



Datenschutz bei Forschungsinformationssystemen

von Bernd Desoi¹

Forschungsinformationssysteme (FIS) werden an immer mehr Hochschulen und Universitäten implementiert. Die Systeme stellen eine integrierte Dokumentations- und Berichtsumgebung dar, die Leistungen und Ausstattung von forschenden Einrichtungen erfassen und sichtbar machen soll, sei es für interne wie externe Berichterstattung, Verwaltung oder auch zur Außendarstellung der Einrichtung. Integriert sind die Systeme durch verschiedenste Schnittstellen, allen voran zu Personalverwaltungssystemen oder auch Haushaltssystemen der jeweiligen Einrichtungen. Zusätzlich müssen die Systeme mit Daten durch die Forscher selbst „gefüttert“ werden. Die Systeme verarbeiten eine Vielzahl von personenbezogenen Daten zu ebenso vielfältigen Zwecken.

Dieser Beitrag gibt einen allerersten Überblick über (I) den Schutzbedarf der personenbezogenen Daten und die (II) Rechtsgrundlagen der Verarbeitung. Ebenso wird betrachtet, welche datenschutzrechtlichen Regelungen bei der Definition von (III) Rollen und Rechte, (IV) der Löschung von Daten, (V) der Verwendung von Bestandsdaten und (VI) der Datenerhebung auf freiwilliger Basis zu beachten sind. Aus den vorher gewonnen Erkenntnissen werden danach (VII) Implementationshinweise zur datenschutzrechtlichen Beteiligung gegeben.

I. Begriff und Bedeutung und Konfliktpotentiale im Umgang mit personenbezogener Daten

Anknüpfungspunkt einer datenschutzrechtlichen Betrachtung ist immer die Verarbeitung personenbezogener Daten. In den Datenschutzgesetzen des Bundes und Länder ist der

¹ Volljurist bei ZENDAS

Begriff „personenbezogene Daten“ üblicherweise definiert als “Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)” (vgl. § 3 Abs. 1 BDSG). Die Datenschutzgesetze beruhen auf dem Recht auf informationelle Selbstbestimmung, welches im Volkszählungsurteil des Bundesverfassungsgerichts erstmals ausformuliert wurde. Dies besagt: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ (BVerfG, Urteil vom 15. Dezember 2013, BVerfGE 65, 1 (43)). Geschützt sind die Betroffenen in allen Phasen der Datenverarbeitung umfassend, also von der Erhebung über weitere Verarbeitung bis hin zur Löschung eines Datums.

Hieraus werden diverse Grundsätze der Datenverarbeitung abgeleitet, die im geltenden Datenschutzrecht wiedergegeben sind. Die Verarbeitung personenbezogener Daten unterliegt dem Verbot mit Erlaubnisvorbehalt. Das heißt sie dürfen nur verarbeitet werden, wenn eine Einwilligung oder eine gesetzliche Ermächtigungsgrundlage diese Art der Verarbeitung erlaubt. Daher können in Forschungsinformationssystemen nicht beliebig personenbezogene Daten verarbeitet werden, vielmehr müssen die sich aus den datenschutzrechtlichen Bestimmungen regelmäßig ergebenden Vorgaben beachtet werden. Das gilt auch dann, wenn personenbezogene Daten etwa durch Publikationen in Fachzeitschriften oder im Internet an sich bereits bekannt sind. Weiterhin gilt der Grundsatz der Erforderlichkeit, wonach eine Verarbeitung personenbezogener Daten nur zulässig ist, wenn sie zur Aufgabenerfüllung erforderlich ist. Der Grundsatz der Datensparsamkeit als gestaltungsorientierte Fortsetzung der Erforderlichkeit verlangt, dass so wenig personenbezogene Daten wie möglich verarbeitet werden und der Kreis der an der Verarbeitung beteiligten Personen möglichst klein zu halten ist. Auch die im Rahmen einer jeden Datenverarbeitung zu treffenden technischen und organisatorischen Maßnahmen verlangen neben der allgemeinen Datensicherheit auch die technische Beschränkung des Datenzugriffs auf solche Personen, die diesen innerhalb der Einrichtung zur Erfüllung ihrer Aufgabe benötigen. Auch folgt daraus, dass Daten, die nicht mehr erforderlich sind, gelöscht werden müssen. Hier wird auch deutlich, dass eine Datenverarbeitung

immer nur zu einem oder mehreren bestimmten Zwecken erfolgen darf (Grundsatz der Zweckfestlegung und -bindung).

Die Motivation zur Beachtung datenschutzrechtlicher Anforderungen ist gerade bei Hochschulen und Universitäten nicht nur rein datenschutzrechtlicher Natur. Entscheidend sind zwei Dimensionen:

Zum einen sind Hochschulen und Universitäten deutlich geprägt von der Eigenständigkeit der Fakultäten, Institute und Lehrstühle. Eine datenschutzgerechte Gestaltung der Forschungsinformationssysteme ist hier Voraussetzung für eine breite Akzeptanz der Systeme, die letztlich die Funktionsfähigkeit gewährleistet. Zum anderen kommt hinzu, dass die Forscher als Betroffene auch Arbeitnehmer der jeweiligen Einrichtung sind, was zu Beteiligungsverfahren von Personal- oder Betriebsräten führen kann. Auch hier gilt es, mögliche Konflikte durch eine datenschutzkonforme Gestaltung von Beginn an zu vermeiden.

II. Rechtsgrundlage(n) für die Erhebung und weitere Verarbeitung von Daten

Aufgrund des statuierten Verbots mit Erlaubnisvorbehalt muss jede Datenverarbeitung mittels eines Forschungsinformationssystems reflektiert werden. Gesetzliche Ermächtigungsgrundlagen erlauben die Datenverarbeitung regelmäßig für bestimmte und festgelegte Zwecke. Angesichts der vielfältigen Einsatzmöglichkeiten werden die Daten innerhalb eines Forschungsinformationssystems für viele verschiedene Zwecke verarbeitet. Ein Blick auf die in Einsatz und Planung befindlichen Forschungsinformationssysteme zeigt, dass sowohl die erfassten Merkmale wie auch die Verwendungszwecke keineswegs einheitlich sind. Die Ermächtigungsgrundlagen beantworten indes nicht nur die Frage nach der Zulässigkeit der Datenverarbeitung zu einem bestimmten Zweck (das „Ob“ der Datenverarbeitung), sondern es ergeben sich auch Vorgaben für die Gestaltung der Datenverarbeitung (das „Wie“ der Datenverarbeitung). Diese betreffen nicht nur die technische und organisatorische Ausgestaltung der Datenverarbeitung, sondern den kompletten Prozess der Implementierung von Datenverarbeitungsverfahren.

Ausgehend von dem jeweiligen Zweck einer Datenverarbeitung muss zunächst hinterfragt werden, ob die Verarbeitung personenbezogener Daten zu diesem Zweck zulässig

ist. Bezogen auf das „Ob“ der Datenverarbeitung sind die Ermächtigungsgrundlagen der Datenverarbeitung für staatliche Hochschulen und Universitäten der Länder zumeist in den jeweiligen Landeshochschulgesetzen oder Landesdatenschutzgesetzen zu finden. Private Hochschulen sowie Hochschulen des Bundes finden diese in dem Bundesdatenschutzgesetz. Meist erlauben Generalklauseln innerhalb der Datenschutzgesetze die Erhebung oder weiter Verarbeitung von personenbezogenen Daten für die Erfüllung der Aufgaben einer öffentlichen Stelle – hier Hochschule oder Universität – oder im Falle privater Hochschulen für die Erfüllung eigener Geschäftszwecke. Je nach Verwendung der Daten können Ermächtigungsgrundlagen auch in speziellen Vorschriften gefunden werden. So ist etwa die Transparenz der Drittmittelforschung in Baden-Württemberg im § 41a Landeshochschulgesetz (LHG) speziell geregelt. Soweit ein Forschungsinformationssystem etwa dazu genutzt wird, ergibt sich die Zulässigkeit der Datenverarbeitung aus dieser Norm.

III. Rollen und Rechte

Neben der Zulässigkeit der Datenverarbeitung erwachsen aus dem Datenschutzrecht weitere Anforderungen für die Gestaltung der Datenverarbeitung. Eine ganz wesentliche Anforderung ist die Definition eines logischen Rechte- und Rollenkonzepts, nach welchem sich die Zugriffsrechte der einzelnen Beteiligten auf etwaige Daten richten. Aus dem logischen Rechte- und Rollenkonzept muss sich nicht nur die Frage des „Ob“ eines Datenzugriffs ergeben, sondern vielmehr die Frage auch des Umfangs des Zugriffsrechtes im Sinne eines lesenden/schreibenden/ändernden Zugriffsrechts. Dazu bedarf es einer genauen Betrachtung der verschiedenen Beteiligten in ihren unterschiedlichen Rollen. Hier sind zunächst die Forscher selbst zu nennen, bei denen regelmäßig zwischen dem einfachen Forscher und Projektverantwortlichen zu unterscheiden ist. Innerhalb der universitären Strukturen sind Zugriffsrechte zunächst innerhalb der universitären Leitungsstrukturen korrespondierend zu den internen Berichtspflichten gegeben. Auf administrativer Ebene können verschiedene Gebiete eingebunden sein. Dies betrifft allgemein die Personalabteilung, Drittmittelabteilung oder auch das universitäre Qualitätsmanagement. Die Zugriffsrechte können im Weiteren noch nach Fakultätsebenen oder auch nach zentralen Ebene differenziert werden, so dass sich hieraus letztlich die Rollen ergeben. Welche Form der Zugriffsrechte der jeweiligen identifizierten Zugriffsrolle eingeräumt wird, muss aus der für die Rolle maßgeblichen Ermächtigungsgrundlage abgeleitet

werden. Es gilt zu fragen: Zur Erfüllung welcher ihnen übertragenen Aufgabe benötigen welche Mitarbeiter (Definition der Rolle) welches Recht des Zugriffs (Definition des Rechts).

Die Erstellung eines logischen Rollen- und Rechtekonzepts ist frühzeitig anzugehen, da sich in einem weiteren Schritt technische Anforderungen an das System ergeben. Diese Anforderungen müssen bereits in der Phase der Auswahl und Beschaffung eines Systems berücksichtigt werden.

IV. Datenlöschung

Das zu erarbeitende Rollen- und Rechtekonzept entscheidet über die Rechte der Beteiligten in den jeweiligen Phasen der Datenverarbeitung. Die Phase der Löschung von Daten ist besonders zu beachten, da keine Datenverarbeitung „ewig“ laufen darf, sondern vielmehr personenbezogene Daten immer dann zu löschen sind, wenn diese zur Erfüllung eines bestimmten Zwecks nicht mehr notwendig sind. Auch in komplexen Verfahren ist daher immer ein abstraktes Löschkonzept zu entwerfen und letztlich in einem aus datenschutzrechtlicher Sicht notwendigen Verfahrensverzeichnis zu dokumentieren.

Für die Bestimmung der Löschfristen ist immer aus Perspektive der jeweiligen Rolle zu fragen, die letztlich zur Erfüllung eines bestimmten Zwecks eingerichtet ist, ob das Datum tatsächlich noch erforderlich ist. Hier reicht es nicht aus, nur das grundsätzliche Datum anzuschauen, sondern vielmehr muss die Erforderlichkeit des Datums im jeweiligen Forschungsinformationssystem hinterfragt werden. Dies betrifft insbesondere Publikationen. Der Umstand der Veröffentlichung bedeutet nicht automatisch, dass man ein personenbezogenes Datum dauerhaft weiter im eigenen System speichern darf. Andererseits bedeutet das Ausscheiden eines Wissenschaftlers wiederum auch keine automatische Pflicht zu Löschung. Sollten andere Prozesse wie Drittmittelanzeigen oder ähnliches im Forschungsinformationssystem verarbeitet werden, ist auch hier zu hinterfragen, wie lange die Information vorgehalten wird. Hier muss man auch immer im Blick haben, welche anderen Systeme diese Daten verarbeiten. Die stark diversifizierte Landschaft der Hochschulverwaltungsprozesse lässt hier keine konkreten Ratschläge zu. Im Ergebnis bleibt immer die eine Frage: Wie lange müssen welche Daten für welchen Zweck im System vorgehalten werden?

Hier wird auch ein weiterer Aspekt des Rollen- und Rechtekonzepts deutlich: Zugriffsberechtigungen dürfen nur so lange bestehen bleiben, wie die jeweilige Rolle den Zugriff benötigt.

V. Verwendung von Bestandsdaten für FIS

Forschungsinformationssysteme werden in aller Regel über Schnittstellen mit verschiedensten bestehenden Systemen innerhalb der Universitäten gekoppelt. Das können etwa Personalverwaltungssysteme oder haushälterische Verwaltungssysteme sein. Hier muss immer auch gefragt werden, ob die personenbezogenen Daten, die in einem bestimmten System vorhanden sind, für den Verwendungszweck, für den sie im FIS verarbeitet werden sollen, verwendet werden dürfen. Dies dürfte in der Regel der Fall sein. In Einzelfällen kann es aber vorkommen, dass Bestandsdaten nicht verwendet werden dürfen, weil im konkreten Fall

- keine Rechtsvorschrift die zweckändernde Nutzung rechtfertigt,
- eine Zweckbegrenzung durch vormalig benutzte Datenschutzhinweise besteht (die beispielsweise im Rahmen der Einstellung Beschäftigten gegenüber gemacht wurden),
- eine zuvor gegebene Einwilligung (die ohnehin nur mit Vorsicht verwendet werden sollte) dies nicht rechtfertigt oder
- eine besondere Geheimhaltungsbedürftigkeit besteht.

Perspektivisch könnte auch in Betracht gezogen werden, beispielsweise bei der Einstellung von Wissenschaftlern entsprechende Datenschutzhinweise zu geben, die nicht zuletzt auch zur Erhöhung der Akzeptanz des Systems beitragen können.

VI. Datenerhebung auf freiwilliger Basis

Je nach Ausgestaltung des FIS kann es notwendig sein, bei der Nutzung jedenfalls teilweise auf Einwilligungen zurückzugreifen. Grundsätzlich sollte dies eine Ausnahme sein, da der Gesetzgeber Regeln geschaffen hat, nach denen Hochschulen personenbezogene Daten verarbeiten dürfen, soweit es für ihre Aufgabenerfüllung erforderlich ist. Jede Einwilligung unterläuft dieses System und sollte daher nur als absolute Ausnahme denkbar sein. Das könnte etwa dann der Fall sein, wenn das FIS gleichzeitig die Publikationen für Webseiten aufbereitet und auch Lichtbilder der Wissenschaftler erforderlich sind. Dies

bedarf aus persönlichkeitsrechtlichen Gründen der Einwilligung. Hier muss klar sein: Eine Einwilligung darf nur freiwillig erfolgen und es darf auch kein faktischer Zwang entstehen. Überdies ist eine Einwilligung widerruflich, das bedeutet im Ergebnis, dass auch die Daten gelöscht werden müssen. Zuletzt muss aus datenschutzrechtlicher Sicht bei der Einwilligung entsprechend informiert werden. Die Hinweispflichten sind hier noch länderspezifisch. Spätestens mit Geltung der Datenschutz-Grundverordnung ab dem 25. Mai 2018 sind jedoch sehr umfangreiche Hinweise zu erteilen. Dies sollte bereits bei der Implementierung berücksichtigt werden.

VII. Implementationshinweise

Die Erfordernisse des Datenschutzes sollten möglichst frühzeitig bei der Implementation eines FIS Beachtung finden. Das gilt nicht nur aus den zuerst genannten Gründen der Konfliktvermeidung, sei es in der universitären Binnenstruktur oder aus Arbeitnehmerperspektive heraus. Auch müssen die Grundstrukturen möglichst bereits bei der Vergabe etwaiger Aufträge feststehen, damit die datenschutzrechtlichen Anforderungen in Vergabeverfahren einfließen können. Vor Inbetriebnahme muss auch ein sogenanntes Verfahrensverzeichnis erstellt werden. Ein Verfahrensverzeichnis ist eine obligatorische Dokumentation für Verfahren der automatisierten Verarbeitung personenbezogener Daten. Hier müssen Verfahrenszwecke, alle personenbezogenen Daten, die Betroffenen, Zugriffsrechte und Löschfristen sowie technischer Aufbau und Schutzmaßnahmen dokumentiert werden. Die Erstellung eines Verfahrensverzeichnisses wird zwar als lästige Pflicht empfunden, oft zeigt sich jedoch, dass Systeme zwar fertig gekauft, aber Prozesse nicht fertiggedacht sind. Das Verfahrensverzeichnis ist insofern eine Chance und kein Problem. Neben den datenschutzrechtlichen Vorgaben sind auch personalvertretungsrechtliche Beteiligungsverfahren zu beachten, die sich aus den jeweiligen Gesetzen für die Verarbeitung personenbezogener Arbeitnehmerdaten ergeben. Gegebenenfalls kann auch die Notwendigkeit einer Vorabkontrolle bzw. Datenschutz-Folgenabschätzung gegeben sein. Hier ist über die Dokumentation eines Verfahrensverzeichnisses hinaus das Ergebnis einer Abwägung zwischen den Zwecken der Datenverarbeitung und den Folgen für die Betroffenen darzustellen und das Ergebnis unter Einbindung des Datenschutzbeauftragten der Einrichtung zu dokumentieren.

Überdies kann sich die Notwendigkeit des Abschlusses einer sogenannten Vereinbarung zu Datenverarbeitung im Auftrag ergeben. Dies ergibt sich aus dem Umfang der Leistung des Anbieters und ist im Rahmen der Vertragsverhandlungen zu klären. Sofern der Anbieter eines Systems Zugriff auf personenbezogene Daten eine FIS erhält – etwa weil er es wartet – ist ein solcher Zusatzvertrag obligatorisch.

Im Ergebnis gilt: Je früher datenschutzrechtliche Betrachtungen berücksichtigt werden, desto besser. Gerade in einem etwaigen Vergabeverfahren sollte bereits klar sein, welcher Funktionsumfang gewollt ist und welche Datenverarbeitungen damit verbunden sind. So kann die Grundlage für ein FIS geschaffen werden, was von allen Seiten akzeptiert wird und letztlich auch nur so funktionieren kann.

17.08.2016

ZENDAS - Die Zentrale Datenschutzstelle der baden-württembergischen Universitäten bietet Informationen rund um das Thema "Datenschutz in der Hochschule" und unterstützt die Universitäten des Landes Baden-Württemberg und ihre Vertragspartner – Hochschulen, Universitäten sowie weitere Bildungs- und Forschungseinrichtungen aus dem Bundesgebiet und deutschsprachigen Ausland. Gegen Entgelt sind auf dem ZENDAS Info-Server (www.zendas.de) zahlreiche datenschutzrechtliche Themen aus der hochschultypischen Sicht nicht nur für Rechtsdezernate oder sonstige Verwaltungseinrichtungen, sondern auch für Rechenzentren und deren Entscheidungsträger aufbereitet.