



Entwurf Juni 07

Paket 2
Umsetzung der AHVG-Revision vom 23. Juni 2006
(Neue AHV-Versichertennummer)

Kommentar zum Erlass der Verordnung
über die Mindeststandards der technischen und organisatorischen
Massnahmen bei der systematischen Verwendung der Versicher-
tennummer ausserhalb der AHV

1	Ausgangslage	1
2	Erläuterungen zu den einzelnen Bestimmungen	2
2.1	1. Abschnitt – Allgemeine Bestimmungen	2
2.2	2. Abschnitt – Technische Spezifikationen	2
2.3	3. Abschnitt – Massnahmen für die Verwendung der richtigen Versichertennummer.....	2
2.3.1	Artikel 5 – sichere Datenquelle bei der Erfassung.....	2
2.3.2	Artikel 6 – Verifizierung	3
2.4	4. Abschnitt – Massnahmen zum Schutz vor missbräuchlicher Verwendung	4
2.4.1	Artikel 7 – Grundsätze	4
2.4.2	Artikel 8 – Datenübetragung über öffentliche Netze	4
2.4.3	Artikel 9 – Verwendung und Bekanntgabe	4
3	Anhänge 1 und 2	4
3.1	Anhang 2 Ziffer 5.....	4

1 Ausgangslage

Das Parlament hat am 23. Juni 2006 eine Revision des AHVG (neue AHV-Versichertennummer) beschlossen¹. Das Gesetz soll spätestens per 1. Januar 2008 in Kraft gesetzt werden. Die Revision betrifft nicht nur die AHV, sondern auch Drittnutzer der neuen Nummer: einerseits wird der Kreis der berechtigten Drittnutzer reguliert, andererseits wird von diesen Drittnutzern im neuen Artikel 50g Absatz 2 Buchstabe a des AHVG verlangt, dass sie „technische und organisatorische Massnahmen treffen für die Verwendung der richtigen Versichertennummer und den Schutz vor deren missbräuchlicher Verwendung“. In Absatz 3 von Artikel 50g des Gesetzes wird das Eidgenössische Departement des Innern verpflichtet, in Absprache mit dem Eidgenössischen Finanzdepartement die Mindeststandards für solche Massnahmen festzulegen. Diese Mindeststandards sollen in einer separaten Verordnung festgelegt werden.

¹ BBI 2006 5777

2 Erläuterungen zu den einzelnen Bestimmungen

2.1 1. Abschnitt – Allgemeine Bestimmungen

Die Artikel 1 und 2 dienen der Klärung der Ziele, welche mit dem neuen Erlass erreicht werden sollen, sowie der Abgrenzung des Geltungsbereichs. Artikel 1 und 2 lehnen sich inhaltlich streng am Auftrag des Gesetzgebers an:

- die Verordnung begrenzt sich mit Artikel 1 inhaltlich auf Bestimmungen, mit welchen sichergestellt werden soll, dass die richtige Versichertennummer verwendet und einer missbräuchlichen Verwendung der Versichertennummer vorgebeugt wird.
- In Artikel 2 wird der Geltungsbereich geklärt: die Verordnung ist – gemäss der übergeordneten Systematik auf Gesetzesstufe - nur für Drittnutzer der Nummer ausserhalb der AHV anwendbar und nicht auch für die AHV selber. Festzuhalten ist somit, dass Arbeitgeber als Organe der AHV nicht darunter fallen.

2.2 2. Abschnitt – Technische Spezifikationen

Im 2. Abschnitt geht es um Spezifikationen für elektronische Datensammlungen. Zum einen darf die Versichertennummer nur an einem einzigen Ablageort innerhalb einer Datenbank gespeichert werden (Art. 3). Dies deshalb, weil kein Zweifel darüber bestehen darf, wo allfällige Korrekturen vorgenommen werden müssen. Überdies wird in Artikel 4 verlangt, dass auf Systemen, in welchen die manuelle Erfassung der Versichertennummer vorgesehen ist, ein Kontrollzifferprüfprogramm installiert wird. So sollen Flüchtigkeitsfehler bei der Eingabe verhindert werden. Weil bei der Verwendung von Strichcode-Technik – je nach Ursprung des Strichcodes – ebenfalls Fehleingaben entstehen können, ist in solchen Fällen analog wie bei der manuellen Erfassung ein Kontrollzifferprüfprogramm zu installieren. Für die Details der Kontrollzifferprüfung wird auf Anhang 1 verwiesen.

In der Praxis sollten die im zweiten Abschnitt verlangten Massnahmen einfach und unter Verwendung handelsüblicher Software-Produkte umsetzbar sein.

2.3 3. Abschnitt – Massnahmen für die Verwendung der richtigen Versichertennummer

Mit der systematischen Verwendung der AHV-Versichertennummer ist aufgrund der entsprechenden gesetzlichen Grundlagen in anderen Sozialversicherungen und in den verschiedenen Bereichen der Verwaltungstätigkeit zu rechnen. Je mehr Drittnutzer es gibt und je intensiver der Datenaustausch unter Verwendung der AHV-Versichertennummer als entscheidendes Zuordnungselement gepflegt wird, desto wichtiger wird es, dass die verwendete Nummer richtig ist. Dabei gibt es aber graduelle Unterschiede: fehlerhafte Nummern in einem geschlossenen Verwaltungssystem oder in kleinen Datenstämmen zeitigen nicht dieselben Folgen wie fehlerhafte Nummern in Systemen mit grossen Datenstämmen oder intensiver Aussenwirkung. Die Verordnung trägt den unterschiedlichen Risiken Rechnung, indem sie sowohl in Bezug auf die Mindestanforderungen bei der Erfassung der Versichertennummer wie bei deren Verifizierung differenzierte Regelungen trifft.

2.3.1 Artikel 5 – sichere Datenquelle bei der Erfassung

Artikel 5 Absatz 1

Satz 1 der Bestimmung bezieht sich lediglich auf die *erstmalige und umfassende* Aufdatierung elektronischer Datensammlungen mit der Versichertennummer und verlangt, dass nur solche Versichertennummern eingespielen werden, welche von der Zentralen Ausgleichsstelle (ZAS) bekanntgegeben (und zugeordnet) wurden. Die Pflicht zum Bezug der Versichertennummer bei der ZAS im Rahmen der umfassenden Aufdatierung der Daten gilt nur für einen eng begrenzten Kreis von Nutzern, von denen ein erhöhtes Risiko ausgeht, weil sie einen sehr grossen Aussenwirkungsgrad bzw. sehr umfassende Datenstämmen betreuen. Dazu gehören – neben den Krankenversicherern nach KVG - die registerführenden Stellen im Sinne von Artikel 2 des Registerharmonisierungsgesetzes (SR 431.02).

Im einzelnen gehören dazu:

- o das von den Kantonen geführte und vom Bundesamt für Justiz betriebene Informatisierte Ständeregister (Infostar);

- o das zentrale Migrationsinformationssystem (ZEMIS) des Bundesamts für Migration;

Sowohl Infostar wie ZEMIS arbeiten mit der ZAS bei der Zuteilung der Nummer zusammen. Darüber hinaus gibt es einen AHV-bezogenen Datenaustausch beispielsweise im Zusammenhang mit Leistungen (Todesmeldungen von Infostar) oder Beitragsrückvergütungen (Ausreisen).

- o Weitere Informationssysteme des Eidgenössischen Departements für auswärtige Angelegenheiten wie VERA und Ordipro (Vernetzte Verwaltung der Auslandschweizerinnen und Auslandschweizer) sowie das Matrikelregister der schweizerischen diplomatischen und konsularischen Vertretungen im Ausland.
- o Die kantonalen und kommunalen Einwohner- und Stimmregister, die als Grundlage für eidgenössische Volksabstimmungen und Nationalratswahlen dienen. Die Richtigkeit der darin geführten Versichertennummer ist aufgrund der Erfassung der gesamten Bevölkerung und des zentralen Stellenwertes dieser Administrationshilfen in den Gemeinwesen besonders wichtig.

Bei Satz 2 geht es um die „weitere Erfassung“: Darunter fallen die Erfassungen in die Datenbanken der Krankenversicherer und Register, wenn sie nach dem erstmaligen Aufdatieren erfolgen – mithin „im laufenden Betrieb“ (wenn etwa jemand neu in die Krankenversicherung eintritt oder in die Gemeinde neu zuzieht). Hierfür sollen diejenigen Sicherheitsstandards gelten, welche generell auch für die übrigen Stellen und Institutionen zur Anwendung kommen.

Absatz 2 -5

Während in Absatz 2 von den Nutzern im Sinne der Selbstverantwortung gefordert wird, nur dann die Versichertennummer in elektronische Datensammlungen aufzunehmen, wenn ausreichende Sicherheit über deren Richtigkeit besteht – wobei der Nutzer auch hier eine Gewichtung anhand der konkreten Umstände vorzunehmen hat – geben die Absätze 3 und 4 dem Nutzer konkrete Anhaltspunkte für ein praktisches und verantwortungsvolles Vorgehen beim Erfassen der Versichertennummer. Der Nutzer kann sich darauf verlassen, nicht gegen die Mindeststandards zu verstossen, wenn er die Erfassung der Nummer im Sinne dieser Vorgaben organisiert. Allerdings ist er frei, in Selbstverantwortung nach Absatz 2 eine andere Lösung zu finden. Absatz 5 ermöglicht die Publikation von empfohlenen Datenquellen durch die ZAS. Diese Massnahme erleichtert es dem Anwender, an Informationen über sichere Datenquellen zu kommen.

2.3.2 Artikel 6 – Verifizierung

Grundsätzlich sollen nur diejenigen Stellen und Institutionen zur periodischen Überprüfung ihrer Datenstämme hinsichtlich der Richtigkeit der Versichertennummer verpflichtet werden, welche bereits bei der erstmaligen und umfassenden Aufdatierung zum Bezug der Nummer bei der ZAS verpflichtet sind. Ist dieser Prozess einmal abgeschlossen, sind laufend vorkommende Mutationen im Rahmen der Vorgaben von Artikel 5 Absatz 2-4 vorzunehmen. In der Praxis wird also etwa ein Krankenversicherer bei der erstmaligen Aufdatierung über korrekte Daten verfügen. Kommt es aber in der Folge zu Mutationen aufgrund von Kassenwechseln, kann die Versichertennummer der Neuzugänge z.B. gestützt auf die noch gültige Versichertenkarte des bisherigen Versicherers (und zusätzlich einer Identitätsprüfung z.B. mit der Kopie des Identitätsausweises) erfasst werden. Mit der Zeit dürften in Datensammlungen mit häufigen Mutationen fehlerhafte Einträge zunehmen. Damit sich solche Fehler und deren weitere Verbreitung korrigieren lassen, sind diejenigen Stellen und Institutionen, von denen ein erhöhtes Risiko ausgeht, nach Absatz 1 von Artikel 6 gehalten, ihre Daten periodisch mit der ZAS abzugleichen.

Dieselbe Verpflichtung soll gemäss Absatz 2 auch heute noch nicht bekannte Stellen und Institutionen treffen, wenn befürchtet werden muss, dass ein Nutzer derart viele falsche Nummern verwendet, dass Betriebsstörungen bei der Durchführung der AHV entstehen oder der Betrieb von anderen Nutzern

gestört wird. Der ZAS wird deshalb in Absatz 2 das Recht zur Anordnung einer Überprüfung eingeräumt.

2.4 4. Abschnitt – Massnahmen zum Schutz vor missbräuchlicher Verwendung

2.4.1 Artikel 7 – Grundsätze

Während Absatz 1 allgemein gültige Grundsätze zum restriktiven und sachlich gerechtfertigten Zugang zu Daten (bei physischen Ablagen) bzw. zum Zugriff (bei elektronischen Datensammlungen) enthält, welche für sämtliche Nutzer gelten, richtet sich Absatz 2 nur an Nutzer, welche komplexe Systeme betreiben. Komplex ist ein System beispielsweise dann, wenn mehrere Anwender-Programme auf dieselbe Datenbank zugreifen oder zahlreiche Nutzer in die Anwendung einbezogen sind. Der Betrieb komplexer Systeme setzt – im Eigeninteresse des Betreibers – in der Praxis ohnehin regelmässig eine Risikoanalyse voraus. In diese Risikoanalyse ist immer auch das Schutzbedürfnis der Versichertennummer einzubeziehen. Entsprechend dem Ergebnis sind die nötigen Massnahmen zu treffen. Für alle übrigen Nutzer – beispielsweise in einer kleinen Arztpraxis - sind gemäss Absatz 3 wenigstens die Sicherheitsvorgaben nach Anhang 2 einzuhalten.

2.4.2 Artikel 8 – Datenübetragung über öffentliche Netze

Beim Datentransfer über öffentliche Netze besteht eine erhöhte Gefahr, dass Daten in den Besitz von Personen gelangen können, für welche sie nicht bestimmt sind. Mit einer dem aktuellen Stand der Technik entsprechenden Verschlüsselung kann diese Gefahr gebannt werden.

2.4.3 Artikel 9 – Verwendung und Bekanntgabe

Ein effektiver Schutz vor Missbrauch setzt einerseits voraus, dass die Versichertennummer nur von Stellen und Institutionen verwendet wird, welche hiezu legitimiert sind. Wer die Nummer ohne entsprechende Berechtigung verwendet, macht sich nach Artikel 87 AHVG strafbar. Indessen kann ein Missbrauch auch durch ein Fehlverhalten einer zur systematischen Verwendung berechtigten Stelle oder Institution entstehen. Die Gefahr besteht insbesondere dann, wenn die Versichertennummer für andere Zwecke als für die vorgesehene Aufgabenerfüllung herangezogen wird oder in unzulässiger Weise an Dritte weitergegeben wird. Dieser Gefahr haben die berechtigten Nutzer Rechnung zu tragen, indem sie mit der nötigen Information in der Aus- und Weiterbildung dafür sorgen, dass das Personal die Versichertennummer nur aufgabenbezogen verwendet und die Nummer an Dritte nur bekannt gibt, wenn dies rechters ist. Dabei sind die jeweils im entsprechenden Aufgabengebiet geltenden rechtlichen Vorgaben für die Datenbekanntgabe zu beachten.

3 Anhänge 1 und 2

Während Anhang 1 eine detaillierte Umschreibung der Kontrollzifferlogik, welche bei der Kontrollzifferprüfung nach Artikel 4 zu beachten ist, beinhaltet, geht es bei Anhang 2 um die minimalen Sicherheitsvorgaben für den Betrieb von Informatikmitteln und Datenspeichern, welche bei der systematischen Verwendung der Versichertennummer eingesetzt werden. Diese Anhänge sind weitgehend selbsterklärend. An dieser Stelle wird daher nur Ziffer 5 des Anhangs 2 als einziger erläuterungsbedürftiger Punkt näher kommentiert.

3.1 Anhang 2 Ziffer 5

Ziffer 5 schreibt vor, dass wichtige Aktivitäten und Ereignisse aufzuzeichnen und regelmässig auszuwerten sind. Darunter fallen – je nach konkreter Ausgestaltung eines Systems – verschiedene Vorgänge, und eine abschliessende für alle Nutzer gültige Aufzählung ist nicht möglich. Als Beispiele zu erwähnen sind hier:

- System-Boot und Shutdown
- Einloggen
- Gescheiterte Authentifikationsversuche
- Gescheiterte Zugriffsversuche
- Vergabe und Änderung von Privilegien
- Alle Aktionen, die erhöhte Privilegien erfordern