TE Dsk Empfehlung 2014/5/23 DSB-D213.131/0002-DSB/2014

JUSLINE Entscheidung

Veröffentlicht am 23.05.2014

Norm

DSG 2000 §1 Abs1;
DSG 2000 §1 Abs2;
DSG 2000 §4 Z1;
DSG 2000 §7 Abs3;
DSG 2000 §30 Abs1;
DSG 2000 §30 Abs6;
DSG 2000 §61 Abs9;
ASVG §31 Abs4 Z1

Text

GZ: DSB-D213.131/0002-DSB/2014 vom 23. Mai 2014

[Anmerkung Bearbeiter: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc. sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

EMPFEHLUNG

Die Datenschutzbehörde spricht aus Anlass der Eingabe der Kurie der niedergelassenen Ärzte der Ärztekammer für *** (Einschreiterin) vom 13. Februar 2012, betreffend Bekanntgabe der Sozialversicherungsnummer zur Anlegung eines „***HIT“-Benutzeraccounts folgende Empfehlung aus:

- Das Amt der *** Landesregierung möge von der Verwendung der Sozialversicherungsnummer bei Erstellung eines „***HIT“-Benutzeraccounts absehen.

- Für die Umsetzung dieser Empfehlung wird eine Fr i s t von d r e i M o n a t e n gesetzt.

Rechtsgrundlagen: § 1 Abs. 1 und 2, § 4 Z 1, § 30 Abs. 1 und 6 des Datenschutzgesetzes 2000 – DSG 2000,BGBl. I Nr. 165/1999 idgF.

Gründe für diese Empfehlung

A. Vorbringen der Beteiligten und Verfahrensgang

1. In ihrer Eingabe vom 13. Februar 2012 führte die Einschreiterin aus, dass zur kontinuierlichen Betreuung in den *** Landespflegeheimen medizinische Aufzeichnungen im EDV-System des Heimes geführt würden. Um ein individuelles Benutzerkonto für diese Software für die verschiedenen behandelnden Ärzte anlegen zu können, sei es laut Aussagen

des Heimträgers erforderlich, die persönliche Sozialversicherungsnummer bekannt zu geben. Durch die zuständige Stelle beim Amt der *** Landesregierung sei dieses Vorgehen damit begründet worden, dass im Hinblick auf die Verarbeitung sensibler Daten sichergestellt werden müsse, dass der angelegte Benutzeraccount zu einer echten Person gehöre und nicht als unpersönlicher „Gemeinschafts-Login“ missbraucht werden könne. Um einen „***HIT“-Account zu bekommen, müsse die entsprechende Person durch die Heimverwaltung mit seinen Qualifikationen im „HR-System“ (Personalverwaltung) des Amtes der *** Landesregierung angelegt werden. Das „Identity Management System (IDM)“ prüfe, ob der Eintrag im „HR-System“ eine Sozialversicherungsnummer habe und ob diese korrekt sei und lege dann automatisiert die Berechtigung an. Die Plausibilität könne durch eine in der Sozialversicherungsnummer enthaltene Prüfsumme errechnet werden. Laut Aussage des Auftraggebers sei dies derzeit der einzig sichere Weg, dem Missbrauch durch unpersönliche Gemeinschafts-Logins vorzubeugen.

2. Das Amt der *** Landesregierung, Gruppe Gesundheit und Soziales, Abteilung Landeskrankenanstalten und Landesheime, gab über Aufforderung der damaligen Datenschutzkommission in seinen Stellungnahmen vom 12. Juli 2012 und 10. September 2013 an, dass personenbezogene Daten von Nutzern bzw. Usern im „***HIT-System“, welches im Datenverarbeitungsregister registriert sei, nur für Identifizierungs- und Authentifizierungszwecke erfasst und verwendet würden. Diese beschränkten sich auf Name, Funktion, Dienst-/Einsatzort und Sozialversicherungsnummer zur adäquaten Parametrisierung des Berechtigungssytems und würden keinem externen Empfängerkreis zur Verfügung gestellt. Darüber hinaus erhalte jeder potentielle „***HIT“-User eine umfassende Unterlage und Information über die Dienstvorschriften für den IT-Betrieb in Landesheimen. Werde ein Zugang zum genannten EDV-System angefordert - dies könne grundsätzlich nur vom Dienststellenleiter des jeweiligen Standortes beantragt werden - so müssten erst die Stammdaten der entsprechenden Person in das Personalveraltungssystem aufgenommen werden. Erst wenn die Benutzerstammdaten am Personalveraltungssystem korrekt und vollständig angelegt seien, würden für diese Person im „IDM-System“ Zugangsberechtigungen entsprechend der Qualifikation und des Zuständigkeitsbereiches vergeben. Als zusätzliche Sperre für Missbrauch werde vom „IDM-System“ kontrolliert, ob eine Sozialversicherungsnummer vorhanden sei und deren Kontrollsumme überprüft. Erst nach zusätzlicher Kontrolle durch einen Mitarbeiter der Stabstelle IT der Abteilung Landeskrankenanstalten und Landesheime werde die Benutzeranforderung freigegeben. Die Sozialversicherungsnummer werde nicht an Ziel-Systeme und Datenanwendungen übergeben, sondern diene als Prüfkriterium, ob es sich um eine echte Person handle. Die Anwendung der Sozialversicherungsnummer eines Arztes bzw. „***HIT“-Users sei somit ein einfaches und adäquates Kriterium zur fehlerfreien sowie dauerhaften Validierung der Berechtigungsidentität. Auch bei einer Interessensabwägung überwiege der Schutz der pflegerischen und medizinischen Daten der Heimbewohner, weil der Eingriff in das schutzwürdige Interesse an der Geheimhaltung der Sozialversicherungsnummer deshalb als geringer einzustufen sei, da diese nur im Rahmen der Userverwaltung erforderlich sei und bei keinen Arbeitsprozessen verwendet oder gar weitergegeben werde.

B. Sachverhaltsfeststellungen

Dem gegenständlichen Fall zugrunde liegt die beim Datenverarbeitungsregister registrierte Datenanwendung „Betrieb einer Datenverarbeitungsanlage zur administrativen Unterstützung in den Bereichen Buchhaltung, Pflegedokumentation, Personalverwaltung, Dienstplanerstellung sowie Material- und Küchenorganisation – Teilanwendung Pflegedokumentation, medizinische und therapeutische Dokumentation für 48 Landespflegeheime und 1 Landesjugendheim“ (DVR-Nr.: ***), auch „***HIT-System“ genannt.

Die Einrichtung eines persönlichen Zuganges zum „***HIT-System“ erfordert zunächst die Aufnahme von Stammdaten der betreffenden Person (Name, Funktion, Dienst- und Einsatzort sowie die Sozialversicherungsnummer) in das Personalverwaltungssystem des Auftraggebers, des Amtes der *** Landesregierung. Das „Identity-Management-System (IDM)“ des Auftraggebers untersucht daraufhin die Plausibilität der Benutzerstammdaten, insbesondere die Echtheit der Sozialversicherungsnummer insofern, als die Kontrollsumme der Sozialversicherungsnummer überprüft wird. Erst nach zusätzlicher Kontrolle durch einen Mitarbeiter der Stabstelle IT des Auftraggebers wird die Zugangsberechtigung entsprechend der Qualifikation und des Zuständigkeitsbereiches freigegeben.

Die Sozialversicherungsnummer ist ausschließlich für Mitarbeiter der Personalverwaltung einsehbar und wird nicht an Ziel-Systeme und Datenanwendungen weitergegeben. Die Heranziehung der Sozialversicherungsnummer der Nutzer dient der Identifizierung- und Authentifizierung bei der Einrichtung eines persönlichen Accounts, es soll sichergestellt werden, dass es sich um eine echte Person handelt.

Beweiswürdigung: Diese Feststellungen beruhen auf den unbestrittenen Ausführungen des Amtes der *** Landesregierung sowie aus der beim Datenverarbeitungsregister unter der DVR-Nr.: *** registrierten Datenanwendung, genannt „***HIT-System“.

C. In rechtlicher Hinsicht folgt daraus:

1. Zur Zuständigkeit der Datenschutzbehörde:

Gemäß § 61 Abs. 9 DSG 2000 in der Fassung BGBl. I Nr. 83/2013 tritt mit Ablauf des 31. Dezember 2013 die Datenschutzbehörde an die Stelle der Datenschutzkommission. Am 1. Jänner 2014 bei der Datenschutzkommission anhängige Verfahren sind nach Maßgabe der Bestimmungen dieses Bundesgesetzes in der Fassung des Bundesgesetzes BGBl. I Nr. 83/2013 von der Datenschutzbehörde fortzuführen.

Das gegenständliche Verfahren war am 1. Jänner 2014 bei der Datenschutzkommission anhängig. Die Datenschutzbehörde ist daher in zeitlicher Hinsicht zur Erlassung dieser Empfehlung zuständig.

2. In der Sache:

Die Sozialversicherungsnummer ist ein personenbezogenes Datum im Sinne des § 4 Z 1 DSG 2000, an der ein Versicherter ein schutzwürdiges Geheimhaltungsinteresse hat.

Nach der Rechtsprechung der Datenschutzkommission darf die Sozialversicherungsnummer nicht als „genereller Identifikator“ verwendet werden, d.h. in Zusammenhängen, die mit sozialversicherungsrechtlichen Sachverhalten nichts zu tun haben; eine solche Verwendung wurde von der ehemaligen Datenschutzkommission bereits wiederholt als unzulässig bezeichnet (vgl. dazu etwa zuletzt die die Empfehlung vom 19. Juli 2013, GZ K210.714/0016-DSK/2013, RIS, mwN).

Die Datenschutzbehörde sieht keinen Anlass von dieser Rechtsansicht abzuweichen.

In ähnlicher Weise hat sich auch der gemäß § 41 DSG 2000 beim Bundeskanzleramt eingerichtete Datenschutzrat bereits mehrmals geäußert (vgl. dazu bspw. die Stellungnahme des Datenschutzrates zur Untersuchung von Alternativen zur Sozialversicherungsnummer in der Bildungsdokumentation vom 25. Februar 2010, abrufbar unter www.bka.gv.at/DocView.axd?CobId=38592).

Im vorliegenden Fall ist nach Ansicht der Datenschutzbehörde kein sozialversicherungsrechtlicher Zusammenhang gegeben, weil die Verwendung der Sozialversicherungsnummer nur der Identifizierung und Authentifizierung eines potentiellen Nutzers zur Erlangung einer Zugangsberechtigung zum sogenannten „***HIT-System“ dient.

Ungeachtet dessen wird von der Datenschutzbehörde keineswegs in Abrede gestellt, dass im Einklang mit §§ 3 bis 5 Gesundheitstelematikgesetz 2012 in Verbindung mit dem E-Government-Gesetz bei Weitergabe von Gesundheitsdaten die Identität jener Personen, die diese Daten verwenden, bei der Implementierung einer Zugangsberechtigung festzustellen ist.

Für die Datenschutzbehörde ist allerdings im Lichte des sich aus § 1 Abs. 2 letzter Satz und § 7 Abs.3 DSG 2000 ergebenden Grundsatzes, wonach ein Eingriff in das Grundrecht auf Datenschutz jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf, nicht nachvollziehbar, weshalb den gesetzlichen Anforderungen nur unter Zuhilfenahme der Sozialversicherungsnummer entsprochen werden kann, zumal laut den Stellungnahmen des Auftraggebers lediglich festgestellt werden soll, ob es sich beim potentiellen Nutzer um eine „echte Person“ handelt. Bei einem behandelnden Arzt könnte die Klärung dieser Frage etwa auch unter Verwendung der Ärzteausweisnummer oder überhaupt – im Einklang mit dem E-Government-Gesetz – mittels Bürgerkarte erfolgen.

Es wird daher empfohlen, an Stelle der Sozialversicherungsnummer eine andere, dem „***HIT“- Benutzer eindeutig zuordenbare Nummer zur Identifizierung zu verwenden.

3. Es war folglich gemäß § 30 Abs. 6 DSG 2000 zur Herstellung des rechtmäßigen Zustandes die obige Empfehlung zu erteilen. Eine Frist von drei Monaten scheint – in Anbetracht des Umstandes, dass eine Neuorganisation des Identifizierungs- und Authentifizierungsvorganges notwendig sein wird – angemessen.

Schlagworte

Empfehlungen, Geheimhaltung, Sozialversicherungsnummer, Stammdaten, Identitätsprüfung, Identifikator, Benutzeraccount, Zugangsberechtigung, fehlender sozialversicherungsrechtlicher Zusammenhang

European Case Law Identifier (ECLI)

ECLI:AT:DSB:2014:DSB.D213.131.0002.DSB.2014

Zuletzt aktualisiert am

22.09.2014