DIGITALE GESELLSCHAFT | FIfF Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V | digitalcourage

Bundesministerium des Innern
Innenminister Dr. Hans-Peter Friedrich
Alt-Moabit 101D
10559 Berlin
poststelle@bmi.bund.de

2. Dezember 2013

Sehr geehrter Herr Bundesminister Dr. Friedrich,

Am 5. und 6. Dezember 2013 wird der Rat „Justiz und Inneres“ den Vorschlag für die EU-Datenschutzverordnung verhandeln. Die unterzeichnenden Datenschutz- und Bürgerrechtsorganisationen möchten in diesem Zusammenhang darauf hinweisen, dass Datenschutz als Grundrecht in der EU von großer Bedeutung ist und durch den Kommissionsvorschlag praktische Anwendung finden soll.

Der Fortschritt bei den Verhandlungen wurde regelmäßig durch unnötige Hindernisse verzögert, wodurch wir nun, zwei Jahre nach der Veröffentlichung des Kommissionsvorschlags, immer noch weit entfernt von einem Abschluss der dringend notwendigen Datenschutzreform sind. Hierdurch entsteht das Risiko, dass in Europa ineffiziente Datenschutzgesetze zur Geltung kommen. Im Jahr 2009 wurde mit der Charta der Grundrechte der Europäischen Union das Recht auf Privatsphäre verankert. Es wäre nun für die Glaubwürdigkeit der EU katastrophal, diesem Recht im Jahr 2013 noch immer keine praktische Bedeutung zuzugestehen. Gerade in den vergangenen Monaten ließ sich beobachten, wie wichtig und relevant die Kommissionsvorschläge sind – um beispielsweise die Datenerfassung auf das notwendige Minimum zu beschränken, um datenschutzfreundliche Voreinstellungen zu sichern und das Recht auf Löschung zu garantieren.

Wir bitten Sie eindringlich, den Rechten von mehr als 500 Millionen europäischen Bürgerinnen und Bürgern den Respekt entgegenzubringen, den sie verdienen. Wir fordern Sie auf, die Verhandlungen nun wirklich zur „Chefsache“ zu machen und keine weiteren Verzögerungen zuzulassen. Wir brauchen dringend harmonisierte und durchsetzbare Datenschutzregeln in ganz Europa.

Wir fordern Sie daher auf, eine konstruktive Haltung einzunehmen und sich insbesondere für die folgenden Punkte einzusetzen:

Eine starke Definition von personenbezogenen Daten. Der Rat schlägt derzeit eine Definition für „pseudonymisierte“ Daten vor. Diese Definition würde dazu führen, dass eine weitere Kategorie von Daten erschaffen wird, für die es einen weniger hohen Schutz geben soll, zum Beispiel im Kontext von Datenpannen. Diese Rechtslücke muss geschlossen werden, um Bürgerrechte – vor allem im digitalen Umfeld – angemessen zu schützen.

Transparenz und Aufsicht garantieren. Die Verarbeitung personenbezogener Daten wird immer komplexer und umfassender. Daher ist es besonders wichtig, dass über jede Datenverarbeitung transparent und leicht verständlich informiert wird. Bürgerinnen und Bürger müssen das Recht haben, genaue und wahrheitsgetreue Informationen darüber zu erhalten, wie ihre Daten verarbeitet werden. Dies setzt unter anderem voraus, dass sie Informationen erhalten, an wen die Daten weitergegeben werden. Die Definition des “Empfängers”, wie sie vom

Rat derzeit vorgeschlagen wird, ist unzureichend. Die Definition darf nicht Behörden in ihrer Amtsausübung ausschließen. Wenn die Weitergabe von Daten an einen bestimmten Empfänger nicht offengelegt werden können, darf dies nur auf den Ausnahmen in Artikel 2 oder 21 des Vorschlags basieren.

Ein Verbot für heimliche Profilbildung. Wir sind zutiefst über die Risiken der Profilbildung besorgt. Wir fordern daher einen wirksamen Schutz der Bürgerinnen und Bürger vor ungewollten Profilbildungen. Der Vorschlag für Artikel 20 ist sehr limitiert: Allein Maßnahmen, die Bürgerinnen und Bürger stark beeinträchtigen können, sollen als verbotene Profilbildungen gelten. Die Formulierung „stark beeinträchtigen" geht dabei noch einen Schritt weiter als „wesentlich beeinträchtigen". Insbesondere bedeutet dies, dass die Berufung auf eine „starke Beeinträchtigung" erst möglich ist, nachdem der Schaden eingetreten ist. Obwohl der Text des Rates einen gewissen Schutz bietet, ist Artikel 20(3) besorgniserregend, da hierdurch die Profilbildung anhand von sensiblen persönlichen Daten zugelassen wird. Dadurch, dass Profiling erlaubt ist sobald Artikel 9(2) Anwendung findet, dürfen sensible Daten zur Profilbildung genutzt werden - was wiederum dazu führt, dass der vorhergesehene Schutz gegen Profilbildung anhand von sensiblen Daten keine praktische Bedeutung hat.

Weitere entscheidende Fragen der Verordnung betreffen unter anderem die Übermittlung von Daten in Drittländer sowie das Recht auf explizite Zustimmung und auf Einspruch, die dem Wesensgehalt der Grundrechte, die im Primärrecht der Union festgeschrieben sind, entsprechen. Die Verordnung kann nur so gut sein wie das schwächste Glied der Kette. Es ist daher unumgänglich, dass alle Lücken, durch die demokratische Rechte unterminiert werden können, geschlossen werden. Wir bitten Sie, Ihren Standpunkt im Hinblick auf die oben genannten Punkte zu überdenken.

Für weitere Fragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Chaos Computer Club
Digitalcourage e. V.
Digitale Gesellschaft e.V.
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung