Standpunkt:
EU Datenschutzgrundverordnung

Mit der Datenschutzgrundverordnung soll die noch aus dem Jahr 1995 stammende Datenschutzrichtlinie abgelöst werden und deren Bestimmungen an die Erfordernisse und Herausforderungen des digitalen Zeitalters angepasst werden. ***Die IBM begrüßt dieses Anliegen ausdrücklich***. Die Europäische Kommission bringt damit Ihr Anliegen zum Ausdruck, das Datenschutzniveau in Europa auf einem einheitlichen, hohen Level festzuschreiben und so Verbrauchern und Unternehmen gleiche und transparente Standards zu geben. ***Ein hohes Datenschutzniveau und eine deutliche Steigerung der Datensicherheit bei Prozessen der Datenverarbeitung sind im Interesse der IBM***.

Neben der hohen Zahl der delegierten Rechtsakte, fehlenden Ausnahmen für anonymisierte oder pseudonymisierte Daten und unklaren Regelungen zur Profilbildung, lassen einzelne Regelungen des vorliegenden Entwurfs jedoch grundsätzliche Zweifel daran aufkommen, ob das Ziel, den Datenschutz europaweit zu stärken und die Datensicherheit zu erhöhen, erreicht werden kann.

Im Folgenden soll an drei Beispielen dargelegt werden, dass der Verordnungsentwurf dem Ziel eher abträglich ist.

1. Rechtsweg

Die durch die Verordnung (VO) angestrebte Harmonisierung wird grundsätzlich begrüßt. Allerdings bedeutet die Wahl des Regelungsinstruments, dass der Rechtsweg zu nationalen Gerichten abgeschnitten wird. Um die Klärung strittiger Entscheidungen (z.B. die Verhängung einer Strafe durch eine Datenschutzbehörde) gerichtlich zu erwirken, müssen die Unternehmen sich nach dem VO-Entwurf direkt an den Europäischen Gerichtshof (EuGH) wenden.

Die Dauer der Verfahren am EuGH führt bei den betroffenen Unternehmen zu Rechtsunsicherheiten und Unklarheiten hinsichtlich geschäftlicher Praktiken. Dienstleistungen und Produkte, die von einer Klärung betroffen sind, werden in dieser Zeit nicht weiter vertrieben werden können. Selbst bei einer für das Unternehmen positiven Entscheidung wird das Vertrauen nachhaltig geschädigt werden.

Das Ziel, den Datenschutz zu vereinheitlichen und Rechtsicherheit für Nutzer und Unternehmen zu schaffen wird verfehlt, da es der Verordnung an entscheidenden Stellen an rechtlich eindeutigen Regelungen fehlt. Vieles wird der späteren Rechtsauslegung durch den EuGH bedürfen.

2. Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer

Die derzeitige Rechtslage sieht eine klare Trennung der Rollen vor. Der *Data Controller* (z.B. eine Bank) hat den direkten Kontakt zu der betroffenen Person (Kunde), dessen Daten mit Einwilligung erfasst werden. Der *Data Processor* (IBM) handelt in den allermeisten Fällen ausschließlich auf Weisung des *Controllers* im Hintergrund.

Dieses Verhältnis wird derzeit auf vertraglicher Basis geregelt. Der *Controller* ist im Außenverhältnis haftbar, der *Processor* im Innenverhältnis durch Vertrag regresspflichtig. Seit der Umsetzung der Datenschutz-Richtlinie haben sich tragfähige Geschäftsvereinbarungen und -umsetzungen etabliert.

Die neue Verordnung enthält Vorschläge, mit denen in die Privatautonomie eingegriffen wird, indem neue Verpflichtungen seitens des *Processors* eingeführt werden, ohne dass dies entweder zum Schutz einer betroffenen Person beitragen oder das Datenschutzniveau insgesamt erhöhen würde. In diesem Zusammenhang ist – neben den Artikeln 26 und 28 – insbesondere der Artikel 77 problematisch, der eine komplette Kopplung der Verantwortung und Haftung von *Controller* und *Processor* vorsieht.

Bei vielen Arten der Datenverarbeitung besteht keine Notwendigkeit für den *Processor* zu wissen, um welche Daten es sich handelt. Dies ist auch im Sinne eines hohen Datenschutzniveaus.

Wenn der *Processor* aber gleichzeitig für alle Vorgänge haftbar gemacht wird, muss er zwingend die vorherigen Schritte des *Controllers* überprüfen. Das wird die Vertragsverhandlungen massiv erschweren, da beide Seiten daran interessiert sein werden, Haftungsrisiken zu minimieren. Zwar gibt es in Art 77 Absatz 3 die Möglichkeit einen Entlastungsnachweis zu erbringen, aber hierbei handelt es sich um eine Beweislastumkehr im Vergleich zur derzeitigen Rechtslage. Dem Verbraucher bleibt die Möglichkeit den *Processor* im Rahmen einer gesamtschuldnerischen Haftung zu belangen (Art. 77 Abs 2).

In letzter Konsequenz müssten Vertragsverhandlungen massiv ausgeweitet und individualisiert werden. Dies stellt sowohl den *Processor* als auch den *Controller* vor gravierende Probleme. Auf Seiten des *Processors* werden die massiven administrativen Aufwendungen dazu führen, dass Cloud-Projekte teurer und gerade für *Controller* in kleinen und mittelständischen Unternehmen unrentabel werden.

Das Ziel, das Datenschutzniveau zu erhöhen, wird verfehlt, weil *Controller* vor dem Hintergrund immer komplexerer Verträge und der damit verbundenen Kosten, die Daten eher selbständig verwalten werden. Dort sind die Daten einer größeren Gefahrenlage ausgesetzt, als in einer Cloud, deren Infrastruktur von Experten rund um die Uhr gewartet, geschützt und weiterentwickelt wird.

3. Haftungsregime und Meldefristen

Das unklare Haftungsregime, die strikten Meldefristen und die fehlende Definition eines „Datenlecks“ werden auf Seiten der Unternehmen dazu führen, dass die gut funktionierenden internen Systeme zur Aufnahme und Meldung von Datenschutzverstößen massiv überlastet werden, da jegliche Art von Datenlecks – z.B. ein verlorener Laptop – unverzüglich gemeldet werden. Dazu trägt auch das unklare Haftungsregime bei, welches massive Strafen auch bei einem ersten Verstoß nicht explizit ausschließt.

Dies wird nicht nur auf Seiten der Unternehmen zu einem jetzt noch nicht zu überblickenden administrativen Mehraufwand führen, sondern auch auf Seiten der für die Aufnahme der Meldungen beauftragten Stellen, die ansonsten die Anzahl der Meldungen nicht verarbeiten können.

Vor dem Hintergrund einer angespannten Haushaltslage von Bund, Ländern und Kommunen ist mit einer deutlich besseren personellen Ausstattung der beauftragten Stellen nicht zu rechnen. Der Ausbau unternehmensinterner Strukturen ist auch vor dem Hintergrund des Verhältnisses zwischen Aufwand und Ertrag zu kritisieren.

Das Ziel, das Datenschutzniveau zu erhöhen, wird verfehlt, weil die Masse der zu erwartenden unternehmensinternen und an Behörden weitergeleiteten Meldungen, das Erkennen schwerwiegender Datenlecks und Datenschutzverstöße zu einer Suche nach der sprichwörtlichen Stecknadel im Heuhaufen machen werden.

Abschließende Betrachtung

Die Regelungen zum Rechtsweg, zu den Verantwortlichkeiten zwischen *Controller* und *Processor* sowie das unklare Haftungsregime sind dazu geeignet, das Ziel des Verordnungsentwurfs zu konterkarieren, da

a) Dienstleistungen und Produkte, die das Datenschutzniveau erhöhen können, durch Rechtsunsicherheit Reputationseinbußen hinnehmen müssen.
b) Angebote – wie das Cloud-Computing – die geeignet sind, Daten professionell zu schützen, für eine Reihe von Interessenten unrentabel werden.
c) interne und externe Datenschutzprozesse durch einen Anstieg von (Bagatell)Meldungen überlastet werden.

Insbesondere die Dokumentations- und Meldepflichten laufen auch dem erklärten Ziel der EU-Kommission zur Datensparsamkeit entgegen, da sie zu einem Anstieg der Datensätze führen werden.

Die IBM ermutigt deshalb alle Beteiligten, den vorliegenden Vorschlag vor dem Hintergrund des Anliegens eines hohen Datenschutzniveaus und einer effektiven Datensicherheit erneut zu prüfen und insbesondere bei den oben beschriebenen Maßnahmen Anpassungen in Erwägung zu ziehen.