Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)054

Bundesverband Deutsche Startups e.V.

BRIEFING:

AUSWIRKUNGEN DER DEUTSCHEN DATENSCHUTZGESETZGEBUNG UND -PRAXIS AUF STARTUP-UNTERNEHMEN

1. EXECUTIVE SUMMARY

Startups bewerten das deutsche Datenschutzrecht die vorherrschende Datenschutzpraxis in seiner geltenden Fassung als außerordentlich hinderlich. Laut dem Deutschen Startup Monitor, einer vom Bundesverband Deutsche Startups jährlich herausgegebenen Studie, sehen insgesamt 50,8 % der Befragten das Datenschutzrecht als Hemmnis für die eigene Geschäftsentwicklung an, wobei davon sogar 29,8 % dieses als schwer bzw. äußerst schwer zu überwinden betrachten.

2. DATENSCHUTZRECHTLICHE HINDERNISSE

Auf unternehmerischen Erfahrungen aufbauend werden vorab die wichtigsten datenschutzrechtlichen Hindernisse für Startups dargestellt.

a. Der datenschutzrechtliche Einwilligungsvorbehalt

Im Gegensatz zum amerikanischen Datenschutzrecht herrscht in Deutschland die so genannte Opt-In-Lösung vor, wonach in die Erhebung personenbezogener Daten bereits im Vorfeld eingewilligt werden muss. Die Opt-In-Lösung bringt jedoch zwangsläufig für innovative Unternehmen Unsicherheiten mit sich. Gerade bei Startups ist das Geschäft meist noch nicht von vornherein definiert und unterliegt noch einem Weiterentwicklungsvorbehalt. Aus diesem Grund kann auch noch nicht von Beginn an abgeschätzt werden, wie und in welchem Ausmaß Daten zukünftig erhoben und verwertet werden. Jede Nutzungsänderung bedarf dabei einer Änderung der Datenschutzerklärung, was wiederum Kosten verursacht und das Unternehmen unflexibel macht – dabei auch auf Nutzer unattraktiv wirkt, da diese bei jeder Änderung erneut der Erklärung zustimmen müssen.

b. Datenschutzbeauftragte in Unternehmen

Hinderlich wirkt für Startups auch die Pflicht zur Bestellung eines Datenschutzbeauftragten im Unternehmen. Bemerkenswert ist hierbei, dass das Selbstverständnis der Datenschutzbeauftragten extrem von ihrer Wahrnehmung im Unternehmen abweicht. Nach einer Studie der Carl von Ossietzky Universität Oldenburg weisen nur 30 % der Nicht-Datenschutzbeauftragten dem Datenschutzbeauftragten

eine besondere Gestaltungskompetenz zu.[1] Damit gerät das Kosten-Nutzen-Verhältnis bei der Pflicht zur Bestellung eines Datenschutzbeauftragten aus dem Gleichgewicht.

c. *Aufsichtsbehörden*

Gegenteilig verhält es sich jedoch mit dem Verhältnis zwischen den Aufsichtsbehörden – in einigen Bundesländern sind es die Landesdatenschutzbeauftragten – und Startups. Diese verfügen aufgrund ihrer öffentlich-rechtlichen Hoheitsmacht über einen zu großen Einfluss auf das operative Geschäft in Unternehmen. Dabei bewegen sich innovative Startups oft in rechtlich noch nicht vollständig geklärten Grauzonen, die einen ständigen Dialog mit den Aufsichtsbehörden erfordern und damit die Geschäftsentwicklung und die Flexibilität dieser Unternehmen hemmen. Solche Dialoge, in denen Datenschutzbeauftragte konkreten Einfluss auf das operative Geschäft ausüben, sind öffentlich bekannt (siehe etwa StudiVZ).

d. *Grundsatz der Datensparsamkeit*

Der dem Datenschutzrecht zugrundeliegende Grundsatz der Datensparsamkeit hemmt die Innovationskraft von Startups. Daten werden oft als „Währung der Zukunft" beschrieben und dieser Grundsatz macht es von vorn herein deutschen Startups unmöglich mit Unternehmen aus den USA in den Wettbewerb zu treten. Entscheidend für den Datenschutz ist nicht die Datenerhebung, sondern die Datenverwertung und nur zweites sollte reguliert werden, da diese Daten sonst nur von Unternehmen außerhalb des europäischen Rechtskreises erhoben und fernab jeglichen Schutzstandards verwertet werden.

Auf der anderen Seite werden Startups zusätzlich Erhebungspflichten für bestimmte Daten auferlegt, die das Unternehmen wohlmöglich gar nicht von sich aus sammeln würde. Bei einer kürzlich umgesetzten EU-Richtlinie[2] geht es darum, dass der umsatzsteuerlich relevante Leistungsort bei Telekommunikations-, Rundfunk- und Fernseh- sowie auf elektronischem Weg erbrachten Dienstleistungen (digitale Produkte)

[1] Das Selbst- und Fremdbild von Datenschutzbeauftragten; von der Carl von Ossietzky Universität Oldenburg in Kooperation mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.; S. 24; abgerufen am 10.12.2014 unter https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/bvd-allgemein/Studie_Selbst-undFremdbild_DSB_08122011.pdf.

[2] Art. 5 der Richtlinie 2008/8/EG

an Nichtunternehmer nun der Staat ist, in dem der Leistungsempfänger ansässig ist oder seinen Wohnsitz bzw. gewöhnlichen Aufenthaltsort hat. Dies hat zur Folge, dass Unternehmen aus der digitalen Wirtschaft die Pflicht auferlegt wird, zum Zwecke der umsatzsteuerlichen Abrechnung umfängliche Kundendaten zu sammeln und über 10 Jahre zu verwahren. Denn je nach dem wo sich ein Kunde zum Zeitpunkt des Kaufabschlusses im europäischen Raum gerade befindet, fällt eine andere Mehrwertsteuer an. Dies widerspricht dem Grundsatz der Datensparsamkeit. So werden Unternehmen in diesem konkreten Fall dazu verpflichtet, umfassende Bewegungsprofile von Ihren Kunden anzulegen.

3. WIRKUNG AUF STARTUPS

Das geltende Datenschutzrecht entfaltet auf Startups die folgenden Wirkungen, die durch Verbesserung der datenschutzrechtlichen Rahmenbedingungen aufgehoben werden sollten.

a. Innovationshemmnis

Ein hoher datenschutzrechtlicher Standard erschwert bzw. verhindert Innovation. Die Erhebung und Verwertung von Daten spielt in der Digitalisierung eine wichtige Rolle. Wenn schon das Sammeln dieser Daten erschwert wird, dann wird die Schaffung darauf aufbauender innovativer Produkte unwahrscheinlich.

b. Wachstumshemmnis

Auch das Wachstum von Startups wird durch einen hohen Datenschutzstandard gehemmt. Aufgrund des weltweit uneinheitlichen Schutzniveaus stehen Startups, die sich im Wachstumsprozess befinden vor dem Problem, bei der Skalierung ihres Geschäftsmodells unterschiedliche Datenschutzstandards zu verbinden. Dies macht es nötig, Produkte und Dienstleistungen auf die Vorgaben des jeweiligen Zielstaates anzupassen, was hohe Investitionskosten verursacht und Startups somit das Wachstum erschwert.

c. *Standortnachteil*

Des Weiteren stellt der hohe Datenschutzstandard einen erheblichen Standortnachteil für Startups dar. Um dieses Schutzniveau einzuhalten, sind schon in der Gründungsphase im Vergleich zu anderen Ländern höhere Investitionen erforderlich, sodass es für Startups mit einem sehr datenreichen Geschäftsmodell attraktiver ist außerhalb Deutschlands zu gründen.

d. *Rechtsunsicherheiten*

Der hohe deutsche Datenschutzstandard führt für Startups und Investoren gleichermaßen zu Rechtsunsicherheit. Die Konsequenz ist, dass immer mehr Investoren aus anderen Ländern nicht in deutsche Startups investieren wollen. In Anbetracht der in Deutschland anzutreffenden sehr schwachen Finanzierungssituation für Startups ist dies fatal.

e. *Zusammenarbeit mit Konzernen*

In praktischer Hinsicht erschwert der hohe Datenschutzstandard auch die Zusammenarbeit von Startups mit größeren etablierten Unternehmen und Konzernen. Gerade die Datenschutz-Compliance von Zulieferern größerer Unternehmen, die auch Startups sein können, wirkt sich auf diese Zusammenarbeit sehr hinderlich aus. Dabei werden aus Gründen der Datenschutz-Compliance in großen Unternehmen so genannte Compliance-Klauseln mit umfassenden Pflichten für Startups und Kontrollrechten für Konzerne in Verträge eingebaut. Ein Startup wird diesen aus Gründen der schwächeren wirtschaftlichen Verhandlungsposition oft zustimmen müssen, sodass sich im Ergebnis etablierte Unternehmen erhebliche Einwirkungsmöglichkeiten auf das operative Geschäft eines Startups sichern können.

f. *Wettbewerbsnachteil*

Die hohen datenschutzrechtlichen Hürden für Startups führen auch zu einem Wettbewerbsnachteil auf globaler Ebene. Gerade Unternehmen aus den USA haben es leichter Daten in Deutschland zu erheben als deutsche Startups. Dies führt zu einem Wettbewerb, dessen Verlierer jetzt schon feststehen.

4. FALLBEISPIELE INNOVATIVER STARTUPS

a. Kamerabasierte Sensorsysteme

Kamerabasierte Sensorsysteme, die keine Bilder ausgeben sondern nur verarbeiten und daraus Entscheidungen ableiten oder reine Textdaten erzeugen, befinden sich in einer Grauzone. Diese finden bspw. in Autos als Parkhilfen Verwendung.

b. Cross Device Tracking

Problematisch ist auch so genanntes Cross Device Tracking. Darunter versteht man eine über die Grenzen einzelner mobiler und nichtmobiler Endgeräte hinausgehende statistische Erfassung von Kundendaten durch Online-Shops. Nutzer verhalten sich je nach dem welches Endgerät gerade benutzt wird unterschiedlich. Diese Technologie ermöglicht es das Verhalten des Nutzers besser zu verstehen.

c. Offline Analytics

Mit Offline Analytics Lösungen versucht man „Brick & Mortar Commerce“ (lokaler Einzelhandel) mit E-Commerce zu verbinden, indem man die Analysemöglichkeit des E-Commerce auf das Ladengeschäft versucht zu übertragen. Auf diese Weise kann dem Ladeninhaber dargestellt werden, an welcher Stelle sich seine Kunden im Laden am längsten aufhalten, welche Produkte besondere Aufmerksamkeit genießen und wie sich Kunden in seinem Laden bewegen. Des Weiteren können diese Offline Daten dann mit den jeweiligen Profildaten im Internet abgeglichen werden, sodass es einen nahezu nahtlosen Übergang zwischen der Geschäftswelt im On- und Offlinebereich geben könnte. Dem steht jedoch der Einwilligungsvorbehalt des Kunden vehement entgegen. Es ist vor allem schwierig von analogen Ladenbesuchern eine Einwilligung in die Verwendung ihrer (Bewegungs-) Daten im Ladenlokal zu erhalten.

d. Soziale Netzwerke

Unterschiedliche Datenschutzstandards im europäischen Raum und vor allem in den USA schaffen unterschiedliche Wettbewerbsbedingungen für die konkurrierenden Unternehmen. Besonders deutlich sieht man diese Unterschiede bei sozialen Netzwerken: So durchsucht LinkedIn nahezu ohne Benachrichtigung die Postfächer der sich registrierenden Nutzer, während diese Möglichkeit Xing aufgrund der hiesigen Datenschutzregeln verwehrt bleibt. Auf diese Weise gewinnt aber LinkedIn schneller

neue Nutzer, da noch nicht registrierte Kontakte per E-Mail im Namen der registrierten Person benachrichtigt werden können. Wie eine solche Situation enden kann, hat bereits StudiVZ verdeutlicht, die hohe Datenschutzstandards zu einem Wettbewerbsvorteil gegenüber Facebook machen wollten und in der Folge den Geschäftsbetrieb eingestellt haben.

e. Big Data

In Deutschland werden datenbasierte und Big-Data- Geschäftsmodelle nie zu Global Playern und das aus einem einzigen Grund: Der Grundsatz der Datensparsamkeit, auf dem das deutsche Datenschutzrecht aufbaut, verträgt sich einfach nicht mit der Grundidee von Big Data, nämlich große Datenmengen zu sammeln und nach neuen Verwertungsmöglichkeiten dieser zu forschen. Das deutsche Datenschutzrecht erschwert schon das Sammeln dieser Daten, während andere Rechtsordnungen, wie die der USA, in dieser Sache liberaler sind. Vor allem sind datenbasierte Geschäftsmodelle nicht per se als gesellschaftlich schädlich zu betrachten. Es gibt viele Projekte, die auf Grundlage umfangreicher Daten einen großen gesellschaftlichen Nutzen mit sich bringen, bspw. In den Bereichen Ökologie, Medizin und Verbraucherschutz,. Das Problem wurzelt dabei nicht im Sammeln der Daten, denn wenn im Internet frei verfügbare Daten nicht von deutschen Unternehmen gesammelt werden können, dann tun es andere. Es ist daher wichtig, in dem Wettbewerb um diese Daten nicht an letzter Stelle zu stehen und alles dafür zu tun um solche Big-Data-Projekte in Deutschland anzusiedeln. Eine zeitgemäße Datenpolitik reguliert die Nutzung der Daten, nicht ihre Erhebung.

f. Matching von Bewerbern und Unternehmen

Der Fachkräftemangel erfordert auch Innovation auf Seiten der Personalvermittler. Hier zu erwähnen sind Geschäftsmodelle, die sich auf das Matching von Kandidaten mit den passenden Unternehmen und umgekehrt fokussieren und dabei die Vorteile des Internets erkannt haben. Der Einwilligungsvorbehalt im Datenschutzrecht erschwert hier das Auffinden geeigneter Kandidatenprofile in sozialen Netzwerken durch Unternehmen.

Bundesverband Deutsche Startups e.V.
Im Haus der Bundespressekonferenz
Schiffbauerdamm 40
10117 Berlin

Tel.: +49 (0) 30 60 98 95 9 - 10
Fax: +49 (0) 30 60 98 95 9 – 19
info@deutschestartups.org

Eingetragen unter VR 32124 B / AG Berlin-Charlottenburg
Vorstand: Thomas Bachem | David Hanf | Erik Heinelt | Christian Miele | Florian Nöll | Stephanie Renda | Sascha Schubert