HINTERGRUND DER ÄNDERUNGSVORSCHLÄGE

Das Datenschutzrecht befindet sich wie kein anderes Rechtsgebiet im Spannungsverhältnis zwischen Rechtssicherheit und Innovationsoffenheit. Dieses spitzt sich bei der Frage nach der Anwendung des datenschutzrechtlichen Zweckbindungsgrundsatzes auf Innovationsprozesse in Startups aus dem Bereich Big Data besonders zu. Der datenschutzrechtliche Zweckbindungsgrundsatz verlangt, dass das datenerhebende Startups an die zum Zeitpunkt der Erhebung bestimmten Zwecke der späteren Datennutzung gebunden ist. Er stellt damit eine Anforderung dar, die Startups angesichts ihrer explorativen und somit prozessoffenen Entwicklung kaum erfüllen können: Wie soll ein Startup die spätere Verwendung der Daten zum Zeitpunkt ihrer Erhebung angeben können, wenn es noch nicht einmal sein Produkt geschweige denn Geschäftsmodell kennt?

Um das Spannungsverhältnis zwischen dem Bedürfnis nach Rechtssicherheit einerseits und nach Innovationsoffenheit des Datenschutzrechts andererseits aufzulösen, bauen die von mir vorgeschlagenen Änderungen des aktuellen Entwurfs der EU-Datenschutz-Grundverordnung (Grund-VO) auf dem wie folgt dargestellten verfassungsrechtlichen Verständnis auf:

Datenschutz als Schutzinstrument für grundrechtlich geschützte Rechtsgüter

Datenschutz stellt grundsätzlich kein eigenständiges Schutzgut dar, sondern ein Regelungsinstrument, das grundrechtliche Gewährleistungsgehalte wie den Schutz der Privatsphäre oder anderer spezieller Freiheitsrechte ermöglichen, unterstützen und fördern soll. Die grundsätzliche Ungeeignetheit von Datenschutz als eigenständiger Gewährleistungsgehalt liegt darin begründet, dass Daten selbst keine Gefahr für den von der Datensammlung oder -verarbeitung Betroffenen auslösen, sondern erst die Informationen, die durch subjektive Interpretationen dieser Daten in Abhängigkeit des jeweiligen sozialen Kontexts entstehen. Da Daten die Grundlage von potentiell später durch Informationsverarbeitung auftretenden Verletzungen bilden, ist eine rechtliche Anknüpfung an Daten jedoch vertretbar. Sie ist darüber hinaus geeignet, den sachlichen Schutzbereich der zu schützenden Gewährleistungsgehalte im Sinne eines konkreten oder auch abstrakten Gefährdungsschutzes vor zu verlagern. Ob die durch den Gesetzgeber zu typisierenden Fälle einen konkreten oder abstrakten Gefährdungsschutz tatsächlich erfordern, ist anhand der jeweils betroffenen – und der gegebenenfalls kollidierenden – Gewährleistungsgehalte zu ermitteln.

Die durch automatisierte Daten- und Informationsverarbeitung typischerweise betroffenen Gewährleistungsgehalte sind mit einem eng verstandenen Schutz der „Privatsphäre“ nicht ausreichend abgebildet. Zu Recht stellt Art. 7 der Charta der Grundrechte der Europäischen Union (EU-Charta) daher nicht auf diesen einen Begriff ab, sondern definiert seinen Gewährleistungsgehalt über eine Aufzählung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation. Auch gewährleistet die Eigenständigkeit von Art. 8 EU-Charta – der insofern von der Regelungskonzeption der Europäischen Konvention für Menschenrechte abweicht – dass sich der darin vorgesehene und hier grundsätzlich als Regelungsinstrument verstandene Datenschutz nicht als Schutz der in Art. 7 EU-Charta genannten Gewährleistungsgehalte erschöpft, sondern auch auf die Garantien der weiteren Grundrechte bezogen werden kann. Neben den in Art. 7 EU-Charta ausdrücklich genannten Gewährleistungsgehalten kommt hier zudem das implizit ebenfalls erfasste Recht auf Selbstdarstellung in der Öffentlichkeit als typischerweise durch die automatische Daten- und Informationsverarbeitung betroffener Gewährleistungsgehalt in Betracht. Des Weiteren kommen die speziellen Freiheitsrechte der Gedanken-, Gewissens- und Religionsfreiheit in Art. 10 EU-Charta, der Meinungsäußerung und der Informationsfreiheit in Art. 11 EU-Charta, der Versammlungs- und Vereinigungsfreiheit in Art. 12, der Kunst- und Wissenschaftsfreiheit in Art. 13 EU-Charta sowie der Berufs-, unternehmeri-

schen und der Eigentumsfreiheit in den Art. 15 bis 17 EU-Charta in Betracht. Auch können die Diskriminierungsverbote der Art. 20 bis 26 EU-Charta durch moderne Daten- und Informationsverarbeitung betroffen sein. Entsprechend der ständigen Rechtsprechung des Bundesverfassungsgerichts kann als eigenständiger Gewährleistungsgehalt zudem das Recht des Einzelnen auf Kenntnis darauf angesehen werden, was Dritte über ihn oder sie mittels systematischer bzw. automatischer Daten- und Informationsverarbeitung wissen. Dieses müsste freilich einem der genannten Grundrechte der EU-Charta zugeordnet werden, da das Informations- und Auskunftsrecht in Art. 8 Abs. 2 EU-Charta hier nicht als eigenständiger Gewährleistungsgehalt, sondern allein als Schutzinstrument zur Durchsetzung der bereits genannten Gewährleistungsgehalte verstanden wird.

Zweckbestimmungs- und Zweckbindungsgrundsatz

Wie anfangs bereits benannt, spielt der Zweckbestimmungs- bzw. Zweckbindungsgrundsatz für Innovationsprozesse in Startups aus dem Bereich Big Data eine herausragende Rolle. Er wurde in Deutschland mit dem Volkszählungsurteil im Staat-Bürger-Verhältnis verfassungsrechtlich anerkannt. Auf einfachgesetzlicher Ebene findet er sich auch für den privaten Sektor in zahlreichen Erlaubnistatbeständen wieder. Unklar ist, wie weit er zwischen Privaten auch verfassungsrechtlich geboten ist.

Für die Beantwortung dieser Frage ist zwischen dem Gebot der Zweckbestimmung einerseits und dem der Zweckbindung andererseits zu unterscheiden. Während das Gebot der Zweckbestimmung nur die Angabe des mit dem jeweils rechtlich relevanten Akt der Datenerhebung bzw. -verarbeitung verfolgten Zwecks erfordert, schränkt das Gebot der Zweckbindung die nachfolgende Verarbeitung der Daten auf die bei ihrer Erhebung angegebenen Zwecke weiter ein. Im Staat-Bürger-Verhältnis folgt die Zweckbindung zwingend aus dem Prinzip der Gesetzmäßigkeit der Verwaltung. Nach ihr darf die Datenerhebung und -verarbeitung nur für gesetzlich festgelegte Zwecke erfolgen, sofern und soweit sie hierfür geeignet und erforderlich ist. Eine nachträgliche Zweckänderung für bereits erhobene Daten ist nach der Rechtsprechung des Bundesverfassungsgerichts möglich, wenn die Zweckänderung selbst wieder auf einer verfassungsgemäßen Gesetzesgrundlage beruht und sie mit den ursprünglichen Zwecken nicht unvereinbar ist. In der Literatur wird meist nicht nur das Gebot der Zweckbestimmung, sondern auch das der weitergehenden Zweckbindung auf das Verhältnis zwischen Privaten übertragen. Eine generelle Geltung des Zweckbindungsgrundsatzes zwischen Privaten ist verfassungsrechtlich jedoch nicht zwingend. Dass hingegen das Gebot der Zweckbestimmung auch für den privaten Sektor gelten muss, ergibt sich aus dem Umstand, dass ohne Zweckangabe eine Bestimmung der mit dem Akt der Datenerhebung bzw. -verarbeitung verbundenen Gefahr für die Gewährleistungsgehalte des Betroffenen nicht möglich wäre. Erst die Angabe des verfolgten Zwecks beschreibt den Kontext der geplanten Datenverarbeitung und damit der Informationsgewinnung und -verwendung. Erst dieser durch den Zweck beschriebene Kontext ermöglicht also die Beurteilung, ob die Informationsgewinnung und -verwendung die grundrechtlichen Gewährleistungsgehalte des Betroffenen verletzt. Demgegenüber ist die Zweckbindung nur dann erforderlich, wenn es kein anderes Mittel gibt, das die Gewährleistungsgehalte des Einzelnen genauso schützt und zugleich kollidierende verfassungsrechtlich geschützte Interessen Dritter nicht weniger beschränkt. Diese Abwägung kann angesichts der Vielfalt und Vielschichtigkeit der widerstreitenden privaten Interessen nicht generell vorgenommen werden.

Verbot mit Erlaubnisvorbehalt: Einwilligung und gesetzliche Ermächtigung

Ob der Zweckbindungsgrundsatz auch zwischen Privaten gilt, hängt zudem von dem spezifischen datenschutzrechtlichen Regelungsinstrument ab, das die durch die moderne Daten- und Informationsverarbeitung gefährdeten grundrechtlichen Gewährleistungen schützen soll. Art. 8 Abs. 2 EU-Charta sieht insofern vor, dass personenbe-

zogene Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“. Der Wortlaut lässt damit offen, wann die Festlegung der Zwecke konkret erfolgen soll und ob eine spätere Verarbeitung an die gegebenenfalls schon bei Erhebung festgelegten Zwecke gebunden sein soll. Zumindest der Zweckbestimmungsgrundsatz ist verfassungsrechtlich garantiert. Ungeachtet dessen ob man Art. 8 Abs. 2 EU-Charta eine unmittelbare oder nur mittelbare Wirkung zwischen Privaten zuerkennt, steht es dem Gesetzgeber im Rahmen einer Abwägung der kollidierenden, grundrechtlich geschützten Interessen somit frei, ob er eine über das Zweckbestimmungsgebot hinausgehende Zweckbindung verlangt und welches der genannten Regelungsinstrumente er wählt.

Entscheidet sich der Gesetzgeber freilich für das Instrument Einwilligung, zieht dieses zwangsläufig die Anwendung des Zweckbindungsgrundsatzes nach sich. Denn das Institut der Einwilligung würde ins Leere laufen, wenn der durch die Einwilligung Begünstigte nicht an ihren Inhalt, sprich den oder die Zweck/e der darin vorgesehenen Daten- und Informationsverarbeitung bzw. -verwendung gebunden wäre. In diesem Lichte stellt sich das Instrument der Einwilligung zwar als das Mittel dar, das dem Betroffenen zumindest theoretisch mehr Einflussmöglichkeiten belässt, dem Verarbeiter der Daten- bzw. Informationen aber grundsätzlich stärker bindet als die gesetzliche Ermächtigungsgrundlage, die zwischen Privaten eine Anwendung des Zweckbindungsgrundsatzes offen lässt.

Folgerungen in Hinsicht auf die Änderungsvorschläge

Das Verständnis des Datenschutzgrundrechts in Art. 8 EU-Charta als reines Schutzinstrument zielt darauf ab, die Komplexität des aktuellen Datenschutzrechts zu reduzieren, indem die vielseitigen und durch die Daten- und Informationsverarbeitung kontextabhängig bedingten Gefahren nicht von einem einzelnen „Supergrundrecht“ aufgefangen werden müssen, sondern den unterschiedlichen grundrechtlichen Gewährleistungsgehalten und damit der jeweils bereits entwickelten Judikatur zugeordnet werden können. Die grundrechtlichen Gewährleistungsgehalte bilden dabei den Maßstab, welcher Kontext der Informationsgewinnung und -verwendung rechtlich relevant ist. Je nach Gefährdungslage kann bzw. muss der Gesetzgeber unter Berücksichtigung der kollidierenden Rechtsgütern Dritter einen konkreten oder abstrakten Schutzansatz wählen.

Stellt sich im Wege einer typisierenden Betrachtung die Gefährdungslage für die durch die Daten- und Informationsverarbeitung Betroffenen als gering dar, genügt grundsätzlich ein konkreter Gefährdungsschutz. Nur eine besondere Gefährdungslage erfordert einen abstrakten Gefährdungsschutz. Letztere wird zum Beispiel angenommen, wenn der Grundrechtseingriff durch die konkrete Daten- bzw. Informationsverarbeitung typischerweise als besonders intensiv vorhergesehen werden kann. Für die Bewertung der Intensität können unter anderem die Umstände der Datenerhebung (zum Beispiel ob die Daten im Wege eines Logins, über Tracking oder Data Mining erhoben werden), die Art der Daten (vergleiche die Diskriminierungsverbote in Art. 20 bis 26 EU-Charta) und ob diese öffentlich zugänglich sind sowie der Grad des Personenbezugs bzw. wie leicht dieser durch den Verarbeiter oder Verwender der Daten bzw. Informationen hergestellt werden kann, herangezogen werden. Auch Profiling, insbesondere wenn kontextvorhersagende Algorithmen zum Einsatz kommen, oder die reine Größe des Datenpools werden als besondere Gefährdungslagen angesehen. Die Datenerhebung bzw. -verarbeitung sowie die Informationsgewinnung und -nutzung erfordern jedenfalls nur dann eine Einwilligung des Betroffenen bzw. eine sonstige gesetzliche Grundlage, wenn eine abstrakte oder zumindest konkrete Gefährdungslage bezogen auf die grundrechtlichen Gewährleistungsgehalte vorliegt.

Setzt der Gesetzgeber danach eine legitime Grundlage für die Datenerhebung- und -verarbeitung bzw. die Informationsgewinnung und -verwendung voraus, steht es ihm

grundsätzlich frei, ob er über die Zweckbestimmung hinaus auch eine Zweckbindung verlangt. Letztere bildet das grundrechtliche Interessen Dritter beschränkendere Instrument. Als noch einschränkender kann sich die Wahl der Einwilligung darstellen, da sie nicht nur die Zweckbindung, sondern auch einen direkten Kontakt des Verarbeiters oder Verwenders der Daten bzw. der Informationen zu dem Betroffenen voraussetzt. Sollen Daten, die auf Grundlage einer Einwilligung erhoben wurden, später gemäß eines gesetzlichen Erlaubnis verwendet werden, dürfen diese gesetzlich vorgegebenen Zwecke nicht mit den in der Einwilligung angegeben unvereinbar sein.

Stellt die Einwilligung nicht mehr die vorherrschende legitime Grundlage für Daten- und Informationsverarbeitungen dar, muss insbesondere das Recht des Einzelnen auf Kenntnis des Wissens Dritter um seine persönlichen Umstände auf andere Weise sichergestellt werden. Hierfür ist die Einwilligung nach praktischer Erfahrung ohnehin nicht das effektivste Instrument. Zielführender als sprachliche Erklärungen können automatisierte Visualisierungen die erforderliche Transparenz herstellen. Falls kein Kontakt des Daten- bzw. Informationsverarbeiters zu den Betroffenen besteht, können diese über allgemein zugängliche Schnittstellen bereitgestellt werden. Hierfür genauso wie für die Angabe der rechtlich relevanten Zwecke sollten Schiedsgerichts- oder andere selbstregulierte Stellen entsprechende Standards festlegen.