Prof. Dr. David Basin: Risikofolgenabschätzung zur Verwendung der AHV-Nummer als Personenidentifikator

Zusammenfassung

Die aktuelle Organisation und Verarbeitung personenspezifischer Daten in verschiedenen administrativen Registern der Schweiz ist organisch gewachsen, in einer Weise, die aus der Sicht des Datenschutzes als problematisch bezeichnet werden muss. Persönliche, oftmals sensitive, Daten sind in über 14 000 administrativen und organisatorischen Registern gespeichert und mit einem einheitlichen Identifikator, der AHVN13, indexiert. Die entsprechenden Computersysteme und die darin gespeicherten Daten sind anfällig für Attacken durch interne und externe Angreifer, welche sich unberechtigten Zugriff auf die Registerdaten verschaffen können. Dieses Risiko ist nicht unerheblich, da viele der Systeme, welche diese Register speichern und verarbeiten, von Organisationen wie Gemeindeverwaltungen, Schulen und Krankenhäusern verwaltet werden, welche nicht den gleich hohen Sicherheitsanforderungen wie die IT-Systeme des Bundes unterliegen.

Sowohl die AHVN13 als auch Identitätsattribute wie Vorname, Nachname und Geburtsdatum werden in diesen Registern verwendet um Personen mit Daten zu verknüpfen. Falls Daten entwendet werden, sind die zugehörigen Personen deshalb identifizierbar. Darüber hinaus macht es die Verwendung der AHVN13 als einheitlicher Personenidentifikator einfach, Daten aus verschiedenen Registern direkt zu verknüpfen. Dies ermöglicht es Angreifern, umfangreiche Informationsprofile der betroffenen Personen zu erstellen. Diese Datenschutzrisiken werden in Zukunft weiter zunehmen, da einerseits immer mehr Organisationen die AHVN13 für die Datenverarbeitung nutzen und andererseits immer mehr Daten gesammelt, gespeichert und verarbeitet werden, insbesondere in relativ unsicheren IT-Systemen von Kantons- und Gemeindeverwaltungen sowie Nichtregierungsorganisationen.

Da die Registerdaten zusammen mit den zugehörigen Identitätsattributen gespeichert sind, würde das alleinige Ersetzen der AHVN13-Nummern in einem Register durch sektorspezifische Identifikatoren oder andere Pseudonyme die Datenschutzrisiken nicht wesentlich reduzieren. Die Registerdaten könnten durch die Verwendung der in den Registern gespeicherten Identitätsattribute weiterhin mit relativ hoher Präzision mit Personen verknüpft werden. Allerdings gibt es Alternativen zum gegenwärtigen Ansatz, welche Datenschutzrisiken erheblich reduzieren. Diese beinhalten eine Umstrukturierung der Verarbeitung, Speicherung und Absicherung der Registerdaten.

Die nachfolgend aufgeführten Massnahmen würden die aktuellen Datenschutzrisiken erheblich reduzieren, insbesondere jene Risiken, welche die kontinuierliche Ausweitung der gegenwärtigen Verwendungsweise der AHVN13 mit sich bringen.

- Einführung von nichtsprechenden Pseudonymen (wie Steuer- oder Krankenkassen-identifikationsnummern) in einer angemessenen Art und Weise. Hierfür können sektorspezifische Identifikatoren in verschiedenen Varianten verwendet werden. Es ist wichtig zu beachten, dass die Speicherung dieser Identifikatoren direkt zusammen mit anderen Identitätsattributen im gleichen Register minimiert wird.

- Pseudonyme müssen für verschiedene Verwaltungs- und Geschäftsprozesse mit Personen verknüpft werden können. Daher ist es notwendig, sowohl technisch als auch organisatorisch sorgfältig zu regulieren und zu kontrollieren, wie und wann diese Verknüpfungen erfolgen.

- Die Erhöhung der Anforderungen an die Sicherheit und die Qualitätssicherung aller Systeme, welche sensitive Daten verarbeiten, die mit der AHVN13 oder sektorspezifischen Identifikatoren indexiert sind. Beides muss über die aktuellen Regelungen des EDI hinausgehen.

Diese Massnahmen sind mit Aufwand verbunden. Insbesondere bietet die Verwendung von sektorspezifischen Identifikatoren nicht die gleiche Bequemlichkeit und Einfachheit, wie dies bei der Nutzung der AHVN13 als ein einheitlicher Identifikator der Fall ist. Ausserdem verursacht der Einsatz sektorspezifischer Identifikatoren in unterschiedlichen Kontexten zusätzliche Kosten bei der Systemanalyse, dem Design und der Implementierung, da berücksichtigt werden muss, wie Identitäten und persönliche Daten in administrativen und anderen organisatorischen Prozessen verwendet werden und dafür angemessene Identifikationskonzepte entwickelt werden müssen. Eine solche Umstellung verändert auch die Art und Weise wie Organisationen mit ihren IT-Systemen arbeiten und wie sie mit ihren Kunden interagieren. Die Entscheidung, wo und wie diese Massnahmen eingesetzt werden, erfordert daher eine Kosten-Nutzen-Analyse, welche ausserhalb des Aufgabenbereichs dieser Studie liegt.

In der Schweiz verfügt der Bund bereits über Erfahrungen mit solchen Massnahmen in unterschiedlichen Kontexten wo sensitive, persönlich identifizierbare Informationen verarbeitet werden, oder er führt entsprechende Projekte durch. Beispiele hierfür sind die Pseudonymisierung von Daten bei statistischen Analysen im Bundesamt für Statistik und aktuelle Projekte zur Einführung sektorspezifischer Identifikatoren für elektronische Patientendossiers und für das Handelsregister. Die Ausweitung dieser Aktivitäten in andere Bereiche wäre aus der Sicht der Risikominderung wünschenswert.

27. September 2017