819/AB XXV. GP

Eingelangt am 25.04.2014

BM für Bildung und Frauen

Anfragebeantwortung

BM BF Bundesministerium für Bildung und Frauen

Frau
Präsidentin des Nationalrates
Mag. Barbara Prammer
Parlament
1017 Wien

Wien, 24. April 2014

Die schriftliche parlamentarische Anfrage Nr. 905/J-NR/2014 betreffend Datenleck bei Schülertests, die die Abg. Mag. Nikolaus Scherak, Kolleginnen und Kollegen am 27. Februar 2014 an die Bundesministerin für Unterricht, Kunst und Kultur richteten, wird wie folgt beantwortet:

Zu Fragen 1 bis 3:

Seit Gründung des Bundesinstituts für Bildungsforschung, Innovation und Entwicklung des österreichischen Schulwesens (BIFIE) wurden nach den vorliegenden Informationen von diesem mit folgenden Unternehmen die wesentlichen Verträge zur Erstellung (von Plattformen) bzw. zur Speicherung und Sicherung von Daten abgeschlossen:

Daten der Informellen Kompetenzmessung (IKM): es werden keine personenbezogenen Schülerdaten erfasst, alle Schülerinnen und Schüler sind in der IKM für das BIFIE anonym:

- Firma Zoe Solutions GmbH – IKM-iiEFS-Plattform als Lizenzprodukt zur Online-Testung als Diagnosetool; Speicherung und Sicherung der Daten der IKM erfolgte in diesen Datenbanken bis 31. Dezember 2013 einerseits auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum und andererseits in der Infrastruktur von Zoe Solutions; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000.
- Firma Kapsch BusinessCom AG – vollständige Neuentwicklung einer IKM-Plattform zur Online-Testung als Diagnosetool (nun im Eigentum des BIFIE); Speicherung der Daten ab 1. Jänner 2014 nur noch auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und ein sogenanntes „Non-Disclosure-Agreement“ bzw. „NDA“ wurde unterzeichnet.

Daten zur Standardisierten Kompetenzorientierten Reife- und Diplomprüfung (SRDP): es werden keine Schülerdaten erfasst:

- Firma Zoe Solutions GmbH – SRDP-iiEFS-Plattform als Lizenzprodukt zur Item-/Aufgabenentwicklung; Speicherung und Sicherung der Daten der SRDP erfolgte in diesen Datenbanken bis 30. Juni 2013 einerseits auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum und andererseits in der Infrastruktur von Zoe Solutions; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000.
- Firma Anexia GmbH – Entwicklung der Item-/Aufgabenentwicklungsplattform für die SRDP (im Eigentum des BIFIE) ab 14. Dezember 2012; Speicherung der Daten fand ausschließlich auf einer BIFIE-Infrastruktur in einem österreichischen Rechenzentrum statt; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und „NDA“ wurde unterzeichnet.
- Firma Anexia GmbH – Entwicklung der Plattform für den Schulkontakt (im Eigentum des BIFIE); Speicherung der Daten nur auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und „NDA“ wurde unterzeichnet.
- Firma Auer – Einrichtung und Konfiguration des Itemgenerators (dh. Satzautomatik für Testhefte; im Eigentum des BIFIE); Speicherung der Daten nur auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und „NDA“ wurde unterzeichnet.

Bildungsstandards: die Erfassung von Schülerdaten erfolgt indirekt personenbezogen und die Datenschutzkommission hat die Korrektheit der Vorgehensweise bei der Testung bestätigt:

- Firma Anexia GmbH – Entwicklung der Item-/Aufgabenentwicklungsplattform für die Bildungsstandards (im Eigentum des BIFIE); Speicherung der Daten nur auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und „NDA“ wurde unterzeichnet.
- BIFIE-Intern – Entwicklung der Rückmeldeplattform zur Überprüfung der Bildungsstandards intern durch die Software-Abteilung im BIFIE entwickelt; Speicherung und Auswertung der Daten erfolgt auf der internen IT-Infrastruktur des BIFIE; Abruf der aufbereiteten Rückmeldedaten erfolgt auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum.
- Firma Anexia GmbH – Entwicklung der Plattform für den Schulkontakt (im Eigentum des BIFIE); Speicherung der Daten nur auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und „NDA“ wurde unterzeichnet.
- Firma Anexia GmbH – Entwicklung der Plattform für Aufgabenauswertung (dh. Kodier- und Rating-Plattform für Aufgaben/Items; im Eigentum des BIFIE); Speicherung der Daten nur auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und „NDA“ wurde unterzeichnet.
- Firma Auer – Einrichtung und Konfiguration des Indesign-Servers für den Satz der Rückmeldeberichte (im Eigentum des BIFIE); Speicherung der Daten nur auf der BIFIE-Infrastruktur in einem österreichischen Rechenzentrum; Vorkehrung Datenschutz und Datensicherheit § 11 DSG 2000 und „NDA“ wurde unterzeichnet.

PISA-Daten: die Erfassung von Schülerdaten erfolgt indirekt personenbezogen und die Datenschutzkommission hat die Korrektheit der Vorgehensweise bei der Testung bestätigt:

- BIFIE-Intern – PISA wird grundsätzlich nur auf der internen IT-Infrastruktur des BIFIE gespeichert und gesichert; die elektronische Testung erfolgt über USB-Sticks ohne Internetverbindung; es ist keine weitere Partnerfirma involviert; Daten werden mittels einer eigenen Applikation der OECD an die OECD weitergegeben

Verantwortlich für die vorstehend genannten Vertragsabschlüsse war das jeweils amtierende Direktorium.
Inhalte der angesprochenen „Non-Disclosure-Agreements“ bzw. „NDAs“ waren immer eine Verschwiegenheitsverpflichtung, technische Vorgaben zur Einhaltung der Datensicherheit (zB. sichere Verwahrung, vertrauliche Kommunikation) sowie rechtliche Vorgaben zur Einhaltung des Datenschutzgesetzes 2000 (insbesondere der §§ 1, 11, 10, 14 und 15 DSG 2000).
Ferner wird darauf hingewiesen, dass das BIFIE, den Anordnungen des BIFIE-Gesetzes 2008 folgend, bei der Wahrnehmung sämtlicher Aufgaben die Grundsätze des Datenschutzes zu wahren hat. Sowohl aus technischer als auch aus rechtlicher Hinsicht bestehen Vorgaben und Richtlinien im BIFIE und es werden die für den Einzelfall notwendigen Vorkehrungen getroffen (ua. Organisationshandbuch, spezielle Richtlinien zur Datensicherheit, NDAs).
Ergänzend wird seitens des Bundesministeriums für Bildung und Frauen bemerkt, dass externen Dienstleistern grundsätzlich alle einschlägigen, in den §§ 10ff und 14 Datenschutzgesetz 2000 vorgesehenen Verpflichtungen zur Datensicherheit vertraglich im Zuge der Beauftragung überbunden werden. Daten werden an diese nur nach dem „need to know“-Prinzip übergeben, wobei die Übertragung verschlüsselt nur an Berechtigte stattfindet.

Zu Fragen 4 und 5:
Nach Auskunft des BIFIE wurde die Firma Zoe Solutions GmbH vom BIFIE bzw. konkret von dem vormaligen, von der damaligen Ressortleitung mit Ende März 2012 abberufenen Direktor des BIFIE einerseits mit der Umsetzung von IT-Dienstleistungen im Bereich der IKM und der SRDP beauftragt sowie andererseits wurde über die iiEFS-Plattform von Zoe Solutions die IKM und die Aufgabenerstellung der SRDP in Deutsch und Mathematik abgewickelt. Nachdem dem Aufsichtsrat des BIFIE und dem Bundesministerium die schwerwiegenden Probleme mit Zoe Solutions bekannt wurden, wurden umgehend Schritte eingeleitet, um die bestehenden gravierenden Mängel im Bereich der IT-Infrastruktur kurzfristig zu sichern und die Zusammenarbeit zu beenden.

Zu Frage 6:
Die IT-Infrastruktur des BIFIE für Plattformen läuft im Rechenzentrum Conova Communications GmbH. Die Vertragsabschlüsse mit Conova Communications GmbH wurden zunächst durch das ab 1. April 2008 amtierende Direktorium geschlossen. 2013 wurde die Vergabe des Rechenzentrums des BIFIE entsprechend den Bestimmungen des Bundesvergabegesetzes 2006 ausgeschrieben. Bestbieter war Conova. Anfang 2014 wurde durch das aktuell amtierende Direktorium mit Conova ein Rahmenvertrag auf unbefristete Zeit abgeschlossen. In diesen Rahmenvertrag wurden Regelungen zu Verschwiegenheit und Datenschutz (ua. Einhaltung §§ 11, 15 DSG 2000) aufgenommen.

Zu Frage 7:
Eine hausinterne IT-Abteilung und eine Software-Entwicklungsabteilung bestehen im BIFIE. Bei den vielen großen und komplexen Projekten in der Software-Entwicklung (Plattformen) ist es

jedoch notwendig, externe Partner und Experten hinzuziehen. Die interne Software-Entwicklungsabteilung stellt dabei die Qualität der externen Auftragsarbeiten sicher. Die interne IT-Abteilung des BIFIE ist für alle internen Prozesse und Serveranlagen am Firmensitz verantwortlich – alle Daten aus den Schülerleistungstests werden in den internen Serveranlagen am Firmensitz verarbeitet. Für die IT-Infrastruktur des BIFIE bei Conova Communications GmbH, dh. für alle Serveranlagen des BIFIE im Rechenzentrum, ist die Betriebsmannschaft von Conova verantwortlich. Im Rahmenvertrag mit Conova wurden Regelungen zu Verschwiegenheit und Datenschutz aufgenommen.

Zu Frage 8:

Nach den vorliegenden Informationen wurde im Zuge der Entwicklung für eine neue IKM-Plattform zur Online-Testung als Diagnosetool diese „alte“ Datenbank durch das BIFIE für Verifikationszwecke an die Partnerfirma Kapsch BusinessCom AG übermittelt. Diese Datenbank der IKM auf den Entwicklungsserver der BIFIE-Partnerfirma enthielt die E-Mail-Adressen aller Lehrkräfte und Schulleitungen, mit denen sich diese im Zeitraum von 25. März 2011 bis 30. Dezember 2012 auf der IKM-Plattform angemeldet haben. Die Datenbank enthält keine sonstigen personenbezogenen Daten von Lehrerinnen und Lehrern oder Schülerinnen und Schülern. Sämtliche Testergebnisse von Schülerinnen und Schülern sind für das BIFIE oder Personen, die in die Datenbank Einblick haben, anonym. Die Datenbank enthält diagnostische Aufgaben, mit welchen Lehrerinnen und Lehrer die Kompetenzen der Schülerinnen und Schüler für eine spätere Förderung ermitteln können; es können aus den Testergebnissen keine Vergleiche abgeleitet werden, die Testergebnisse sind nicht unter standardisierten Bedingungen entstanden. Der Entwicklungsserver auf der sich die Datenbank befand, war laut Angaben der Partnerfirma des BIFIE nicht ungeschützt, sondern gesichert, passwortgeschützt, verschlüsselt und nur einer eingeschränkten Liste von fixen IP-Adressen zugänglich. Mittels eines platzierten Symbolic Link wurden die Daten laut Kapsch BusinessCom AG zugänglich gemacht, jedoch nur wenn der genaue URL (IP-Adresse) einem zugreifenden Dritten bekannt war – und nur für diesen – bestand die Möglichkeit, die Daten einzusehen und auch herunterzuladen. Die Daten bzw. die betroffene Datenbank waren nicht indexiert, dh. über diverse Suchfunktionen (google, webcrawler) konnten die Dateien auch nicht gefunden werden. Sonstige Daten oder Datenbanken, mit denen das BIFIE arbeitet, sind von diesem Vorfall nicht betroffen.

Zu Frage 9:

Das BIFIE verfügt über eine hausinterne IT-Abteilung, ist aber dennoch gemäß BIFIE-Gesetz 2008 im Sinne der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit der Gebarung verpflichtet und ermächtigt bestimmte Dienstleistungen, auch solche im IT-Bereiche, außer Haus entwickeln zu lassen. Zur Frage, ob das Datenleck bei In-House-Entwicklung hätte vermieden werden können: Die Ermittlungen des Bundeskriminalamts und der Staatsanwaltschaft laufen noch, eine Beurteilung kann erst nach Abschluss dieser Ermittlungen erfolgen.

Zu Fragen 10 bis 13:

Am 18. Dezember 2013 erging ein Schreiben der Firma Zoe Solutions GmbH bzw. eines Vertreters dieser Firma an die Direktoren des Bundesinstituts für Bildungsforschung, Innovation und Entwicklung des österreichischen Schulwesens (BIFIE) sowie in Kopie an die Bundesministerin (damals) für Unterricht, Kunst und Kultur und an den Vorsitzenden des Aufsichtsrates des BIFIE. In diesem Schreiben, das sich zunächst primär und ausführlich mit möglichen Rechtstreitigkeiten zwischen dem BIFIE und der Firma Zoe Solutions GmbH im Bereich des

Lizenzrechts befasste, wurde im letzten Absatz ganz generell und ohne jegliche genauere Angabe (zB. welcher Server ist betroffen, Nennung des URL o.ä.) auf einen „Verstoß gegen Datenschutzbestimmungen“ sowie „auf vorgefundene Daten aller für die IKM registrierten Schulen und Lehrpersonen sowie die Testergebnisse aller Schülerinnen und Schüler“ hingewiesen.

Das BIFIE informierte umgehend die Partnerfirma Kapsch BusinessCom AG, die mit der Entwicklung der IKM-Plattform beauftragt war. Eine Überprüfung der Datensicherheit durch die Partnerfirma ließ keine Gefährdung erkennen, woraufhin das BIFIE am 20. Dezember 2013 ein Schreiben an die Firma Zoe Solutions GmbH richtete, in dem um Konkretisierung der Vorwürfe ersucht wurde. Dieses blieb unbeantwortet. Daraufhin wurde am 4. Februar sowie am 22. Februar 2014 neuerlich bei der Firma Zoe Solutions GmbH bzw. deren Vertreter urgiert, ihre bzw. seine Vorwürfe zu präzisieren. Auch diese Schreiben blieben unbeantwortet. Auch eine telefonische Urgenz führte zu keinen konkreteren Angaben. Das BIFIE leitete seinerseits das Schreiben vom 20. Dezember 2013 an den Aufsichtsratsvorsitzenden des BIFIE wie auch an das Bundesministerium weiter. Alle Schreiben an Zoe Solutions GmbH wurden jeweils von beiden Direktoren unterzeichnet, da beide laut Institutsordnung auch für den Bereich IT, im BIFIE im Department „Zentrales Management & Services“ verankert, zuständig sind.

Das Bundesministerium (damals) für Unterricht, Kunst und Kultur hat in der Folge umgehend Kontakt mit dem BIFIE aufgenommen und um Aufklärung in der Angelegenheit ersucht. Nach zunächst mündlichen bzw. telefonischen Kontakten wurde das BIFIE mit Schreiben vom 9. Jänner 2014 auch um eine schriftliche Stellungnahme zu dem Schreiben der Firma Zoe Solutions GmbH aufgefordert. Diese Stellungnahme seitens des BIFIE traf mit 15. Jänner 2014 im Bundesministerium ein. Das Direktorium legte in diesem Schreiben dar, dass es sich bereits intensiv um die Aufklärung dieser „Behauptungen“ kümmere, bisher aber keinerlei Hinweise habe, dass ein solcher Vorfall tatsächlich eingetreten sei. Das BIFIE hatte bereits ab 19. Dezember 2013 mit seiner Partnerfirma Kapsch BusinessCom AG Kontakt aufgenommen und von Seiten der Partnerfirma wurde nach Prüfungsvorgängen mehrmals versichert, dass keine Daten öffentlich zugänglich seien.

Mit Datum 24. Februar 2014 – also einen Tag vor Bekanntwerden des „Datenlecks“ durch die Tageszeitung „Die Presse“ erhielt das BIFIE dann ein Schreiben von Zoe Solutions GmbH, in dem weitere rechtliche Schritte angekündigt wurden und folgendes erwähnt wurde: „in diesem Sinne haben wir [Zoe Solutions] zur Kenntnis genommen, dass keine Bereitschaft besteht, das Problem auf partnerschaftlicher Ebene aufzuarbeiten, nehmen diese Entwicklung mit einem gewissen Befremden – jedenfalls mit Bedauern – zur Kenntnis, wiewohl sie nicht in unserem Einflussbereich liegt. Wir haben bis zum heutigen Tage von Ihnen [BIFIE] nicht einmal ansatzweise eine Erklärung der von uns aufgezeigten Missstände erhalten“. Das Schreiben enthielt keine Information zu dem im ersten Schreiben vom 18. Dezember 2013 angeführten „Datenleck“.

Am 25. Februar 2014 übermittelte die Firma Zoe Solutions GmbH bzw. deren Vertreter um 19.30 Uhr in einer E-Mail an einen der beiden Direktoren des BIFIE einen Screenshot des „Datenlecks“ – allerdings mit geschwärztem URL (dh. eine Behebung des Zugriffs war mit dieser Information nicht möglich). In der Folge erstattete das Direktorium des BIFIE eine Anzeige bei der Staatsanwaltschaft, da es sich ganz offenbar um eine gezielten Angriff auf Daten des BIFIE, die bei Kapsch BusinessCom AG gespeichert wurden, handelte. Gegenwärtig ermitteln Staatsanwaltschaft und Bundeskriminalamt.

Zu Frage 14:
Nein, das BIFIE wurde nach dessen Auskunft vor dem 18. Dezember 2013 auf keine Mängel im Bereich Datenschutz aufmerksam gemacht. Losgelöst davon wird auf die Ausführungen zu Fragen 4 und 5 betreffend bekannt gewordene gravierende Mängel im Bereich der IT-Infrastruktur hingewiesen.

Zu Frage 15:
Der Hinweis wurde nach den vorliegenden Informationen, wie vorstehend ausgeführt, keineswegs ignoriert, vielmehr wurde seitens BIFIE diesem Hinweis wiederholt und sorgfältig nachgegangen. Der Prozess der Klärung zwischen BIFIE und dem Partnerunternehmen Kapsch BusinessCom AG ist dokumentiert. Die Einschätzung, dass es sich bei dem Schreiben von Zoe Solutions GmbH um eine „Drohgebärde“ handelte, stammt von einem der Direktoren des BIFIE auf Anfrage von der Tageszeitung „Die Presse“ rund zwei Stunden vor der Veröffentlichung des ersten Artikels über ein „Datenleck“. Die journalistische Anfrage bezog sich auf das Schreiben von Zoe Solutions vom 18. Dezember 2013 und nicht auf den Zugang zur Datenbank. Auch die Schritte, die das BIFIE oder die Firma Kapsch BusinessCom AG konkret unternommen hatten, um die Datensicherheit zu prüfen, stellten keinen Gegenstand der journalistischen Anfrage dar.

Zu Frage 16:
Das „Datenleck“ wurde durch die Berichterstattung der Tageszeitung „Die Presse“ am 25. Februar 2014 öffentlich gemacht.

Zu Frage 17:
Zwischen dem 18. Dezember 2013 (Schreiben Zoe Solutions GmbH an BIFIE) und dem 25. Februar 2014 verfügten weder das BIFIE, Kapsch BusinessCom AG noch das Bundesministerium über irgendwelche relevanten Angaben in dieser Angelegenheit, die hätten öffentlich gemacht werden können. Der einzige Hinweis bestand in einer Andeutung eines vom BIFIE geschiedenen ehemaligen Vertragspartners, der einen „Verstoß gegen die Datenschutzbestimmungen“ angeführt und von „öffentlich zugänglichen Daten“ geschrieben hatte, aber auch auf wiederholte Nachfrage hierzu keinerlei Konkretisierung vorgelegt und keine Unterstützung angeboten hatte.

Zu Fragen 18, 20 und 23:
In mehreren Stufen (TÜV-Prüfung der Datensicherheit des BIFIE, Sicherheitsaudits, …) wird die Datensicherheit des BIFIE überprüft. Weiters sind die Ergebnisse der Ermittlungen des Bundeskriminalamts abzuwarten. Unter Hinweis auf die Ausführungen zu den bereits gesetzten Schritten im Rahmen der vorangegangenen Fragestellungen und nicht zuletzt im Hinblick auf den umfassenden Daten-Sicherheitscheck des BIFIE soll durch eine von Transparenz und Offenheit getragene Aufklärungsarbeit und den nachfolgend dazu vorliegenden zukünftigen Ergebnissen das Vertrauen der Schülerinnen und Schüler, Lehrerinnen und Lehrer als auch der Erziehungsberechtigten wieder gewonnen werden.

Zu Frage 19:
Unter Hinweis auf die obigen Ausführungen zu Frage 9 ist zu bemerken, dass eine hausinterne IT-Abteilung und Software-Entwicklungsabteilung im BIFIE bereits bestehen. Die Kosten hierfür sind im laufenden Budget des BIFIE enthalten. Die jährlichen Personalkosten belaufen sich auf insgesamt ca. EUR 980.000 an allen Standorten.

Zu Fragen 21 und 22:
Vorderhand sind die Ergebnisse der Ermittlungen des Bundeskriminalamts abzuwarten. Zu einem rechtsstaatlichen Verfahren gehört es, dass die nach der Kompetenzverteilung berufenen Verwaltungsbehörden oder Gerichte den maßgeblichen Sachverhalt prüfen und die in ihrem jeweiligen Zuständigkeits- und Wirkungsbereich fallenden Verfügungen treffen. Das Setzen von strafrechtlichen Konsequenzen ist den Strafgerichten vorbehalten.

Zu Fragen 24 bis 26 und 28:
Grundsätzlich werden die sensitiven Datenbanken und Anwendungen bei der Bundesrechenzentrum GmbH und weiteren nach aktuellen ISO-Standards zertifizierten Rechenzentren betrieben. Das Bundesrechenzentrum verfügt über eine flächendeckende ISO 27.001-Zertifizierung, die regelmäßig extern evaluiert wird. Für Mitarbeiterinnen und Mitarbeiter der BRZ gilt gemäß § 17 BRZ-Gesetz die volle Verpflichtung zur Amtsverschwiegenheit.
Externen Dienstleistern werden die einschlägigen, in den §§ 10ff und 14 Datenschutzgesetz 2000 vorgesehenen Verpflichtungen zur Datensicherheit vertraglich überbunden. Es wird auch auf die bestehenden Allgemeinen Vertragsbedingungen der Republik Österreich für IT-Leistungen (AVB-IT) verwiesen, in denen Standards in Verbindung mit Geheimhaltung und Datensicherheit/Datenschutz festhalten sind. Die Einhaltung dieser Standards wird vom Ressort von Auftragnehmern eingefordert und geprüft. Interne Evaluierungen und Überprüfungen durch die IT-Abteilungen des Ressorts erfolgen regelmäßig.

Zu Frage 27:
Im Zuge der Fort- und Weiterbildungsveranstaltungen für die Mitarbeiterinnen und Mitarbeiter des Ressorts werden E-Government-Seminare angeboten, in denen auch die Themen Datenschutz und Datensicherheit behandelt werden. Weiters finden im Zuge von Multiplikatorinnen- und Multiplikatoren-Veranstaltungen und Fachkonferenzen seit einigen Jahren regelmäßig Workshops und Vorträge zu den Themen Datenschutz und Datensicherheit in der Bildungsverwaltung statt. Für die Zielgruppe der Lehrenden gibt es über die Pädagogischen Hochschulen IKT-themenspezifische Bildungsangebote, die auch Aspekte der Datensicherheit und des Datenschutzes thematisieren.
Diverse zielgruppenspezifische Informationsmaterialien, Handreichungen und Richtlinien stehen den Mitarbeiterinnen und Mitarbeitern des Ressorts zur Verfügung bzw. wurden auch an die jeweiligen Zielgruppen weitergeleitet. Das IKT-Sicherheitsportal (des Bundeskanzleramtes, des Bundesministeriums für Finanzen und der ASIT) bündelt aktuelle Informationen und spricht insbesondere auch die öffentliche Verwaltung sowie Lehrende als spezielle Zielgruppe an.

Die Bundesministerin:

Gabriele Heinisch-Hosek eh.