

---

**12829/J XXV. GP**

---

Eingelangt am 27.04.2017

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

## Anfrage

der Abgeordneten Dr. Jessi Lintl  
und weiterer Abgeordneter  
an die Bundesministerin für Gesundheit und Frauen  
**betreffend Cybersicherheit! - Auch im Hauptverband der  
Sozialversicherungsträger?**

Der Rechnungshof beschäftigte sich in seinem Bericht Bund 2014/8 mit Cybersicherheit und dem Schutz von IT-Infrastrukturen. In diesem Fall ging es um den Hauptverband der Sozialversicherungsträger, der zentrale Register betrieb, die unter anderem strukturierte Daten über Personen, Wirtschaftstreibende sowie Leistungserbringer enthielten. Bei der Prüfung hielt der Rechnungshof unter anderem folgendes fest:

- *„Ein auf den Ministerratsvorträgen basierendes Konzept zur Aufrechterhaltung der kritischen Infrastruktur und der Verteilungssysteme sowie ein Cyber Sicherheitskonzept für die Sozialversicherung waren nicht vorhanden. Es waren keine zentralen Strukturen und umfassenden Maßnahmen zur Erreichung eines definierten Schutzniveaus im Bereich Cybersicherheit gesetzt worden*
- *Eine gesetzliche Regelung sowie eine Gesamtstrategie zur Cyber Sicherheit in der Sozialversicherung waren nicht vorhanden.*
- *IT-Sicherheitsfachleute, welche die Aufgaben eines Sozialversicherungs Computer Emergency Response Teams (CERT) als Kernaufgabe für die Sozialversicherung wahrgenommen hätten, gab es nicht.*
- *Ein die Sozialversicherung übergreifendes Krisenmanagement und Kontinuitätspläne zur Bewältigung etwaiger Angriffe auf die IT-Struktur der Sozialversicherung fehlten.*
- *Zentral koordinierte und einheitliche Schutz- und Sicherheitsstandards der Einrichtungen der Sozialversicherung waren nicht vorhanden.*
- *Cybersicherheitsvorfälle waren nicht zwingend zu dokumentieren und weiterzuleiten; somit konnten entsprechende Maßnahmen nicht immer erarbeitet werden.*
- *Katastrophenübungen, die eine Beeinträchtigung weite Teile der IT der Sozialversicherung zum Inhalt hatten, wurden nicht durchgeführt.“*

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

Zu dieser Thematik und kritisierten Punkten gab der Rechnungshof eine Schlussbemerkung mit zahlreichen Empfehlungen ab. Mittlerweile sind seit dem Bericht des Rechnungshofes einige Jahre verstrichen, weshalb eine Evaluierung der Umsetzung der Empfehlungen an der Zeit ist. Das sensible Thema Cybersicherheit ist aktueller denn je, was die zahlreichen Vorfälle und Medienberichte darüber in diesem Bereich zeigen.

Im Jänner 2014 wurde durch eine Anfragebeantwortung zur Anfrage 186/J mit GZ des BMG-11001/0283-I/A/15/2013 bzw. durch öffentliche Medienberichte bekannt, dass im Bereich einer externen Dienstleistung zu ELGA Programmierkapazität zum Zentralen Patientenindex (ZPI) im Hauptverband der Sozialversicherungsträger durch einen NSA nahen IT-Dienstleister zugekauft wurde. Zum Zeitpunkt des Bekanntwerdens der NSA-Spionagetätigkeit war der Auftrag bereits abgeschlossen. Die Kosten für diese Dienstleistung beliefen sich auf 2.928.098,-- (Brutto einschließlich Reisekosten).

In diesem Zusammenhang richten die unterfertigten Abgeordneten an die Bundesministerin für Gesundheit und Frauen nachstehende

### ANFRAGE

1. Haben Sie bereits die Empfehlung des Rechnungshofes aus dem Bericht Bund 2014/8 an Ihr Ressort, wonach eine Regelung zur zentralen Umsetzung einer Cyber Sicherheitsstrategie in der Sozialversicherung an den Gesetzgeber heranzutragen, umgesetzt?
2. Wenn nein, warum nicht?
3. Wenn ja, wann werden Sie die vom Rechnungshof empfohlene Regelung dem Gesetzgeber vorlegen? (Bitte um Angabe des Umsetzungszeitrahmens und des geplanten In-Kraft-Tretens der Regelung)
4. Planen Sie die vom Rechnungshof empfohlene Regelung umzusetzen?
5. Wenn nein, warum nicht?
6. Wenn ja, wie weit sind die Planungen gediehen? (Bitte um Angabe eines Zeitrahmens der einzelnen Planungsschritte)
7. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an ihr Ressort und an den Hauptverband der österreichischen Sozialversicherungsträger, wonach mögliche Indikatoren bezüglich Aktivierung einer Scheinfirma zu definieren wären und die Register der Sozialversicherung auf diese — unter Beachtung des Datenschutzes und der rechtlichen Rahmenbedingungen — automationsunterstützt auszuwerten wären, bereits umgesetzt?
8. Wenn ja, wie sehen die Umsetzungsmaßnahmen dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)

9. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
10. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an ihr Ressort und an den Hauptverband der österreichischen Sozialversicherungsträger, wonach die von Experten zur Früherkennung von geplantem Sozialbetrug (Scheinfirma) definierten Indikatoren (Daten) zeitgerecht in die Register einzutragen wären und notwendigenfalls ein diesbezüglicher Gesetzesvorschlag an den Gesetzgeber heranzutragen wäre.
11. Wenn ja, wann werden Sie die vom Rechnungshof empfohlene Regelung dem Gesetzgeber vorlegen? (Bitte um Angabe des Umsetzungszeitrahmens und des geplanten In-Kraft-Tretens der Regelung)
12. Planen Sie die vom Rechnungshof empfohlene Regelung umzusetzen?
13. Wenn nein, warum nicht?
14. Wenn ja, wie weit sind die Planungen gediehen? (Bitte um Angabe eines Zeitrahmens der einzelnen Planungsschritte)
15. Wenn ja, wie sehen Ihre Umsetzungsmaßnahmen und jene des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
16. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an ihr Ressort und an den Hauptverband der österreichischen Sozialversicherungsträger, wonach zur Abwehr und Bewältigung von Cyber Sicherheitsvorfällen eine umfassende Cyber Sicherheitsstrategie für den Sozialversicherungsbereich zu erarbeiten und umzusetzen wäre?
17. Wenn ja, wie sehen Ihre Umsetzungsmaßnahmen und jene des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
18. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
19. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an ihr Ressort und an den Hauptverband der österreichischen Sozialversicherungsträger, wonach zur operativen Bearbeitung der Cyber Sicherheitsbereiche in der Sozialversicherung ein Sozialversicherungs CERT im Rahmen der Zielsteuerung einzurichten wäre und in Abstimmung mit dem BMASK der Trägerkonferenz zur Beschlussfassung vorzulegen wäre, bereits umgesetzt?
20. Wenn ja, wie sehen Ihre Umsetzungsmaßnahmen und jene des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
21. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)

22. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach zur gemeinsamen Umsetzung des One-Stop-Shop von Personenstandsbehörden und Sozialversicherungsträgern die Übernahme der Daten aus dem Zentralen Personenstandsregister der Personenstandsbehörden in die Zentrale Partnerverwaltung des Hauptverbands zeitnah umzusetzen wäre, bereits umgesetzt?
23. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
24. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
25. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach bei voneinander abweichender Datenlage Datenkonsistenz herzustellen wäre und die zuständigen Einrichtungen wie Meldebehörde oder Personenstandsbehörde über den erhobenen Sachverhalt zu informieren wären, bereits umgesetzt?
26. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
27. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
28. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach die Daten zu Unternehmen, Vereinen und sonstigen Betroffenen aus dem Unternehmensregister-Verwaltung in die Zentrale Partnerverwaltung zu übernehmen wären, bereits umgesetzt?
29. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
30. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
31. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach für den Datenaustausch mit anderen Tätigkeitsbereichen, die keine gesetzliche Ermächtigung zur Übertragung der Versicherungsnummer hatten, zukünftig die Verwendung des bereichsspezifischen Personenkennzeichens vorzusehen wäre, bereits umgesetzt?
32. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um

Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter  
Anführung der gesetzlichen Grundlage)

33. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw.  
Umsetzungsprobleme im Detail)
34. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund  
2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger,  
wonach die Versicherungsnummer — falls unumgänglich — über den  
Tätigkeitsbereich der Sozialversicherung hinaus nur noch verschlüsselt zu  
übertragen wäre, bereits umgesetzt?
35. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der  
österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um  
Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter  
Anführung der gesetzlichen Grundlage)
36. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw.  
Umsetzungsprobleme im Detail)
37. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund  
2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger,  
wonach alle Schnittstellen des Hauptverbands zu anderen Tätigkeitsbereichen  
bei anstehenden Weiterentwicklungen mit der Möglichkeit zur Nutzung des  
bereichsspezifischen Personenkennzeichens auszustatten wären, bereits  
umgesetzt?
38. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der  
österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um  
Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter  
Anführung der gesetzlichen Grundlage)
39. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw.  
Umsetzungsprobleme im Detail)
40. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund  
2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger,  
wonach die Inhalte der Cyber Sicherheit nach Priorität gereiht aufzuarbeiten  
und verbindlich umzusetzen wären, bereits umgesetzt?
41. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der  
österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um  
Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter  
Anführung der gesetzlichen Grundlage)
42. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw.  
Umsetzungsprobleme im Detail)
43. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund  
2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger,  
wonach für die Sozialversicherung ein Krisenmanagement einzurichten wäre  
und dieses die Risikoanalysen durchzuführen, Kontinuitätspläne zu entwickeln  
und Krisenübungen durchzuführen hätte, bereits umgesetzt?

44. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
45. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
46. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach Sicherungs- und Schutzstandards für die Einrichtungen der Sozialversicherung vorzusehen wären, dem jeweiligen Aufgabengebiet und den verwendeten Daten anzupassen wären und dessen verbindliche Kontrolle einzurichten wäre, bereits umgesetzt?
47. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
48. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
49. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach eine Meldepflicht bei Cyber Sicherheitsvorfällen für alle Einrichtungen der Sozialversicherung verbindlich vorzusehen wäre und die Bewertung bzw. Einstufung des jeweiligen IT-Sicherheitsvorfalls den Sicherheitsfachleuten des Sozialversicherungs CERT vorbehalten sein sollte und anhand definierter Strukturen und Prozesse alle potenziell gefährdeten Einrichtungen der Sozialversicherung zu informieren und entsprechende Maßnahmen zu empfehlen wären, bereits umgesetzt?
50. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
51. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
52. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach die Mitarbeiter der Sozialversicherung im Umgang mit der IT-Infrastruktur weiterhin auf mögliches Fehlverhalten zu sensibilisieren und in definierten Abständen zentral koordinierte und abgestimmte Schulungen vorzusehen wären, bereits umgesetzt?
53. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)

54. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
55. Wurden die Empfehlungen des Rechnungshofes aus dem Bericht Bund 2014/8 an den Hauptverband der österreichischen Sozialversicherungsträger, wonach IT-Sicherheitsfachleute der Sozialversicherungsträger verbindlich anhand von Katastrophenübungen zu schulen wären, bereits umgesetzt?
56. Wenn ja, wie sehen die Umsetzungsmaßnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger dazu im Detail aus? (Bitte um Anführung des Zeitpunktes des In-Kraft-Tretens der Maßnahmen unter Anführung der gesetzlichen Grundlage)
57. Wenn nein, warum nicht? (Bitte um Darstellung der Gründe bzw. Umsetzungsprobleme im Detail)
58. Welche Maßnahmen wurden im Jahr 2014 nach Bekanntwerden einer möglichen NSA-Spionagetätigkeit eines ehemaligen Dienstleisters ergriffen um etwaige Manipulationen (Trojaner, Hintertüren, schädlicher Programmcode, Spionage, unberechtigter Datenabfluss) im Zentralen Patientenindex (ZPI) auszuschließen?
59. Welche Firma, Dienstleister oder österreichische Behörde hat im Jahr 2014 den Programmcode der beiden eingesetzten Programmierer der Firma CSC überprüft?
60. Wurde dieser Vorfall im Jahr 2014 der Datenschutzkommission gemeldet?
61. Welche zentralen Funktionen führt der Patientenindex (ZPI) des Hauptverbandes der österreichischen Sozialversicherungsträger im System ELGA aus?
62. Welche genauen Daten der Patienten (taxative Aufzählung) enthält der Patientenindex (ZPI)?
63. Welche Systeme, Dienstleister, Datenregister und Behörden haben über den Hauptverbandes der österreichischen Sozialversicherungsträger Zugriff auf den Patientenindex (ZPI)?