffenenrechte



- Transparente Informationen zur Datenverarbeitung (Art. 12 DSGVO)
- Datenschutzhinweise mit konkreten Angaben (Art. 13, 14 DSGVO)
- Auskunft über eine Datenverarbeitung (Art. 15 DSGVO)
- Berichtigung von bereits erhobenen Daten (Art. 16 DSGVO)
- Löschung von Daten (Art. 17 DSGVO)
- Zugriff auf Daten einschränken (Art. 18 DSGVO)
- Datenportabilität (Art. 20 DSGVO)
- Widerspruch gegen eine Verarbeitung einlegen (Art. 21 DSGVO)

Die HAW Hamburg hat Anfragen bzgl. der Betroffenenrechte innerhalb eines Monats nach Eingang zu bearbeiten, im Sinne des Art. 12 Abs. 3 DSGVO. Häufig handelt es sich dabei um sogenannte Auskunfts- und Löschersuchen nach Art. 15 und 17 DSGVO.

Bei Eingang einer Anfrage ist diese umgehend an den*die Datenschutzkoordinator*in der HAW Hamburg weiterzuleiten. Der*die Datenschutzkoordinator*in wird die Anfrage in Zusammenarbeit mit der entsprechenden Organisationseinheit und ggf. dem Datenschutzbeauftragten bearbeiten. Dies betrifft Auskunfts-, Lösch-, Berichtigungs-, Einschränkungsersuchen, aber auch Anfragen bzgl. Datenportabilität und Widersprüche gegen eine Datenverarbeitung. Achtung: Letzteres betrifft keine Widerrufe nach vorherig getätigter Einwilligung (bspw. Newsletterabmeldungen etc.). Auf die Darstellung der Betroffenenrechte Berichtigungs-, Einschränkungsersuchen, Anfragen bzgl. Datenportabilität und Widersprüche wurde verzichtet, da Sie in der Praxis von eher geringerer Relevanz sein dürften.

VVT: Betroffenenanfragen sind in privacy port unter „Anfragen von Betroffenen" zu hinterlegen.

4.1 Auskunftsersuchen

Die Organisationseinheit, bei der die personenbezogenen Daten der betroffenen Person überwiegend verarbeitet und gespeichert werden, koordiniert das Auskunftsbegehren (bei Studierenden ist dies bspw. das Studierendensekretariat, bei Mitarbeiter*innen der

Personalservice). Ziel ist eine Zusammenstellung sämtlicher Daten der betroffenen Person, die durch die HAW Hamburg verarbeitet werden. Die Datenauskunft wird anschließend durch die*den Datenschutzkoordinator*in nach Rücksprache mit dem zuständigen Präsidiumsmitglied freigegeben.

Ein Auskunftsersuchen ist unverzüglich an die*den Datenschutzkoordinator*in weiterzuleiten.

4.2 Löschbegehren

Ein Löschersuchen ist unverzüglich an die*den Datenschutzkoordinator*in weiterzuleiten.

Bei einem Löschbegehren erfolgt die Löschung der nicht mehr erforderlichen personenbezogenen Daten bei vorliegender Löschberechtigung durch die zuständige Organisationseinheit. Ist eine vollständige Löschung der personenbezogenen Daten aus den Systemen der HAW Hamburg durch die zuständige Organisationseinheit nicht möglich, erfolgt eine Löschung durch das ITSC.

Stehen der Löschung Aufbewahrungspflichten entgegen, erfolgt eine Sperrung der personenbezogenen Daten. Dies kann z.B. bedeuten, dass nur ein*e zuständige*r Mitarbeiter*in der Organisationseinheit Zugriff auf die personenbezogenen Daten der betroffenen Person hat, bis die Daten nach Erlöschen der Aufbewahrungspflichten gelöscht werden müssen. Die Dokumentation ist von dem betroffenen Bereich an den*die Datenschutzkoordinator*in weiterzuleiten.

5. Umgang mit Datenschutzverletzungen

Im Falle einer Verletzung des Schutzes personenbezogener Daten ist diese der zuständigen Aufsichtsbehörde durch die HAW Hamburg zu melden (Art. 33, 34 DSGVO).2 In Einzelfällen ist die HAW Hamburg auch verpflichtet, die Betroffenen zu benachrichtigen. All diese Fragen sind binnen 72 Stunden zu klären.

Damit diese Zeiten eingehalten werden können, müssen Datenschutzverletzungen unverzüglich an den*die Datenschutzkoordinator*in weitergeleitet werden. Die Personen, die davon erfahren oder eine entsprechende Verletzung feststellen, melden NICHT selbst der Aufsichtsbehörde, sondern dies erfolgt durch den*die Datenschutzkoordinator*in nach entsprechender Prüfung und Dokumentation sowie der Freigabe durch das zuständige Präsidiumsmitglied.

[2] Anm.: Grundsätzlich handelt es sich bei den meisten Fällen von Datenschutzverletzungen um Angriffe oder Missbrauch durch Externe und/oder Interne. Die Ursachen liegen in der Existenz von Schwachstellen in den technischen oder organisatorischen Maßnahmen und fallen sehr oft in das Gebiet der IT- oder Informationssicherheit. Aber auch physikalische Angriffe (unverschlossene Büros mit Akten, Einbrüche) sind denkbar. Ebenso können Datenschutzaspekte insbesondere bzgl. der Wiederherstellbarkeit oder Verfügbarkeit durch Unfälle oder äußere Ereignisse (Brand, technischer Defekt) verletzt werden.

Erste Ansprechperson ist daher der*die Datenschutzkoordinator*in. Bei einem Bezug zu dem Einsatz von IT-Systemen, technischen Angriffen oder Ausfällen bzw. einem Angriff mit IT-Systemen ist der Informationssicherheitsbeauftragte der Hochschule zu informieren. Außerdem müssen die Verantwortlichen in den jeweiligen Organisationseinheiten in Kenntnis gesetzt werden, um bei der Aufklärung und Bewertung mitzuwirken.

Die Bewertung, ob die Aufsichtsbehörde und die betroffenen Personen zu informieren sind, trifft die*der Datenschutzkoordinator*innen nach Rücksprache mit dem zuständigen Präsidiumsmitglied.

Die zuständige Aufsichtsbehörde ist nur zu informieren, wenn die Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Zu berücksichtigen sind dabei Kriterien wie z.B. ein möglicher finanzieller Schaden der Betroffenen oder eine Beeinträchtigung des Rufs der Betroffenen. Nur wenn es sich um ein hohes Risiko für die Betroffenen handelt, sind diese unverzüglich zu informieren (Art. 34 DSGVO).

VVT: Vorgänge zu Datenschutzverletzungen sind im VVT unter „Vorfälle" zu hinterlegen.

6. Beantwortung von datenschutzrechtlichen Fragen

Sowohl die zuständige Ansprechperson des MMKHs als auch die*der Datenschutzkoordinator*in der HAW Hamburg werden frühzeitig in datenschutzrechtlich relevante Prozesse eingebunden.

7. Schulung und Sensibilisierung

Für eine erfolgreiche Umsetzung des Datenschutzes an der HAW Hamburg ist die Sensibilisierung der Mitarbeiter*innen ein wesentlicher Faktor. Ziel ist es, den Datenschutz während der Aufgaben im Bewusstsein zu verankern, damit das Datenschutzniveau an der HAW Hamburg kontinuierlich gesteigert werden kann.

Eine verbindliche datenschutzrechtliche Grundlagenschulung wird im Onboarding-Prozess verankert. Die Beschäftigten, die im Rahmen ihrer Tätigkeit eine Vielzahl personenbezogener Daten verarbeiten, werden regelmäßig (mindestens einmal pro Jahr) im Datenschutz geschult.

Zusätzlich schult das MMKH in verschiedenen Bereichen.

Zusätzlich werden datenschutzrechtliche Erstinformationen auf der Webseite der HAW Hamburg als zentraler Anlaufpunkt bei allen Fragen um den Datenschutz installiert. Darüber hinaus kann auf das Datenschutzportal des MMKHs zurückgegriffen werden, welches sowohl über aktuelle datenschutzrechtliche Entwicklungen im Hochschulkontext informiert, als auch Checklisten und Übersichten parat hält. URL: https://www.hh-datenschutz.de/

8. Zusammenarbeit mit Dritten

8.1 Auftragsverarbeitung

Bei einer Beauftragung externer Dritter mit der Verarbeitung von personenbezogenen Daten liegt in der Regel eine Auftragsdatenverarbeitung nach Art. 28 DSGVO vor. In diesem Fall ist ein sogenannter Auftragsverarbeitungsvertrag (AVV) zu vereinbaren Die HAW Hamburg hat ihre Partner sorgfältig auszuwählen. So darf sie nur mit Partnern zusammenzuarbeiten, die der HAW Hamburg einen hinreichenden Schutz gewährleisten, damit die geplante Datenverarbeitung datenschutzkonform und sicher erfolgt.

Die HAW Hamburg stellt Vertragsmuster zur Verfügung. Diese sollen grundsätzlich genutzt werden.

Auftragsverarbeitungsverträge sind durch das MMKH zu prüfen, soweit nicht das unveränderte Muster der HAW Hamburg verwendet wird. Die dem Vertrag beizufügenden TOMs sind durch den IT-Sicherheitsbeauftragten zu prüfen und freizugeben. Eine Vorlage des Vertrages zur Unterzeichnung durch den*die Präsident*in erfolgt durch das Justitiariat. Verträge, die das ITSC betreffen, werden durch die Leitung des ITSC unterzeichnet.

Erst mit Freigabe und Unterzeichnung des AVVs durch den*die Präsident*in der HAW Hamburg ist eine Zusammenarbeit mit dem Partner erlaubt.

Gleiches gilt für den Fall, dass die HAW Hamburg personenbezogene Daten für einen Dritten verarbeitet – also selbst Auftragnehmerin ist. Dies kann bspw. beim Ausrichten von Veranstaltungen der Fall sein, die in den Räumlichkeiten der HAW Hamburg durchgeführt werden, oder beim Hosting. Auch in diesen Fällen sind Auftragsverarbeitungsverträge zu schließen.

Vorherige Datentransfers sind grundsätzlich zu unterlassen oder vorab mit dem*der Datenschutzkoordinator*in abzustimmen.

VVT: Abgeschlossene AVVs sind im entsprechenden Verarbeitungsprozess zu hinterlegen, ausgenommen die HAW Hamburg agiert als Auftragnehmerin. Dann sind die AVVs unter „Verarbeitungstätigkeit als Auftragsverarbeiter" abzulegen.

8.2 Gemeinsame Verantwortlichkeit

Für den Fall, dass sowohl die HAW Hamburg als auch ein externer Dritter für die Verarbeitung personenbezogener Daten verantwortlich sind, ist eine Vereinbarung zu schließen (Art. 26 Absatz 1 DSGVO). Dies kann z.B. mit einer anderen Hochschule im Rahmen eines Forschungsprojekts oder eines Kooperationsstudiengangs eintreten. Aus dieser Vereinbarung ergeben sich u. a. die Aufgaben und Verantwortlichkeiten gegenüber den Betroffenen und die Daten, die der jeweilige Vertragspartner verarbeitet. Vorherige Datentransfers sind

grundsätzlich zu unterlassen oder vorab mit dem/der Datenschutzkoordinator*in abzustimmen. Die Unterzeichnung ist in elektronischer Form möglich.

Die HAW Hamburg stellt ein Vertragsmuster zur Verfügung, das grundsätzlich verwendet werden soll.

Die Verträge sind durch das MMKH zu prüfen, soweit nicht das unveränderte Muster der HAW Hamburg verwendet wird. Die dem Vertrag beizufügenden TOMs sind durch den IT-Sicherheitsbeauftragten zu prüfen und freizugeben. Eine Vorlage des Vertrages zur Unterzeichnung durch den*die Präsident*in erfolgt durch das Justitiariat.

VVT: Abgeschlossene Verträge sind unter „Gemeinsame Verantwortliche/ Joint Controller" abzulegen.

8.3 Weitergabe von Daten an Drittstaaten

Die Weitergabe von personenbezogenen Daten an Partner in Drittländern (außerhalb der EU bzw.
des EWR) kann für die HAW Hamburg insbesondere bei der Nutzung von digitalen Tools, Social Media, als auch bei Kooperationsstudiengängen bedeutsam sein. In diesen Fällen reicht bspw. ein Abschluss eines AVVs nicht aus. Es bedarf vielmehr weiterer Absicherungsmaßnahmen in Form von Zertifizierungen oder Standardvertragsklauseln (gem. Art. 40 f. DSGVO). Standardvertragsklauseln bestimmen die Anwendbarkeit der DSGVO für die jeweilige Vertragsbeziehung mit dem Partner aus einem Drittland.

Aufgrund der Rechtsprechung des Europäischen Gerichtshofs (EuGH) wird derzeit in vielen Fällen eine Weiterleitung von personenbezogenen Daten in Drittländer datenschutzrechtlich bedenklich sein, insbesondere in Staaten wie die USA.

Es ist daher der*die Datenschutzkoordinator*in einzubinden.

VVT: Abgeschlossene Verträge sind unter „Datenübermittlung an Dritte außerhalb der EU" abzulegen.

9. Verantwortlichkeiten / Akteure

9.1 Verantwortlichkeit der HAW Hamburg

Die HAW Hamburg ist als Körperschaft des öffentlichen Rechts verantwortlich für die Einhaltung der datenschutzrechtlichen Bestimmungen. Damit obliegt es formal dem Präsidium sicherzustellen, dass die gesetzlichen und die in der DSGVO enthaltenen Anforderungen an den Datenschutz berücksichtigt werden.

9.2 Verantwortung der einzelnen Organisationseinheiten

Die Umsetzung der datenschutzrechtlichen Vorgaben liegt in der Verantwortung der für den jeweiligen Prozess zuständigen Mitarbeiter*innen.

9.3 Datenschutzkoordinator*in

Für die Koordination der datenschutzrechtlichen Belange ist die*der Datenschutzkoordinator*in erste Ansprechperson. Die*der Datenschutzkoordinator*in berät hinsichtlich des Weiteren Vorgehens und koordiniert den Einsatz der weiteren Akteure.

Die*der Datenschutzkoordinator*in ist insbesondere erste Ansprechperson bei

- Vorabkontrollen: vor der Einführung neuer Prozesse/Verfahren sind diese vorab datenschutzrechtlich zu bewerten. Die Bewertung erfolgt nach Rücksprache mit der*dem Datenschutzkoordinator*in durch das MMKH und/oder die datenschutz nord GmbH;
- Dokumentation (VVT)
- Durchführung von Datenschutz-Folgenabschätzungen
- Prüfung von datenschutzrechtlichen Verträgen
- Bearbeitung von Betroffenenanfragen

9.4 Datenschutzmultiplikator*innen

Um die Anforderungen des Datenschutzes an der HAW Hamburg weiterzuentwickeln und bei Bedarf anzupassen, sollen Multiplikator*innen zur Umsetzung und Weiterentwicklung des Datenschutzes in den verschiedenen Bereichen eingesetzt werden.

Diese sollen perspektivisch die*den Datenschutzkoordinator*in unterstützen und einzelne Aufgaben übernehmen sowie eine Schnittstellenfunktion zum MMKH übernehmen.

9.5 Informationssicherheitsbeauftragte*r

Die*der (behördliche) Informationssicherheitsbeauftragte*r ist mit seinen*ihren Aufgaben in der Informationssicherheitsleitlinie der Freien und Hansestadt Hamburg (IS-LL) verankert. Die für den Datenschutz wesentlichen Aufgaben umfassen:

- Beratung der Datenschutzkoordinator*innen (bzgl. der betreuten VVTs), des Datenschutzbeauftragten, des ITSC sowie des Präsidiums in Fragen der Informationssicherheit;
- Beratung bei Ausschreibungen, die datenschutzrelevante Verfahren betreffen, um bereits durch die Erstellung der Ausschreibungsunterlagen die Eignung technischer und organisatorischer Maßnahmen besser gewährleisten zu können;
- Bewertung der grundsätzlichen Eignung technischer und organisatorischer Maßnahmen zur Gewährleistung des Datenschutzes;

- Information der Datenschutzkoordinator*innen sowie des ITSC über konkrete Sicherheitsvorfälle, die den Datenschutz trotz umgesetzter technischer und organisatorischer Maßnahmen gefährden können.

9.6 Multimediakontor Hamburg (MMKH)

Das MMKH ist eine gemeinsame Einrichtung der sechs staatlichen Hamburger Hochschulen.

Das MMKH unterstützt die HAW Hamburg in allen datenschutzrelevanten Themen. Sei es bei allgemeinen Themen, wie der Erstellung von Datenschutzhinweisen, dem Prüfen von Verträgen oder von Rechtsgrundlagen, als auch bei individuellen projektbezogenen Anliegen. Hierbei handelt es sich nicht um eine klassische Rechtsberatung, sondern vielmehr um eine Begleitung der Hochschulen in Datenschutzfragen, um etwaige Datenschutzrisiken aufzuzeigen, Empfehlungen auszusprechen und damit eine Entscheidungsfindung zu erleichtern. Nach den geltenden Regelungen der DSGVO muss eine Hochschule als Verantwortliche für die jeweiligen Datenverarbeitungsprozesse die abschließende Entscheidung und Risikoabwägung eigenständig vornehmen.

Die Organisationseinheiten können sich bei Fragen zum Datenschutz direkt an das Team des MMKHs wenden. Der*die Datenschutzkoordinator*in ist bei einer Erstanfrage in CC zu setzen und über das Ergebnis einer Anfrage zu informieren. Damit eine Erstanfrage zeitsparend gelingt, stellt das MMKH einen online Fragebogen zur Verfügung, welcher ausgefüllt direkt an das MMKH-Team gesandt werden kann. Den Fragebogen erreichen Sie unter: [URL wird ergänzt]. Das Team können Sie darüber hinaus gern auch direkt kontaktieren, unter datenschutz@mmkh.de.

9.7 behördlicher Datenschutzbeauftragter

Die datenschutz nord GmbH ist externer behördlicher Datenschutzbeauftragter gemäß Art. 39 EU-DSGVO.

Anlage 1: typische Rechtsgrundlagen im Hochschulkontext

- EU-Datenschutzgrundverordnung (DSGVO), insbesondere Art. 6, 9, 88 DSGVO
- Bundesdatenschutzgesetz (BDSG), insbesondere § 26
- Hamburgisches Hochschulgesetz (HmbHG), insbesondere § 111 HmbHG
- Hamburgisches Datenschutzgesetz (HmbDSG), insbesondere §§ 11, 12 HmbDSG
- Hamburgisches Archivgesetz (HmbArchG)
- Hamburgisches Statistikgesetz (HmbStatG)
- Hamburgisches Beamtengesetz (HmbBG)
- Satzungen der HAW Hamburg, insbesondere über die Verarbeitung personenbezogener Daten.

Satzungen der HAW Hamburg sind unter folgendem Link abrufbar: HAW Hamburg: Gesetze, Verordnungen, Satzungen (haw-hamburg.de)