

Stellungnahme IBM Deutschland zur EU-Datenschutz-Grundverordnung

IBM Deutschland begrüßt grundsätzlich die von der Kommission vorgelegte EU-Datenschutz-Grundverordnung (VO). Die bestehenden Regelungen stammen aus dem Jahr 1995 und somit aus einer Zeit, als das Internet, mobile Endgeräte und die digitale Vernetzung von Wirtschaft und Verbrauchern noch nicht in der heutigen Dichte existierten.

IBM erkennt an, dass die Regelungen zu Datenschutz, Datenverarbeitung und -weitergabe einer grundlegenden Neuausrichtung bedürfen, auch und ganz besonders im Hinblick auf das Verhältnis zwischen Verbraucher und Wirtschaft.

Als ein global agierendes Unternehmen **unterstützt IBM die Kommission** grundsätzlich in Ihrem Bestreben, das Datenschutzniveau zu harmonisieren und damit gleiche Wettbewerbsvoraussetzungen in den Mitgliedsstaaten der EU zu schaffen. Vor diesem Hintergrund **begrüßt IBM** das von der Kommission vorgesehene One-Stop-Shop-Verfahren, welches – wenn es konsequent angewendet wird – die Rechtssicherheit für die beteiligten Akteure erhöhen, bürokratischen Aufwand mindern und ein Anreiz für die Etablierung gemeinsamer Standards sein kann.

Der vorliegende Entwurf erscheint in wesentlichen Teilen aber **nicht dazu geeignet**, Wettbewerb zu stärken, Verbraucher effektiv zu schützen und Verfahren in Unternehmen und öffentlichen Stellen transparenter und effizienter zu gestalten. Die vielen undifferenzierten Vorschriften zur Speicherung, Dokumentation, Identifikation und Kommunikation wirken wie ein Versuch, die digitale Welt mit Mitteln der analogen Welt zu regulieren. Die Kommission sollte mehr Mut beweisen, den Weg in eine digitale Welt zu ebnen und Rahmenbedingungen einer nachhaltigen Entwicklung zu schaffen; stattdessen läuft die Vorlage dem Anliegen nach Schaffung von Wachstum und Arbeitsplätzen entgegen.

Im Einzelnen:

- Die hohe Zahl sog. **delegierter Rechtsakte** (Art. 86 der VO i.V.m. Art 290 AEUV) schafft Unsicherheiten auf Seiten von Unternehmen und Verbrauchern. ***IBM fordert die Bundesregierung auf, die delegierten Rechtsakte unter fachlichen Aspekten zu prüfen und dann auf Streichung oder Konkretisierung zu drängen.***
- Die in der VO an verschiedenen Stellen vorgesehenen **Dokumentations- und Rechenschaftspflichten** (vgl. u.a. Art. 22 (2) und Art 28 (2)) sowie die Datenschutz-Folgenabschätzungen (Art. 33) bedeuten einen erheblichen bürokratischen Mehraufwand für die betroffenen Unternehmen mit der Konsequenz, dass die behaupteten Entlastungen für Unternehmen nivelliert werden. Sie laufen auch ganz grundsätzlich der Intention der VO, mit Daten verantwortlich umzugehen, zuwider, da Daten neu gespeichert, verwaltet und systematisiert werden müssen. ***IBM bittet die Bundesregierung in ihren Verhandlungen darauf hinzuwirken, dass neue, administrative Aufwendungen für Unternehmen vermieden werden.***
- Die **24-Stunden Frist zur Benachrichtigung** einer Behörde (Art. 31) ist in der Praxis kaum zu leisten und läuft dem Grundgedanken der VO zuwider. Bei einer strikten Auslegung der Regelung wird es zu undifferenzierten Meldungen auch kleinster Verstöße kommen, die dazu geeignet sind, eine effektive Arbeit der Aufsichtsbehörden zu unterminieren. ***IBM fordert die Bundesregierung auf, von der 24 Stunden Frist Abstand zu nehmen und ferner genauer zu spezifizieren, in welchen Fällen von Verletzung des Schutzes personenbezogener Daten die jeweilige Behörde eingeschaltet werden muss.***
- Das **Sanktionsregime** (Art. 79) lehnt sich ohne zwingenden Grund an das Wettbewerbsrecht an, in dem vorsätzliche Verstöße geahndet oder sanktioniert werden. Die vorgesehenen Sanktionen differenzieren nicht zwischen vorsätzlichem und leicht bzw. grob fahrlässigem Handeln, und sehen für den Fall eines „ersten, unbeabsichtigten Verstoßes“ (Art 79. (3)) lediglich vor, dass die Behörde von einer Sanktion absehen kann. ***IBM fordert die Bundesregierung nachdrücklich auf, sich im Hinblick auf das Sanktionsregime für eine Differenzierung zwischen Fahrlässigkeit und Vorsatz sowie ein striktes und***

juristisch eindeutig formuliertes abgestuftes Sanktionsverfahren einzusetzen.

- Die vorgesehene **explizite Einwilligung** in die Verarbeitung personenbezogener Daten (Art. 4 (8)) ist undifferenziert, wirft Fragen nach der technischen Machbarkeit auf und läuft dem Bestreben nach mehr Transparenz entgegen, da unabhängig von Risiko oder Geschäftszusammenhang zukünftig eine explizite Einwilligung erforderlich ist. ***IBM Deutschland bittet die Bundesregierung, auf eine differenzierte Regelung hinzuwirken, die Inhalt, Risiko, Zeitpunkt und Kontext der Datenverarbeitung berücksichtigt und die implizite Einwilligung weiterhin ermöglicht.***
- Die VO trennt nicht scharf zwischen **Verantwortlichem und Auftragsdatenverarbeiter** (Art. 22, 24, 26, 27, 28). Dies steht sowohl im Widerspruch zum Anspruch der VO klare Verantwortlichkeiten zu definieren (Erwägungsgrund 62), als auch im Widerspruch zu geltendem deutschen Recht (vgl. § 11 (1) BDSG) und gefährdet neue Geschäftsmodelle, wie das Cloud-Computing. ***IBM Deutschland fordert die Bundesregierung auf, sich für klar abgrenzbare Verantwortlichkeiten von Verantwortlichem und Auftragsdatenverarbeiter einzusetzen.***
- Artikel 20 der VO stuft die **mathematische Auswertung und Analyse** von Daten als besonders risikoreich ein und erlaubt diese nur unter sehr strikten Voraussetzungen. Dieser Verbotsvorbehalt verkennt den Nutzen dieser Technologien in vielen Sektoren, insbesondere im Gesundheitsbereich, und verletzt den Grundsatz der technologischen Neutralität. Die Nutzung von Analyseverfahren sollte nicht über die bestehenden Schutzvorschriften (generellen Grundsätze der rechtmäßigen Verarbeitung von Daten, insbesondere Information und Einwilligung des Nutzers, Transparenz und Datensicherheit) hinaus geregelt werden. ***IBM Deutschland bittet die Bundesregierung, auf eine Entfernung oder zumindest eine deutliche Überarbeitung von Artikel 20 zu drängen.***