

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. Mehr als drei Viertel der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils knapp 10 Prozent kommen aus sonstigen Ländern der EU und den USA, 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine

zukunftsorientierte Netzpolitik

Big Data in der Datenschutz-Grundverordnung ein.

< TT. Monat JJJJ >

Seitensverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Susanne Dehmel
Bereichsleiterin
Datenschutz
Tel.: +49.30.27576-223
Fax: +49.30.27576-51-223
s.dehmel@bitkom.org

Der Rat der Europäischen Union berät derzeit noch über den Kommissionsentwurf für eine Datenschutz-Grundverordnung. Der Fokus liegt unter anderem darauf,

den Entwurf so auszugestalten, dass er auch neue Datenverarbeitungstechnologien zulässt, aber gleichzeitig deren Risiken mitberücksichtigt. Vor diesem Hintergrund sind die nachfolgend aufgeführten Vorschläge zu den aus unserer Sicht wichtigsten Vorschriften in Bezug auf Big Data erarbeitet worden. Ziel dieser Vorschläge ist es, es den europäischen Unternehmen zu ermöglichen, neue Technologien einzusetzen und innovative Datenverarbeitungen zu entwickeln, während gleichzeitig die Privatsphäre und das Persönlichkeitsrecht der EU-Bürger geschützt werden.

Zusammenfassung

Präsident

Prof. Dieter Kempf

Eine große Rolle für den möglichen Einsatz von Big Data Analysen spielen

Hauptgeschäftsführer

Dr. Bernhard Rohleder

- die Möglichkeit zur Verarbeitung anonymisierter Daten,
- die Definition von pseudonymisierten Daten,
- die Erlaubnistatbestände (für die Verarbeitung von pseudonymisierten Daten),
- die Einwilligung und deren Widerruf und
- die Regelungen zur Profilbildung.

Stellungnahme

< Kurztitel >

Seite 2

1 Die Definition von anonymisierten und pseudonymisierten Daten

Die Definition des personenbezogenen Datums sowie der Anonymisierung sind bestimmen den sachlichen Anwendungsbereich der Verordnung und damit auch die Frage inwieweit technische Unkenntlichmachung des Personenbezuges ein Mittel sein kann, um Big Data Analysen unter Wahrung der Privatsphäre des Einzelnen rechtssicher zu ermöglichen. Wenn anonymisierte Daten losgelöst von den engen Vorgaben der Verordnung hinsichtlich Zweckbindung etc. verarbeitet werden können, ist zum einen ein Anreiz gesetzt, möglichst viele Daten zu anonymisieren und zum anderen wird innovationshemmender Aufwand vermieden. Um neue Anwendungen zu entwickeln kann es notwendig sein, mit Daten auch jenseits des engen Korsetts der Zweckbindung zu experimentieren. Damit diese Vorteile erreicht werden können müssen das personenbezogene Datum und die Kriterien für die Anonymisierung so ausgestaltet werden, dass sie für die verarbeitenden Stellen klare Anforderungen aufstellen, deren Umsetzung und Überwachung praktikabel sind.

Dafür schlagen wir vor:

- In die Definition des personenbezogenen Datums und entsprechend in die Definition des anonymisierten Datums sollte entsprechend § 3 Abs. 6 BDSG das Element des „unverhältnismäßig großen Aufwands an Zeit, Kosten und Arbeitskraft“ aufgenommen werden.
- Die vom Rat bereits eingefügte Definition des pseudonymisierten Datums ist in diesem Zusammenhang ebenfalls sehr hilfreich. Sie sollte lediglich noch klarer formuliert werden.

2 Ergänzung der Erlaubnistatbestände für die Verarbeitung

Ein bewährtes Mittel, um Analysen zu nützlichen Zwecken wie der der Optimierung von Diensten zuzulassen und gleichzeitig unerwünschte Rückschlüsse auf einzelne Personen zu vermeiden ist die Verarbeitung von Daten in pseudonymisierter Form.

- Es wäre sinnvoll, Verarbeitungen in pseudonymisierter Form entsprechend der Vorschrift in § 15 TMG Abs. 3 zuzulassen, so lange sichergestellt ist, dass das Pseudonym nicht aufgehoben wird.

Es erweist sich ferner in der Praxis immer wieder als problematisch, dass es momentan keine Rechtsgrundlage gibt, Daten, die zu einem rechtmäßigen Zweck erhoben wurden und die in anonymisierter Form zu einem anderen Zweck weiterverarbeitet werden sollen, zum Zweck der Anonymisierung nochmals zwischen zu speichern.

- Es wäre wünschenswert, dass eine Klarstellung erfolgt, dass die Speicherung zu diesem Zweck zulässig ist.

Stellungnahme

< Kurztitel >

Seite 3

Anlage mit Formulierungsvorschlägen:

Zu 1) Definition des personenbezogenen Datums und seiner Anonymisierung

Article 4

Ratstext vom 30.06.2014	Vorschlag:
<p>(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly (...), in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.</p>	<p>(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly (...), by means that are technically feasible, do not involve a disproportionate effort, and are reasonably likely to be used by the controller or by any other natural or legal person, working together with the controller in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.</p> <p>It follows that unique identifiers provided by devices, applications, tools, and protocols need not necessarily be considered personal by the data controller in all circumstances</p>
<p>(3b) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution.</p>	<p>(3b) 'pseudonymisation' means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, which is subject to separate and distinct technical and organisational controls to prevent such relation, or that the data subject's name and other identifying features are replaced with another identifier so that identifiability of the data subject is considerably impeded. Pseudonymous data shall be considered as personal data.</p>
	<p>(3c) (new)</p> <p>'Anonymous data' means any data that has been collected, altered or otherwise processed in such a way that it can no longer be attributed to a data subject, including where any personally identifying features are replaced with a code so that the data subject can</p>

Stellungnahme

< Kurztitel >

Seite 4

	no longer be identified, or that such attribution would require a disproportionate amount of time, cost and effort; anonymous data shall not be considered personal data.
<p>Recital 23:</p> <p>The principles of data protection should apply to any information concerning an identified or identifiable natural person. Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation does therefore not concern the processing of such anonymous information, including for statistical and research purposes. The principles of data protection should not apply to deceased persons, unless information on deceased persons is related to an identified or identifiable natural person.</p>	

* Fußnote

Zu 2) Ergänzung der Erlaubnistatbestände für die Verarbeitung

Article 6 Lawfulness of Processing

Ratstext vom 30.06.2014	Vorschlag:
1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:	1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
...	

Stellungnahme

< Kurztitel >

Seite 5

<p>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</p>	
	<p>(b2):„the processing is necessary for the performance of a contract or entering into a contract which is related to a commercial or professional activity of the data subject and only personal data of the data subject is affected which is related to such commercial or professional activity.</p>
	<p>(g)Die Verarbeitung ist beschränkt auf pseudonymisierte Daten aus einer oder mehreren Datenquellen für berechnigte Zwecke der verantwortlichen Stelle, wobei die betroffene Person angemessen geschützt ist. Von einem angemessenen Schutz ist auszugehen, wenn die Daten rechtmäßig erhoben worden sind und</p> <p>die Pseudonymisierung so erfolgt, dass die Informationen durch Dritte nicht auf die einzelne betroffene Person zurückgeführt werden können sowie</p> <p>die betroffene Person über die Datenverarbeitung in geeigneter Weise informiert wird und ihr ein Widerspruchsrecht nach Artikel 19 Absatz 3a eingeräumt wird.</p> <p>Die pseudonymen Daten und die Ergebnisse der Verarbeitung von pseudonymen Daten dürfen ohne vorherige Einwilligung der betroffenen Person nicht mit den Klardaten des Trägers des Pseudonyms zusammengeführt werden. Die Ergebnisse der Zusammenführung von pseudonymen Daten dürfen nicht zur Repersonalisierung der betroffenen Person führen.</p> <p>(h) Die Verarbeitung dient der</p>

Stellungnahme

< Kurztitel >

Seite 6

	Anonymisierung rechtmäßig erhobener personenbezogener Daten.

Article 19 Right to object

Ratstext vom 30.06.2014	Vorschlag
<p>1. The data subject shall have the right to object, on reasoned grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (...) (f) of Article 6(1); the personal data shall no longer be processed unless the controller demonstrates (...) legitimate grounds for the processing which override the interests or (...) rights and freedoms of the data subject..</p>	
<p>1a. (...) Where an objection is upheld pursuant to paragraph 1 (...), the controller shall no longer (...)183 process the personal data concerned except for the establishment, exercise or defence of legal claims</p>	
<p>2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object (...) at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (...) and shall be presented clearly and separately from any other information</p>	
<p>Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.</p>	
	<p>3a. Where pseudonymous data are processed based on Article 6(1)(g), the data subject shall have the right to object free of charge to the processing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be</p>

Stellungnahme

< Kurztitel >

Seite 7

clearly distinguishable from other
information.
