

CHANCEN DER DIGITALISIERUNG NUTZEN - FÜR EINE WIRTSCHAFTS- UND ORDNUNGSPOLITISCH AUSBALANCIERTE E-PRIVACY- VERORDNUNG

BESCHLUSS DES MIT-BUNDESVORSTANDS VOM 14. MAI 2018

Im Koalitionsvertrag heißt es wörtlich: „Wir werden uns auf EU-Ebene (außerdem) für eine Privacy-Verordnung einsetzen, die im Einklang mit der EU-Datenschutz-Grundverordnung die berechtigten Interessen von Verbraucherinnen und Wirtschaft angemessen und ausgewogen berücksichtigt.“ Ein modernes Datenrecht ist eine Grundvoraussetzung, um die Chancen der Digitalisierung für die deutsche Wirtschaft zu verwirklichen. Nur mit einem ausbalancierten, praktikablen, verlässlichen und gleiche Wettbewerbsbedingungen wahren Rechtsrahmen werden wir in Deutschland innovative Geschäftsmodelle, neue Arbeitsplätze und nachhaltiges Wachstum in der digitalen Wirtschaft realisieren. Die bislang vorgelegten Vorschläge für eine E-Privacy-Verordnung sind aus Sicht der MIT wirtschafts- und datenschutzpolitisch unausgewogen, da sie den großen digitalen Plattformen einseitig Wettbewerbsvorteile zuspielen.

Die MIT fordert die Bundesregierung deshalb auf:

1. Den Datenschutz bei E-Privacy in Einklang mit der Datenschutzgrundverordnung zu regeln

Die E-Privacy-Verordnung darf legitime Geschäftsmodelle, die auf der Verarbeitung endgerätebezogener Informationen beruhen, nicht behindern. Sie darf hier nicht weniger Verarbeitungsbefugnisse als die DS-GVO zur Verfügung stellen. Die Verarbeitungsbefugnisse dürfen im Vergleich zur DS-GVO nicht restriktiver ausfallen. Die rechtlichen Erlaubnistatbestände dürfen – insbesondere mit Blick auf die Technikregulierung – nicht stärker beschnitten werden als dies nach der DS-GVO möglich ist.

2. Gleiche Wettbewerbsbedingungen für alle Geschäftsmodelle sicherzustellen.

Die Verarbeitungsregeln und Technikvorgaben der E-Privacy-Verordnung müssen wettbewerbsneutral ausgestaltet werden. An keiner Stelle darf es zu rechtlichen oder faktischen Wettbewerbsvorteilen für bestimmte Geschäftsmodelle oder Infrastrukturen kommen. Die Wettbewerbsfähigkeit der europäischen Digitalwirtschaft darf bei der Verwirklichung von Datenschutz und Datenkontrolle nicht aus den Augen verloren werden.



MIT

MITTELSTANDS- UND
WIRTSCHAFTSVEREINIGUNG
DER CDU/CSU

3. Die Datenverarbeitung praxistauglich und zukunftsfest zu regulieren.

Die bislang auf dem Tisch liegenden Vorschläge bedürfen dringend eines Realitätschecks. Die E-Privacy-Verordnung muss rechtsklar gestaltet sein, um die notwendige Rechtssicherheit für Anbieter und Verbraucher zu schaffen. Nach dem derzeitigen Stand würden die intendiert gesetzlich erlaubten, ja selbst einwilligungsbasierte Datenverarbeitungsprozesse für die klare Mehrheit der Angebote oftmals nicht darstellbar sein. Auch in dieser Hinsicht würden geschlossene, proprietäre Log-In-Plattformen begünstigt.

Begründung:

Als MIT akzeptieren wir keine ideologische Regulierung im Verbotmodus. Wir wollen, dass Deutschland und Europa mit datengetriebenen Innovationen wettbewerbsfähig bleiben. Dabei stehen wir für einen zukunftstauglichen, risikobasierten Datenschutz, der die informationelle Selbstbestimmung in der Praxis gewährleistet. Ein Datenschutzrecht, das gut gemeint ist, tatsächlich aber die vielfach bereits bestehende Datenvormacht der Quasi-Monopolisten der Plattformwirtschaft weiter stärkt, lehnen wir genauso ab wie eine Datenpolitik, die auf ein umfassendes Social-Scoring wie in China hinausläuft. Mit der E-Privacy-Verordnung besteht die Chance, im Einklang mit der Datenschutzgrundverordnung (DS-GVO) einen zukunftstauglichen, Innovationen und fairem Wettbewerb verpflichteten Datenschutz-Rechtsrahmen für Kommunikations- und Mediendienste zu schaffen. Für die Vielfalt und Qualität digitaler Medienangebote ist dies besonders wichtig. Daten sind längst das Entgelt und die Gegenleistung für die Inanspruchnahme von Webangeboten, insbesondere journalistisch-redaktionellen. Digitale Medien sind daher in besonderer Weise auf praktikable und ökonomisch tragfähige Datenverarbeitungsmöglichkeiten angewiesen, um sich unternehmerisch refinanzieren zu können. Eine unabhängige, plurale und für alle Bürgerinnen und Bürger gleichermaßen gut erreichbare digitale Medienlandschaft ist indes wichtiger denn je, um den gesellschaftlichen Konsens über unsere Grundwerte unter den Bedingungen der Digitalisierung zu erhalten.

Zu den Forderungen im Einzelnen:

1. Die Schieflage der bisherigen Vorschläge bei den Verhandlungen in Brüssel muss ausgeglichen werden. Der Koalitionsvertrag bildet hierfür die Grundlage. Das hierin enthaltende Übereinstimmungsgebot zwischen der DS-GVO und der geplanten E-Privacy-Verordnung ist die vereinbarte Verhandlungslinie für die Position der Bundesregierung in Brüssel. Es darf im Regierungsalltag nicht verwässert werden. DSGVO und E-Privacy-VO sollten ursprünglich als einheitliches Datenschutzpaket verabschiedet werden. Nachdem die ab dem 25. Mai 2018 anwendbare DSGVO einen differenzierten, risikobasierten Datenschutzansatz bereitstellt, schießt die E-Privacy-VO nach dem derzeitigen Stand diesen gerade aus. .
2. Wie eine Reihe von Untersuchungen (u.a. die WIK-Studie im Auftrag des BMWI) belegen, würden durch die E-Privacy-VO nach dem derzeitigen Entwurf die Datenverarbeitungsmöglichkeiten für den digitalen Handel, die Medien- und Internetwirtschaft in Deutschland massiv beschnitten. Damit droht an empfindlicher Stelle eine ordnungspolitische Schieflage mit erheblichen negativen Konsequenzen für die Angebots- und Medienvielfalt in Europa und Deutschland. Der Marktzutritt wird kleineren Unternehmen, die keinen Rückgriff auf einen über Jahre angereicherten Datenpool haben, erheblich erschwert, während die großen digitalen Plattformen aufgrund ihres Log-In-Effekts nur noch weiter gestärkt würden.

3. Die Digitalisierung lebt vom Austausch von Daten. Der freie Datenfluss ist ein elementarer Bestandteil auf dem Weg zu modernen Konzepten wie der „Smart City“. Europa darf hier im Wettbewerb mit Asien und Amerika nicht den Anschluss verlieren. Deswegen muss berücksichtigt werden wie man Daten am besten nutzen den Schutz natürlicher Personen zugleich aber durch Anonymisierung, Pseudonymisierung oder Verschlüsselung auch hinreichend schützen kann.