UNIVERSITÄT SIEGEN

Der Kanzler

Allgemeine Dienstanweisung
für den Umgang mit personenbezogenen Daten

Zur Gewährleistung der Datensicherheit an der Universität Siegen und zur Wahrung der gesetzlichen Bestimmungen zum Datenschutz ergeht diese „Allgemeine Dienstanweisung für den Umgang mit personenbezogenen Daten“. Sie dient dazu, den Umgang mit personenbezogenen Daten möglich zu machen und zugleich den unbefugten und unberechtigten Zugriff auf Daten zu verhindern.

1. Anwendungsbereich und Begriffe:

1.1 Diese Dienstanweisung richtet sich an alle in der Zentralverwaltung der Universität Siegen Beschäftigten. Sie enthält sowohl Regelungen für den Umgang mit personenbezogenen Daten, welche automatisiert (§ 3 Abs. 5 Datenschutzgesetz [DSG] NW), also mit Hilfe elektronischer Datenverarbeitungsanlagen (z.B. PCs, Workstations und Server) verarbeitet werden, als auch solche, die nicht automatisiert (§ 3 Abs. 6 DSG NW), also in Akten (einschließlich Bild- und Tonträger) oder ähnlichem erfasst sind.

1.2 Personenbezogene Daten sind „Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 3 Abs. 1 DSG NW). Hierzu gehören z.B. Name, Alter, Familienstand, Wohnort, gesundheitliche Verhältnisse, Prüfungsnoten.

1.3 Unter Datenverarbeitung wird das Erheben, Speichern, Verändern, Übermitteln (einschließlich der Gewährung des Zugriffes), Sperren, Löschen (endgültige physische Vernichtung) sowie Nutzen von personenbezogenen Daten verstanden (§ 3 Abs. 2 DSG NW).

2. Zulässigkeitsvoraussetzungen:

2.1 Personenbezogene Daten dürfen nur verarbeitet (erhoben, gespeichert, verändert oder genutzt) werden, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der verarbeitenden Stelle erforderlich ist oder die betroffene Person eingewilligt hat.

2.2 Personenbezogene Daten sind vor unberechtigtem Zugriff zu schützen und gegen jegliche Form des Missbrauchs zu sichern. Missbräuchliche Verarbeitung liegt vor, wenn sie gegen Datenschutzbestimmungen oder andere zum Schutz personenbezogener Daten erlassene Vorschriften verstößt.

Postanschrift:
Universität Siegen
D-57068 Siegen

Hausanschrift:
Universität Siegen
Herrengarten 3
D-57072 Siegen

Anfahrt:
Öffentliche Verkehrsmittel:
3 Fußminuten vom Bhf. Siegen,
PKW: BAB A 45 - Ausfahrt Siegen

Homepage:
http://www.uni-siegen.de

3. Technische und organisatorische Maßnahmen, Zugangsregelungen

3.1 Die Dienststelle gewährleistet, dass durch geeignete, dem Stand der Technik entsprechende organisatorische und technische Maßnahmen personenbezogene Daten gegen Missbrauch gesichert werden[1].

3.2 Wegen der hohen Sensibilität werden alle DV-Systeme mit personenbezogenen Anwendungen bzw. Daten der Zentralverwaltung von einem Firewall-System geschützt. Es verhindert die unberechtigte Nutzung aller im Zentralverwaltungsbereich betriebenen Datenverarbeitungsanlagen.

3.3 Soll die Speicherung personenbezogener Daten in begründeten Einzelfällen auf nicht vernetzten PCs erfolgen, so sind besondere Maßnahmen und Regelungen zum Datenschutz und zur Datensicherheit zu ergreifen.

3.4 Nur Berechtigte dürfen auf die für sie notwendigen Systeme und Daten zugreifen.

3.5 Die Nutzung der Anwendungssysteme ist nur für eingetragene, berechtigte Nutzerinnen und Nutzer durch Eingabe einer User-Identifikation (UserId) möglich. Unbefugte Nutzungsversuche werden gesondert verfolgt.

3.6 Der Zugang auf die Server ist nur mit einem mindestens 8-stelligen Passwort möglich. Das Passwort muss Zeichen aus mindestens 3 der folgenden Kategorien enthalten: Kleinbuchstaben, Großbuchstaben, Ziffern oder Sonderzeichen. Der Benutzername darf nicht Teil des Passwortes sein. Die Verwendung von Umlauten oder „ß“ wird nicht empfohlen (vgl. Passwortrichtlinie der Universität Siegen vom 13. Dezember 2011).
Geläufige Begriffe, Namen oder Geburtstage sollten nicht verwendet werden. Die Einhaltung dieser Passwortregelung wird kontrolliert.

3.7 Ist das Endgerät nicht unter dienstlicher Aufsicht, ist die Anwendung zu verlassen und sich aus dem System auszuloggen. Bei kurzzeitiger Abwesenheit reicht die Aktivierung des Passwortschutzes der Windows-Oberfläche und das Verschließen des Raumes.

4. Nutzungsregelungen für den DV-Einsatz:

4.1 PCs, Workstations und Server dürfen für private Zwecke nur insoweit verwendet werden, als dienstliche Belange nicht entgegenstehen.

4.2 Datenträger und Dateien mit personenbezogenen Daten dürfen grundsätzlich nicht aus dem Dienstbereich entfernt werden. Gesetzliche Auskunfts- und Übermittlungspflichten bleiben unberührt.

4.3 Eine unautorisierte Veränderung des eingesetzten Programms sowie selbständige Eingriffe in die Hardware und Software durch den Anwender sind untersagt.

4.4 Das Einbringen und Nutzen privater Programme/Software, insbesondere auch Spielprogramme, ist aus Datensicherheits- (Viren etc.) und Urheberrechtsgründen untersagt.

---

[1] Informationen hierüber erteilt das Dezernat 2, Abteilung 2.4

4.5 Das Kopieren von Programmen ist nur bei ausdrücklicher Gestattung erlaubt; die urheberrechtlichen Vorgaben des Softwareherstellers sind zu beachten.

5. Allgemeine, unabhängig von der Art und Form der Datenverarbeitung zu beachtende Regeln:

5.1 Datenträger sind einem unberechtigten Zugriff zu entziehen. Die Aufbewahrung hat deshalb in gesicherten Behältnissen bzw. gesicherten Räumen zu erfolgen. Datenträger dürfen nur in verschlossenen Behältnissen oder, soweit möglich, in verschlüsselter Form übermittelt oder versandt werden.

5.2 In Bereichen mit Publikumsverkehr darf diesem eine Sichtmöglichkeit auf den Bildschirm oder Datenträger (Listen/Akten etc.) nicht ermöglicht werden. Beim Verlassen des Raumes ist der Passwortschutz zu aktivieren oder das Gerät auszuschalten. Der Raum ist zu verschließen.

5.3 Die Geräte- und Aktenschränkeschlüssel sind unter Verschluss zu verwahren.

5.4 Unrichtig erhobene Daten sind zu berichtigen. Personenbezogene Daten, die in unzulässiger Weise gespeichert sind oder deren Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich sind, müssen so gelöscht werden, dass eine missbräuchliche Verarbeitung ausgeschlossen ist; falls erforderlich, ist der Datenträger sicher zu vernichten. Die Aufbewahrungsfristen für gespeicherte Daten und Datenträger richten sich nach den für die einzelnen Belange/Zwecke vorgeschriebenen gesetzlichen bzw. festgelegten Aufbewahrungsfristen.

6. Übermittlung von Daten und Auskünfte:

6.1 Bei der Übermittlung von Daten über das Verwaltungsnetz ist zu beachten, dass Dritte insbesondere durch Missbrauch „mithören“ können. „Mithören“, Ausspionieren, Aufzeichnen sowie Verändern fremder Daten aus dem Verwaltungsnetz sowie das Stören der Kommunikation sind verboten. Die Benutzerin oder der Benutzer darf aus dem Verwaltungsnetz nur diejenigen Daten auf ihren oder seinen Rechner leiten, die für sie oder ihn bestimmt sind.

6.2 Eine Datenübermittlung/-weitergabe an Stellen innerhalb der Hochschule (z. B. innerhalb eines Dezernates oder von Dezernat zu Dezernat oder von einem Dezernat an einen Fachbereich) ist zulässig, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist.

6.3 Eine Datenübermittlung/-weitergabe an Behörden oder sonstige öffentliche Stellen ist grundsätzlich nur erlaubt, wenn eine Rechtsvorschrift oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt oder die betroffene Person schriftlich eingewilligt hat. Die auskunftersuchende Behörde oder sonstige Stelle hat ihr Auskunftsbegehren schriftlich zu begründen. Die Auskunft soll schriftlich erfolgen.

6.4 Sollte in dringendem Einzelfall eine fernmündliche Auskunft an eine Behörde oder sonstige öffentliche Stelle notwendig sein, ist hierfür der Dezernent/die Dezernentin zuständig. Dieser/diese hat die sachlichen und gesetzlichen Voraussetzungen zu

prüfen und über die Auskunft zu entscheiden. Die Entscheidungsgründe sind schriftlich festzuhalten und zu den Akten zu nehmen.

6.5 Datenauskünfte an die betroffene Person sollen in der Regel schriftlich erfolgen. Weitergehende Verfahren (z. B. Akteneinsicht etc.) sind durch den Dezernenten/die Dezernentin zu entscheiden. Mündliche Datenauskünfte dürfen im Einzelfall nur nach einwandfreier Identifizierung der betroffenen Person an diese gegeben werden. Das Recht der Beschäftigten auf Einsicht in ihre Personalakte bleibt unberührt.

6.6 Die Weitergabe von personenbezogenen Daten an Dritte, insbesondere an Privatpersonen, ist ohne schriftliches Einverständnis der betroffenen Person nicht statthaft.

7. Verfahrensregister

7.1 Alle Verfahren zur automatisierten Verarbeitung personenbezogener Daten sind nach § 8 DSG NW bei der/dem behördlichen Datenschutzbeauftragten anzumelden. Ausnahme: Verfahren zur automatisierten Verarbeitung personenbezogener Daten, die aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden. Z.B: Serienbriefaktionen und kurzfristige Erstellung einer Adressdatei, die nach Ausdruck der Briefe wieder gelöscht wird.

7.2 Vordrucke für die Erstellung des Verfahrensverzeichnisses sind bei der/dem Datenschutzbeauftragten der Universität Siegen erhältlich.

Auf die Straf- und Bußgeldvorschriften der §§ 33, 34 DSG NW wird besonders verwiesen.

Siegen, den 25. Februar 2015

Der Kanzler

gez.
Ulf Richter