

## **Inhalt**

- A. Vorbemerkungen
- B. Begriffsbestimmungen
- C. Rechtliche Grundlagen
- D. Ziel der Verfahrensbeschreibung und Abgrenzung
- E. Inhalt und Form der Verfahrensbeschreibung
- F. Verantwortlichkeit für die Erstellung der Verfahrensbeschreibungen
- G. Zeitpunkt der Erstellung
- H. Übermittlung der Verfahrensbeschreibung an die Datenschutzbeauftragten
- I. Einsichtnahme in die Verfahrensbeschreibungen
- J. Ausfüllhinweise

## **A. Vorbemerkungen**

Das Hamburgische Datenschutzgesetz ([HmbDSG](#)) regelt die Verarbeitung personenbezogener Daten durch öffentliche Stellen, um das Recht einer jeden Person zu schützen, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen, soweit keine Einschränkungen im HmbDSG oder in anderen, speziellen Rechtsvorschriften (z.B. Hamburgisches Hochschulgesetz ([HmbHG](#))) zugelassen sind.

Um die Rechtmäßigkeit und die Transparenz der vielfältigen Datenverarbeitungen zu gewährleisten, hat der Gesetzgeber mit dem HmbDSG den öffentlichen Stellen der Freien und Hansestadt Hamburg (FHH) – und somit auch den 6 öffentlichen Hamburger Hochschulen und der Staats- und Universitätsbibliothek Hamburg (SUB) – konkrete Vorgaben gemacht, die vielfach

bereits seit mehr als 20 Jahren gelten. Ziel dieser Rechtsnormen ist es, die Transparenz der Verarbeitungsprozesse von personenbezogenen Daten und deren Sicherheit zu gewährleisten und damit das im Grundgesetz verankerte informationelle Recht auf Selbstbestimmung der Betroffenen (Studierende, Mitarbeiter, Kunden, ...) sicherzustellen.

Etwas unbürokratischer und anschaulicher könnte formuliert werden: Als Mitarbeiterinnen und Mitarbeitern der Hochschulen und der Staatsbibliothek werden uns vielfältige, personenbezogene Daten von Dritten anvertraut, um sie im Rahmen unserer öffentlichen Aufgaben und Geschäftsprozesse zu verarbeiten. Diese Dritten (Betroffene) haben einen Anspruch darauf, dass wir mit ihren Daten sorgsam, sensibel und verantwortungsbewusst umgehen und jeglichen Missbrauch verhindern. Um diese Zielvorgaben zu erfüllen, haben wir die konkreten Rechtsgrundlagen in klaren Zweckbestimmungen zu dokumentieren, transparente Verarbeitungsprozesse (einschl. Löschen / Sperren von Daten) zu definieren sowie konkrete technisch-organisatorische Maßnahmen („TOM's“) zum Schutz der Daten einzurichten.

Der Gesetzgeber fordert die Daten verarbeitenden Stellen in den §§ 8 und 9 HmbDSG auf, bereits vor Einführung des automatisierten Verfahrens, die Verfahrensprozesse und ihre Sicherheitsaspekte zu beschreiben und zu bewerten, sofern personenbezogene Daten verarbeitet werden. Vielfach haben sich die Hochschulleitungen auch gegenüber Ihren Personalräten in (Rahmen-)Dienstvereinbarungen verpflichtet, diese gesetzlichen Grundlagen umzusetzen und einzuhalten.

## **B. Begriffsbestimmungen**

### **Personenbezogene Daten...**

sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (siehe auch § 4 HmbDSG – Begriffsbestimmungen). Damit sind alle Angaben über persönliche und sachliche Verhältnisse gemeint, die über eine lebende natürliche Person etwas aussagen, unabhängig davon, in welcher technischen Form (z.B. Bildaufnahme) dies geschieht. Der Begriff hält die Einbeziehung neuer technischer Verfahren in das Gesetz offen. Bestimmbar ist eine Person auch dann, wenn nur unter Verwendung eines Zusatzwissens der Personenbezug hergestellt werden kann, aber immer nur für diejenige Stelle, die selbst über das erforderliche Zusatzwissen verfügt oder verfügen kann.

Zu den personenbezogenen Daten zählen alle Informationen, die die Person selbst beschreiben (z.B. Name, Geschlecht, Alter, Religionszugehörigkeit, Familienstand, Ausbildung); es muss sich also nicht um sensible Daten (siehe auch § 5 Abs. 2 HmbDSG) handeln.

### **Datenverarbeitung...**

ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten. Im Einzelnen ist

1. Erheben das Beschaffen von Daten über Betroffene,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern das inhaltliche Umgestalten von Daten,
4. Übermitteln das Bekanntgeben von Daten an Dritte in der Weise, dass die Daten weitergegeben, zur Einsicht bereitgehalten oder veröffentlicht werden oder dass Dritte in einem automatisierten Verfahren bereitgehaltene Daten abrufen,
5. Sperren das Verhindern weiterer Verarbeitung von Daten,
6. Löschen das Unkenntlichmachen von Daten oder das Vernichten des Datenträgers,
7. Nutzen jede sonstige Verwendung von Daten ungeachtet der dabei angewendeten Verfahren.

### **Daten verarbeitende Stellen...**

im rechtlichen Sinn des § 2 Abs. 1 HmbDSG ist die die jeweilige Hochschule / Universität bzw. die SUB vertreten durch das Präsidium/Direktorium. Als eigenständige Daten verarbeitende Stellen sind – bei Zugrundelegung des sogenannten funktionalen Behördenbegriffs, wie er vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit interpretiert wird – allerdings auch die jeweiligen Personalräte und die sogenannte verfasste Studierendenschaft (AStA / Studierendenparlament) zu benennen. Sie handeln aufgrund spezieller, eigener Rechtsgrundlagen.

Im Zusammenhang mit dem Erstellen von Verfahrensbeschreibungen ist ferner der Begriff fachverantwortliche Stelle von den gemeinsamen Datenschutzbeauftragten geprägt worden. Dies ist regelhaft die Stelle der jeweiligen Institution, der vom Präsidium / Direktorium die organisatorische Zuständigkeit für die Datenverarbeitung übertragen wurde.

## **Verfahren**

Der Begriff des Verfahrens ist nicht programmtechnisch zu verstehen, sondern vielmehr unter dem Gesichtspunkt von organisatorischen Arbeitsabläufen und Zuständigkeiten (z.B. Studierendenverwaltung, Prüfungsverwaltung, Lehrgangsplanung, Personalverwaltung, Forschungsprojekt „xyz“, etc.). Verfahren können dabei mehrere Softwareprogramme und eine ganze Reihe von Dateien beinhalten.

Umgekehrt kann aber beispielsweise eine einheitliche softwaretechnische Grundlage (z.B. CampusNet, HIS in One) von mehreren eigenständigen Verfahren (Studierendenverwaltung, Prüfungsverwaltung, Raumplanung, ...) genutzt werden.

## **Automatisiertes Abrufverfahren**

Den Verfahren zur automatisierten Direktabfrage von personenbezogenen Datenbeständen (Online-Anschlüsse) als Informationsaustausch kommt unter dem Aspekt des Datenschutzes besondere Bedeutung zu, weil die abrufende Stelle nach Einrichtung eines solchen Anschlusses über den gesamten Bestand der von der Daten verarbeitenden Stelle bereitgehaltenen Daten verfügen kann. Die mögliche Übermittlung einer sehr umfangreichen Anzahl personenbezogener Daten birgt erhebliche Gefahren für das Recht auf informationelle Selbstbestimmung in sich. Aus diesem Grund und wegen der besonderen Risiken der Online-Anschlüsse wird die Einrichtung solcher Verfahren an besondere Zulässigkeitsvoraussetzungen gebunden.

Nach § 11 Abs. 1 HmbDSG ist bei den Hochschulen und der Staatsbibliothek die Einrichtung derartiger automatisierter Abrufverfahren prinzipiell nur auf der Grundlage ausdrücklicher Rechtsvorschriften zugelassen; die Einrichtung solcher Verfahren wird nicht dem Ermessen und der Einzelabwägung der beteiligten Hochschulen überlassen. Die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist vorher zu hören. Nicht betroffen sind dagegen Online-Anschlüsse, mit denen nicht personenbezogene (z.B. statistische) Einzeldaten übermittelt werden. § 11 Abs. 1 HmbDSG findet ferner keine Anwendung auf diejenigen Fälle, in denen Hochschulen als Auftrag gebende Stellen im Rahmen der Auftragsdatenverarbeitung ihre personenbezogenen Datenbestände bei Auftrag nehmenden Stellen (z.B. externen Rechenzentren) abrufen.

Es bedarf keiner besonderen Erwähnung durch den Gesetzgeber, dass automatisierte Abrufverfahren nur in Betrieb genommen werden dürfen, wenn vorher die technischen und organisatorischen Maßnahmen nach § 8 HmbDSG sowohl bei der übermittelnden Stelle als auch bei den Stellen, denen die Daten übermittelt werden, getroffen sind.

§ 11 Abs. 3 HmbDSG berücksichtigt wegen der gleichen Interessenlage die Einrichtung automatisierter Abrufverfahren innerhalb einer Hochschule / der Staatsbibliothek für den Fall, dass die übermittelnde Einheit und die Einheit, der die Daten übermittelt werden, unterschiedliche Aufgaben wahrnehmen. Die Zulassung erfolgt unter den gleichen Voraussetzungen wie beim Abruf durch Dritte, doch tritt an die Stelle einer Rechtsverordnung des Senats ein innerdienstlicher Organisationsakt der Hochschulleitung / des Direktoriums. Auch hier ist die bzw. der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit vorher zu hören.

Nach § 11 Abs. 4 HmbDSG sind automatisierte Abrufverfahren nicht zulässig im Verhältnis der Hochschulen / der Staatsbibliothek zu Stellen außerhalb des öffentlichen Bereichs. Privaten Stellen soll kein unmittelbarer Zugriff auf Datenbanken der öffentlichen Verwaltung mit personenbezogenem Inhalt ermöglicht werden. Dies gilt nicht in den Fällen, in denen die Betroffenen ihre eigenen Daten abrufen können.

Wenn die Daten verarbeitende Stelle die Daten veröffentlichen dürfte oder es sich um einen Anschluss an Datenbestände handelt, die jedem ohne oder nach besonderer Zulassung offen stehen, bestehen gegen automatisierte Abrufverfahren ebenfalls keine Bedenken; in diesen Fällen kommen die Absätze 1 bis 4 des § 11 HmbDSG nicht zur Anwendung.

### **Gemeinsame und verbundene automatisierte Dateien**

Mit dem § 11 a HmbDSG werden rechtliche Rahmenbedingungen für die Institutionsübergreifende Datenverarbeitung aus gemeinsamen oder verbundenen automatisierten Dateien festgelegt. Die Gefährdungslage bezüglich der informationellen Selbstbestimmung und damit der Regelungsbedarf verdichten sich in den Fällen, in denen mehrere Stellen in einem automatisierten Verfahren lesend (Abruf) und schreibend (Eingabe, Veränderung, Löschung) unmittelbar auf einen Datenbestand zugreifen können, der entweder als gemeinsame (zentrale) Datei oder als Dateienverbund konzipiert ist. Diese Fälle sind dadurch gekennzeichnet, dass der Datenbestand ohne zentrale Kontrolle durch eine bestimmte Daten verarbeitende Stelle von allen angeschlossenen Stellen unmittelbar bedient werden kann und dass die eingebende Stelle keine Kontrolle darüber hat, wer eine von ihr eingegebene Information abrufte. Neben dem Umfang der Verarbeitungsbefugnis der einzelnen beteiligten Stellen sind hier vor allem die datenschutzrechtlichen Verantwortlichkeiten gegenüber den Betroffenen zu regeln und zu bestimmen, welche Stelle die technischen und organisatorischen Maßnahmen zur Daten- und IT-Sicherheit trifft.

Bereichsspezifische Beispiele für Regelungen über gemeinsame Dateien finden sich in Hamburg u.a. in § 111 Abs. 4 Hamburgisches Hochschulgesetz (HmbHG).

§ 11 a HmbDSG orientiert sich in Aufbau und Inhalt an §11 HmbDSG (Automatisiertes Abrufverfahren). Danach bedarf die Einrichtung der näher bezeichneten automatisierten Dateien, in oder aus denen mehrere hamburgische öffentliche Stellen personenbezogene Daten verarbeiten dürfen, der ausdrücklichen Zulassung durch eine Rechtsvorschrift. In einer Parallele zu §11 Absatz 2 Satz 1 HmbDSG wird der Senat ermächtigt, die Einrichtung solcher Dateien durch Rechtsverordnung zuzulassen. Auch hier wird die obligatorische Beteiligung der oder des HmbBfDI festgeschrieben.

§ 11 a Abs. 2 HmbDSG regelt in Anlehnung an §11 Absatz 3 HmbDSG den Fall, dass gemeinsame oder verbundene Dateien innerhalb einer öffentlichen Stelle zwischen Einheiten mit unterschiedlichen Aufgaben eingerichtet werden sollen. Die Zulässigkeitsvoraussetzungen sind die gleichen wie beim externen Verbund, nur entfällt hier das Erfordernis einer Rechtsvorschrift. Analog dem Vorgehen aus § 11 HmbDSG erfolgt auch hier die Zulassung durch die Leiterin oder den Leiter der Daten verarbeitenden Stelle nach Ziff. 1.1 der Verfahrensbeschreibung.

### **C. Rechtliche Grundlagen**

Eine Verfahrensbeschreibung ist - mit 2 Ausnahmen die der Gesetzgeber vorgesehen hat - nach § 9 Abs. 1 HmbDSG für jedes automatisierte Verfahren mit dem personenbezogene Daten verarbeitet werden vor seiner Inbetriebnahme zu erstellen. Dies gilt unabhängig von der Art und der Sensibilität der Daten. Verfahrensbeschreibungen sind zudem laufend auf neuestem Stand zu halten.

#### **§ 9 Abs. 1 HmbDSG - Verfahrensbeschreibung**

Die Daten verarbeitende Stelle legt in einer laufend auf dem neuesten Stand zu haltenden Verfahrensbeschreibung für jedes automatisierte Verfahren, mit dem personenbezogene Daten verarbeitet werden sollen, fest

1. den Namen und die Anschrift der Daten verarbeitenden Stelle,
2. die Bezeichnung des Verfahrens und seine Zweckbestimmungen,
3. die Art der verarbeiteten Daten sowie die Rechtsgrundlage ihrer Verarbeitung oder die Ziele, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
4. den Kreis der Betroffenen,

5. die Empfängerinnen oder Empfänger oder den Kreis der Empfängerinnen und Empfänger, die Daten erhalten können,
6. eine beabsichtigte Datenübermittlung nach § 17 Absätze 2 und 3,
7. Fristen für die Sperrung und Löschung der Daten,
8. die technischen und organisatorischen Maßnahmen nach § 8,
9. die Art der Geräte, die Stellen, bei denen sie aufgestellt sind sowie das Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung.

Die Daten verarbeitende Stelle kann die Angaben nach Satz 1 für mehrere gleichartige Verfahren in einer Verfahrensbeschreibung zusammenfassen.

Die Verfahrensbeschreibung muss nach § 9 Abs. 2 HmbDSG jedoch nicht erstellt werden, für Verfahren,

1. deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht,
2. die der Unterstützung der allgemeinen Bürotätigkeit dienen, insbesondere Verfahren der Textverarbeitung, Vorgangsverwaltung, Terminüberwachung und der Führung von Adress-, Telefon- und vergleichbaren Verzeichnissen, soweit sie keine Beeinträchtigung der Rechte Betroffener erwarten lassen. Eine solche Beeinträchtigung droht z.B., wenn sensitive Daten im Sinne des § 5 Abs. 1 Satz 2 HmbDSG Gegenstand der Verarbeitung sind.

Für Verfahren der allgemeinen Bürokommunikation müssen damit keine Verfahrensbeschreibungen erstellt werden. Diese Verfahren lassen auch im Allgemeinen keine Gefährdung des Rechts auf informationelle Selbstbestimmung erwarten. Wenn jedoch im konkreten Anwendungsfall Anhaltspunkte für mögliche Gefährdungen dieses Rechts bestehen, ist auch für Verfahren der allgemeinen Bürokommunikation eine Verfahrensbeschreibung zu erstellen.

Die Zuordnung eines Verfahrens zur allgemeinen Bürokommunikation oder zu den Verfahren, für die eine Verfahrensbeschreibung zu erstellen ist, muss am Einzelfall vorgenommen werden. Auch mit Software, die mit der allgemeinen Bürokommunikation zur Verfügung gestellt wird (z.B. MS-Excel oder MS-Word), lassen sich Verfahren unterstützen, für die eine Verfahrensbeschreibung erstellt werden muss. Ein entscheidendes Zuordnungskriterium ist u.a., ob das eingesetzte Verfahren an praktisch allen Büroarbeitsplätzen genutzt werden könnte. In diesem Fall werden in der Regel keine zusätzlichen Datenfelder z.B. über eine reine Adressverwaltung

hinaus angelegt. Wenn jedoch für den speziellen Anwendungsfall zusätzliche personenbezogene Datenfelder angelegt und genutzt werden, ist dies ein Indiz, dass eine Erstellungspflicht bestehen kann, da in diesem Fall eine Gefährdung des Rechts auf informationelle Selbstbestimmung bestehen könnte.

#### **D. Ziel der Verfahrensbeschreibung und Abgrenzung**

Verfahrensbeschreibungen dienen dem Ziel, die Öffentlichkeit über Art und Umfang von automatisierten Verarbeitungen personenbezogener Daten zu unterrichten. Dieses Informationsrecht ergibt sich aus Artikel 21 Abs. 3 der EG-Datenschutzrichtlinie. § 9 Abs. 3 Satz 2 HmbDSG legt fest, dass die Verfahrensbeschreibungen von jeder Person eingesehen werden können. Der Personenkreis, die Einsicht nehmen können ist, nicht auf den Kreis der Betroffenen beschränkt.

Das Ziel der Öffentlichkeitsinformation ist damit auch Maßstab für den Umfang und den Detaillierungsgrad der Verfahrensbeschreibung. Die Punkte 2, 3 und 5 der Verfahrensbeschreibung können auch genutzt werden, wenn Betroffene ihr Auskunftsrecht nach § 18 HmbDSG geltend machen.

Verfahrensbeschreibungen bilden für die Daten verarbeitenden Stellen zugleich ein Instrument der Selbstkontrolle, z.B. bei der Festlegung von Sperrungs- und Lösungsfristen.

Die Verfahrensbeschreibung ist klar von einer Verfahrens- oder Projektdokumentation abzugrenzen. Während die Verfahrensbeschreibung der Öffentlichkeitsinformation dient und einen Überblick über das Verfahren gewährleistet, enthält die Verfahrensdokumentation alle zum Verständnis und zur Abwicklung eines automatisierten Verfahrens notwendigen Informationen. Die Dokumentation gibt über die aktuellen Arbeitsabläufe, Regeln und Programme des Verfahrens Auskunft und dient sowohl der Pflege als auch der Prüfung von automatisierten Verfahren. Derartig detaillierte Informationen sind in einer Verfahrensbeschreibung nicht enthalten.

#### **E. Inhalt und Form der Verfahrensbeschreibung**

Die Inhalte, die in die Verfahrensbeschreibung aufzunehmen sind, sind im § 9 Abs. 1 Satz 1 HmbDSG festgelegt. Die Verfahrensbeschreibung sollte aus sich heraus verständlich sein und



kein besonderes Vorwissen oder spezifische Kenntnisse voraussetzen. Abkürzungen sollten möglichst allgemeinverständlich erläutert werden.

Die Form der Verfahrensbeschreibung ist nicht vorgeschrieben. Eine übersichtliche Darstellung, etwa in Form einer Tabelle bzw. eines einheitlichen Formulars, erleichtert der Öffentlichkeit den Informationszugang. Das Muster des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ([HmbBfDI](#)) wurde von uns im Hinblick auf die organisatorischen Bedürfnisse der Hochschulen angepasst.

Zu einzelnen Inhalten kann ggf. auf bereits erstellte Dokumente (siehe u.a. auch der Hinweis auf möglicherweise vorhandene Leit- und Richtlinien in Ziffer 8 des Formulars (Ankreuzfelder)) verwiesen werden. In diesem Fall sollten die Dokumente in den Anhang der Verfahrensbeschreibung aufgenommen werden. Der Verweis auf einen Anhang bietet sich insbesondere an für die Beschreibung der technischen und organisatorischen Maßnahmen nach § 8 HmbDSG und für die Beschreibung der Art der Geräte, der Stellen, bei denen sie aufgestellt sind sowie für das Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung. Das Informationsrecht für die Öffentlichkeit besteht zu diesen Inhalten nur, soweit die Sicherheit des Verfahrens durch die Einsichtnahme nicht beeinträchtigt wird.

Häufig erhöht jedoch bereits eine überblicksartige Veröffentlichung derartiger Informationen das Risiko, dass ein IT-Verfahren angegriffen wird. Unser Formular zur Verfahrensbeschreibung differenziert daher bewusst zwischen dem sogenannten öffentlichen Teil (§ 9 Abs. 1 Ziff. 1 – 7 HmbDSG) und dem nicht-öffentlichen Teil (Ziff. 8 und 9).

Die Entscheidung über die Veröffentlichung des nicht-öffentlichen Teils der Verfahrensbeschreibung obliegt der Daten verarbeitenden Stelle.

## **F. Verantwortlichkeit für die Erstellung der Verfahrensbeschreibungen**

Die Daten verarbeitende Stelle erstellt die Verfahrensbeschreibungen. Bei Verfahren, die in mehreren Daten verarbeitenden Stellen zum Einsatz kommen, ist eine Koordination oder ein zumindest teilweiser Verweis auf eine bereits vorhandene Beschreibung bzw. die Übernahme dieser Inhalte sinnvoll.

## **G. Zeitpunkt der Erstellung**

Die Verfahrensbeschreibung ist vor der Einführung oder wesentlichen Änderung eines Verfahrens zu erstellen. Die Beschreibung ist laufend aktuell zu halten. Zudem fordert § 19 Abs. 6 HmbDSG zu einer regelmäßigen Überprüfung der Erforderlichkeit im Abstand von 4 Jahren auf.

## **H. Übermittlung der Verfahrensbeschreibung an die Datenschutzbeauftragten**

Die Verfahrensbeschreibung ist vor der Einführung oder einer wesentlichen Änderung an die gemeinsame Datenschutzbeauftragte der Hamburger Hochschulen (UHH, HfMT, HFBK, HCU und TUHH) bzw. den behördlichen Datenschutzbeauftragten der Staats- und Universitätsbibliothek Hamburg zu übersenden.

Die Übersendung der Verfahrensbeschreibung ersetzt nicht die in § 23 Abs. 4 HmbDSG geregelte Beteiligung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Dieser ist bereits über die Planung neuer Anwendungen zur Nutzung der Informations- und Kommunikationstechnik rechtzeitig zu unterrichten, sofern personenbezogene Daten verarbeitet werden sollen.

## **I. Einsichtnahme in die Verfahrensbeschreibungen**

Die Verfahrensbeschreibungen können bei der Daten verarbeitenden Stelle von jeder Person eingesehen werden. Für Angaben nach § 9 Abs. 1 Nummer 8 und 9 HmbDSG gilt dies nur, soweit die Sicherheit des Verfahrens nicht beeinträchtigt wird. Neben den Daten verarbeitenden Stellen halten die behördlichen Datenschutzbeauftragten, hier also die gemeinsame Datenschutzbeauftragte der Hamburger Hochschulen UHH, HfMT, HFBK, HCU und TUHH, bzw. der Datenschutzbeauftragte der SUB, die Verfahrensbeschreibungen zur Einsicht bereit.

Es bleibt den Daten verarbeitenden Stellen überlassen, die Verfahrensbeschreibungen (ggf. auch nur den öffentlichen Teil) aus Transparenzgründen zusätzlich im Intranet und/oder Internet zu veröffentlichen. Eine gesetzliche Verpflichtung hierzu besteht nicht. Als gemeinsame Datenschutzbeauftragte begrüßen wir die Bestrebungen der öffentlichen Verwaltung zu mehr Transparenz zu gelangen (Stichworte: OpenData und OpenGovernment) und empfehlen dies auch den von uns betreuten Hochschulen bzw. der Staats- und Universitätsbibliothek Ham-

burg. Zudem erleichtert eine zumindest hochschulinterne Veröffentlichung von Verfahrensbeschreibungen das Erstellen von weiteren Verfahrensbeschreibungen in anderen Fachbereichen und liefert anschauliche Informationen über „wie mache ich es“. Anzumerken bleibt aber auch, dass das gerade verabschiedete Hamburgische Transparenzgesetz nach unserer Lesart keine Veröffentlichung der Verfahrensbeschreibungen vorschreibt.

## **J. Ausfüllhinweise**

### zum Vorblatt (Seite 1 des Formulars Verfahrensbeschreibung)

- Bezeichnung des Verfahrens

Verwenden Sie einen möglichst sprechenden Begriff der das Verfahren präzise und konkret beschreibt (z.B. Prüfungsverwaltung der Fakultät xyz, Personalaktenverwaltung, Bewerbungsverfahren, etc.). Bitte verwenden Sie dieselbe Bezeichnung wie unter Punkt 2.1 der Verfahrensbeschreibung.

- Daten verarbeitende Stelle

Im Rahmen der Kooperationsvereinbarung zum hochschulübergreifenden Datenschutz sind die auf Seite 1 des Formulars Verfahrensbeschreibung genannten Institutionen als Daten verarbeitende Stellen nach § 2 Abs. 1 HmbDSG zu definieren.

Eigenständige Daten verarbeitende Stellen im rechtlichen Sinne sind die jeweiligen Mitarbeitervertretungen sowie bei den Hochschulen die sogenannte verfasste Studierendenschaft. Abhängig von der konkreten vertraglichen Ausgestaltung kann im Einzelfall auch ein einzelnes Forschungsprojekt als eigenständige Daten verarbeitende Stelle anzusehen sein. Siehe auch Pkt. B dieser Handreichung. Die Daten verarbeitende Stelle ist anzukreuzen bzw. im Freitextfeld anzugeben (beispielweise bei den Personalräten und Asten).

- Neue Verfahrensbeschreibung / Änderung/Ergänzung

Sofern die Verfahrensbeschreibung erstmals erstellt wird handelt es sich um eine „Neue Verfahrensbeschreibung“. Bei Verfahrensaktualisierungen, beispielsweise aufgrund einer Migration auf neue IT-Technik, der Implementierung einer neuen Verfahrensschnittstelle oder der Erhebung zusätzlicher personenbezogener Daten ist das Feld „Änderung/Ergänzung“ anzukreuzen.

- Sammelbeschreibung  
Auf die Begriffsbestimmungen unter Pkt. B wird hingewiesen. Nach § 9 Abs. 1 Satz 2 HmbDSG kann die Daten verarbeitende Stelle die erforderlichen Angaben für mehrere gleichartige Verfahren in einer Verfahrensbeschreibung zusammenfassen. Eine Sammelbeschreibung kommt in Betracht, wenn
  - a) innerhalb einer Stelle mehrere Benutzer gleiche oder gleichartige Verfahren nutzen (z. B. gleiche Anwendungen auf mehreren PC),
  - b) mehrere fachverantwortliche Stellen bei einer Daten verarbeitenden Stelle (im Sinne von Pkt. 1.1 der Verfahrensbeschreibung) gleiche Verfahren nutzen (z. B. Verfahren zur Evaluation, zum eLearning, etc.). Wird die Sammelbeschreibung nicht von der Daten verarbeitenden Stelle selbst erstellt, so sind in der Verfahrensbeschreibung der Auftragnehmer und (in einer zusätzlichen Liste) alle Daten verarbeitenden Stellen anzugeben.
  
- Einsichtnahme  
Die Verfahrensbeschreibung ist auf Antrag jeder Person zur Einsichtnahme vorzulegen. Der Antrag ist an keine Formvorschriften gebunden. Es reicht aus, bei der Daten verarbeitenden Stelle bzw. der / dem Datenschutzbeauftragten zu erscheinen und um Einsicht zu bitten. Der Gesetzgeber hat es in § 9 Abs. 3 HmbDSG jedoch den Daten verarbeitenden Stelle überlassen, ob die gesamte Verfahrensbeschreibung einschließlich der IT-technischen Sicherheitsaspekte (von uns als nicht-öffentlicher Teil bezeichnet) vorgelegt wird oder lediglich die Punkte 1 bis 7 der Verfahrensbeschreibung (öffentlicher Teil). Die Entscheidung trifft die fachverantwortliche Stelle (Punkt 1.2 der Verfahrensbeschreibung). Das Auswahlkästchen für die eingeschränkte Veröffentlichung (nur der sogenannte öffentliche Teil) auf Antrag ist im Formular als Standard aktiviert.
  
- Automatisiertes Abrufverfahren  
Besondere Rechtsgrundlagen (hier: § 11 HmbDSG) gelten für Verfahren, aus denen personenbezogene Daten automatisiert abgerufen werden, sofern diese nicht Datenbestände betreffen, die jeder oder jedem zur Benutzung offenstehen oder deren Veröffentlichung zulässig wären (z.B. Bibliothekskataloge, die jedermann im Internet benutzen kann, aber auch gebührenpflichtige Datenbanken, zu denen jeder Zugang hat, soweit er die Gebühren bezahlt). Hinsichtlich der weiteren Rechtsgrundlagen wird auf Pkt. B dieser Handreichung verwiesen.  
Bitte kreuzen Sie ggf. an ob es sich um ein automatisiertes Abrufverfahren durch Dritte oder um ein automatisiertes Abrufverfahren innerhalb der Daten verarbeitenden Stelle nach Ziff. 1.1. der Verfahrensbeschreibung handelt.

- Gemeinsame verbundene automatisierte Dateien

In § 11 a HmbDSG werden rechtliche Rahmenbedingungen für die Datenverarbeitung aus gemeinsamen oder verbundenen automatisierten Dateien festgelegt. Hinsichtlich der weiteren Rechtsgrundlagen wird auf Pkt. B dieser Handreichung verwiesen.



Bitte kreuzen Sie bei Bedarf an ob es sich bei dem beschriebenen Verfahren um einen Teil eines gemeinsamen oder verbundenen Verfahrens handelt in oder aus denen mehrere auch externe Daten verarbeitende Stellen personenbezogene Daten verarbeiten sollen (§ 11 a Abs. 1 HmbDSG), oder ob es sich ggf. um einen Teil eines gemeinsamen oder verbundenen Verfahrens handelt mit denen personenbezogene Daten innerhalb der Daten verarbeitenden Stelle nach Ziff. 1.1 der Verfahrensbeschreibung aus unterschiedlichen Aufgabengebieten verarbeiten werden sollen (§ 11 a Abs. 2 HmbDSG).

#### Zu Ziffer 1

- Rechtlich verantwortliche Stelle nach § 2 Abs. 1 HmbDSG ist die jeweilige Hochschulleitung bzw. das Direktorium der Staats- und Universitätsbibliothek Hamburg. Ferner ggf. die Personalräte und Asten der vorstehend genannten Institutionen. Anzugeben sind hier der Name der Institution und die Anschrift.
- Fachverantwortliche Stelle(n) sind die jeweiligen Einrichtungen der Institution der die organisatorische Zuständigkeit für die in Rede stehenden Datenverarbeitungen übertragen wurden. Ggf. sind hier auch mehrere Stellen aufzuführen. Aus Gründen der Transparenz sollte in diesen Fällen eine kurze Aufgabenabgrenzung dargestellt werden. Anzugeben sind hier der Name der fachlich /organisatorisch zuständigen Stelle und die Anschrift.

#### Zu Ziffer 2.1

- Verwenden Sie einen möglichst sprechenden Begriff der das Verfahren präzise und konkret beschreibt (z.B. Prüfungsverwaltung der Fakultät xyz, Personalaktenverwaltung, Bewerbungsverfahren, etc.). Identischer Eintrag zur „Bezeichnung des Verfahrens“ auf Seite 1 der Verfahrensbeschreibung.
- Beschreiben Sie die Inhalte des (Fach-)Verfahrens mit kurzen Sätzen. Denken Sie daran, dass die Verfahrensbeschreibung in erster Linie zur Information der Öffentlichkeit bestimmt ist, also auch ohne detaillierte Fachkenntnisse verständlich sein sollte. Die Datenverarbeitungsprozesse im Hinblick auf die personenbezogenen Daten stehen dabei im Focus.

- Sofern Verknüpfungen bzw. Abhängigkeiten zu anderen Verfahren bestehen (z.B. Schnittstellen, manuelle und technische Datenübermittlung, etc.) sind diese Verfahren zu benennen. Verwenden Sie nach Möglichkeit die dort verwendete Kurzbezeichnung des Verfahrens.
- Im Rahmen der Verfahrens-Kurzbeschreibung (Ziff. 2.1.1) und der Verfahrensabhängigkeiten (Ziff. 2.1.2) haben wir bereits konkrete Hinweise zur Berücksichtigung der Bestimmungen des Hamburgischen Archivgesetzes ([HmbArchG](#) ) in das Musterformular aufgenommen. Unabhängig von der Frage der Verarbeitung personenbezogener Daten sind (fast) sämtliche Dokumente / Daten der Hochschulen / Universitäten vor einer Löschung / Vernichtung dem Staatsarchiv Hamburg zwecks Prüfung ihrer Archivwürdigkeit anzubieten. Selbstverständlich ist es den Daten verarbeitenden Stellen freigestellt, hier eigene Formulierungen zu verwenden. Die Formulierung kann entfallen, sofern das Staatsarchiv Hamburg im jeweiligen Einzelfall eine Archivwürdigkeit der in Rede stehenden personenbezogenen Daten grundsätzlich verneint hat (siehe [§ 3 Abs. 4 HmbArchG](#) )

#### Zu Ziffer 2.2 - Zweckbestimmungen

- Der Gesetzgeber fordert in Bezug auf die Verarbeitung der personenbezogenen Daten die konkrete, präzise und abschließende Darstellung aller Zwecke. Um ein allgemein verständliches Beispiel darzustellen, das uns allen als Krankenversicherte aus dem Alltag bekannt sein dürfte, verweisen wir auf eine Darstellung der Zweckbestimmungen einer Verfahrensbeschreibung aus dem Versicherungsbereich:

Die Krankenversicherung als Solidargemeinschaft hat die Aufgabe, die Gesundheit der Versicherten zu erhalten, wiederherzustellen oder ihren Gesundheitszustand zu verbessern. Um diese Aufgaben wahrnehmen zu können, muss die Kasse Daten erheben, verarbeiten und nutzen. Für die Krankenversicherung ergibt sich die gesetzliche Grundlage aus § 284 SGB V sowie § 10 Aufwendungsausgleichgesetz (AAG), für die Pflegeversicherung bei der Krankenkasse aus § 94 SGB XI. Folgende Zwecke sind dort genannt:


- Feststellung des Versicherungsverhältnisses
- Ausstellung der Krankenversichertenkarte
- Durchführung von Beitragsangelegenheiten
- Prüfung und Gewährung von Leistungen
- Unterstützung der Versicherten bei Behandlungsfehlern
- Kostenerstattung

- Bestimmung des Zuzahlungsstatus, Ermittlung der Belastungsgrenze
- Beitragsrückerstattung
- Beteiligung des Medizinischen Dienstes
- Abrechnung mit den Leistungserbringern
- Wirtschaftlichkeits- und Qualitätsprüfung bei Leistungserbringern
- Abrechnung mit anderen Leistungsträgern
- Durchführung von Erstattungs- und Ersatzansprüchen gegenüber Dritten
- Vorbereitung, Vereinbarung und Durchführung von morbiditätsorientierten Vergütungsstrukturen
- Vorbereitung, Durchführung und Qualitätssicherung von Modellvorhaben und integrierten Versorgungsformen
- Durchführung des Risikostrukturausgleichs und des Risikopools
- Vorbereitung und Durchführung von strukturierten Behandlungsprogrammen
- Durchführung des Versorgungsmanagements
- Abschluss und Durchführung von Pflegesatzvereinbarungen, Vergütungsvereinbarungen sowie Leistungs- und Qualitätsvereinbarungen
- Beratung über Maßnahmen der Prävention und Rehabilitation
- Koordinierung pflegerischer Hilfen
- statistische Zwecke
- Aufgaben als Einzugsstelle der Sozialversicherungsbeiträge
- Gewinnen von Mitgliedern (§ 284 Abs. 4 SGB V)
- Durchführung des AAG
- Übernahme der Behandlungskosten für nicht Versicherungspflichtige (§ 264 SGB V)

Aus dem Beispiel wird der Detaillierungsgrad der vollständig darzustellenden Zweckbestimmungen deutlich. Für alle nicht aufgeführten Zwecke dürfen die verarbeiteten Daten nicht verwendet werden!

Um den Bezug zu den Hochschulen wiederherzustellen: Eine der Zweckbestimmungen der Studierendenverwaltung ist z.B. die Übermittlung bestimmter Studierendendaten an die Krankenkasse im Rahmen der Immatrikulation.

Keinesfalls sind Zweckbestimmungen zulässig wie „Unterstützung der Strafverfolgungsbehörden“, „Aufklärung von Straftaten“, da dies keine originären Aufgaben der Hochschulen / der Staatsbibliothek sind (die Behörden verfügen aber über entsprechende - im Einzelfall nachzuweisende - Rechtsgrundlagen, um auf vorhandene Daten zugreifen zu dürfen.

Als Vorgabe haben wir bereits das Anbiere-Verfahren gem. §§ 1-3 HmbArchG in das Formular aufgenommen. Selbstverständlich ist es den Daten verarbeitenden Stellen freigestellt, hier eigene Formulierungen zu verwenden. Der Textbaustein kann entfallen, sofern das Staatsarchiv Hamburg im jeweiligen Einzelfall eine Archivwürdigkeit der zugrundeliegenden personenbezogenen Daten grundsätzlich verneint hat (siehe [§ 3 Abs. 4 HmbArchG](#) .

### Zu Ziffer 3.1 – Art der verarbeiteten personenbezogenen Daten

- Personenbezogene Daten nach § 5 Abs. 1 Satz 2 HmbDSG

Besondere Sensibilität genießt die Verarbeitung von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit der Betroffenen hervorgehen, sowie von Daten über Gesundheit oder Sexualleben. Werden diese Daten verarbeitet ist das Feld anzukreuzen.

- Die verarbeiteten personenbezogenen Daten sind einzeln aufzuführen. Dabei können jedoch Datenkategorien gebildet werden (z.B.: Privatanschrift anstelle von Straße, Hausnummer, Zusatz, PLZ, Ort / Kontoverbindung anstelle von Kontonummer, BLZ, Name der Bank). Die personenbezogenen Daten sind mit einer laufenden Nummer zu versehen, da in der Folge hierauf Bezug zu nehmen ist. Der Verweis auf ein vorhandenes Dokument (als Anlage zur Verfahrensbeschreibung) ist möglich, beispielsweise weil im Rahmen der Software-Dokumentation eine Datenfeld-Übersicht bereits vorhanden ist. Diese ist aber dann auch im Rahmen eines Antrags auf Einsichtnahme mit vorzulegen.

Im Mittelpunkt der Darstellung stehen die personenbezogenen Inhaltsdaten der Betroffenen. Diese Betrachtung ergibt sich aus Zielsetzung des Gesetzgebers, mit der Verfahrensbeschreibung die Öffentlichkeit transparent zu informieren (siehe auch Punkt D



dieser Handreichung). Auf die Darstellung der ebenfalls verarbeiteten personenbezogenen Daten der zuständigen Mitarbeiterinnen und Mitarbeiter (soweit es sich um administrative Kennungen der Nutzer, Administratoren, etc. handelt) kann daher in aller Regel verzichtet werden, sofern das Verfahren nicht gerade diese Datenverarbeitungen zum Inhalt hat (z.B. zentrale Mailserver, Identity Management Systeme, usw.). Diese administrativen Daten sind ohnehin im Rahmen der durchzuführenden Vorabkontrolle nach § 8 HmbDSG zu betrachten.

#### Zu Ziffer 3.2 – Rechtsgrundlagen oder Ziele ...

- Die Verarbeitung personenbezogener Daten ist nur zulässig, soweit das HmbDSG oder eine besondere Rechtsvorschrift (z.B. HmbHG, HmbBG, HmbPersVG) über den Datenschutz sie erlaubt oder die Betroffenen eingewilligt haben. Daher sind an dieser Stelle die konkreten rechtlichen Grundlagen zu nennen.


Hierbei sind die konkreten gesetzlichen Rechtsnormen (z.B. §§, Absätze, Ziffern / Nummern) aufzuführen. Bei der Angabe von Paragraphen / Absätzen / Ziffern aus Satzungen, Grundordnungen, Dienstvereinbarungen, etc. ist ggf. auch die übergeordnete rechtliche Grundlage zu verweisen („i.V.m. = in Verbindung mit“). Sofern der Betroffene in die Datenverarbeitung eingewilligt hat sind ggf. vorhandene vertragliche Grundlagen (z.B. Benutzungsordnung bei Bibliotheken) zu benennen. Eine Einwilligung reicht als Anspruchsgrundlage nur dann aus, wenn Sie tatsächlich freiwillig und informiert erfolgt. Sofern sich hinsichtlich der Arten der verarbeiteten personenbezogenen Daten unterschiedliche Rechtsgrundlagen ergeben, ist auf die jeweiligen Daten Bezug zu nehmen (Verweis auf die laufende Nummer aus Ziff. 3.1 der Verfahrensbeschreibung).

#### Zu Ziffer 4 – Kreis der Betroffenen / Betroffenenengruppen

- In Ziff. 4 wird **auf die konkreten Angaben aus Ziff. 3.1 Bezug genommen** und es erfolgt die Zuordnung zu den Betroffenen bzw. Betroffenenengruppen. Abhängig von den im Rahmen des Verfahrens verarbeiteten Inhaltsdaten sind dies beispielweise Studierende, Mitarbeiter, stud. Hilfskräfte, Benutzer, Kunden, etc.. Bei der Darstellung sollten die Einzelangaben aus Ziffer 3.1 sachgerecht zusammengefasst werden um die Übersichtlichkeit zu wahren. **Beispiel: lfd. Nr. 1 bis 10 (aus Ziff. 3.1) = Studierendendaten, ...** Wie oben bereits dargestellt ist nicht die / der einzelne Betroffene namentlich zu nennen, sondern die jeweilige Betroffenenengruppe.

Meist ergibt sich die erste Gruppe der Betroffenen aus den zugrundeliegenden Zweckbestimmungen (z.B. Nutzerdaten im Bibliothekssystem => Nutzer der Bibliothek sind betroffen). Es gibt aber weitere personenbezogene Daten, die durch den Umgang mit Softwaresystemen entstehen. Hier sollte man sich fragen, wer mit dem System arbeitet, wer ein System nutzt. Sofern es sich um reine Authentifizierungsdaten und Log-Dateien im Zusammenhang mit der Anmeldung an dem IT-System handelt können diese Daten in aller Regel auch im Zuge der Vorabkontrolle nach § 8 Abs. 4 HmbDSG betrachtet werden. Soweit sich aber inhaltliche Verarbeitungsprozesse durch das Personal ergeben (Bearbeitungsstatus, zu dokumentierende Entscheidungsvorgänge) sind diese auch in der Verfahrensbeschreibung darzustellen. Im Zusammenhang mit den zunehmenden Web-Anwendungen sind beispielsweise auch zunächst unbekannte Nutzer bei Internetdiensten zu berücksichtigen, die über Netzwerkadressen identifiziert werden können.

#### Zu Ziffer 5 – (Kreis der) Empfängerinnen und Empfänger, die Daten erhalten können

- Mit diesem Formular wird das HmbBfDI-Musters zur Verfahrensbeschreibung 1 : 1 umgesetzt, auch wenn die Reihenfolge der Darstellung dieser Ziffer nicht unbedingt zweckmäßig erscheint. Als Empfängerinnen / Empfänger sind nicht namentliche benannte Personen zu verstehen, sondern organisatorische Rollen, die diese wahrnehmen (z.B. Personalsachbearbeitung, Reisekostenstelle).
- Zu Ziff. 5.1  
Unter Ziffer 5.1 sind die Empfängerinnen und Empfänger **außerhalb der eigenen Daten verarbeitenden Stelle nach Ziff. 1.1** aufzuführen. Bei der Darstellung sollten die Einzelangaben aus Ziffer 3.1 sachgerecht zusammengefasst werden um die Übersichtlichkeit zu wahren.  
Das Musterformular enthält bereits einen Vorschlag bezüglich der gesetzlichen Vorgaben des Hamburgischen Archivgesetzes (HmbArchG). Dieser Textbaustein kann entfallen, sofern das Staatsarchiv Hamburg im jeweiligen Einzelfall eine Archivwürdigkeit grundsätzlich verneint hat (siehe [§ 3 Abs. 4 HmbArchG](#) ) .
- Zu Ziff. 5.2  
Sofern die Datenverarbeitung ganz oder teilweise an externe Dienstleister (nicht gemeint ist hier das eigene Rechenzentrum oder die eigene Fakultäts-IT) ausgelagert wurde sind die entsprechenden Angaben an dieser Stelle zu dokumentieren.

Auch Software- und Hardware-Wartungen fallen unter diesen Punkt, sofern der Zugriff auf die personenbezogenen Daten dabei nicht ausgeschlossen werden können.

In Ziffer 5.2.1 sind alle Auftragnehmer mit (Firmen-)Name und Anschrift darzustellen.

Ziffer 5.2.2 konkretisiert, auf welche personenbezogenen Daten der Auftragnehmer im Rahmen seiner Vertragserfüllung zugreifen könnte.

- Zu Ziff. 5.3

Dieser Punkt wird regelhaft am meisten auszufüllen sein. Er bezieht sich auf die Empfängerinnen und Empfänger **innerhalb der eigenen Daten verarbeitenden Stelle nach Ziff. 1.1** die andere Aufgaben wahrnehmen. Welche Stellen konkret zu benennen sind, sollte sich aus den entsprechenden Organisationsverfügungen ergeben. Bei der Darstellung sind die Einzelangaben aus Ziffer 3.1 sachgerecht zusammenzufassen, um die Übersichtlichkeit zu wahren.


#### Zu Ziff. 6 – beabsichtigte Datenübermittlung an Stellen außerhalb der EU

Bei der Übermittlung personenbezogener Daten an Stellen außerhalb der Europäischen Union und an über- oder zwischenstaatliche Stellen sind die Voraussetzungen des § 17 Abs. 2 und 3 HmbDSG zu beachten. Die Verarbeitungsprozesse sind unter Ziff. 6 zu dokumentieren. Sofern eine entsprechende Übermittlung stattfindet, sind die Empfänger und die konkreten Zweckbestimmungen einschließlich der Rechtsgrundlagen zu dokumentieren.

#### Zu Ziff. 7 – Fristen für die Löschung und Sperrung der Daten

Das HmbDSG (hier insbesondere § 19 Abs. 2 und 3 HmbDSG) verpflichtet die Daten verarbeitenden Stellen, sich bereits vor Inbetriebnahme des jeweiligen Verfahrens Gedanken zu machen, wie lange die verarbeiteten personenbezogenen Daten benötigt werden. Das Ergebnis dieser Betrachtung ist in Ziff. 7.1 und 7.2 konkret zu dokumentieren. Neben rechtlichen Grundlagen z.B. aus dem Steuer- und Handelsrecht sind dabei auch Satzungsregelungen, etc. zu betrachten. Ggf. ist bei unterschiedlichen Kriterien auf das jeweilige personenbezogene Datum aus Ziff. 3.1 Bezug zu nehmen.

Bezüglich der gesetzlichen Vorgaben des HmbArchG sind im Musterformular bereits entsprechende Vorschläge berücksichtigt. Selbstverständlich ist es den Daten verarbeitenden Stellen freigestellt, hier eigene Formulierungen zu verwenden.

Der Textbaustein kann entfallen, sofern das Staatsarchiv Hamburg im jeweiligen Einzelfall eine Archivwürdigkeit der zugrundeliegenden personenbezogenen Daten grundsätzlich verneint hat (siehe [§ 3 Abs. 4 HmbArchG](#) )

#### Zu Ziffer 8 – Technische und organisatorische Maßnahmen

Mit Ziffer 8 beginnt der nicht-öffentliche Teil der Verfahrensbeschreibung. Die Daten verarbeitende Stelle kann diese sicherheitsrelevanten Informationen veröffentlichen, ist aber nicht dazu verpflichtet. Zu dokumentieren ist hier die Verfahrenssicherheit. Zunächst wird dokumentiert, ob die personenbezogenen Daten vollständig automatisiert verarbeitet werden, oder ob es darüber hinaus auch noch Verfahrensteile gibt die manuell, also ohne IT-technische Unterstützung, umgesetzt werden (z.B. Evaluationsvorhaben bei denen handschriftliche Fragebögen verteilt und eingesammelt werden, um dann die Antworten elektronisch zu erfassen und weiter zu verarbeiten).

Der Verweis auf vorhandene Dokumente in der Anlage (Ergebnis der Vorabkontrolle nach § 8 Abs. 4 HmbDSG, IT-Sicherheitskonzepte, Rechte- und Rollenkonzepte, IT-Grundschutzaudit, usw.) ist möglich und kann durchaus sinnvoll sein.

- Zu Ziffern 8.1 – 8.5

Das HmbDSG fordert in § 8 Abs. 2 HmbDSG in Bezug auf die verarbeiteten personenbezogenen Daten deren

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität und
- Revisionsfähigkeit.

Die ergriffenen Maßnahmen zur Zutrittskontrolle (Kontrolle des Zutritts zu DV-Anlagen), Zugangskontrolle (Kontrolle der Nutzung von DV-Anlagen), Zugriffskontrolle (Kontrolle des Zugriffs auf Daten), Weitergabekontrolle (Kontrolle der Übertragung und Übermittlung von digitalen Daten), Eingabekontrolle (Kontrolle ob und wem Daten verarbeitet wurden, Auftragskontrolle (Kontrolle ob die Datenverarbeitung gemäß den Weisungen des Auftraggebers erfolgt), Verfügbarkeitskontrolle (Kontrolle des Schutzes vor Verlust und Zerstörung der Daten) und Organisationskontrolle (Kontrolle ob die Daten gemäß ihrer Zweckbestimmung verarbeitet werden können) sind in unter den Ziffern 8.1 bis 8.5 zu dokumentieren.

Auch hier verweisen wir auf Punkt D der Handreichung. Die Darstellung soll klar und verständlich sein. Die inhaltlichen Detailfragen zur IT-Sicherheit sind in der Vorabkontrolle zur Verfahrenssicherheit nach § 8 Abs. 4 HmbDSG zu dokumentieren.

- Zu Ziffer 8.6

Zu beschreiben sind die baulichen und organisatorischen Maßnahmen zur Verfahrenssicherheit (z.B.: Sicherungsmaßnahmen bei Archivräumen, Personalaktenverwaltung, Schließkonzepte (nur berechtigte Mitarbeiter haben Zugang)). Ggf. sind auch die Prozesse Transport und Vernichtung personenbezogener Daten zu beschreiben (externe und interne Vernichtung von Papier und Datenträgern, vertragliche und organisatorische Maßnahmen). Der Verweis auf vorhandene Dokumente (Ergebnis der Vorabkontrolle nach § 8 Abs. 4 HmbDSG, IT-Sicherheitskonzepte, Rechte- und Rollenkonzepte, IT-Grundschutzaudit, usw.) ist möglich und gewünscht.

- Zu Ziffer 8.7

Unter Ziffer 8.7 sind die üblichen organisatorischen Rahmenregelungen zur IT-Sicherheit erfasst. Sie vermitteln einen ergänzenden Hinweis auf das etablierte Datenschutzniveau in der verantwortlichen Institution. Keinesfalls ersetzen die Hinweise die Dokumentation zur Vorabkontrolle die von der verantwortlichen Stelle durchzuführen ist. Bitte kreuzen Sie an welche Richtlinien im Bereich Ihrer fachverantwortlichen Stelle (Ziff. 1.2 der Verfahrensbeschreibung) bzw. institutionsweit gelten.

**!** Ergänzende Hinweise:

- Unstrittig ist die Gültigkeit der IT-Vorschriften der FHH für sämtliche Verfahren, die im Verwaltungsnetz der FHH implementiert sind.
- Die IT-Vorschriften der FHH gelten nach unserer Rechtsauffassung umfassend auch für die Staats- und Universitätsbibliothek Hamburg (Landesbetrieb der BWF).
  
- Für alle Verfahren im Wissenschaftsnetz der jeweiligen Hochschule / Universität kann eine unmittelbare Gültigkeit rechtlich nicht abgeleitet werden. Die gDSB geht daher davon aus, dass vergleichbare Regelungen etabliert worden sind. Auf diese sollte unter Ziff. 8.7. hingewiesen werden.

### Zu Ziffer 9

- In Ziffer 9.1 sind die verwendeten End-Geräte (Desktop/Tower-PC, Notebooks, Netbooks, Tablet-PC, Smartphones, etc.) mit ihren jeweiligen Betriebssystemen aufzuführen. Gleiches gilt für die Server-seitige Hardware, die Netzkomponenten und die Übertragungswege. Ferner ist die im Rahmen des Verfahrens verwendete Software (mit Versionsnummer) zu dokumentieren.
- Ziffer 9.2 dokumentiert das vor Ort etablierte Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung:
  - Auf welchem Wege werden die Daten (verschlüsselt) übermittelt?
  - Wer darf wann, welche Daten sperren? (organisatorische Regelung)
  - Wer darf wann, welche Daten löschen? (organisatorische Regelung)
  - Wer gibt Auskunft bei Anfragen von Betroffenen / jeder Person?
  - Wie erfolgt die Benachrichtigung der Betroffenen bei erstmaliger Erhebung von Daten?

Die rechtlichen Grundlagen für die Darstellung ergeben sich aus § 12 a HmbDSG - Unterrichtung bei der Erhebung -.

### Zu Ziffer 10

- Bei der Ziffer 10 des Formulars handelt es sich um eine Erweiterung des HmbBfDI-Musters um eine institutionsinterne Kommunikation zwischen der fachverantwortlichen Stelle und der das Verfahren betreuenden IT-Stelle zu erleichtern. Ferner werden die notwendigen dienstlichen Kommunikationsdaten der externen Datenschutzbeauftragten der Hamburger Hochschulen UHH, HfMT, HFBK, HCU und TUHH bzw. des behDSB der Staatsbibliothek dargestellt.
- Fachverantwortliche Stelle und Datenschutzbeauftragte/r ergänzen die Verfahrensbeschreibung neben der dienstlichen Emailadresse + Telefonnummer um ein aussagekräftiges Geschäftszeichen. Versionsnummer und Stand (Datum) der Verfahrensbeschreibung sind zu dokumentieren.

### Zu Ziffer 11 – Informationen zur Vorabkontrolle

- Abschließend dokumentiert die fachverantwortliche Daten verarbeitende Stelle (gemäß Ziff. 1.2 der Verfahrensbeschreibung) den aktuellen Sachstand in Bezug auf die vom Gesetzgeber geforderte Vorabkontrolle nach § 8 Abs. 4 HmbDSG.

Die Übersendung der Dokumentation der Vorabkontrolle an die / den Datenschutzbeauftragte/n ist freigestellt, sofern die fachverantwortliche Daten verarbeitende Stelle (Ziff. 1.2) zu dem Ergebnis gekommen ist, dass von dem Verfahren keine besondere Gefahr für die Rechte der Betroffenen ausgeht.

- Im Rahmen der Vorabkontrolle ist auch zu prüfen, ob die rechtlichen Vorgaben in Bezug auf
  - ein automatisiertes Abrufverfahren innerhalb der Daten verarbeitenden Stelle bzw.
  - die Verarbeitung gemeinsamer und verbundener automatisierter Dateien innerhalb der Daten verarbeitenden Stelleumgesetzt wurden. Über das Ergebnis wird durch entsprechendes Ankreuzen des vorliegenden Sachverhalts informiert.

---

Für Rückfragen und weitere Informationen zum Datenschutz wenden Sie sich bitte an:

**Gemeinsame Datenschutzbeauftragte der Hamburger Hochschulen  
UHH, HfMT, HFBK, HCU & TUHH | Datenschutzbeauftragter der SUB  
Prof. Dr. Gabriele Beger | Bernd Uderstadt**

Büro:

Staats- und Universitätsbibliothek Hamburg Carl von Ossietzky - Landesbetrieb  
D-20146 Hamburg \* Von-Melle-Park 3 (HG, 2. OG, Zimmer 270)

📞 +49 40 42838-5801

📠 +49 40 42838-3352

✉️ [datenschutz@sub.uni-hamburg.de](mailto:datenschutz@sub.uni-hamburg.de)\* (Funktionspostfach Hochschul-Datenschutz)  
[datenschutzbeauftragter@sub.uni-hamburg.de](mailto:datenschutzbeauftragter@sub.uni-hamburg.de)\* (Datenschutzbeauftragter der SUB)

\*= Bitte beachten Sie, dass der Versand unverschlüsselter Emails unsicher ist, also von unbefugten Dritten mitgelesen werden könnte. Schutzwürdige Nachrichten mit personenbezogenen oder vertraulichen Inhalten sollten Sie daher auf konventionellem Postweg an uns richten.

© gDSB/Staats- und Universitätsbibliothek Hamburg (SUB) - Dieser Text ist urheberrechtlich geschützt. Eine Vervielfältigung oder Weitergabe ist nur innerhalb der Hamburger Hochschulen UHH, HfMT, HFBK, HCU, TUHH sowie der SUB zulässig, soweit hieran keine Änderungen vorgenommen werden und insbesondere der Urheberhinweis nicht entfernt wird. Die Nutzung durch externe Dritte mit Quellenangabe ist gestattet.