Umgang mit Akten und Schriftgut, etc.
- Hinweise und Empfehlungen -

Als Mitarbeiterin und Mitarbeiter einer öffentlichen Hamburger Einrichtung haben Sie auch im Umgang mit personenbezogenen Daten in nicht elektronischer Form (Akten, Schriftgut, Karteien, Register, etc.) die Verantwortung für die Wahrung des Datenschutzes
(vgl. § 7 und § 8 Abs. 3 HmbDSG (Hamburgisches Datenschutzgesetz)).

Durch entsprechende technisch-organisatorische Maßnahmen (die sogenannten TOM's) ist bei der „analogen Datenverarbeitung" insbesondere der Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern. Gleichermaßen dürfen aber auch die Schutzziele der automatisierten Datenverarbeitung nicht außer Acht gelassen werden:

Zu gewährleisten ist, dass

1. nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. die personenbezogenen Daten während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei bleiben (Integrität),
3. die personenbezogenen Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. die personenbezogenen Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit)

(vgl. § 8 Abs. 2 HmbDSG).

Hierzu im Folgenden einige Hinweise und Empfehlungen zum Umgang mit Akten und Schriftgut:

- Grundsätzlich ist das Erheben personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist (siehe § 12 Abs. 1 HmbDSG, Grundsatz der Zweckgebundenheit).
- Die Zulässigkeit der Verarbeitung personenbezogener Daten in Akten richtet sich hierbei zunächst nach den bereichsspezifischen Datenschutzbestimmungen (z.B. HmbHG (Hamburgisches Hochschulgesetz), ggf. in Verbindung mit korrespondierenden Hochschul-Ordnungen und -Satzungen, HmbBG, HmbPersVG, HmbArchG, usw. . Eine vollständige Auflistung aller Spezialnormen ist bei der Vielzahl unterschiedlicher Aufgaben im Hochschulbereich unmöglich. Zudem sind Ihnen „Ihre speziellen Rechtsgrundlagen und zulässigen Verarbeitungsszwecken“ im Rahmen der täglichen Aufgabenerledigung sicherlich bestens bekannt).
- Fehlen entsprechende spezialgesetzliche Regelungen so gelten die allgemeinen Bestimmungen des hiesigen Landesdatenschutzgesetzes -> HmbDSG
- Sind weder bereichsspezifische Vorschriften vorhanden, noch das allgemeine Datenschutzrecht anwendbar, so bedarf es einer informierten und freiwilligen Einwilligung der / des Betroffenen (vgl. § 5 Abs. 1 HmbDSG).

- Nicht besetzte Büroräume sollten grundsätzlich verschlossen werden (Schlüssel-, Transponder oder Kartensystem). Der Schlüssel ist abzuziehen; Schlüssel, Transponder, Chipkarte etc. sind sicher zu verwahren.
- Kennzeichnen Sie Ihre Schlüssel, etc. nicht mit Aufschriften oder Anhängern, aus denen hervorgeht, zu welchem Schloss sie passen
- Nutzen Sie - sofern erforderlich - farbliche Markierungen, die Ihnen helfen, mehrere Schlüssel, etc. schnell richtig zuzuordnen, aber für Dritte im Falle eines Verlusts keinen Informationswert besitzen
- Stellen Sie sicher, dass sich Besucherinnen und Besucher nur in Ihrem oder im Beisein einer Kollegin oder eines Kollegen in Ihrem Büro aufhalten.
- Ist dies aus dienstlichen Gründen im Ausnahmefall nicht möglich, halten sie die Unterlagen mit personenbezogenem Inhalt bei Abwesenheit unter Verschluss (verschlossener Schrank, Schreibtisch o. ä.)

- Versenden Sie Akten und Schreiben mit personenbezogenen Daten, die einem besonderen

Amtsgeheimnis unterliegen (z. B. Personaldaten, Sozialdaten, Gesundheitsdaten) sowohl im internen Postgang als auch extern nur im verschlossenen Umschlag, ggf. mit der Aufschrift "vertraulich".

- Versenden Sie personenbezogene Daten grundsätzlich nicht per Fax. Faxgeräte sind in vielen Behörden und Firmen an zentraler, gut zugänglicher Stelle installiert, so dass ein Versenden per Fax die Vertraulichkeit von vornherein ausschließt.
- Vergewissern Sie sich ggf. vorab, ob ein gesicherter Transportweg und Empfang gewährleistet werden kann.
- Versenden Sie personenbezogene Daten grundsätzlich nicht unverschlüsselt per Email.
- Falls Sie im Rahmen Ihrer Aufgabenwahrnehmung personenbezogene Daten in Akten / Aktenmappen außerhalb Ihrer Büroräume bearbeiten (z. B. bei Auswärtsterminen, Veranstaltungen, u.ä.), schützen sie diese gegen unbefugte Zugriffe.
- Geben Sie die Akte / die Unterlagen nicht unbeaufsichtigt aus der Hand.
- Halten Sie sie im PKW / in öffentlichen Verkehrsmitteln unter Verschluss
- Bringen Sie die Akte / die Unterlagen bei Dienstschluss möglichst wieder in das Büro. Ist dies nicht möglich, nehmen Sie sie zwischenzeitlich zuhause sicher unter Verschluss.
- Personenbezogene Daten in Akten sind zu löschen, sobald ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist (Grundsatz der Zweckgebundenheit, vgl. § 19 Abs. 3 HmbDSG).
- Beachten Sie ggf. Ihre jeweiligen bereichsspezifischen Aufbewahrungsfristen.
- Bedenken Sie ferner, dass Sie auch diese Daten vor einer Vernichtung dem Staatsarchiv Hamburg zur Archivierung anzubieten haben (siehe § 19 Abs. 4 HmbDSG i.V.m. § 3
- HmbArchG (Hamburgisches Archivgesetz)). Für Beschäftigte der Universität Hamburg gilt die Anbietungspflicht gegenüber dem dortigen Universitätsarchiv (UAHH).
- Papiergut mit personenbezogenem Inhalt ist (nach entsprechender Freigabe durch das Staatsarchiv / Universitätsarchiv; s.o.) datenschutzgerecht zu entsorgen.
- Nutzen Sie bei kleineren Mengen einen geeigneten Papier-Schredder (sollte in aller Regel vor Ort vorhanden sein).
- Alternativ und bei größeren Mengen empfehle ich für die sichere Entsorgung und Vernichtung die Nutzung eines zertifizierten Dienstleisters der üblicherweise bereits an Ihrer Institution vorhanden ist (z.B. Elbe Werkstätten GmbH, Reisswolf Deutschland GmbH, Recall Deutschland GmbH, etc.).

Die ordnungsgemäße Vernichtung ist von der beauftragten Firma zu protokollieren; die Pro-

tokolle sind vom Auftraggeber (Hochschule / Universität / Staatsbibliothek) zu Dokumentationszwecken (Stichwort: Revisionssicherheit) aufzubewahren.

Meine Hinweise und Empfehlungen sind dem großen Themenkomplex der ‚Informationssicherheit' zuzuordnen die im Zusammenhang mit einer sicheren, verantwortungsbewussten Datenverarbeitung neben den technischen Fragestellungen zur IT-Sicherheit zunehmend an Bedeutung gewinnt. Ausgehend von einer im April 2013 in Kraft getretenen Informationssicherheits-Leitlinie (IS-LL) der Freien und Hansestadt Hamburg (FHH) sind auch die BWFG und ihre nachgeordneten Hochschulen, Universitäten, Bibliotheken ein sachgerechtes Informationssicherheitsmanagement (InSiMa) - einschließlich der Bestellung von Informationssicherheitsbeauftragten (InSiBe) - zu entwickeln. Wenden Sie sich bei Fragen zur technisch-organisatorischen Informationssicherheit also gerne auch an Ihre / Ihren InSiBe. An UHH, TUHH wurden mittlerweile eigene IS-LL veröffentlicht.

Quelle:

Für den vorstehenden Text wurden größere Textpassagen des ULD Schleswig-Holstein genutzt -> https://www.datenschutzzentrum.de/backup-magazin/backup04.pdf .

Kontakt:

Bernd Uderstadt
Datenschutzbeauftragter (DSB) der Universität Hamburg (UHH)
sowie externer DSB der Hmb. Hochschulen HfMT, HFBK, HCU, TUHH
und der Staats- und Universitätsbibliothek Hamburg (SUB)

Universität Hamburg, Stabsstelle Recht, DSB (UHH/R16)
Mittelweg 177 (Rm. N 0051) * D-20148 Hamburg
Telefon: +49 40 42838-2957
E-Mail: datenschutz [at] uni-hamburg.de
Internet: https://www.hh-datenschutz.de

//
Versionierung und Gültigkeit
Dok.: 161020_DSB--Umgang_mit_Akten_und_Schriftgut.docx

Version	Datum	von	Beschreibung der Änderung(en)
1.0-1.2	2011-2014	DS-Ref/gDSB (SUB)	Ohne Versionierung
1.3	27.04.2015	DSB (KoopDS)	Layout
1.4	28.10.2015	DSB (KoopDS)	Kl. Inhaltl. Anpassungen
1.5	28.07.2016	DSB (KoopDS)	Löschung CC-Lizenzhinweis; Aktualisierung Stand InSiMa
1.6	20.10.2016	DSB (KoopDS)	Anpassung Kommunikationsdaten
Gültig bis:	**24.05.2018**		ab 25.05.2018 gilt die EU DS-GVO