Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)053

Stellungnahme für das Fachgespräch
„Startups, Mittelstand und der Datenschutz in der digitalen Welt“ des Ausschusses Digitale Agenda am 4. März 2015

Verfasser:

Stephan Noller
Geschäftsführer CEO nugg.ad

4. März 2015

1) Welche regulatorischen Rahmenbedingungen im Bereich des Datenschutzes müssen aus Ihrer Sicht gegeben sein, um der Wirtschaft – insbesondere kleinen (wie Startups) und mittleren Unternehmen im Bereich der digitalen Wirtschaft – ein möglichst hohes Maß an Rechtssicherheit bei möglichst geringem bürokratischen Aufwand zu ermöglichen, und gleichzeitig das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger sicherzustellen ? Gibt es konkrete bürokratische Hindernisse und ggf. hohe Bürokratiekosten, die abgebaut werden müssten, zum Beispiel um Innovationen nicht im Wege zu stehen ?

SN: Wichtig sind eindeutige Regelungen, die für alle Player gleichermassen gelten („level playing field"), inkl. der Anbieter aus dem aussereuropäischen Raum (Marktort-Prinzip, Abschaffung von Sonder-Regelungen wie Safe-Harbor). Idealerweise sollten diese Regelungen für den ganzen EU-Raum gleichermassen gelten. Die überaus klare Regelung in TMG 15.3 für den Umgang mit pseudonymen Daten kann als positives Vorbild gelten. Neben einer klaren rechtlichen Lage ist eine unzweideutige Aufsicht und Verfolgung von Verstössen wichtig, dafür sollten Aufsichtsbehörden und Datenschutzbeauftragte mit ausreichend Mandat und Mitteln ausgestattet sein. In Bereichen wo Selbstregulierung eine Option ist sollte diese bevorzugt werden, da sie flexibler auf neue technische Anforderungen reagieren kann und von der Industrie mitgestaltet werden kann.

2) Wie bewerten Sie vor diesem Hintergrund den sog. „Risikobasierten Ansatz" im Sinne der Differenzierung von Art und Umfang der datenschutzrechtlichen Pflichten nach potenzieller Grundrechtsbetroffenheit? Gibt es eine unterschiedliche Sensibilität der unterschiedlichen Datenarten bzw. gibt es risikofreie Daten? Inwieweit ist dieser Ansatz geeignet, das Recht auf informationelle Selbstbestimmung in der digitalen Welt sicherzustellen?

SN: Es gibt zweifellos unterschiedliche Risiko-Klassen von Daten, sowohl hinsichtlich Inhalt (z.B. Gesundheitsdaten vs. Medien-Nutzung) als auch hinsichtlich technischer Merkmale, hier insbs. Identifizierbarkeit (anonym/pseudonym/personenbeziehbar/personenbezogen). Vollständig anonymisierte oder ausreichend pseudonymisierte Daten zur Medien-Nutzung können z.B. als ziemlich risikofrei gelten (in Deutschland/EU). Vor dem Hintergrund der erheblichen wirtschaftlichen Potentiale von Big-Data Anwendungen ist es von entscheidender Bedeutung, Nutzungsmöglichkeiten von Daten weit zu fassen und ggf. von Prinzip der Zweckbindung bei der Datenerhebung abzuweichen. Ein risikobasierter Ansatz kann in dem Zusammenhang hilfreich sein.

3) Welche regulatorischen Voraussetzungen müssen aus Ihrer Sicht gegeben sein, um datenbasierte Geschäftsmodelle (insbes. durch die Nutzung sog. „Big-Data"), aber auch Innovationen wie z. B. „Autonomes Fahren" insbesondere in Deutschland und Europa zu ermöglichen? Welche Rolle können in diesem Kontext die Konzepte einer Pseudonymisierung bzw. Anonymisierung zur Schutzerhöhung für Betroffene einnehmen? Welche anderen technischen Schutzkonzepte sind darüber hinaus denkbar?

SN: Die in TMG 15(3) geregelte Pseudonymisierung von Daten für bestimmte Zwecke kann handlungsleitend sein für die regulatorische Rahmensetzung. Schon heute werden auf der Basis dieses Paragraphen Big-Data Anwendungen datenschutzkonform umgesetzt – das informierte Opt-Out, eingebettet in eine konsequente Selbstregulierung der Industrie, hat hier auch erwiesenermassen gute Lösungen im Sinne der informationellen Selbstbestimmung und der Datensouveränität/Transparenz geschaffen.

4) Ist aus Ihrer Sicht der im derzeitigen deutschen und europäischen Datenschutzrecht festgelegte Einwilligungsvorbehalt (als „Opt-In-Lösung“) richtig und kann dieser angesichts der derzeitigen Herausforderungen der Digitalisierung das Recht auf informationelle Selbstbestimmung wirksam schützen? Falls nicht, wie müsste er aus Ihrer Sicht modifiziert oder weiterentwickelt werden, um der gerade bei Startups kontinuierliche bestehenden Perspektive einer Weiterentwicklung gerecht zu werden? Wäre eine Computeridentifikation – sofern in der DSGVO geregelt - noch in Europa möglich? Würde dann ein Zustimmungsvorbehalt möglicherweise dazu führen, dass dies einigen US-Unternehmen möglich bleibt und damit deren Rolle im Wettbewerb gestärkt würde, insbesondere gegenüber dem deutschen Mittelstand und Startups?

SN: Opt-In ist für kritische Daten mit eindeutigem Personenbezug oft die richtige Lösung – allerdings muss insgesamt darauf hingewiesen werden, dass mit einem Opt-In Regime selbst in derartigen Fällen häufig keine informierten Entscheidungen herbeigeführt werden (Opt-In/AGB Zustimmung wird „weggeklickt“ und nicht gelesen). Damit entsteht in vielen Fällen die ungünstige Situation einer weitgehenden und rechtlich bindenden Zustimmung zur Datenverwendung, ohne dass tatsächlich eine informierte Entscheidung getroffen worden wäre.
Lösungen auf Basis von pseudonymen oder anonymen Daten + Opt-Out, wie schon derzeit im TMG vorgesehen, sind dem vorzuziehen – insbs. auch da viele Big-Data Anwendungen gut ohne direkten Personenbezug realisiert werden können.
US-Unternehmen sind aus diversen Gründen üblicherweise stärker in B2C Geschäftsmodellen, d.h. sie haben meist bereits eine direkte Beziehung zum Endkunden und können daher oft problemlos eine Zustimmung einholen. Europäische Unternehmen agieren häufiger in B2B Zusammenhängen ohne direkten Kundenkontakt. Daher ist von einer Verschiebung hin zu einer strikten Opt-In policy tatsächlich eine Stärkung von US-Unternehmen und eine Schwächung von Anbietern in der EU zu erwarten.
Zusätzlich werden mit Opt-In basierenden Geschäftsmodellen kritischer Datensätze generiert, die bei Hacking oder anderweitig unerlaubtem Zugriff grössere Probleme verursachen können, als z.B. pseudonmyisierte Datensätze.

5) Wie bewerten Sie die Innovations- und Wachstumschancen für kleine (wie Startups) und mittleren Unternehmen der digitalen Wirtschaft vor dem Hintergrund eines in Aussicht stehenden einheitlichen europäischen Rechtsrahmens für den Datenschutz durch die Datenschutzgrundverordnung? Welche Bedeutung messen Sie vor diesem Hintergrund – und vor dem Hintergrund der Wettbewerbsgleichheit - dem Marktortprinzip zu, nach dem alle Anbieter, die in Europa ihre Dienste anbieten, dem europäischen Datenschutzrecht unterliegen sollen?

SN: Mit dem Inkrafttreten der Datenschutz-Verordnung würde für alle 28 Mitglieds-Staaten ein einheitlicher Rechtsrahmen für den Umgang mit Daten gesetzt. Damit hätten europäische Startups einen ähnlich grossen Markt zur Verfügung wie Konkurrenten aus den USA (von weiteren rechtlichen Rahmenbedingungen und der Vielsprachigkeit mal abgesehen). Die Bedeutung für Wachstum und Ansiedelung digitaler Startups wäre demnach erheblich, insbesondere dann, wenn tatsächlich das Marktort-Prinzip durchgesetzt würde. Dies würde aber die Abschaffung von Sonder-Regelungen wie z.B. Safe-Harbor voraussetzen.

6) Wie bewerten Sie Datensicherheit und ein europaweit einheitliches Datenschutz-Niveau als Standortfaktor und als Wettbewerbsmerkmal? Muss die EU-Reform ihrer Meinung nach durch gesetzgeberische Anpassungen auf nationaler Ebene flankiert werden? Wo sehen Sie konkrete Vorteile aus Sicht der Unternehmen, wenn es um Datenschutz als Standortfaktor und Wettbewerbsmerkmal geht?

SN: Wie gesagt – europäisch einheitliche Regeln für den Umgang mit Daten wären ein positiver Standortfaktor, vorausgesetzt natürlich, dass diese Regeln vernünftig sind und auch konsequent umgesetzt werden. Das Instrument der Verordnung ist demnach meiner Ansicht nach klar zu bevorzugen (und damit keine nationalen Sonder-Regelungen). Handlungsleitend für vernünftige Regularien für digitale und Big-Data Startups können wie gesagt die Regelungen im deutschen Telemedien-Gesetz gelten (die sich im aktuellen Parlaments-Entwurf der EU-Verordnung zwar in Teilen wiederfinden, allerdings deutlich weniger verbindlich und derzeit ohne Wegfall der Zustimmungserfordernis, daher aus unternehmerischer Sicht relativ unbrauchbar).
Wenn mit der EU-Verordnung ein modernes und digital-kompatibles Regelungswerk gelingt, könnte dies langfristig sogar ein Wettbewerbsvorteil für EU-Technologien auf dem Weltmarkt zur Folge haben.

7) Gibt es aus Ihrer Sicht - ergänzende Instrumente (beispielsweise im Bereich der Werbung; Auditierung, Gütesiegel etc.), die das Recht auf informationelle Selbstbestimmung zusätzlich wirksam schützen können? Wenn ja, wie müssten diese ausgestaltet sein? Welche Rahmenvorgaben bedarf es, um wirklich aussagefähige und wirksame Audits oder Gütesiegel zu bekommen?

SN: Modelle der Selbstregulierung sind gerade im Bereich der Werbung erwiesenermassen erfolgreiche Instrumente für den Ausgleich der Interessen von Regulierer, Bürger und Unternehmen, insbs. dann wenn sie von den Verbänden (wie z.B. ZAW, EASA) entschlossen umgesetzt und nach verbindlichen Prinzipien koordiniert werden. Gerade Mechanismen wie „public shaming", Siegel-Entzug usw. können in der digitalen Wirtschaft sehr wirksam sein, da die Wechselbarrieren zu anderen Anbietern häufig sehr gering sind. Ein starkes Siegel, ggf. mit teil-staatlicher Aufsicht, das dennoch wirtschaftskompatibel aufgesetzt ist, könnte von erheblicher Bedeutung sein für die Wahrung der Standards und die Implementierung „in den Köpfen der Entwickler/Unternehmer". Das vom ULD in Kiel ursprünglich ins Leben gerufene EuroPrise-Siegel kann als Muster einer solchen Lösung gelten.

8) Welche Instrumente und Möglichkeiten sehen Sie, um die Daten-Souveränität der Nutzer beispielsweise durch privacy by design und privacy by default, durch nutzerkompatible Formen der AGBs und spezifische Opt-Out-Möglichkeiten, Interoperabilität von Daten zwischen Diensten, der Ermöglichung von entsprechenden Datenschutzeinstellungen (jenseits der grundsätzlichen Einwilligung in AGB) oder Transparenz-Verpflichtungen zu erhöhen und so auch die Akzeptanz neuer Geschäftsmodellen zu stärken?

SN: Das Netz bietet sehr smarte Möglichkeiten der Interaktion – diese müssen konsequent auch für die Herstellung von Transparenz und Kontolle genutzt werden. So ist z.B. eine Information über verwendete Daten direkt im ausgelieferten Werbe-Banner (per anklickbarem icon), die mit einem Klick Auskunft über die konkret verwendeten Daten, deren Ursprung und die Verrechnungsvorschrift (Algorithmus) geben kann, ein riesen Fortschritt im Vergleich zu Regelungen die in AGBs versteckt sind.
Zusätzlich könnte an einem einheitlichen Daten-Labeling vergleichbar mit „nutrition-labeling" gearbeitet werden in der Art, dass bestimmte Daten-Arten mit leicht verständlichen Symbolen erkannt werden („erzeugt personenbeziehbare Daten", „erzeugt nur pseudonyme Daten", „Daten werden nicht mit Dritten geteilt" etc.).
Darüberhinaus wäre eine generell Bevorzugung von Open-Data Prinzipien, quelloffenheit und Interoperabilität hilfreich um Transparenz und Kontrolle sicherzustellen.

9) Ist das Prinzip der Datensparsamkeit aus Ihrer Sicht noch zeitgemäß? Welche anderen Instrumente sind denkbar, die das Recht auf informationelle Selbstbestimmung und die Entwicklung von Innovationen und neuer und innovativer Geschäftsmodelle in Einklang bringen?

SN: Datensparksamkeit ist ein sehr kluges und hochwirksames Prinzip – sie sollte keinesfalls einfach aufgegeben werden. Allerdings erfordern Big-Data

Anwendungen neue Möglichkeiten. So wäre es z.B. möglich, Daten hinsichtlich ihres Pseudonymisierungs-Levels sparsam abzulegen, und je nach Anlass eine zusätzliche Nutzungserlaubnis zur Re-Identifikation vom Nutzer einzuholen, z.B. wenn neue medizinische Erkenntnisse vorliegen. Die Schwierigkeit wird in Zukunft darin bestehen, Regelungen zu finden die in Teilen zu „Daten-Verschwendung" führen, in anderen Teilen aber das Prinzip der Sparksamkeit aufrechterhalten. Dabei sollte auch über einen Bereich öffentlicher Daten nachgedacht werden, z.B. im Bereich smart-cities, aber auch für medizinische Forschung, smarkt-Energy oder Bevölkerungs-Statistik usw.

10) Was sind aus Ihrer Sicht denkbare Ansätze, wie das (nationale und europäische) Datenschutzrecht weiterentwickelt werden kann, um im Kern mit der heutigen Entwicklung mithalten zu können und wie bewerten Sie vor diesem Hintergrund mögliche Vorschläge, nach denen sich die Weiterentwicklung des Datenschutzrechtes an einem materiellen Immaterialgüterrecht und dem Recht der Verfügung über Daten und deren Nutzung orientieren sollte, um einerseits auch den Marktwert personenbezogener Daten zu unterstreichen und den Rechtsträger mit Ausschließlichkeitsrechten auszustatten? Sollten und wenn ja wie, der Wert personenbezogener Daten in die kartell- wettbewerbs- und fusionsrechtliche Bewertung von Unternehmen einfließen?

SN: Der Wert von Daten ist unbestritten, insofern sollte auch über Möglichkeiten nachgedacht werden die Rechte an den Daten und deren Verwertung bei BürgerInnen zu stärken. Allerdings hat ein Grossteil der derzeit relevanten Daten keinen direkten oder gar keinen Personenbezug, ausserdem wird die wirtschaftliche Bedeutung auf der Ebene individueller Personen überschätzt. Der Anteil von Daten ohne Personenbezug wird durch Machine-to-Machine Kommunikation und Industrie 4.0-Anwendungen noch zunehmen. Ich würde vermuten, dass ein System der maximalen wirtschaftlichen Nutzung mit gewissen Transparenz- und Kontrollvorschriften + der dadurch entstehenden indirekten Nutz-Effekte für BürgerInnen z.B. durch kostenlose Nutzung von Internet-Angeboten letztlich zu bevorzugen wäre.

11) Wie beurteilen Sie den Zielkonflikt sicherheitspolitischer Interessen und einem effektiven Grundrechtschutz, bspw. bei Fragen des Schutzes von Grundrechten durch die Sicherung der Privatsphäre einerseits (beispielsweise durch Verschlüsselung und Anonymisierung) und dem Interesse von Geheimdiensten, die Integrität digitaler Infrastrukturen und Datenschutz bspw. durch Zero-Day-Exploits zu untergraben andererseits?

SN: Sowohl zivilgesellschaftlich als auch aus öknonomischer Sicht ist es von entscheidender Bedeutung, eine digitale Infrastruktur zu schaffen, die sicher und vertrauenswürdig ist – d.h. Überwachung sollte ein Ausnahmefall bleiben mit richterlicher Anordnung etc.
Die Regierung sollte mit konkretem Handeln, z.B. durch ein no-spy Siegel für netzkritische Hardware, Förderung von EU-Hardware-Produzenten, Förderung von Open-Source Ansätzen bei Beschaffung etc. demonstrieren, dass permanente Massenüberwachung keine Option ist.

12) Welche konkreten Innovationshemmnisse sehen Sie für deutsche IT Startups und welche Beispiele können Sie dafür nennen? Für wie zentral halten Sie eine

Fokussierung der Politik auf die finanziellen Mittel von IT Startups? Welche anderen Aufgaben- und Problemfelder halten Sie für ebenfalls wichtig? Haben Sie konkrete Vorschläge für eine Hilfestellung für IT Startups, die sich nicht mit der Frage der Finanzierung beschäftigen?

SN: IT-Startups leiden in Deutschland und Europa unter einer chronischen Unterfinanzierung. Staatliche Hilfen zur Erleichterung von VC-Investments sowie direkt staatliche Hilfen (z.B. KfW, HTGF) sind daher sehr zu begrüssen. Zusätzlich wären es hilfreich das Bild des/der GründerIn zu stärken und Gründen von Unternehmen generell zu erleichtern, z.B. durch Abbau administrativer Hürden oder Übergangshilfen im Bereich Sozial- und Krankenversicherung.