

XXV.GP.-NR
905 /J

27. Feb. 2014

Anfrage

der Abgeordneten Dr. Nikolaus Scherak, Mag. Niko Alm, Kolleginnen und Kollegen

an die Bundesministerin für Unterricht, Kunst und Kultur

betreffend Datenleck bei Schülertests

Laut eines Artikels im heutigen Standard (27.02.2014) sollen nun „angesichts des größten Datenskandals der österreichischen Schulgeschichte“ alle zentralen Schultests bis zur vollständigen Klärung des BIFIE-Datenlecks gestoppt werden. Diese Ankündigung habe Unterrichtsministerin Gabriele Heinisch-Hosek gestern am 26.02.2014 im Bundesrat gemacht.

Dennoch stellt sich die Frage, wie die Daten der "Informellen Kompetenzmessung" (IKM) von 2011 und 2012 und die E-Mail-Adressen von 37.000 Lehrern auf rumänische Server gelangen konnten, wo sie nun unverschlüsselt und damit prinzipiell zugänglich für jeden Internetnutzer liegen.

Wenn der Staat im Namen der Bildungspolitik Daten sammelt, so hat er auch dafür Verantwortung zu übernehmen und größte Sorgfalt bei der Sicherung und Aufbewahrung walten zu lassen.

Dieses Bewusstsein scheint hier gefehlt zu haben, aus diesem Grund stellen die unterfertigten Abgeordneten nachstehende

Anfrage:

1. Mit welchen Unternehmen wurden welche Verträge zur Erstellung und Speicherung bzw. Sicherung folgender Daten seit der Gründung des BIFIE bzw. seit der Einführung der Tests a) bis d) abgeschlossen:
 - a) Daten der informellen Kompetenzmessung
 - b) Daten zur Zentralmatura
 - c) Bildungsstandardsdaten
 - d) Pisa-Daten
2. Welche genauen Vereinbarungen sind zum Datenschutz und zur Datensicherheit hinsichtlich der in Frage 1 genannten Daten getroffen worden?
3. Welche Vorkehrungen zum Datenschutz und zur Datensicherheit werden grundsätzlich bei der Zusammenarbeit des BMUKK bzw. des BIFIE mit externen Unternehmen und Organisationen vorgesehen?

4. Weshalb wurde die erst 2010 gegründete Klagenfurter zoe solutions GmbH (mit 2 Mitarbeitern und einer Bilanzsumme von 53.177 Euro im Jahr 2012) vom BIFIE bzw. vom BMUKK mit der Betreuung und Sicherung der IKM Daten beauftragt?
5. Wer war für den Vertragsabschluss mit zoe solutions GmbH seitens des BIFIE verantwortlich?
6. Wurden außer mit der zoe solutions GmbH Verträge mit weiteren IT-Dienstleistungsunternehmen geschlossen?
 - a) Wenn ja, mit welchen IT-Dienstleistungsunternehmen? Wer war innerhalb des BIFIE für die Vertragsabschlüsse verantwortlich?
 - b) Welche datenschutzrechtlichen Regelungen waren Vertragsinhalt?
7. Weshalb leistet sich das BIFIE mit rund 100 Mitarbeitern keine hausinterne IT?
8. Wie gelangten die sensiblen Daten auf besagten ausländischen ungeschützten Server?
9. Hätte aus Sicht des BMUKK das Datenleck durch eine hausinterne IT des BIFIE verhindert werden bzw. überhaupt erst gar nicht entstehen können?
10. Wie sind das BMUKK und das BIFIE mit dem Hinweis der zoe solutions GmbH vom 18. Dezember 2013, dass ungesicherte Daten im Internet aufgetaucht seien, umgegangen?
11. Wer wurde vom BMUKK innerhalb des BIFIE am 18. Dezember 2013 über das drohende Datenleck informiert?
12. Was haben das BMUKK und das BIFIE seit dem Hinweis der zoe solutions GmbH vom 18. Dezember 2013 hinsichtlich der Datenschutzprobleme und der Offenlegung sensibler Daten unternommen?
13. Welche konkreten Schritte haben die beiden Direktoren des BIFIE in diesem Zusammenhang gesetzt und welcher der beiden Direktoren war zu diesem Zeitpunkt für den IT-Bereich verantwortlich?
14. Wurde das BIFIE bereits vor dem 18. Dezember 2013 auf mögliche Datenschutzmängel durch zoe solutions GmbH oder eine anderes qualifiziertes IT-Dienstleistungsunternehmen aufmerksam gemacht?

- a) Wenn ja, durch welches IT-Sicherheitsunternehmen?
 - b) Welche konkreten Hinweise hat wer im BIFIE erhalten?
 - c) Wann hat wer im BIFIE konkrete Hinweise erhalten?
15. Wer war für die Entscheidung, die Hinweise zu ignorieren, verantwortlich bzw. wer hat diese als „Drohgebärde eines in Unfrieden geschiedenen Vertragspartners“ (derStandard vom 26.02.2014) eingestuft?
16. Durch wen wurde das Datenleck öffentlich gemacht?
17. Wieso wurde das oben genannte Datenleck nicht sofort zu dem Zeitpunkt öffentlich gemacht, als das BIFIE davon Kenntnis erlangte?
18. Welche Maßnahmen sehen das BMUKK und das BIFIE vor, damit es nicht mehr zu unzulässigen Veröffentlichungen von Daten kommt?
19. Ist zukünftig eine hausinterne IT-Abteilung im BIFIE vorgesehen?
- a) Wenn ja, ab wann und welche Kosten werden damit verbunden sein?
 - b) Wenn nein, weshalb nicht?
20. Welche Konsequenzen werden aufgrund dieses Vorfalls in Hinblick auf das BIFIE seitens des BMUKK gezogen?
21. Haben Mitarbeiter_innen des BIFIE im Zusammenhang mit diesem Vorfall strafrechtliche Konsequenzen zu erwarten?
22. Wenn ja, welche Mitarbeiter_innen?
23. Welche konkreten Maßnahmen sehen das BMUKK und das BIFIE zur Wiederherstellung des Vertrauens der Bürger_innen vor?
24. Welche Vorkehrungen zum Datenschutz und zur Datensicherheit bestehen konkret für das BMUKK? Seit wann werden diese angewandt?
25. Erfolgt eine regelmäßige Evaluierung, Überprüfung und Anpassung dieser Vorkehrungen?
26. Wenn eine regelmäßige Evaluierung und Überprüfung erfolgt, welche Konsequenzen werden und wurden daraus gezogen bzw. welche Anpassungen werden und wurden vorgenommen?
27. Gibt es Datenschutzs Schulungen im BMUKK?

- a) Wenn ja, wie sind sie konkret ausgestaltet und wer nimmt daran teil?
- b) Wann und wie häufig finden sie statt?
- c) Sind sie verpflichtend für alle Mitarbeiter_innen?
- d) Wenn nein, warum gibt es keine Datenschutzeschulungen?
- e) Sind solche künftig vorgesehen? Wenn ja, ab wann?

28. Wie sehen die Vorkehrungen zum Datenschutz und zur Datensicherheit im BMUKK insbesondere im Hinblick auf Daten von Schüler_innen und Lehrer_innen aus?

W. Scherndl O. T. G. M.
A. M.