Datenschutz

Die Regeln des Datenschutzes sind auf mehrere Gesetze verteilt. Regelungen zum Datenschutz finden sich unter anderen im Bundesdatenschutzgesetz (BDSG), in den Landesdatenschutzgesetzen der Bundesländer sowie im Telekommunikationsgesetz (TKG) und im Telemediengesetz (TMG). Alle diese Datenschutzregeln haben dasselbe Ziel: Jeder Mensch soll sich frei und ohne Überwachung bewegen können. Dieser Grundsatz wird aus der Entscheidung des Bundesverfassungsgesetzes zur informationellen Selbstbestimmung hergeleitet. Das Recht auf informationelle Selbstbestimmung wird aus dem Grundrecht Art.1 Abs. 1 (Menschenwürde) und Art. 2 Abs.1 (Handlungsfreiheit) hergeleitet.

Struktur des Datenschutzes

Die Struktur des Datenschutzrechts ist einfach. Es gibt eine Regel und zwei Ausnahmen:

- Regel: Die Nutzung personenbezogener Daten ist verboten.
- Die Ausnahmen lauten: Ein Gesetz erlaubt ausdrücklich die Nutzung von personenbezogenen Daten für bestimmte Zwecke. Die Betroffenen haben eine Einwilligung in die Nutzung ihrer personenbezogenen Daten erteilt.

Personenbezogene Daten

Die Regeln des Datenschutzes bestimmen die Nutzung von Daten nur dann, wenn es sich um personenbezogene Daten handelt. Zu den personenbezogenen Daten nach § 3 Abs. 1 BDSG gehören Angaben beziehungsweise Informationen zu einer bestimmten oder bestimmbaren Person wie an folgendem Beispiel von Leon aufgezeigt:

Mit dem Zeitpunkt der Immatrikulation bekommt der Student Leon vom Studierendensekretariat Post mit Matrikelnummer und PIN. Zeitnah bekommt auch der zentrale IT-Service der Hochschule Daten wie den Namen des Studierenden, die Matrikelnummer, die verschlüsselte PIN, das Geburtsdatum sowie die Studienrichtung übermittelt. Diese Personenstammdaten werden jetzt in das Identity Management (IDM) zur Account-Verwaltung, Passwortverwaltung unter anderem gesendet. Im IDM einer Hochschule werden Personenstammdaten der Hochschulangehörigen aus den Verwaltungssystemen übernommen, die dann der IT-Infrastruktur zur Verfügung gestellt werden. Leon kann sich jetzt auch mit der Matrikelnummer und PIN ein Passwort setzen. Die personenbezogenen Daten werden auch von den Diensten wie zum Beispiel E-Mail, Moodle, BSCW verwendet. Bei der Nutzung der Dienste ist die Erstellung eines Verfahrensverzeichnisses erforderlich. Leon kann jetzt mit Matrikelnummer und Passwort auf die internen IT-Dienste der

Universität zugreifen.

Weitere Beispiele für personenbezogene Daten nach § 3 BDSG sind IP-Adressen, Personalausweisnummer, Telefonnummer sowie die Sozialversicherungsnummer.

> “
>
> ?
>
> Diskutieren Sie, welche personenbezogenen Daten möchten Sie von sich nicht weitergeben.

Verbot der Nutzung personenbezogener Daten

Die Datenerhebung, -verarbeitung und -nutzung von personenbezogenen Daten ist verboten (§ 4 Abs. 1 BDSG). Durch diese grundsätzliche Regelung macht der Gesetzgeber klar, dass personenbezogene Daten ein wertvolles, empfindliches Gut sind, mit dem sorgsam umgegangen werden muss.

> “
>
> !
>
> Deine Daten gehören Dir.

Gesetzliche Erlaubnis

Die erste Ausnahme zum grundsätzlichen Verbot ist die gesetzliche Erlaubnis. Soweit die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch ein Gesetz oder eine Rechtsvorschrift erlaubt sind, dürfen personenbezogene Daten verwendet werden (siehe dazu § 4 BDSG). Die Betroffenen sind daran gebunden und müssen die Nutzung der Daten dulden.

- Mit der Einschreibung von Leon (siehe oben) wurden viele personenbezogene Daten von der Hochschulverwaltung übernommen und weiter an die universitäre IT-Infrastruktur

übergeben. Die gesetzliche Erlaubnis ergibt sich aus dem Hochschulgesetz des Landes, sowie der Einschreibordnung der jeweiligen Hochschule. Leon kann sich gegen die Verwendung der Daten im Rahmen gesetzlicher Erlaubnisse nicht wehren.
- E-Prüfungen sind zulässig, soweit sie in Prüfungsordnungen von Hochschulen beschrieben sind. Auch hier bewegt sich eine Hochschule im rechtlich abgesicherten Bereich. Sobald die Hochschule aber Daten nutzt, die nicht in einer Prüfungsordnung oder einer anderen gesetzlichen Erlaubnis beschrieben sind, ist sie auf die Einwilligung der Studierenden angewiesen.Weitere Informationen zu E-Prüfungen und Recht finden Sie hier:

  http://ep.elan-ev.de/wiki/Rechtsfragen.

> “
>
> ## In der Praxis
>
> Ein Beispiel zur Regelung der E-Prüfungen findet man in der Rahmenprüfungsordnung (Seite 13) bei der Universität Duisburg-Essen:

http://www.uni-due.de/imperia/md/content/zentralverwaltung/bereinigte_sammlung/8_00_5.pdf

Eine Ordnung für E-Learning-Verfahren können Sie bei der Bergischen Universität Wuppertal einsehen (http://www.verwaltung.uni-wuppertal.de/am/2012/am12057.pdf) . Die Ordnung regelt netzangebundene Lern-, Lehr- und Prüfverfahren, die personenbezogene Daten zum Zwecke der wissenschaftlichen Ausbildung erheben, verarbeiten und nutzen. Hier werden die Datennutzung im Rahmen neuer Veranstaltungsformen aufgezeigt und geregelt.

Einwilligung

Die Erhebung solcher Daten, die üblicherweise in Präsenzveranstaltungen genutzt werden, ist durch die existierenden rechtlichen Regelungen gedeckt. Ungewöhnliche, neue Veranstaltungsformen, die das Potential von Lernplattformen nutzen und bei denen zum Beispiel Daten über das Verhalten der Studierenden laufend erhoben und gespeichert werden, um eine Verlaufsleistung der Studierenden zu bewerten, müssen durch eine Einwilligung der Studierenden gedeckt sein. Dies ist zum Beispiel dann der Fall, wenn in einem Kurs zum Projektmanagement die Studierenden ein begrenztes Budget an Zeit und an virtuellem Geld erhalten und jede ihrer Aktionen von der Plattform festgehalten und durch die Dozentinnen und Dozenten bewertet werden.

Wirksamkeit der Einwilligung. Allerdings ist eine Einwilligung gem. § 4a BDSG nur dann wirksam, wenn

- eine freie Entscheidung des Betroffenen zur Einwilligung führt,

- die Betroffenen umfassend über die Art der erhobenen Daten und den Umfang der Verarbeitung informiert werden,
- die Einwilligung schriftlich erfolgt.

Bei einer Einwilligung für Veranstaltungsformate, bei denen mehr personenbezogene Daten erhoben werden, als es in Präsenzveranstaltungen üblich ist, müssen mehrere Randbedingungen beachtet werden:

- Freiwillig ist eine Einwilligung nur dann, wenn sie sich auf eine Wahl- oder Wahlpflichtveranstaltung bezieht. Im Pflichtbereich wäre eine Einwilligung nicht freiwillig und damit unwirksam.
- Der Text der Einwilligung muss die geplante Erhebung und Nutzung der Daten umfassend beschreiben.
- Die Einwilligung muss schriftlich festgehalten werden. Dies kann durch Papier mit Unterschrift geschehen. Eine Einwilligung kann aber auch elektronisch erteilt werden (§ 13 Abs. 2 TMG). Der Text der Einwilligung kann so in einer Lernplattform platziert werden, dass die Teilnehmenden einer Veranstaltung mit einem Klick bestätigen müssen, dass sie die Einwilligung erteilen. Diese Erteilung muss in den Logfiles der Lernplattform gespeichert werden, damit die Hochschule in einem Konfliktfall nachweisen kann, dass bestimmte Studierende in die Nutzung der Daten einer bestimmten Veranstaltung zu einem bestimmten Zeitpunkt eingewilligt haben.

Missbrauch der Einwilligung. Der Text der Einwilligung muss auch den Hinweis enthalten, dass die Einwilligung jederzeit ohne negative Folgen für die Betroffenen zurückgezogen werden kann. Dies könnte Studierende mit schlechten Klausurergebnissen dazu verleiten, am Ende einer Veranstaltung die Einwilligung zurückzuziehen. Das folgenlose Zurückziehen der Einwilligung könnte dazu führen, dass den Studierenden kein Fehlversuch angerechnet wird und sie eine Prüfung so lange wiederholen, bis Ihnen das Ergebnis zusagt. So ein Verhalten ist nicht erlaubt. Die Hochschule muss das nicht dulden, denn die Studierenden missbrauchen ihre formale Rechtsposition (§ 242 BGB).

Einwilligung zur Nutzung von Facebook. Professor K. bietet zur Gruppenarbeit seiner Studierenden eine Facebook-Seite an. Das ist ein Online-Angebot der Hochschule. Selbst wenn die Studierenden in die Nutzung von Facebook freiwillig einwilligen, ist die Wirksamkeit der Einwilligung trotzdem zweifelhaft. Die Datenschutzbestimmungen von Facebook genügen wegen ihrer Unklarheit nicht den Anforderungen des deutschen Datenschutzrechts. Die Datenschutzbestimmungen von Facebook sind zwar sehr lang, enthalten aber weder klare Angaben zum Umfang der erhobenen Daten noch enthalten sie klare Angaben zur Verwendung der Daten. So wird zum Beispiel erklärt, dass Daten zur Verbesserung der Dienste an Dritte weitergegeben werden. Unklar bleibt, wann welche Daten an wen weitergegeben werden. Eine Einwilligung, die auf unvollständigen Informationen beruht, ist nicht bindend. Allerdings ist aufgrund der Organisationsstruktur von Facebook nicht deutsches, sondern irisches Datenschutzrecht für die Beurteilung der Rechtmäßigkeit relevant (OVG Schleswig Holstein, 2013). Damit ist die Unklarheit der Datenschutzbestimmungen bei Facebook mit deutschem Datenschutzrecht nicht angreifbar. Die Datenschutzbestimmungen werden aber unter dem Gesichtspunkt des Verbraucherschutzes mit deutschem Recht angegriffen (LG Berlin, http://www.vzbv.de/8981.htm). Die einschlägigen

Gerichtsverfahren sind noch nicht abgeschlossen. Damit ist juristisch noch nicht endgültig geklärt, ob die Datenschutzerklärungen von Facebook eine ausreichende Grundlage für bindende Einwilligungen sind. Professor K. sollte sehr vorsichtig damit sein, Facebook-Seiten für seinen Unterricht einzusetzen.

> “
>
> !
>
> Schütze Deine Privatsphäre.

Apps/Cloud Computing. Die Nutzung von Apps wird aus Sicht einer Hochschule dann problematisch, wenn in den Apps personenbezogene Daten der Studierenden an Dritte übertragen werden. Viele Apps nutzen nicht nur die Daten, die die Nutzer/innen eigenhändig in die App eingeben, sie nutzen auch das Umfeld des Betriebssystems, um weitreichende personenbezogene Daten zu erheben und an Dritte weiter zu verkaufen. Da die Weitergabe von personenbezogenen Daten an Dritte bei vielen App-Anbietern beziehungsweise -anbieterinnen das Geschäftsmodell ausmacht, wird die Hochschule wenig Erfolg bei dem Versuch haben, die App-Betreiber/innen zum Verzicht auf die Daten-Weitergabe zu bewegen. Die Hochschule muss dann auf den Einsatz verzichten.

Die Nutzung von Cloud Computing kann ebenfalls problematisch werden, wenn die Nutzungsbedingungen eine Kontrolle der Daten nicht garantieren. Die Nutzungsbedingungen von Google sind ähnlich unscharf wie die Nutzungsbedingungen von Facebook. Die Professorin W. würde die Daten ihrer Studierenden gefährden, wenn sie Google Drive zum Schreiben von Texten in ihrem Seminar einsetzen würde.

> “
>
> ?
>
> Überlegen Sie noch einmal, was ist eine gesetzliche Erlaubnis? Vergleichen Sie Ihre Gedanken mit Abschnitt 5.

> “
>
> # In der Praxis
>
> Die FH Düsseldorf hat im Juni 2013 den Service von Microsoft „Office 365” für Studierende auf Cloud-Basis eingeführt. Einwilligungen der Studierenden tragen

> den Prozess. Der Prozess wurde mit der Landesdatenschutzbehörde abgestimmt. Dies ist eine gelungene Auslagerung von Datenverarbeitung durch eine Hochschule.

http://www.fh-duesseldorf.de/a_fh/zeigeNewsLang?c_id=c20130620095024

> “
>
> !
>
> Eine Hochschule muss auf die Nutzung eines Cloud-Dienstes verzichten, wenn der Cloud-Anbieter die Einhaltung des Datenschutzes nicht garantieren kann (§ 11 BDSG).

Die Struktur des Datenschutzrechts in **Österreich** richtet sich nach den gleichen Grundprinzipien: Die Verwendung personenbezogener Daten ist verboten. Sie ist erlaubt, wenn ein Gesetz die Verwendung ausdrücklich gestattet oder wenn die Betroffenen der Verwendung zustimmen (§ 1 Abs. 2 DSG Ö). Die Zustimmung muss freiwillig, umfassend und in Kenntnis der Sachlage erfolgen (§ 4 Nr. 14 DSG Ö). Damit sind die Ausführungen für das Datenschutzrecht auf Österreich übertragbar.

In der **Schweiz** finden sich Regelungen zum Datenschutz in Gesetzen des Bundes und in Gesetzen der Kantone. Das Bundesgesetz über den Datenschutz regelt die grundlegende Struktur. Auch in der Schweiz ist die Verwendung personenbezogener Daten verboten, es sei denn, dass ein Gesetz die Verwendung ausdrücklich erlaubt oder dass die Betroffenen in die Verwendung eingewilligt haben (Art 17 DSG CH). Die Einwilligung muss freiwillig, umfassend und in Kenntnis der Sachlage erfolgen (Art. 4 Abs. 5 DSG CH). Damit sind die Ausführungen für das Datenschutzrecht auf die Schweiz übertragbar.

> “
>
> !
>
> Zahlreiche weiterführenden Links und Literaturhinweise finden Sie bei Diigo, versehen mit den Schlagworten #l3t, #recht, #de bzw. #at und #ch.

Revision #2
Created 28 February 2025 21:16:19 by Bernd Grabner
Updated 13 February 2026 14:20:46 by Github Admin