Datenschutzhinweise für die Rechner und Netze an der Hochschule Fulda

Rechtsgrundlagen

1. Personenbezogene Daten
2. Rechtsgrundlagen der Verarbeitung
3. Schutzmechanismen
4. Löschen von Dateien
5. Ausdrucken personenbezogener Daten
6. Allgemeine Hinweise

1. Rechtsgrundlagen

Rechtsgrundlagen sind

- die *Verordnung (EU) 2016/679* des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung DS-GVO**), die seit 25. Mai 2018 in Kraft ist, sowie
- das **Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG)** in der Fassung vom 03. Mai 2018, das ergänzend zur DS-GVO für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise gilt.

Das *Bundesdatenschutzgesetz (BDSG)* gilt im Wesentlichen für Bundesbehörden.

Seitenanfang

2. Personenbezogene Daten

Gegenstand des Datenschutzes sind personenbezogene Daten. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ("betroffene Person") beziehen (Art. 4 Nr. 1 DS-GVO). Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer *Online*-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Seitenanfang

3. Rechtsgrundlagen der Verarbeitung

Soweit für Verarbeitungsvorgänge personenbezogener Daten eine Einwilligung der betroffenen Person erforderlich ist, dient Art. 6 Abs. 1 lit. a DS-GVO als Rechtsgrundlage.

Bei der Verarbeitung von personenbezogenen Daten, die zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, erforderlich ist, dient Art. 6 Abs. 1 lit. b DS-GVO als Rechtsgrundlage. Dies gilt auch für Verarbeitungsvorgänge, die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind.

Soweit eine Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der die Hochschule Fulda unterliegt, dient Art. 6 Abs. 1 lit. c DS-GVO als Rechtsgrundlage.

Für den Fall, dass lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person eine Verarbeitung personenbezogener Daten erforderlich machen, dient Art. 6 Abs. 1 lit. d DS-GVO als Rechtsgrundlage.

Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der Hochschule Fulda übertragen wurde, so dient Art. 6 Abs. 1 lit. e DS-GVO i.V.m. einer einschlägigen, spezialrechtlichen bundes- oder landesrechtlichen Norm als Rechtsgrundlage für die Verarbeitung.

Seitenanfang

4. Schutzmechanismen

a. Die Verarbeitung personenbezogener Daten auf öffentlich zugänglichen Arbeitsplatzrechnern ist untersagt.

b. Arbeitsplatzrechner in Büroräumen sind besonders zu schützen, wenn auf ihnen personenbezogene Daten verarbeitet werden.

- Das Büro muss abgeschlossen werden, wenn es verlassen wird.
- Die Anmeldung am Rechner muss über ein sicheres Passwort geschützt sein.
- Das Starten des Arbeitsplatzrechners (*Boot*-Vorgang) muss durch ein Kennwort ("BIOS-Passwort", siehe Abschnitte "Funktionen" und "Sicherheit" in der deutschen Erklärung zum BIOS oder besser erklärt im Abschnitt "Configuration" in der englischen Erklärung zum BIOS) geschützt sein. Dieser Schutz muss auch dann wirksam sein, wenn ein *Eindringling* den Rechner mit einer eigenen CDROM, DVD, einem *Memory Stick* oder etwas Ähnlichem starten will. Falls der Rechner nicht über einen derartigen Kennwortschutz verfügt, dürfen die personenbezogenen Daten nur verschlüsselt auf der Festplatte gespeichert werden.
- Der Rechner muss entweder gegen Diebstahl gesichert sein oder er darf nur mit Wechselplatten betrieben werden, die nachts in einem einbruchsicheren Schrank aufbewahrt werden.
- Auf **portablen Datenträgern** (Festplatten in *Notebooks*, Wechselplatten, CDROM, DVD, *Memory Stick*, usw. dürfen personenbezogene Daten **nur verschlüsselt** gespeichert werden.
- Auf **Netzlaufwerken** der Hochschule, der **Hessenbox** und ähnlichen externen Speichermedien dürfen sensible personenbezogene Forschungsdaten nach Art. 9 DS-GVO, der die Verarbeitung besonderer Kategorien personenbezogener Daten

regelt, ebenfalls **nur verschlüsselt** gespeichert werden. Für die Verschlüsselung der Daten ist die jeweilige Person verantwortlich, die die Daten auf diesen Speichermedien ablegt.

c. Falls das Betriebssystem des Rechners den Schutz personenbezogener Daten unterstützt, müssen die entsprechenden Schutzmechanismen verwendet werden.

Seitenanfang

5. Löschen von Dateien

Das normale Kommando zum Löschen einer Datei streicht nur den Namen der Datei aus systeminternen Listen (z. B. dem Dateiverzeichnis), während der Dateiinhalt nicht zerstört wird. Speicherbereiche von gelöschten Dateien können unter Umständen (mit einigem Aufwand und entsprechender Kenntnis) wieder in lesbare Dateien verwandelt werden. Ein Zerstören der Dateiinhalte ist nur mit speziellen Betriebssystem-Kommandos (diese Kommandos werden nur von einigen Betriebssystemen zur Verfügung gestellt) oder speziellen Programmen möglich.

Falls ein Datenträger, auf dem personenbezogene Daten gespeichert worden sind, für den allgemeinen Betrieb freigegeben oder ausgesondert werden soll, müssen vorher alle Dateiinhalte zerstört werden.

Seitenanfang

6. Ausdrucken personenbezogener Daten

Personenbezogene Daten dürfen nur ausgedruckt werden, wenn die Druckausgabe persönlich überwacht wird.

Seitenanfang

7. Allgemeine Hinweise

Jede Person, die **mit personenbezogenen Daten** arbeitet, sollte ihre Arbeit **besonders verantwortungsvoll** durchführen, da alle Schutzmechanismen nur dann ihren Zweck erfüllen, wenn sie von den Beteiligten ernst genommen werden.

Zum Schluss noch einige allgemeine Tipps:

a. Lassen Sie keine schriftlichen Unterlagen herumliegen, aus denen Ihre Passwörter ersichtlich sind.
b. Lassen Sie keine andere Person unter Ihrer Kennung arbeiten.
c. Holen Sie Ausgabelisten und Datenträger mit personenbezogenen Daten persönlich ab, anstatt jemanden zu schicken.
d. Lassen Sie keine portablen Datenträger (CDROM, DVD, *Memory Stick*, usw.) mit personenbezogenen Daten herumliegen, sondern verschließen Sie die Datenträger in einem einbruchsicheren Schrank bevor Sie das Büro verlassen.

e. Speichern Sie personenbezogene Daten auf portablen Datenträgern nur in verschlüsselter Form.

Denken Sie daran, dass Sie persönlich in erster Linie für den Schutz der Ihnen anvertrauten Daten verantwortlich sind.

Seitenanfang

Letzte Änderung: 02. November 2021 | PDF-Version

Der erforderliche *Acrobat Reader* zum Lesen der PDF-Datei kann z. B. kostenlos von der Firma *Adobe* bezogen werden.