Verordnung über die Mindeststandards der technischen und organisatorischen Massnahmen bei der systematischen Verwendung der AHV-Versichertennummer ausserhalb der AHV

vom xxxxx *Entwurf Juni 2007*

Das Eidgenössische Departement des Innern

gestützt auf Artikel 50*g* Absatz 3 des Bundesgesetzes vom 20. Dezember 1946[1] über die Alters- und Hinterlassenenversicherung (AHVG),

im Einvernehmen mit dem Eidgenössischen Finanzdepartement

verordnet:

1. Abschnitt:. Allgemeine Bestimmungen

Art. 1 Zweck

Mit dieser Verordnung soll sichergestellt werden, dass Stellen und Institutionen, welche zur systematischen Verwendung der Versichertennummer berechtigt sind, ausreichende technische und organisatorische Massnahmen treffen, um:

a. die richtige Versichertennummer zu verwenden; und
b. die missbräuchliche Verwendung der Versichertennummer zu verhindern.

Art. 2 Geltungsbereich

Diese Verordnung gilt für alle Stellen und Institutionen, welche die Versichertennummer nach den Artikeln 50*d* und 50*e* AHVG systematisch verwenden.

2. Abschnitt: Technische Spezifikationen

Art. 3 Speicherung der Versichertennummer

Die Versichertennummer darf innerhalb einer Datenbank nur an einem Ort gespeichert werden.

1 SR **831.10**

Art. 4 Manuelle Erfassung der Versichertennummer

[1] Die Versichertennummer darf in einer elektronischen Datensammlung nur manuell erfasst werden, wenn eine Kontrollzifferprüfung gemäss Anhang 1 durchgeführt wird.

[2] Der manuellen Erfassung gleichgestellt ist das Einlesen der Versichertennummer mittels eines Strichcodes.

3. Abschnitt: Massnahmen für die Verwendung der richtigen Versichertennummer

Art. 5 Sichere Datenquellen bei der Erfassung

[1] Bei der erstmaligen und umfassenden Aufdatierung ihrer elektronischen Datensammlungen dürfen die registerführenden Stellen nach Artikel 2 des Registerharmonisierungsgesetzes vom 23. Juni 2006[2] und die Versicherer nach Artikel 11 des Bundesgesetzes vom 18. März 1994[3] über die Krankenversicherung (KVG) die Versichertennummer nur erfassen, wenn ihnen die Nummer nach einem Verfahren gemäss Artikel 134^{quater} Absatz 2 oder 4 der Verordnung vom 31. Oktober 1947[4] über die Alters- und Hinterlassenenversicherung (AHVV) bekannt gegeben wurde. Bei weiteren Erfassungen gelten die Absätze 2 – 4 sinngemäss.

[2] Alle andern Stellen und Institutionen dürfen die Versichertennummer in elektronischen Datensammlungen nur erfassen, wenn über deren Richtigkeit ausreichende Sicherheit besteht.

[3] Die ausreichende Sicherheit ist gewährleistet, wenn die Versichertennummer in einem Verfahren nach Artikel 134^{quater} Absatz 2 oder 4 AHVV bekanntgegeben wurde.

[4] Die ausreichende Sicherheit wird vermutet, wenn über die Identität der zur erfassten Versichertennummer gehörenden Person keine Zweifel bestehen und eine der nachfolgenden Quellen für die Nummer verwendet wird:

a. der Versicherungsausweis der AHV nach Artikel 135bis AHVV;
b. die im Zeitpunkt der Erfassung gültige Versichertenkarte nach Artikel 42*a* KVG;
c. die im Zeitpunkt der Erfassung aktuelle schriftliche oder elektronische Datenbekanntgabe eines Organs der AHV,
d. die im Zeitpunkt der Erfassung aktuelle schriftliche oder elektronische Datenbekanntgabe einer von der ZAS als ausreichend sicher empfohlenen Stelle oder Institution.

[5] Die ZAS veröffentlicht die als ausreichend sichere Datenquellen empfohlenen Stellen und Institutionen im Sinne von Absatz 4 Buchstabe d im Internet.

2 SR 431.02
3 SR 832.10
4 SR **831.101**

Art. 6 Verifizierung der erfassten Versichertennummer

[1] Stellen und Institutionen nach Artikel 5 Absatz 1 müssen periodisch prüfen, ob sämtliche erfassten Versichertennummern mit den dazugehörigen Personendaten, welche für die Zuweisung der Nummer relevant sind, übereinstimmen. Die Überprüfung erfolgt in einem Verfahren nach Artikel 134^{quater} Absatz 2 oder Absatz 4 AHVV.

[2] Vermutet die ZAS, dass eine Stelle oder Institution nicht die richtige Versichertennummer verwendet, so ordnet sie eine Überprüfung an.

4. Abschnitt: Massnahmen zum Schutz vor missbräuchlicher Verwendung

Art. 7 Grundsätze

[1] Der Zugang zu Datensammlungen, welche die Versichertennummer enthalten, ist nur den Personen einzuräumen, welche die Versichertennummer zur Erfüllung ihrer Aufgaben benötigen. Bei elektronischen Datensammlungen sind die Lese- und Schreiberechte entsprechend einzuschränken.

[2] Wird die Versichertennummer in komplexen Systemen systematisch verwendet, sind die nötigen Schutzmassnahmen gestützt auf eine detaillierte Risikoanalyse zu treffen.

[3] Beim Betrieb von Informatikmitteln und Datenspeichern sind die minimalen Sicherheitsvorgaben nach Anhang 2 einzuhalten.

Art. 8 Datenübertragung über öffentliche Netze

Werden Datensätze, welche die Versichertennummer enthalten, über das öffentliche Netzübertragen, so sind sie nach dem Stand der Technik zu verschlüsseln.

Art. 9 Verwendung und Bekanntgabe

Stellen und Institutionen, welche die Versichertennummer verwenden, haben ihr Personal in Aus- und Weiterbildung darüber zu informieren, dass die Versichertennummer nur aufgabenbezogen verwendet und nur entsprechend den gesetzlichen Vorgaben bekannt gegeben werden darf.

Art. 10 Inkrafttreten

[1] Diese Verordnung tritt unter Vorbehalt von Absatz 2 und 3 xxxxx in Kraft.

[2] Artikel 5 Absatz 4 Buchstabe a tritt am 1. Juli 2008 in Kraft.

[3] Artikel 5 Absatz 4 Buchstabe b tritt am 1. Januar 2009 in Kraft.

xxx.xxx.2007 Eidgenössisches Departement des Innern:

Pascal Couchepin

Anhang 1

Kontrollzifferprüfung (Artikel 4)

A. Aufbau der Versichertennummer

x_{n-12}	x_{n-11}	x_{n-10}	x_{n-9}	x_{n-8}	x_{n-7}	x_{n-6}	x_{n-5}	x_{n-4}	x_{n-3}	x_{n-2}	x_{n-1}	x_n
			.				.				.	
Ländercode			**9-stellige Nummerierung**									**Prüfziffer**
7	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**7**

B. Beschreibung der Kontrollzifferlogik

Die Kontrollziffer ist die letzte Ziffer (x_n). Sie wird wie folgt errechnet:

- in einem ersten Schritt werden die Ziffern von rechts nach links, beginnend mit der vorletzten (x_{n-1}), abwechselnd mit 3 und 1 multipliziert. Anschließend werden diese Produkte addiert werden:

  Zwischensumme = $(3x_{n-1}) + (1x_{n-2}) + (3x_{n-3})$ ….

- In einem nächsten Schritt wird die Zwischensumme so ergänzt, dass die Gesamtsumme dem nächsthöheren Vielfachen der Zahl 10 entspricht: Die ergänzende Zahl ist die Kontrollziffer x_n.

Hinweis:

Ist die Zwischensumme bereits ein Vielfaches von 10, ist die Kontrollziffer 0.

C. Illustration des Prinzips

Versichertennummer	**7**	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**→ ? ←**
Multiplikator	1	3	1	3	1	3	1	3	1	3	1	3	
Ergebnis	7	15	6	3	2	9	4	15	6	21	8	27	← Zwischensumme: 123
Ergänzung zum nächsthöheren Vielfachen von 10	130 ist die Zahl, welche – ausgehend von der Zwischensumme 123 - dem nächsthöheren Vielfachen von 10 entspricht. Die Zwischensumme muss also mit der Zahl 7 ergänzt werden →												**? = 7**

Anhang 2

Minimale Sicherheitsvorgaben für den Betrieb von Informatikmitteln und Datenspeichern, die bei der systematischen Verwendung der Versichertennummern eingesetzt werden

1. Der Zugang zu Informatikmitteln und Datenspeicher muss physisch gesichert sein. Beim Einsatz mobiler Informatikmittel und Datenspeicher muss mit Hilfe von dem Stand der Technik entsprechenden kryptographischen Verfahren (Datenverschlüsselung) sichergestellt sein, dass die Nutzung bzw. der Zugriff für Unberechtigte nicht möglich ist.

2. Der Zugriff auf Informatikmittel und Datenspeicher muss mit Hilfe von angemessenen, dem Stand der Technik und der Risikolage entsprechenden Informatiksicherheitsmassnahmen geschützt sein. Diese Massnahmen müssen mindestens den Einsatz von handelsüblicher und aktuell gehaltener Software zur Entdeckung und Beseitigung von Malware (Antiviren-Software), sowie den Einsatz von (zentralen oder persönlichen) Firewall-Systemen umfassen.

3. Benutzer und Benutzerinnen, die auf Informatikmittel und Datenspeicher zugreifen, müssen authentifiziert werden. Werden für die Authentifizierung Passwörter eingesetzt, so gelten die folgenden Anforderungen:
   a. Länge
      - Benutzerpasswort mindestens 8 Stellen
   b. Zusammensetzung
      - Grossbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen
      - Mindestens zwei dieser Kategorien müssen enthalten sein.
      - Trivial-Passwörter wie Benutzer-ID, Name, Vorname, Geburtsdatum usw. dürfen nicht verwendet werden.
   c. Gültigkeit
      - Beim Verdacht, dass Unberechtigte ein Passwort kennen, muss dieses umgehend geändert werden.
   d. Weitergabe
      - Das Benutzerpasswort ist geheim zu halten und darf nicht weitergegeben werden.

4. Die Betriebs- und Anwendungssoftware von Informatikmitteln muss möglichst zeitnah mit aktuellen Fehlerbehebungsupdates (Patches) ausgerüstet werden.

5. Auf Informatiksystemen sind wichtige Aktivitäten und Ereignisse aufzuzeichnen und regelmässig auszuwerten.

6. Die Rekonstruktion und Wiederverwendbarkeit von Daten nach einem möglichen Datenverlust muss in einem Datensicherungskonzept beschrieben und regelmässig geübt werden.

7. Werden Informatikmittel und Datenspeicher repariert, entsorgt oder vernichtet, so muss sichergestellt sein, dass sie keine Versichertennummern mehr enthalten und dass solche nicht rekonstruiert werden können.