Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)055

Stellungnahme zum Thema:

"Startups, Mittelstand und der Datenschutz in der Digitalen Welt"

von Herrn Dean Ceulic,

Posteo.de

Antworten und Stellungnahmen von Posteo zum Fragenkatalog für das Fachgespräch „Startups, Mittelstand und der Datenschutz in der digitalen Welt" des Ausschusses Digitale Agenda am 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?

Die hohen deutschen und europäischen Rahmenbedingungen im Bereich des Datenschutzes stehen der Wirtschaft und Innovationen nicht im Wege. Im Gegenteil: Europäische Unternehmen haben die Chance, die strengeren Regelungen zum Datenschutz für sich zu nutzen und sich mit anspruchsvollen Datenschutzkonzepten von Mitbewerbern, zum Beispiel aus dem US-amerikanischen Raum, abzusetzen. Europäische Unternehmen können Vorreiter für neue, vertrauenswürdigere Geschäftsmodelle sein - wenn sie diese Chance erkennen und ergreifen. Seit den Veröffentlichungen von Edward Snowden gibt es international eine Trendwende hin zu mehr Datenschutz. Längst sind es nicht mehr nur auf Datenschutz spezialisierte Unternehmen wie Posteo, die auf Datensicherheit und Verschlüsselung setzen. Selbst große US-Großkonzerne wie z.B. Apple Inc. unternehmen mittlerweile starke Anstrengungen, um die Privatsphäre ihrer Kundinnen und Kunden besser zu schützen. Dies ist notwendig geworden, um Vertrauen zurückzugewinnen: Die Verbraucherinnen und Verbraucher setzen nur noch wenig Vertrauen in Unternehmen, von denen bekannt ist, dass sie in großem Ausmaß personenbezogene Daten sammeln und verarbeiten - ohne, dass die Verbraucherinnen und Verbraucher einen wirklichen Einfluss darauf hätten.

Rahmenbedingungen im Bereich des Datenschutzes dürfen nicht aufgeweicht werden

Dennoch erwägt die Bundesregierung aktuell, das hohe deutsche und europäische Datenschutzniveau aufzuweichen. Das regulatorische Aufweichen des Datenschutzes wäre fatal, und würde ein gänzlich falsches Signal an deutsche und europäische Unternehmen aussenden. Die hohen deutschen Datenschutzstandards sind zu einem relevanten Standortfaktor geworden, der nicht leichtfertig aufgegeben werden darf. Gerade Datensparsamkeit und die Zweckbindung beim Verwenden von Daten stärken das Vertrauen der Verbraucherinnen und Verbraucher in deutsche Unternehmen und helfen, das Grundrecht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger zu stärken. Diese Instrumente dürfen nicht aufgegeben werden. Auch, weil beide Faktoren den Unternehmen klare Handlungsanweisungen vorgeben und somit Unsicherheiten minimieren, wie Daten erhoben und verarbeitet werden dürfen - gerade Datensparsamkeit und Zweckbindung stärken die Rechtssicherheit.

Gestaltungsspielräume sind auch bei hohen Datenschutzstandards vorhanden

Das Internet selbst ist technologisch neutral. Es bietet als Wirtschaftsraum zahlreiche Möglichkeiten, wie Geschäftsbeziehungen zwischen Anbietern und den Kundinnen und Kunden ausgestaltet werden können. Der Trend geht seit mehreren Jahren hin zu neuen Geschäftsmodellen, bei denen der private Nutzer auch zahlende Kundin bzw. Kunde ist -

und nicht nur unfreiwilliger (und oft auch unwissender) Lieferant persönlicher Daten. Rein werbefinanzierte Dienste sind nicht mehr das Ton angebende Geschäftsmodell im Internet. Datenschutz zu vernachlässigen oder die entsprechenden Gesetzesregelungen gar aushöhlen zu wollen, ist nicht zeitgemäß und sogar gefährlich: Anbieter von Diensten und Produkten im Internet werden immer häufiger gehackt und Ihnen kommen Daten abhanden. Die Medien berichten in immer kürzer werdenden Abständen über Fälle von Datendiebstahl. Nicht so bekannt ist, dass die Terabyte-großen Datenmengen aus solchen "Data Breaches" im Internet meistens "frei" verfügbar sind. Und nicht nur Hacker verschaffen sich Zugriff auf Daten: Auch Geheimdienste "saugen" laut den Snowden-Dokumenten sprichwörtlich Daten bei Unternehmen ab und speichern sie in großen Rechenzentren. Die Bürgerinnen und Bürger sind angesichts dieser Entwicklung zu Recht verunsichert. Die zwingend erforderliche Berücksichtigung strenger datenschutzrechtlicher Vorgaben ist auch für Unternehmen von wachsender Bedeutung: Sie schützt vor Risiken wie Datendiebstahl und Wirtschaftsspionage - und beugt einem damit einhergehenden Reputationsverlust vor.

Hohe Datenschutzstandards sind kein Innovationshemmnis

Geschäftlicher Erfolg ist auch mit hohen Datenschutzstandards nachweislich und branchenübergreifend möglich. In solchen Geschäftsmodellen liegt die Chance für etwas Neues: Für neue Unternehmen, deren Geschäftsmodelle nicht mehr auf längst bekannte Technologien und Wege setzen. Neue Geschäftsmodelle behandeln Technologien als Mittel zum Zweck, um den privaten Nutzer zur Kundin bzw. zum Kunden zu machen und ihm einen Mehrwert zu liefern. Auch für Unternehmen, die solche Ansätze nicht verfolgen und in ihnen erst einmal keinen Mehrwert sehen, ist es zumutbar und absolut notwendig, die datenschutzrechtlichen Anforderungen zu erfüllen. Dies gilt auch für Startups, für Hersteller von vernetzten Geräten oder für App-Entwickler.

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?

Beim Thema Datenschutz muss zwischen Daten mit Personenbezug und z.B. öffentlich verfügbaren Daten (Open Data) differenziert werden. Dies wird in der Debatte häufig nicht ausreichend berücksichtigt. Auch differenziert der Gesetzgeber bereits zwischen verschiedenen Datenarten und stellt -je nach Datenart- unterschiedliche Anforderungen an Unternehmen: So wird zum Beispiel zwischen Verkehrsdaten, Inhaltsdaten und weiteren personenbezogenen Daten wie Bestandsdaten unterschieden.

Besonderer Schutz für Verkehrs- und Verbindungsdaten

Gerade die sensiblen Verkehrsdaten wie z.B. IP-Adressen, also Daten, die häufig von Unternehmen erhoben und verarbeitet werden, stehen in Deutschland unter einem besonderen Schutz. E-Mailanbieter wie Posteo dürfen Verkehrsdaten z.B. nur für die Dauer von maximal 7 Tagen speichern und lediglich zum Beheben technischer Störungen sowie zum Erkennen von Missbrauch (z.B. Spam) verwenden. Es ist nicht erlaubt, Verkehrsdaten auf einfache Anfragen von Behörden herauszugeben. Verbindungs- und Verkehrsdaten (wie IP-Adressen) müssen auch auf europäischer Ebene unter einem

besonderen Schutz stehen, da ihre Auswertung das Erstellen weitgehender Persönlichkeitsprofile erlaubt. Insbesondere das Speichern von Verkehrsdaten auf Vorrat ist abzulehnen, da dies nach Auffassung mehrerer höchster Gerichte die Grundrechte der Bürgerinnen und Bürger unverhältnismäßig hoch beeinträchtigt.

Speichern von Bestandsdaten stets mit Risiko verbunden

Auch das Speichern personenbezogener Daten durch Unternehmen ist für die betroffene Kundin bzw. den Kunden stets mit einem gewissen Risiko verbunden. Nutzer wissen in der Regel nicht, wie ein Unternehmen Daten wie Namen, Adressen oder Konto-/Kreditkartendaten vor Diebstahl schützt (zum Beispiel durch Verschlüsselung) - oder ob es Kundendaten evtl. sogar selbst verkauft, verwertet oder weitergibt. Personenbezogene Daten sollten nur dann verarbeitet werden dürfen, wenn ein Gesetz es erlaubt und wenn der Betroffene eingewilligt hat. Unternehmen, die personenbezogene Daten verarbeiten, müssen sich angesichts der fortschreitenden Digitalisierung auf die mit ihr einhergehenden Risiken einstellen und Kundendaten immer so gut wie möglich absichern.

Datensparsamkeit und Zweckbindung schaffen Rechtssicherheit

Datensparsamkeit und die Zweckbindung beim Verwenden von Daten sichern nicht nur das Grundrecht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung. Beide Faktoren geben auch Unternehmen klare Handlungsanweisungen und minimieren Unsicherheiten, wie sie Daten erheben und verarbeiten dürfen - insbesondere auch untereinander. Ein "risikobasierter Ansatz" birgt die Gefahr von Rechtsunsicherheiten für Unternehmen bei der praktischen Anwendung und würde Gerichte voraussichtlich für viele Jahre beschäftigen. Angesichts eines rasanten technologischen Wandels sind diese effektiven gesetzlichen Schutzmechanismen unerlässlich – auch und gerade auf europäischer Ebene.

Sonstige anfallende Daten & "Big Data"

Ebenso muss das Verwenden anderer anfallender Datenarten, wie z.B. von Daten aus vernetzten Geräten und Prozessen, den strengen datenschutzrechtlichen Bestimmungen unterliegen und an einen definierten Zweck gebunden sein. Nur so kann sichergestellt werden, dass "Big Data" nicht zu einem Datenschutz-Desaster erster Güte wird. Sonst würden gesammelte Daten, die ja stets einen Informationswert besitzen, unkontrolliert zweckentfremdet, verkauft und verknüpft. Dies kann gesamtgesellschaftlich nicht gewollt sein: Die Analyse von Massen-Daten würde aller Voraussicht nach zu verschiedensten Zwecken genutzt. Die Gefahr liegt hierbei darin, dass das ungehemmte Auswerten und Verknüpfen von Daten sich schnell auf die Möglichkeiten der freien Lebensgestaltung und Persönlichkeitsentfaltung auswirken würde. Neues Wissen über Zusammenhänge zwischen dem Verhalten von Personen oder Personengruppen öffnet potentiell der Diskrimierung ganzer Bevölkerungsteile Tür und Tor, z.B. im Hinblick auf die Bewertung ihrer Kreditwürdigkeit, ihrer Kaufkraft oder ihrer Einschätzung durch Versicherungen, Vermieter oder Arbeitgeber.

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?

Big-Data Geschäftsmodelle erfordern von Unternehmen einen starken Drang zur Monopolisierung. Aus ökonomischer Sicht können die verwerteten Daten nur dann einen Marktwert erzielen, wenn sie exklusiv angeboten werden. Dies führt im schlechtesten Fall in einem marktdynamischen Umfeld zu einer x-fachen Sammlung von Daten, die schwer zu rechtfertigen ist.

Pseudonymisierung und Anonymisierung sind Mindest-Anforderungen bei Big-Data-Geschäftsmodellen. Auch das Verschlüsseln von Daten und Verbindungen ist notwendig und empfehlenswert. Welche regulatorischen Voraussetzungen aus Sicht von Posteo erfüllt sein müssen, um datenbasierte Geschäftsmodelle rechtssicher zu ermöglichen, ist im Absatz "Sonstige anfallende Daten & "Big Data" der Frage 2) aufgeführt.

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?

Das Opt-In-Prinzip ist richtig, es behindert Startups und junge Firmen keineswegs in ihrer Weiterentwicklung - und es funktioniert. Es muss sichergestellt bleiben, dass ein Nutzer seine Einwilligung bewusst und eindeutig erteilt. Es ist zumutbar und absolut notwendig, dass sich auch Startups, Hersteller von vernetzten Geräten oder App-Entwickler mit datenschutzrechtlichen Regelungen intensiv auseinandersetzen müssen.

"Opt-In-Prinzip" funktioniert

Ein sehr gutes Beispiel für das Funktionieren von "Opt-In" ist das Newsletter-Marketing, bei dem ein Versand (und die Verarbeitung von Daten) nur mit dem ausdrücklichen Einverständnis der Kundin bzw. des Kunden erfolgen darf. Auch Unternehmen aus dem Ausland halten sich an diese Vorschriften. Und trotz (oder wahrscheinlich auch gerade wegen) dieser Vorschriften entwickelt sich der Markt für das Newsletter-Marketing seit Jahren sehr positiv.

Unternehmen holen sich aktiv das Einverständnis von Kundinnen und Kunden ein, bevor sie ihnen Newsletter zusenden. Diese Verfahren haben sich etabliert und die Unternehmens-internen Prozesse der Versender sind inzwischen darauf ausgelegt. Sowohl für die Anbieter wie auch für die Verbraucherinnen und Verbraucher bewirkt dies ein hohes Maß an Rechtssicherheit bei dem Umgang mit persönlichen Daten.

Siehe im Weiteren die Ausführungen bei Frage 5).

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?

Die strengeren deutschen und europäischen Rahmenbedingungen im Bereich des Datenschutzes stehen der Wirtschaft und Innovationen nicht im Wege. Ein einheitlicher europäischer Rechtsrahmen für den Datenschutz ist nicht nur aus Verbrauchersicht notwendig, er ist auch aus Unternehmenssicht wünschenswert: Eine europaweite Datenschutzgrundverordnung kann den Unternehmen größere Rechtssicherheit verschaffen und kann die Chancengleichheit der Unternehmen innerhalb des europäischen Binnenmarktes erhöhen. Es ist außerdem grundsätzlich zu befürworten, dass eine Datenschutzgrundverordnung auch für Unternehmen gilt, die ihren Sitz außerhalb der Europäischen Union haben und sich mit ihren Angeboten an EU-Bürger wenden.

Ein europäischer Binnenmarkt baut also Rechtsunsicherheiten für Unternehmen ab. Insbesondere kleinere und mittlere Unternehmen werden davon profitieren, da es ihren tatsächlich verfügbaren Zielmarkt vergrößert. Ein Aufgeben eigener, hoher Standards schafft allerdings eine verschlechterte Ausgangsposition für deutsche Unternehmen und würde die Bemühungen um die Schaffung eines europäischen Binnenmarktes ad absurdum führen.

Eine Festlegung des Marktortprinzips für nicht-europäische Unternehmen ist in diesem Zusammenhang offensichtlich notwendig, um allen in der europäischen Union tätigen Unternehmen die gleiche Wettbewerbsumgebung und Rechtssicherheit zu bieten. In diesem Zusammenhang muss das "Safe Harbour" Abkommen evaluiert werden.

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?

Datenschutz entwickelt sich zu einer so genannten "Selling Proposition" und wird von den Verbraucherinnen und Verbrauchern inzwischen als hoher Mehrwert wahrgenommen. Sie achten -wie im Übrigen auch zunehmend die Unternehmen selbst- vermehrt auf den Standort ihrer gespeicherten Daten. Deutschland ist hier mit führend und sollte seine starke Position nicht aufgeben.

Siehe insbesondere auch die Ausführungen zu Punkt 1).

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?

Das Thema Auditierung, Zertifizierung und Gütesiegel ist im Bereich Datenschutz ein Schwieriges. Es stellt sich die Frage, von welchen Stellen diese vorgenommen werden könnten. Die Staaten und somit auch dazugehörige Behörden haben durch das Bekanntwerden der Überwachung der Bürgerinnen und Bürger durch Geheimdienste einen Vertrauensverlust erlitten. Vor diesem Hintergrund könnten staatlich ausgestellte "Datenschutz-Gütesiegel" oder durch Behörden vorgenommene Zertifizierungen das Vertrauen der Verbraucherinnen und Verbraucher in Unternehmen womöglich sogar mindern denn erhöhen.

Dennoch sind solche ergänzenden Instrumente grundsätzlich sinnvoll und begrüßenswert und Posteo ist dazu bereit, bei Vorhaben für Zertifizierungen im IT-Sicherheitsbereich in einen Dialog zu treten und diese ggf. zu unterstützen. Vor dem Hintergrund der Geheimdienst-Enthüllungen kann der Staat -unter der Voraussetzung einer gelebten Transparenz- versuchen, mit Hilfe solcher Instrumente verloren gegangenes Vertrauen zurück zu gewinnen. Dies erfordert allerdings eine gelebte Transparenz bei den Partnern.

Auch freiwillige Sicherheits-Audits sind empfehlenswert: Posteo hat z.B. gerade erst ein externes Sicherheits-Audit für eine neue Verschlüsselungs-Komponente durchführen lassen, die bald auf den Markt gehen wird. Hierzu wurde ein privatwirtschaftliches Auditierungs-Unternehmen beauftragt.

Die regulierte Selbstregulierung oder eigene Initiativen der Industrie sind als ergänzende Instrumente begrüßenswert und können bestehende, regulatorische Rahmenbedingungen in bestimmten Fällen besser umsetzen. Sie geben darüber hinaus betroffenen Unternehmen die Möglichkeit, sich zu beteiligen und stellen damit eine Brücke zwischen staatlicher Regulierung und Privatwirtschaft dar. Eine Vielzahl von durch die Industrie eingeführten Datenschutz- oder Sicherheits-Siegeln mit unklaren Vorgaben kann aber auch zur Verunsicherung der Verbraucherinnen und Verbraucher führen.

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 Geschäftsmodelle zu stärken?

Daten haben einen Eigentümer: den jeweiligen Kunden. Dieser Eigentümer muss im Rahmen der gesetzlichen Bestimmungen die Möglichkeit besitzen, über den Verbleib seiner Daten bei einem Unternehmen zu bestimmen. Offene Standardprotokolle für den Datenaustausch und -umzug sind deshalb zu bevorzugen, um einen "Lock-In-Effekt" von Nutzern zu vermeiden. Bei Posteo ist es den Kundinnen und Kunden über offene Standards zum Beispiel möglich, ihre Daten (E-Mails, Kalender- und Adressbuchdaten) zu importieren und zu exportieren. Kündigt ein Kunde, kann er selbst bestimmen, zu welchem Zeitpunkt sein Postfach und die darin verbliebenen Daten gelöscht werden. Es muss ein Recht auf Datenportabilität geben, das in einem freien Marktgefüge eigentlich selbstverständlich sein sollte. Der Wettbewerb zwischen Anbietern wird so gestärkt. Auch der Bildung von Monopolen wird so vorgebeugt. Dies verbessert die Daten-Souveränität der Bürgerinnen und Bürger.

Maßnahmen wie privacy by design und privacy by default sind zu begrüßen, da sie eine

technologische Basis von Datenschutz-Maßnahmen darstellen. Bei der Spezifikation von Kommunikations- und Datenverarbeitungs-Protokollen muss dies bereits berücksichtigt werden.

Nutzerfreundliche AGBs stehen oft dem Anspruch von Unternehmen gegenüber, sich gegen Abmahnung zu schützen. Eine Verbesserung der Lage hin zu nutzerfreundlicheren und lesbaren AGBs ist wünschenswert.

Es ist richtig, dass Unternehmen gewissen Transparenz-Verpflichtungen unterliegen. Im Hinblick auf zusätzliche Transparenz-Verpflichtungen sollte aber nicht überreguliert werden. Vielmehr ist es wichtig, dass es Unternehmen erlaubt ist, von sich aus transparent zu agieren und zum Beispiel Transparenz-Berichte herauszugeben. In Deutschland war die Gesetzeslage hierzu nicht eindeutig: Da deutsche TK-Anbieter gleich durch mehrere Gesetze (u.a. TKG und G10-Gesetze) Verschwiegenheitspflichten unterliegen, musste Posteo zunächst ein Rechtsgutachten über die Zulässigkeit von Transparenzberichten erstellen lassen, bevor Posteo im Mai 2014 als erster deutscher TK-Anbieter einen Transparenzbericht veröffentlichen konnte. Der monatelange Vorgang bis zur Veröffentlichung war für Posteo mit enormen Kosten und Aufwänden verbunden.

Es muss künftig eine Rechtssicherheit für europäische Unternehmen geben, dass solche Transparenzberichte, die z.B. statistische Zahlen zu Auskunftsersuchen von Behörden umfassen, legal und "gewollt" sind. Solche Berichte müssen nicht in allen Fällen verpflichtend sein - sollten aber rechtlich möglich sein. In den USA sind Transparenzberichte bereits seit vielen Jahren etabliert. Die meisten deutschen Unternehmen geben weiterhin keine Transparenzberichte heraus.

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?

Das Prinzip der Datensparsamkeit ist zeitgemäßer denn je: Technologie ist kompromittierbar und Fälle von Datendiebstahl häufen sich. Staaten und Unternehmen sollten nur Daten erheben, die tatsächlich benötigt werden. Nur Daten, die nicht erhoben werden, können nicht gestohlen werden.

Datensparsamkeit ist die erste und wichtigste Voraussetzung für Datenschutz - sie ist mit anderen Instrumenten nicht ersetzbar. Und: Datensparsamkeit und Innovation sind kein Widerspruch. Verantwortungsvoller Umgang mit Daten gehört vielmehr zu seriösem, verantwortungsvollen Unternehmertum im 21. Jhd. dazu. Die Reputation eines Unternehmens hängt heutzutage entscheidend davon ab, ob sein Geschäftsmodell auch Datensicherheit mit einschließt. Ergänzende Instrumente zur Datensparsamkeit, die ebenfalls notwendig sind: Das Anonymisieren und Pseudonymisieren von Daten sowie das Verwenden verschiedener Verschlüsselungstechnologien und freier Software.

Posteo erhebt zum Beispiel keinerlei personenbezogene Daten seiner Kundinnen und Kunden, Anmeldung und Bezahlvorgänge erfolgen anonym. Außerdem verfügt Posteo über ein innovatives und umfassendes Verschlüsselungskonzept.

Neue, innovative Geschäftsmodelle verfügen immer häufiger über durchdachte und innovative Datenschutzkonzepte. Seit dem Bekanntwerden der Überwachung der

Bürgerinnen und Bürger durch Geheimdienste und dem zunehmendem Datenklau durch Kriminelle werden solche Angebote verstärkt nachgefragt. Und auch für Unternehmen ist es in einer wissensbasierten Ökonomie überlebenswichtig, auf den Schutz ihrer Daten zu achten.

In der Debatte über die angebliche Unvereinbarkeit von Datenschutz und neuen Geschäftsmodellen wird häufig auf Datenarten Bezug genommen, um die es bei den strengen Datenschutzregelungen gar nicht geht - da diese vor allem Daten mit Personenbezug betreffen.

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?

Es ist nicht notwendig, das deutsche oder europäische Datenschutzrecht abzuschwächen, um mit einer "Entwicklung mithalten zu können".
Europäische Unternehmen haben die Chance, die strengeren Regelungen zum Datenschutz für sich zu nutzen: Gerade Unternehmen, deren Geschäftsmodell auf dem Verarbeiten personenbezogener Daten basiert, können mit anspruchs- und verantwortungsvollen Datenschutzkonzepten überzeugen und sich so von Mitbewerbern, zum Beispiel aus dem US-amerikanischen Raum, absetzen.

Ein einheitlicher Datenschutzrahmen für die Europäische Union, das allen Unternehmen und Behörden im EU-Binnenmarkt einen sehr hohen Datenschutzstandard auferlegt, ist zu begrüßen, da dies im Sinne der Verbraucherinnen und Verbraucher und der Unternehmen ist. Besonderes Augenmerk sollte darauf gelegt werden, den Verbraucherinnen und Verbrauchern ein durchsetzungsfähiges Selbstbestimmungs- und Informationsrecht bei der Verarbeitung ihrer personenbezogenen Daten einzuräumen.

Personenbezogene Daten sollten nur dann verarbeitet werden dürfen, wenn ein Gesetz es erlaubt und wenn der Betroffene eingewilligt hat. Verbindungs- und Verkehrsdaten (wie IP-Adressen) müssen unter einen besonderen Schutz gestellt werden, da ihre Auswertung das Erstellen weitgehender Persönlichkeitsprofile erlaubt. Daten haben einen Eigentümer: den jeweiligen Kunden. Dieser Eigentümer muss im Rahmen der gesetzlichen Bestimmungen die Möglichkeit besitzen, über den Verbleib seiner Daten bei einem Unternehmen zu bestimmen. Das Interesse der Unternehmen an Daten wiegt nicht so schwer wie die Rechte der Verbraucherinnen und Verbraucher an ihren Daten.

11) Wie beurteilen Sie den Zielkonflikt sicherheitspolitischer Interessen und einem effektiven Grundrechtsschutz, 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?

Es besteht kein "Zielkonflikt" zwischen sicherheitspolitischen Interessen und einem effektiven Grundrechtsschutz. Es ist das zentrale Merkmal eines Rechtsstaats, dass beide Pole (die Freiheit des Einzelnen/der Grundrechtsschutz sowie das Sicherheitsbedürfnis) in einem ausgewogenen Verhältnis zueinander stehen. Gerät dieses Verhältnis in Ungleichgewicht, wie es durch die Überwachung der Bürgerinnen und Bürger durch Geheimdienste geschieht, besteht die Gefahr, dass sich ein Staat von rechtsstaatlichen Prinzipien entfernt.

Um die Demokratie in der digitalen Welt wieder zu stärken, ist es unerlässlich, ein ausgewogeneres Verhältnis zwischen beiden Polen wieder herzustellen. Internationalen, flächendeckenden Überwachungstätigkeiten von Geheimdiensten lässt sich nur mit Maßnahmen zur Verschlüsselung, zur Datensparsamkeit und zur Anonymisierung begegnen. Dies ist im Interesse der Bürgerinnen und Bürger - und auch im Interesse von Unternehmen und Behörden.

Geheimdienste und Strafverfolgungsbehörden haben diverse Möglichkeiten, über legale Wege, die mit dem Rechtsstaat vereinbar sind, ihren Auftrag zu erfüllen. Wenn Geheimdienste oder andere staatliche Stellen die Ausnutzung von Zero-Day-Expoloits oder den Einbau von so genannten Backdoors fordern, nützt dies immer auch anderen: So entsteht ein Schwarzmarkt für Sicherheitslücken und es ist ohne Zweifel davon auszugehen, dass auch Kriminelle sich genauso Zugriff auf bestehende Software-Sicherheitslücken verschaffen. Solche Forderungen untergraben jegliche Bemühungen um den Schutz der Privatsphäre der Bürgerinnen und Bürger. Eine Regierung muss ihren Bürgerinnen und Bürgern das uneingeschränkte Grundrecht auf ihre Privatsphäre gewährleisten: Hier gibt es nur ein Entweder-Oder.

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?

Datenschutzregelungen

Strenge Datenschutzregelungen sind kein Innovationshemmnis. Es ist zumutbar, zeitgemäß und absolut notwendig, dass sich auch Startups, Hersteller von vernetzten Geräten oder App-Entwickler mit datenschutzrechtlichen Regelungen intensiv auseinandersetzen müssen.
Und nicht jedes innovative IT-Unternehmen benötigt Fremdkapital:
Posteo ist z.B. ein sehr innovativer E-Mailanbieter (Stichwort: Verschlüsselungstechnologien & Datenschutz). Dennoch ist Posteo seit seiner Gründung (2009) eigenfinanziert, unabhängig und stets ohne Fremdkapital ausgekommen. Für das Produkt gab es von Anfang an eine große Nachfrage und Zahlungsbereitschaft - ein weiterer Beleg dafür, dass es einen Markt für verbraucherfreundliche, auf Datenschutz basierende Geschäftsmodelle im Internet gibt. Es gibt viele weitere Beispiele für Unternehmen, die nicht zwingend auf eine externe Kapitalzuführung angewiesen sind.

Fremdkapital

Viele IT Startups, die z.B. forschungsintensive Geschäftsmodelle verfolgen, sind auf die

Verfügbarkeit von Investitionskapital angewiesen - und hier kann die Politik stärker fördern und Rahmenbedingungen verbessern. Hierzulande wird häufig darüber debattiert, warum kein "deutsches Silicon Valley" existiert. Am hohen europäischen Datenschutzniveau liegt es nicht: Vielmehr ist es die hohe Verfügbarkeit von Investitionskapital, die andere Regionen (z.B. das Silicon Valley) für bestimmte Gründer attraktiver macht. Junge Unternehmen werden dort finanziert, bis sie einen hohen Marktanteil erreicht haben. Dann wird darüber nachgedacht, wie dies geschäftlich amortisiert werden kann. Diese Philosophie ist in Deutschland nicht verbreitet.

Fördergelder

Hinzu kommt eine Praxis der Vergabe von Fördergeldern, die häufig nur für größere Unternehmen brauchbar ist: Der Verwaltungsaufwand und die Mindesthöhe der Fördersummen schließen kleine und mittlere Unternehmen von vornherein aus. So befördert die Politik Innovationshemmnisse und fördert nur Unternehmen mit etablierten Geschäftsmodellen. Ein Lichtblick sind in diesem Zusammenhang Förderprogramme der KfW. Doch bleiben diese unter ihrem Potential: Die Höhe der Förderungen muss größer sein und besser mit dem Wachstum der Unternehmen skalieren, und das Beantragen muss einfacher und schneller möglich sein.

Über Posteo

Posteo ist ein unabhängiger und innovativer deutscher E-Mailanbieter mit Sitz in Berlin. Posteo bietet anonyme, sichere und nachhaltige E-Mail-Postfächer, Adressbücher und Kalender an und verfügt über ein umfassendes Verschlüsselungskonzept. Das Angebot ist komplett werbefrei und eigenfinanziert. Gegründet wurde Posteo 2009. Wir wollen einen Impuls für mehr Sicherheit, Datenschutz und Nachhaltigkeit im Internet geben und Alternativen anbieten: Für alle, die genug von Daten sammelnden Konzernen, werbeverseuchten Posteingängen und der allgegenwärtigen Überwachung im Internet haben. Und für alle, denen es wichtig ist, ökonomisch wie ökologisch nachhaltig zu handeln.

Unser Anliegen ist es, die Daten unserer Kundinnen und Kunden zu schützen und sie nicht meistbietend an die Werbewirtschaft zu verkaufen. Deshalb erheben wir keine personenbezogenen Daten und verzichten auf Tracking-Tools. Wir verschlüsseln stets mit den neuesten Technologien - und fördern die Verbreitung offener Standards. Wir setzen uns aktiv für die digitalen Bürgerrechte ein: Im Mai 2014 hat Posteo als erster deutscher Telekommunikations-Anbieter einen Transparenzbericht veröffentlicht.
Nach Bekanntwerden des NSA-Skandals wurde unser Angebot vielfach in den Medien empfohlen und von Computerzeitschriften getestet. Posteo ist Testsieger bei Stiftung Warentest (Ausgabe 02/2015).

Posteo verfügt über ein umfassendes Nachhaltigkeitskonzept. Wir arbeiten mit echtem Ökostrom von Greenpeace Energy, nicht mit Zertifikate-Strom, der oft als Ökostrom beworben wird. Der Einsatz effizienter Hardware sowie das Verwenden von Recyclingpapier ist für uns genauso selbstverständlich wie unser Firmenkonto bei der GLS-Bank. Wir wollen ein guter Arbeitgeber sein: Posteo setzt ausschließlich auf unbefristete Festanstellungen. Bei Posteo gibt es außerdem täglich einen kostenfreien bio-vegetarischen Mittagstisch.

In unserem Posteo Lab auf dem Berliner Kreuzberg können Interessierte Posteo

ausprobieren, Postfächer eröffnen und Guthaben aufladen. Außerdem bieten wir dort persönliche Verschlüsselungstrainings an (OpenPGP und S/MIME).

Posteo ist auf Datensparsamkeit ausgerichtet (Privacy by design and default). Bei der Konzeption unseres Angebotes haben wir uns an den Anforderungen des Bundesdatenschutzgesetzes (§3a - Datenvermeidung und Datensparsamkeit) orientiert:

Anmeldung ohne Angabe persönlicher Daten

Posteo-Kundinnen bzw. -Kunden melden sich an, ohne persönliche Daten anzugeben. Wir verzichten generell auf das Speichern personenbezogener Daten. So beugen wir Datenhalden vor und handeln nach dem Grundsatz der Datensparsamkeit. Wir geben unseren Kundinnen und Kunden die Hoheit über ihre Daten zurück und stärken so ihr Recht auf informationelle Selbstbestimmung.
Im TKG ist geregelt, dass E-Mailanbieter keine Bestandsdaten erheben müssen, wenn diese nicht (z.B. zu Abrechnungszwecken) benötigt werden. Posteo macht von dieser Regelung Gebrauch.

Anonyme Zahlung

Das Guthaben von Posteo-Postfächern wird stets anonym aufgeladen - egal ob per Überweisung, per Paypal, per Kreditkarte oder in Bar gezahlt wird. Wir verknüpfen Daten, die wir bei Zahlungen erhalten, grundsätzlich nicht mit den E-Mail-Postfächern. Hierfür haben wir 2009 ein eigenes Posteo-Bezahlsystem entwickelt, mit dem wir alle Zahlungsvorgänge anonymisieren. 2015 wurde das Bezahlsystem um neue gesetzliche Anforderungen erweitert. Detaillierte Informationen über unser Bezahlsystem bieten wir unter: https://posteo.de/site/bezahlung an.

Verschlüsselung bei Posteo

Posteo verfügt über ein umfassendes und innovatives Verschlüsselungskonzept. Posteo setzt stets die neuesten Verschlüsselungstechnologien ein, wie z.B. die innovative Technologie DANE/TLSA, die verschiedene Schwachstellen der gängigen Transportwegverschlüsselung eliminiert. Der Zugriff auf die Server erfolgt grundsätzlich über verschlüsselte Verbindungen. Damit unsere Kundinnen und Kunden darauf vertrauen können, dass die verschlüsselte Verbindung wirklich mit dem Posteo-Server stattfindet, setzen wir ein so genanntes erweitertes (grünes) Sicherheitszertifikat ein, mit dem sie auf einen Blick den Verschlüsselungspartner erkennen können. Die Transportweg-Verschlüsselung schützt Daten während der Übertragung vor unbefugten Mitlesern: Die Inhalte einer E-Mail ebenso wie die Metadaten. Die Festplatten aller Posteo-Server sind vollständig verschlüsselt. Kalender- und Adressbücher sind individuell verschlüsselbar. Die Posteo-Eingangsverschlüsselung verschlüsselt auf Wunsch alle neu eingehenden E-Mails mit S/MIME oder PGP - unabhängig davon, ob der Absender einer E-Mail diese ursprünglich verschlüsselt hatte oder nicht. Detaillierte Informationen zu unserem Verschlüsselungskonzept bieten wir unter: https://posteo.de/site/verschluesselung an.

Posteo Lab
Methfesselstrasse 36
10965 Berlin-Kreuzberg
(Öffnungszeiten: Montag-Freitag: 15 -18 Uhr)

https://posteo.de
support@posteo.de