Datenschutz für das Digitale Zeitalter – Die EU-Datenschutz-Grundverordnung

Am 25. Mai 2016 ist die EU-Datenschutz-Grundverordnung in Kraft getreten. Sie wird ab Mai 2018 in allen Mitgliedstaaten der EU unmittelbar anwendbar sein. Mit der Verordnung gibt sich Europa einheitliche und zukunftsorientierte Regeln für die digitalisierte Datenökonomie des 21. Jahrhunderts.

Datenschutzrecht als Zukunftsthema

In nie dagewesenem Umfang werden heute personenbezogene Daten erhoben, verarbeitet und weiterverarbeitet. Und aufgrund der fortschreitenden Digitalisierung werden es in Zukunft immer mehr: Smart Homes, Smart Cars, Plattformen zur digitalen Vernetzung – die Liste ließe sich beliebig fortsetzen. Vor diesem Hintergrund wird die Frage nach den datenschutzrechtlichen Rahmenbedingungen immer wichtiger: Wer darf was mit den Daten der Nutzer digitaler Dienste tun? Wo liegen die Grenzen zulässiger Datennutzungen?

Angesichts der Chancen und Herausforderungen von „Big Data“ bedarf es Regeln, die die Datensouveränität des Einzelnen und das große wirtschaftliche und gesellschaftliche Potenzial der Digitalisierung in einen angemessenen Ausgleich bringen. Datenschutz und „Big Data“ sind hierbei keineswegs unvereinbare Gegensätze. Notwendig sind vielmehr ausgewogene staatliche Steuerungsinstrumente, die sowohl den Interessen der Nutzer digitaler Dienste als auch den legitimen ökonomischen Interessen der datenverarbeitenden Unternehmen Rechnung tragen.

Ein einheitlicher Rechtsrahmen für Europa

In einer international vernetzten Datenökonomie sind rein nationale Datenschutzregeln allerdings nicht ausreichend. Deshalb legte die Europäische Kommission im Jahr 2012 den Entwurf einer EU-Datenschutz-Grundverordnung vor. Ziel war es, die EU-Datenschutz-Richtlinie aus dem Jahr 1995 zu ersetzen und das europäische Datenschutzrecht an die Herausforderungen des digitalen Zeitalters anzupassen. Im Dezember 2015 schließlich einigten sich Europäisches Parlament, Rat und Kommission auf einen endgültigen Verordnungstext, der seit Verkündung im Amtsblatt der EU am 25. Mai 2016 in Kraft ist. Die neuen europäischen Datenschutzvorgaben werden nach einer zweijährigen Übergangsphase ab Mai 2018 unmittelbar anwendbar sein. Bestehende nationale Regelungen werden durch die vorrangige Datenschutz-Grundverordnung zu einem großen Teil abgelöst werden.

Eine der größten Errungenschaften der Datenschutz-Grundverordnung ist die Schaffung eines europaweit einheitlichen „Level Playing Field“ im Bereich des Datenschutzes. Gemeint ist, dass alle Mitgliedstaaten der Euro-

päischen Union im Bereich der Digitalökonomie nach denselben Spielregeln spielen. Wettbewerbsverzerrungen infolge unterschiedlicher nationaler Datenschutzregeln werden weitgehend beseitigt. Dies schafft Rechtssicherheit sowohl für Bürgerinnen und Bürger als auch für Unternehmen.

Der Harmonisierungseffekt wird zudem durch das neu eingeführte „Marktortprinzip“ noch verstärkt: Danach gilt die EU-Verordnung auch für solche Datenverarbeiter, die zwar nicht in der EU niedergelassen sind, aber auf dem hiesigen Markt Waren und Dienstleistungen anbieten – dies betrifft zum Beispiel Unternehmen wie Google und Facebook.

Stärkung der Datensouveränität

Die Datenschutz-Grundverordnung schafft einen Rechtsrahmen, der eine Balance zwischen den Interessen der Bürgerinnen und Bürger am Schutz ihrer Daten und den legitimen ökonomischen Interessen der Wirtschaft an der Nutzung personenbezogener Daten herstellt. Der selbstbestimmte Umgang der Bürgerinnen und Bürger mit den eigenen Daten wird durch zahlreiche Neuerungen gestärkt: Die Informationspflichten, die zum Beispiel Anbieter von Smartphone Apps oder sozialen Netzwerken gegenüber ihren Nutzern erfüllen müssen, sind klarer gefasst als bislang. So verlangt die neue Verordnung ausdrücklich, dass digitale Anbieter ihre Nutzungsbedingungen leicht zugänglich, verständlich und in klarer Sprache abfassen. Die konkreten Zwecke der Datennutzung sind vom Anbieter transparent zu machen. Darüber hinaus müssen die datenschutzrechtlichen Einwilligungen der Nutzer eindeutig und unmissverständlich bekundet werden – Stillschweigen oder das Bestätigen bereits vorangekreuzter Kästchen reichen nicht aus. All diese Vorgaben stärken die Datensouveränität der Nutzer.

Neu ist auch, dass die Datenschutz-Grundverordnung ein Recht auf Datenportabilität enthält. Nutzer digitaler Dienste haben demnach unter bestimmten Voraussetzungen das Recht, die Übertragung ihrer Daten von einem Unternehmen zu einem anderen Unternehmen zu verlangen. Hinzu kommt das Recht, von einem datenverarbeitenden Unternehmen konkrete Auskunft darüber zu erlangen, welche Daten es über sie gespeichert hat und wie lange und auf welche Weise die Daten verwendet werden. Nutzer können zudem die unverzügliche Löschung ihrer Daten verlangen, wenn diese für den Datenverarbeitungszweck nicht mehr benötigt werden.

Flexibilität für digitale Geschäftsmodelle

Neben der Stärkung der Rechte von Nutzern digitaler Dienste sichert die Datenschutz-Grundverordnung auch die legitimen ökonomischen Interessen der Wirtschaft an der Nutzung personenbezogener Daten. Im Zuge der Rats- und Trilogverhandlungen hat sich die Bundesregierung zum einen dafür eingesetzt, etablierte Geschäftsmodelle, die auf die Nutzung personenbezogener Daten angewiesen sind, zu erhalten. Zum anderen war es ein Anliegen der Bundesregierung, die Vorgaben der Datenschutz-Grundverordnung so zu gestalten, dass sie einen offenen und zukunftsorientierten Rechtsrahmen auch für neue, innovative Geschäftsmodelle darstellt.

Eine wichtige Errungenschaft ist, dass die Anonymisierung und Pseudonymisierung personenbezogener Daten im Verordnungstext stärker verankert sind. Anonymisierung bezeichnet das Verändern personenbezogener Daten derart, dass die Daten nicht mehr einer Person zugeordnet werden können. Bei der Pseudonymisierung werden die personenbezogenen Daten durch Pseudonyme ersetzt, um die Identifizierung einer Person zu erschweren. Beide Methoden ermöglichen die Verarbeitung großer Mengen von Daten ohne direkten Personenbezug – das ist wichtig für Big-Data-Anwendungen und stärkt den Datenschutz. Ein konkretes Beispiel: Die Datenschutz-Grundverordnung stellt ausdrücklich klar, dass die Nutzung von Daten zu

anderen als ursprünglich vorgesehenen Zwecken insbesondere dann zulässig sein kann, wenn die Daten in anonymisierter oder pseudonymisierter Form weiterverarbeitet werden. Gerade für den Bereich kommerzieller Datenweiterverarbeitungen schafft diese Vorschrift einen hinreichend offenen und flexiblen Rahmen.

Differenzierte Haftungsregeln

Begleitet werden die Vorgaben zur Zulässigkeit von Datennutzungen durch klare und differenzierte Regelungen zur Haftung von Unternehmen, die Daten rechtswidrig verwenden. So haftet ein Unternehmen beispielsweise nicht, wenn es nachweisen kann, dass es nicht für die schadensbegründenden Ursachen verantwortlich ist. Datenverarbeiter, die im Auftrag anderer Unternehmen handeln, wie zum Beispiel Cloud-Dienste-Anbieter, haften nur, wenn sie speziell an Auftragsdatenverarbeiter gerichtete Pflichten aus der Datenschutz-Grundverordnung verletzen oder gegen rechtmäßige Weisungen des Auftraggebers verstoßen und dabei in Widerspruch zur Datenschutz-Grundverordnung handeln. Diese auch auf Betreiben der Bundesregierung erreichten Regelungen sind ein großer Fortschritt gegenüber dem ursprünglichen Verordnungsentwurf der Kommission. Dieser hatte noch eine kumulative Haftung vorgesehen, wonach sich Auftragsdatenverarbeiter sämtliches Fehlverhalten der Auftraggeber im Rahmen der Nutzung der personenbezogenen Daten hätten zurechnen lassen müssen.

Grenzüberschreitende Harmonisierung der Datenschutzaufsicht

Eine wirkliche Harmonisierung des Datenschutzrechts in Europa kann nur gelingen, wenn auch die Auslegung und Anwendung der Verordnung durch die unabhängigen nationalen Datenschutzaufsichtsbehörden harmonisiert und koordiniert werden. Ein europaweit gültiges Datenschutzrechtsregime erfordert daher einheitliche Regelungen darüber, welche Datenschutzbehörde bei grenzüberschreitenden Datenverarbeitungsvorgängen die Einhaltung der Datenschutz-Grundverordnung kontrolliert. Hier ist ein so genannter „One-Stop-Shop-Mechanismus“ vorgesehen. Danach soll stets die Aufsichtsbehörde in dem Mitgliedstaat federführend zuständig sein, in dem das Unternehmen seine Hauptniederlassung hat. Geht es um eine Niederlassung in anderen Ländern, werden die Aufsichtsbehörden der jeweils anderen Länder in die Entscheidungsfindung einbezogen. Sollten die verschiedenen Aufsichtsbehörden zu unterschiedlichen Auffassungen gelangen, ist ein Streitschlichtungsmechanismus vor dem Europäischen Datenschutzausschuss („European Data Protection Board“) vorgesehen.

Anpassung des deutschen Datenschutzrechts

Der deutsche Gesetzgeber ist gefordert, bis zur Anwendbarkeit der Datenschutz-Grundverordnung im Mai 2018 das gesamte deutsche Datenschutzrecht auf seine Vereinbarkeit mit den neuen Regeln hin zu überprüfen. Nationale Datenschutzvorschriften können nur dann erhalten werden, wenn die Datenschutz-Grundverordnung eine Öffnungsklausel vorsieht, die den Erhalt der Vorschrift ermöglicht. Im Übrigen wird die vorrangige Datenschutz-Grundverordnung das bestehende nationale Datenschutzrecht ersetzen.

Ist diese Umstellung geschafft, schließen sich für Wirtschaft und Datenschutzaufsicht praktische Herausforderungen bei der Anwendung des neuen Rechts an. Der Umstand, dass die Datenschutz-Grundverordnung insbesondere im kommerziellen Bereich weniger detailliert ist als das bestehende Bundesdatenschutzgesetz, wird eine ausgewogene Auslegung der Verordnung sowohl auf Seiten der Wirtschaft als auch auf Seiten der Aufsichtsbehörden nötig machen. Ziel dabei sollte sein, den mit der Verordnung beabsichtigten Ausgleich zwischen legitimen ökonomischen Interessen und dem Recht auf Privatheit in jedem Einzelfall in der Praxis umzusetzen.

Kontakt: Philipp-Lennart Krüger
Referat: Zentrales Rechtsreferat