Christos Paraschiakos
Hamburg, 2/2017

Die Datenschutz-Grundverordnung: Ein Paradigmenwechsel

1. Einleitung

Daten über uns werden laufend gesammelt. Dies gilt vor allem im Internet: Facebook verfolgt mit seinem Like-Button unsere Streifzüge durch das Netz – auch außerhalb seiner eigenen Seite. Google sichtet in seinem Maildienst unsere Kommunikation, um daraus Neigungen und Interessen abzulesen. Unsere Smartphones erzeugen Standortdaten, die sich zu einem detaillierten Bewegungsprofil zusammensetzten lassen. Auch die immer beliebter werdenden *Wearables* wie Fitnessarmbänder und *smarte* Uhren sammeln und verarbeiten laufend Informationen über unsere Gesundheit und unser Verhalten. Aus all diesen Informationen lassen sich wiederum weitreichende Rückschlüsse ziehen – vor allem, wenn Sie in großen Mengen, als *Big Data*, vorliegen. Unternehmen nutzen diese Daten gerne. Mit ihrer Hilfe können zum Beispiel gezielt Kaufempfehlungen beworben oder die finanzielle Leistungsfähigkeit von Kunden besser eingeschätzt werden. Diese Daten sind folglich kommerzialisierbar – mit dem Verkauf und der Auswertung dieser Daten lässt sich bares Geld verdienen. Schätzungen zufolge werden die personenbezogenen Daten aller EU-Bürger zusammen im Jahr 2020 fast 1 Billion Euro wert sein.

Mit dieser Entwicklung sind zahlreiche Gefahren verbunden. Oft wissen wir gar nicht, welches Unternehmen über welche Daten von uns verfügt. Dies ist besonders beklagenswert, weil Unternehmen diese Daten nutzen, um computergestützt auf weitere private Informationen zu schließen, die wir niemals preisgeben wollten. Ein weiteres Problem ist, dass diese Daten keineswegs sicher vor dem unbefugten Zugriff Dritter sind – das zeigen nicht zuletzt auch die Enthüllungen über das Zusammenwirken von Nachrichtendiensten und IT-Unternehmen. Eine nicht zu unterschätzende Gefahr liegt zudem darin, dass künftig wirtschaftlicher Druck auf Bürger ausgeübt wird, laufend private Daten preiszugeben, um etwa höhere Beitragszahlungen bei Lebensversicherungen oder Krankenkassen zu vermeiden. Auch kann es vorkommen, dass Unternehmen schlichtweg falsche Schlussfolgerungen ziehen und Bürger – im geschäftlichen oder privaten Verkehr – deswegen benachteiligt oder gar ausgegrenzt werden.

Die Kontrolle über die eigenen, personenbezogenen Daten ist im digitalen Zeitalter für ein Leben in Selbstbestimmung von großer Bedeutung. Nicht zuletzt deswegen gewinnt die grundrechtliche Dimension des Datenschutzes auch im Unionsrecht immer mehr an Bedeutung. Im digitalen Zeitalter gilt es, diese Kontrolle wieder zurückzugewinnen. Dieses

Ziel soll nach dem Willen des europäischen Gesetzgebers die neue Datenschutz-Grundverordnung (DS-GVO) verwirklichen. Sie tritt am 25. Mai 2018 in Kraft und läutet einen Paradigmenwechsel im europäischen Datenschutzrecht ein.

2. Ziele und Instrumente der Verordnung

Mit Blick auf die bereits geschilderte Gefahrenlage verfolgt die DS-GVO im wesentlichen drei Ziele: Die Rechte der Bürger sollen gestärkt und ihre Durchsetzung verbessert werden. Für Unternehmen soll es einfacher werden, sich an die europäischen Regeln zu halten. Schließlich soll datenschutzrechtliche Vorsorge dadurch betrieben werden, dass datenschutzfreundliche Computersysteme den Regelfall darstellen.

2.1. Stärkung des Rechts auf informationelle Selbstbestimmung

Das zentrale Ziel, die Rechte der Bürger und deren Durchsetzung zu stärken, verfolgt die Verordnung zunächst, indem Sie selbst Klarheit schafft: Zunächst stellt sie die Datenschutzrechte der Bürgerinnen klar heraus und benennt diese. So verbietet sie es grundsätzlich, die Bereitstellung von Diensten an die Erhebung dafür nicht erforderlicher Daten zu koppeln. Außerdem begründet sie das Recht, eigene Daten elektronisch abzufragen und weiterzuverwenden. Mit standardisierten Symbolen muss verständlich darüber informiert werden, was mit den von uns preisgegebenen Daten geschieht. Diese Rechte werden in zweifacher Hinsicht abgesichert: Zum einen durch Sanktionen in Form von Geldbußen, zum anderen durch erweiterte Rechtsschutzmöglichkeiten, die nunmehr etwa Interessenverbänden wie Verbraucherschutzorganisationen erlauben, Verbandsklagen zu erheben.

2.2. Rechtslage für Unternehmen vereinfachen

Die Rechtslage wird für Unternehmen zunächst dadurch vereinfacht, dass an die Stelle der bisherigen europäischen Datenschutzrichtlinie nunmehr eine Verordnung tritt, die unmittelbar auch für die Unternehmen und Bürgerinnen gilt. Damit gelten in allen Mitgliedsstaaten die gleichen Regeln.

2.3. Datenschutzfreundliche Computersysteme

Die DS-GVO identifiziert datenschutzfreundliche Computersysteme als zentrales Instrument dafür, dass in Zukunft nicht mehr Daten anfallen und gespeichert werden, als für die jeweilige Dienstleistung unbedingt nötig. Nutzer sollen in der Lage sein, Dienste anonym

oder unter einem Pseudonym zu nutzen. Daher setzt die DS-GVO auf die Prinzipien „*data protection by design and by default*“.

3. Reichweite der DS-GVO

Die Verordnung schützt natürliche, lebende Personen vor der Verarbeitung ihrer personenbezogenen Daten – ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsortes. Die Grundsätze des Datenschutzes gelten für alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

Erfasst wird grundsätzlich jede Verarbeitung personenbezogener Daten, unabhängig davon, ob sie automatisiert geschieht. Die DS-GVO nimmt dabei jeden in die Pflicht, der Daten verarbeitet und eine Niederlassung in einem Mitgliedsstaat der Union hat. Aber selbst Datenverarbeiter, die keine Niederlassung in der Union haben, werden erfasst, sofern sie gezielt Dienste für Personen, die sich in der Union aufhalten, anbieten.

4. Rechte von betroffenen Bürgern

4.1. Recht auf Transparenz und Information

Die Verfasser der DS-GVO sehen in der Transparenz ein zentrales Werkzeug, um den Schutz der informationellen Selbstbestimmung zu gewährleisten. Daher soll für betroffene Bürger stets erkennbar sein, wenn ihre personenbezogenen Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden oder werden sollen. Diese Informationen sollen mithilfe von standardisierten Bildsymbolen übermittelt werden, um einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu verschaffen. Bürgerinnen müssen zudem stets über die Existenz eines Verarbeitungsvorgangs und seine Zwecke informiert werden, insbesondere, wenn dieser im Verborgenen abläuft. Sie verfügen schließlich über ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, um sich von der Rechtmäßigkeit der Datenverarbeitung überzeugen zu können.

4.2. Grundsatz der informierten Einwilligung

Auch die Bedeutung der Einwilligung als frei gefasste Entscheidung des Einzelnen wird gestärkt. Die Verarbeitung von Daten darf grundsätzlich nur mit der bewussten und ausdrücklichen Einwilligung der betroffenen Person geschehen. Die Einwilligung ist nur wirksam, wenn sie ohne Zwang und nach klarer Informationen über den Zweck erteilt wurde. Dabei gilt, dass ein Vertrag nicht an die Verarbeitung von Daten gebunden sein darf, die mit

der erbrachten Leistung oder dem Produkt nichts zu tun hat. Das Ersuchen um Einwilligung muss zudem in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen. Die Einwilligung ist zudem jederzeit widerrufbar.

Für ohne Einwilligung, also rechtswidrig verarbeitete Daten besteht ein Anspruch auf Löschung. Gleiches gilt grundsätzlich, wenn die betroffene Person ihre Einwilligung widerruft oder der Verarbeitung widerspricht. Darüber hinaus schützt die DS-GVO in besonderem Maße personenbezogene Daten, die für Grundrechte und Grundfreiheiten sensibel sind. Ihre Verarbeitung ist grundsätzlich verboten und nur in seltenen Ausnahmefällen zulässig. Auch personenbezogene Daten von Kindern werden von der DS-GVO besonders geschützt, hierfür bedarf es grundsätzlich der Einwilligung der Eltern.

4.3. Rechte auf Auskunft, Berichtigung und Löschung

Betroffenen Personen gibt die DS-GVO Instrumente an die Hand, damit sie unentgeltlich Zugang zu Daten (Auskunftsrecht) oder deren Berichtigung oder Löschung beantragen oder erhalten und gegebenenfalls von ihrem Widerspruchsrecht Gebrauch machen können. Sie verfügen über ein Recht auf Berichtigung sowie ein Recht auf Vergessenwerden und ein Recht auf Einschränkung der Verarbeitung.

Zudem werden sie vor Ausgrenzung und Benachteiligung durch automatisiertes Profiling geschützt. Zum Schutz der Rechte dieser Personen müssen die Verarbeiter von Daten bereits im Vorfeld Strategien festlegen und Maßnahmen ergreifen, die insbesondere dem Grundsatz des Datenschutzes durch Technik (*data protection by design*) und durch datenschutzfreundliche Voreinstellungen (*data protection by default*) Rechnung tragen.

4.4. Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, ihre personenbezogenen Daten, die sie bereitgestellt hat, in einem maschinenlesbaren Format zu erhalten. Sie hat zudem das Recht, diese Daten einem anderen ohne Behinderung zu übermitteln. Damit wird der freie Datenverkehr gestärkt.

4.5. Beschwerde- und Klagerechte

Jede betroffene Person hat das Recht, bei der zuständigen Aufsichtsbehörde eine Beschwerde gegen die rechtswidrige Verarbeitung ihrer Daten einzureichen. In der Regel wird dies die Aufsichtsbehörde an ihrem gewöhnlichen Aufenthaltsort sein. Die Behörde soll dann die rechtswidrige Handlung unterbinden und sanktionieren. Hilft die Behörde der Beschwerde nicht ab, so können die betroffenen Bürgerinnen hiergegen Klage erheben.

Parallel dazu haben Bürger das gerichtlich durchsetzbare Recht, sich den aus einer rechtswidrigen Datenverarbeitung resultierenden Schaden von den Schädigern ersetzten zu lassen. Sie können auch Verbände mit der Verfolgung ihrer Rechte beauftragen. Schließlich erlaubt es die DS-GVO den Mitgliedsstaaten, unabhängig von einer solchen Beauftragung ein eigenes Beschwerde- und Klagerecht solcher Verbände vorzusehen. Die Mitgliedsstaaten können auch Verwaltungs- sowie strafrechtliche Sanktionen für Verstöße gegen die Verordnung vorsehen.

5. Voraussetzungen der Datenverarbeitung

Schließlich stärkt die DS-GVO das Recht auf informationelle Selbstbestimmung, indem sie die zentralen Grundsätze der Verarbeitung personenbezogener Daten festlegt und diese auch für Private verbindlich macht.

Bei der Verarbeitung von Daten haben sich Unternehmen an die folgenden Regeln zu halten:

- Personenbezogene Daten müssen auf **rechtmäßige Weise**, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Für die Rechtmäßigkeit bedarf es in der Regel der Einwilligung der betroffenen Person.
- Die Daten müssen zudem **sachlich richtig** und auf dem neuesten Stand sein. Datenverarbeiter müssen die erforderlichen Maßnahmen ergreifen, um dies zu gewährleisten.
- Die Erhebung, Verarbeitung und Speicherung personenbezogener Daten muss stets **zweckgebunden** sein und in einem angemessenen Verhältnis zum jeweiligen Zweck stehen. Erledigt sich der Zweck nachträglich, so besteht ein Anspruch auf „Vergessenwerden“, also auf Löschung der Daten. Auch muss die Sicherheit der Daten gewährleistet sein.
- Personenbezogene Daten müssen schließlich in einer Form gespeichert werden, die die **Identifizierung** der betroffenen Person ermöglicht, allerdings nur so lange, wie es für den Zweck der Datenverarbeitung erforderlich ist.
- Personenbezogene Daten müssen in einer Weise verarbeitet werden, die einen **angemessenen Schutz** der personenbezogenen Daten gewährleistet. Die Anforderungen an die Sicherheit der Verarbeitung werden dabei detailliert ausbuchstabiert.

Darüber hinaus müssen Unternehmen auch bestimmte organisatorische Maßnahmen ergreifen, die eine strikte Einhaltung der oben genannten Regeln sicherstellen sollen. Die Datenverarbeiter müssen klar die **Einhaltung dieser Grundsätze nachweisen können**. Sie

müssen insbesondere ein Verzeichnis von Verarbeitungstätigkeiten führen und sind zur Kooperation mit der jeweiligen Aufsichtsbehörde verpflichtet. Sie müssen zudem in der Regel einen **unternehmenseigenen Datenschutzbeauftragten benennen** und diesen frühzeitig in alle relevanten Datenschutzfragen einbinden.

Schließlich **haften** Datenverarbeiter **für die Schäden**, die betroffenen Personen durch eine rechtswidrige Datenverarbeitung entstanden sind. Für Verstöße gegen die Verordnung können von den Aufsichtsbehörden zudem für die Schwere des Verstoßes angemessene und abschreckende **Geldbußen** verhängt werden, die bei Unternehmen bis zu 20 Mio. € bzw. 4 % des jährlichen globalen Gesamtumsatzes ausmachen dürfen. Damit schafft die DS-GVO eine abschreckende Drohkulisse, die rechtswidrige Praktiken finanziell äußerst unattraktiv erscheinen lässt.

6. Aufsicht

Die Mitgliedsstaaten werden von der DS-GVO dazu verpflichtet, **unabhängige Aufsichtsbehörden** zu errichten und diese angemessen auszustatten. Die Aufgabe dieser Behörden ist es, die Anwendung der Verordnung in ihrem Hoheitsgebiet zu überwachen, Aufklärung in Datenschutzfragen zu betreiben, Gesetzgeber und Exekutive in Datenschutzfragen zu beraten sowie betroffene Personen bei ihrer Rechtsdurchsetzung zu unterstützen. Allerdings bedarf es für die konkrete Umsetzung noch zusätzlicher mitgliedsstaatlicher Regelungen. Diese müssen etwa die konkreten Untersuchungs-, Abhilfe-, Sanktions-, Genehmigungs- und Beratungsbefugnisse der Aufsichtsbehörde regeln. An die Besetzung der Behörde stellt die DS-GVO ebenfalls Anforderungen im Hinblick auf Transparenz und demokratische Legitimation.

7. Fazit

Die DS-GVO schafft einen einheitlichen europäischen Rahmen für einen Datenschutz, der erstmalig den Anforderungen des digitalen Zeitalters und der kommerziellen Motivation zahlreicher Datenverarbeitungsvorgänge Rechnung trägt. Damit läutet die Europäische Union einen Paradigmenwechsel ein, der das Grundrecht auf informationelle Selbstbestimmung stärkt.

Quellen

- http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679
- https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung

- http://www.datensicherheit.de/aktuelles/eu-datenschutz-grundverordnung-so-wappnen-sich-unternehmen-26360
- https://www.datenschutz-praxis.de/fachnews/datenschutz-anpassungs-und-umsetzungsgesetz-im-bundeskabinett-beschlossen/