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 ein.

Ziel der Weiterentwicklung des europäischen Datenschutzrechts muss sein, es den europäischen Unternehmen zu ermöglichen, neue Technologien einzusetzen und innovative Datenverarbeitungen zu entwickeln, um international konkurrenzfähig zu sein, während gleichzeitig die Privatsphäre und das Persönlichkeitsrecht der EU-Bürger geschützt werden.

1 Problematik Big Data und geltende Datenschutzprinzipien

- Das geltende Datenschutzrecht und auch die Verordnung versucht Datenmissbrauch bzw. Eingriffe in die Privatsphäre/informationelle Selbstbestimmung dadurch zu verhindern, dass schon die Datenerhebung, aber auch die Verarbeitung von personenbezogenen Daten auf ein Minimum begrenzt wird.

- Wenn aber die Wertschöpfung zukünftig auf einer möglichst intelligenten Datenverarbeitung beruhen soll, ist das Potential dieses Konzepts, das geeignet ist, einen Standortnachteil zu begründen, weil es die Datenverarbeitung selbst beschränkt.

- Die wichtigen Grundsätze der Datensparsamkeit und der Zweckbindung widersprechen grundsätzlich dem bei Big Data gängigen Ansatz, aus einer möglichst großen Menge von unterschiedlichen Daten Muster zu erkennen, die nützliche Erkenntnisse erbringen. Das führt zu großer Rechtsunsicherheit bei den potentiellen Anwendern von Big Data Methoden.

- Mit der Anonymisierung von personenbezogenen Daten lässt sich in vielen Fällen die Anwendung des Datenschutzes umgehen. Allerdings ist diese oft schwierig, aufwändig und die Auslegung, wann Daten nach der EU-VO wirklich anonymisiert sind, ist umstritten.

Bundesverband
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

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

- In einigen Bereichen wie z.B. der medizinischen Forschung scheidet die Anonymisierung aus, weil Daten rückverfolgbar sein müssen, um Fehler ausschließen zu können. Hier bedarf es einer rechtssicheren Grundlage im Gesetz für die Verarbeitung der Daten. In vielen Fällen könnten sie weitgehend pseudonymisiert verarbeitet werden.

- Wie also die unerwünschten Folgen der Datenverarbeitung, nämlich mögliche Verletzungen der Privatsphäre oder die Verwendung der Daten zu unerwünschten Zwecken (vom Individuum unerwünscht o. von der Gesellschaft) verhindern?

2 Mittelfristige Strategie:

- Mehr Fokus auf die Nutzung der Ergebnisse der Datenverarbeitung legen. Die meisten Daten sind nur in einem bestimmten Kontext von Wert, aber auch nur in bestimmten Kontexten sensibel.

- Das Datenschutzrecht nicht überfrachten, sondern die Missbrauchspotentiale dort bekämpfen, wo sie vorhersehbar sind oder auftauchen. Durch Digitalisierung ist Datenschutzrecht auf einmal für praktisch alle Sachverhalte des Lebens „zuständig“. Dafür ist es nicht gemacht.

  - Beispiel: Diskriminierung bei Krankenversicherung – ob Verhaltens/Risikobasierte Tarife gewünscht sind und wer zu welchen Konditionen versichert wird ist eine Frage der Solidargemeinschaft, nicht des Datenschutzes.

  - Beispiel: Persönlichkeitsverletzung im Internet durch Rufschädigung o.ä. – zivilrechtliche Instrumente (einmal geplantes rote Linie Gesetz De Maizière)

- Aufklärung der Unternehmen und der Bevölkerung über den Nutzung von Big Data fördern, gesellschaftlichen Diskurs über Chancen und selbstgesetzte Grenzen des Einsatzes der Technologie.

- Einsetzung einer Art Ethik-Kommission für den Umgang mit Aussagen/ Vorhersagen von Analyseprogrammen.

3 Kurzfristige Strategie:

- Die Regelungen der EU-Datenschutzverordnung so gestalten, dass innovative Formen der Datenverarbeitung jedenfalls nicht soweit erschwert werden, dass es für europäische Unternehmen/Forschung einen starken Wettbewerbsnachteil bedeutet.

- Problem bei Abstimmung der deutschen Positionen: stark verbraucherlastige Sicht des BMJV, Wirtschaftssicht lange Zeit unterrepräsentiert wegen Zurückhaltung BMWI.

- Die Datenschutzverordnung darf nicht wieder 20 Jahre halten, sondern muss in kürzeren Abständen evaluiert oder generell befristet werden.

- Hauptprobleme für die Etablierung innovativer Geschäftsmodelle in Bereichen mit Big Data wie E-Health, E-Mobility, Smart Energy und Industrie 4.:
  - Ein nur mit engen, statischen Ausnahmen versehenes Verarbeitungsverbot von personenbezogenen oder -beziehbaren Daten,
  - Rechtsunsicherheit durch unklare Regelungen
  - Aufwändige (formale) Voraussetzungen für die Datenverarbeitung.

- Daher schlagen wir vor, bei der Verordnung vorrangig auf folgende Punkte zu achten (welche in Teilen auch bereits von der Breg aufgegriffen wurden):
  - Möglichkeit zur Verarbeitung anonymisierter Daten,
  - Definition von pseudonymisierten Daten,
  - Erlaubnistatbestände
    - für die Verarbeitung pseudonymisierter Daten
    - für die Verarbeitung im berechtigten Interesse des Verarbeiters
    - für die Verarbeitung nach zulässiger Zweckänderung
  - Einwilligung und deren Widerruf
  - die Regelungen zur Profilbildung.
  - Riskobasierter Ansatz zur Verringerung von bürokratischem Aufwand.

Welche Änderungen zu den einzelnen Themen sinnvoll sind, ist in den folgenden Abschnitten ausgeführt.

4 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 wie in § 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.

5 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 pseudonymsierter Form.

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

- Um die Rechte der Betroffenen zu wahren, bietet sich entweder die Widerspruchslösung wie im geltenden TMG an oder eine Abwägungsklausel (beide Varianten in den Formulierungsvorschlägen der Anlage)

Es erweist sich ferner in der Praxis immer wieder als problematisch, dass es momentan keine ausdrückliche 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 sollte klargestellt werden, dass die Speicherung zu diesem Zweck zulässig ist.

Weiterhin wurde von der Kommission und dem Parlament der Erlaubnistatbestand „eigenes berechtigtes Interesse oder Interesse Dritter an der Verarbeitung, der kein überwiegendes berechtigtes Interesse des Betroffenen entgegensteht“ in Frage gestellt. Dieser Erlaubnistatbestand existiert im deutschen Recht schon seit langem und ist als eine Art „Auffangtatbestand“ für alle Sachverhalte wichtig, die der Gesetzgeber so im Einzelnen nicht vorhersehen kann. Der Rat hat diesen Erlaubnistatbestand vorgesehen, er sollte unbedingt erhalten werden.

Die nachträgliche Zweckänderung ist sowohl für bestehende als auch für zukünftige Geschäftsmodelle und Datenflüsse notwendig und sollte auch möglich sein, wenn berechtigte Interessen des Verarbeitenden oder Dritter bestehen und keine schwerer wiegenden Interessen des Betroffenen dagegen stehen.
die Möglichkeit zur Zweckänderung. Der Bedarf, bestehende Datenbanken aus verschiedenen Quellen und Anwendungsbereichen für weitere Zwecke zusammenzuführen, wird im Zeitalter von Big Data Analysen ansteigen. Dabei wird die Konstellation auftreten, dass eine neue Analysemöglichkeit eingesetzt werden soll, die zum Zeitpunkt der Datenerhebung noch nicht vorgesehen war. Hier wird oft der Zweck der dann durchzuführenden Analyse nicht dem entsprechen, zu dem die Daten ursprünglich erhoben wurden. Hierin liegt gerade ein hohes Innovations- bzw. Mehrwertpotential bei Big Data Analysen.

- Daher sollte Art. 6 Abs.1 lit. f) DS-GVO in Art. 6 Abs. 4 DS-GVO-E aufgenommen werden.

Big-Data-Analysen haben in vielen Fällen einen stark explorativen, interaktiven Charakter. Die solche Analysen einsetzenden Experten interessieren sich primär für neue Arten der Betrachtung von Daten, um neue Aspekte in kurzer Zeit zunächst prototypisch umsetzen zu können. Man versucht oft, unbekannte Zusammenhänge zu entdecken. Data Scientists gehen mit Daten explorativ und in hohem Maße interaktiv um. Ihre Kreativität wird von Werkzeugen unterstützt, mit denen sich auf einfache Art und Weise komplexe Analysen formulieren lassen. Eine Zweckbindung, wie sie gegenwärtig als Prinzip im Datenschutz verankert ist, erschwert den explorativen Charakter von Big-Data-Analysen in der Praxis sehr. Ein Verbot der Zweckänderung würde ihn in vielen Fällen unmöglich machen.

- Zu erwägen wäre auch eine Art „Experimentierklausel“, welche die Verarbeitung von Daten zur Erforschung neuer Analysemethoden in einem geschützten Rahmen zulassen würde.

6 Einwilligung

Einwilligungen sollten dort zum Einsatz kommen, wo kein üblicher Erlaubnistatbestand für die Datenverarbeitung oder besonderes Risiko für den Betroffenen besteht. Es darf keine zu starren Formvorgaben geben. Wenn das Instrument Einwilligung zu inflationär gebraucht wird, verliert es seine Warnfunktion, wird lästig und nicht mehr ernst genommen.

Zuletzt gab es von Seiten der Bundesregierung sehr kleinteilige Vorschläge hierzu, die maßgeblich unter verbraucherrechtlichen Gesichtspunkten formuliert waren und deren Praktikabilität zweifelhaft war.

- Hier sollte der Status Quo im Ratstext unterstützt werden.
- Die Informationspflichten sollten nochmals darauf geprüft werden, ob sie weiter entschlackt werden könnten.

Schwierig in Bezug auf Big Data wird es insbesondere sein, den Betroffenen so zu informieren, dass er eine informierte Entscheidung treffen kann bzw. bei der Zweitverwertung von Daten wird es oft gar nicht möglich sein, an den Betroffenen direkt ranzukommen, um eine Einwilligung einzuholen. . In vielen Fällen wie z.B. bei Verwendung von nur pseudonymisiert gespeicherten Daten wird es nicht möglich und auch nicht unbedingt im Sinne des Betroffenen sein, hierfür eine Einwilligung einzuholen. Hier wäre der Erlaubnistatbestand wie vorgeschlagen auf Basis einer Interessenabwägung sinnvoll und würde die Erprobung neuer Datenverarbeitungsmethoden unterstützen sowie den administrativen Aufwand begrenzen.

7 Regelungen zur Profilbildung

Die Änderung des Wortlautes des bisherigen Artikels 15 der Datenschutz-Richtlinie 95/46 im jetzigen Artikel 20 des Verordnungsentwurfs der Kommission hat zu erheblicher Unsicherheit darüber geführt, welche bisher zulässigen Profilbildungen weiterhin zulässig sind und was zukünftig nicht mehr erlaubt sein soll. Die Bundesregierung hat bereits mit einem vorgelegten Vorschlag den Versuch unternommen, eine Regelung zu schaffen, die einerseits eine sehr weite Definition im Sinne eines umfassenden Schutzes der Betroffenen zugrunde legt, andererseits aber eine differenzierte, risikobasierte Regelung unterschiedlicher

Sachverhalte vornimmt. Dieser Ansatz ist grundsätzlich richtig. Mit der konkreten Ausgestaltung der Regelung wie sie im Dezember vorgelegt wurde, kann er jedoch nicht befriedigend umgesetzt werden.

- Zum einen ist problematisch, dass die Regelung im Gegensatz zu den bisherigen Vorschlägen, bereits bei der Erhebung/Verarbeitung von Daten zur Erstellung eines Profils ansetzt – in der Regel besteht die Gefahr negativer Auswirkungen für den Betroffenen nur, wenn Profile dazu benutzt werden, Bewertungen vorzunehmen (wie z.B. Entscheidung über die Erteilung eines Kredits oder Aufnahme in ein Bewerbungsverfahren). Dies kam in der Formulierung des Rates zum Profiling vom 30.06. („intended to use a profile to evaluate personal aspects…) stärker zum Ausdruck.

- Ferner scheint die Öffnungsklausel aus Art. 20a (1a) lit. b) in Art. 20 zu fehlen. Es müsste auch für die Profilbildung eine Öffnungsklausel für den nationalen Gesetzgeber vorgesehen werden.

- Die von der Bundesregierung vorgeschlagene Definition in Art. 4 Abs. 12a ist sehr weit und setzt bereits bei der reinen Informationsgewinnung an. Insbesondere in Verbindung mit der Neufassung in Art. 20, wonach die Nutzung der durch die Profilbildung gewonnen Informationen entweder nur mit Einwilligung des Betroffenen (Art. 20 Abs. 1a) oder nur mit pseudonymen Daten (Art. 20 Abs. 1 d) zulässig sein soll, würde der Anwendungsbereich der Nutzung von Profilinformationen bis zur Nichtanwendbarkeit eingeschränkt. Dies würde der eigentlichen Regelungsidee des Profiling nicht gerecht. Hier sollte eine klare Regelung für die Möglichkeit der zulässigen und rechtmäßigen Nutzung von pseudonymen Daten zum Zwecke der Profilbildung aufgenommen werden.

Anlage mit Formulierungsvorschlägen:

Zu 4) Definition des personenbezogenen Datums und seiner Anonymisierung

Article 4

Ratstext vom 30.06.2014	Vorschlag:
(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 identifiersuch 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.	(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. **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**
(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.	(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.**
	(3c) (new)

	'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 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.
Recital 23: 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.	

* Fußnote

Zu 5) 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:
…	
(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;	
	(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.
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. [This subparagraph shall not apply to processing carried out by public authorities in the exercise of their public duties .	Sollte so beibehalten werden.
"Widerspruchslösung"	**(g) : The processing is limited to pseudonymous data from one or more data sources collected for legitimate purposes of the controller and the data subject is adequately protected. Adequate protection is given** **if the data has been collected legitimately and the pseudonymization**

	was done in a way that no information can be linked to a certain data subject by a third person and **if the data subject is informed in an adquate manner and has the right to object as layed down in Article 19 3a.** **The pseudonymous data and results of the processing may not be linked with known data of the data subject without his/her prior consent. The results of a combination of data may not cause the identification of the data subject.**
"Abwägungslösung"	**(g) Processing is limited to pseudonymous data from one or more data sources collected legitimately and the controller has taken effective measures to make sure that the results of the processing cannot be linked with known data of the data subject or lead to re-identification of the data subject except where the interests or fundamental rights of the data subject are obviously affected.**
	(h) The processing serves the anonymization of legitimately collected data.
	Formulierungsvorschlag für Art.6 Abs.4 DS-GVO-E: *Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung einer der in Absatz 1 ~~Buchstabe 1 a bis f~~ genannten Gründe zutreffen. Dies gilt insbesondere bei Änderung von Geschäfts- und allgemeinen Vertragsbedingungen.*

Article 19 Right to object

Ratstext vom 30.06.2014	Vorschlag
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 person-	

al 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..	
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	
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	
Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	
	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 clearly distinguishable from other information.