mpuls_S und die Intevation GmbH aus datenschutzrechtlicher Sicht

mpuls_S ist eine Software, mit der Anträge, Vergabe und Abwicklung von Deutschlandstipendien verwaltet werden können, mithin personenbezogene Daten verarbeitet werden.

Aus datenschutzrechtlicher Sicht ist der Vorgang unter zwei Gesichtspunkten bedeutsam:

1. Muss die Software an sich vom Funktionsumfang her aus datenschutzrechtlicher Sicht geeignet sein.
2. Ist zu prüfen, ob die Hochschule beim Betrieb der Software einen Dienstleister einschaltet, beispielsweise beim Application Service Providing. Wenn ja, liegt eine Datenverarbeitung im Auftrag vor, die zur Voraussetzung hat, dass der Auftragnehmer – etwas pauschal ausgedrückt - hinsichtlich der Gewähr, für ausreichenden Schutz der Daten zu sorgen, geprüft werden muss.

Wenn eine Hochschule die Software mpuls_S der Fa. Intevation GmbH einsetzt, erfolgt dies nach dem Angebot der Fa. Intevation GmbH in der Form, dass die Software gehostet wird. Für das Hosting greift die Fa. Intevation GmbH auf die Dienstleistung der OpenIT GmbH zurück.
Damit liegt eine Datenverarbeitung im Auftrag vor (§ 7 LDSG BW[1]) und zwar zum einen zwischen Hochschule und Intevation GmbH und zum andern zwischen Intevation GmbH und OpenIT GmbH (§ 11 BDSG).

Die Hochschule hat den Auftragnehmer sorgfältig auszuwählen, wobei besonders zu berücksichtigen ist, ob der Auftragnehmer ausreichend Gewähr dafür bietet, dass er die für eine datenschutzgerechte Datenverarbeitung erforderlichen technischen und organisatorischen Maßnahmen zu treffen in der Lage ist (§ 7 Abs. 2 LDSG BW).

Verantwortlich für die gesamte Datenverarbeitung, auch beim Auftragnehmer, ist der Auftraggeber, dessentwegen er vollumfänglich Kenntnis von den Vorgängen bei Intevation GmbH und deren Subunternehmer haben muss.

[1] Genannt werden in diesem Dokument Vorschriften des baden-württembergischen Landesdatenschutzgesetzes. In den anderen Bundesländern finden sich jedoch ebenfalls entsprechende gesetzliche Regelungen, so dass das Dokument problemlos auf andere Bundesländer übertragen werden kann.

ZENDAS hatte zur Klärung diverser Fragen zwischen Juli und Anfang Oktober 2011 mit der Fa. Intevation GmbH mehrmalig Kontakt und konnte an einigen Punkten aus datenschutzrechtlicher Sicht Verbesserungen erreichen.

Leider gelang dies nicht vollständig und nicht in zwei wesentlichen Fragestellungen, so dass ZENDAS mit Stand vom 11.10.11 zum Ergebnis kommen, dass **gegen den Einsatz der Software mpuls_S in der zu diesem Zeitpunkt bestehenden Version datenschutzrechtliche Bedenken bestehen**.

Das Dokument erhebt keinen Anspruch auf die Vollständigkeit der datenschutzrechtlich zu prüfenden Fragestellungen, gibt aber eine Übersicht der wesentlichen Aspekte, die ZENDAS näher untersucht hat und kann zu eigenen, ggf. weitergehenden Prüfungen eine Hilfestellung sein.

Gleich zu Beginn gehen wir auf die zwei Punkte ein, die ZENDAS bewogen hat, datenschutzrechtliche Bedenken gegen den Einsatz der Software zu artikulieren.

1. Anonymisierungsfunktion

Die Software bietet eine sog. „Anonymisierungsfunktion". Dabei werden aus den Datensätzen bestimmte Felder gelöscht. Welche Felder nicht gelöscht werden, lässt sich der Auflistung unter 7.2. des Dokuments „Spezifikation Formulare – Datenmodell Stipendiatinnen und Stipendiaten"[2] (Stand 05.08.11) entnehmen.

Die so „anonymisierten" Daten können dem BMBF für die programmbegleitende Evaluation zur Verfügung gestellt werden. Dazu können sie auf einen Auswertungsserver übertragen werden.

1.1. Bewertung

Die Bezeichnung Anonymisierungsfunktion halten wir für **irreführend**, weil sie suggeriert, es werden im Sinne des Datenschutzrechts anonyme Daten hergestellt. Dies ist aber nicht der Fall:
Der verbliebene Datensatz ist aus der Summe der Merkmale für die Hochschule nach wie vor **personenbeziehbar** (z.B. Geschlecht, Studienfachrichtung, Staatsangehörigkeit, Semesterzahl, etc.). **Die Anonymisierungsfunktion ist also nicht geeignet, an Stelle der Löschung eine Anonymisierung durchzuführen.**

[2] Soweit hier auf Dokumente zu mpuls_S verwiesen wird, sind diese im Internet zu finden unter http://doku.mpuls-s.de/

Würde die Hochschule damit dem BMBF Daten zur Verfügung stellen, stellt sie personenbezogene Daten zur Verfügung, wofür wir **keine** Rechtfertigung erkennen.

Vom Einsatz einer Software, die eine Funktion bietet, die das Wort „Anonymisierung“ in sich trägt, die aber nicht das erfüllt, was das Wort „Anonymisierung“ rechtlich beinhaltet, muss datenschutzrechtlich abgeraten werden.

Für entsprechend kritisch halten wir die Ausführungen im Anwenderhandbuch (Stand 26.09.11), wonach mpuls_S bei allen Funktionen den Datenschutzanforderungen entspricht (S. 5).

Zwar könnte ein „Workaround“ darin bestehen, dass organisatorisch geregelt wird, dass diese Funktion nicht genutzt wird und die Software von vorneherein so konfiguriert wird, dass keinerlei Daten an das BMBF übertragen werden. Jedoch kennen Datenschutzbeauftragte zur Genüge, welches Schicksal organisatorische Maßnahmen in aller Regel früher oder später ereilt: Sie werden vergessen. Insbesondere dann, wenn der Sachbearbeiter wechselt. Irgendwann wird dann eine Funktion, die „Anonymisierung“ heißt, auch mit dem Gedanken verwendet, sie tue dies, was die Bezeichnung vorgibt.

Leider hat die Firma die Vorschläge von ZENDAS nicht aufgegriffen, die Funktion entweder einfach umzubenennen oder den Umfang der Daten, die nach Ausführen der Funktion noch übrig bleiben, dahingehend zu verringern, dass man tatsächlich von „anonymen“ Daten im Sinne von bspw. § 3 Abs. 6 LDSG BW sprechen kann. Die Intevation GmbH hält den im StipG abgegrenzten Datensatz (gemeint war wohl der für die Statistikmeldung nach § 13 StipG) für sinnvoll und sieht dies als „guten Bezug, einen unter allen DS-Beauftragten der teilnehmenden Hochschulen konsensfähigen Umfang zu definieren“.
ZENDAS hält diesen Umfang bei Bezeichnung der Funktion unter Verwendung eines datenschutzrechtlichen Terminus allerdings gerade nicht für konsensfähig.

2. Protokolldaten

mpuls_S schreibt – wie viele andere Softwareprodukte auch – Protokolldaten.
Protokolldaten sind in aller Regel personenbezogen, da entweder ein Benutzername oder die IP-Adresse derer protokolliert wird, die auf die Software zugreifen. Hierbei sind Daten von Mitarbeitern der Hochschule betroffen.
Das Schreiben dieser Daten muss – wie jede andere Datenverarbeitung auch – gerechtfertigt werden können.

Auch mpuls_S schreibt Protokolldaten:

Sowohl bei erfolgreichen als auch bei nicht erfolgreichen Zugriffen werden an verschiedenen Stellen unter anderem protokolliert:

1. vollständige IP-Adresse.
2. Datum und Uhrzeit des Zugriffs.
3. Methode (HTTP Verb) des Zugriffs mit Pfad und Protokollversion
4. HTTP Statuscode
5. Anzahl übertragener Bytes
6. Vollständige URL des anfragenden Benutzers inklusive GET-Parameter
7. Browserkennung des anfragenden Benutzers

Der Zweck der Protokollierung wurde mit der technisch-organisatorischen Maßnahme der „Eingabekontrolle“ (§ 9 Abs. 3 Nr. 7 LDSG BW) angegeben.

Die Protokollierung ist so umgesetzt, dass Zugriff auf die Protokolldaten auf Seiten der Hochschule, die das Hosting beauftragt, niemand hat, auch nicht Nutzer mit der Rolle Administrator. Lediglich die Systemadministratoren der Intevation GmbH haben im Rahmen ihrer Arbeit Zugriff auf die Protokolldaten.

Entsprechend müsste, wenn die verantwortliche Stelle Hochschule also zur Eingabekontrolle auf die Daten zugreifen möchte, eine Anfrage an die Intevation GmbH gehen. Begründet wird dies damit, dass der Auftraggeber gerade nicht mehr tief im Detail arbeiten möchte, sondern dafür der Auftragnehmer zur Verfügung steht.

2.1. Bewertung

Wenn eine Hochschule mpuls_S einsetzt, ist sie diejenige Stelle, die **jegliche** damit verbundene Verarbeitung personenbezogener Daten rechtfertigen muss.
Dies gilt auch dann, wenn sie die Firma Intevation GmbH mit dem Hosting beauftragt. Dann liegt eine Datenverarbeitung im Auftrag vor, bei der die Verantwortung für jegliche Datenverarbeitung aber gerade beim Auftraggeber verbleibt.
Die Protokollierung wird pauschal mit der Eingabekontrolle begründet. Dies bedeutet, dass jedes einzelne Datum in den Logfiles damit begründet wird. Diese Begründung ist jedoch für eine Reihe von derzeit protokollierten Merkmalen nicht nachvollziehbar.
Sinn und Zweck der Eingabekontrolle ist es, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem im Datenverarbeitungssys-

tem eingegeben worden sind. Damit sind die zu diesem Zweck erforderlichen Daten schon von Gesetzes wegen klar begrenzt.
ZENDAS hat unter anderem die Frage gestellt, wozu man unter diesem Gesichtspunkt dann dafür beispielsweise nachstehende Daten benötigt:

- Methode (HTTP Verb) des Zugriffs mit Pfad und Protokollversion
- HTTP Statuscode
- Anzahl übertragener Bytes
- Vollständige URL des anfragenden Benutzers inklusive GET-Parameter
- Browserkennung des anfragenden Benutzers

Die Intevation GmbH hat ZENDAS daraufhin mitgeteilt, dass sie nicht die einzelnen Einträge in die Protokolldatei diskutieren werde.

Damit wird die datenschutzrechtliche Verantwortlichkeit eklatant verkannt.

Bislang ist der Umfang der Protokolldaten nicht nachvollziehbar für die Hochschule zu rechtfertigen. Die Hochschule muss allerdings die Rechtfertigung dafür übernehmen. Aus datenschutzrechtlicher Sicht erscheint uns der derzeitige Umfang der Protokollierung zu umfassend.
Dem Einsatz der Software begegnen aus diesem Grund datenschutzrechtliche Bedenken.

Zudem muss sich jede Hochschule bewusst sein, dass sie für einen Zugriff auf die Protokolldaten die (kostenpflichtige?) Unterstützung der Intevation GmbH benötigt.

3. Rechtsgrundlage für die Datenverarbeitung, Umfang der Felder

Die Hochschule darf nur dann personenbezogene Daten verarbeiten, wenn dafür entweder eine Rechtsgrundlage vorliegt oder die Betroffenen eingewilligt haben (vgl. § 4 LDSG BW). Es dürfen entsprechend auch nur diejenigen Daten verarbeitet werden, die von der Rechtsgrundlage bzw. der Einwilligung gerechtfertigt werden.

Rechtsgrundlage für die Datenverarbeitung sind das Gesetz zur Schaffung eines nationalen Stipendienprogramms (StipG) sowie die Verordnung zur Durchführung des Stipendienprogramm-Gesetzes (StipV). § 3 StipG und § 2 StipV enthalten einen Katalog der Auswahlkriterien, mithin der Daten, die die Hochschule verarbeiten darf. Hinzu kommen noch Daten für die Bundesstatistik nach § 13 StipG.

Darunter sind beispielsweise mit Behinderung auch Daten, die das Gesetz als „besondere Arten personenbezogener Daten“ einstuft (§ 33 LDSG BW). Diese dürfen u.a. verarbeitet werden, wenn eine besondere Rechtsvorschrift dies vorsieht (§ 33 Abs. 1 Nr. 1 LDSG BW). Die Rechtsvorschriften des StipG und der StipV sind solche Rechtsvorschriften.
Zudem ist es auch möglich, ein Stipendium zu beantragen, ohne Angaben zu diesen Punkten zu machen.

Damit liegt u.E. eine ausreichende Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Hochschule vor.

Die Beschreibung „Spezifikation Formulare – Datenmodell Stipendiatinnen und Stipendiaten“ (Stand 05.08.11) enthält die Felder und damit die Daten, die das Programm verarbeitet. Dieser Katalog entspricht u. E. dem, was die Rechtsgrundlagen als zu verarbeitende Daten gestatten und geht nicht darüber hinaus.

4. Speicherdauer

Da weder das StipG noch die StipV bereichsspezifische Regelungen zur Speicherdauer der Daten enthalten, ist das allgemeine Datenschutzrecht (LDSG BW) zu beachten.
Danach sind personenbezogene Daten u.a. dann zu löschen, wenn „ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.“ (§ 23 Abs. 1 Nr. 2 LDSG BW).
Hierfür ist zu unterscheiden zwischen denjenigen, denen eine Förderung versagt wurde und denjenigen, die schließlich die Förderung erhalten:

4.1. Abgelehnte Bewerber

Eine Bemerkung vorweg: Wir halten es nicht für zulässig, mit der Begründung, die Bewerber könnten sich nächstes Semester wieder bewerben, die Daten zu speichern (genau diese Begründung wird aber auf dem Hinweisblatt zum Datenschutz angegeben, das die Software anbietet, siehe dazu 6.). Denn erstens ist ungewiss, ob sie dies tatsächlich tun und es würde somit bei einer Vielzahl von Personen zu einer nicht erforderlichen Speicherung auf Vorrat kommen und zweitens können sich bis dahin auch persönlichen Umstände und damit Auswahlkriterien geändert haben, so dass die Daten nicht mehr richtig sind.
Es stellt aus unserer Sicht kein Problem dar, wenn die Bewerber eine vollständige neue Bewerbung abgeben müssen.

Nicht mehr erforderlich zur Aufgabenerfüllung der Hochschule sind die Daten der abgelehnten Bewerber dann, wenn sie keine rechtlichen Schritte gegen die Ablehnung mehr geltend machen können.
Wir gehen davon aus, dass die Ablehnung mit einer Rechtsbehelfsbelehrung erfolgt.
Damit werden die Ablehnungsbescheide nach einem Monat bestandskräftig. Wer nach Bestandskraft dagegen vorgehen möchte, muss Gründe geltend machen, die einen Antrag auf Wiedereinsetzung in den vorigen Stand rechtfertigen. Ein Antrag auf Wiedereinsetzung in den vorigen Stand ist im Regelfall bis max. 1 Jahr seit dem Ende der versäumten Frist zulässig (§ 60 Abs. 3 Verwaltungsgerichtsordnung).
Wenn man diesen Fall mit berücksichtigt, ergibt sich damit eine maximale Aufbewahrungsfrist von 13-14 Monaten nach Zusendung des Bescheids.

Nicht davon erfasst sind natürlich die Fälle, in denen die Bestandskraft eines Bescheids nicht erreicht wird, weil Rechtmittel eingelegt werden. Dann darf natürlich auch die Löschung erst erfolgen, wenn das Verfahren endgültig abgeschlossen ist.

4.2. Geförderte Stipendiaten

Die Daten der angenommenen Bewerber, also letztliche geförderten Stipendiaten, werden zunächst natürlich während der Dauer der Förderung zur Aufgabenerfüllung benötigt.

Die Fa. Intevation GmbH hatte in Übereinstimmung mit dem BMBF die Aufbewahrungsfrist auf 6 Jahre gesetzt. Begründet wird dies damit, dass die Geldmittel den Ländern unter den Bedingungen der ANBest-P (Allgemeine Nebenbestimmungen zur Projektförderung) zur Verfügung gestellt werden. Nach Ziffer 6.5. seien die Unterlagen fünf Jahre nach Vorlage der Verwendungsnachweise vorzulegen. Verwendungsnachweise seien bis zum 30.6. des auf die Förderung folgenden Jahres vorzulegen. So ergeben sich insgesamt 6 Jahre.
Das Wissenschaftsministerium in Baden-Württemberg leitet die Mittel nicht unter Verweis auf die ANBest-P weiter, hat jedoch vergleichbare Bedingungen.

Daher **teilt ZENDAS die Überlegungen zur Aufbewahrungsdauer**.

Allerdings sind wir nicht der Auffassung, dass dies **im System mpuls_S zu** erfolgen hat. Im Gegenteil:
Das führende System für den Nachweis von Zahlungen und damit der Mittelverwendung ist das Mittelbewirtschaftungssystem, in dem die entsprechenden Unterlagen enthalten sind sowie die Unterlagen in Papierform. Dort werden die Zahlungen nach-

gewiesen, ein Speichern im mpuls_S bedeutet noch nicht, dass tatsächlich die Zahlung selbst abgewickelt wurde.
Entsprechend ist es als Nachweis nicht geeignet, damit ist die Speicherung dort auch nicht erforderlich.

Selbst wenn es geeignet wäre, sind die Nachweise schon anderweitig – in den dafür führenden Systemen - an der Hochschule vorhanden, so dass die Speicherung in mpuls_S zusätzlich erfolgen würde. Dies würde jedoch dem Grundsatz der Datenvermeidung und -minimierung widersprechen.

Aus unserer Sicht sind damit die Daten der geförderten Studierenden dann nicht mehr zur Aufgabenerfüllung erforderlich, wenn die Statistik bedient ist. Diese erfolgt immer nach Ablauf eines Kalenderjahres, so dass man eine Aufbewahrungsfrist von ebenfalls 13-14 Monaten benötigt.

4.3. Umsetzung

Die Software bietet nach Aussage der Fa. Intevation GmbH die Möglichkeit, Akten zu löschen. Zur Umsetzung der Aufbewahrungsdauer finden sich Ausführungen im Anwenderhandbuch (Stand 26.09.2011) auf S. 10-11.

Akten von abgelehnten Bewerbern werden im Ergebnis nach max. 12 Monaten, Akten von bewilligten Stipendiaten nach ca. max. 6 Jahren „anonymisiert“.

Hinsichtlich der von ZENDAS kritisierten Aufbewahrungsdauer von 6 Jahren in dem Produkt mpuls_S bietet Intevation GmbH folgendes an:

Wir können Ihnen aber einen "Workaround" anbieten. Technisch können wir für jeden Vertragspartner die Frist der Aufbewahrungsdauer der bewilligten Stipendien einstellen und können dies auch kostenlos bei Vertragsabschluss tun. Wir wollen uns hier aber absichern und werden dies durch ein Zusatzblatt zum Vertrag realisieren, in diesem erklärt die Hochschule, welche Anonymisierungsfrist sie wünscht und dass sie sich über die damit verbundenen Nachteile bzw. Konsequenzen bewusst ist.

4.4. Bewertung

Aus unserer Sicht lässt sich die Speicherung der Daten der abgelehnten Bewerber für max. 13-14 Monate rechtfertigen. Nach Aussage der Firma Intevation GmbH wird die Akte nach der Voreinstellung nach 2 x 180 Tagen in der Wiedervorlage gelistet und

kann dort zum Löschen gekennzeichnet werden. Damit ist der maximale Zeitraum eingehalten.

Wichtig: Die Akte muss **gelöscht** werden, die Anonymisierung reicht nicht aus, da sie keine Anonymisierung im Sinne der Datenschutzgesetzte ist und damit nach wie vor personenbezogene Daten vorhanden sind, die aber gerade gelöscht werden müssen.

Was die Aufbewahrungsdauer der Daten derjenigen angeht, die gefördert werden, teilen wir die Auffassung, dass die Daten 6 Jahre verfügbar sein müssen.
Die Hochschule muss allerdings prüfen, ob sie dafür mpuls_S benötigt oder ob die Daten im Falle einer Rechnungsprüfung nicht ohnehin schon anderweitig, z.B. im Mittelbewirtschaftungssystem, vorhanden sind. **In diesem Fall wäre eine Speicherung in mpuls_S nicht mehr erforderlich.** Dem Grundsatz der Datenvermeidung und –minimierung folgend, sind die Hochschulen dann gehalten, den „Workaround“ von Intevation in Anspruch zu nehmen.

5. Pseudonymisierung/Statistik

Die Software bietet die Möglichkeit, die Statistik nach § 13 StipG zu beliefern und die dafür notwendigen Daten zur Verfügung zu stellen.
Welche Felder das Programm zur Verfügung stellt, lässt sich Kapitel 7.3. des Dokuments „Spezifikation Formulare – Datenmodell Stipendiatinnen und Stipendiaten“ (Stand 05.08.11) entnehmen.

Die Felder entsprechen dem Katalog des § 13 StipG.

6. Hinweisblatt zum Datenschutz

Die Software gibt ein Hinweisblatt zum Datenschutz an die Hand, das den Bewerbern auszuhändigen ist und dieses Aushändigen in der Software durch Setzen eines Kennzeichens vermerkt wird.
Das vorgegebene Hinweisblatt enthält zur Begründung der Speicherdauer die Ausführung "um eine erneute Bewerbung im nächsten Auswahlverfahren vereinfachen zu können". Wie oben ausgeführt halten wir diese Argumentation nicht für überzeugend.

6.1. Bewertung

Wenn eine Hochschule dieses Hinweisblatt verwendet, macht sie sich auch die Begründung für die Speicherdauer zu eigen. Wie gesagt hat ZENDAS aus datenschutzrechtlicher Sicht Bedenken gegen diese Argumentation.

Ein „Workaround“ wäre dergestalt möglich, dass die Hochschule nicht das vorgegebene Hinweisblatt nutzt, sondern ein selbst gestaltetes verwendet.

7. Vertrag mit OpenIT GmbH

Wenn der Auftragnehmer Subauftragnehmer einsetzt, muss er seinerseits entsprechende Verträge über die Datenverarbeitung im Auftrag abschließen.
Nach Aussage der Fa. Intevation GmbH liegt ein Vertrag gem. § 11 BDSG vor.
Auf ausdrückliche Nachfrage wurde ZENDAS mitgeteilt:

Antwort: Wir haben mit der OpenIT GmbH einen umfangreichen Rahmenvertrag.
Dieser gilt für den Standort Düsseldorf, welcher nach IT-Grundschutz/ISO 27001 zertifiziert ist (siehe auch http://www.openit.de/it_grundschutz.html). Wir und jeder unserer Vertragspartner darf die Hardware dort kontrollieren. Die OpenIT GmbH muss eine Verlagerung aus Düsseldorf vorab mit uns abstimmen. Einen Umzug ins aussereuropäische Ausland haben wir darüber hinaus ausgeschlossen.

Wir weisen darauf hin, dass das sich das Zertifikat (lediglich) auf die Netzwerkinfrastruktur bezieht. Da es im vorliegenden Fall aber darum geht, dass auf einer Hardware personenbezogene Daten verarbeitet werden, stellen sich eine Reihe weiterer Fragen, wie z.B. der Zugang geregelt ist, welche technischen-organisatorischen Maßnahmen (§ 9 LDSG BW) mithin getroffen wurden.
Das Zertifikat ersetzt also nicht die Prüfung der technischen-organisatorischen Maßnahmen, soweit sie nicht die Netzwerkinfrastruktur betreffen.

7.1. Aufbewahrung von Backupmedien

Im Rahmen dieser Maßnahmen ist festzustellen, dass der Umgang mit Backupmedien aus unserer Sicht **derzeit** unzureichend ist. Das Backup erfolgt nämlich über eine zweite Platte im selben Rechner.
Damit ist für den Fall einer physikalischen Zerstörung keine Absicherung vorgesehen.

Die Fa. Intevation GmbH hat aber erklärt, an einem weiteren Standort der OpenIT GmbH eine Backup-Möglichkeit mit eigner Software bis zur KW 47 im Jahr 2011 zu schaffen.

Im Falle der Umsetzung bestehen an dem Punkt des Backups keine weiteren Bedenken.

8. Technische Anmerkungen zur Software mpuls_S

Bei einem Test der Software mpuls_S sind uns folgende Punkte aufgefallen:

8.1. URL-Manipulation "showSettings"

Durch eine einfache URL-Manipulation der Funktion "showSettings" ist es für einen Sachbearbeiter möglich, auf alle "Konto"-Daten anderer Benutzer zu kommen. Damit kann er sich insbesondere auch den Nutzernamen des Administrators erschließen, was wir kritisch sehen.

8.2. URL-Manipulation "stipendium/case/select"

Durch eine einfache URL-Manipulation der Funktion "stipendium/case/select" ist es für einen Sachbearbeiter möglich, auf eine Akte zuzugreifen, die für das Löschen vorgemerkt ist und die für die Sachbearbeiter nicht mehr zugänglich sein sollte.

8.3. Passwort-Policy

Die Passwort-Policy "acht Zeichen bestehen und zwei Nicht-Buchstaben enthalten" entspricht nicht den nötigen datenschutzrechtlichen Anforderungen, zumal hier auf sensible Daten der Stipendiaten zugegriffen werden kann.

Siehe auch:
Umgang mit Passwörtern, R3 + R4

http://www.baden-wuerttemberg.datenschutz.de/service/lfd-merkblaetter/passwort.htm

8.4. Passwort-Änderung

Bei der Funktion "changePassword" wird das bestehende Passwort nicht überprüft. Im Hinblick auf die sehr lange SESSION-Gültigkeit (ca 25 Minuten) entspricht dies ebenfalls nicht den nötigen datenschutzrechtlichen Anforderungen.

8.5. Bewertung

Fa. Intevation GmbH stimmt inhaltlich damit überein. 8.3. und 8.4. sei nicht aufwändig umzusetzen, die anderen Punkte würden mehr Aufwand verursachen. Sie möchte diese bis Ende des Jahres umgesetzt haben.

Nach Auffassung von ZENDAS müssen die Punkte vor einem Produktiveinsatz zwingend umgesetzt sein.

9. Ergänzender Hinweis: Freie Software

mpuls_S wird als freie Software zur Verfügung gestellt (Anwenderhandbuch (Stand 26.09.2011, S. 5)). Allerdings scheint sie bzw. die entsprechende Konfiguration der Komponenten noch nicht vollständig veröffentlicht zu sein.

Eine Alternative wäre also ggf., dass die Hochschule die Software selbst weiter entwickelt und insbesondere die derzeitigen Ausschlussgründe für den Einsatz beseitigt.

lu/14.10.11