

DATENSCHUTZ

KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Big Data

Wie Big Data Katastrophenhilfe unterstützt

Interview mit Mila Romanoff, Datenschutzspezialistin Global Pulse

Big Data @ Telekommunikationsnetzbetreiber

Klaus Steinmaurer

Der Weg von personenbezogenen zu anonymen Daten

Viktoria Haidinger

Big Data: datenschutzrechtliche Lösungsansätze

Rainer Knyrim

Open Data sorgenfrei publizieren

Brigitte Lutz

Datenschutz-GVO: Der Datenschutzbeauftragte

Hans-Jürgen Pollirer

Kameras im Wald

Thomas Sonnenschein



Rainer Knyrim
Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte

Big Data: datenschutzrechtliche Lösungsansätze

Anonymisierung; Zweckbindung; Zustimmung; Forschungsprivileg. Big Data als eine Art neuer „Wundertechnologie“ ist als Schlagwort derzeit in aller Munde; dabei sollen Daten – das „Öl des 21. Jahrhunderts“ – in bisher noch nicht dagewesenem Umfang nutzbringend ausgewertet werden. Dieser Beitrag beschäftigt sich mit den datenschutzrechtlichen Fragen von Big Data und mit Lösungsansätzen dafür.

Einleitung

Big Data bezeichnet Datenmengen, die zu groß oder zu komplex sind oder sich zu schnell ändern, um sie mit händischen und klassischen Methoden der Datenverarbeitung auszuwerten. Mit Big Data wird ergänzend auch oft der Komplex der Technologien beschrieben, die zum **Sammeln und Auswerten dieser Datenmengen verwendet werden**.¹

Die Branchen, in denen Big Data eingesetzt wird, werden immer zahlreicher, als Beispiele² seien etwa Standortsuchen für Geschäftsansiedelungen³, der Gesundheitsbereich, Verkehr⁴, Controlling⁵ oder auch Hilfsprojekte der Vereinten Nationen⁶ genannt.

Datenschutzfragen bei Big Data Personenbezogen, pseudonymisiert oder anonymisiert?

Eine der Grundfragen bei der Arbeit mit großen Datenmengen ist, ob diese Arbeit

in personenbezogener, pseudonymisierter oder anonymisierter Form erfolgt. Erfolgt sie von Beginn bis zum Ergebnis in **personenbezogener Form**, dann ist das **DSG voll anwendbar** und es treten die nächstgenannten Probleme der Zweckbindung und Zustimmung auf, ebenso wie alle Themen des formellen Datenschutzrechts.⁷ Erfolgt die Verarbeitung in **pseudonymisierter Form**, dann ist diese **im DSG 2000 privilegiert**: Indirekt personenbezogene Daten sind bei der **Meldepflicht** sowie beim **internationalen Datenverkehr** privilegiert und bei der **Verwendung indirekt personenbezogener Daten** kann keine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen entstehen. Erfolgt die Verarbeitung in **anonymisierter Form**, sodass jeglicher Personenbezug entfernt ist, dann fällt die **Datenverarbeitung überhaupt aus dem DSG heraus**.⁸

Daher muss zunächst bei jedem Big Data-Projekt festgestellt werden, **in welcher**

Form die Daten verarbeitet werden, und zwar **in allen Verarbeitungsschritten** von der Erhebung und Zusammenführung über die Aufbereitung bis zum Ergebnis der Verarbeitung. Dabei muss hinterfragt werden, ob die Daten – wie oft zunächst behauptet – **tatsächlich ausreichend pseudonymisiert oder anonymisiert wurden**.

¹http://de.wikipedia.org/wiki/Big_Data. Siehe auch den Beitrag von Steinmaurer zur Definition von Big Data in diesem Heft Dako 2015/33. ²Weitere Beispiele siehe bei Mayer-Schönberger/Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (2013). ³Bspw bietet das Unternehmen Streetlight Data in den USA an, aus Bewegungsdaten von Mobiltelefonen, GPS-Daten aus Fahrzeugen, die mit Daten des US Census (Volkszählung) verknüpft werden, für praktisch jeden Punkt in den USA feststellen zu können, welche potenziellen Kunden dort vorbeifahren, damit Geschäftsansiedelungen entsprechend zielgruppenorientiert geplant werden können; www.streetlightdata.com/technology/. Siehe dazu auch den Artikel von Steinmaurer in diesem Heft Dako 2015/33. ⁴Zeger, Big Data statt Big-Foot? – Die (Daten)Zukunft der Mobilität, ZVR 2013/258. ⁵Gänßlen/Losbichler, Big Data – ein Segen für das Controlling? CFOaktuell 2014, 144. ⁶Siehe das Interview mit Romanoff von UN Global Pulse in diesem Heft Dako 2015/32. ⁷Insb allfällige DVR-Meldepflicht und Genehmigungspflicht bei internationalem Datenverkehr. ⁸Siehe dazu Knyrim, Datenschutzrecht² Kap 2.6.1.

Die Form der Datenverarbeitung ist die erste Frage, wenn es um die Zulässigkeit von Big Data geht.

Zweckbindung?

Ein weiteres datenschutzrechtliches Problem⁹ ist das **Zweckbindungsprinzip**. Laut § 6 Abs 1 Z 2 DSGVO dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Dieser Grundsatz steht somit der Idee von Big Data diametral entgegen, möglichst viele Daten aus verschiedensten Datenanwendungen miteinander zu kombinieren und für einen neuen Zweck zu verwenden. Laut dem Zweckbindungsgrundsatz darf schon die Ermittlung von Daten nur dann geschehen, wenn der Zweck der Ermittlung von vornherein definiert, dh festgelegt wurde. Dies ist eines der Grundprobleme von Big Data: Oft kommt man erst später auf die Idee, Daten aus einer bestehenden und für eine ganz andere geschaffene Datenanwendung für Big Data zu anderen Zwecken weiterzuverwenden, zB große Mengen an Geschwindigkeitsdaten aus GPS-Navigationssystemen von Autos als Grundlage für die Aufstellung von Radargeräten durch die Polizei zu verwenden.¹⁰

Das Problem der Zweckbindung kann nur durch eine wirkliche Anonymisierung oder Pseudonymisierung umgangen werden, andernfalls bieten sich nur die folgenden datenschutzrechtlichen Lösungsansätze an, um Big Data – allenfalls in eingeschränkter Form – datenschutzrechtskonform durchzuführen.

Datenschutzrechtliche Lösungsansätze für Big Data Zustimmung

Ist es nicht, wie oben ausgeführt, möglich, die Daten ausreichend zu anonymisieren oder pseudonymisieren, so bietet sich an, die Zustimmung der Betroffenen zur Verarbeitung der Daten in Big Data einzuholen. Wie weiter oben ausgeführt, muss eine Zustimmung im Datenschutzrecht jedoch „in Kenntnis der Sachlage für den konkreten Fall“ erfolgen. Genau dies ist aber das Problem bei Big Data: Meist weiß man zu Beginn der Datenverarbeitung noch gar nicht, dass die Daten später für Big Data weiterverwendet werden sollen, und kann

daher keine ausreichend präzise Zustimmungserklärung formulieren. Die Einholung von Zustimmungserklärungen für Big Data ist somit nur dann sinnvoll, wenn zu Beginn der ursprünglichen Datenverarbeitung bereits klar ist, in welcher Form genau die Daten durch wen für welche Big Data-Anwendungen weiterverwendet werden sollen.

Die Zustimmungserklärung muss daher neben dem ursprünglichen Zweck auch die weitere Nutzung für Big Data exakt und abschließend umschreiben.

Wissenschaftliche Forschung und Statistik

Einen weiteren datenschutzrechtlichen Lösungsansatz für Big Data kann § 46 DSGVO beinhalten,¹¹ der Regelungen über die spätere Weiterverwendung von Daten für wissenschaftliche Forschung und Statistik enthält.¹²

Auftraggeber dürfen Big Data nach § 46 Abs 1 DSGVO zu wissenschaftlicher Forschung oder statistischer Untersuchung aber nur betreiben, wenn das gewünschte Ergebnis anonymisiert ist. Sie dürfen dazu als Datenquelle entweder personenbezogene öffentliche Daten oder personenbezogene eigene Daten verwenden, die sie zu anderen Zwecken ermittelt haben. Hier ist ausnahmsweise eine spätere Zweckänderung der Datenverarbeitung zulässig. Daten von Dritten, also solche, die er nicht selbst erhoben und verarbeitet hat, darf der Auftraggeber hingegen nur in indirekt personenbezogener Form, also pseudonymisiert verwenden, die Verwendung in dieser Form ist aber jedenfalls zulässig. Zu beachten ist allerdings, dass Zweck einer solchen Big Data-Anwendung nur konkrete (punktuelle) Auswertungen bestehender Datenbestände für wissenschaftliche Forschung oder Statistik sein können, die unter Anwendung wissenschaftlicher Methoden durchgeführt werden muss.¹³ Denkbar wäre somit, dass ein Unternehmen statistisch die durchschnittliche Kundenzufriedenheit mit einzelnen Unternehmensprodukten ermittelt, in dem sie die Kundenkorrespondenz einmalig auswertet. Unzulässig wäre hingegen nach dieser Bestimmung die laufende Überführung von personenbezo-

genen Daten in eine Big Data-Anwendung.¹⁴

HINWEIS

Genügt dies dem Auftraggeber nicht, so hat er nach § 46 Abs 2 DSGVO ua die Möglichkeit, Daten mit Zustimmung der Betroffenen oder aufgrund einer Genehmigung der Datenschutzbehörde für wissenschaftliche Forschung und Statistik zu verwenden.

Diese Bestimmung kann zur Anwendung kommen, wenn der Auftraggeber zB Daten von Dritten nicht in anonymisierter oder pseudonymisierter Form, sondern in personenbezogener Form verwenden möchte¹⁵ oder er sie für mehr als bloß einmalige Untersuchungen verwenden möchte. Sofern es keine besonderen gesetzlichen Vorschriften gibt, ist dies allerdings nur mit Zustimmung des Betroffenen – siehe dazu bereits oben – oder mit Genehmigung der Datenschutzbehörde erlaubt. Die Genehmigung der Datenschutzbehörde muss vom Auftraggeber beantragt werden, erfolgt in Bescheidform¹⁶ und wird nur unter bestimmten Voraussetzungen erteilt. „Knackpunkt“ für eine Genehmigung durch die Behörde ist allerdings, dass an der wissenschaftlichen Forschung oder Statistik ein öffentliches Interesse besteht. Bei rein privatwirtschaftlichen, kommerziellen Big Data-Anwendungen, insb im Bereich des Marketing oder Vertriebs wird ein solches nur sehr schwer bis gar nicht zu argumentieren sein. Eine Genehmigung der Datenschutzbehörde für Big Data wird daher voraussichtlich nur im

⁹Big Data beinhaltet noch eine Reihe weiterer Probleme, wie etwa die Datensicherheit oder den Grundsatz der Datensparsamkeit, die hier aus Platzgründen jedoch nicht erörtert werden können; siehe zu diesen zB die Ausführungen zu Big Data-Sicherheit und Prävalenzfehlern bei Big Data in Feiler/Fina, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303, sowie Dohr/Pollirer/Weiss/Knyrim, DSGVO § 6 Anm 6. ¹⁰Dies hat der Navigationsgerätehersteller TomTom in den Niederlanden gemacht, www.spiegel.de/netzwelt/gadgets/standortsuche-fuer-radarfallen-tomtom-entschuldigt-sich-fuer-deal-mit-der-polizei-a-759464.html. ¹¹So auch Kotschy in einem Vortrag auf der 35. Internationalen Konferenz der Datenschutzbehörden im September 2013 in Warschau. ¹²Siehe weiterführend dazu auch Suda, Datenanwendung für wissenschaftliche Forschung und Statistik, in Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 293 ff, und Jahnel, Handbuch Datenschutzrecht (2010) 437 ff. ¹³ErläutRV zu § 46 DSGVO 2000. ¹⁴Feiler/Fina, Datenschutzrechtliche Schranken für Big Data, MR 2013, 303 (304). ¹⁵Nach § 46 Abs 5 DSGVO ist allerdings auch in jenen Fällen, in welchen gem den vorstehenden Bestimmungen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in personenbezogener Form zulässig ist, der direkte Personenbezug unverzüglich zu verschlüsseln, wenn in einzelnen Phasen der wissenschaftlichen oder statistischen Arbeit mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann, und der Personenbezug der Daten ist gänzlich zu beseitigen, sobald er für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig ist. ¹⁶Dohr/Pollirer/Weiss/Knyrim, DSGVO § 46 Anm 11. Die Datenschutzbehörde kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

Bereich der öffentlichen Verwaltung, öffentlich geförderter Forschungsprojekte oder bei der Forschung mit öffentlichem Interesse zu erlangen sein.

Zusammenfassung

Zusammengefasst ergeben sich im Wesentlichen¹⁷ nur die folgenden Möglichkeiten, mit Big Data zu arbeiten:

- Mit **Ausgangsdaten in völlig anonymisierter Form**, wobei es dann auch nur völlig anonymisierte Ergebnisse geben kann;
- wenn die **Zustimmung der Betroffenen eingeholt wird**, die aber nach den Erfordernissen einer konkreten und transparenten Zustimmung formuliert sein muss. Somit eignet sich diese Lösung nur für bereits bei Beginn der ursprünglichen Datenanwendung klar vordefinierte Big Data-Anwendungen,¹⁸ wobei eine spätere Änderung der Anwendung die Zustimmung ungültig macht und deren Neueinholung erfordert;
- wenn **punktuell wissenschaftliche oder statistische Untersuchungen** mit wissenschaftlichen Methoden gemacht werden und entweder nur Daten aus eigenen Datenanwendungen (dann auch personenbezogen) oder bei Daten von Dritten diese nur in indirekt personenbezogener (pseudonymisierter) Form verwendet werden und das Ergebnis nur indirekt personenbezogen ist;

- wenn **wissenschaftliche oder statistische Untersuchungen**, die im öffentlichen Interesse liegen, von der Datenschutzbehörde individuell genehmigt werden.

Zukünftige Entwicklung

Big Data ist auch im Rahmen der **Verhandlungen zur DSGVO** ein großes politisches Thema. So hat die **Art 29-Datenschutzgruppe eine Stellungnahme zu Big Data abgegeben**, in der sie klargestellt hat, dass der Nutzen aus Big Data nur dann erreicht werden kann, wenn gleichzeitig die Ansprüche der Betroffenen auf Datenschutz gewährleistet sind.¹⁹

Die Entwurfstexte zur DSGVO zeigen, dass das **Zweckbindungsprinzip** künftig im Vergleich zur bestehenden Rechtslage **aufgeweicht werden soll, um eine spätere Weiterverwendung – auch für Big Data – zumindest durch denselben Auftraggeber zu ermöglichen**. So spricht ein geleakter Text des EU-Rates²⁰ vom 3. 6. 2015 in einem zusätzlich eingefügten Art 6 Abs 3 a von den Bedingungen unter denen Daten für an-

dere Zwecke weiterverwendet werden dürfen, und Art 6 Abs 4 davon, dass Daten für andere Zwecke weiterverwendet werden dürfen, selbst wenn dessen Zweck mit dem ursprünglichen nicht vereinbar ist, aber die Interessen des Auftraggebers an der Nutzung dafür überwiegen. Ebenso enthielt schon der ursprüngliche Entwurf der EU-Kommission im Jahr 2012²¹ in Art 20 eine **Bestimmung über Profiling**, die seitdem heftig diskutiert wird. Es bleibt daher abzuwarten, ob und wie sich die Rechtslage zu Big Data durch die DSGVO in Zukunft verändern wird.

Dako 2015/35

¹⁷ In Einzelfällen, wie etwa bei der Bonitätsbeurteilung von Kreditnehmern durch Banken nach dem BWG, kann Big Data auch auf Basis einer gesetzlichen Verpflichtung betrieben werden. Siehe *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 6 Anm 6b. ¹⁸ **Denkbar** wäre dies etwa bei Kundenbindungsprogrammen im Einzelhandel, bei denen klar vordefiniert wird, welche Datenbestände über Kunden zusammengeführt und ausgewertet werden sollen, und dies in der Zustimmung zum Kundenbindungsprogramm entsprechend transparent ausformuliert wird. ¹⁹ *Art 29-Datenschutzgruppe*, Stellungnahme vom 16. 9. 2014 zu Big Data, WP 221, siehe die Zusammenfassung von *Haidinger*, *Dako* 2014, 48. ²⁰ Der Text findet sich unter www.parlament.gv.at/PAKT/EU/XXV/EU/05/87/EU_58737/imfname_10536086.pdf ²¹ Der Entwurf ist mit sämtlichen Materialien unter <http://statewatch.org/news/2015/jun/eu-council-dp-reg-consolidated-3-6-15-9281-15-1.pdf> abrufbar.

Zum Thema

Über den Autor

Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte in Wien.
Tel: +43 (0)1 533 16 95, E-Mail: knyrim@preslmayr.at, Internet: www.preslmayr.at