TUM THINK TANK

Stärkung des risikobasierten Ansatzes der DSGVO

Stefan Brink & Christiane Wendehorst
Arbeitsgruppe DSGVO am TUM Think Tank

1. Kontext

Die DSGVO schützt alle personenbezogenen Daten gleichermaßen, unabhängig davon, ob sie „privat", belangvoll, geheim oder von besonderem Wert für den Betroffenen oder Dritte sind. Damit führt die DSGVO eine Grundlinie fort, die seit der Volkszählungsentscheidung des Bundesverfassungsgerichts besteht, wonach es in digitalen Zeiten „keine belanglosen Daten" mehr gebe. In gewisser Abweichung von dieser Linie werden zwar „besonders sensible Daten" in besonderer Weise geschützt (heute: Art. 9 DSGVO), allerdings gibt es umgekehrt keine personenbezogenen Daten, die aus dem Schutzregime der DSGVO herausfielen. Auch vom Betroffenen nicht wertgeschätzte Daten, auch allgemein verfügbare, etwa im Internet einfach auffindbare personenbezogene Daten oder Daten zu allgemeinbekannten Persönlichkeiten lösen die Pflichten des Verantwortlichen aus – und sind in der Debatte um den Datenschutz häufiger Anlass für Unmut von Datenverarbeitern, die sich ohne hinreichenden Anlass gegängelt sehen und in dieser Hinsicht „Prinzipienreiterei" der Datenschützer vermuten. Dass es gerade die Unvorhersehbarkeit des Wertes und der Bedeutung personenbezogener Daten ist, welche in Zeiten der Vernetzung und Bildung umfassender Profile von Menschen den pauschalen Schutz aller personenbezogenen Daten vor Manipulation und Bevormundung durchaus vernünftig erscheinen lässt, wird in den öffentlichen Debatten selten akzeptiert oder ganz übersehen.

Schon bei der Präsentation der DSGVO legte die EU-Kommission großen Wert auf die Feststellung, dass dieser Entwurf einen „risikobasierten Ansatz" verfolge: Personenbezogene Daten würden differenziert geschützt, je nachdem, welches tatsächliche Risiko mit ihrer Verarbeitung verbunden sei. In diesem Kontext wurde nicht nur auf Art. 9 DSGVO verwiesen, sondern auch auf die Vorgaben zur Datensicherheit (Art. 32 Abs. 1 DSGVO), zur Melde- und Benachrichtigungspflicht nach Datenpannen (Art. 33 und 34 DSGVO) und zur Datenschutz-Folgenabschätzung (Art. 35 DSGVO). Hier werden die Pflichten des Verantwortlichen in Abhängigkeit zu den mit der Verarbeitung verbundenen „Risiken für die Rechte und Freiheiten natürlicher Personen" gebracht und in einer dem Verhältnismäßigkeitsprinzip angemessenen Weise ausgestaltet.

Die Kritik an der (mangelnden) Ausgestaltung des risikobasierten Ansatzes in der DSGVO wurde in den letzten Jahren allerdings immer lauter: Zum einen wurde bemängelt, dass auch risikolose Verarbeitungen den Prinzipien des Datenschutzes (Art. 5 DSGVO) unterworfen blieben und ihre Verarbeitung eine Grundlage in Art. 6 Abs. 1 DSGVO finden muss. Zum anderen wurde mit Blick auf die Rechtsprechung des EuGH und die Auslegungspraxis der Aufsichtsbehörden beobachtet, dass der risikobasierte Ansatz nicht durchgehend angewandt wurde, etwa bei der Vollzugspraxis der Aufsichtsbehörden keine erkennbare Rolle spielte, und dass dem Datenschutz im Verhältnis zu konkurrierenden Interessen und Rechten unter Berufung auf ein angestrebtes hohes Datenschutzniveau (Erwägungsgrund 10) ein unverhältnismäßig hoher Stellenwert eingeräumt wurde (in Abweichung von Erwägungsgrund 4).

2. Reformvorschlag

Vor diesem Hintergrund hat die Arbeitsgruppe den folgenden Vorschlag zu einer Reform von Art. 5 DSGVO entwickelt:

Artikel 5 DSGVO

(3) Die Grundsätze dieser Verordnung zum Schutz personenbezogener Daten sind so auszulegen, dass Vorgaben dieser Verordnung in einem angemessenen Verhältnis zu dem mit ihnen jeweils verfolgten Zweck stehen und insbesondere die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos einer Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen (risikobasierter Ansatz) berücksichtigen. Maßnahmen zum Schutz personenbezogener Daten sind mit den Interessen oder Grundrechten und Grundfreiheiten anderer Personen als der betroffenen Person in einen angemessenen Ausgleich zu bringen.

Erwägungsgrund:

Gemäß Absatz 3 von Artikel 5 sind die allgemeinen Datenschutzgrundsätze und die übrigen Vorgaben dieser Verordnung so auszulegen, dass sie in einem angemessenen Verhältnis zu dem mit den jeweiligen Vorgaben dieser Verordnung verfolgten Zweck stehen und dass sie den freien Verkehr personenbezogener Daten nicht unangemessen beeinträchtigen.

Das Recht auf Schutz personenbezogener Daten und die Interessen oder Grundrechte und Grundfreiheiten anderer Personen als der betroffenen Person sind von den Verantwortlichen, den Aufsichtsbehörden und Gerichten in einen angemessenen Ausgleich zu bringen.

Damit soll sichergestellt werden, dass sich auch das zweite in Absatz 1 von Artikel 1 genannte Ziel dieser Verordnung in den Datenschutzgrundsätzen nach Artikel 5 wiederfindet und dass die in Erwägungsgrund 4 genannte Abwägung zwischen dem Recht auf Schutz der personenbezogenen Daten und anderen Grundrechten stattfinden kann.

Zu den Grundrechten und geschützten Interessen, die mit dem Recht auf Schutz personenbezogener Daten gegebenenfalls in einem Spannungsverhältnis stehen, gehören insbesondere Gedanken-, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung und Informationsfreiheit, unternehmerische Freiheit, und Vielfalt der Kulturen, Religionen und Sprachen sowie die Wissenschafts- und Forschungsfreiheit. Aber auch das Recht auf Achtung des Privat- und Familienlebens sowie das Recht auf Datenschutz Dritter sind zu berücksichtigen, etwa wenn die durch eine betroffene Person gegebene Einwilligung in die Verarbeitung ihrer personenbezogenen Daten auch Auswirkungen auf andere Personen hat, deren personenbezogene Daten nicht unmittelbar verarbeitet wurden, die aber persönliche Merkmale mit der betroffenen Person, deren Daten verarbeitet wurden, teilen.

Besondere Bedeutung kommt in diesem Zusammenhang dem risikobasierten Ansatz zu, welcher auch andere Rechtsakte der Union, namentlich Verordnungen (EU) 2022/2065 und (EU) 2024/1689 prägt. Nach diesem risikobasierten Ansatz haben durch Regulierung begründete Rechte und Pflichten, die zum Schutz gegen die Verwirklichung von Risiken für Sicherheit, Gesundheit und andere Grundrechte geschaffen wurden, stets in einem angemessenen Verhältnis zur Schwere dieser Risiken zu stehen. Der Begriff des Risikos soll dabei im Einklang mit anderen Vorschriften dieser Verordnung und ihren Erwägungsgründen, namentlich Erwägungsgründen 75 ff., verstanden werden und unter anderem Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person vor dem Hintergrund von Art, Umfang, Umständen und Zwecken der Verarbeitung berücksichtigen. Dabei sollte auch der Anzahl der von seinen Verarbeitungstätigkeiten betroffenen Personen, wesentliche Bedeutung zukommen.

3. Einordnung

Nachfolgend findet sich eine zusammenfassende Übersicht der Vor- und Nachteile des Vorschlags zur weiterführenden Diskussion.

Vorteile

- Einfache Ergänzung der Prinzipien mit bekanntem Ansatz sollte auch im (mit eingeschränkten Änderungsmöglichkeiten agierenden) Omnibus machbar sein
- Korrektur von Ungleichgewichten in Rechtsprechung und Aufsicht
- rbA vor die Klammer gezogen anstatt in der DSGVO breit verteilt

Nachteile

- Abstraktheit der Formulierung
- Festschreibung einer Selbstverständlichkeit
- Befürchtung von Rechtsunsicherheit

ARBEITSGRUPPE DSGVO

Die Arbeitsgruppe DSGVO am TUM Think Tank bringt Expertinnen und Experten aus Wissenschaft, Praxis, Aufsicht und Zivilgesellschaft zur Weiterentwicklung der DSGVO zusammen. Dies ist einer von vier konkreten, rechtlich anschlussfähigen Reformbausteinen, die sowohl Datenschutz wirksamer machen als auch verantwortliche Datennutzung für Wirtschaft und Gesellschaft erleichtern.

Der TUM Think Tank bietet die organisatorische Plattform. Initiiert wurde die Arbeitsgruppe von Kai Zenner, Max Schrems, Boris Paal und Markus Siewert.

INSTITUTION

TUM Think Tank | Hochschule für Politik München | Technische Universität München

DISCLAIMER

Der vorliegende Reformvorschlag (Version 1.0) wird von einer Mehrheit der Arbeitsgruppe mitgetragen, auch wenn nicht alle Mitglieder allen Teilen gleichermaßen zustimmen und durchaus auch abweichende Meinungen existieren.

Die Vorschläge verstehen sich nicht als Endpunkt, sondern als Ausgangspunkt für weiterführende Diskussionen. In den kommenden Wochen und Monaten wird die Arbeitsgruppe diese Vorschläge – insbesondere vor dem Hintergrund der derzeit teilweise kontrovers geführten Debatten zum Digital Omnibus – weiterentwickeln und zusätzliche Reformbausteine ausarbeiten.

Die in diesem Bericht geäußerten Inhalte und Ansichten geben ausschließlich die Meinung der Autoren wieder und sind nicht dem TUM Think Tank als Institution oder seinen Mitgliedern zuzuschreiben.

KONTAKT

tumthinktank@hfp.tum.de
https://tumthinktank.de

Mitglieder der Arbeitsgruppe DSGVO

Christoph Bausewein | Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Linda Bienemann | Persönliche Referentin Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Franziska Boehm | FIZ-Karlsruhe & Karlsruher Institut für Technologie (KIT)

Stefan Brink | Wissenschaftliches Institut für die Digitalisierung der Arbeitswelt (WIDA) / Berlin

Thomas Fuchs | Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (HmbBfDI)

Niko Härting | HÄRTING & Deutscher Anwaltverein

Peter Hense | Spirit Legal Rechtsanwaltsgesellschaft mbH

Boris Paal | Technische Universität München

Frederick Richter | Stiftung Datenschutz

Max Schrems | noyb

Louisa Specht-Riemenschneider | Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Christiane Wendehorst | Universität Wien

Michael Will | Bayerisches Landesamt für Datenschutz (BayLDA)

Kai Zenner | MEP Axel Voss, Europäisches Parlament & TUM Think Tank