Oktober 2007

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

Erläuterungen zum Erlass der Verordnung des EDI über die Mindeststandards der technischen und organisatorischen Massnahmen bei der systematischen Verwendung der Versichertennummer ausserhalb der AHV

1 Ausgangslage

Das Parlament hat am 23. Juni 2006 eine Revision des AHVG (neue AHV-Versichertennummer) beschlossen[1]. Das Gesetz soll per 1. Dezember 2007 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] BBl 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 Artikel 2 Absatz 1 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 Absatz 1 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. In Absatz 2 der Bestimmung wird darauf Rücksicht genommen, dass kaum ein Schutzbedürfnis in Bezug auf die Richtigkeit der Versichertennummer besteht, wenn eine Datensammlung nicht aktiv bewirtschaftet wird. In solchen Fällen kommt es nicht zu Mutationen – beispielweise bei statistischen Auswertungen gestützt auf statische Registerabzüge – und es ist nicht mit einer Weiterverbreitung der (falschen) Nummer und in der Folge mit Schaden bei Drittnutzern zu rechnen. Hier sollen nur diejenigen Normen beachtet werden, welche dem Schutz vor Missbrauch der Versichertennummer dienen.

2.2 2. Abschnitt – Massnahmen für die Sicherstellung der Verwendung der richtigen Versichertennummer

Im 2. Abschnitt geht es um Massnahmen für die Sicherstellung der Verwendung der richtigen Versichertennummer. Betroffen davon sind nur Nutzer, welche die Nummer in elektronischen Datensammlungen verwenden.

Artikel 3 beinhaltet die Anforderung an elektronische Systeme in ihrer Gesamtheit: Sowohl die Datenbankarchitektur wie die Programme und Applikationsmechanismen müssen so ausgestaltet werden, dass kein Zweifel darüber aufkommen kann,:

- welche Nummer zu welcher Person gehört, und
- wenn mehrere Nummern zu einer Person gehören, welche davon die aktuell gültige sein soll. Dies ist insbesondere bei Systemen notwendig, welche die Daten historisieren. Nur die Eindeutigkeit in Bezug auf das Datenfeld, welches die aktuelle Nummer enthält – verbunden mit einer eindeutigen Verbindung zu den dazugehörigen Daten einer Person - erlaubt es, eine Verifizierung in Bezug auf die Richtigkeit der verwendeten Versichertennummer durchzuführen.

In Artikel 4 wird 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 wie bei der manuellen Erfassung ein Kontrollzifferprüfprogramm zu installieren. Bei der Verwendung von Magnetstreifen oder Microprozessoren-Chips, wie sie für die Versichertenkarte der Krankenversicherung vorgesehen sind, entfällt die Notwendigkeit einer Kontrollzifferprüfung. Für die Details der Kontrollzifferprüfung wird auf Anhang 1 verwiesen. In der Praxis sollten die in Artikel 4 verlangten Massnahmen einfach und unter Verwendung handelsüblicher Software-Produkte umsetzbar sein.

2.2.1 Artikel 5 – Sichere Datenquelle bei der Erfassung

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. Um den grössten Risiken in

Bezug auf die Verbreitung falscher Versichertennummer vorzubeugen, sieht bereits Artikel 134quinquies AHVV für die Register und die Krankenversicherer eine Sonderregelung in Bezug auf die erstmalige Aufdatierung der Datenbestände und die Verifizierung der Nummer vor.

Während in Absatz 1 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 2 und 3 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 eine andere Lösung zu finden. Absatz 4 ermöglicht die Publikation von empfohlenen Datenquellen durch die ZAS. Diese Massnahme erleichtert es dem Anwender, an Informationen über sichere Datenquellen zu kommen.

2.3 3. Abschnitt – Massnahmen zum Schutz vor missbräuchlicher Verwendung

2.3.1 Artikel 6 – 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 Datenbanken im gleichen System betrieben werden oder mehrere Anwender-Programme auf dieselbe Datenbank zugreifen oder aber 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 sind immer auch das Schutzbedürfnis der Versichertennummer und die Problematik der unerlaubten Zusammenführung von Datenbanken einzubeziehen. Um dieser Problematik Rechnung zu tragen, könnte bei Systemen, in denen mehrere Datenbanken jeweils die Versichertennummer enthalten, unterschiedliche Verschlüsselungen für die Versichertennummer eingesetzt werden, so dass sich auch für Systemadministratoren Hindernisse ergeben, eine unzulässige Datenbankzusammenführung vorzunehmen. Entsprechend dem Ergebnis der Risikoanalyse sind die nötigen Massnahmen zu treffen. Im Übrigen haben sämtliche Nutzer – beispielsweise auch eine kleine Arztpraxis - gemäss Absatz 3 wenigstens die Sicherheitsvorgaben nach Anhang 2 einzuhalten.

2.3.2 Artikel 7 – Datenübertragung 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. Als öffentlich zu betrachten ist jedes Netz, welches nicht einem abschliessend definierten Kreis von Nutzern, welche einer besonderen Zutrittskontrolle unterworfen sind (z.B. amtsinternes Netz), vorbehalten ist. Mit einer dem aktuellen Stand der Technik entsprechenden Verschlüsselung kann diese Gefahr gebannt werden.

2.3.3 Artikel 8 – 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 rechtens 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