Bericht des Rechnungshofes

Register im Hauptverband der österreichischen Sozialversicherungsträger

Inhalt

Inhaltsverzeichnis

Abkürzungen

Abkürzungsverzeichnis

Abs.	Absatz
AJ	Auskunftserteilung an Justiz– und Verwaltungsbehörden
AMS	Arbeitsmarktservice
ANSP	Anspruchsdatenbank
ASVG	Allgemeines Sozialversicherungsgesetz
AVI	Amtliche Verlautbarungen
B–KUVG	Beamten–Kranken– und Unfallversicherungsgesetz
BERE	Berechtigungssystem für Standardprodukte
BKA	Bundeskanzleramt
BM...	Bundesministerium ...
BMASK	für Arbeit, Soziales und Konsumentenschutz
BMF	für Finanzen
BMG	für Gesundheit
BMI	für Inneres
BMSVG	Betriebliches Mitarbeiter– und Selbständigenvorsorgegesetz
BMV	Betriebliche (Mitarbeiter–)Vorsorge im Hauptverband
bPK	bereichsspezifisches Personenkennzeichen
bspw.	beispielsweise
BSVG	Bauern–Sozialversicherungsgesetz
BUAG	Bauarbeiter–Urlaubs– und Abfertigungsgesetz
BUAK	Bauarbeiter–Urlaubs– und Abfertigungskasse
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
DSG 2000	Datenschutzgesetz 2000
e–card	Chipkarte der Sozialversicherung
E–GovG	E–Government–Gesetz
EDV	Elektronische Datenverarbeitung
EKO–BDB	Erstattungskodex Basisdatenbank
ELDA	Elektronischer Datenaustausch mit den Sozialversicherungsträgern
ELGA	Elektronische Gesundheitsakte
ePK	Elektronisches Pensionskonto
EUR	Euro
FB	Familienbeihilfedatenbank

Abkürzungen

GmbH	Gesellschaft mit beschränkter Haftung
GSVG	Gewerbliches Sozialversicherungsgesetz
Hauptverband	Hauptverband der österreichischen Sozialversicherungs–träger
HONO	Honorarordnungsverwaltung
i.d.(g.)F.	in der (geltenden) Fassung
i.V.m.	in Verbindung mit
IT	Informationstechnologie
IT–SV GmbH	IT–Services der Sozialversicherung GmbH
KONS	e–card–Konsultationssystem
KV–Träger	Krankenversicherungs–Träger
LDAP	Lightweight Directory Access Protocol (elektronischer Verzeichnisdienst)
LIVE	Leistungsinformation für Versicherte
Mio.	Million(en)
Mrd.	Milliarde(n)
rd.	rund
RH	Rechnungshof
RIS	Rechtsinformationssystem des Bundes
SozDok	Dokumentation des österreichischen Sozialversicherungs-rechts
SV	Sozialversicherung
SV–DSV	SV–Datenschutzverordnung 2001
TZ	Textzahl(en)
Z–PI	Zentraler Patientenindex
z.B.	zum Beispiel
ZG	Zentrales Gewerberegister
ZMR	Zentrales Melderegister
ZPR	Zentrales Personenstandsregister
ZPV	Zentrale Partnerverwaltung
ZUP	Zugriffsprotokolle der Online–Verarbeitung des Hauptverbands
ZVD	Zentrale Versicherungsdatei

Wirkungsbereich des Bundesministeriums für Arbeit, Soziales und Konsumentenschutz

Register im Hauptverband der österreichischen Sozialversicherungsträger

Der Hauptverband der österreichischen Sozialversicherungsträger betrieb zentrale Register, die unter anderem strukturierte Daten über Personen, Wirtschaftstreibende sowie Leistungserbringer enthielten. Eine gesetzliche Regelung für die Sozialversicherung zur verpflichtenden Umsetzung einer Internet (Cyber) Sicherheitsstrategie fehlte ebenso wie ein spezielles Team von IT–Sicherheitsfachleuten (Computer Emergency Response Team) zum koordinierten Schutz der IT–Infrastruktur.

Beim Datenaustausch zwischen der Sozialversicherung und anderen staatlichen Tätigkeitsbereichen wurden historisch bedingt oftmals die personenbezogenen Daten mittels (Sozial–) Versicherungsnummer zugeordnet, obwohl mit dem E–Government–Gesetz 2004 hiefür die Alternative einer Zuordnung mittels eines bereichsspezifischen Kennzeichens geschaffen wurde. Dies würde zu einem erhöhten Schutz beim elektronischen Austausch von personenbezogenen Daten führen.

Bereichsübergreifende Arbeitsgruppen des BMASK und des Hauptverbands der österreichischen Sozialversicherungsträger und eine Studie der Universität Wien behandelten die Nutzung der Registerdaten zur Erkennung und Verhinderung von Sozialbetrug mittels Scheinfirmen. Konkrete Maßnahmen zur Einrichtung von Früherkennungsmechanismen waren noch nicht umgesetzt. Teilweise war eine Auswertung von Registerdaten zur Früherkennung aufgrund ungenügender Dateninhalte oder verzögerter Datenerfassung nicht möglich.

KURZFASSUNG

Prüfungsziele

Ziel der Gebarungsüberprüfung war die Darstellung und Beurteilung zentraler Register des Hauptverbands der österreichischen Sozialversicherungsträger (Hauptverband). Weiters waren die Möglichkeiten der Früherkennung von Sozialbetrug durch Scheinfirmen unter Verwendung der Registerinhalte Gegenstand der Gebarungsüberprüfung. Darüber hinaus wurden die Vorkehrungen hinsichtlich der Internet (Cyber) Sicherheit der Registerinhalte im Internet (Cyber Raum) beurteilt. (TZ 1)

Ausgangslage Register

Allgemeines

Ein Register ist ein vollständiges und strukturiertes Verzeichnis von Daten, die ein bestimmtes Merkmal verbindet. Die Führung eines Registers beruhte grundsätzlich auf einer gesetzlichen Verpflichtung. Diese beschrieb unter anderem die Bezeichnung des Registers, den Inhalt der Daten, die Zielsetzungen, die Zugangsberechtigungen, die Datenübermittlungen an andere bzw. von anderen Registern und den Eigentümer. (TZ 2)

Bei der Gebarungsüberprüfung wurden jene Register betrachtet, die Grundlage für das Verwaltungshandeln der Sozialversicherung waren. Die Betriebs– und Wartungskosten dieser 15 Register für das Jahr 2012 betrugen rd. 6,17 Mio. EUR, die Weiterentwicklungskosten rd. 2,44 Mio. EUR. (TZ 2)

Register im Hauptverband

Zur Verwaltung der Stammdaten und der Versicherungsverhältnisse wurde vom Hauptverband die Kernapplikation „Zentrale Versicherungsdatenspeicherung“ betrieben. Darüber hinaus wurden vom Hauptverband weitere zentrale Register geführt. Diese dienten der Erfassung und Verarbeitung von sozial– und pensionsrechtlichen Daten. Mit der Zentralisierung der IT–Infrastruktur (IT–SV GmbH) und der Zentralisierung der Register ging jedoch keine Vereinheitlichung der Sicherheits– und Schutzstandards im gesamten Bereich der Sozialversicherung einher. (TZ 3)

Ausgangslage Verwaltungsreforminitiative

Der Gesetzgeber hatte mit dem E–Government–Gesetz (E–GovG) und im Rahmen von Verwaltungsreforminitiativen verstärkt die Nutzung zentraler Register und die elektronische Kommunikation zur Optimierung und Beschleunigung von Verwaltungsverfahren beabsichtigt. Ziel war zudem die Reduzierung von Behördenwegen für den Bürger und die Wirtschaft (One–Stop–Shop). (TZ 4)

Die Zielvorgaben zu den Verwaltungsreforminitiativen der Bundesregierung zur Nutzung zentraler Register und den damit möglichen Entlastungen für die Bürger und Wirtschaft sowie die Beschleunigung von Verwaltungsverfahren waren zweckmäßig. Daraus ergaben sich jedoch Herausforderungen zum Schutz der in den Registern der Sozialversicherung gespeicherten Daten. (TZ 4)

Generelle Problemlage bei Registern

Verwaltungsvereinfachung und One–Stop–Shop

Das Prinzip des One–Stop–Shop war mit der Erfassung einer Geburt durch die jeweilige Personenstandsbehörde sowie der elektronischen Übertragung der Daten an die Sozialversicherungsträger für 77 % der Personenstandsfälle grundsätzlich verwirklicht. 23 % der Meldungen erforderten einen getrennten Behördenweg des Bürgers zur Erfassung der Daten beim jeweiligen Sozialversicherungsträger. Dies war erforderlich, weil die betroffenen Personenstandsbehörden technisch nicht in der Lage waren, die Daten elektronisch zu übermitteln. Mit der geplanten Umsetzung des Zentralen Personenstandsregisters (ZPR) Ende 2013 sollten von den Personenstandsbehörden alle Änderungen von Personenstandsfällen elektronisch vom ZPR in die Zentrale Partnerverwaltung (ZPV) des Hauptverbands übertragen werden. Damit würde die zusätzliche Erfassung der Daten beim jeweiligen Sozialversicherungsträger entfallen. (TZ 5)

Konsistenz der Daten

Ein Abgleich der Daten der ZPV des Hauptverbands bezüglich der Namensschreibweise natürlicher Personen mit dem Zentralen Melderegister (ZMR) und den Registern der Personenstandsbehörden war nicht vorgesehen. Fallweise lagen der Sozialversicherung Dokumente vor, die den aktuellen Einträgen in den anderen Registern widersprachen. Bei abweichender Datenlage wurde kein Abgleich mit der jeweilige Einrichtung durchgeführt. (TZ 6)

Nutzung von „Führenden Registern“

Der Hauptverband benötigte für die „Zentrale Partnerverwaltung“ u.a. die Daten von Unternehmen, Vereinen und sonstigen Betroffenen. Die Daten zu Unternehmen und Vereinen bezog der Hauptverband von einem externen Dienstleister. Für die Bereitstellung der Daten wurden an den externen Dienstleister im Geschäftsjahr 2012 pauschal 45.000 EUR bezahlt. Die Statistik Austria führte im Unternehmensregister–Verwaltung alle Unternehmen, Vereine und sonstigen Betroffenen. Die Statistik Austria teilte mit, dass die vom Hauptverband benötigten Daten durch das Unternehmensregister–Verwaltung bereitgestellt werden könnten. Eine Übernahme der Daten aus dem Unternehmensregister–Verwaltung war noch nicht erfolgt. (TZ 7)

Datenabgleich mittels Personenkennzeichens

Die Umsetzung zentraler Register und der elektronische Datenaustausch über staatliche Tätigkeitsbereiche hinweg verlangten nach einer insgesamt höheren Sicherheit der gespeicherten Daten und einem sicheren elektronischen Datenaustausch. Dazu wurde vom Gesetzgeber das E–Government–Gesetz beschlossen. Trotz der Einführung des Systems des bereichsspezifischen Personenkennzeichens (bPK) im Jahr 2004 wurden vom Hauptverband weiterhin Schnittstellen betrieben, die einen Datenaustausch mit anderen Tätigkeitsbereichen mittels Versicherungsnummer bewerkstelligten. Die Verwendung der Versicherungsnummer als eindeutiger Identifikator bei der Übertragung personenbezogener Daten stellte keinen ausreichenden Schutz vor der Zuordnung durch Unbefugte dar. (TZ 8)

Schnittstellen

Die vom Hauptverband betriebenen Schnittstellen – welche zur Datenübertragung über den Tätigkeitsbereich der Sozialversicherung hinaus genutzt wurden – unterstützten bis auf die Schnittstelle zur Statistik Austria nicht den Datenaustausch mittels bPK. (TZ 9)

Sozialbetrug durch Scheinfirmen

Früherkennung von Scheinfirmen

Das BMASK, der Hauptverband, das BMF, das BMJ und das BMI beschäftigten sich in interministeriellen Arbeitsgruppen mit Möglichkeiten, wie systematischer Sozialbetrug – besonders jener mittels Scheinfirmen – unter anderem durch die Nutzung von Daten aus den Registern der Sozialversicherung und der Verknüpfung mit anderen Registern der öffentlichen Verwaltung erkannt und verhindert werden könnte. (TZ 10)

Eine Gebietskrankenkasse beschäftigte sich aktuell mit einer derartigen automatisationsunterstützten Methodik, mit deren Hilfe anhand auffälliger Muster bei festgelegten Merkmalen verdächtige Firmen detektiert werden konnten. Bei anderen Sozialversicherungsträgern kamen derartige Methoden hingegen noch nicht zum Einsatz. (TZ 10)

Nach Schätzung des BMF wurden rd. 300 Scheinfirmen pro Jahr gegründet, wodurch es zu einem potenziellen Schaden durch Abgaben– und Beitragsausfälle von rd. 300 Mio. EUR kam. (TZ 10)

Dateninhalt und Datenaktualität

Aus dem Endbericht eines vom BMASK beauftragten Forschungsprojekts ging hervor, dass die Anwendung einer automationsunterstützten Auswertung von Indikatoren zur Erkennung von Sozialbetrug wesentlich von den zur Verfügung stehenden Dateninhalten und der Datenaktualität abhängt. Es zeigte sich, dass nicht alle hiefür notwendigen Daten erfasst bzw. rechtzeitig erfasst wurden. (TZ 11)

Cyber Sicherheit

Allgemeines

Im Mai 2012 wurde vom Ministerrat ein „Cyber Security Gesamtkonzept“ und im März 2013 dazu ein umfassendes und proaktives Konzept „Österreichische Strategie für Cyber Sicherheit“ beschlossen. Ziel war die Einbindung strategisch relevanter Betreiber von kritischer Infrastruktur zur Gewährleistung der Cyber Sicherheit unter breiter Einbindung von Experten aus Verwaltung, Wissenschaft und Wirtschaft. 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 Cyber Sicherheit gesetzt worden. (TZ 12)

Cyber Sicherheit in der Sozialversicherung

Im Bereich der Sozialversicherung waren Teilaspekte der Cyber Sicherheit in Form von Arbeitsgruppen, Prozessen und Sicherheitsmaßnahmen einzelner IT–Betreiber verwirklicht. Eine verpflichtende Teilnahme bzw. Übernahme von Sicherheitsstandards durch die Sozialversicherungsträger bestand nicht. Eine gesetzliche Regelung sowie eine Gesamtstrategie zur Cyber Sicherheit in der Sozialversicherung waren nicht vorhanden. (TZ 13, 14)

Computer Emergency Response Team (CERT) in der Sozialversicherung

Innerhalb der Sozialversicherung beschäftigten sich Arbeitsgruppen mit Aspekten der Cyber Sicherheit. IT–Sicherheitsfachleute, welche die Aufgaben eines Sozialversicherungs CERT als Kernaufgabe für die Sozialversicherung wahrgenommen hätten, gab es nicht. (TZ 15)

Krisenmanagement und Kontinuitätspläne

Spezifische Kontinuitätspläne von Sozialversicherungsträgern, der IT–Services der Sozialversicherung GmbH und der Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. – SVC sowie der Allgemeinen Unfallversicherungsanstalt waren vorhanden. Ein die Sozialversicherung übergreifendes Krisenmanagement und Kontinuitätspläne zur Bewältigung etwaiger Angriffe auf die IT–Struktur der Sozialversicherung fehlten. (TZ 16)

Sicherungs– und Schutzstandards

Die zentralen Dienstleister der Sozialversicherung hatten definierte Schutzstandards. Trotz der Maßnahmen dieser zentralen IT–Dienstleister bestand auch aus Sicht des Hauptverbands „aufgrund der vorhandenen Schnittstellen zu den dezentralen, sicherheitstechnisch nicht harmonisierten Bereichen ein nicht zu unterschätzendes und nicht einschätzbares Risikopotenzial“. Zentral koordinierte und einheitliche Schutz– und Sicherheitsstandards der Einrichtungen der Sozialversicherung waren nicht vorhanden. (TZ 17)

Meldepflicht bei kritischen Vorfällen

Angriffe auf Systeme der Sozialversicherung, erfolgte Schädigungen sowie erfolgreiche unbefugte Zugriffe wurden nicht zwingend an einen zentralen Dienstleister kommuniziert. Cyber Sicherheitsvorfälle waren nicht zwingend zu dokumentieren und weiterzuleiten; somit konnten entsprechende Maßnahmen nicht immer erarbeitet werden. (TZ 18)

Sensibilisierung der Mitarbeiter

Die IT–Services der Sozialversicherung GmbH entwarf zur Sensibilisierung Awareness–Letters und übermittelte diese an alle Mitarbeiter der Sozialversicherung. Die Sozialversicherungsträger boten den Mitarbeitern Schulungen zum sicheren Umgang mit der IT–Infrastruktur an. Vorgaben für alle Sozialversicherungsträger zu Inhalt, Umfang und Zeitabständen zwischen den Schulungen bestanden nicht. (TZ 19)

Katastrophenübungen

Der Hauptverband beauftragte eine Fachhochschule sowie Hersteller von Sicherheitsprodukten zur Überprüfung der zentralen IT–Einrichtungen der Sozialversicherung, simulierte Angriffe durchzuführen. Katastrophenübungen, die eine Beeinträchtigung weiter Teile der IT der Sozialversicherung zum Inhalt hatten, wurden nicht durchgeführt. (TZ 20)

Kenndaten zu den Registern im Hauptverband der österreichischen Sozialversicherungsträger	
Bezeichnung des Registers	**Rechtsgrundlagen**
Zentrale Partnerverwaltung (ZPV)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Zentrale Versicherungsdatei (ZVD)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Zugriffsprotokolle der Online–Verarbeitung des Hauptverbands (ZUP)	Datenschutzgesetz 2000 i.d.g.F.
Berechtigungssystem für Standardprodukte (BERE)	Datenschutzgesetz 2000 i.d.g.F.
Dokumentation des österreichischen Sozialversicherungsrechts (SozDok)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Amtliche Verlautbarungen (AVI)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Honorarordnungsverwaltung (HONO)	Bundesgesetz über die Dokumentation im Gesundheitswesen i.d.g.F. Verordnung zum Gesundheitsdokumentationsgesetz vom 30. Juni 2010
Betriebliche (Mitarbeiter–) Vorsorge im Hauptverband (BMV)	Betriebliches Mitarbeiter– und Selbständigenvorsorgegesetz – BMSVB
Erstattungskodex Basisdatenbank (EKO–BDB)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Elektronisches Pensionskonto (ePK)	Allgemeines Pensionsgesetz i.d.g.F.
Zentraler Patientenindex (Z–PI)	ELGA–Gesetz (Gesundheitstelematikgesetz 2012)
Leistungsinformation für Versicherte (LIVE)	Allgemeines Sozialversicherungsgesetz i.d.g.F. Gewerbliches Sozialversicherungsgesetz i.d.g.F. Bauern–Sozialversicherungsgesetz i.d.g.F. Beamten–Kranken– und Unfallversicherungs-gesetz i.d.g.F.
Familienbeihilfedatenbank (FB)	Allgemeines Sozialversicherungsgesetz i.d.g.F. Gewerbliches Sozialversicherungsgesetz i.d.g.F. Bauern–Sozialversicherungsgesetz i.d.g.F. Familienlastenausgleichsgesetz 1967 i.d.g.F.
e–card–Konsultationssystem (KONS)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Anspruchsdatenbank (ANSP)	Allgemeines Sozialversicherungsgesetz i.d.g.F.

Quelle: RH

Register im Hauptverband der österreichischen Sozialversicherungsträger

Prüfungsablauf und –gegenstand

1 Der RH überprüfte von April bis August 2013 beim Hauptverband der österreichischen Sozialversicherungsträger (Hauptverband) und dem BMASK die Gebarung hinsichtlich der Register im Sozialversicherungsbereich. Im Rahmen der Überprüfung wurden vom RH Informationen bei der Datenschutzkommission, der Stammzahlenregisterbehörde, dem BKA, dem BMI, der IT–Services der Sozialversicherung GmbH und der Statistik Austria eingeholt.

Ziel der Gebarungsüberprüfung war die Darstellung und Beurteilung zentraler Register des Hauptverbands. Weiters waren die Möglichkeiten der Früherkennung von Sozialbetrug durch Scheinfirmen unter Verwendung der Registerinhalte Gegenstand der Gebarungsüberprüfung. Darüber hinaus wurden die Vorkehrungen hinsichtlich der Internet (Cyber) Sicherheit der Registerinhalte im Internet (Cyber Raum) beurteilt.

Der Prüfungszeitraum bezog sich vornehmlich auf das Jahr 2012.

Zu dem im November 2013 übermittelten Prüfungsergebnis nahmen das BMASK und der Hauptverband im Februar 2014 Stellung. Der RH erstattete seine Gegenäußerung im April 2014.

Ausgangslage Register

Allgemeines

2 Für den Begriff der Register bestand keine gesetzliche Definition. Nachfolgend wurde die in der Bundesverwaltung gängige Beschreibung „Ein Register ist ein vollständiges und strukturiertes Verzeichnis von Daten, die ein bestimmtes Merkmal verbindet“ übernommen.

Die Führung eines Registers setzte eine gesetzliche Verpflichtung voraus. Aus diesen gesetzlichen Vorgaben leiteten sich unter anderem die Bezeichnung des Registers, der Inhalt der Daten, die Zielsetzungen, die Zugangsberechtigungen, die Datenübermittlungen an andere bzw. von anderen Registern, der jeweilige Eigentümer des Registers und allenfalls dessen Dienstleister als technischer Betreiber ab.

Bei der Gebarungsüberprüfung wurden jene Register betrachtet, die Grundlage für das Verwaltungshandeln der Sozialversicherung waren. Die Betriebs– und Wartungskosten dieser 15 Register für das Jahr 2012 betrugen rd. 6,17 Mio. EUR, die Weiterentwicklungskosten rd. 2,44 Mio. EUR.

Daten zu den evaluierten Registern der Sozialversicherungsträger		
Bezeichnung	**Kenngrößen (gerundet)**	**Betriebs– und Wartungskosten 2012**
		in EUR
Zentrale Partnerverwaltung (ZPV)	13,3 Mio. aktuelle Partner gespeichert 2 Mrd. Zugriffe 2012	1.257.000
Zentrale Versicherungsdatei (ZVD)	92 Mio. Versicherungsverhältnisse gespeichert 93 Mio. Änderungen/Eingaben 2012 50 Mio. Abfragen 2012	2.000.000
Zugriffsprotokolle der Online–Verarbeitung des Hauptverbands (ZUP)	9 Mio. Protokollierungen pro Tag 45.000 Abfragen 2012	184.000
Berechtigungssystem für Standardprodukte (QBADMIN/BERE)	630.000 Datensätze gespeichert 20 Mio. Zugriffe 2012	30.000
Dokumentation des österreichischen Sozialversicherungsrechts (SozDok)	1,5 Gigabyte gespeicherte Daten (Text) 1.400 Zugriffe 2012	84.000
Amtliche Verlautbarungen (AVI)	10 Gigabyte gespeicherte Daten 15.000 Zugriffe 2012	141.000
Honorarordnungsverwaltung (HONO)	1,4 Mio. Datensätze gespeichert 213.000 Zugriffe 2012	432.000
Betriebliche (Mitarbeiter–) Vorsorge im Hauptverband (BMV)	82 Mio. Datensätze gespeichert 225.000 Abfragen 2012	128.000
Erstattungskodex Basisdatenbank (EKO–BDB)	130.000 Datensätze (Pharmanummern)	237.000
Elektronisches Pensionskonto (ePK)	5,5 Mio. Pensionskonten gespeichert 30.000 Zugriffe 2012	280.000
Zentraler Patientenindex (Z–PI)	15,5 Mio. Personendatensätze gespeichert	718.000
Leistungsinformation für Versicherte (LIVE)	1,4 Mio. Leistungsinformationen 2012 150.000 Zugriffe 2012	128.000
Familienbeihilfedatenbank (FB)	9 Mio. Datensätze gespeichert 110.000 Abfragen 2012	3.000
e–card Konsultationssystem (KONS)	831 Mio. Datensätze gespeichert 115 Mio. Konsultationen 2012	552.000 Betrieb u. Wartung gemeinsam mit ANSP
Anspruchsdatenbank (ANSP)	10,2 Mio. Versicherte und Angehörige 115 Mio. Zugriffe 2012	Betrieb u. Wartung gemeinsam mit KONS
Summe		**6.174.000**

Quelle: Hauptverband

Register im Hauptverband

3.1 Dem Hauptverband oblag die zentrale Erbringung von Dienstleistungen für die Sozialversicherungsträger. Zu diesen zentralen Dienstleistungen gehörten unter anderem

- die Vergabe von einheitlichen Versicherungsnummern und deren Verknüpfung mit dem bereichsspezifischen Personenkennzeichen (bPK) zur Verwaltung personenbezogener Daten im Rahmen der an die Sozialversicherung gesetzlich übertragenen Aufgaben sowie

- die Errichtung und Führung einer zentralen Anlage zur Aufbewahrung und Verarbeitung der für die Versicherten bzw. den Leistungsbezug bedeutsamen Daten aller versicherten Personen, Dienstgeber sowie Leistungserbringer (Ärzte, Krankenanstalten, Hebammen, etc.).

In Umsetzung einer zentralen IT–Strategie wurde die IT–Services der Sozialversicherung GmbH mit dem Ziel einer verstärkten Zusammenarbeit auf dem Gebiet der automationsunterstützten Datenverarbeitung und der Bündelung der strategischen Kompetenz des IT–Bereichs durch die Sozialversicherungsträger und den Hauptverband gegründet.

Im Jahr 2003 beschloss der Hauptverband, die lokalen Register zur Verwaltung der Stammdaten von Personen, Wirtschaftstreibenden sowie Leistungserbringern zu zentralisieren. Ziel des Projekts „Zentrale Partnerverwaltung“ (siehe Anhang ZPV) war es, die Datenqualität der Stammdaten nachhaltig zu verbessern. Die Produktivsetzung erfolgte im Mai 2008. Im Jahr 2012 waren rd. 13,3 Mio. Partner der Sozialversicherungen gespeichert, und es wurden rd. 2 Mrd. Zugriffe getätigt.

Die Umsetzung der ZPV erforderte ein den externen Partnern und den rd. 20.000 Zugriffsberechtigten in der Sozialversicherung entsprechendes Berechtigungssystem (siehe Anhang BERE) mit Zugriffsprotokollierung (siehe Anhang ZUP).

Zur Verarbeitung der Versicherungsdaten der Versicherten wurde die „Zentrale Versicherungsdatei“ (siehe Anhang ZVD) geschaffen. Diese diente innerhalb des Sozialversicherungsbereichs (Hauptverband) u.a. der Leistungsfeststellung (Pensionsberechnung) bei den Pensionsversicherungsträgern und der Berechnung des Allgemeinen Pensionskontos sowie der Feststellung des Krankenversicherungsschutzes (e–card), der Ausgabe von Versicherungsverläufen (Versicherungsdatenauszug) und der Berechnung der Rezeptgebührenobergrenze. Im Jahr 2012 waren rd. 92 Mio. Versicherungsverhältnisse gespeichert.

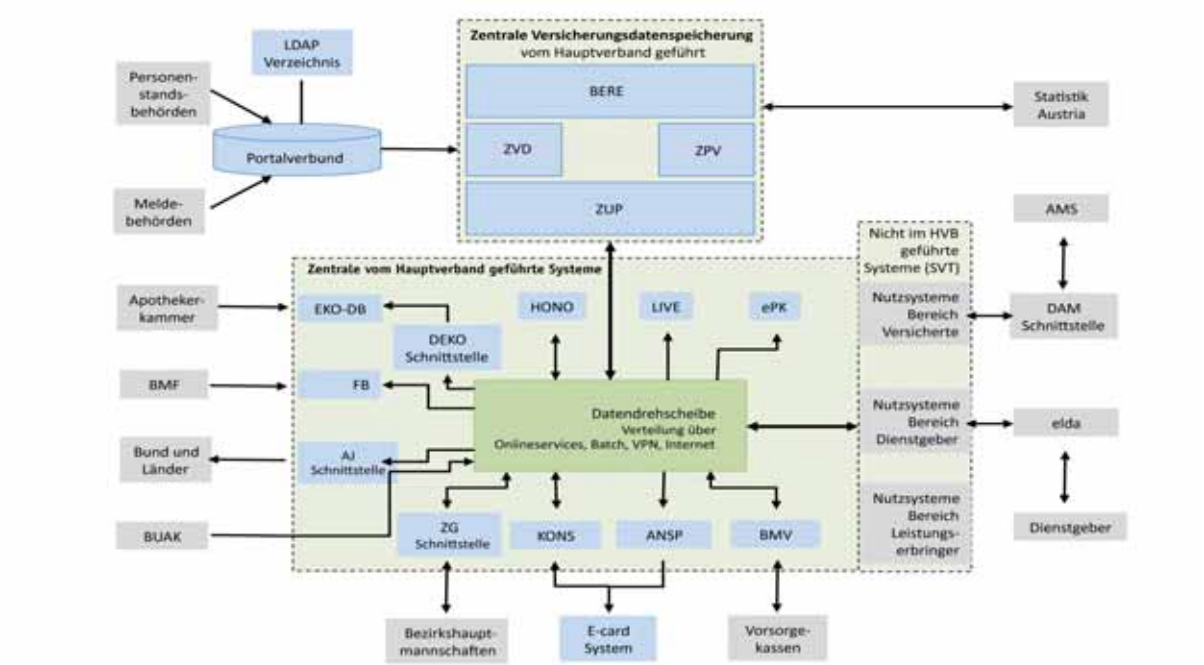
Die „Zentrale Partnerverwaltung“, das „Berechtigungssystem für Standardprodukte“, das „Zugriffsprotokoll der Online–Verarbeitung des Hauptverbands“ und die „Zentrale Versicherungsdatei“ bildeten gemeinsam die Kernapplikation „Zentrale Versicherungsdatenspeicherung“ zur Verwaltung der Stammdaten und der Versicherungsverhältnisse.

Darüber hinaus wurden vom Hauptverband weitere zentrale Register geführt. Diese dienten der Erfassung und Verarbeitung von sozial– und pensionsrechtlichen Daten. In der nachfolgenden Abbildung werden die Register und deren Verbindungen dargestellt. Im Anhang werden die Register inhaltlich beschrieben.

Zum Datenaustausch in der Allgemeinen Sozialversicherung bzw. mit anderen Tätigkeitsbereichen der Verwaltung wurden Schnittstellen entwickelt. Diese waren über eine zentrale Datendrehscheibe mit den Registern des Hauptverbands verbunden.

Eine den zentralen IT–Strukturen und der zentralen Registerlandschaft angemessene Vereinheitlichung der Sicherheits– und Schutzstandards in der Sozialversicherung wurde nicht umgesetzt. Dem Hauptverband waren die von den jeweiligen abfrageberechtigten Einrichtungen der Sozialversicherung etablierten Sicherheits– und Schutzstandards nicht bekannt.

Zentrale Register im Hauptverband, Datenaustausch und Datendrehscheibe



Vom Hauptverband geführte Systeme und Schnittstellen

LDAP	Lightweight Directory Access Protocol (elektronischer Verzeichnisdienst)
ZPV	Zentrale Partnerverwaltung
ZVD	Zentrale Versicherungsdatei
ZUP	Zugriffsprotokolle der Online–Verarbeitung des Hauptverbandes
BERE	Berechtigungssystem für Standardprodukte
SozDok	Dokumentation des österreichischen Sozialversicherungsrechts
AVI	Amtliche Verlautbarungen
HONO	Honorarordnungsverwaltung
BMV	Betriebliche (Mitarbeiter–) Vorsorge im Hauptverband
DEKO	Datenaustausch Erstattungskodex
EKO–DB	Erstattungskodex Basisdatenbank
ePK	Elektronisches Pensionskonto
Z–PI	Zentraler Patientenindex
LIVE	Leistungsinformation für Versicherte
FB	Familienbeihilfedatenbank
AJ	Auskunftserteilung an Justiz– und Verwaltungsbehörden
KONS	e–card–Konsultationssystem
ANSP	Anspruchsdatenbank
ZG	Zentrale Gewerberegisterdatenbank

Externe Systeme und Betreiber

BUAK	Bauarbeiter– Urlaubs– und Abfertigungskasse
AMS	Arbeitsmarktservice
DAM	Datenaustausch mit dem AMS
elda	Elektronischer Datenaustausch mit den Sozialversicherungsträgern
BMF	Bundesministerium für Finanzen

Quelle: Hauptverband

3.2 Der RH anerkannte die strukturierte zentrale Konsolidierung der IT–Strukturen und der Register im Hauptverband. Er bemerkte jedoch kritisch, dass mit der Zentralisierung der IT–Infrastruktur (IT–SV GmbH) und der Zentralisierung der Register keine Vereinheitlichung der Sicherheits– und Schutzstandards im gesamten Bereich der Sozialversicherung einherging. Der RH empfahl dem Hauptverband, im Rahmen der Umsetzung einer Cyber Sicherheitsstrategie (TZ 12) gemeinsame Sicherheits– und Schutzstandards für die Sozialversicherung umzusetzen (TZ 17).

3.3 *Das BMASK teilte in seiner Stellungnahme mit, dass es die Umsetzung der Empfehlungen im Rahmen der rechtlichen Möglichkeiten unterstützen werde.*

Laut Stellungnahme des Hauptverbands bestünden grundsätzlich keine Einwände gegen das Prüfungsergebnis „Register im Hauptverband" und der Darstellung der Register; er werde die Empfehlungen im Rahmen der rechtlichen Möglichkeiten unterstützen.

3.4 Der RH hielt eine zeitnahe Umsetzung konkreter diesbezüglicher Maßnahmen für zweckmäßig.

Ausgangslage Verwaltungsreforminitiative

4.1 Der Gesetzgeber hatte mit dem E–Government–Gesetz (E–GovG) und im Rahmen von Verwaltungsreforminitiativen verstärkt die Nutzung zentraler Register und die elektronische Kommunikation zur Optimierung und Beschleunigung von Verwaltungsverfahren beabsichtigt. Ziel war zudem die Reduzierung von Behördenwegen für den Bürger und die Wirtschaft (One–Stop–Shop).

Daraus ergaben sich hinsichtlich einer zunehmend digitalisierten Welt für die Bundesregierung besondere Herausforderungen, wie die Erkennung von Sozialbetrug mit Hilfe elektronischer Medien und der Schutz kritischer Infrastruktur mittels Cyber Sicherheit. Diesen Herausforderungen sollte durch modernste zur Verfügung stehende Mittel und durch ein breites Zusammenwirken im Rahmen eines Gesamtkonzepts begegnet werden. (Vortrag an den Ministerrat vom 1. März 2011 mit dem Aspekt „Daten nützen und schützen")

4.2 Der RH bewertete die Zielvorgaben zu den Verwaltungsreforminitiativen der Bundesregierung zur Nutzung zentraler Register und den damit möglichen Entlastungen für die Bürger und Wirtschaft sowie die Beschleunigung von Verwaltungsverfahren als zweckmäßig. Er wies auf die Herausforderungen zum Schutz der in den Registern der Sozialversicherung gespeicherten Daten hin.

Bei der Gebarungsüberprüfung stellte der RH Handlungsbedarf hinsichtlich Sicherheit des Datenaustausches, der Möglichkeit der Nutzung von Daten für die Früherkennung von Sozialbetrug sowie der für den Sozialversicherungsbereich übergreifend geltenden Sicherheitsstandards (Cyber Sicherheit) im IT–Bereich (Cyber Raum) fest. Der RH wies dazu insbesondere auf seine Empfehlungen zum Datenaustausch mittels bPK (TZ 8), zur Früherkennung von Scheinfirmen (TZ 10), zur fehlenden gesetzlichen Regelung bezüglich Cyber Sicherheit (TZ 13) und zur notwendigen Errichtung eines Sozialversicherungs CERT (TZ 15) hin.

Generelle Problemlage bei Registern

Verwaltungsvereinfachung und One–Stop–Shop

5.1 Die Bundesregierung beschloss im Ministerratsvortrag vom 8. April 2009 für ausgewählte Lebensbereiche, darunter Geburt, Eheschließung und Todesfall, Maßnahmen umzusetzen, die zu einer raschen Entlastung der Bürger führen.

Die geforderte Verwaltungsvereinfachung zeigte sich dadurch, dass z.B. bei Geburt, Eheschließung und Todesfall die Daten von der jeweiligen Personenstandsbehörde (Standesamt) erfasst und im jeweiligen lokalen Register eingetragen wurden. Die jeweilige Personenstandsbehörde war zumeist in der Lage, die Daten mit allen versicherungsrechtlichen Angaben an den Datenverbund des Hauptverbands und damit an den zuständigen Sozialversicherungsträger zu melden. Im Jahr 2012 erfolgten 77 % der diesbezüglichen Meldungen an die Sozialversicherungsträger elektronisch; 23 % der Meldungen erforderten einen getrennten Behördenweg des Bürgers zur Erfassung der Daten beim jeweiligen Sozialversicherungsträger. Die betroffenen Personenstandsbehörden waren technisch nicht in der Lage, die Daten elektronisch zu übermitteln.

Mit der geplanten Umsetzung des Zentralen Personenstandsregisters (ZPR) bis Ende 2013 sollten von den Personenstandsbehörden alle Änderungen von Personenstandsfällen elektronisch vom ZPR in die Zentrale Partnerverwaltung (ZPV) des Hauptverbands übertragen werden. Damit würde die Erfassung der Daten beim jeweiligen Sozialversicherungsträger entfallen.

5.2 Der RH sah in der Erfassung einer Geburt durch die jeweilige Personenstandsbehörde sowie der elektronischen Übertragung der Daten an die Sozialversicherungsträger für 77 % der Personenstandsfälle das Prinzip des One–Stop–Shops grundsätzlich verwirklicht. Er merkte jedoch kritisch an, dass ein definierter Verwaltungsprozess nicht allen Bürgern

gleichermaßen zur Verfügung stand. Der RH empfahl daher dem Hauptverband, zur vollständigen Umsetzung des One–Stop–Shops von Personenstandsbehörden und Sozialversicherungsträgern die Übernahme der Daten aus dem ZPR der Personenstandsbehörden in die ZPV des Hauptverbands zeitnah umzusetzen.

5.3 *Laut Stellungnahme des BMASK sei die Umsetzung der Datenübernahme aus dem Zentralen Personenstandsregister ZPR durch die Sozialversicherungsträger zwar wünschenswert, die Operativsetzung des ZPR jedoch nach Informationen des BMASK verzögert und nunmehr erst für den 1. November 2014 vorgesehen.*

Laut Stellungnahme des Hauptverbands könnte mit der Umsetzung des ZPR ein wesentlicher Teil der Arbeiten für die zusätzliche Erfassung von Daten beim jeweiligen Sozialversicherungsträger entfallen, allerdings werde dies erst bei tatsächlich vollständiger Anwendbarkeit des ZPR der Fall sein. Solange nicht alle Personendatensätze im ZPR vorhanden seien, sei eine vollständige Nutzung des ZPR nicht möglich. Nach Informationen des Hauptverbands werde dies – wegen der notwendigen Rückerfassungsarbeiten – noch Jahre dauern.

5.4 Der RH entgegnete dem Hauptverband, dass technische Vorbereitungen seinerseits unabhängig von einer verspäteten Umsetzung des ZPR möglich seien. Er verblieb daher bei seiner Empfehlung.

Konsistenz der Daten

6.1 Unter Datenkonsistenz versteht der RH die Widerspruchsfreiheit der Datenbestände eines Registers gegenüber anderen mit gleichartigen Datenfeldern. Ein Datenabgleich der Register der Sozialversicherung mit anderen staatlichen Registern war grundsätzlich nicht vorgesehen. Ein Abgleich der Daten der ZPV des Hauptverbands bezüglich der Namensschreibweise natürlicher Personen mit dem Zentralen Melderegister (ZMR) und den Registern der Personenstandsbehörden war nicht vorgesehen. Fallweise lagen der Sozialversicherung Dokumente vor, die den aktuellen Einträgen in den anderen Registern widersprachen.

6.2 Der RH hatte in seinem Bericht zur Verwaltungsreforminitiative Register der Bundesverwaltung (Reihe Bund 2012/5, TZ 5) einen Paradigmenwechsel von der isolierten Sicht einzelner Register zu einer nutzenstiftenden Gesamtschau der unterschiedlichen Datensammlungen als notwendig erachtet. Er hatte kritisiert, dass bei abweichender Datenlage kein Abgleich mit der jeweilige Einrichtung durchgeführt wurde.

Der RH empfahl daher dem Hauptverband, bei voneinander abweichender Datenlage Datenkonsistenz herzustellen, indem die zuständigen Einrichtungen, wie Meldebehörde oder Personenstandsbehörde, über den erhobenen Sachverhalt informiert werden.

6.3 *Laut Stellungnahme des BMASK werde die Bedeutung konsistenter Datenlagen erkannt. Das BMASK wies jedoch darauf hin, dass weder dem Ressort noch dem Hauptverband eine entsprechende Kompetenz zur Herbeiführung einer solchen Vereinheitlichung zukomme.*

6.4 Der RH entgegnete dem BMASK, dass bei abweichender Datenlage ein gemeinsames Vorgehen der jeweiligen Einrichtungen den Abgleich der Daten ermöglichen würde. Er verblieb daher bei seiner Empfehlung.

Nutzung von „Führenden Registern“

7.1 Führende Register sind jene, deren Datenqualität als besonders gesichert anzusehen ist, bspw. das ZMR hinsichtlich des Namens oder das Unternehmensregister–Verwaltung hinsichtlich der Unternehmen, Vereine und sonstigen Betroffenen[1] aufgrund der eingehenden Prüfung der erfassten Dokumente und Daten.

Der Hauptverband benötigte für die „Zentrale Partnerverwaltung“ u.a. die Daten zu Unternehmen, Vereinen und sonstigen Betroffenen. Die Daten zu Unternehmen und Vereinen bezog der Hauptverband von einem externen Dienstleister. Der Grund für die Beauftragung eines externen Dienstleisters lag nach Aussage des Hauptverbands an den Anforderungen der Sozialversicherungsträger. Diese benötigten spezielle Suchfunktionen, die vom Firmenbuch (BMJ) und vom Vereinsregister (BMI) zum Zeitpunkt der Implementierung nicht zur Verfügung gestellt wurden. Für die Bereitstellung der Daten wurden an externe Dienstleister im Geschäftsjahr 2012 pauschal 45.000 EUR bezahlt.

Die Statistik Austria führte im Unternehmensregister–Verwaltung (siehe RH–Bericht Reihe Bund 2012/5) alle Unternehmen, Vereine und sonstigen Betroffenen. Auf Anfrage des RH teilte die Statistik Austria mit, dass die vom Hauptverband benötigten Daten durch das Unternehmensregister–Verwaltung bereitgestellt werden könnten. Ebenso wären die durch die Sozialversicherungsträger geforderten Suchfunktionen umsetzbar.

[1] nicht natürliche Personen, die weder im Firmenbuch noch im Vereinsregister erfasst waren (Einzelpersonengesellschaften)

Der Hauptverband und die Statistik Austria führten Gespräche, die eine Übernahme der Daten aus dem Unternehmensregister–Verwaltung in die ZPV zum Ziel hatten. Während der Gebarungsüberprüfung wurden vom Hauptverband bereits die Kennziffer des Unternehmensregisters (KUR) und die Klassifizierung nach Wirtschaftszweigen (OENACE) aus dem Unternehmensregister–Verwaltung übernommen.

7.2 Der RH wies darauf hin, dass die Übernahme der Daten zu Unternehmen, Vereinen und sonstigen Betroffenen aus dem Unternehmensregister–Verwaltung der Strategie des Bundes, „führende Register" zu nutzen, entspräche. Der RH kritisierte, dass eine Übernahme der Daten aus dem Unternehmensregister–Verwaltung noch nicht erfolgt war. Er empfahl dem Hauptverband, die Daten zu Unternehmen, Vereinen und sonstigen Betroffenen aus dem Unternehmensregister–Verwaltung in die ZPV zu übernehmen. Bei Umsetzung der Empfehlung des RH würde der Hauptverband jährlich 45.000 EUR an den externen Dienstleister einsparen.

Datenabgleich mittels Personenkennzeichens

8.1 Die Umsetzung zentraler Register und der elektronische Datenaustausch über staatliche Tätigkeitsbereiche hinweg verlangten nach einer insgesamt höheren Sicherheit der gespeicherten Daten und einem sicheren elektronischen Datenaustausch. Dazu wurde vom Gesetzgeber das E–GovG beschlossen. Um den entsprechenden datenschutzrechtlichen Grundlagen gerecht zu werden, sollen für natürliche Personen keine einheitlich flächendeckend geltenden Personenkennzeichen[2] (Identifikatoren) verwendet werden. Um Daten in gesetzlich geregelten Situationen zu einer natürlichen Person aus verschiedenen Tätigkeitsbereichen zusammenführen zu können, wurde das bereichsspezifische Personenkennzeichen (bPK) geschaffen.

Die Verwendung der Versicherungsnummer zum Datenaustausch mit anderen Tätigkeitsbereichen als dem Sozialversicherungs–Bereich war historisch begründet, weil vor der Einführung des bPK zumeist die Versicherungsnummer als eindeutiger Identifikator verwendet wurde. Damit war die Verankerung der Versicherungsnummer in den Materiengesetzen begründet.

Trotz der Einführung des bPK–Systems im Jahr 2004 wurden vom Hauptverband jedoch weiterhin Schnittstellen betrieben, die einen Datenaustausch mit anderen Tätigkeitsbereichen mittels Versicherungsnummer bewerkstelligten.

[2] Als Personenkennzeichen bzw. eindeutiger Identifikator wird im Sozialversicherungsbereich die Versicherungsnummer verwendet.

Von der Datenschutzkommission wurde in einer Stellungnahme an den RH die Verwendung der Sozialversicherungsnummer als genereller Identifikator in Zusammenhängen, die mit sozialversicherungsrechtlichen Sachverhalten nichts zu tun haben, als unzulässig bezeichnet, es sei denn, es gebe eine gesetzliche Ermächtigung. Zum Zweck der Sicherung der Geheimhaltungsinteressen der Betroffenen hätte eine Verschlüsselung der Versicherungsnummer – bei Übertragung über den Tätigkeitsbereich der Sozialversicherung hinaus zu erfolgen.

8.2 Der RH bewertete die Verwendung der Versicherungsnummer als eindeutigen Identifikator bei der Übertragung von personenbezogenen Daten als nicht ausreichenden Schutz vor der Zuordnung durch Unbefugte. Er empfahl dem Hauptverband, für den Datenaustausch mit anderen Tätigkeitsbereichen, die keine gesetzliche Ermächtigung zur Übertragung der Versicherungsnummer hatten, zukünftig die Verwendung des bPK vorzusehen. Der RH empfahl dem Hauptverband weiters, die Versicherungsnummer – falls unumgänglich – über den Tätigkeitsbereich der Sozialversicherung hinaus nur noch verschlüsselt zu übertragen.

8.3 *Laut Stellungnahme des BMASK stimme dieses vollinhaltlich zu, dass die Verwendung der Sozialversicherungsnummer zur Personenidentifikation grundsätzlich nicht wünschenswert sei. Nach Meinung des BMASK dürfte eine derartige Vorgangsweise auch der österreichischen E–Government Strategie widersprechen und sollte daher möglichst vermieden werden. Anzustreben sei vielmehr eine durchgehende Verwendung des bereichsspezifischen Personenkennzeichens (bPK), wobei hier allerdings insbesondere der jeweilige Materiengesetzgeber aufgerufen sei, eine Änderung der entsprechenden Rechtslage herbeizuführen.*

Laut Stellungnahme des Hauptverbands hätte dieser keine Rechtsgrundlage dafür, andere Stellen zu veranlassen, das bPK–Konzept umzusetzen, weil der Datenaustausch öffentlicher Stellen zu wesentlichen Teilen auf den Regeln für Amtshilfe beruhe. Der Hauptverband sei jedenfalls dazu bereit, das bPK–Konzept umzusetzen und habe dies in Zusammenarbeit mit der Statistik Austria für die Vollziehung der Volkszählungsregeln (Registerzählung) bereits erfolgreich bewiesen. Daher liege es nicht am Hauptverband, wenn andere Stellen dieses Konzept nicht benützen, abgesehen davon, dass der Gesetzgeber selbst in manchen Gesetzen ausdrücklich die Sozialversicherungsnummer als eindeutigen Identifikator vorsieht.

Schnittstellen

9.1 Der Hauptverband hatte in der ZPV natürliche Personen mit dem bPK ausgestattet. Die vom Hauptverband betriebenen Schnittstellen, die zur Datenübertragung über den Tätigkeitsbereich der Sozialversicherung hinaus genutzt wurden, unterstützten bis auf die Schnittstelle zur Statistik Austria nicht den Datenaustausch mittels bPK. Somit war eine kurzfristige Umstellung von der Versicherungsnummer auf das bPK seitens des Hauptverbands technisch nicht möglich.

9.2 Der RH empfahl dem Hauptverband, alle Schnittstellen des Hauptverbands zu anderen Tätigkeitsbereichen bei anstehenden Weiterentwicklungen mit der Möglichkeit zur Nutzung des bPK auszustatten.

9.3 *Laut Stellungnahme des BMASK stimme dieses der Empfehlung des RH vollinhaltlich zu.*

Laut Stellungnahme des Hauptverbands werte dieser die mehrfachen Verweise des RH auf das bereichsspezifische Personenkennzeichen (bPK) positiv und sei auch bereit, diese Personenkennzeichen umfassend zu verwenden. Das sei allerdings nur dann möglich, wenn auch die anderen betroffenen Stellen das bPK–Konzept umsetzen würden, was nach den praktischen Erfahrungen des Hauptverbands noch bei Weitem nicht bei allen Dienststellen (des Bundes, der Länder, Gemeinden und anderer öffentlich–rechtlichen Körperschaften) der Fall sei.

9.4 Der RH verwies auf die vom Hauptverband betriebenen Schnittstellen, die bis auf die Schnittstelle zur Statistik Austria nicht den Datenaustausch durch bPK unterstützten. Der RH verblieb daher bei seiner Empfehlung.

Sozialbetrug durch Scheinfirmen

Früherkennung von Scheinfirmen

10.1 Das BMASK, der Hauptverband, das BMF, das BMJ und das BMI beschäftigten sich in interministeriellen Arbeitsgruppen mit Möglichkeiten, wie systematischer Sozialbetrug – besonders jener mittels Scheinfirmen – unter anderem durch die Nutzung von Daten aus den Registern der Sozialversicherung und der Verknüpfung mit anderen Registern der öffentlichen Verwaltung erkannt und verhindert werden könnte.

Nach Schätzung des BMF wurden rd. 300 derartige Scheinfirmen pro Jahr gegründet, wodurch es zu einem potenziellen Schaden durch Abgaben– und Beitragsausfälle von rd. 300 Mio. EUR[3] kam.

[3] Lohnabgaben (z.B. Beiträge an die Gebietskrankenkassen), teilweise auch Umsatzsteuerausfälle

Das BMASK beauftragte im Februar 2010 ein Forschungsprojekt[4] „Sozialbetrug, auch im Zusammenhang mit Lohn– und Sozialdumping“, um Sachverhalte und Problemlagen zu typisieren, woraus Lösungsansätze zur Vermeidung von Abgabenhinterziehung bzw. zur erfolgreichen Rechtsverfolgung zu erarbeiten waren. Im März 2012 wurde hiezu ein Endbericht vorgelegt.

Das Forschungsprojekt zeigte unter anderem, dass sich speziell im Bau– und Baunebengewerbe in den letzten Jahren eine spezielle Form der organisierten Abgaben–[5] und Steuerhinterziehung mittels Scheinfirmen etabliert hatte. Dabei wurden Firmen gegründet, die zwar formal als Gesellschaft im Firmenbuch existierten, jedoch keinerlei Vermögenswerte aufwiesen. Die Studie führte aus, dass solche Scheinfirmen bspw. hunderte Dienstnehmer innerhalb weniger Wochen bei der Sozialversicherung angemeldet hatten, aber letztendlich keine Lohnnebenkosten abgeführt wurden. Musste in der Folge über eine derartige Firma ein Konkursverfahren eingeleitet werden, konnten die offenen Forderungen der Sozialversicherung bzw. Finanz (wie auch jene der sonstigen Gläubiger) nicht bedient werden, weil keine Eigenwerte vorhanden waren. Die Dienstnehmer derartiger Scheinfirmen waren bei Kontrollen der Baustellen ordnungsgemäß angemeldet bzw. sozialversichert und konnten im Bedarfsfall auch alle Leistungen der Sozialversicherung[6] in Anspruch nehmen, obwohl Lohnnebenkosten nicht abgeführt wurden.

Im Endbericht des Forschungsprojekts wurden neben Vorschlägen zur Verschärfung von Rechtsnormen auch organisatorische Empfehlungen formuliert. Dabei wurde die Früherkennung von Betrug und Missbrauch bei Scheinfirmen als essenziell dargestellt und unter anderem empfohlen, Softwarelösungen auszuarbeiten, die mittels verschiedener Indikatoren die Einrichtung einer Scheinfirma möglichst frühzeitig erkennen lassen. Eine Gebietskrankenkasse beschäftigte sich aktuell mit einer derartigen automationsunterstützten Methodik, mit deren Hilfe anhand auffälliger Muster bei festgelegten Merkmalen[7] verdächtige Firmen detektiert werden konnten. Bei anderen Sozialversicherungsträgern kamen derartige Methoden hingegen noch nicht zum Einsatz.

[4] Endbericht der Rechtswissenschaftlichen Fakultät der Universität Wien (Univ.–Prof. Dr. Susanne Reindl–Krauskopf, Univ.–Prof. Dr. Sabine Kirchmayr–Schliesselberger, Ao. Univ.–Prof. Mag. Dr. Michaela Windisch–Graetz, Mag. Martin Meissnitzer): „Sozialbetrug, auch im Zusammenhang mit Lohn– und Sozialdumping“

[5] Kranken–, Unfall–, Pensionsversicherungs–, Arbeitslosenversicherungsbeiträge, Zuschläge an die Bauarbeiter–Urlaubs– u. Abfertigungskasse (BUAK)

[6] Leistungen der Kranken–, Unfall–, Pensions– und Arbeitslosenversicherung

[7] bspw. Firmenname, Firmensitz, Anzahl der Dienstnehmer, Branche, Meldemoral, Beitragsrückstand

10.2 Der RH erachtete die Früherkennung von geplantem Sozialbetrug mittels Scheinfirmen als essenziell zur Reduktion des Einnahmenentgangs für die öffentliche Hand. Er wies kritisch darauf hin, dass bisher keine weitergehenden Initiativen gesetzt wurden. Er empfahl daher dem Hauptverband, gemeinsam mit dem BMASK mögliche Indikatoren bezüglich Aktivierung einer Scheinfirma zu definieren und die Register der Sozialversicherung auf diese – unter Beachtung des Datenschutzes und der rechtlichen Rahmenbedingungen – automationsunterstützt auszuwerten.

10.3 *Laut Stellungnahme des BMASK werde eine Arbeitsgruppe mit den Sozialpartnern und dem Hauptverband eingerichtet, die sich mit dem Sozialbetrug durch Scheinfirmen bzw. mit der Früherkennung von Scheinfirmen befassen werde. Die Arbeitsgruppe solle auch die Empfehlungen des RH diskutieren. Das BMASK verwies weiters auf das Arbeitsprogramm der Österreichischen Bundesregierung 2013 – 2018, wo im Kapitel 01 Wachstum und Beschäftigung in Österreich unter anderem auch Maßnahmen gegen Scheinanmeldungen angeführt seien.*

11.1 Aus dem Endbericht zum Forschungsprojekt ging hervor, dass die Anwendung einer automationsunterstützten Auswertung von Indikatoren zur Erkennung von Sozialbetrug wesentlich von den zur Verfügung stehenden Dateninhalten und deren Datenaktualität abhängt. Es zeigte sich, dass nicht alle hiefür notwendigen Daten erfasst bzw. rechtzeitig erfasst wurden.

So wurde bspw. um einen besseren Überblick hinsichtlich neu beginnender Baustellen zu gewinnen und so die Baustellenkontrollen für die Betrugsbekämpfung zu erleichtern, im Juli 2011 eine Novelle zum Bauarbeiter–Urlaubs– und Abfertigungsgesetz mit dem Ziel verabschiedet, eine Baustellendatenbank durch die Urlaubs– und Abfertigungskasse einzurichten.

Arbeitgeber waren verpflichtet, für Baustellen, deren Dauer fünf Arbeitstage überschritt, Angaben zur Lage der Baustelle, zum Zeitpunkt des Arbeitsbeginns, zu Art und Umfang der Arbeiten, zur voraussichtlichen Anzahl der Beschäftigten und den Namen der vorgesehenen Aufsichtsperson zu melden. Daten zu den ausführenden Dienstnehmern, wie bspw. Name und Versicherungsnummer, waren nicht zu melden bzw. zu erfassen. Im Endbericht des erwähnten Forschungsprojekts findet sich hiezu der Hinweis, dass auch die Erfassung der aktuell tätigen Dienstnehmer in der Baustellendatenbank zu prüfen wäre, um die Früherkennung von Scheinfirmen zu verbessern.

11.2 Der RH beanstandete die unvollständige und nicht rechtzeitige Erfassung von Indikatoren geplanten Sozialbetrugs. Er empfahl dem Hauptverband, gemeinsam mit dem BMASK jene von Experten zur Früherkennung geplanten Sozialbetrugs (Scheinfirma) definierten Indikatoren (Daten) zeitgerecht in die Register einzutragen. Notwendigenfalls wäre ein diesbezüglicher Gesetzesvorschlag an den Gesetzgeber heranzutragen.

Cyber Sicherheit

Allgemeines

12.1 Für den Begriff Cyber Sicherheit besteht keine gesetzliche Definition. Nachfolgend wird die in der Bundesverwaltung gängige Beschreibung „Cyber Sicherheit ist die Summe aller Maßnahmen, die Bedrohungen, Angriffe und Schädigungen aus modernen Netzwerken und Onlinediensten verhindern sollen“ übernommen.

Die Österreichische Bundesregierung verfolgte das Ziel, die Cyber Sicherheit in Österreich zu heben. Dazu beschloss der Ministerrat im März 2008 das „Programm zum Schutz kritischer Infrastruktur“. In diesem wurde die „Aufrechterhaltung des Sozialsystems und der Verteilungssysteme als kritische Infrastruktur[8] angeführt und somit die wesentliche Bedeutung für die Aufrechterhaltung der gesellschaftlichen Funktionen hervorgehoben. Politik und Verwaltung sind für die Gestaltung der Rahmenbedingungen verantwortlich, damit ein klar definiertes Schutzniveau erreicht wird.“

Im Mai 2012 beschloss der Ministerrat zudem ein „Cyber Security Gesamtkonzept“ und im März 2013 ein umfassendes und proaktives Konzept „Österreichische Strategie für Cyber Sicherheit“. Ziel war die Einbindung strategisch relevanter Betreiber von kritischer Infrastruktur zur Gewährleistung der Cyber Sicherheit unter breiter Einbindung von Experten aus Verwaltung, Wissenschaft und Wirtschaft.

Ein auf den Ministerratsbeschlüssen basierendes Konzept zur Aufrechterhaltung der kritischen Infrastruktur und der Verteilungssysteme sowie ein Cyber Sicherheitskonzept für die Sozialversicherung waren nicht vorhanden.

[8] Die Störung oder Zerstörung kritischer Infrastruktur hat schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche soziale Wohl der Bevölkerung oder die effektive Funktionsweise staatlicher Einrichtungen.

12.2 Der RH stimmte der Einschätzung, die Aufrechterhaltung des Sozialsystems und der Verteilungssysteme als kritische Infrastruktur anzusehen, zu. Er bemerkte jedoch kritisch, dass der Hauptverband im Bereich der Sozialversicherung keine zentralen Strukturen und umfassenden Maßnahmen zur Erreichung eines definierten Schutzniveaus hinsichtlich des Bereichs Cyber Sicherheit setzte. Er empfahl daher dem Hauptverband, gemeinsam mit dem BMASK zur Abwehr und Bewältigung von Cyber Sicherheitsvorfällen eine umfassende Cyber Sicherheitsstrategie für den Sozialversicherungsbereich zu erarbeiten und umzusetzen.

12.3 *Laut Stellungnahme des BMASK würden umgehend Gespräche mit dem Hauptverband aufgenommen, um gemeinsam geeignete Maßnahmen zur Umsetzung einer Cyber–Sicherheitsstrategie zu prüfen und zu entwickeln.*

Laut Stellungnahme des Hauptverbands würden die Ausführungen zur Cyber Security berücksichtigt und als wertvoller Auftrag zur Weiterarbeit an diesem Thema betrachtet.

Cyber Sicherheit in der Sozialversicherung

13.1 Im Bereich der Sozialversicherung wurden Teilaspekte der Cyber Sicherheit in Arbeitsgruppen behandelt. Eine verpflichtende Teilnahme bzw. Übernahme von Sicherheitsstandards durch die Sozialversicherungsträger bestand nicht.

Institutionalisierte Strukturen der Cyber Sicherheit, wie die Einsetzung von Steuerungsgruppen und die Einsetzung eines Computer Emergency Response Teams sowie die Risikobeurteilung, die Vorgabe von Mindestsicherheitsstandards, das Umsetzen von Krisenmanagement und Kontinuitätsplänen unter Einbindung externer Experten etc. waren nicht vorhanden. Ein Handbuch zur IT–Sicherheit lag vor, war aber von der Trägerkonferenz noch nicht beschlossen worden.

Ziel des Datenschutzgesetzes 2000 (DSG 2000) war der Schutz personenbezogener Daten sowie die Datensicherheit. Die Datenschutzverordnung (SV–DSV) für die gesetzliche Sozialversicherung bezog sich auf das DSG 2000 und enthielt auch Vorgaben zu Datensicherheitsmaßnahmen. Maßnahmen im Rahmen der Cyber Sicherheit unterstützten zwar auch diese gesetzlichen Vorgaben des DSG 2000, der Fokus der Cyber Sicherheit sollte aber auf dem Erhalt der Funktionalität der Systeme und der Abwehr von Angriffen liegen.

Eine gesetzliche Regelung zur Umsetzung einer Gesamtstrategie zur Cyber Sicherheit in der Sozialversicherung bestand nicht.

13.2 Der RH kritisierte die fehlende Gesamtstrategie zur Cyber Sicherheit, weil eine solche zur Bewältigung kritischer Vorfälle im IT–Bereich der Sozialversicherung unverzichtbar ist. Außerdem kritisierte er, dass das BMASK bisher keine diesbezügliche gesetzliche Regelung angeregt hatte. Er empfahl daher dem BMASK, eine gesetzliche Regelung zur zentralen Umsetzung einer Cyber Sicherheitsstrategie in der Sozialversicherung an den Gesetzgeber heranzutragen.

Maßnahmen zur Cyber Sicherheit

14.1 Cyber Sicherheit bestand aus IT–Bereichen, die unter anderem

- sich allgemein mit Computersicherheit beschäftigten,
- kritische Infrastruktur definierten,
- IT–Sicherheitsrisiken dokumentieren,
- IT–Sicherheitsrisiken abschätzten,
- Bedrohungsszenarien entwarfen,
- präventive Maßnahmen erarbeiteten,
- Lösungen für konkrete Vorfälle erarbeiteten,
- im Anlassfall Vorortunterstützung anboten,
- als Koordinatoren bei Vorfällen mitwirkten,
- Warnungen vor Sicherheitslücken herausgaben,
- im CERT–Verbund Informationen austauschten,
- Sicherheits– und Schutzstandards entwarfen,
- Kontinuitätspläne entwickelten,
- Kommunikationsstrategien für den Ernstfall entwarfen und
- Schulungen veranstalteten.

In der Sozialversicherung befassten sich unterschiedliche Arbeitsgruppen mit einzelnen Aspekten der Cyber Sicherheit. Die Sozialversicherungsträger wirkten in verschiedenen Arbeitsgruppen mit, aber nicht alle Sozialversicherungsträger in allen Arbeitsgruppen. Die Arbeits-

gruppen konnten zwar nicht von Einzelnen blockiert werden, die Ergebnisse waren aber auch nicht zwingend umzusetzen. Eine Gesamtstrategie zur Cyber Sicherheit war nicht vorhanden.

14.2 Der RH stellte kritisch fest, dass eine Gesamtstrategie zur Cyber Sicherheit in der Sozialversicherung fehlte. Er empfahl dem Hauptverband, die Inhalte der Cyber Sicherheit nach Priorität gereiht aufzuarbeiten und verbindlich umzusetzen.

Computer Emergency Response Team (CERT) in der Sozialversicherung

15.1 Das BKA installierte und finanzierte das sogenannte Government Computer Emergency Response Team (GovCERT). Dieses beschäftigte sich mit dem operativen Bereich der Sicherheit von Computersystemen und des Internets sowie dem Schutz von kritischer Infrastruktur für den staatlichen Bereich. Es diente als Anlaufstelle in Fragen der IT–Sicherheit sowie für präventive und reaktive Maßnahmen im Bereich der öffentlichen Verwaltung.

Der Hauptverband war Partner des GovCERT und beteiligte sich an Arbeitsgruppen. Innerhalb der Sozialversicherung beschäftigten sich Arbeitsgruppen mit Aspekten der Cyber Sicherheit. IT–Sicherheitsfachleute, welche die Aufgaben eines Sozialversicherungs CERT als Kernaufgabe für die Sozialversicherung wahrgenommen hätten, gab es nicht.

15.2 Der RH wies kritisch darauf hin, dass bisher keine operative IT–Sicherheitsgruppe, die sich mit der Cyber Sicherheit in der Sozialversicherung zu beschäftigen hätte, eingerichtet war. Er empfahl dem Hauptverband, zur operativen Bearbeitung der Cyber Sicherheitsbereiche in der Sozialversicherung ein Sozialversicherungs CERT (SV–CERT) einzurichten. Dieses wäre im Rahmen der Zielsteuerung als verbindliche Struktur zu definieren und in Abstimmung mit dem BMASK der Trägerkonferenz zur Beschlussfassung vorzulegen, um den Schutz der kritischen Infrastruktur zu verbessern.

Krisenmanagement und Kontinuitätspläne

16.1 Der Ministerratsvortrag vom Mai 2012 „Cyber Security Gesamtkonzept“ befasste sich mit einer „Österreichischen Strategie zur Cyber–Sicherheit“. Ziel war die Erstellung einer Cyber Sicherheits–Risikoanalyse der verschiedenen Sektoren der kritischen Infrastruktur unter breiter Einbindung von Experten aus Verwaltung, Wissenschaft und Wirtschaft.

Im Rahmen eines Risikomanagements waren die möglichen Krisenfälle zu analysieren, bewerten, überwachen und Kontinuitätspläne zu entwickeln. Kontinuitätspläne beinhalteten die Entwicklung von Strategien, welche die Tätigkeiten und Prozesse einer kritischen Infrastruktur im Falle einer Unterbrechung vor ernsthaften Schäden schützen sollten und alternative Abläufe ermöglichten. Aufbauend auf den Ergebnissen waren Strategien und Prozesse zur Bewältigung der Krisenfälle zu entwerfen und Krisenübungen durchzuführen.

Laut Aussage des Hauptverbands bestanden spezifische Kontinuitätspläne von Sozialversicherungsträgern, der IT–Services der Sozialversicherung GmbH (IT–SV GmbH) und der Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. – SVC sowie der Allgemeinen Unfallversicherungsanstalt. Ein die Sozialversicherung übergreifendes Krisenmanagement und Kontinuitätspläne waren jedoch nicht vorhanden.

Die IT–SV GmbH hatte ein aktives Betriebskontinuitätsmanagement mit jährlichen Übungen geschaffen. Nach Meinung des Hauptverbands könnte dieses zu einem übergreifenden Cyber Sicherheit–Krisenmanagement ausgebaut werden.

16.2 Der RH bemerkte kritisch, dass ein zentrales Krisenmanagement und zentrales Kontinuitätsmanagement zur Bewältigung etwaiger Angriffe auf die IT–Infrastruktur der Sozialversicherung fehlte. Er empfahl dem Hauptverband, ein für die Sozialversicherung übergreifendes Krisenmanagement einzurichten. Dieses hätte die Risikoanalysen zu erstellen, Kontinuitätspläne zu entwickeln und Krisenübungen durchzuführen.

Sicherungs– und Schutzstandards

17.1 Die zentralen Dienstleister der Sozialversicherung (IT–Services der Sozialversicherung GmbH, Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. – SVC) hatten definierte Schutzstandards. Trotz der Maßnahmen dieser zentralen IT–Dienstleister bestand auch aus Sicht des Hauptverbands „aufgrund der vorhandenen Schnittstellen zu den dezentralen, sicherheitstechnisch nicht harmonisierten Bereichen ein nicht zu unterschätzendes und nicht einschätzbares Risikopotential“.

Zentral koordinierte und einheitliche Schutz– und Sicherheitsstandards der Einrichtungen der Sozialversicherung waren nicht vorhanden. Nicht ausreichend IT–technisch gesicherte Einrichtungen in der Sozialversicherung konnten aufgrund nicht erhobener Daten durch den Hauptverband nicht erkannt werden.

17.2 Der RH merkte kritisch an, dass in den nicht einheitlichen Sicherungs– und Schutzstandards der Sozialversicherung ein erhöhtes Risiko bestand. Er empfahl dem Hauptverband, Sicherungs– und Schutzstandards für die Einrichtungen der Sozialversicherung vorzusehen, dem jeweiligen Aufgabengebiet und den verwendeten Daten anzupassen und deren verbindliche Kontrolle einzurichten.

Meldepflicht bei kritischen Vorfällen

18.1 Angriffe auf Systeme der Sozialversicherung, erfolgte Schädigungen sowie erfolgreiche unbefugte Zugriffe wurden nicht zwingend an einen zentralen Dienstleister kommuniziert. An den Hauptverband gemeldete Cyber Sicherheitsvorfälle wurden nicht anhand definierter Strukturen und Prozesse an alle potenziell gefährdeten Einrichtungen der Sozialversicherung gemeldet.

18.2 Der RH hob kritisch hervor, dass Cyber Sicherheitsvorfälle nicht zwingend zu dokumentieren und weiterzuleiten waren und somit entsprechende Maßnahmen nicht immer erarbeitet werden konnten. Er empfahl dem Hauptverband, eine Meldepflicht bei Cyber Sicherheitsvorfällen für alle Einrichtungen der Sozialversicherung verbindlich vorzusehen. Die Bewertung bzw. Einstufung des jeweiligen IT–Sicherheitsvorfalls sollte den zuständigen Sicherheitsfachleuten des einzurichtenden SV–CERT vorbehalten sein. Anhand definierter Strukturen und Prozesse wären alle potenziell gefährdeten Einrichtungen der Sozialversicherung zu informieren und entsprechende Maßnahmen zu empfehlen.

Sensibilisierung der Mitarbeiter

19.1 Die Sensibilisierung und Bewusstseinsbildung der Mitarbeiter bildete eine zentrale Aufgabe zur Vermeidung von Risiken im Umgang mit der IT–Infrastruktur. Die IT–SV GmbH versendete zu diesem Zweck regelmäßig Awareness–Letters und übermittelte diese an alle Mitarbeiter der Sozialversicherung. Die Sozialversicherungsträger boten den Mitarbeitern Schulungen zum sicheren Umgang mit der IT–Infrastruktur an. Vorgaben für die Sozialversicherungsträger zu Inhalt, Umfang und Zeitabständen zwischen den Schulungen bestanden nicht.

19.2 Der RH anerkannte die Sensibilisierung und Bewusstseinsbildung der Mitarbeiter der Sozialversicherung mittels Awareness–Letters. Er kritisierte jedoch die fehlenden Vorgaben zu Inhalt, Umfang und Zeitabständen zwischen den Schulungen. Er empfahl dem Hauptverband, die Mitarbeiter der Sozialversicherungsträger im Umgang mit der IT–Infrastruktur weiterhin auf mögliches Fehlverhalten zu sensibilisieren und in regelmäßigen Abständen zentral koordinierte und abgestimmte Schulungsinhalte vorzusehen.

Katastrophenübungen

20.1 Bei den bisherigen Katastrophenübungen und Simulationen durch das GovCERT beschränkte sich das Aufgabengebiet zur Abwehr von Cyber Sicherheitsvorfällen auf die Bundesverwaltung. Die Besonderheiten von Bedrohungsszenarien in der Sozialversicherung wurden nicht eigens betrachtet. Der Hauptverband beauftragte eine Fachhochschule sowie Hersteller von Sicherheitsprodukten zur Überprüfung der zentralen IT–Einrichtungen der Sozialversicherung, simulierte Angriffe durchzuführen. Katastrophenübungen, die eine Beeinträchtigung weiter Teile der IT der Sozialversicherung zum Inhalt hatten, wurden nicht durchgeführt.

20.2 Der RH sah in simulierten Angriffen durch externe Beauftragte einen ersten Schritt zur Umsetzung einer Sicherheitsstrategie und deren Überprüfung. Gleichzeitig wies der RH kritisch darauf hin, dass gerade die für den Hauptverband erforderlichen Katastrophenübungen, die eine Beeinträchtigung weiter Teile der Sozialversicherung zum Inhalt hätten, jedoch nicht durchgeführt wurden. Er empfahl dem Hauptverband, IT–Sicherheitsfachleute der Sozialversicherungsträger verbindlich anhand von Katastrophenübungen zu schulen.

Getroffene Maßnahme

21 Der Hauptverband kam der Empfehlung des RH, die an die Datenschutzkommission bereits übermittelten DVR–Meldungen auf Aktualität zu überprüfen und allenfalls erforderliche Änderungen zu melden, bereits während der Überprüfung durch den RH an Ort und Stelle nach.

Schlussbemerkungen/Schlussempfehlungen

22 Zusammenfassend hob der RH folgende Empfehlungen hervor:

BMASK

(1) Es wäre eine gesetzliche Regelung zur zentralen Umsetzung einer Cyber Sicherheitsstrategie in der Sozialversicherung an den Gesetzgeber heranzutragen. (TZ 13)

Hauptverband der österreichischen Sozialversicherungsträger und BMASK

(2) Mögliche Indikatoren bezüglich Aktivierung einer Scheinfirma wären zu definieren und die Register der Sozialversicherung auf diese – unter Beachtung des Datenschutzes und der rechtlichen Rahmenbedingungen – automationsunterstützt auszuwerten. (TZ 10)

(3) Die von Experten zur Früherkennung von geplantem Sozialbetrug (Scheinfirma) definierten Indikatoren (Daten) wären zeitgerecht in die Register einzutragen. Notwendigenfalls wäre ein diesbezüglicher Gesetzesvorschlag an den Gesetzgeber heranzutragen. (TZ 11)

(4) Zur Abwehr und Bewältigung von Cyber Sicherheitsvorfällen wäre eine umfassende Cyber Sicherheitsstrategie für den Sozialversicherungsbereich zu erarbeiten und umzusetzen. (TZ 3, 12)

(5) Zur operativen Bearbeitung der Cyber Sicherheitsbereiche in der Sozialversicherung wäre ein Sozialversicherungs CERT im Rahmen der Zielsteuerung einzurichten und in Abstimmung mit dem BMASK der Trägerkonferenz zur Beschlussfassung vorzulegen. (TZ 15)

Hauptverband der österreichischen Sozialversicherungsträger

(6) Zur gemeinsamen Umsetzung des One–Stop–Shop von Personenstandsbehörden und Sozialversicherungsträgern wäre die Übernahme der Daten aus dem Zentralen Personenstandsregister der Personenstandsbehörden in die Zentrale Partnerverwaltung des Hauptverbands zeitnah umzusetzen. (TZ 5)

(7) Bei voneinander abweichender Datenlage wäre Datenkonsistenz herzustellen. Die zuständigen Einrichtungen wie Meldebehörde oder Personenstandsbehörde wären über den erhobenen Sachverhalt zu informieren. (TZ 6)

(8) Die Daten zu Unternehmen, Vereinen und sonstigen Betroffenen wären aus dem Unternehmensregister–Verwaltung in die Zentrale Partnerverwaltung zu übernehmen. (TZ 7)

(9) Für den Datenaustausch mit anderen Tätigkeitsbereichen, die keine gesetzliche Ermächtigung zur Übertragung der Versicherungsnummer hatten, wäre zukünftig die Verwendung des bereichsspezifischen Personenkennzeichens vorzusehen. (TZ 8)

(10) Die Versicherungsnummer wäre – falls unumgänglich – über den Tätigkeitsbereich der Sozialversicherung hinaus nur noch verschlüsselt zu übertragen. (TZ 8)

(11) Alle Schnittstellen des Hauptverbands zu anderen Tätigkeitsbereichen wären bei anstehenden Weiterentwicklungen mit der Möglichkeit zur Nutzung des bereichsspezifischen Personenkennzeichens auszustatten. (TZ 9)

(12) Die Inhalte der Cyber Sicherheit wären nach Priorität gereiht aufzuarbeiten und verbindlich umzusetzen. (TZ 14)

(13) Für die Sozialversicherung wäre ein Krisenmanagement einzurichten. Dieses hätte die Risikoanalysen durchzuführen, Kontinuitätspläne zu entwickeln und Krisenübungen durchzuführen. (TZ 16)

(14) Sicherungs– und Schutzstandards wären für die Einrichtungen der Sozialversicherung vorzusehen, dem jeweiligen Aufgabengebiet und den verwendeten Daten anzupassen und dessen verbindliche Kontrolle einzurichten. (TZ 3, 17)

(15) Eine Meldepflicht bei Cyber Sicherheitsvorfällen für alle Einrichtungen der Sozialversicherung wäre verbindlich vorzusehen. Die Bewertung bzw. Einstufung des jeweiligen IT–Sicherheitsvorfalls sollte den Sicherheitsfachleuten des Sozialversicherungs CERT vorbehalten sein. Anhand definierter Strukturen und Prozesse wären alle potenziell gefährdeten Einrichtungen der Sozialversicherung zu informieren und entsprechende Maßnahmen zu empfehlen. (TZ 18)

(16) Die Mitarbeiter der Sozialversicherung wären im Umgang mit der IT–Infrastruktur weiterhin auf mögliches Fehlverhalten zu sensibilisieren und in definierten Abständen zentral koordinierte und abgestimmte Schulungen vorzusehen. (TZ 19)

(17) IT–Sicherheitsfachleute der Sozialversicherungsträger wären verbindlich anhand von Katastrophenübungen zu schulen. (TZ 20)

ANHANG

Zentrale Partnerverwaltung (ZPV)

Zentrale Versicherungsdatei (ZVD)

Zugriffsprotokolle (ZUP)

Berechtigungsdatenbank (BERE)

Dokumentation des österreichischen Sozialversicherungs-rechts (SozDok)

Amtliche Verlautbarungen (AVI)

Honorarordnungsverwaltung (HONO)

Betriebliche (Mitarbeiter–)Vorsorge im Hauptverband (BMV)

Erstattungskodex Basisdatenbank (EKO–BDB)

Elektronisches Pensionskonto (ePK)

Zentraler Patientenindex (Z–PI)

Leistungsinformation für Versicherte (LIVE)

Familienbeihilfedatenbank (FB)

e–card Konsultationssystem (KONS)

Krankenversicherung – Anspruchsdatenbank (ANSP)

Zentrale Partnerverwaltung (ZPV)

(1) Allgemeines

In der zentralen Partnerverwaltung (ZPV) waren die Stammdaten aller rd. 13,3 Mio. Partner der Sozialversicherungen gespeichert. Im Jahr 2012 erfolgten rd. 2 Mrd. Zugriffe auf die ZPV.

(2) Inhalt und Aufgaben des Registers

Die ZPV diente zur Erfassung der Stammdaten aller Partner der österreichischen Sozialversicherungen. Dazu zählten die Versicherten, die Dienstgeber und die Leistungserbringer. In der ZPV wurde ein Rollenkonzept verwirklicht, das eine einmalige Anlage der Stammdaten zu einer Person erforderte und die Zuordnung einer oder mehrerer Rollen unterstützte.

(3) Zuständigkeit

Der Hauptverband hatte den gesetzlichen Auftrag, eine zentrale Anlage[9] zur Aufbewahrung und Verarbeitung der für die Versicherten bzw. den Leistungsbezug bedeutsamen Daten zu führen. Die organisatorische und technische Betriebsführung wurde von der IT–SV GmbH wahrgenommen.

(4) Kosten

Die Betriebs– und Wartungskosten der ZPV für das Jahr 2012 betrugen rd. 1,26 Mio. EUR, die Weiterentwicklungskosten rd. 1,51 Mio. EUR.

(5) Elektronische Datenübermittlung und Abfragen

Stammdaten wurden zur Zeit der Gebarungsüberprüfung von den Personenstandsbehörden elektronisch direkt an den Hauptverband gemeldet (70 %) oder von den lokalen Sozialversicherungsträgern erfasst. Mit der Umsetzung des ZPR war geplant, Änderungen bei den Stammdaten mittels Änderungsdienstes direkt von den Personenstandsbehörden im Wege des ZPR in die ZPV zu übertragen.

[9] § 31 Abs. 4 Z 3a ASVG

Abfrageberechtigt waren im Rahmen ihrer gesetzlichen Aufgaben unter anderem:

- 20.000 Benutzer in den Sozialversicherungen,
- Arbeitsmarktservice (AMS),
- BMI im Bereich Grundversorgung,
- Krankenfürsorgeanstalten,
- Pensionsversicherung,
- Gerichte über die Schnittstelle AJ,
- e–card: Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. – SVC.

Abgefragt wurden Daten im Rahmen der gesetzlichen Aufgaben unter anderem vom

- Zentralen Melderegister (ZMR),
- Vereinsregister über einen externen Dienstleister,
- Firmenbuch über einen externen Dienstleister,
- Adressregister,
- Zentralen Gewerberegister (ZG).

Zentrale Versicherungsdatei (ZVD)

(1) Allgemeines

In der „Zentralen Versicherungsdatei (ZVD)“ waren alle erforderlichen Versicherungsdaten abgelegt.

(2) Inhalt und Aufgaben des Registers

Die ZVD umfasste Angaben[10] zu den Versicherungszeiten sowie Sozialversicherungs–Beitragsgrundlagen (bis zur Höchstbeitragsgrundlage) aller Personen in der Pensions–, Kranken–, Unfall– und/oder Arbeitslosenversicherung unter anderem nach dem

- ASVG (unselbständige Beschäftigung als Arbeiter bzw. Angestellter),
- GSVG (selbständige Erwerbstätigkeit),
- BSVG (Erwerbstätigkeit in der Land– und Forstwirtschaft) und dem
- B–KUVG (Beamte bzw. Bezieher eines Ruhe– oder Versorgungsgenusses).

In der ZVD waren im April 2013

- rd. 92 Mio. Versicherungsverhältnisse,
- rd. 208 Mio. Versicherungszeiten und
- rd. 249 Mio. Beitragsgrundlagen

gespeichert.

Im Jahr 2012 wurden in der ZVD rd. 93 Mio. Änderungen bzw. Eingaben sowie rd. 50 Mio. Abfragen[11] durchgeführt.

[10] Daten ab dem Jahr 1920 sind erfasst

[11] automatische Verständigungen nicht enthalten

(3) Zuständigkeit

Dem Hauptverband der österreichischen Sozialversicherungsträger oblag unter anderem die zentrale Erbringung von Dienstleistungen für die Sozialversicherungsträger[12] sowie die Errichtung und Führung einer zentralen Anlage zur Aufbewahrung und Verarbeitung der für die Versicherung bedeutsamen Daten aller versicherten Personen sowie Leistungsbezieher auf automatisationsunterstütztem Weg (ZVD). Die Dateneinbringung erfolgte durch die einzelnen Sozialversicherungsträger, das AMS und die Krankenfürsorgeanstalten, die auch für die jeweiligen Inhalte verantwortlich waren. Betrieben wurde die ZVD von der IT–SV GmbH.

(4) Kosten

Die Betriebs– und Wartungskosten der ZVD für das Jahr 2012 betrugen rd. 2 Mio. EUR.

(5) Elektronische Datenübermittlung und Abfragen

Die Daten der ZVD standen auch anderen Einrichtungen außerhalb des Sozialversicherungsbereichs zur Verfügung. Auskünfte wurden an Justiz– und Verwaltungsbehörden erteilt, Daten an das BMASK bzw. an die Allgemeine Unfallversicherungsanstalt weitergegeben sowie ein automatisiertes Meldeverfahren mit dem AMS durchgeführt. Weiters wurden die Daten den Landesregierungen im Zuge eines Meldeverfahrens bezugnehmend auf die Gewährung eines Krankenversicherungsschutzes für Mindestsicherungsbezieher zur Verfügung gestellt.

Für die Datenübermittlungen wurde nicht das bPK, sondern die Sozialversicherungsnummer bereichsübergreifend als eindeutiger Identifikator verwendet.

(6) Zweck des Registers

Die Daten der ZVD dienten innerhalb des Sozialversicherungsbereichs (Hauptverband) unter anderem der Leistungsfeststellung (Pensionsberechnung) der Pensionsversicherungsträger und der Berechnung des Allgemeinen Pensionskontos (ePK) sowie der Feststellung des Krankenversicherungsschutzes (e–card), der Ausgabe von Versicherungs-

[12] § 31 Abs. 4 Z 3a ASVG

verläufen (Versicherungsdatenauszug) und der Berechnung der Rezeptgebührenobergrenze.

Weiters führte der Hauptverband mittels ZVD–Daten interne Berechnungsläufe[13] durch; ebenso erstellte er Statistiken und Auswertungen.

[13] Rückerstattungen, Nach– und Rückverrechnungen

Zugriffsprotokolle (ZUP)

(1) Allgemeines

Im Register Zugriffsprotokolle (ZUP) wurden alle Datenzugriffe der Online–Verarbeitungen des Hauptverbands mit Zugriffen auf personenbezogene Daten protokolliert (rd. 9 Mio. Einträge täglich). Im Jahr 2012 wurden rd. 45.000 Abfragen erfasst.

(2) Inhalt und Zweck des Registers

Die Erstellung von Zugriffsprotokollen diente zur möglichen Überprüfung der Rechtmäßigkeit der abgefragten Daten. Das DSG 2000 verlangt eine Protokollierung der Datenzugriffe zur Wahrung der Auskunftsrechte Betroffener.[14]

(3) Zuständigkeit

Die Zuständigkeit des Registers lag allein beim Hauptverband. Betrieben wurde es von der IT–SV GmbH.

(4) Kosten

Die Betriebs– und Wartungskosten der ZUP für das Jahr 2012 betrugen rd. 184.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Die Daten wurden ausschließlich innerhalb des Hauptverbands generiert und Auswertungen an die betroffenen Einrichtungen weitergeleitet.

[14] § 26 DSG 2000

Berechtigungsdatenbank (BERE)

(1) Allgemeines

Das Berechtigungssystem für Standardprodukte (BERE) verwaltet in der Datenbank die Zugriffsberechtigungen der Benutzer. Es zählt zusammen mit der ZVD, der ZPV und dem ZUP zur zentralen Versicherungsdatenspeicherung.

(2) Inhalt und Aufgaben des Registers

BERE diente zur Authentifizierung und Autorisierung von SV–Mitarbeitern und steuerte damit die Zugriffe auf Daten und Applikationen.

(3) Zuständigkeit

Der Hauptverband war verpflichtet, seine Daten gegen unberechtigte Zugriffe zu schützen, was mit dieser Applikation IT–mäßig umgesetzt wurde. Die organisatorische und technische Betriebsführung wurde von der IT–SV GmbH wahrgenommen.

(4) Kosten

Die Betriebs– und Wartungskosten der BERE für das Jahr 2012 betrugen rd. 30.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Alle Datenübermittlungen erfolgten innerhalb des Hauptverbands und steuerten interne Verarbeitungsprozesse.

Dokumentation des österreichischen Sozialversicherungsrechts (SozDok)

(1) Allgemeines

Die SozDok diente zur Dokumentation des österreichischen Sozialversicherungsrechts. Sie enthielt rd. 79.000 Textdokumente, die im Internet abrufbar waren. Gesetzestexte betreffend die Sozialversicherung waren in der SozDok und im RIS zu finden.

(2) Inhalt und Zweck des Registers

Die SozDok stellte allen mit der Materie befassten Einrichtungen aktuelle Informationen zum österreichischen Sozialversicherungsrecht zur Verfügung. Insbesondere diente sie als Zugang zum Sozialrecht auf Detailebene für alle Versicherten, Beitragszahler und Sozialrechtslegisten.

Enthalten waren sämtliche sozialversicherungsrechtlich relevanten Gesetze und Durchführungsverordnungen sowie Entscheidungen, Erlässe, Hinweise auf Gesetzesmaterialien, Protokolle und Hilfslisten. Die SozDok hatte ihren Schwerpunkt in der zeitlichen Aufbereitung der Vorschriften und der Darstellung des Durchführungsrechts. Die SozDok ergänzte die Dokumentation des RIS und die Dokumentationen der Länder.

Zwischen SozDok und RIS bestanden Überschneidungen im Bereich des Sozialversicherungsrechts. Die SozDok stellte jedoch Inhalte zur Verfügung, die im RIS nicht enthalten waren. Es handelte sich hiebei um Verordnungen, Amtliche Verlautbarungen, Arbeitsbehelfe, Weisungen und Vorschriften für die Kassen sowie speziell aufbereitetes EU–Recht. Historisch betrachtet wurde die SozDok vor dem RIS implementiert.

Die verhältnismäßig geringe Anzahl von rd. 1.400 Abfragen jährlich war einerseits darin begründet, dass es sich um eine sehr spezifische Sachmaterie handelte, andererseits konnten Abfragen zum Sozialversicherungsrecht über das RIS erfolgen. Über die Anzahl der RIS–Abfragen zum Sozialversicherungsrecht wurden keine Aufzeichnungen geführt.

(3) Zuständigkeit

Der Hauptverband hatte eine zentrale Dienstleistung zu erbringen,[15] die den Aufbau und die Führung einer Dokumentation des österreichischen Sozialversicherungsrechts im übertragenen Wirkungsbereich nach den Weisungen des BMASK umfasste. Die organisatorische und technische Betriebsführung wurde von der IT–SV GmbH wahrgenommen.

(4) Kosten

Die SozDok wurde jeweils zur Hälfte vom Hauptverband und vom BMASK finanziert. Die Betriebs– und Wartungskosten der SozDok für das Jahr 2012 betrugen rd. 168.000 EUR. Der Anteil des Hauptverbands betrug 84.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Die SozDok wurde inhaltlich vom Hauptverband geführt. Alle Datenübermittlungen aus der SozDok erfolgten im Wege von Online–Abfragen unter www.sozdok.at und im Behördenintranet über http://sozdok.sozvers.at.

[15] § 31 Abs. 4 Z 4 ASVG

Amtliche Verlautbarungen (AVI)

(1) Allgemeines

Das Register „Amtliche Verlautbarungen – AVI“ befand sich seit 2002 in Betrieb und wurde von allen Versicherungsträgern genutzt. Mitte 2010 wurde mit der Rückerfassung von Verlautbarungen und Verträgen begonnen. Das Register enthielt rd. 2.700 Dokumente.

(2) Inhalt und Zweck des Registers

Das Register erfüllte die gesetzliche Vorgabe, wonach der Hauptverband die im Internet zu verlautbarenden Rechtsvorschriften und deren Änderungen jederzeit ohne Identitätsnachweis und gebührenfrei zugänglich zu machen hatte.[16] Alle ab 1. Jänner 2002 verlautbarten Rechtsvorschriften konnten in ihrer verlautbarten Form vollständig und auf Dauer ermittelt werden.

Im Unterschied zum RIS war das AVI auch als Vertragsdokumentation vorgesehen, weil nach dem 3. Sozialrechts–Änderungsgesetz 2009 die vertraglichen Beziehungen zwischen Sozialversicherungsträgern und Mitgliedern der Gesundheitsberufe zu verlautbaren waren. Dazu kamen noch eine Reihe weiterer Regelungen und Festsetzungen der Bundesschiedskommission, die zu veröffentlichen waren. Allfällige Änderungen und Zusatzvereinbarungen wurden laufend kundgemacht. Mit jährlich rd. 15.000 Datenzugriffen wurde das Register hauptsächlich von Sachbearbeitern genutzt.

(3) Zuständigkeit

Das Register AVI wurde vom Hauptverband aufgrund gesetzlicher Vorgaben geführt. Die organisatorische und technische Betriebsführung wurde von der IT–SV GmbH wahrgenommen.

(4) Kosten

Die Betriebs– und Wartungskosten des Registers AVI für das Jahr 2012 betrugen rd. 141.000 EUR.

[16] § 31 Abs. 4 Z 6 ASVG

(5) Elektronische Datenübermittlung und Abfragen

Das Register AVI wurde inhaltlich vom Hauptverband befüllt. Die Dokumente wurden im Hauptverband aufbereitet und an die IT–SV GmbH auf elektronischem Wege weitergeleitet und dort in die AVI gespeichert. Alle Datenübermittlungen aus dem Register AVI erfolgten im Wege von Online–Abfragen unter www.avsv.at.

Honorarordnungsverwaltung (HONO)

(1) Allgemeines

Die Honorarordnungsverwaltung (HONO) diente der Zuordnung von Tarifpositionen der einzelnen Versicherungsträger zu Leistungen. Sie umfasste 1,4 Mio. Datensätze.

(2) Inhalt und Aufgaben des Registers

Die HONO stellte für alle Fachbereiche der KV–Träger eine einheitliche Oberfläche dar, um Metatarifpositionen[17] anzulegen, zu ändern und Leistungspositionen zuordnen zu können. Sie ermöglichte die Zuordnung von Leistungskatalogen unterschiedlicher KV–Träger über alle Leistungsbereiche[18] hinweg. Durch diese Zuordnung konnten die Leistungskataloge der KV–Träger sozialversicherungs– bzw. bundesweit vereinheitlicht und vergleichbar gemacht werden.

Die HONO ermöglichte eine Verknüpfung der Metatarifpositionen zu den entsprechenden Positionen im Katalog ambulanter Leistungen, wodurch eine Dokumentation ambulanter Leistungen im Bereich der Krankenanstalten[19] und im Bereich der niedergelassenen Versorgung[20] erstellt werden konnte.

Der Hauptverband führte rd. 8.500 Metatarifpositionen, welchen die 140.000 Trägerpositionen zugeordnet wurden.

(3) Zuständigkeit

Die HONO wurde organisatorisch vom Hauptverband geführt. Die technische Betriebsführung wurde von der IT–SV GmbH wahrgenommen.

17 Bei einer Metatarifposition handelt es sich um einen Überbegriff, der sozialversicherungsweit mehrere gleichartige Leistungen beschreibt.

18 Unter Leistungsbereiche fallen niedergelassene Ärzte, Zahnärzte, Ambulatorien/Institute, Heilbehelfsmittel, Transportwesen und nichtärztliche Gesundheitsberufe.

19 intramuraler Bereich

20 extramuraler Bereich

(4) Kosten

Die Betriebs– und Wartungskosten der HONO für das Jahr 2012 betrugen rd. 432.000 EUR, die Weiterentwicklungskosten rd. 358.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Die Metatarifpositionen in der HONO wurden von den Fachabteilungen im Hauptverband angelegt, erstellt oder zugeordnet. Datenübermittlungen in die HONO erfolgten aus den Abrechnungssystemen ALVA[21] und NOVA[22]. Aus der HONO wurden Daten in das Data Warehouse der KV–Träger sowie des Hauptverbands übermittelt.

[21] ALVA steht für „automatisiert Leistungen von Vertragspartnern abrechnen“ und stellt das Standardprodukt zur Abrechnung der Gebietskrankenkassen dar.

[22] NOVA stellt das Vertragspartnerabrechnungsprogramm der Sonderversicherungsträger dar.

Betriebliche (Mitarbeiter–)Vorsorge im Hauptverband (BMV)

(1) Allgemeines

Der Hauptverband war gesetzlich dazu verpflichtet, bezüglich der Umsetzung der Betrieblichen Mitarbeiter– und Selbständigenvorsorge (Abfertigung NEU) mitzuwirken. Um dieser Verpflichtung gerecht zu werden, wurden in einer Datenbank[23] alle relevanten Daten hiezu gespeichert und den „Betrieblichen (Mitarbeiter–)Vorsorgekassen – BMV“ als zentrale Sammelstelle zur Verfügung gestellt.

(2) Inhalt und Aufgaben des Registers

Nachdem die Dienstgeber bzw. Selbstständigen Beitrittsverträge mit einer Betrieblichen Vorsorgekasse abgeschlossen hatten, hatten diese die Verträge an den Hauptverband der österreichischen Sozialversicherungsträger weiterzuleiten. In der BMV–Datenbank im Hauptverband der österreichischen Sozialversicherungsträger wurden diese Verträge sowie die zugehörigen Anwartschaftszeiten, Beitragsgrundlagen, Beiträge, Verfügungsansprüche und Verfügungen hiezu gespeichert und sowohl an die jeweilige Betriebliche Vorsorgekasse als auch an den zuständigen Sozialversicherungsträger weitergemeldet.

In der BMV–Datenbank waren auf einem Speicherplatz von rd. 10 Gigabyte (Stand 2012) rd. 82 Mio. Datensätze gespeichert.

Im Jahr 2012 wurden rd. 225.000 Abfragen an die BMV–Datenbank durchgeführt.

(3) Zuständigkeit

Die Sozialversicherungsträger sowie der Hauptverband waren gesetzlich zu einer Kooperation mit der Betrieblichen Vorsorgekasse verpflichtet.[24] So hatten die Sozialversicherungsträger bzw. der Hauptverband alle relevanten Daten, wie bspw. die Stammdaten der Anwartschaftsberechtigten und des Arbeitgebers, Beginn, Ende und Beendigungs-

[23] „Betriebliche (Mitarbeiter–)Vorsorge im Hauptverband – BMV“

[24] § 27 BMSVG

grund jedes Arbeitsverhältnisses sowie die jährlichen Lohndaten den Betrieblichen Vorsorgekassen zur Verfügung zu stellen.

(4) Kosten

Die Sozialversicherungsträger und der Hauptverband waren berechtigt, die anfallenden Investitions– sowie laufenden Kosten den Betrieblichen Vorsorgekassen in Rechnung zu stellen.[25]

Die Betriebs– und Wartungskosten der BMV für das Jahr 2012 betrugen rd. 128.000 EUR, die an die Betrieblichen Vorsorgekassen weiterverrechnet wurden.

(5) Elektronische Datenübermittlung und Abfragen

Der Datenaustausch der BMV im Hauptverband mit den Betrieblichen Vorsorgekassen bzw. dem zuständigen Sozialversicherungsträger erfolgte täglich im Rahmen einer Stapelverarbeitung (Batch–Verarbeitung).

(6) Zweck des Registers

Damit die Betrieblichen Vorsorgekassen die Anwartschaftsberechtigten jährlich unter anderem über deren erworbene Abfertigungsanwartschaft[26] informieren konnten, war es notwendig, die hiefür erforderlichen Daten, wie bspw. die jeweiligen Lohnzetteldaten,[27] der Sozialversicherungsträger zur Verfügung zu stellen. Der Austausch der Mitarbeitervorsorgedaten zwischen Vorsorgekassen und Sozialversicherungsträger erfolgte zentral über die BMV–Datenbank des Hauptverbands der Sozialversicherungsträger.

[25] §§ 26, 27 BMSVG

[26] § 25 Abs. 2 BMSVG

[27] § 27 Abs. 5 BMSVG

Erstattungskodex Basisdatenbank (EKO–BDB)

(1) Allgemeines

In der Erstattungskodex Basisdatenbank (EKO–BDB) wurden die Basisdaten für die Rezeptdatenabrechnung der Apotheken und hausapothekenführenden Ärzte sowie aktuelle Regeldaten für die Arzneimittelbewilligung erstellt.

(2) Inhalt und Aufgaben des Registers

Neben der Möglichkeit systemübergreifender Datenauswertungen hinsichtlich des Rahmen–Pharmavertrages oder spezifischer Medikamententhemen wurde aus dem Datenbestand der EKO–BDB der Erstattungskodex[28] generiert.

Durch die EKO–BDB wurden Prozesse, wie z.B. automatische Datenübernahme in den elektronischen Workflow, optimiert. Die EKO–BDB unterstützte das Infotool[29] hinsichtlich Wartung und Optimierung.

(3) Zuständigkeit

Gemäß § 31 Abs. 3 Z 12 ASVG oblag dem Hauptverband die Herausgabe eines Erstattungskodex (EKO) der Sozialversicherung für die Abgabe von Arzneispezialitäten auf Rechnung eines Sozialversicherungsträgers im niedergelassenen Bereich. Die organisatorische Betriebsführung erfolgte durch den Hauptverband, die technische Betriebsführung durch die IT–SV GmbH.

[28] Gemäß § 31 Abs. 3 Z 12 ASVG obliegt dem Hauptverband die Herausgabe eines Erstattungskodex (kurz EKO) der Sozialversicherung für die Abgabe von Arzneispezialitäten auf Rechnung eines Sozialversicherungsträgers im niedergelassenen Bereich. In dieses Verzeichnis sind jene für Österreich zugelassenen, erstattungsfähigen und gesichert lieferbaren Arzneispezialitäten aufzunehmen, die nach den Erfahrungen im In– und Ausland und dem aktuellen Stand der Wissenschaft eine therapeutische Wirkung und Nutzen für Patienten und Patientinnen im Sinne der Ziele der Krankenbehandlung (§ 133 Abs. 2 ASVG) annehmen lassen. Darüber hinaus gibt der Hauptverband zweimal im Jahr ein Druckwerk als Arbeitsbehelf für seine Vertragspartner heraus.

[29] Monatlich aktualisiertes Serviceinstrument, das umfassende Informationen zu den Arzneimitteln im Erstattungskodex anbot.

(4) Kosten

Die Betriebs– und Wartungskosten der EKO–BDB für das Jahr 2012 betrugen rd. 237.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Die EKO–BDB war primär als Informationsplattform eingerichtet. Der Zugriff erfolgte überwiegend durch Internet– bzw. e–card–Applikationen. In der EKO–BDB wurden keine sensiblen bzw. personenbezogenen Daten geführt, so dass keine Protokollierung erfolgte. In der EKO–BDB waren rd. 130.000 Datensätze mit einem Speichervolumen von rd. 66 Gigabyte abgelegt. Pro Jahr wurden rd. 700.000 Datensatzänderungen durchgeführt.

Elektronisches Pensionskonto (ePK)

(1) Allgemeines

Für alle in der gesetzlichen Pensionsversicherung Versicherten, die ab 1. Jänner 1955 geboren waren, war ein Pensionskonto einzurichten. Auf diesem Pensionskonto wurden die Beitragsgrundlagen aller erworbenen Versicherungszeiten erfasst. Jeder Versicherte konnte die Information über den Stand des Pensionskontos (Kontomitteilung) abrufen.

(2) Inhalt und Aufgaben des Registers

Die Gesamtgutschriften und der jeweilige monatliche Pensionswert waren aus dem ePK ersichtlich.

(3) Zuständigkeit

Die organisatorische und technische Betriebsführung wurde von der IT–SV GmbH wahrgenommen.

(4) Kosten

Die Betriebs– und Wartungskosten des ePK für das Jahr 2012 betrugen rd. 280.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Die Daten waren über Online–Dienste einsehbar. Datenübermittlungen aus diesem Register erfolgten nicht.

Zentraler Patientenindex (Z–PI)

(1) Allgemeines

Die Architektur der „Elektronischen Gesundheitsakte – ELGA“ sah keine zentrale Speicherung von Gesundheitsdaten vor. Vielmehr sollten die dezentral gespeicherten Dokumente (z.B. Befunde, Medikationsübersicht) zu einem bestimmten Patienten im Anlassfall zu einem Gesundheitsakt zusammengeführt werden können. Die Datenanwendung „Zentraler Patientenindex – Z–PI“ war hiebei notwendig, um den jeweiligen Patienten eindeutig zu identifizieren und die Verweisregister, in denen sich Verweise auf ELGA–Gesundheitsdaten dieses Patienten befinden können, zu lokalisieren.

Somit war es möglich, die entsprechenden Gesundheitsdaten einem bestimmten Patienten zuzuordnen. Der Z–PI war nur einer von mehreren Bausteinen des gesamten ELGA–Systems und wurde vom Hauptverband erstellt; andere Teile sollten bspw. vom BMG[30] bzw. einer Arbeitsgruppe der Bundesländer[31] entwickelt werden.

Es war gesetzlich vorgesehen, dass unter anderem das öffentlich zugängliche Gesundheitsportal mit Informationen für die Bevölkerung (ELGA–Bürgerportal) am 1. Jänner 2014 in Produktionsbetrieb[32] gehen kann. Danach sollten schrittweise weitere Teile von ELGA in Betrieb genommen werden.

(2) Inhalt und Aufgaben des Registers

Der Z–PI enthielt als Verzeichnis aller Patienten grundlegende Angaben zur jeweiligen Person. Dies waren neben den Namensangaben der Patienten[33] (Name, Geburtsdatum, akademische Grade) auch Personenmerkmale (Geburtsort, Geschlecht, Staatsangehörigkeit, Sterbedatum), sowie Adressdaten und Identitätsdaten (Sozialversicherungsnummer, bPK–Gesundheit, lokale Patientenkennungen).

Im Rahmen der Vorbereitungsaktivitäten für den geplanten Produktivbetrieb waren im Z–PI auf einem Speicherplatz von rd. 150 Gigabyte rd. 15,5 Mio. Personendatensätze gespeichert.

30 der Gesundheitsdienstanbieter–Index (z.B. Arzt, Krankenhaus)

31 Informationssicherheits– und Managementsystem (ISMS)

32 § 27 Abs.1 i.V.m. § 23 Gesundheitstelematikgesetz 2012

33 § 18 Abs. 2 Gesundheitstelematikgesetz 2012

Da der Produktivbetrieb des Z–PI im Zusammenhang mit dem ELGA–Bürgerportal planmäßig mit 1. Jänner 2014 starten sollte, erfolgten zur Zeit der RH–Prüfung noch keine Zugriffe.

(3) Zuständigkeit

Für die Umsetzung der „Elektronischen Gesundheitsakte – ELGA“ war ein „Zentraler Patientenindex – Z–PI“ gesetzlich vorgesehen.[34] Dieser war vom Hauptverband der Sozialversicherungsträger im übertragenen Wirkungsbereich einzurichten und zu betreiben.

(4) Kosten

Die Betriebs– und Wartungskosten des Z–PI für das Jahr 2012 betrugen rd. 718.000 EUR, die Weiterentwicklungskosten rd. 433.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Da der Z–PI als integraler Bestandteil des ELGA–Systems konzipiert war, sollten keine Abfragen von außen direkt an den Z–PI, sondern über ein Zugriffssystem an ELGA erfolgen. Es war vorgesehen, dass einerseits die

- Patienten nach einer Anmeldung mittels Bürgerkarte (bzw. Handysignatur) ihre jeweiligen ELGA–Daten, und andererseits die

- Gesundheitsdatenanbieter (z.B. Arzt, Krankenhaus) nach einer Authentifizierung sowie Nachweis des Behandlungszusammenhanges diese Daten

einsehen können.

(6) Zweck des Registers

Der Z–PI war notwendig, um jedem Patienten bei Bedarf eindeutig die – dezentral gespeicherten – zugehörigen Gesundheitsdokumente zuordnen zu können, sowie den Patienten selbst den elektronischen Zugriff auf die eigenen Gesundheitsdaten zu ermöglichen.

[34] §§ 4, 15, 18, 24 Gesundheitstelematikgesetz 2012

Leistungsinformation für Versicherte (LIVE)

(1) Allgemeines

LIVE diente zur Dokumentation und Beauskunftung der Kosten der durch Versicherte in Anspruch genommenen Leistungen. Für das Jahr 2012 erhielten 1.426.288 Versicherte die Leistungsinformation.

(2) Inhalt und Aufgaben des Registers

Gemäß § 81 ASVG hatten Krankenversicherungsträger einmal im Kalenderjahr die Versicherten über die Kosten der in Anspruch genommenen Leistungen zu informieren. LIVE hatte ihren Schwerpunkt in der Aufbereitung der Kosten, die durch die Inanspruchnahme von Sachleistungen von Versicherten und deren Angehörigen entstanden. Die in LIVE gespeicherten Daten wurden, falls vom Versicherten angefordert, postalisch versendet.

(3) Zuständigkeit

Die organisatorische Betriebsführung erfolgte durch den Hauptverband; die technische Betriebsführung wurde von der IT–SV GmbH wahrgenommen.

(4) Kosten

Die Betriebs– und Wartungskosten der LIVE für das Jahr 2012 betrugen rd. 128.000 EUR, die Weiterentwicklungskosten rd. 143.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

LIVE wurde inhaltlich über eine Schnittstelle aus dem Data Warehouse der Oberösterreichischen Gebietskrankenkasse befüllt. Jährlich erfolgten rd. 150.000 Zugriffe durch Online–Abfragen auf LIVE.

Familienbeihilfedatenbank (FB)

(1) Allgemeines

Das Register wird rd. 110.000–mal jährlich abgefragt. Trotz der starken Nachfrage war der Aufwand für den Hauptverband relativ gering, weil die Daten vom Familienlastenausgleichsfonds geliefert wurden.

(2) Inhalt und Zweck des Registers

Für eine Reihe von Feststellungen (Angehörigeneigenschaft, Kinderzuschüsse, Waisenpension usw.) benötigten die Sozialversicherungsträger Informationen darüber, ob für ein Kind über das vollendete 18. Lebensjahr hinaus Familienbeihilfe bezogen wurde.

Die Datenbank beinhaltete Informationen über die Zuerkennung bzw. den Bezug von Familienbeihilfe von Kindern über das 18. Lebensjahr hinaus. Die Daten wurden den Sozialversicherungsträgern zur Verfügung gestellt. Das Register enthielt rd. 9 Mio. Datensätze.

(3) Zuständigkeit

Die Zuständigkeit des Registers lag allein beim Hauptverband.

(4) Kosten

Die Betriebs– und Wartungskosten der FB für das Jahr 2012 betrugen rd. 3.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Die Daten wurden vom BMF im Wege der Bundesrechenzentrum GmbH automatisch und elektronisch an das Register übermittelt. Die Abfragen erfolgen über das SV–Intranet. Abfrageberechtigt waren die Sozialversicherungsträger.

(6) Weiterentwicklung des Registers

Es waren keine Weiterentwicklungen des Registers geplant. Die Übermittlung der Daten erfolgte mit der Sozialversicherungsnummer als Personenkennung. Es bestand eine generelle Empfehlung des Datenschutzrates für Bereiche, die nicht der Ingerenz der Sozialversicherung unterlagen, als Personenkennung das bPK anstatt der Sozialversicherungsnummer zu verwenden.

e–card Konsultationssystem (KONS)

(1) Allgemeines

Das e–card Konsultationssystem (KONS) diente der Speicherung von Arztkonsultationen als Nachweis für eine Inanspruchnahme von Leistungen sowie deren Verrechnung. Für das Jahr 2012 fielen rd. 115 Mio. Datensätze an.

(2) Inhalt und Aufgaben des Registers

Arztkonsultationen werden als Nachweis von Arztbesuchen anspruchsberechtigter Personen gespeichert. Zweck ist es, die Funktion des Krankenscheines als versicherungs– und leistungsrechtlichen Anspruchsnachweis zu ersetzen. KONS enthielt neben der Versicherungsnummer die Vertragspartnernummer des Arztes, den Zeitpunkt der Behandlung, den leistungs– und verrechnungszuständigen Versicherungsträger, die Art des Behandlungsfalls und Daten über Art der Konsultation.

Je Konsultation wurde ein Datensatz generiert. Die Anzahl der Datensätze in KONS betrug mit Stand Mai 2013 830.711.084.

(3) Zuständigkeit

Die organisatorische Betriebsführung erfolgte durch den Hauptverband; die technische Betriebsführung oblag der Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. – SVC.

(4) Kosten

Das Register Konsultationsdatenbank (KONS) und die Anspruchsdatenbank (ANSP) wurden gemeinsam geführt. Die gemeinsamen Betriebs– und Wartungskosten von KONS und ANSP für das Jahr 2012 betrugen 552.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

KONS war als integrierter Bestandteil des gesamten e–card–Systems konzipiert. Die Konsultationsdaten wurden aus KONS entsprechend den jeweiligen Verrechnungszeiträumen den jeweiligen verrechnungs– und leistungszuständigen Trägern sowie Krankenfürsorgeanstalten, die am e–card–System teilnahmen, für deren Verrechnung und Leistungsdokumentation bereitgestellt.

Krankenversicherung – Anspruchsdatenbank (ANSP)

(1) Allgemeines

Mit der Anspruchsdatenbank (ANSP) war es bei einer Inanspruchnahme von Arztkonsultationen möglich, den Anspruch auf Leistungen nachzuweisen und für den Vertragspartner eine Verrechnungsgrundlage zu schaffen. In der ANSP waren mit Stand Mai 2013 rd. 10,2 Mio. Versicherte und Angehörige sowie rd. 11.000 Vertragspartner gespeichert. Zusammen mit den Zugriffen auf die Konsultationsdatenbank wurden rd. 115 Mio. Zugriffe im Jahr 2012 registriert.

(2) Inhalt und Aufgaben des Registers

Bei Arztkonsultationen wurden vom e–card–System verschiedene Anspruchsprüfungen ausgelöst. Die Anspruchsprüfungen gliederten sich in

- eine versicherungsrechtliche Komponente, bei der geprüft wurde, ob der Anspruch aufgrund eines Versicherungsverhältnisses vorlag,

- eine leistungsrechtliche Komponente, bei der geprüft wurde, ob im selben Behandlungszeitraum bereits eine Konsultation derselben Fachgruppe erfolgt war,

- eine arztanspruchsrechtliche Komponente, bei der geprüft wurde, ob ein aufrechter Vertrag des Arztes bestand.

Verlief einer der Prüfschritte negativ, wurde ein Anspruch auf eine ärztliche Leistung auf Kosten eines Krankenversicherungsträgers als nicht bestehend ausgewiesen.

Die ANSP wurde als Tabelle innerhalb der Konsultationsdatenbank geführt. Die Datenbestände der Tabellen wurden tagesaktuell aus den datenführenden Systemen der Krankenversicherungsträger erzeugt. Zweck der ANSP war es, bei einer Inanspruchnahme von Leistungen einen Anspruch ausweisen zu können und für den Vertragspartner eine Verrechnungsgrundlage zu schaffen.

(3) Zuständigkeit

Die ANSP war nicht ausdrücklich gesetzlich vorgesehen; die Grundlage für die ANSP ergab sich aus den gesetzlichen Bestimmungen des ASVG,[35] wonach die e–card als Karte zu gestalten war, die den Zugriff auf die gespeicherten Daten autorisierte und alle Arten von Krankenscheinen zu ersetzen hatte. Dem Hauptverband oblag die organisatorische Betriebsführung der ANSP; die technische Betriebsführung erfolgte durch die Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. – SVC.

(4) Kosten

Die ANSP und die KONS wurden gemeinsam geführt. Die gemeinsamen Betriebs– und Wartungskosten der ANSP und der KONS für das Jahr 2012 betrugen 552.000 EUR.

(5) Elektronische Datenübermittlung und Abfragen

Bei Arztkonsultationen wurden verschiedene Anspruchsprüfungen ausgelöst. Die Daten der Anspruchsdatenbank wurden tagesaktuell aus der ZVD übernommen.

[35] § 31a Abs. 2 ASVG i.V.m. § 31c Abs. 1 ASVG