Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 17. Jahrgang, Heft 4, Dezember 2017

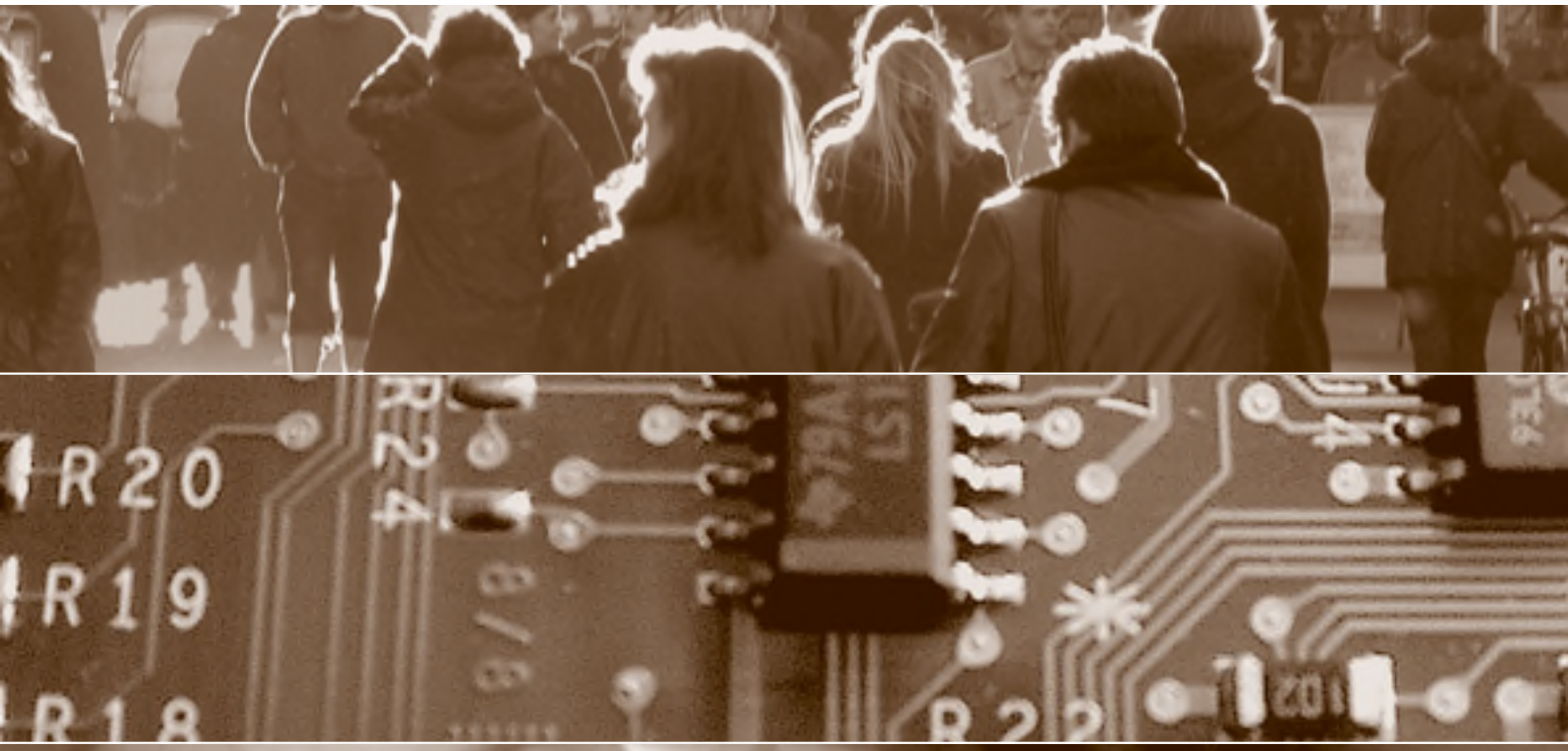
Schwerpunkt:

User Tracking

fokus: Personendaten ohne Identifizierbarkeit?

fokus: Maschinelle Profilierung durch KI

report: Follow-up: Zum Anwendungsbereich der DSGVO



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
User Tracking

Personendaten ohne Identifizierbarkeit?

Das Datenschutzrecht knüpft am Begriff der Personendaten an. Unter dem Stichwort der «Singularisierung» geistert die Auffassung herum, Daten müssten selbst dann als personenbezogen gelten und der Datenschutz eingehalten werden, wenn nicht ermittelt werden kann, um wen es bei den Daten geht. Ist der Begriff der Personendaten aufgeweicht worden?

Maschinelle Profilierung durch KI

Computer können Menschen etwa aus Bild und Ton in vielerlei Hinsicht einschätzen – bald übertreffen sie die Menschen darin qualitätsmässig. Welche Konsequenzen hat das und wo führt das hin?

Personalisierung im (Online-)Marketing

Eine Website, die automatisch in der richtigen Sprache angezeigt wird, eine Kaufempfehlung, die das passende Kabel zum neuen TV-Gerät bereithält, oder eine Reiseverbindung, die sich bei Verspätungen aktualisiert – die Möglichkeiten des personalisierten Marketings nehmen zu. Wie funktioniert diese Individualisierung?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, lic. iur. Marco Fey

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Inland: CHF 174.00, Jahresabo Ausland: CHF 199.00, Einzelheft: CHF 48.00
PrintPlu§: Jahresabo Inland: CHF 195.00, Jahresabo Ausland CHF 220.00

PrintPlu§: Das PrintPlu§-Abonnement bietet die Möglichkeit, bequem und zeitgleich zur Printausgabe jeweils das PDF der ganzen Ausgabe herunterzuladen. Detaillierte Informationen finden Sie unter www.schulthess.com/printplus.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa,
Tel. +41 (0)44 928 56 11, pietro.stuck@fachmedien.ch

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Zum Anwendungsbereich der DSGVO

Im Mai 2018 tritt die EU-Datenschutzgrundverordnung in Kraft. Ist sie auch auf schweizerische Unternehmen anwendbar, wenn und weil diese als Auftragsverarbeiter eines Verantwortlichen mit Niederlassung in der EU tätig sind oder umgekehrt Daten durch einen EU-Auftragsverarbeiter verarbeiten lassen?

Über die Sicherheit digitaler Coupons

Treueprogramme als Kundenbindungsmittel werden in der digitalen Welt zur Realität. Ebenfalls Realität ist, dass manche kommerziellen Anbieter bereits im Design ihrer digitalen Treueprogramme Sicherheitsfehler gemacht haben. Wie kann verhindert werden, dass Treuepunkte vervielfältigt und im schlimmsten Fall gegen Bargeld eingetauscht werden?

Mitarbeiterüberwachung: Der Fall Bărbulescu

Der EGMR hat im Entscheid Bărbulescu gegen Rumänien die konventionsrechtlichen Anforderungen an die Mitarbeiterüberwachung konkretisiert. Er nimmt dabei eine strenge Haltung ein. Übertreibt er damit? Ist die Überwachung der Mitarbeiter künftig unzulässig?

Digitalisierung braucht wirksamen Datenschutz

Die schrankenlose Digitalisierung wird dazu führen, dass niemand mehr unbeobachtet leben kann. Einen solchen digitalen Totalitarismus will niemand, weder einen staatlichen noch einen wirtschaftlichen. Darum muss die Digitalisierung verträglich für die Menschen und verträglich für die freiheitliche Gesellschaft umgesetzt werden. Nur Hand in Hand mit dem Datenschutz angegangen und verwirklicht, kann die Digitalisierung Erfolg bringen. Wer dies übersieht, hat schon verloren.

report

forum

Personendaten ohne Identifizierbarkeit?

Das Zauberwort «Singularisierung» ist seit der DSGVO in aller Munde. Ändert sich nun der Begriff des Personendatums?

David Rosenthal, lic. iur., Lehrbeauftragter an der Universität Basel, Counsel, Homburger AG, Zürich david.rosenthal@homburger.ch

Datenschutz betrifft nur Daten, die sich auf «identifizierbare» Personen beziehen. Der Beitrag zeigt, was das bedeutet und was noch als Personendatum gilt und was nicht.

Der Datenschutz wurde in den letzten Jahren stark an die Entwicklungen im Online-Bereich angepasst. Doch am zentralen Begriff der Personendaten wurde nichts geändert. Oder doch? Unter dem Stichwort der «Singularisierung» geistert die Auffassung herum, Daten müssten selbst dann als personenbezogen gelten und der Datenschutz eingehalten werden, wenn nicht ermittelt werden kann, um wen es bei den Daten geht. Ist der Begriff der Personendaten aufgeweicht worden?

Stellen Sie sich folgende Situation vor: Eine Sicherheitskamera nimmt nachts in einer menschenleeren, schwach beleuchteten Strasse auf, wie ein Mann mit Einkaufstüten den Gehsteig entlangläuft und auf einer Bananenschale ausrutscht, seine Tüten fallen lässt und alle Waren auf den Boden fallen. Er fällt so unglücklich, dass er mit seinem Hintern direkt auf einer Packung Eiern landet. Die Situation ist einmalig. Der Videoclip wird im Internet zum Hit, aber niemand weiss, wer der Mann ist, niemand kann ihn erkennen, und er hat sein Malheur auch niemandem erzählt. Darf der Videoclip geteilt werden? Unter dem geltenden Datenschutzgesetz (DSG): Ja. Es liegen keine Personendaten vor, da der Protagonist nicht zu identifizieren ist. Der Fall ist klar.

Und nun diese Situation: Eine Zeitung hat herausgefunden, wie sie die persönlichen Interessen der Leser ihrer Website aufgrund der Aufrufe von Artikeln genauestens ermitteln kann. Dazu wird bei jedem Leser ein Cookie[1] gesetzt. Einer Registrierung bedarf es hingegen nicht; die Zeitung will gar nicht wissen, wer die Personen sind, nur, was ihnen gefällt. Die Daten der Leser werden über Jahre gespeichert, deren Interessenprofil immer genauer. IP-Adressen werden keine gespeichert. Muss die Zeitung über diese Profilbildung auf der Website informieren? Findet das DSG Anwendung?

Auch hier ist die Antwort an sich klar: Es liegen keine Personendaten vor. Die Cookies erlauben die Wiedererkennung der Benutzer und die Profilbildung; eine Identifizierung der Leser ist jedoch nicht möglich und für die Zeitung auch gar nicht von Interesse. Doch diese Antwort wird vielen gefühlt wesentlich schwerer fallen, wird doch ein gläserner Leser erzeugt. Die Zeitung kennt mit der Zeit die geheimsten Interessen ihrer Benutzer, was es ihr wiederum erlaubt, sie aufgrund ihrer Persönlichkeit zu «manipulieren», etwa durch entsprechende Werbung Dritter. Auch dies «umschifft» das DSG, da keine Personendaten weitergegeben werden. Weitergedacht lässt sich diese Technik auch benutzen, um Personen unterschiedlich zu behandeln, die einen besser, die anderen schlechter. Identifizierbar sein müssen sie dafür nicht.

Das zweite Beispiel macht klar, warum wir uns instinktiv unwohl fühlen: Wir fürchten eine Diskriminierung aufgrund der Bearbeitung unserer Daten. Was also liegt näher, als hierzu den Datenschutz anzurufen? Dagegen spricht zunächst nur, aber immerhin, ein formales Element: Der Schutz vor Diskriminierung durch andere Private ist im Schweizer Recht wie auch sonst die Drittwirkung von Grundrechten die Ausnahme[2]. Dagegen spricht aber auch, dass es schon aus systematischen Gründen unsauber und falsch ist, unerwünschte Diskriminierungen unter Privaten über den Datenschutz zu verhindern, nur weil dabei Daten im Spiel sind. Da Daten heute überall das Mittel zum Zweck sind, ist dies natürlich verlockend. Doch zu regeln sind solche Fälle über jene Gesetzgebung, die dem betreffenden Sachverhalt wirklich naheliegt: Soll eine Diskriminierung zum Beispiel von Versicherten verhindert werden, so ist dies im Versicherungsrecht zu klären, und nicht über eine allgemeine Regel im Datenschutz, deren Streu- und Breitenwirkung für niemanden vorhersehbar ist und eine Klärung

der Sachgerechtigkeit und angemessene politische Willensbildung unmöglich ist.

Ausweitung des Begriffs der Personendaten?

In Datenschutzkreisen wird indes versucht, Situationen wie im zweiten Beispiel auf andere Weise zu erfassen. Benutzt wird ein Kniff: Es wird argumentiert, dass die betroffene Person im zweiten Beispiel trotz allem identifiziert bzw. identifizierbar ist, weil zwar ihr Name nicht bekannt ist, jedoch zahlreiche andere Angaben und sie sich anhand ihres Profils auch klar von anderen Personen unterscheiden lässt. Die Person ist damit «singularisiert», und dies soll genügen, um als identifiziert bzw. identifizierbar zu gelten. Zur Unterstützung wird angeführt, dass nun auch die EU-Datenschutzgrund-Verordnung (DSGVO) in ihrer Legaldefinition des Begriffs der personenbezogenen Daten[3] auf eine Identifikation durch «Online-Kennungen» wie Cookies oder IP-Adressen verweist; das dadurch ermöglichte Profiling wie im zweiten Beispiel wird sogar ausdrücklich erwähnt[4]. Hinzu kommt, dass in Teilen der EU das Konzept der Drittwirkung wesentlich stärker etabliert wird und es beinahe zum Selbstverständnis gehört, dass auch der Datenschutz vor einer Ungleichbehandlung auch unter Privaten schützen soll; die Qualifikation der betreffenden Daten als Personendaten ist das Mittel und der Weg dazu.

Doch ist dieser Kniff zulässig? Genügen Daten einer singularisierten Person, um als Personendaten zu gelten? Hierzu muss der Rechtsbegriff der Personendaten genauer analysiert werden. Angelpunkt ist dabei die Frage der Bestimmbarkeit, denn als Personendaten gelten heute alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen[5]. Das soll sich auch im revidierten DSG[6] nicht ändern[7]. Die «Bestimmung» einer Person meint deren Identifizierung[8]. Im Schweizer Recht ist zu prüfen, ob ein unverhältnismässiger Aufwand betrieben werden muss, um ein bestimmtes Datum einer bestimmten Person zuordnen zu können. Ist dies der Fall, gelten die Daten als anonym und somit nicht (mehr) als Personendaten, auch wenn eine theoretische Möglichkeit der (Re-)Identifikation bestehen sollte[9]. Dieser Test ist allgemein anerkannt und findet sich auch in anderen Schweizer Erlassen. So definiert Art. 25 Abs. 1 Humanforschungsverordnung[10] die Anonymisierung als Vorgang, bei welchem alle «Angaben, die in ihrer Kombination die Wiederherstellung des Bezugs zu einer Person ohne unverhältnismässigen Aufwand erlauben, irreversibel unkenntlich gemacht oder gelöscht werden». Insbesondere unkenntlich gemacht oder gelöscht werden müssen Namen, Adresse, Geburtsdatum und eindeutig kennzeichnende Identifikationsnummern. Der EDÖB hat in Stellungnahmen anonymisierte Daten ebenfalls als solche Daten definiert, «die überhaupt nicht mehr oder nur noch mit ausserordentlichem Aufwand» mit einer bestimmten Person verknüpft werden können[11].

Der Schutz vor Diskriminierung durch andere Private ist im Schweizer Recht wie auch sonst die Drittwirkung von Grundrechten die Ausnahme.

Die Europäische Union folgt einem vergleichbaren Ansatz, und zwar sowohl in der heute noch geltenden Datenschutzrichtlinie[12] wie auch in der DSGVO, die ab Mai 2018 gelten wird. Demnach sind nur, aber immerhin, jene Mittel der direkten oder indirekten Identifizierung einer Person zu berücksichtigen, die «nach allgemeinem Ermessen wahrscheinlich genutzt werden»[13]. Hierzu müssen «alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand», herangezogen werden, ebenso die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen[14].

Keine ergebnisorientierte Auslegung

Nun besteht insoweit Einigkeit, als das Erfordernis der Identifizierbarkeit nicht bedeutet, dass der Datenbearbeiter in der Lage sein muss,

Kurz & bündig

Am Begriff des Personendatums hat sich auch mit der DSGVO nichts geändert. Es gilt nach wie vor der «relative» Ansatz, der darauf abstellt, ob derjenige, der Zugang zu bestimmten Daten hat, die davon betroffenen Personen identifizieren kann oder nicht. Das gilt auch in der EU, wo dies der EuGH mit seinem Entscheid betreffend IP-Adressen jüngst bestätigt hat. Daran ändert auch der Begriff der «Singularisierung» nichts. Ein Datensatz singularisiert eine Person, wenn er wie ein Fingerabdruck so speziell ist, dass er sich nur auf sie beziehen kann, auch wenn nicht bekannt ist, um wen es geht. Wie etwa bei genetischen Daten. Die DSGVO erwähnt die Singularisierung zwar als Indiz für eine Identifizierbarkeit, aber sie alleine genügt eben nicht. Hierzu stellt der Beitrag den «Referenzdaten-Test» vor: Demnach liegen Personendaten vor, wenn zwischen den fraglichen Daten und dem Bearbeiter bereits vorliegenden oder zugänglichen Datensätzen einer einzelnen, realen Person eine Übereinstimmung hergestellt werden kann. Genetische Daten und IP-Adressen sind daher nie per se Personendaten.

den Namen, das Geburtsdatum oder etwa die Adresse der betroffenen Person zu kennen oder die Person sogar kennen oder sie kontaktieren können muss. Keine Einigkeit besteht hingegen in der Frage, wie viele individualisierende Elemente erforderlich sind, um von einer Identifizierung bzw. Identifizierbarkeit auszugehen. Die Vertreter der Singularisierung[15] stellen sich auf den Standpunkt, dass jede eineindeutige Individualisierung genügt. Auf dieser Basis werden in der EU heute zum Beispiel (anders als in der Schweiz[16]) personalisierte Cookies bereits als Personendaten betrachtet, auch wenn der Betreiber einer Website keinerlei Möglichkeiten hat, herauszufinden, wer hinter einem Cookie steckt oder dies sogar mehrere Personen sein können, die sich einen Browser teilen. Sie machen analog dem zweiten Einführungsbeispiel geltend, ein Cookie erlaube die Profilbildung und mache es daher nötig, die diesbezügliche Datenbearbeitung datenschutzrechtlich zu regulieren. Sie begründen dies damit, dass auch wenn die betroffenen Personen nach traditionellem Verständnis anonym bleiben, die Datenbearbeitung sie direkt betrifft und sie damit in ihrer Persönlichkeit verletzen kann. Sie argumentieren also mit der *Wirkung* der Bearbeitung von Daten. Erfolgt diese individualisiert auf eine ganz bestimmte Person ausgerichtet, so liegen Personendaten vor.

Kaum jemand hat eine klare, reflektierte und vertiefte Vorstellung davon, was sich abseits von Standardsituationen hinter dem Begriff der «Identifizierung» einer Person wirklich verbirgt.

Nach der hier vertretenen Auffassung ist ein solches, rein ergebnisorientiertes Begriffsverständnis abzulehnen. Es folgt dem Gedanken, dass der Datenschutz dort gelten soll, wo er gelten sollte, was jeglicher Rechtssicherheit entbehrt; die möglichen Auswirkungen einer Datenbearbeitung können kein entscheidendes Kriterium dafür sein, ob es sich bei bestimmten Daten um Personendaten handelt und daher das Datenschutzrecht zur Anwendung gelangt. Doch auch in der Sache selbst ist es nicht zielführend, eine Person bereits dann als identifiziert oder identifizierbar zu betrachten, wenn die sie betreffenden Daten sich von den Daten aller anderen Personen unterscheiden, also ein eineindeutiger Datensatz vorliegt. Würde diesem Ansatz gefolgt, müsste konsequenterweise auch die Videoaufnahme im ersten Beispiel als Personendatum gelten: Die Situation ist einmalig. Obwohl die Person darin zweifellos singularisiert ist, steht ihre Anonymität ausser Frage. Dass aber auf anonyme Daten der Datenschutz nicht anwendbar ist, stellen auch die Vertreter der Singularisierung jedenfalls de lege lata nicht infrage.

Doch welche weiteren Voraussetzungen müssen zur Singularisierung einer Person in einem Datensatz hinzutreten, damit Personendaten vorliegen? Diese Frage ist bisher nicht autoritativ beantwortet worden, weder in der Schweiz noch in der EU, und ist auch wissenschaftlich wenig eingehend erörtert. Das erstaunt etwas, zumal es sich doch um den zentralsten Begriff des Datenschutzes handelt. Wer jedoch mit Fachleuten spricht, merkt rasch, dass kaum jemand eine klare, reflektierte und vertiefte Vorstellung davon hat, was sich abseits von Standardsituationen hinter dem Begriff der «Identifizierung» einer Person wirklich verbirgt und wie Fallkonstellationen darunter sauber subsumiert werden können[17]. Entsprechend unsystematisch ist die Vorgehensweise in der Praxis.

Der Referenzdaten-Test

Ein Ansatz, der sich allerdings bewährt und bisher als vergleichsweise zuverlässig erwiesen hat, ist eine Methode, die hier als «Referenzdaten-Test» bezeichnet wird. Sie stellt die Frage, ob zwischen (a) den zur Diskussion stehenden Daten (dem *Prüfdatensatz*) und (b) den Daten einer einzelnen, realen Person, die dem Datenbearbeiter unabhängig vom Prüfdatensatz entweder schon vorliegen oder ihm zugänglich sind (der *Referenzdatensatz*), soweit eine Übereinstimmung besteht (ein *Match*), dass ein eineindeutiger Bezug zwischen den beiden Datensätzen möglich ist. Ist dies der Fall, so liegen Personendaten vor.

Die Anwendung sei am Beispiel von Gensequenzen, wie sie in der Forschung verwendet werden, verdeutlicht. Ist eine Gensequenz hinreichend lang und wird sie damit zum einmaligen «Fingerabdruck» der betreffenden Person; damit ist diese singularisiert. Nach dem Referenzdaten-Test sind solche Gendaten trotzdem so lange als anonym zu betrachten und keine Personendaten, als es nicht möglich ist, über eine Gendatenbank oder ein biologisches Sample sie tatsächlich mit einer einzelnen, realen (und damit auf irgendeine Weise vorbekannten) Person zu verknüpfen. Genetische Daten sind somit nicht *per se* Personendaten, auch wenn dies de lege ferenda von Vertretern der Singularisierung teilweise gefordert wird[18]. Diese Forderung wurde allerdings selbst im Entwurf für ein revidiertes DSG (E-DSG)[19] nicht übernommen: Genetische Daten gelten dem-

nach zwar als besonders schützenswert nach Art. 4 Bst. c Ziff. 3 E-DSG, doch ist unabhängig davon – wie bei allen besonderen Datenkategorien gemäss Art. 4 Bst. c E-DSG – erforderlich, dass es sich um Personendaten handelt.

Der Bundesrat wendete den Referenzdaten-Test allerdings auch schon an, so mit Bezug auf die Frage, wann biologisches Material hinreichend anonymisiert gelten kann. Dazu führte er in seiner Botschaft zum Humanforschungsgesetz an, dass es zwar möglich sei, aus biologischem Material genetische Daten zu gewinnen, die theoretisch über Referenzdaten verglichen werden könnten. Von einem Vorhandensein solcher Referenzdaten bzw. Vergleichsproben könne jedoch nur in seltenen Fällen ausgegangen werden, und der Zugriff auf diese dürfe in aller Regel jedoch praktisch unmöglich oder rechtlich unzulässig sein[20].

Die «Halbwertszeit» von Daten und andere ungeklärte Fragen

Ob der Referenzdaten-Test tatsächlich in allen Fällen tauglich ist, sei an dieser Stelle offengelassen. So sind gewisse Fragen bisher erst ansatzweise geklärt, so etwa, über welchen Zeitraum das Verfügbarwerden von Referenzdaten zu prüfen ist. Soll dies nur für jene Zeitdauer getan werden, in welchem die Daten einen Nutzwert haben und daher ein Interesse an der Identifikation besteht? Oder kommt es darauf an, wie lange sie der betroffenen Person «schädlich» sein können? Klar ist nur, dass jedes Datum über eine «Halbwertszeit» verfügt und diese seine Identifizierbarkeit mit der Zeit abnehmen lässt, weil auch das Interesse an einer personenbezogenen Nutzung und damit der Identifikation abnimmt.

Ist uns eine Person bekannt (und daher identifizierbar bzw. identifiziert), die wir von der täglichen Pendlerfahrt vom Sehen her kennen? Muss uns ihr Name bekannt sein?

Nicht abschliessend beantwortet ist auch die Frage, wie genau die Person vorbekannt sein muss, auf die sich der Referenzdatensatz bezieht. Wir alle glauben zwar ein Verständnis dafür zu haben, wann für uns eine Person als uns «bekannt» gilt, aber eine generell-abstrakte Regel zu definieren, wann dies der Fall ist, ist enorm schwierig. Ist uns eine Person bekannt (und daher identifizierbar bzw. identifiziert), die wir von der täglichen Pendlerfahrt vom Sehen her kennen? Muss uns ihr Name bekannt sein? Und was, wenn wir zwar den

Fussnoten

1 Ein nicht sprechender, für jeden Benutzer vom Server neu generierter, eineindeutiger Code, der im Browser des Benutzers gespeichert wird und der Website zugeordnet ist. Bei jedem neuerlichen Besuch der Website kann der Server den Code abrufen und erkennt den Benutzer als einen früheren Benutzer wieder und kann so die Aktivitäten des Benutzers über einen längeren Zeitraum überwachen.

2 Art. 35 Abs. 3 BV sieht immerhin vor, dass die Behörden dafür sorgen sollen, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden. Dies gilt zum Beispiel im Bereich des Arbeitsrechts oder in gewissen Konstellationen des Kartellrechts.

3 Art. 4 Ziff. 1 DSGVO.

4 Erwägung 30 der DSGVO.

5 Art. 3 Bst. a DSG.

6 Gemäss dem Entwurf der Botschaft des Bundesrates vom 15. September 2017 (Botschaft), zitiert als E-DSG; zum Zeitpunkt dieses Artikels existierte noch keine im Bundesblatt publizierte Fassung der Botschaft und des Entwurfs (vgl. dazu <http://swissblawg.ch/2017/09/entwurf-des-datenschutzgesetzes.html>).

7 Art. 4 Bst. a E-DSG.

8 Botschaft, S. 81.

9 BBl 1988 II 444 f. Ziff. 221.1

10 SR 810.301.

11 Vgl. etwa EDÖB, Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS, Version 15.4.2014, S. 5.

12 Richtlinie 95/46/EG.

13 Erwägung 26 der DSGVO.

14 Ebd.

15 Sie bildeten bisher keine klare Lehre. Der Autor begegnet der Ansicht, die Singularisierung genüge zur Bestimmbarkeit jedoch in etlichen Aussagen von Datenschützern und anderen Fachleuten. Allerdings erwecken diese in aller Regel den Eindruck, nicht das Ergebnis einer wissenschaftlich vertieften Auseinandersetzung mit dem Thema zu sein. Auch sind dem Autor keine wissenschaftlichen Schriften zu dieser Problematik bekannt.

16 Vgl. Art. 45c FMG.

17 Das tut auch die Botschaft nicht (S. 81). Sie setzt den Begriff vielmehr voraus.

18 So etwa im Rahmen der Vernehmlassung zur Revision des Gesetzes über genetische Untersuchungen am Menschen (GUMG), vgl. dazu <https://www.bag.admin.ch/bag/de/home/themen/mensch-gesundheit/biomedizin-forschung/genetische-untersuchungen/aktuelle-rechtsetzungsprojekte1.html>.

19 Text: <http://swissblawg.ch/2017/09/entwurf-des-datenschutzgesetzes.html>.

20 BBl 2009 8096.

21 BGE 136 II 508, E. 3.

22 Entscheid des EuGH vom 19. Oktober 2016 (C-582/14), Rz. 44–49.

23 Ebd., Rz. 33–34, mit Verweis auf den Entscheid des EuGH vom 24. November 2011 (C-70/10).

24 BGE 136 II 508.

25 Erwägung 26 der DSGVO («To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out»; der deutsche Text spricht vom «Aussondern»).

Namen und die Anschrift der Insassen eines bestimmten Zuges kennen, sie für uns aber nicht relevant sind, nicht persönlich bekannt und es auch nie sein werden und wir mit ihnen auch keine Interaktion haben werden? Erforderlich wird immerhin sein, dass Gewissheit besteht, dass sich der Referenzdatensatz auf eine Person bezieht, die es wirklich gibt und nur auf sie, also z.B. nicht auf eine Gruppe von Personen, die sich eine Identität teilen.

Wird eine Person durch einen Datensatz singularisiert, liegen damit noch keine Personendaten vor. Es müssen weitere Voraussetzungen erfüllt sein.

Klar ist auch, dass im Zusammenhang mit diesen Fragen noch eine weitere Differenzierung zu beachten ist. Jedenfalls unter dem Schweizer Recht genügt selbst die Existenz von passenden Referenzdaten nicht, um bezüglich der Prüfdaten von Personendaten auszugehen. Nach geltendem Recht ist auch erforderlich, dass die Personen, die Zugang zu den Prüfdaten haben, nicht nur die Möglichkeit haben, auf die Referenzdaten zuzugreifen (oder die betroffene Person sonst identifizieren können), sondern sie auch ein Interesse daran haben, den dafür nötigen Aufwand zu betreiben. Dies wird gemeinhin als der «relative» Charakter des Begriffs des Personendatums bezeichnet. Er wurde durch die bundesgerichtliche Rechtsprechung bestätigt[21] und soll auch im Rahmen der Revision des DSG nicht abgeschafft werden.

Der «relative» Ansatz gilt auch in der EU

Im Gegensatz dazu wird in der EU in Datenschutzkreisen teils noch immer der «absolute» Ansatz vertreten, wonach es genügt, wenn es für eine beliebige Person möglich ist, die Prüfdaten einer bestimmten Person zuzuordnen und sie so zu identifizieren. Die Vertreter des absoluten Ansatzes liegen mit ihrer Ansicht sehr nahe an jenem der Singularisierung als hinreichende Voraussetzung einer Identifizierung. Allerdings erteilte der Europäische Gerichtshof (EuGH) dieser Ansicht in seinem viel beachteten Entscheid vom 19. Oktober 2016 eine Absage.

Der Fall handelte von IP-Adressen, die der Betreiber einer Website von seinen Besuchern aufzeichnete. Jede dieser IP-Adressen kann vom Provider einem bestimmten Kunden zugeordnet werden. Dieses Wissen des Providers genügte allerdings nicht, um die IP-Adressen auch aus der Sicht des Betreibers der Website als Personendaten erscheinen zu lassen. Hierfür müsse zuerst geprüft werden, ob die Möglichkeit, die aufgezeichnete IP-Adresse mit den Zusatzinformationen zu verknüpfen, über die der Internetzugangsanbieter verfügt, «ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann», d.h., ob es wahrscheinlich ist, dass der Betreiber der Website es einsetzt[22]. Dies wurde im vorliegenden Fall bejaht, weil es ihm nach dem anwendbaren Recht möglich sei, im Falle von Cyberattacken die Person zu identifizieren, und er die Daten just zu diesem Zweck sammelte. Es war für das Gericht aber auch klar, dass die IP-Adressen für den Internetzugangsanbieter in jedem Fall Personendaten sind, da dieser jederzeit die Mittel hatte, um den Kunden zu identifizieren[23]. Der EuGH wendete damit faktisch ebenfalls den Referenzdaten-Test an, und zwar basierend auf der relativen Methode. Die Singularisierung, die in jedem Fall gegeben war, genügte somit nicht zur Annahme von Personendaten. Der Entscheid des EuGH entspricht diesbezüglich einem früheren Entscheid des Bundesgerichts zur selben Thematik[24]. Die Rechtslage in der EU und der Schweiz ist somit vergleichbar.

Auch unter der DSGVO ergibt sich nichts anderes. Sie erwähnt die Singularisierung zwar in den Erwägungen zur Legaldefinition des Personendatums, erachtet sie aber offenbar ebenfalls nur als Indiz für eine Identifizierbarkeit[25]. Daran ändert auch der Umstand nichts, dass die Legaldefinition wie erwähnt nebst dem Namen einer Person auch auf «Kennnummern» verweist, die zu einer Identifizierbarkeit führen. Sie können zwar – wo mit einem Datensatz verknüpft – zur Singularisierung der betreffenden Person führen, weil ihre Daten mittels Kennnummer von jenen aller anderen Personen unterschieden werden können. Trotzdem verlangt auch die Legaldefinition der DSGVO, dass sie tatsächlich zur Identifikation oder Identifizierbarkeit führt. Daran ändert bei genauer Betrachtung auch die zitierte Erwägung 30 der DSGVO nichts: Sie besagt, dass IP-Adressen und Cookies zwar zu einer Identifizierung und zur Profilierung führen *können,* stellt aber nicht fest, dass damit zwangsläufig auch Personendaten vorliegen. Im zweiten (Schul-) Beispiel aus der Einführung liegen jedenfalls nach der hier vertretenen Ansicht ebenfalls keine Personendaten vor. Solche würden erst dann geschaffen – wie in der Praxis wohl häufig der Fall –, wenn die Profile mit einer Registrierung eines Lesers verknüpft werden. Wie spezifisch diese Registrierung sein muss, sei an dieser Stelle aus Platzgründen nicht weiter erörtert.

Fazit

Wird eine Person durch einen Datensatz singularisiert, liegen damit noch keine Personendaten vor. Es müssen weitere Voraussetzungen erfüllt sein, wie sie etwa durch den oben beschriebenen Referenzdaten-Test geprüft werden können. Dies gilt sowohl unter dem bestehenden Recht wie auch unter der DSGVO und dem Entwurf für ein revidiertes DSG. Allerdings ist vermehrt damit zu rechnen, dass im Sinne einer ergebnisorientierten Auslegung und ohne vertiefte Reflexion die Vorschriften des Datenschutzes auch auf Fälle angewandt werden, die de lege lata nicht darunterfallen. Eine solche *wirkungsorientierte* Definition von Personendaten mag vor dem Hintergrund der Entwicklungen der Informationsgesellschaft interessant und im Ergebnis vielleicht sogar verständlich sein. Sauber ist sie jedoch nicht. In der laufenden Datenschutzrevision wurde die Chance einer Anpassung des Systems zudem bereits verpasst. ■

Schulthess §

Herausgeber:
Dr. iur. Bruno Baeriswyl,
Prof. Dr. iur. Beat Rudin,
Prof. Dr. Bernhard M. Hämmerli,
Prof. (em.) Dr. iur. Rainer J. Schweizer,
Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion:
Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin

Sprache: deutsch

☑ **JA,** ich profitiere vom **Mini-Abo** von **digma** und erhalte **2 Ausgaben** zum Kennenlernpreis von nur **CHF 58.–** (inkl. MWST und Versandkosten).

Vorname / Name

Firma

Strasse / Nr.

PLZ / Ort

E-Mail

Datum / Unterschrift

Abonnement-Bedingungen

Wenn ich digma danach weiterlesen möchte, muss ich nichts weiter tun und erhalte im Jahresabonnement 4 Printausgaben zum Preis von CHF 174.00 (inkl. MWST, zzgl. CHF 6.00 Versandkosten). Falls ich digma nicht weiter beziehen möchte, melde ich mich spätestens 7 Tage nach Erhalt der 2. Testausgabe bei Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich, E-Mail: service@schulthess.com, Fax: +41 (0)44 200 29 28.

A

Nicht frankieren
Ne pas affranchir
Non affrancare

Geschäftsantwortsendung Invio commerciale-risposta
Envoi commercial-réponse

Schulthess Juristische Medien AG
Kundenservice
Zwingliplatz 2
Postfach 2218
8021 Zürich