

Abteilung:	Zentrale Dienste
Name:	Claus-Toni Bertram
Telefon:	+49 6131 39-25382
Telefax:	+49 6131 39-20709
Unser Zeichen:	ZD/2107 / Hm.
Datum:	30.09.93

VERWALTUNGSVERFÜGUNG NR. 6/ 93 für den Bereich Campus und Germersheim

Dienstanweisung über den Datenschutz und die Datensicherung in der Universität Mainz

Sehr geehrte Damen und Herren,

beigefügt erhalten Sie zur Kenntnisnahme die Dienstanweisung über den Datenschutz und die Datensicherung in der Universität Mainz vom September 1993, die der Präsident unter Beteiligung des Gesamtpersonalrates erlassen hat. Diese ist ab sofort zu beachten. Sämtliche vorher erlassenen Dienstanweisungen über den Datenschutz und die Datensicherung an der Universität Mainz treten außer Kraft.

Mit freundlichen Grüßen
Im Auftrag

(Vogel-Arnoldi)

Anlage

DIENSTANWEISUNG

über den Datenschutz und die Datensicherung in der Johannes Gutenberg-Universität Mainz (Bereich Campus und Germersheim)

1. Meldepflicht

1.1 Gemäß § 10 Abs. 1 LDSG sind dem Landesbeauftragten für den Datenschutz zu melden

- alle Verfahren einschließlich der von ihnen betroffenen Dateien, mit denen personenbezogene Daten verarbeitet werden,
- alle manuell geführten Dateien, aus denen personenbezogene Daten an Dritte übermittelt werden.

Die Anmeldung hat vor der ersten Speicherung personenbezogener Daten durch den Anwender (das sind die Universitätsstellen bzw. –angehörigen, die solche Daten speichern wollen) über den Präsidenten und das Ministerium für Bildung, Wissenschaft, Jugend und Kultur zu erfolgen. Die Anmeldung soll 6 Wochen vor der ersten Speicherung dem Ministerium vorliegen. Formblätter hierzu sind bei der Abteilung Zentrale Dienste (Tel. 39-24218) erhältlich.

1.2 Personenbezogene Daten sind nach der Begriffsbestimmung des Landesdatenschutzgesetzes Einzelangaben über persönliche oder sachliche Verhältnisse einer Person, wenn ihre Identität aufgrund dieser Einzelangaben festgestellt werden kann (z. B. Anschrift, Geburtsdatum, Familienstand, Einkommen, Staatsangehörigkeit, Berufsbezeichnung, Grundbesitz, KFZ-Kennzeichen, Werturteile, Prognosedaten).

2. Pflicht zur Geheimhaltung

2.1 Gemäß § 8 Abs. 1 LDSG ist allen Anwendern, die personenbezogene Daten verarbeiten, untersagt, diese zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen.

- 2.2 Gemäß § 8 Abs. 2 LDSG sind alle Anwender, die personenbezogene Daten verarbeiten, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Die Verpflichtung erfolgt durch den Präsidenten oder den hierzu Beauftragten unter Anwendung des Vordrucks gemäß Anlage.

Dem/der Verpflichteten ist eine Durchschrift der Verpflichtung zusammen mit dem Text des Landesdatenschutzgesetzes in der jeweils geltenden Fassung sowie die Dienstanweisung auszuhändigen.

Die allgemeinen Geheimhaltungs- und Amtsverschwiegenheitspflichten (z. B. § 30 Verwaltungsverfahrensgesetz, § 70 Landesbeamtengesetz) bleiben unberührt.

3. Auskunfterteilung

Das Recht auf Auskunftserteilung über gespeicherte Daten ist unterschiedlich geregelt für

- Mitarbeiter/innen der Dienststelle (s. Nr. 3.1),
- andere Personen (s. Nr. 3.2).

- 3.1 Nach § 34 BDSG i. V. m. § 2 Abs. 3 LDSG können Mitarbeiter/innen im Hinblick auf ihre bei der Dienststelle gespeicherten Daten Auskunft verlangen über

- die zu ihrer Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,
- den Zweck der Speicherung und
- Personen und Stellen, an die regelmäßig ihre Daten übermittelt werden, wenn diese Daten automatisiert verarbeitet werden.

- 3.2 Andere Personen können nach § 12 Abs. 1 LDSG Auskunft beantragen über

- die zu ihrer Person gespeicherten Daten und
- die Stellen, denen diese Daten regelmäßig übermittelt werden.

- 3.3 Auskünfte nach Nr. 3.1 und 3.2 erteilen jeweils für ihren Zuständigkeitsbereich die Dekane/Dekaninnen, die Leiter/innen wissenschaftlicher bzw. zentraler Einrichtungen oder Betriebseinheiten sowie die Abteilungsleiter/innen der Zentralen Verwaltung.

4. Sicherungsmaßnahmen

Zur Gewährleistung des Datenschutzes sind folgende Sicherungsmaßnahmen zu beachten:

4.1 Zugangskontrolle

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle).

Deshalb sind:

- 4.1.1 Räume oder Datenverarbeitungsanlagen, in / mit denen personenbezogene Daten verarbeitet werden, bei Abwesenheit der berechtigten Personen, auch wenn dies nur vorübergehend ist, zu verschließen / zu sichern.
- 4.1.2 Datenträger mit personenbezogenen Daten (Disketten, Ausdrucke), sofern nicht mit ihnen gearbeitet wird, unter Verschluss zu halten.

4.2 Speicher-, Zugriffs-, Benutzer- und Datenträgerkontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können. Weiterhin ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert, gelöscht oder entfernt werden können oder dass unbefugte Eingaben vorgenommen werden. Es ist zu gewährleisten, dass berechtigte Personen ausschließlich auf die ihrer Berechtigung unterliegenden Daten zugreifen können.

Deshalb ist:

- 4.2.1 Speicherung, Übermittlung, Veränderung und Löschung von Daten sowie deren Auswertung und Ausdruck nur auf Anweisung der Dekane/Dekaninnen, der

Leiter/innen der wissenschaftlichen und zentralen Einrichtungen und Betriebseinheiten sowie der Leiter/innen der Abteilungen der Zentralen Verwaltung sowie deren jeweiligen Beauftragten zulässig.

- 4.2.2 Fertigung der Kopie eines Datenträgers mit personenbezogenen Daten (z. B. Diskette) nur zulässig, wenn dies für die Aufgabenerfüllung oder zum Zwecke der Datensicherung erforderlich ist. Bei Herstellung einer Kopie sind Zeitpunkt und Anlass aufzuzeichnen. Die Kopien sind getrennt von dem Originalbestand aufzubewahren.
- 4.2.3 der Datenträger mit einem Aufkleber zu versehen, der folgende Angaben enthält:
- Bezeichnung des Datenträgers
 - Kennzeichnung des Datenträgers als Original oder Kopie
 - Daten der letzten Änderung
 - Namenszeichnung der Verantwortlichen.
- 4.2.4 Zugang zu den Dateien mit personenbezogenen Daten nur für Dekane/Dekaninnen, Leiter/innen der wissenschaftlichen und zentralen Einrichtungen und Betriebseinheiten sowie den Leitern/innen der Abteilungen der Zentralen Verwaltung sowie deren jeweiligen Beauftragten zulässig.
- 4.2.5 Ohne besondere Genehmigung des Präsidenten ist es unzulässig, Datenverarbeitungsanlagen, auf denen personenbezogene Daten gespeichert sind, mit Datenverarbeitungsanlagen zu vernetzen, die zu Lehr- oder Forschungszwecken eingesetzt werden.

Eine solche Genehmigung kann erteilt werden, wenn durch Vorlage eines Datenschutzkonzeptes der Nachweis erbracht wird, dass die personenbezogenen Daten durch benutzer- oder benutzergruppenspezifische Zugriffsberechtigungen oder durch benutzerbezogene Authentisierungsverfahren wirksam geschützt werden können. Die Genehmigung ist mit der Auflage zu verbinden, dass das vorgeschlagene Datenschutzkonzept in die Praxis umzusetzen ist und alle zugriffsberechtigten Personen auf das Datengeheimnis besonders verpflichtet werden.

Die Speicherung personenbezogener Daten auf lokale, entnehmbare Speichermedien – ausgenommen zum Zweck der Datensicherung – ist nicht zulässig.

Ein Anschluss nicht zugangsgeschützter Personalcomputer an ein Netz, auf dem personenbezogene Daten verarbeitet werden, ist nicht zulässig.

4.3 Eingabekontrolle

Es ist sicherzustellen, dass nachträglich feststellbar ist, welche personenbezogenen Daten in welcher Zeit von wem in ein Datenverarbeitungssystem eingegeben worden sind. Deshalb sind Eingabe, Veränderung und Löschung solcher Daten automatisiert zu protokollieren. Ist dies aus technischen Gründen nicht möglich, sind sie in anderer Weise zu protokollieren.

4.4 Übermittlungskontrolle

Die Übermittlung personenbezogener Daten an Dritte ist unter Angabe des Empfängers und des Anlasses festzuhalten. Werden personenbezogene Daten als Ausdruck weitergegeben, so ist in den Auszügen auf die Geheimhaltungsvorschriften hinzuweisen.

4.5 Transportkontrolle

Die Versendung von Datenträgern mit personenbezogenen Daten (z. B. Disketten) ist in einem verschlossenen Umschlag oder in verschlossenen Transportbehältern (Kassetten etc.) durchzuführen. Die Versendung ist schriftlich festzuhalten (Transportkontrolle).

5. Einwilligung der Betroffenen

Die Verarbeitung personenbezogener Daten ist zulässig, soweit die oder der Betroffene eingewilligt hat oder das LDSG oder eine andere Rechtsvorschrift dies erlaubt und die Verarbeitung nach Maßgabe der Bestimmungen des LDSG erfolgt, sofern dem nicht besondere Rechtsvorschriften des Bundes oder Landes vorgehen. Auf die Ausnahmeregelungen des § 12 LDSG wird hingewiesen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände

eine andere Form angemessen ist. Im Bereich der wissenschaftlichen Forschung kann ein solcher besonderer Umstand auch vorliegen, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind die Gründe, aus denen sich die erhebliche Beeinträchtigung des Forschungszweckes ergibt, schriftlich festzuhalten, ebenso die sich aus Nachfolgendem ergebenden Hinweise.

Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, den Verwendungszweck der Daten und den möglichen Empfängerkreis aufzuklären. Dabei ist die oder der Betroffene unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

6. Die Kontrolle der Einhaltung dieser Dienstanweisung obliegt den Dekanen/Dekaninnen, den Leitern/innen der wissenschaftlichen und zentralen Einrichtungen und Betriebseinheiten sowie den Leitern/innen der Abteilungen der Zentralen Verwaltung.

Mainz, im September 1993

(Universitätsprofessor Dr. Josef Reiter)

**Verpflichtung zur Einhaltung des Datengeheimnisses
nach § 8 LDSG und § 5 BDSG**

von

Familienname

Vorname

1. Ich verpflichte mich, das Datengeheimnis gemäß § 8 Landesdatenschutzgesetz (LDSG) und § 5 Bundesdatenschutzgesetz (BDSG) zu wahren.
2. Mir ist bekannt, dass es untersagt ist, geschützte personenbezogene Daten unbefugt zu einem anderen als zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren. Diese Verpflichtung besteht auch noch nach Beendigung meiner Tätigkeit fort.
3. Ich bin darauf hingewiesen worden, dass andere Geheimhaltungspflichten aufgrund gesetzlicher Bestimmungen und die Bestimmungen der Dienstanweisung Datenschutz ebenfalls zu beachten sind.
4. Mir ist bekannt, dass Verstöße gegen die Verpflichtung zur Wahrung des Datengeheimnisses nach § 37 LDSG und §§ 43/44 BDSG mit Geld- oder Freiheitsstrafe geahndet werden können; davon unberührt bleibt die Strafbarkeit nach anderen Vorschriften, z. B. §§ 203; 353 b Strafgesetzbuch (StGB).
5. Der Text der Verpflichtung, die Dienstanweisung Datenschutz, das Landesdatenschutzgesetz sowie das Bundesdatenschutzgesetz sind auf der Homepage der Abteilung Zentrale Dienste der Johannes Gutenberg-Universität Mainz unter folgendem Pfad abrufbar:

<http://zope.verwaltung.uni-mainz.de/orga/Datenschutz>

Die Wortlaute des § 8 LDSG und des § 5 BDSG sind nachfolgend aufgeführt.

Ort, Datum

Unterschrift

§ 8 LDSG Datengeheimnis

- (1) Den bei der verantwortlichen Stelle oder in deren Auftrag beschäftigten Personen, die dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, diese Daten zu einem andern als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.
- (2) Die in Absatz 1 Satz 1 genannten Personen sind bei der Aufnahme ihrer Tätigkeit über ihre Pflichten nach Absatz 1 sowie die sonstigen bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten und auf deren Einhaltung zu verpflichten.

§ 5 BDSG Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.