Jörg Brust
AOK-Bundesverband

Aktionsforum
Telematik im Gesundheitswesen

Managementpapier
„Pseudonymisierung / Anonymisierung

Kommentare zum 1. Meilenstein

Hallo Herr Strobel,

hier mein Vorschlag für 3.2.1.
"Pseudonymisieren ist das Ersetzen des Namens und anderer Indentifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (§ 3 Absatz 6a BDSG).

Beim P. geht es also darum die Feststellung der Identität des Betroffenen zu unterbinden. Zugleich soll gewährleistet bleiben, dass die Angaben über eine Kennzeichen miteinander verbunden bleiben. Dies geschieht indem alle auf die konkrete Person hinweisenden Angaben (wie z.B. Name, Anschrift, Geburtsdatum oder personenbezogene Nummern) so verändert werden, dass das Individuum nicht mehr herausgefunden werden kann, aber gleichwohl über ein zu generierendes Kennzeichen erkennbar bleibt, dass die Daten zu einer bestimmten, aber nicht mehr bestimmbaren Person gehören. So entsteht ein Datensatz, der zwar noch erkennen lässt, dass zu einer z.B. weibliche Person im Alter von x Jahren bestimmte Angaben vorliegen; die Identität der Person ist jedoch nicht ersichtlich.

Dann kann es mit Absatz zwei aus dem Text weitergehen. Danach noch folgender Satz: Pseudonymisieren ist eine abgeschwächte Form der Anonymisierung."

Hier mein Vorschlag für 3.2.2
"Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§3 Absatz 6 BDSG).

Beim A. geht es also darum, von vorneherein zu verhindern, dass eine Zuordnung von Angaben zu irgendeiner Person noch möglich ist. Dies geschieht indem alle auf eine Person hinweisende Angaben (wie z.B. Name, Anschrift, Geburtsdatum oder personenbezogene Nummern) ersatzlos entfernt werden oder so verändert werden, dass die Identität der Person nicht mehr herauszufinden ist. Im Gegensatz zum Pseudonymisieren werden die die Person betreffenden Angaben nicht durch ein Kennzeichen miteinander verbunden. Sie stehen vielmehr nach dem Anonymisieren wie statistischen Daten nebeneinander.

Dann kann es mit Absatz zwei aus dem Text weitergehen."

Hinweisen möchte ich noch auf die verschieden Pseudonymisierungsverfahren. (z.B: Das Kennzeichen ist abcd. Es entstand aus der Personennummer 1234). Es gibt reversible oder irreversible Verfahren. Erstere erlauben es von dem Kennzeichen auf die konkrete Person rückzuschließen. Irreversible verhindern einen Rückschluss auf die verschlüsselten Angaben (von abcd kann nicht auf 1234 zurück geschlossen werden). Davon zu unterscheiden ist die Frage der Eindeutigkeit des Verschlüsselungsverfahrens. Bei einen nicht eindeutigen Verfahren wird beim ersten Pseudonymiserungsvorgang aus 1 einmal a; beim zweiten Psyeudoymisierungvorgang wird aus 1 jedoch ein anderer Buchstabe). Bei einem eindeutigen Verfahren muss gewährleistet sein, dass immer das selbe Kennzeichen für ein Person generiert wird. (im obigen Beispiel aus 1 immer a, aus 2 immer b usw.) Auch ein irreversibler Schlüssel kann so ausgestaltet sein. Das ihm zugrundeliegende mathematische Verfahren, verhindert jedoch die Rückschlüsse. Soweit mir bekannt, wird im AOK-System ein sog. Blow-Fish Alogarithmus für eine irreversible aber eindeutige Verschlüsselung eingesetzt.

Staatliche Datenschützer scheinen nur ein irreversibles Pseudonymiserungsverfahren zu akzeptieren. Von der Akzeptanz hängt ab, ob die im Ergebnis verschlüsselten Daten als Daten anzusehen sind, die vom Schutz der Datenschutzgesetz befreit sind oder nicht. Wenn das Pseudnoymiserungsverfahren nicht ausreicht, sind die Daten wie Sozialdaten bzw. wie Daten i.S.d. § 3 Abs. 1 BDSG zu behandeln; unterliegen also voll dem Datenschutz. Insoweit sind die Positionspapier genannten Tabellen kritisch einzustufen.

Bonn, 24. Juni 2002