BUNDESMINISTERIUM FÜR GESUNDHEIT

Alois Stöger
Bundesminister

Frau
Präsidentin des Nationalrates
Mag.[a] Barbara Prammer
Parlament
1017 Wien

GZ: BMG-11001/0349-I/A/15/2011

Wien, am 3. Februar 2012

Sehr geehrte Frau Präsidentin!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 10089/J des Abgeordneten Dr. Karlsböck und weiterer Abgeordneter** nach den mir vorliegenden Informationen wie folgt:

Fragen 1 bis 27:
Zur vorliegenden parlamentarischen Anfrage habe ich eine Stellungnahme des Hauptverbandes der österreichischen Sozialversicherungsträger einholen lassen.

Ich darf nunmehr in Beantwortung dieser Anfrage das als Beilage angeschlossene Antwortschreiben des Hauptverbandes, das eine umfassende Darstellung des Informations- und IT-Sicherheitsmanagements der Krankenversicherungsträger beinhaltet, dem Parlament zur Verfügung stellen.

Beilage

Radetzkystraße 2, 1031 Wien Telefon **+43 1 71100-4300** Fax **+43 1 71100-14300**
Internet **www.bmg.gv.at** E-Mail **alois.stoeger@bmg.gv.at**

HAUPTVERBAND DER ÖSTERREICHISCHEN SOZIALVERSICHERUNGSTRÄGER

A-1031 WIEN KUNDMANNGASSE 21 POSTFACH 600 DVR 0024279
VORWAHL Inland: 01, Ausland: +43-1 TEL. 711 32 / Kl. 1211 TELEFAX 711 32 3775

Zl. 12-REP-43.00/11 Sd/Ht

Wien, 31. Jänner 2012

An das
Bundesministerium für Gesundheit
Radetzkystraße 2
1030 Wien

Per E-Mail

Betr.: Parlamentarische Anfrage Nr. 10089/J (Abg. Dr. Karlsböck und weitere Abgeordnete) betreffend Informations- und IT-Sicherheitsmanagement der Krankenkassen

Bezug: Ihre E-Mail vom 15. Dezember 2011, GZ: 90 001/222-II/A/7/2011

Sehr geehrte Damen und Herren!

Der Hauptverband der österreichischen Sozialversicherungsträger nimmt wie folgt Stellung:

Allgemein darf ausgeführt werden, dass die im vorliegenden Zusammenhang in Rede stehenden Unterlagen in Summe mehrere tausend Dokumente umfassen. Diese Dokumente stehen der Aufsichtsbehörde selbstverständlich bei Bedarf jederzeit zur Verfügung, wir ersuchen aber um Verständnis, dass es schon aus rein technischen Gründen nicht möglich ist, diese nach anderen Themen gegliederten Unterlagen in lesbarer Form im Einzelnen im Zusammenhang mit einer Anfragebeantwortung vorzulegen.

Wir haben jedoch versucht, statt bloßer ja/nein-Antworten zwecks besseren Verständnisses auf einige Details näher einzugehen.

1. Verfügen die einzelnen Krankenkassen über ein zeitgemäßes Informations- und IT-Sicherheitskonzept?
2. Wenn nein, warum nicht?

Ja. Die Krankenversicherungsträger arbeiten in IT-Angelegenheiten (Grundsätze siehe die EDV-Richtlinien, avsv 87/2006 idF 260/2011) in der Praxis weitgehend über eine gemeinsame Tochtergesellschaft, die IT-Services der Sozialversicherung GmbH (ITSV), zusammen. Damit ist auch ein einheitliches Sicherheitsniveau sichergestellt.

Diese Institution verfügt über ein zeitgemäßes Informations- und IT-Sicherheitskonzept entsprechend der ISO/IEC 27001:2005. Auch dort, wo andere IT-Organisationen wie die SVD Büromanagement GmbH bzw. für das e-card-System die Sozialversicherungs-Chipkartengesellschaft SVC bestehen, sind solche Konzepte vorhanden und wird die gleiche Linie eines hohen Sicherheitsniveaus eingehalten.

3. Sind diese Informations- und IT Sicherheitskonzepte dokumentiert und auditierbar?
4. Wenn nein, warum sind sie nicht dokumentiert bzw. auditierbar?

Ja.

5. Entsprechen die Informations- und IT-Sicherheitskonzepte dem Österreichischen Informationssicherheitshandbuch, der Norm ISO/IEC 27001 oder einem anderen anerkannten Informationssicherheitsstandard?
6. Wenn nein, auf welcher Grundlage bauen sie auf?

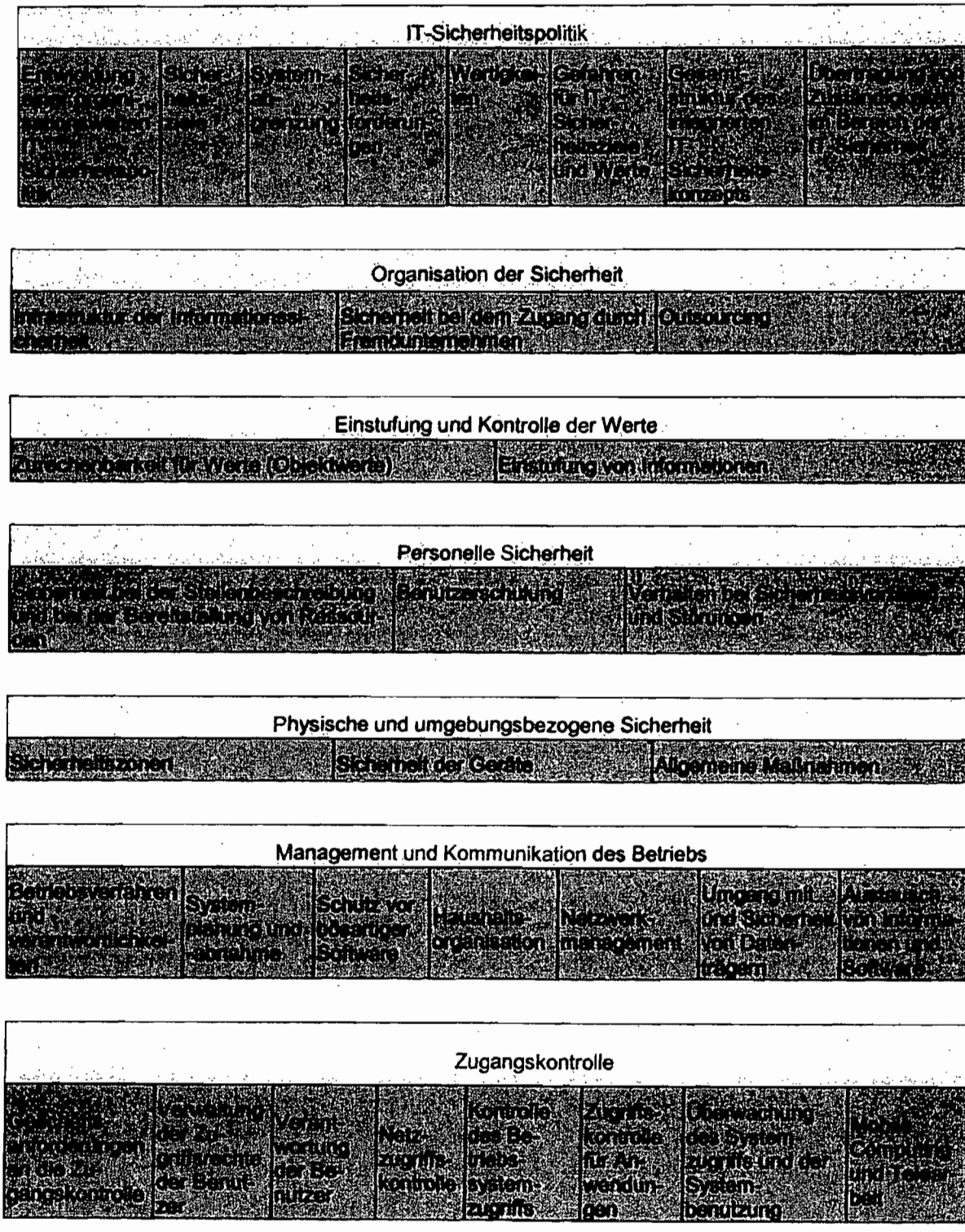
Ja, die ITSV ist ISO 27001 zertifiziert. Das Internetportal der österreichischen Sozialversicherung wurde im Zuge einer Risikoanalyse auf Grundlage der ISO 27001 evaluiert. Im Bereich des e-card-Systems richtet sich das integrierte Sicherheitskonzept nach folgenden technischen Normen:

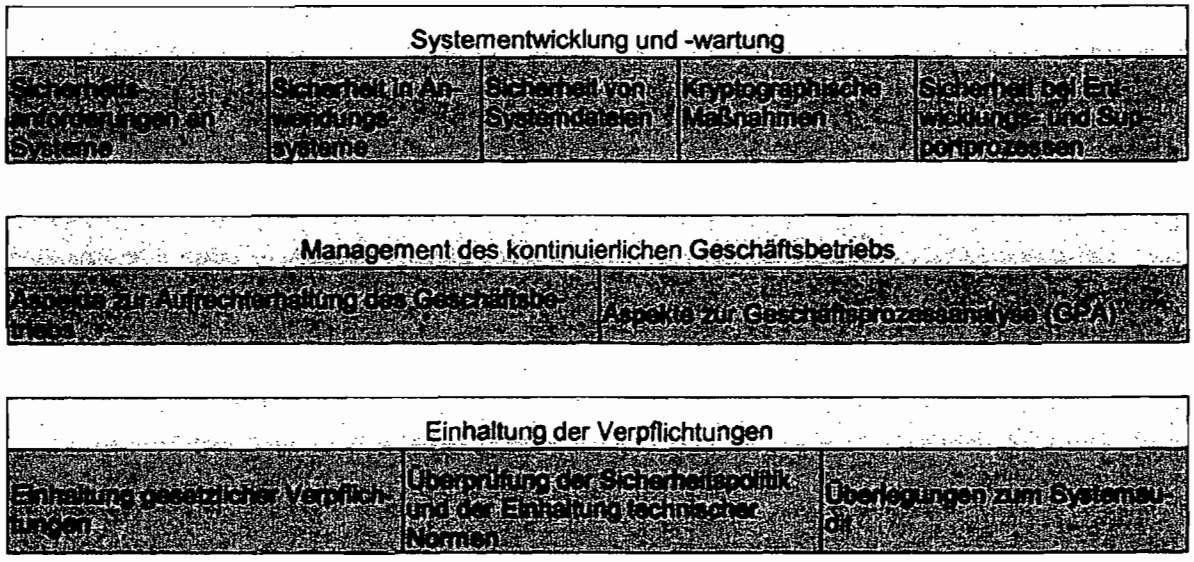
- ÖNORM A 17799 Informationstechnologie - Leitfaden für das Management der Informationssicherheit (jetzt: ISO/IEC 27002) und den
- Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC).

7. Welche Themenkreise umfassen die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen?

Von der ITSV wurde die ISO 27001 Zertifizierung für *alle* Aufgaben und alle Standorte erlangt. Ein *integriertes* Sicherheitskonzept ist die Grundlage der Gesamtheit aller IT-Sicherheitsmaßnahmen auch der SVC. Aufbauend darauf erfolgt die Umsetzung in Form von Sicherheitspolitik, Sicherheitsrichtlinien, Verfahrensanwei-

sungen und Einzelmaßnahmen. Die folgende Aufstellung bietet einen groben Überblick über die Themenkreise des Integrierten Sicherheitskonzeptes des e-card-Systems:





Das Internetportal der österreichischen Sozialversicherung umfasst diesbezüglich folgende Themenkreise:

- Übergabe von Softwareprodukten an den Betrieb
- Qualitätssicherung
- Releasemanagement
- Schnittstellen zu Backend Systemen
- Servicelevels
- Styleguide
- Supportkonzept
- Betriebsstandards
- Softwareentwicklungsstandards
- Technische Architektur
- Vorgehensmodelle
- Policy Authentifizierung und elektronische Signatur
- Policy Barrierefreiheit

Im Wesentlichen umfassen Sicherheitsmaßnahmen Verfahrensweisen, Prozeduren und Mechanismen, die die Sicherheit eines IT-Systems erhöhen. Dies kann *auf unterschiedliche Arten erreicht werden, die in der Folge beispielhaft dargestellt werden.* Sicherheitsmechanismen dienen dazu

- Risiken vermeiden,
- Bedrohungen oder Schwachstellen verkleinern,
- unerwünschte Ereignisse entdecken,
- die Auswirkung eines unerwünschten Ereignisses eingrenzen,
- Risiken überwälzen oder
- es möglich machen, einen früheren Zustand wiederherzustellen.

Von der STGKK werden folgende Bereiche genannt:

- Klassifizierung
- Physische Sicherheit
- Zugriffskontrolle

- Sicherheit von Kommunikation und Betrieb
- Sicherheit bei Systementwicklung und Wartung
- Umgang mit Sicherheitsvorfällen
- Aufrechterhaltung der Betriebsbereitschaft
- Einhaltung von Sicherheitsvorschriften

Bei der SGKK sind folgende Themenkreise umfasst:

- Regelungen für Mitarbeiter
- PC-Richtlinien; Benutzung von Endgeräten
- Sicherheitssensibilisierung
- Geregelte Einarbeitung neuer Mitarbeiter
- Regelungen für den Einsatz von Fremdpersonal
- Bauliche und infrastrukturelle Maßnahmen
- Regelungen betreffend Zutrittsberechtigungen
- Einbruchschutz
- Videounterstützte Überwachung
- Alarmanlage für die Nachtstunden
- Portierdienst
- Brandschutz
- Besonderer Brandschutz für zentrale IT-Einrichtungen
- Rauchverbot
- Maßnahmen bei der Stromversorgung; USV-Einrichtung
- Materielle Sicherung von Leitungen und Verteilern
- Geeignete Aufstellung der IT-Systeme und Server
- Einrichtung eines Datensicherungsraumes für die zentrale Datensicherung
- Einrichtung eines Datenschutzraumes für die Aufbewahrung von Datenträgern
- Sichere Aufbewahrung von Datenträgern in Schutzschränken
- Vorkehrungen zur Vorbeugung von Virenbefall
- Netzabsicherung mit Firewalls
- Regelmäßige Datensicherung
- Einsatz kryptografischer Verfahren bei der Datenübermittlung
- Einsatz kryptografischer Verfahren bei Fernzugriffen in das eigene Netzwerk (Remote-Access via VPN)
- Nutzung eines Authentifizierungsservers beim Fernzugriff (RSa-Token)
- Absicherung des Wireless LAN (WLAN)
- Regelungen für den Datenzugriff; Benutzerverwaltung; Rechteverwaltung
- Regelungen für den Passwortgebrauch
- Bildschirmsperre
- Absicherung der USB-Ports (in Arbeit)
- Verschlüsselung mobiler Notebooks
- Lizenzverwaltung und Lizenzaudits der Herstellerfirmen (zuletzt Microsoft)
- Redundante Auslegung von Netzwerkkomponenten
- Update & Upgrade von Soft- und Hardware im Netzbetrieb

Die BVA erwähnt dazu folgende Themenkreise:

- Sicherheitsleitlinie (Stellenwert der Informationsverarbeitung, Sicherheitsziele, Sicherheitsniveau, Strategien für das IT-Sicherheitsmanagement);

- Verantwortlichkeiten und Pflichten (Geschäftsführung, Führungskräfte, IT-Sicherheitsorganisation, Applikations- und Projektverantwortliche, Mitarbeiter);
- Risikostrategien, Risikoanalyse, Restrisiko, Risikoakzeptanz;
- Maßnahmen der IT-Sicherheit: (Klassifizierung von Informationen und IT-Anwendungen, Integrität von Daten und Informationen, Organisationsweite Richtlinien zu Sicherheitsmaßnahmen, Desaster Recovery Planung, Nachfolgeaktivitäten zur Überprüfung und Aufrechterhaltung der IT-Sicherheit, IT-Sicherheitsdokumentation);
- Life Cycle der IT-Sicherheitspolitik.

8. Umfassen die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen zumindest alle der nachfolgenden Themenkreise?

- **Sicherheitspolitik und -strategie, Richtlinien**
- **Sicherheitsorganisation**
- **Klassifizierung**
- **Personalsicherheit**
- **Physische Sicherheit**
- **Sicherheit von Kommunikation und Betrieb**
- **Zugriffskontrolle**
- **Sicherheit bei Systementwicklung und -wartung**
- **Umgang mit Sicherheitsvorfällen**
- **Aufrechterhaltung der Betriebsbereitschaft**
- **Einhaltung von Sicherheitsvorschriften**

9. Wenn nein, warum umfassen sie nicht alle der folgenden Themenkreise?

Ja.

10. Decken die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen organisatorische, personelle und technische Aspekte gleichermaßen ab?

11. Wenn nein, warum nicht?

Ja.

12. Wann wurden die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen in den letzten zwei Jahren auf ihre Wirksamkeit geprüft?

13. Wenn nein, warum wurden sie nicht geprüft?

Die ITSV wurde 2011 durch externe Auditoren geprüft. Dieses letzte Auditing zur Feststellung der ISO/IEC 27001:2005 Zertifizierung fand im September/Oktober 2011 statt.

Für den Bereich des e-card-Systems wurden für verschiedene Teile des Sicherheitskonzeptes folgende Audits durchgeführt:

- Januar 2008: Audit VPN und OWA Zugang SVC System (Auditor: sec4you)
- August 2008: Review der Qualitätssicherungs-Prozesse der SVC (Auditor: Software Quality Lab)

Für 2012 ist eine Zertifizierung nach der ISO/IEC 27001 vorgesehen.

Für das Internetportal der österreichischen Sozialversicherung erfolgten folgende Audits:

- Dezember 2009 durch eine umfassende Risikoanalyse auf Basis ISO 27001 (Auditor: HMP Beratungs GmbH)
- Oktober 2010: Audit WebFarm (Auditor: Deloitte)
- Oktober 2011: Audit Internetauftritt (Auditor: Govcert.at)
- Jänner 2012: Audit Internetauftritt – Überprüfung der Umsetzung von Maßnahmen (Auditor: IBM)
- Sonst periodische Cert Audits (Auditor: Gov-Cert.at)

14. Wenn ja, von wem wurden die Informations- und IT-Sicherheitskonzepte der einzelnen Kassen geprüft?

Die ITSV wurde von der CIS Certification & Information Security Services GmbH, einem in Österreich akkreditierten ISO 27001 Zertifizierungsunternehmen, geprüft.

Bezüglich e-card-System und Internetportal der österreichischen Sozialversicherung wird auf die Antwort zu Frage 12 verwiesen.

15. Wenn ja, welche Aspekte wurden bei den Informations- und IT-Sicherheitskonzepten der einzelnen Kassen geprüft?

Bei der ITSV wurden alle Kontrollen der ISO 27001 geprüft.

Bezüglich e-card-System wird auf Frage 12 verwiesen.

Für das Internetportal der österreichischen Sozialversicherung wurden alle relevanten Aspekte geprüft.

16. Wenn ja, liegen Prüfberichte vor und mit welchen Ergebnissen bzw. Handlungsempfehlungen?
17. Wenn nein, warum nicht?

Zu Art und Umfang der – weitgehend sehr technisch gehaltenen und ohne Vorwissen bzw. eingehende begleitende Erklärungen nicht ohne Weiteres verständlichen – Unterlagen sei auf die Einleitung verwiesen. Es wird um Verständnis ersucht, dass diese Unterlagen gesammelt nicht vorgelegt oder zitiert werden.

Das Audit der ITSV wurde mit einem Auditbericht der CIS Certification & Information Security Services GmbH dokumentiert.

Im Bereich des e-card-Systems liegen zu jedem dieser Audits entsprechende Prüfberichte samt Handlungsempfehlungen vor.

Der Bereich des Internetportals der österreichischen Sozialversicherung wird laufend auf Schwachstellen überprüft und diese behoben. Im letzten Audit wurde eine Schwachstelle im Content Display System des Internetauftritts der Sozialversicherungen durch XSS (= Cross Site Scripting) aufgezeigt, die sich aber nicht direkt auf die eigenen Daten ausgewirkt hat, sondern als möglicher Angriffspunkt für die Besucher der Webseiten verwendet werden hätte können. Dieser wurde, um einem möglichen Reputationsschaden präventiv entgegenzuwirken, im November 2011 nach umfangreichen Arbeiten beseitigt. Im Jänner 2012 wird die erfolgreiche Beseitigung durch einen externen Dienstleister nochmals überprüft.

Auch die IT-relevanten Büroeinrichtungen bei den Sozialversicherungsträgern werden einschlägigen Prüfungen unterzogen.

18. Wurden die ggf. abgegebenen Handlungsempfehlungen aus den Prüfberichten vollständig umgesetzt?
19. Wenn nein, warum nicht?

Die Zertifizierung des von der ITSV eingeführten und nachgewiesenen Informationssicherheits-Managementsystems wurde nach ISO/IEC 27001:2005 ohne Erteilung von Auflagen erteilt.

Im Bereich des e-card-Systems wurden alle relevanten Handlungsempfehlungen umgesetzt.

Im Internetportal der österreichischen Sozialversicherung wurden alle identifizierten Schwachstellen behoben.

20. Gibt es bei den einzelnen Krankenkassen Datenklassifizierungsschemen in Bezug auf Vertraulichkeit?
21. Wenn nein, warum nicht?

In der ITSV werden zur Wahrung der Vertraulichkeit von Informationen alle Informationen, die in der ITSV einlangen, bearbeitet, aufbewahrt oder weitergegeben werden, in drei Vertraulichkeitsstufen eingeteilt:

- vertraulich
- intern
- öffentlich.

Der Umgang mit Dokumenten ist wird im Rahmen der Informationssicherheitsrichtlinien der ITSV geregelt und sieht insbesondere unterschiedliche Handhabungspflichten hinsichtlich

- der Kennzeichnung,
- der Aufbewahrung in Abwesenheit,
- der Weitergabe intern;
- der Weitergabe extern,
- des Ausdrucks,
- der Entsorgung - Papier;
- der Entsorgung - Datenträger

je Vertraulichkeitsstufe vor.

Im Bereich des e-card-Systems gibt es vier Stufen: „Offen", „Intern", „Vertraulich", „Geheim". Am Internetportal der österreichischen Sozialversicherung gibt es ein e-Government-konformes Sicherheitsklassenkonzept.

22. Regeln diese Datenklassifizierungsschemen den Umgang mit Daten von der Übernahme/Anlage bis zu ihrer Löschung/Vernichtung, d.h. über deren gesamten Lebenszyklus hinweg?
23. Wenn nein, warum nicht?

Ja.

24. Werden §14 und §15 des Datenschutzgesetzes (DSG) 2000 vollständig umgesetzt?
25. Wenn nein, warum nicht?

Ja.

26. Welche Unterlagen liegen vor, die diese Umsetzung belegen? (z.B. Vertraulichkeitsvereinbarungen, Unterlagen über durchgeführte Sensibilisierungsmaßnahmen, vertragliche Vereinbarungen mit Dritten, Prüfberichte, Konzepte)
27. Wenn nein, warum liegen keine vor?

Die ITSV hat zur Erreichung der ISO 27001-Zertifizierung ihr Informationssicherheitsmanagementsystem dokumentiert. Diese Dokumentation umfasst die Sicherheitspolitik der ITSV, aufgabenspezifische Sicherheitsrichtlinien, Vertraulichkeitsverpflichtungen für alle Mitarbeiter, externe Mitarbeiter und Lieferanten, Dokumentation zu Awarenessmaßnahmen und interne Audits und vieles mehr. So werden beispielsweise bereits im Rahmen des Einstellungsprozesses neue Mitarbeiter über die bestehende Geheimhaltungsverpflichtung nachweislich in Kenntnis gesetzt. Im Rahmen des Beschaffungsprozesses wird die Notwendigkeit des Abschlusses von datenschutzrechtlichen Dienstleisterverträgen (§§ 10 und 11 DSG 2000) geprüft bzw. diese abgeschlossen. Eine eigene Datenschutzschulung und eine Arbeitsrechtsschulung (in der auch die bestehenden Informationssicherheitsrichtlinien behandelt wer-

den) sowie weiterer Maßnahmen (Informationssicherheitswettbewerb) dienen der Steigerung der Awareness der Mitarbeiter der ITSV.

Im Bereich des e-card-Systems liegen Dienstverträge und Vertraulichkeitsvereinbarungen vor. Im Bereich des Internetportals der österreichischen Sozialversicherung relevante Konzepte, Auditergebnisse, Umsetzungsdokumentation. Zu solchen Unterlagen, die aufgrund des Umgangs mit personenbezogenen Daten auch bei den Sozialversicherungsträgern bestehen, gehören:

- Verpflichtung zur Verschwiegenheit und zur Wahrung des Datengeheimnisses bei Eintritt neuer Mitarbeiter,
- Vertraulichkeitsvereinbarungen mit Dritten,
- Unterlagen über durchgeführte Sensibilisierungsmaßnahmen,
- Merkblätter bei Verwendung von externen Datenträgern,
- Dienstanweisungen,
- eine für alle Mitarbeiter stets zugängliche Datenschutz-Entscheidungssammlung (im Intranet)
- die Datenschutz-Rechtsgrundlagen werden allen Mitarbeitern in einer Datenbank zur jederzeitigen Einsicht zur Verfügung gestellt,
- Protokollierung der beim Datenverarbeitungsregister gemeldeten Datenanwendungen,
- Zugriffsprotokollierung (soweit sich die Applikation im Verantwortungsbereich der WGKK befindet)

Im Zuge der Grundschulung neuer Mitarbeiter erfolgt eine Belehrung über die Datenschutzbestimmungen. In Dienstanweisungen wird auf die Bestimmungen des Datenschutzgesetzes, auf die Datenschutzverordnung des Hauptverbandes, die Verschwiegenheitspflicht nach § 460a ASVG und § 8 Abs. 3 DO.A und DO.B sowie § 7 Abs. 4 DO.C verwiesen. Für die in Krankenanstalten vorliegenden Daten gilt zusätzlich noch die Verschwiegenheit nach den Krankenanstaltengesetzen.

Mit freundlichen Grüßen
Für den Hauptverband:

Dr. Josef LANDLHOFER