Was ist die DSGVO?

Maximilian von Grafenstein, Amélie Heldt, Kevin Klug, Jörg Pohle, Wolfgang Schulz

Neue Rechte für VerbraucherInnen, neue Pflichten für Unternehmen: Das europäische Datenschutzrecht erhält ein massives Update, denn am 25. Mai 2018 tritt die EU-Datenschutzgrundverordnung (DSGVO) in Kraft. Damit können UserInnen einfacher herausfinden, was Facebook, Google & Co. alles speichern. Wird die DSVGO den Datenverkehr wirklich transparenter machen? Oder alles doch nichts Neues? Unsere Forscherinnen und Forscher beleuchten in diesem Zusammenhang weitere Themen wie Algorithmenethik, künstliche Intelligenz, Microtargeting oder den CLOUD Act. Dieses brandneue Dossier sorgt hoffentlich für Durchblick im Datendschungel!

1 | DSGVO – was steht dahinter?

Datenschutz – ein Thema, das bislang nur für Datenschutzbeauftragte von Interesse schien. Wenige Wochen vor ihrer Inkraftsetzung am 25. Mai 2018 ist die DSGVO ein Leitthema auf nationaler, europäischer und internationaler Ebene, da sie sowohl den öffentlichen als auch den privaten Sektor betrifft und viele Änderungen bei der Verarbeitung personenbezogener Daten mit sich bringt.

Das Recht auf Schutz personenbezogener Daten ist in der Grundrechtecharta der Europäischen Union in Artikel 8 verankert. Die EU hat jedoch nicht auf die Grundrechtecharta gewartet, um personenbezogene Daten zu schützen. Um den Informationsfluss im Binnenmarkt zu erleichtern und gleichzeitig die Daten der Bürger zu schützen, haben das Europäische Parlament und der Rat am 24. Oktober 1995 die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verabschiedet. Um dieses Recht zu stärken und einen Standard auf EU-Ebene zu setzen, wurde die DSGVO als Verordnung angestrebt. Beachtlich ist, dass es sich dabei nicht um eine Richtlinie handelt, die die einzelnen Mitgliedstaaten mit einem Umsetzungsgesetz für sich hätten interpretieren können, sondern dass der EU-Gesetzgeber die Verordnung gewählt hat, die unmittelbare Wirkung entfaltet.

Der Standard in Deutschland war durch das Bundesdatenschutzgesetz (BDSG) bereits hoch, obwohl der Schutz auf verfassungsrechtlicher Ebene per se nicht verankert war: das Grundgesetz regelt den Schutz personenbezogener Daten nicht ausdrücklich. Dieses Grundrecht auf „informationelle Selbstbestimmung“ wurde durch die Rechtsprechung des Bundesverfassungsgerichts in Art. 2 Abs. 1 GG auf der Grundlage des allgemeinen Persönlichkeitsrechts nach Art. 1 und 2 festgelegt. Es schützt (u.a.) die Entscheidungsfreiheit des Einzelnen darüber, wann und in welchem Umfang

persönliche Daten weitergegeben werden. Der monetäre Wert dieser Daten ist irrelevant; diese müssen jedoch mit einer bestimmten Person verbunden sein – unabhängig davon ob es sich um eine private oder juristische Person handelt.

Eine wichtige Veränderung der DSGVO ist, dass der räumliche Anwendungsbereich der DSGVO ist weiter geworden als bisher im BDSG: Die Verordnung ist schon dann anwendbar, wenn die Datenverarbeitung im Zusammenhang damit steht, dass den Betroffenen innerhalb der EU Waren oder Dienstleistungen angeboten werden, oder das Verhalten betroffener Personen beobachtet wird, soweit ihr Verhalten in der EU erfolgt (Art. 3 DSGVO). Es kommt dabei nicht darauf an, ob die Datenverarbeitung in der EU stattfindet. Angesichts der globalen digitalen Wirtschaft ist dies ein konsequenter Schutzmechanismus, der ökonomische Akteure dazu verpflichtet, die Rechte der europäischen VerbraucherInnen in Bezug auf ihre personenbezogenen Daten ernst zu nehmen. Die DSGVO könnte auch eine Vorbildfunktion für andere Staaten entwickeln, ihre Datenschutzpolitik anzugleichen.

Amélie Heldt

2 | Die vier wichtigsten Innovationen der EU Datenschutz-Grundverordnung

Die DSGVO wird am 25. Mai mit einem doppelten Versprechen anwendbar: Sie soll nicht nur einen besseren Schutz für die von der automatischen Datenverarbeitung Betroffenen leisten, sondern auch einen Wettbewerbsvorteil für die Datenverarbeiter darstellen. Doch wie sieht der aus?

Die Datenschutz-Grundverordnung ersetzt die bisher geltende EU Datenschutz-Richtlinie sowie die auf ihr beruhenden nationalen Datenschutzgesetze und passt die darin vorgesehenen Regelungen an die Herausforderungen des Internetzeitalters an. Als Verordnung hat sie – anders als die Richtlinie – unmittelbare Geltung in allen Mitgliedsstaaten der EU. Aus Perspektive der Wirtschaft wird die DSGVO oftmals als große Hürde kritisiert, insbesondere weil sie keine regulatorischen Neuerungen mit sich brächte, die für die Bewältigung der Herausforderungen geeignet seien.

Diese Herausforderungen liegen in der hohen Innovationsdynamik auf datengetriebenen Märkten, die sich mit folgender Frage zusammenfassen lassen: Wie kann der Gesetzgeber vor Risiken von Innovationen schützen, die er definitionsgemäß noch gar nicht kennt? Der DSGVO wird nachgesagt, dass sie keinen neuen Regelungsansatz wagt, der mit dieser Herausforderung umgehen könnte, sondern denselben (klassischen) Ansatz aus der alten Richtlinie fortschreibt: alter Wein in neuen

Schläuchen. Bei genauerem Hinsehen hält die DSGVO allerdings sehr wohl gesetzgeberische Innovationen bereit, die vor allem für europäische Unternehmen, die personenbezogene Daten verarbeiten, einen Wettbewerbsvorteil darstellen können.

Das Marktortprinzip: Common Level Playing Field für europäische und außereuropäische Unternehmen

Vor Geltung der DSGVO gab es Klagen von in Europa ansässigen, datenverarbeitenden Unternehmen, die gegenüber außereuropäischen Unternehmen einen Wettbewerbsnachteil erlitten: ausländische Unternehmen mussten nicht die strengen Datenschutzgesetze der EU einhalten. Das Marktortprinzip – eine der wichtigsten Neuerungen der DSGVO – stellt für alle Unternehmen nun ein „Common Level Playing Field" her. Damit gilt die DSGVO für alle gleich, egal ob man in- oder außerhalb der EU personenbezogene Daten verarbeitet. Die Anwendbarkeit der Verordnung hängt also nicht mehr ausschließlich vom Sitz der Unternehmen in der EU ab. Vielmehr ist die Verordnung auch auf Unternehmen anwendbar, die ihren Sitz außerhalb der EU haben, deren Datenverarbeitung aber im Zusammenhang mit Waren oder Dienstleistungen steht, die in der EU angeboten werden (oder die Verarbeitung auf eine Beobachtung von menschlichen Verhaltensweisen hinausläuft, die in der EU stattfinden).

Der risikobasierte Ansatz: Zwischen effektivem Risikoschutz und Innovationsoffenheit

Dass die DSGVO für alle datenverarbeitenden Unternehmen gleichermaßen gilt, sagt freilich noch nichts darüber aus, ob sie datengetriebene Innovationen – für die es zweifelsohne ein gesellschaftliches Bedürfnis gibt – unnötig behindert. In diesem Zusammenhang stellt der sogenannte risikobasierte Ansatz eine der wichtigsten Neuerungen der DSGVO dar. Der risikobasierte Ansatz besagt, dass die allgemeinen Grundsätze, die prinzipiell für jede Verarbeitung personenbezogener Daten gelten, entsprechend des spezifischen Risikos im jeweiligen Verarbeitungskontext anzuwenden sind.

Die Verarbeitungsgrundsätze – wie zum Beispiel die Grundsätze der Rechtmäßigkeit der Verarbeitung, der Transparenz, der Datenminimierung und der Zweckbindung – sind also nicht immer alle in gleicher Weise anzuwenden. Vielmehr hängt es vom jeweiligen Risiko ab, ob und vor allem wie diese Grundsätze umzusetzen sind. Bei einem sehr hohen Risiko sind die Grundsätze strikter anzuwenden, als wenn die Datenverarbeitung nur ein geringes Risiko mit sich bringt.

Die DSGVO stellt damit nicht für jede Datenverarbeitung die gleiche regulatorische Bürde da. Für risikoreiche Bearbeitungen ist diese Bürde höher und für risikoarme Verarbeitungen niedriger. Damit hat der Verbreiter personenbezogener Daten einen wesentlichen Spielraum, wie er seine Datenverarbeitung ausgestalten möchte, welches Risiko er dabei für die Betroffenen verursacht – und wie hoch letztendlich die regulatorischen Anforderungen an seine Datenverarbeitung sind. Somit kann der Verarbeiter personenbezogener Daten seine datengetriebenen Innovationsprozesse im

Wesentlichen selbst gestalten. Mit dem risikobasierten Ansatz hat der Gesetzgeber also grundsätzlich ein innovationsoffenes Gesetz geschaffen.

Instrumente der Ko-Regulierung: Innovationsfördernde Effekte von Verhaltensrichtlinien und Zertifikaten

Der risikobasierte Ansatz geht allerdings mit einer erheblichen Rechtsunsicherheit einher. Denn selbst wenn ein Datenverarbeiter versucht, die Datenschutzgrundsätze bestmöglich in Anbetracht des jeweiligen Risikos umzusetzen, weiß er nicht, ob er mit dieser konkreten Umsetzung den Erwartungen der zuständigen Datenschutzbehörde entspricht. Auch dieses Problem hat der Gesetzgeber jedoch erkannt und deshalb Verfahren der sogenannten „Ko-Regulierung" in der Verordnung etabliert. Über diese Verfahren ist der Datenverarbeiter in der Lage, die Umsetzung der Grundsätze gemeinsam mit der zuständigen Datenschutzbehörde zu konkretisieren.

Solche Verfahren sind in der DSGVO vor allem in Form von Zertifizierungsmechanismen und Verhaltensrichtlinien (Codes of Conduct) vorgesehen. Über Zertifizierungsmechanismen können die Verarbeiter von Daten die Datenschutzgrundsätze für einzelne Verarbeitungsprozesse konkretisieren – beziehungsweise für datengetriebene Produkte oder Dienstleistungen, die auf bestimmten Verarbeitungsprozessen beruhen. Ein solches Zertifikat muss zunächst von der Datenschutzbehörde genehmigt werden. Hat ein Datenverarbeiter seine konkrete Umsetzung der Datenschutz-Grundsätze für seine Prozesse oder Produkte in Form eines solchen Zertifikats standardisiert, kann er sich grundsätzlich darauf verlassen, dass seine Datenverarbeitung von der Datenschutzbehörde als mit der DSGVO vereinbar angesehen wird.

Ähnlich verhält es sich mit Verhaltensrichtlinien. Datenverarbeiter in einem bestimmten Sektor – zum Beispiel in der Automobil-, Versicherungs- oder Werbeindustrie – können sich einen gemeinsamen „Code of Conduct" geben. Wer sich an einem solchen, von einer Datenschutzbehörde genehmigten Code of Conduct hält, kann von der Vereinbarkeit seiner Datenverarbeitung mit der DSGVO grundsätzlich ausgehen. In der Folge profitieren sowohl Unternehmen als auch VerbraucherInnen durch eine erhöhte Rechtssicherheit. Diese Wirkung darf nicht unterschätzt werden: Wissenschaftliche Arbeiten weisen darauf hin, dass eine solche Entlastung innovationsfördernde Effekte mit sich bringt. Diese bestehen unter anderem in der Signalwirkung, die Datenschutz-Zertifikate und Verhaltensrichtlinien auf VerbraucherInnen, GeschäftskundInnen und InvestorInnen haben können.

Vom Zuckerbrot zur Peitsche: Die erhöhten Bußgeld-Androhungen

Nicht alle Akteure lockt die Aussicht auf erhöhte Rechtssicherheit. Einige Unternehmen mögen durchaus zu dem Schluss kommen, dass sich die Einhaltung datenschutzrechtlicher Vorgaben – vor allem bei einem hohen Risiko – ökonomisch schlichtweg für sie nicht lohnt (etwa weil der Aufwand, diese hohen Risiken zu

reduzieren, zu kostspielig wäre). Für diesen Fall hält der Gesetzgeber ebenfalls eine Neuerung bereit, und zwar in Form erheblich höherer Bußgelder für Datenschutzverstöße: Die Bußgelder richten sich dabei auch nach dem Umsatz des rechtsbrüchigen Unternehmens. Für einen Verstoß gegen bestimmte Datenschutzvorschriften muss mit einer Zahlung in Höhe von bis zu 4% des weltweiten Jahresumsatzes gerechnet werden. Durch diese massiv erhöhten Bußgeld-Androhungen entsteht letztlich ein Wettbewerbsvorteil für Unternehmen, die sich um eine ordnungsgemäße Umsetzung der Datenschutzvorschriften bemühen.

Damit diese vier Neuerungen aber auch tatsächlich zum vielbeschworenen Wettbewerbsvorteil der DSGVO führen, müssen alle Beteiligten dieses Regelungskonzept verstehen und zu ihrem Vorteil nutzen. Dazu gehört zunächst, dass die Datenschutzbehörden und Gerichte die DSGVO in dem hier beschriebenen Sinne auslegen. Die datenverarbeitenden Unternehmen müssen den Regelungsansatz als Geschäftsgelegenheit nutzen. Nur wenn diese die Einhaltung der DSGVO als Wettbewerbsvorteil sehen und sich entsprechend am Markt positionieren, können die innovationsfördernden Effekte eintreten. Letztendlich hängt es auch von den GeschäftskundInnen und VerbraucherInnen datengetriebener Produkte und Dienstleistungen ab, ob sich der Wettbewerbsvorteil realisiert. Nur wenn diese die Einhaltung der DSGVO als Qualitätsmerkmal ansehen und durch ihre Kaufentscheidung honorieren, kann sich der Kreislauf von Angebot und Nachfrage in Hinsicht auf datenschutzfreundliche Produkte schließen, und der innovative Regulierungsansatz seine volle Dynamik auf dem Markt entfalten.

Max von Grafenstein

3 | Was genau leistet die DSGVO im Hinblick auf algorithmische Entscheidungen – und was nicht?

Für ein aktuelles Gutachten der Bertelsmann-Stiftung habe ich zusammen mit Stephan Dreyer vom Hans-Bredow-Institut untersucht, ob die individuellen Rechte bei der Verwendung der eigenen Daten für vollautomatisierte ADM-Systeme (algorithmic decision making, kurz: ADM), die mit Umsetzung der DSGVO wirksam werden, auch systematische Mängel oder Diskriminierungen ganzer Personengruppen beheben können. Diese Systeme arbeiten ohne menschliches Zutun und fallen somit unter die Regelung der DSGVO, nach der bei automatisierten Entscheidungen – wenn sie überhaupt zulässig sind – künftig erklärt werden muss, wie sie zustande gekommen sind: Art. 15 Abs. 1 DSGVO besagt, dass von automatisierten Entscheidungen betroffene Individuen ein Recht auf „aussagekräftige Informationen über die involvierte Logik“ haben.

Allerdings regelt die DSGVO vorrangig den Schutz Einzelner, für die fehlerhafte Bewertung oder systematische Benachteiligung größerer Gruppen durch automatisierte Entscheidungen ist die neue Datenschutzverordnung blind. Um die Diskriminierung bestimmter Gruppen durch algorithmische Entscheidungsverfahren aufzudecken, reichen die klassischen Auskunfts- und Abwehrrechte des Individuums nicht aus: Allein dadurch, dass der oder die Einzelne mitgeteilt bekommt, wie die automatisierte Entscheidung zustande gekommen ist, ändert sich für diskriminierte Gruppen nichts. Da die DSGVO keineswegs fordert, Geschäftsgeheimnisse durch Transparenzpflichten zu ruinieren, können wir gegenwärtig auch nicht mit einer vollständigen Offenlegung von mathematisch-statistischen Verfahren – wie zum Beispiel dem Schufa-Score – rechnen, auch wenn die Unternehmen mehr erklären müssen als zuvor.

Wenn algorithmische Entscheidungsverfahren über die Vergabe eines Kredits oder die Besetzung einer Stelle entscheiden, geht's also nicht unbedingt fairer zu. Für Diskriminierung durch Algorithmen und künstliche Intelligenz greift die neue DSGVO deutlich zu kurz.

Wolfgang Schulz

4 | Ist der Datenskandal um Facebook berechtigt? Kann die DSGVO dem entgegen wirken?

Nein, der Skandal ist nicht berechtigt. Facebook hat nur getan, wofür es von den NutzerInnen eine Einwilligung erhalten hat. Dass diese die verschiedenen Erklärungen, etwa die Data Policy, die Privacy Policy oder die Community Guidelines der Social Media-Plattform nicht gelesen haben, bevor sie in Facebooks Datenverarbeitung eingewilligt haben, ist sicher ein Problem – aber keines, für das Facebook verantwortlich ist. Die gleichen NutzerInnen haben auch die DSGVO nicht gelesen. Wenn man der öffentlichen Debatte derzeit folgt – etwa zum sogenannten Datenskandal der Deutschen Post – dann zeigt sich, dass die allermeisten Menschen Erwartungen an die DSGVO haben, die sie nicht erfüllt. Und die sie auch nicht erfüllen will, wie der Europäische Gesetzgeber sowohl im Gesetzestext als auch in den Erwägungsgründen ausführlich geschrieben hat.

So wird etwa in der Öffentlichkeit unablässig der Eindruck erweckt – und zwar explizit auch von den Datenschutzaufsichtsbehörden – dass eine Datenverarbeitung grundsätzlich nur mit Einwilligung zulässig sei. Die DSGVO sagt aber anderes: Artikel 6 Absatz 1 Punkt f erlaubt eine Datenverarbeitung etwa, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" ist. Und Erwägungsgrund 47 führt dazu aus: „Die Verarbeitung personenbezogener Daten zum

Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

Die DSGVO wird insofern dem „Datenskandal" nicht entgegenwirken können, weil die Skandalisierung nach völlig eigenen Regeln abläuft, die mit der Rechtslage nicht zwangsläufig etwas zu tun haben müssen. In Bezug auf die Nutzung von Daten für Wahlkämpfe sei hier etwa auf § 50 Absatz 1 Bundesmeldegesetz verwiesen, wonach Meldedaten an „Parteien, Wählergruppen und andere Trägern von Wahlvorschlägen" herausgegeben werden. Und im Zusammenhang mit dem Vorwurf von WählerInnenmanipulation sei hier auf den ehemaligen Bundesvorsitzenden der SPD verwiesen: „Ich bleibe dabei: Daß wir oft an Wahlkampfaussagen gemessen werden, ist nicht gerecht."

Jörg Pohle

5 | Macht Trump's schnell durchgewunkener CLOUD Act die DSGVO unwirksam?

Neu ist, dass US-Ermittlungsbehörden nun ungeachtet von Regelungen ausländischen Rechts auf im Ausland gespeicherte Daten zugreifen können, insofern sie von US-Unternehmen verwaltet und verarbeitet werden. Damit werden erstmal die Befugnisse von US-Behörden erweitert und der Zugang zu Daten vereinfacht. Der 18 U.S.C. § 2713 verpflichtete Provider und Cloud-Anbieter Inhalte herauszugeben, „unabhängig davon, ob sich die Kommunikation, Aufzeichnung oder andere Informationen innerhalb oder außerhalb der U.S. befinden". Dienstanbieter haben aber die Möglichkeit, behördlichen Anordnungen binnen 14 Tagen zu widersprechen, soweit die Herausgabe ausländischem Recht widersprach. Zu einer gerichtlichen Kontrolle – also möglicherweise der Änderung oder Aufhebung einer behördlichen Anordnung – kommt es aber nur bei Rechtskollision mit sogenannten „qualifizierten Ländern". Das sind dann wiederum Länder, die ein Datenschutzabkommen mit den USA unterzeichnet haben. Hierbei führt das Gericht dann eine sogenannte Güterabwägung durch und prüft das Ermittlungsinteresse, die Interessen des qualifizierten Landes und die Wahrscheinlichkeit oder das Ausmaß der Straftat im Ausland.

In Europa ist ab dem 25. Mai 2018 die DSGVO anwendbar. Darin werden die unterschiedlichen datenschutzrechtlichen Regelungen der Mitgliedsstaaten der EU auf ein einheitliches Schutzniveau angeglichen. Hierbei sind insbesondere die Art. 44 ff. DSGVO interessant. Die regeln nämlich die Datenübertragung in Drittländer und versuchen damit sicherzustellen, dass das gewährleistete Schutzniveau nicht einfach durch Datenexport untergraben werden kann. Die EU-Kommission muss unter Beachtung von Rechtsprechung, Rechtsstaat, von Menschenrechten und

Grundfreiheiten der wirksamen Überwachung der Einhaltung von Datenschutzregeln durch unabhängige Aufsichtsbehörden sowie der Verpflichtungen durch internationale Übereinkommen nachkommen.

Offiziell soll mit dem CLOUD Act die grenzüberschreitende Ermittlung vereinfacht werden. Hier ergeben sich oft Behinderungen mit Gesetzen anderer Länder. Und da die DSGVO auch auslandsbezogene Sachverhalte regelt, kann es durchaus zu Konflikten mit dem CLOUD Act kommen. Das Abkommen zielt darauf, ein Privatsphäre- und Datenaustausch-Abkommen mit den USA zu schließen, das den Behörden wiederum eine in Gesetz gegossene Zugriffsbeschränkung und Kontrollmöglichkeit in den USA gewährt. Erst dann wird ausländisches Recht (hier die DSGVO) durch den CLOUD ACT überhaupt erst berücksichtigt. Selbst wenn die EU ein entsprechendes Abkommen unterzeichnete und ein qualifiziertes „Land" würde, wäre noch immer fraglich, ob das Verfahren den hohen Anforderungen der DSGVO gerecht wird.

Kevin Klug