DATENZUGANG, DATENTEILUNG, DATENTREUHAND

Neue Instrumente der Datenpolitik

Frederick Richter, LL.M.

Bereits vor einem Jahr hatte die Bundesregierung skizziert, wie ihre für diesen Herbst angekündigte „Datenstrategie" aussehen soll. Eines der stark betonten Ziele ist die Erleichterung des Zugangs zu Daten. Die EU-Kommission hat in ihrer in diesem Jahr vorgelegten „Digitalstrategie" ebenfalls die Bedeutung besserer Verfügbarkeit und intensiverer Nutzung von Daten hervorgehoben. In beiden Papieren werden Daten als Schlüsselressource gesellschaftlichen Wohlstands gesehen und als Lösungshilfe für nahezu alle großen Aufgaben wie Umweltschutz, Klimaschutz, Innovationen und den Zusammenhalt der Gesellschaft. Daten werden offenbar als eine Art universelles Wundermittel betrachtet, seit wir im Datenzeitalter leben.

„Teile und herrsche (dann nicht mehr?)"

„Wissen ist Macht" heißt es schon lange. Weil in der digitalen Welt vor allem Daten Wissen enthalten und Macht generieren, heißt es inzwischen „Daten sind Macht". Damit das allgemeine Wohl und der Wettbewerb auf den Märkten nicht unter zu großer Machtfülle einzelner Akteure leiden, müssen die richtigen Instrumente gefunden werden. Eine kartellrechtliche Zerschlagung von Datenmonopolisten wird dabei als letztes Mittel angesehen. Die EU-Wettbewerbskommissarin und andere ziehen es vor, dass Daten „geteilt" werden. Hinter dieser eher untechnischen Begrifflichkeit verbirgt sich natürlich nicht etwa eine Halbierung von Datenbeständen, sondern eine Vervielfältigung. Im Anwendungsbereich der DSGVO würde eine Zugangsgewährung bzw. Weitergabe von Datenbeständen eine rechtfertigungspflichtige Verarbeitung bedeuten. Ob der Anwendungsbereich des Datenschutzrechts infolge von Personenbezug eröffnet ist, muss daher vor allen weiteren Überlegungen zum Datenteilen geklärt werden.

Mit dem rechtspolitischen Konzept einer Datenteilungspflicht unter dem griffigen und wohlklingenden Motto „Daten für alle" entstand 2019 ein Lösungsvorschlag, der geeignet scheint Bewegung in die Debatte um neue Wege zur Förderung der Datennutzung einerseits und zur Begrenzung von Datenmacht andererseits zu bringen. Es geht dabei um Umsetzungsmöglichkeiten und Erfolgschancen einer Regulierung von nicht-personenbezogenen Daten zur Wettbewerbsförderung. Eine solche Pflicht zum Teilen anonymer und anonymisierter Daten überträgt in gewisser Weise den im öffentlichen Bereich schon länger diskutierten Open-Data-Gedanken auf den privaten Sektor.

Was ist nun der Bezug zum Datenschutz – wo dieser doch nun einmal die von einer etwaigen Datenteilungspflicht allein umfassten anonymen Daten gar nicht erfasst? Einerseits ist die Abgrenzung zwischen einem „Open Data im nicht-öffentlichen Bereich" und dem sachlichen Anwendungsbereich des Datenschutzrechts von entscheidender Bedeutung. Und andererseits gibt es eine Parallele in der Zielstellung: Sowohl

der Datenschutz als auch der Vorschlag zu einer Datenteilungspflicht bezwecken einen Ausgleich von Machtungleichgewichten. Zwar nennt das Datenschutzrecht selber ein solches Schutzziel nicht, doch begreifen nicht wenige den Datenschutz auch als Machtausgleichsinstrument und nicht „nur" als Mittel zum Zweck des Privatsphärenschutzes. Auch durch das Datenteilen sollen Machtverzerrungen ausgeglichen werden – allerdings nicht mit Blick auf das Individuum, sondern mit Blick auf den Wettbewerb. Einem eher humanistisch ausgerichteten Machtausgleichsinstrument wie dem Datenschutz steht mit der Datenteilung somit ein eher ökonomisch motivierter Ansatz gegenüber.

Eine weitere Parallele findet sich innerhalb des Datenschutzrechts und zwar mit dem Recht auf Datenübertragung aus Art. 20 DSGVO. Dieses junge Betroffenenrecht sucht sogar beide zuvor genannten Ansätze zu verbinden. Es soll sowohl die persönliche Datenkontrolle der einzelnen Person steigern als auch den Wettbewerb im Datenmarkt fördern, indem Betroffene die sie betreffenden Daten weg von Datenmonopolisten und hin zu (bestenfalls datenschutzaffineren) anderen Anbietern transferieren können. Die Idee hinter dem Portabilitäts- und Portierungsrecht der Verbraucher erscheint sehr lobenswert. In der Praxis spielt der Artikel 20 gleichwohl noch keine Rolle – wegen Unkenntnis in der Nutzerschaft, vor allem aber wegen (datenschutzrechtlich zulässiger) Inkompatibilität der digitalen Angebote. Ohne eine Pflicht zur Interoperabilität könnte die Datenportabilität ein bloßes Recht auf dem Papier bleiben.

Wo beginnt der Datenschutz?

Was die Datenteilung betrifft, so erscheint die Abgrenzung zum Datenschutz zunächst trivial: Entweder sein Anwendungsbereich ist durch einen Personenbezug der zu teilenden Daten eröffnet, dann ist der Anwendungsbereich einer Datenteilungspflicht verschlossen. Oder die Daten stehen mangels Personenbezug oder Personenbeziehbarkeit außerhalb des Datenschutzes und wären einer Datenteilung bzw. Datenumverteilung zugänglich.

Doch wie zukunftsfest ist diese eingängige Abgrenzung angesichts stetig steigenden Rechenleistungen und immer besserer Auswertungsmöglichkeiten mit Big-Data-Methoden, die De-Anonymisierungen durch das Übereinanderlegen von Datenmustern und -rastern erleichtern? Und wie wäre mit dem Risiko umzugehen, dass anonyme oder anonymisierte Daten den Einflussbereich eines Verantwortlichen zwar ohne Bedenken verlassen, im Einflussbereich eines anderen Verantwortlichen aber auf eine bestimmbare Person zurückgeführt werden können? Der Daten-für-alle-Vorschlag sieht diesbezüglich die Verantwortlichkeit beim Unternehmen, das die Daten abgibt. Das datengebende Unternehmen habe vor einer Weitergabe nicht-personenbezogener oder vormals personenbezogener Daten sicherzustellen, dass auch zukünftig keine Re-Identifizierung möglich ist – eine nicht zu unterschätzende Aufgabe, selbst für die vom Vorschlag adressierten marktbeherrschenden Unternehmen.

Wer kann Anonymität garantieren?

Die Verantwortungslast bezüglich einer nachhaltigen Anonymisierung scheuen Unternehmen auch deshalb, weil Orientierungspunkte für die Anonymisierung fehlen. Noch gibt es keinerlei Normen oder Standards für den relevanten Vorgang des Anonymisierens. Wie eine hinreichend belastbare Anonymisierung erreicht werden kann, dazu gibt es bislang keine offiziellen Maßgaben, keine Kurzpapiere, Entschließungen, Orientierungshilfen oder andere Anwendungshinweise – weder von der Konferenz der deutschen Datenschutzaufsichtsbehörden noch vom EU-Datenschutzausschuss. Dies bewirkt Unsicherheiten sowohl in Bezug auf das beschriebene Konzept des Datenteilens als auch allgemein in Bezug auf das Nutzen anonymer Daten. Denn wenn mangels Regelung die zu erfüllenden Voraussetzungen für eine belastbare und rechtssichere Anonymisierung unklar sind, kann dies im Effekt dazu führen, dass Daten nicht genutzt werden, obwohl von ihnen mangels Personenbezug eigentlich gar kein Risiko für Rechte und Freiheiten natürlicher Personen mehr ausgehen kann.

Daten zu treuen Händen?

In der Datenstrategie der Bundesregierung spielt ein weiteres neues Instrument eine Rolle: Das freiwillige Datenteilen soll durch vertrauenswürdige Datentreuhänder gefördert werden. Die dazugehörigen Datentreuhandmodelle werden im politischen Raum im Zusammenhang mit der Lösung unterschiedlicher Fragestellungen der Datenpolitik diskutiert. Ein Ergebnis wissenschaftlicher Auseinandersetzung mit den verschiedenen Modellen, ihren Zwecken, Randbedingungen und Limitationen ist derzeit jedoch noch nicht verfügbar. Auch praktische Vorbilder sind noch rar. In Großbritannien gibt es erste Erfahrungen mit dem Instrument eines „Data Trust". Im Rahmen dieses Projekts haben bei der UK Biobank eine halbe Million Personen freiwillig ihre Gesundheitsdaten sozusagen „zu deren treuen Händen" hinterlegt, damit die Einrichtung sie nach festgelegten Prinzipien zu Forschungszwecken freigibt.

Ein ähnliches Konzept verfolgt aktuell das Robert-Koch-Institut mit seiner (nicht mit der Corona-Warn-App zu verwechselnden) Datenspende-App.

Zu klären sein wird jedoch zunächst, welches Problem mit einer Datentreuhand vornehmlich gelöst werden soll. Denn abhängig davon, ob es um eine industrie-, wettbewerbs- oder datenschutzpolitische Fokussierung geht und davon, welchen Nutzen man sich von Datentreuhändern verspricht, fällt die Definition von Datentreuhändern unterschiedlich aus. Der Begriff der „Datentreuhand" ist nicht klar abgegrenzt und wird für ganz unterschiedliche Funktionen und Geschäftsmodelle verwendet. Eine Datentreuhand könnte verschiedene Formen haben und sehr unterschiedliche Funktionen wahrnehmen:

- Stärkung individueller Kontrolle über Datenflüsse
- Förderung der Teilhabe der Datensubjekte an wirtschaftlicher Verwertung von Daten
- Förderung von Datenteilung und Verfügbarmachung von Daten zur Förderung von Innovation und Wettbewerb
- Bereitstellung qualitativ hochwertiger Daten für Wissenschaft und Forschung
- Einschränkung der marktbeherrschenden Stellung großer Plattformbetreiber
- Förderung vertrauenswürdiger europäischer Plattformangebote
- Bildung eines Vertrauensankers und Vermittlers zwischen Datengebern und Datennehmern

Die multifunktionale Treuhand

Welche diese Aufgaben eine kommende Datentreuhand übernehmen soll, ist politisch noch nicht entschieden. Die Koalitionspartner der Bundesregierung setzten in ihren jeweiligen Positionspapieren vom Mai dieses Jahres dazu unterschiedliche Schwerpunkte. Die Unionsfraktion sieht in Datentreuhandmodellen vor allem eine "gute Möglichkeit, Teilen von Daten und die Nutzung durch Dritte über neutrale Instanz zu erleichtern und private wie unternehmerische Ansprüche geltend zu machen." Die SPD betont eher den verbraucherbezogenen Aspekt und zielt ab auf den „Aufbau einer Datentreuhänderstruktur für den Schutz persönlicher und personenbezogener Daten und eine parallele, sektorbezogene Struktur für den Austausch und zum Teilen von nicht-personenbezogenen Datensets zwischen unterschiedlichen Akteuren". Die Praxis solle wie folgt aussehen: „Datentreuhänder verwalten die Verwendung von persönlichen Daten nach den Bedürfnissen und persönlichen Einstellungen der Bürgerinnen und Bürger. Sie organisieren die Durchsetzung persönlicher Rechte, gewährleisten eine datensparsame Autorisierung gegenüber Dritten (etwa auf Grundlage eines Personal Identity Management Systems) und können auch die temporäre Überlassung von Daten an Dritte etwa zu Forschungszwecken organisieren."

Klare Ausrichtung notwendig

Datentreuhandmodelle sollen Chancen im Umgang mit Daten eröffnen, indem sie das Teilen von Daten erleichtern, die Verfügung über Daten durch Datensubjekte vereinfachen und das Vertrauen in die Datenwirtschaft erhöhen. Wegen des denkbar weiten Anwendungsbereichs von Datentreuhändern und der bislang arg begrenzten praktischen Erfahrungen wird eine Umsetzung wohl nur schrittweise erfolgen können. Zudem müssen die Wechselwirkungen zwischen Markt, Technologie und Recht im Blick behalten werden und natürlich stets Datenschutzkonformität gewahrt sein. Ob, wann und wie eine Umsetzung der verschiedenen datenpolitischen Ideen erfolgt, bleibt daher abzuwarten. Die Frage des Zugangs zu Daten wird jedoch immer mehr in den Vordergrund rücken. Zukünftig wird es weniger darum gehen, wem Daten „gehören", sondern vor allem, wer die Daten nutzen darf. Treuhandmodelle scheinen durchaus geeignet, Anreize zu setzen, um das freiwillige Teilen von Daten und die Nutzung durch Dritte über eine neutrale Instanz zu erleichtern.

Über den Autor

Frederick Richter, LL.M.
ist Vorstand der Stiftung Datenschutz.

▶ https://stiftungdatenschutz.org/startseite/

STIFTUNG DATENSCHUTZ