Republik Österreich
Datenschutz behörde

NEWSLETTER 4/2015

Stammzahlenregister (SZR)

Leitung: Mag. Marcus Hild LL.M.
hat in Wien Jus studiert, einen postgraduate Lehrgang in Informationsrecht besucht, ist eingetragener Mediator und seit 2005 in der Datenschutzbehörde für die Stammzahlenregisterbehörde und Internationales zuständig.


Foto: DSB

Die Stammzahlenregisterbehörde wurde durch das E-Governmentgesetz geschaffen und hat ihre Tätigkeit im Jahr 2005 als Organisationseinheit der Datenschutzkommission aufgenommen.
Die Stammzahlenregisterbehörde entwickelt, betreibt und beaufsichtigt die Kernkomponenten des österreichischen E-Government. Die Aufgabe der Behörde ist es sicherzustellen, dass diese zuverlässig funktionieren und die elektronische Verarbeitung von personenbezogenen Daten mit Hilfe von E-Government Werkzeugen datenschutzkonform umgesetzt wird.
Zu diesem Zweck werden von der Datenschutzbehörde 4 verschiedene Datenanwendungen betrieben.

A. Das Stammzahlenregister. SZR.

Diese Datenanwendung ist kein Register, obwohl die Bezeichnung das nahelegt, sondern eine Datenanwendung zur Errechnung:

- eindeutiger elektronischer Identitäten, die anhand von ZMR (Zentrales Melderegister) oder ERnP Daten durch einen besonders sicheren Verschlüsselungsmechanismus erzeugt werden und (Personen) Stammzahlen genannt werden,
- von bereichsspezifischen Personenkennzeichen und
- von verschlüsselten bereichsspezifischen Personenkennzeichen.

Sowohl technisch als auch organisatorisch ist diese Datenanwendung mit beinahe 300 Millionen Erledigungen (im Jahr 2014) eine große Herausforderung. Die Datenschutzbehörde bedient sich dabei des Bundesministeriums für Inneres als Dienstleister für den Betrieb einer Großrechenanlage und zur Unterstützung bei der Kundenbetreuung.

B. Das Ergänzungsregister für natürliche Personen. ERnP.

Die eindeutige Identität (verschlüsselte Stammzahl) einer Person wird durch einen Vergleich der Stammdaten einer Person mit dem zentralen Melderegister hergestellt. Für Personen die nicht im Melderegister eingetragen sein müssen/können, aber dennoch Services des österreichischen E-Government nutzen wollen oder müssen, wird dieses nicht öffentliche Ergänzungsregister betrieben.

C. Das Ergänzungsregister für sonstige Betroffene. ERsB.

Die eindeutige Identität eines Unternehmens (unverschlüsselte Stammzahl) wird durch einen Vergleich der Stammdaten des Unternehmens mit dem Firmenbuch, dem Vereinsregister oder dem Ergänzungsregister für sonstige Betroffene hergestellt. Diese verwenden ihre Firmenbuchnummer, Vereinsregisternummer oder Ergänzungsregisternummer als (Unternehmens) Stammzahl. Für Unternehmen oder andere „sonstige Betroffene“ (vor allem Einzelunternehmer und Personengemeinschaften), die nicht im Firmenbuch oder dem Vereinsregister eingetragen sein müssen/können, aber dennoch Services des österreichischen E-Government nutzen wollen oder müssen, wird dieses öffentliche Ergänzungsregister betrieben.

Nähere Informationen zur Stammzahlenregisterbehörde finden Sie auf unserer Homepage www.dsb.gv.at.

Im Fokus

Wie umgehen mit Daten-Keksen?

Mag. Michael Suda

Die bekannte Online-Enzyklopädie „Wikipedia“ (deutschsprachige Version, Stand: 27.7.2015) definiert sie folgendermaßen:

„Ein Cookie (englisch [ˈkʊki]; zu deutsch Keks oder Plätzchen; auch Magic Cookie, engl. für magisches Plätzchen) ist in seiner ursprünglichen Form eine Textdatei auf einem Computer. Sie enthält typischerweise Daten über besuchte Webseiten, die der Webbrowser beim Surfen im Internet speichert. Im für den Anwender besten Fall dient ein Cookie dazu, dass er sich beim wiederholten Besuch einer verschlüsselten Seite nicht erneut anmelden muss – das Cookie teilt dem besuchten Rechner mit, dass er schon einmal da war. Im für den Anwender schlechtesten Fall speichert das Cookie Informationen über komplexes privates Internetverhalten und übermittelt diese, ähnlich wie ein Trojanisches Pferd, ungefragt an einen Empfänger. Anders als das Trojanische Pferd ist ein Cookie jedoch nicht versteckt und vom Anwender einseh- und löschbar.“

Cookies bilden (neben der Speicherung der IP-Adresse) für Website-Betreiber die wichtigste Möglichkeit, Nutzer (genauer: deren Hard- und Software) wiederzuerkennen. Nicht nur der eigentliche Betreiber einer aufgerufenen Website sondern auch Dritte, insbesondere Werbeunternehmen, können technisch Cookies setzen und den User damit wiedererkennen (und sein Surf-Verhalten analysieren).

Cookies bilden einen datenschutzrechtlichen Spezialfall, seit die EU-Gesetzgebung im Jahr 2009 versucht hat, ihre Verwendung zu regulieren (in einer Novelle zur sogenannten Telekom-Datenschutzrichtlinie 2002/58/EG). Verlangt wird die Einwilligung des Webseitenbenutzers in das Speichern von Cookies. Allerdings bleibt unklar, wie ein solcher „Opt-in“ aussehen muss, da sich Text und Erwägungsgründe des EU-Rechts teilweise widersprechen.

Die Bestimmung wird vielfach als nicht zielführend kritisiert. Die meisten gängigen Webbrowser erlauben es dem Nutzer ohnehin bereits, das Setzen von Cookies zu sperren oder an eine Zustimmung zu binden. Da aber (fast) jede Website Cookies setzt, führen die dann ständigen aufgehenden Warn- und Zustimmungsfenster regelmäßig dazu, dass die Funktion als „störend“ wieder abgeschaltet wird. Auch ist der Nutzer, der dem Setzen von Cookies nicht zustimmt, von der Benutzung vieler Webdienste ausgeschlossen, oder die Funktionalität der Dienste ist eingeschränkt.

In Österreich wurden die EU-Vorgaben in § 96 Abs. 3 TKG 2003 umgesetzt, ohne „Cookies“ auch nur ansatzweise zu erwähnen oder deren Funktion zu beschreiben, sodass die Bestimmung nur von Spezialisten als Cookie-Regelung identifiziert werden kann. Demnach sind Netz- und Websitebetreiber verpflichtet, den Nutzer über die Ermittlung, Verarbeitung und Übermittlung personenbezogener Daten sowie den Zweck der Datenverwendung, die Rechtsgrundlage und die Dauer der Datenverwendung zu informieren und dessen Zustimmung einzuholen. Vom EU-Recht vorgesehene Ausnahmen gelten, wenn der Zweck der (Cookie-) Datenverwendung ausschließlich die Übertragung einer Nachricht oder die Zurverfügungstellung eines vom Nutzer gewünschten Dienstes ist. Wer die Informationspflichten nach § 96 Abs. 3 TKG 2003 nicht erfüllt, kann vom örtlich zuständigen Fernmeldebüro mit einer Geldstrafe von bis zu 37 000 Euro belegt werden. Das Gesetz weist der DSB in diesem Zusammenhang keine besonderen Aufgaben zu.

Für Internet-Nutzerinnen und –Nutzer dürfte es praktikabler sein, beim Internet-Surfen vom Cookie-Setzen als Standardfall auszugehen und in regelmäßigen Abständen das vom verwendeten Browser für Cookies bestimmte Verzeichnis zu überprüfen und alle oder zumindest unerwünschte Cookies (z.B. solche von Dritt-Anbietern wie Internet-Werbeunternehmen) zu löschen.

Ausgewählte Entscheidungen der DSB

Telefonische Bekanntgabe einer Ladung zur Einvernahme durch die Kriminalpolizei an den Arbeitgeber

Die Datenschutzbehörde hat sich in ihrem Bescheid vom 27. April 2015, GZ: DSB-D122.257/0003-DSB/2015, bezüglich einer Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten in Folge telefonischer Bekanntgabe einer Ladung des Beschwerdeführers zur Einvernahme durch die Kriminalpolizei an seinen Arbeitgeber für unzuständig erklärt.

Dabei ging die Datenschutzbehörde davon aus, dass es sich bei den vom Bezirksinspektor gesetzten Schritten um Erkundigungen und die Ladung und Vernehmung des Beschwerdeführers, somit um Maßnahmen im Sinne der §§ 152ff StPO handelte, die wiederum gemäß § 91 Abs. 2 StPO der Gewinnung, Sicherstellung, Auswertung oder Verarbeitung einer Information zur Aufklärung des Verdachts einer Straftat dienten. Kriminalpolizeiliches Handeln, das nicht von einer Justizbehörde (Gericht oder Staatsanwaltschaft) angeordnet worden ist, stellt zwar Verwaltungshandeln dar, erfolgt jedoch im Dienste der Gerichtsbarkeit, da die Staatsanwaltschaft gemäß § 20

Abs. 1 StPO das Ermittlungsverfahren leitet. Unter „Gerichtsbarkeit“ im Sinne des § 31 DSG 2000 ist die Gesetzesvollziehung durch jede Justizbehörde, demnach auch durch die Staatsanwälte als „Organe der Gerichtsbarkeit“ gemäß Art. 90a B-VG, zu verstehen. Da es gemäß § 106 Abs. 1 Z 2 StPO nunmehr möglich gewesen wäre, gegen die Vorgehensweise des Bezirksinspektors als Organ der gesetzlich gemäß § 18 Abs. 2 StPO mit den Aufgaben der Kriminalpolizei betrauten Sicherheitsbehörde wegen des Eingriffs in das subjektive Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten bei Durchführung einer Ermittlungsmaßnahme Einspruch an das zuständige Landesgericht zu erheben, besteht (anders als in der Zeit des Ausschlusses der gerichtlichen Zuständigkeit nach § 106 StPO) keine Rechtschutzlücke. Es gibt daher keinen Grund, § 31 Abs. 2 DSG 2000 so auszulegen, dass eine Zuständigkeit der Datenschutzbehörde begründet wird (Verweis auf den Bescheid der Datenschutzkommission vom 7. November 2012, K121.862/0012-DSK/2012).

Kriminalpolizei und Datenschutz, Zuständigkeitsfrage wieder offen

Bescheid der DSB vom 27. 4. 2015, DSB-D122.257/0003-DSB/2015

Erkenntnis des VfGH vom 30. 6. 2015, G 233/2014 ua

Eines der Ziele des Gesetzgebers bei der Reform der Strafprozessordnung (BGBl. I Nr. 19/2004, in Kraft seit 1. 1. 2008) war es, im Vorverfahren (Ermittlungsverfahren) ein einheitliches Rechtsschutzsystem gegen Eingriffe durch Gericht, Staatsanwaltschaft und Kriminalpolizei zu schaffen. Auch gegen aus eigener Macht vorgenommene Eingriffe der Polizei bei der Datenverwendung mit dem Zweck der Gewinnung, Sicherstellung, Auswertung oder Verarbeitung einer Information zur Aufklärung des Verdachts einer gerichtlich strafbaren Handlung (= kriminalpolizeiliche Datenverwendung) sollte ein Einspruch bei Gericht gemäß § 106 Abs.1 StPO an die Stelle der datenschutzrechtlichen Beschwerde treten.

Durch das Strafprozessrechtsänderungsgesetz 2013, BGBl. I Nr. 195/2013, wurde ab 1. 1. 2014 die Möglichkeit des Einspruchs bei Gericht gegen Ermittlungsmaßnahmen der Kriminalpolizei neuerlich eröffnet (zuvor aufgehoben durch das Erkenntnis des Verfassungsgerichtshofs [VfGH] vom 16. 12. 2010, VfSlg 19281/2010).

Im Bescheid vom 27. 4. 2015 hatte sich die DSB näher mit dieser Rechtslage zu befassen. Der Beschwerdeführer behauptete, durch die telefonische Bekanntgabe einer Ladung zur Einvernahme durch die Kriminalpolizei an seinen Arbeitgeber im Recht auf Geheimhaltung verletzt worden zu sein (ein Ermittlungsverfahren wegen des Verdachts einer Straftat wider das Suchtmittelgesetz war anhängig, wurde später jedoch von der Staatsanwaltschaft eingestellt).

Die DSB wertete dies als kriminalpolizeiliche Datenverwendung, die gemäß § 31 Abs. 2 DSG 2000 im Dienste der Gerichtsbarkeit erfolgte. Anders als in einer früheren Entscheidung (Bescheid der Datenschutzkommission vom 7.11.2012, K121.862/0012-DSK/2012) bestehe seit 1. 1. 2014 keine Rechtsschutzlücke mehr. Ein Einspruch gegen die gerügte Vorgehensweise bei Gericht wäre möglich gewesen, die Annahme einer Doppelzuständigkeit (Gericht und DSB) würde dem Gesetz einen verfassungswidrigen Inhalt unterstellen. Daher folgte die DSB den Einwänden der belangten Sicherheitsbehörde und wies die Beschwerde wegen Unzuständigkeit zurück.

Durch das Erkenntnis des Verfassungsgerichtshofs (VfGH) vom 30. 6. 2015 ist jedoch neuerlich, wirksam ab 1. 8. 2016, die Bestimmung über die Zuständigkeit der Gerichte für Einsprüche gegen kriminalpolizeiliche Ermittlungsmaßnahmen als verfassungswidrig aufgehoben worden. Begründet wird dies vom VfGH damit, dass es dem Betroffenen nicht zuzumuten sei, die Abgrenzung zwischen kriminalpolizeilichen Ermittlungen und sicherheitspolizeilicher Gefahrenabwehr zu treffen und damit das Risiko einzugehen, den falschen Rechtsschutzweg zu wählen (in den Anlassverfahren des Verwaltungsgerichts Wien ging es nicht um Datenschutz sondern um die Abgrenzung von kriminalpolizeilichen Maßnahmen zu Akten unmittelbarerer sicherheitspolizeilicher Befehls- und Zwangsgewalt).

Sollte der Gesetzgeber keine „Sanierung“ der Bestimmungen der StPO vornehmen, wäre ab 1. 8. 2016 im Beschwerdefall neuerlich zu prüfen, inwieweit die DSB gemäß § 31 DSG 2000 für Beschwerden gegen eine kriminalpolizeiliche Datenverwendung, soweit diese nicht vom einem Organ der Gerichtsbarkeit angeordnet wurde, zuständig ist.

Löschung von erkennungsdienstlich ermittelten Daten

Dem Beschwerdeführer wurden aufgrund des Verdachtes des versuchten Betruges nach § 146 StGB von Polizeibeamten Fingerabdrücke abgenommen und es wurden von ihm auch Fotos angefertigt.

Das vom Beschwerdeführer gestellte Löschungsbegehren wurde von der Landespolizeidirektion Oberösterreich u.a. mit der Begründung abgelehnt, dass schon der Verdacht des versuchten Betruges nach § 146 StGB die Durchführung dieser Maßnahmen rechtfertigen würde. Daraufhin wandte sich der Beschwerdeführer an die Datenschutzbehörde. Diese hat in ihrem Bescheid vom 9. Februar 2015 GZ: DSB-D122.244/0001-DSB/2015, ausgesprochen, dass allein der Verdacht der Begehung des versuchten Betruges nach § 146 StGB die Abnahme von Fingerabdrücken bzw. die Anfertigung von Lichtbildern nicht rechtfertigt, sondern es wäre vielmehr gemäß § 65 SPG auf den Einzelfall („Ausführung der Tat“, „Persönlichkeit des Betroffenen“) einzugehen. Die Verweigerung der vom Beschwerdeführer begehrten Löschung erfolgte daher zu Unrecht.

Aktualisierungspflicht DVR, VDS-Datenanwendungen sind zu streichen

Empfehlung der DSB vom 1. Juli 2015, DSB-D215.814/0003-DSB/2015

Anlässlich eines Kontrollverfahrens hat die DSB einem Unternehmen aus der Branche der Kommunikationsdienstleister folgende Empfehlungen erteilt:

1. Datenanwendungen (DAN), die ausschließlich die Durchführung der vom Verfassungsgerichtshof aufgehobenen Vorratsdatenspeicherung (VDS) zum Gegenstand hatten, wären nach dem 1. Juli 2014 unverzüglich durch Änderungsmeldung aus dem DVR zu streichen gewesen. Dass für die VDS eingeführte Software (Durchlaufstelle zu den Sicherheitsbehörden gemäß DSVO) noch verwendet wird, ist nicht entscheidend.
2. Die DVR-Eintragung muss aktuell gehalten werden, Änderungen der Firma (hier: aus einer Aktiengesellschaft wurde schon vor Jahren eine Ges.m.b.H.) sind unverzüglich zu melden.

Die DSB hielt allgemein fest, dass „das DVR jedermann ein wahrheitsgemäßes, der Realität der meldepflichtigen Datenverwendung durch einen datenschutzrechtlichen Auftraggeber bestmöglich angenähertes Bild bieten soll" und daher vom Auftraggeber regelmäßig zu prüfen und zu aktualisieren ist.

Diese Empfehlung ist innerhalb der gesetzten Dreitagesfrist umgesetzt worden.

Keine Eintragung elterlicher Vollmachten auf einer Bürgerkarte für Minderjährige

Bescheid der DSB Bescheid vom 09. Juni 2015, GZ: DSB-D433.003/0001-DBS/2015

Es ist dies der erste Fall, in welchem die Datenschutzbehörde als Stammzahlenregisterbehörde über ein Ansuchen mit Bescheid abzusprechen hatte.

Dieser Entscheidung lag folgender Sachverhalt zugrunde:

Das antragstellende Ehepaar begehrte für die mj. gemeinsame Tochter die Ausstellung einer Bürgerkarte sowie für sich die Eintragung einer Vertretungsvollmacht auf der Bürgerkarte ihrer Tochter.

Die Datenschutzbehörde hat den Antrag auf Ausstellung einer Bürgerkarte mangels Zuständigkeit zurückgewiesen, da die Datenschutzbehörde keine Signaturprodukte anbietet sondern nur die Personenbindung auf einem vorhandenen Signaturprodukt bewirkt (§ 4 Abs. 2 E-GovG).

Der Antrag der Eltern auf Eintragung einer Vertretungsvollmacht auf der Bürgerkarte der gemeinsamen Tochter wurde abgewiesen. Begründet wurde dies damit, dass die Voraussetzungen gemäß § 9 Abs. 2 StZRegBehV nicht erfüllt waren.

Gegen diese Bescheide wurde Beschwerde an das Bundesverwaltungsgericht erhoben.

DSB kein vorlagefähiges Gericht iSd Art. 267 AEUV

Bescheid der DSB Bescheid vom 11. August 2015, GZ: DSB-D122.359/0005-DSB/2015

Die Datenschutzbehörde hatte in diesem Fall zum ersten Mal zu entscheiden, ob sie ein vorlagefähiges Gericht im Sinne des Art. 267 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) ist.

Eine Landwirtin erachtete sich durch die (unionsrechtlich vorgeschriebene) Veröffentlichung der von ihr innerhalb eines Jahres bezogenen Agrarförderungen in ihrem Recht auf Geheimhaltung verletzt und begehrte, unter Hinweis auf das Urteil des EuGH vom 9. November 2010 in den verbundenen Rechtssachen C-92/09 und 93/09, die Einholung einer Vorabentscheidung durch den EuGH.

Die Datenschutzbehörde hat die Beschwerde – soweit es um die Veröffentlichung ging – abgewiesen. Soweit es um den Antrag auf Einholung einer Vorabentscheidung ging, wurde der Antrag zurückgewiesen und wie folgt begründet:

Infolge der jüngeren Rechtsprechung des EuGH zur Frage, was unter einem Gericht im Sinne des Art. 267 AEUV zu verstehen ist, ist die Datenschutzbehörde – anders als die ehemaligen Datenschutzkommission – nicht mehr als vorlagefähiges Gericht zu betrachten (vgl. dazu das Urteil Belov, C 394/11, Rn 49 und 52, sowie das Urteil TDC, C-222/13, Rn 37).

Gegen den Bescheid wurde Beschwerde an das Bundesverwaltungsgericht erhoben.

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Wissenschaftsfonds-Novelle 2015
- Änderung des Telekommunikationsgesetzes, des KommAustria-Gesetz u.a.

Weblink:

- Parlament aktiv: alle Stellungnahmen

Weitere Informationen:

Impressum:
Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Hohenstaufengasse 3, 1010 Wien, E-Mail: dsb@dsb.gv.at, Web: http://www.dsb.gv.at

Offenlegung gemäß § 25 Mediengesetz:
Der Newsletter der DSB ist ein wiederkehrendes elektronisches Medium (§ 1 Abs. 1 Z 5a lit. c MedienG); die gesetzlich gebotenen Angaben sind über folgenden Link abrufbar: http://www.dsb.gv.at/impressum.