



Resolution: Rettet unsere Grundrechte – für einen starken Datenschutz in Europa!

Antragsteller/in: Rena Tangens, Digitalcourage e.V., Marktstraße 18, 33602 Bielefeld

Adressat: Thomas de Maizière, Bundesinnenminister

Text:

Appell an den Bundesinnenminister: Bekennen Sie sich eindeutig zum Datenschutz Ihrer Bürgerinnen und Bürger, statt sie den internationalen Datenmärkten auszuliefern!

Begründung:

Globale Big-Data-Konzerne sehen unsere persönlichen Daten als das neue Erdöl und sind entsprechend rücksichtslos dabei, sie auszubeuten. Die datensammelnde Wirtschaft will möglichst ungehindert Zugriff auf all unsere Daten haben.

Noch im Juni will der EU-Ministerrat seine Fassung der Datenschutzverordnung beschließen. Die EU würde damit grundlegende Prinzipien über Bord werfen, die uns schützen. Das betrifft uns alle – denn wenn die EU-Datenschutzverordnung in Brüssel beschlossen wird, gilt sie unmittelbar und deutsches Datenschutzrecht wird hinfällig.

Es ist Aufgabe der Politik, der Datengier Schranken zu setzen und die Persönlichkeitsrechte der Bürgerinnen und Bürger per Gesetz wirksam zu schützen. Leider tut das hierfür verantwortliche Innenministerium bei den Verhandlungen im EU-Ministerrat das Gegenteil. Statt die Grundrechte der Bürgerinnen und Bürger zu schützen, hat es offen Ohren für die Lobbyisten der Daten-Dealer.

Für uns ist unsere Menschenwürde unverzichtbar. Wir wollen nicht auf Zahlen reduziert werden. Wir wollen auch morgen unsere Entscheidungsfreiheit nicht an Algorithmen von Konzernen abgeben.

Jetzt im Juni ist die allerletzte Chance, im zukünftigen europäischen Recht unsere Werte zu verteidigen. Wenn das Datenschutzrecht schwach ist, dann verlieren die Menschen in der digitalen Welt ihre Freiheit.

Wir appellieren an den Bundesinnenminister:

Bekennen Sie sich eindeutig zum Datenschutz Ihrer Bürgerinnen und Bürger, statt sie den internationalen Datenmärkten auszuliefern!

Setzen Sie sich im EU-Ministerrat entschieden für folgende Punkte ein:

1. Bürgerinnen und Bürger sollen das Recht auf einen datenschutzfreundlichen Service bekommen. (privacy-friendly-service)
2. Leistungen dürfen nicht von der Preisgabe unnötiger Daten abhängig gemacht werden. Das heißt, eine Taschenlampen-App muss auch funktionieren, wenn wir keinen Zugriff auf unser Adressbuch geben. (Datensparsamkeit und Kopplungsverbot)
3. Daten dürfen nur für die Zwecke verwendet werden, für die sie erhoben wurden. (Zweckbindung)
4. Bürgerinnen und Bürger müssen der Verarbeitung ihrer Daten ausdrücklich zustimmen. Es reicht nicht, wenn Firmen behaupten, sie hätten ein "berechtigtes Interesse". Nur die informierte Zustimmung sichert unser Recht auf informationelle Selbstbestimmung. (explizite Einwilligung)
5. Forschung darf keine Hintertür für Firmen werden, persönliche Daten beliebig und ohne Zustimmung der Betroffenen zu nutzen. Dies gilt insbesondere für Daten, die Rückschlüsse auf die Gesundheit zulassen.