

von Dr. Sebastian Kraska

Globaler Datenschutz: Strategie statt Compliance?

Für viele Unternehmensverantwortlichen stellt das Datenschutzrecht bislang vielfach ein bloßes Randthema dar, in welchem der Gesetzgeber den Unternehmen mehr oder weniger hinderliche Regelungen auferlegt hat. Dabei übersehen die Unternehmen die strategische Relevanz datenschutzrechtlicher Regelungen.

Hintergrund: „Dreigleisige Entwicklung“

Im Umgang mit personenbezogenen Daten ist eine Art dreigleisiger Entwicklung zu beobachten: (1) die datenschutzrechtlichen Regulationsanforderungen gerade für europäische Unternehmen steigen beständig an, (2) auf staatlicher Seite beobachtet man in der Tendenz eine zunehmende Zusammenführung personenbezogener Daten der Bürger und (3) zugleich geben die Betroffenen gerade im Internet zunehmend personenbezogene Daten preis.

Regelungsgegenstand: „Wer darf welche Daten zu welchem Zweck nutzen?“

Auf dem Gebiet des Datenschutzrechts wird die Frage behandelt, wer welche Daten zu welchem Zweck nutzen darf. Damit sind die datenschutzrechtlichen Vorgaben nicht allein irgendein weiteres Gesetz, dessen Befolgung nur allein deshalb erfolgt, um Bußgelder zu vermeiden. Das Datenschutzrecht regelt letztlich die wirtschaftlichen Nutzungsmöglichkeiten von personenbezogenen Daten.

Kulturell unterschiedliche Ansätze im Umgang mit personenbezogenen Daten

Weltweit sind kulturelle Unterschiede im Umgang mit personenbezogenen Daten festzustellen. Im asiatischen Raum beispielsweise genießen personenbezogene Daten an sich keinen generellen Schutz, wenn der Betroffene nicht im Einzelnen auf deren Schutzwürdigkeit gesondert und bewusst hingewiesen hat.

Europa: Datenschutz verfassungsrechtlich geschützte Rechtsposition

Im europäischen Raum herrscht der Gedanke vor, dass der Schutz personenbezogener Daten eine verfassungsrechtlich geschützte Rechtsposition jedes Einzelnen zu sein habe und Unternehmen daher nur bedingt bzw. unter Achtung der verfassungsrechtlich geschützten Rechtsposition des Einzelnen personenbezogenen Daten wirtschaftlich nutzen können.

Blick in die USA: Einräumung weitgehender Nutzungsrechte

Im US-amerikanischen Raum wird vornehmlich der Ansatz verfolgt, dass sich Unternehmen nahezu umfassende Nutzungsrechte hinsichtlich preisgegebener personenbezogener Daten von den Betroffenen erteilen lassen können.

Dies mag mit der generellen Prägung der USA zusammenhängen, den Unternehmen wie Privatpersonen weite Freiheiten hinsichtlich ihrer (wirtschaftlichen) Betätigung einzuräumen und nur so weit als unbedingt erforderlich regulierend einzugreifen.

Datenschutz als Gegenstand europäischer Wirtschaftspolitik

Ausgehend von dem Regelungsansatz der europäischen Gesetzgebungsorgane, dass personenbezogene Daten nur von Unternehmen verarbeitet werden dürfen, die über ein angemessenes Datenschutzniveau verfügen, eignet sich das Datenschutzrecht mit zunehmender Digitalisierung der Geschäftsprozesse auch als Gegenstand zur Durchsetzung europäischer Wirtschaftsinteressen.

Wirtschaftspolitik (1/8): Angemessenes Datenschutzniveau

Während für Unternehmen in den Mitgliedsstaaten der Europäischen Union und des Europäischen Wirtschaftsraumes aufgrund der Geltung entsprechender EU-Datenschutzrichtlinien und darauf berufender nationaler Regelungen ein angemessenes Datenschutzniveau per se als sichergestellt gilt, erlauben die datenschutzrechtlichen Vorgaben einen Transfer von Daten an Unternehmen außerhalb der EU/des EWR nur, wenn auch hierbei ein angemessenes Datenschutzniveau sichergestellt wird.

Wirtschaftspolitik (2/8): Export europäischer Datenschutzpolitik

Die Sicherstellung dieses „angemessenen Datenschutzniveaus“ bei der datenempfangenden Stelle kann hierbei auf vielerlei Weise erfolgen. Vereinfacht gesprochen bestehen folgende Möglichkeiten: (1) das datenempfangende Unternehmen unterschreibt so genannte „EU-Standardverträge“ und verpflichtet sich zur Einhaltung europäischer Datenschutzstandards, (2) ein ganzes Land gibt sich Datenschutzregelungen nach europäischem Vorbild und setzt diese auch durch (über die Vergleichbarkeit der Regelungen und das Maß ihrer Durchsetzung entscheidet die EU-Kommission im Einzelfall), (3) ein Unternehmensverbund gibt sich in Absprache mit den Datenschutz-Aufsichtsbehörden globale die europäischen Datenschutzstandards berücksichtigende Unternehmensrichtlinien im Umgang mit personenbezogenen Daten oder (4) im Fall US-amerikanischer Unternehmen können diese sich im Rahmen einer Selbst-Zertifizierung zur Einhaltung datenschutzrechtlicher Vorgaben nach europäischem Muster verpflichten (so genanntes „Safe-Harbor-Konzept“).

Wirtschaftspolitik (3/8): EU-Standardverträge

Die EU-Standardverträge exportieren letztlich die europäischen Vorstellungen im Umgang mit den übermittelten personenbezogenen Daten auf sämtliche datenempfangende Unternehmen. Wenngleich die Verträge vor allem hinsichtlich der Rechte der europäischen Datenschutz-Aufsichtsbehörden in der Praxis bislang jedenfalls eher selten vollkommen ausgeschöpft werden, so unterliegen die ausländischen Unternehmen hinsichtlich der empfangenden Daten damit doch faktisch europäischen Datenschutzvorgaben.

Wirtschaftspolitik (4/8): Angemessenes Datenschutzniveau qua Beschluss der EU-Kommission?

Auch die Entscheidungen der EU-Kommission über die Angemessenheit des Datenschutzniveaus haben letztlich wirtschaftspolitisch relevante Tragweite. Denn die Einschätzung der EU-Kommission, ob ein Drittland den europäischen Datenschutzvorgaben vergleichbare Datenschutzregelungen aufgestellt hat und – noch wichtiger – diese vor allem auch durchsetzt entscheidet letztlich über die Frage, ob europäische Unternehmen vereinfacht Daten mit Unternehmen in diesen Ländern austauschen können (von Interesse mag in diesem Kontext auch die insofern richtlinienwidrige Umsetzung auf deutscher Ebene sein, trotz Angemessenheitsentscheidung der EU-Kommission den Datenexport nur beschränkt zuzulassen).

Wirtschaftspolitik (5/8): Datenschutzgesetze sind anwendbar aber global (noch) nicht durchsetzbar
Erwähnung verdient auch der Umstand, dass gerade im Internet nationale Datenschutzregelungen zwar häufig anwendbar sind, aber faktisch (noch) nicht durchgesetzt werden können. Es gibt indes verschiedene Bestrebungen vor allem auf europäischer Ebene (zuletzt aber auch auf dem G8-Gipfe), die

Datenschutzvorgaben vor allem im Internet auch durchzusetzen.

Wirtschaftspolitik (6/8): „Tochtergesellschaft in Geiselhaft“

Interessant ist auch die Entwicklung, dass zunehmend die Tochtergesellschaften für jene Datenverarbeitungen verantwortlich gemacht bzw. zu dieser befragt werden, die an sich allein von der (in einem anderen Rechtsraum ansässigen ausländischen) Muttergesellschaft durchgeführt werden.

Wirtschaftspolitik (7/8): Abkehr vom Personenbezug

Wie an anderer Stelle bereits ausgeführt zeichnet sich eine Entwicklung ab, unabhängig von einem etwaigen Bezug von Daten zu einer natürlichen Person in als besonders sensibel definierten Verarbeitungsbereichen sämtliche Datenverarbeitung zu regulieren.

Wirtschaftspolitik (8/8): Datentransfer innerhalb der Unternehmensgruppe

Auch das vielfach von den Unternehmen kritisierte Fehlen eines so genannten Konzernprivilegs hat letztlich wirtschaftspolitische Tragweite, bevorzugt es doch eine bestimmte Art der Unternehmensstrukturierung aus datenschutzrechtlichen Gründen. Zum (vereinfachten) Hintergrund: auch der Datenaustausch zwischen verbundenen Unternehmen (z.B. zwei Unternehmen desselben Konzerns) wird datenschutzrechtlich als Übermittlung „zwischen Dritten“ reguliert.

US-Unternehmen und Datenschutz: strategische Aspekte beachten

Gerade US-amerikanische Internetunternehmen sollten ihre Positionierung zum Thema Datenschutz überdenken und das Thema der europäischen Regulierungstendenzen mehr unter strategischen Gesichtspunkten denn unter Compliance-Aspekten verfolgen.

Denn US-Unternehmen sehen wie dargestellt personenbezogene Kundendaten in der Regel als wirtschaftliches Gut („Asset“) und unternehmenswertbildenden Bestandteil an, deren wirtschaftliche Nutzung im Ermessen des Unternehmens steht, ohne dass die Betroffenen wesentliche Einflussrechte auf den Umgang mit ihren personenbezogenen Daten nehmen können.

Die Verantwortung für eigenes Handeln hat bei diesem Umgang mit eigenen Daten einen hohen Stellenwert und liegt in erster Linie beim Betroffenen selbst. In Europa hingegen versucht der Gesetzgeber, den Betroffenen vor seinem eigenen Handeln zu schützen.

Fazit

Gerade die amerikanische IT-Industrie sollte aufgrund ihrer Bedeutung und Innovationskraft die eigene Positionierung zum Thema Datenschutz überdenken und europäische Regulierungstendenzen nicht nur unter Compliance-Aspekten verfolgen, sondern zusätzlich auch eigene strategische Positionen hierzu entwickeln.

Autor:

Dr. Sebastian Kraska

Rechtsanwalt