CDU/CSU-Gruppe in der evp - fraktion im europäischen parlament

Positionspapier

Modernisierung der DSGVO: Auf dem Weg zur Version 2.0

25. Mai 2021

Die Versprechen der Datenschutzgrundverordnung (DSGVO) sind vielfältig. Sie soll die Privatsphäre schützen und das Selbstbestimmungsrecht des Einzelnen garantieren. Sie soll digitale Gatekeeper in ihre Schranken weisen. Sie soll ein Bollwerk gegen den Überwachungsstaat und den Überwachungskapitalismus sein. Das Gesetz ist - für Befürworter - der neue Goldstandard des Datenschutzes. Versucht man eine ehrliche Bewertung der DSGVO drei Jahre nach ihrer Anwendung vorzunehmen, wird man allerdings auch andere Ansichten hören. Viele Bürger, Forschungsinstitute, gemeinnützige Organisationen und kleine Unternehmen beklagen sich enorm über ein weiteres EU-Bürokratiemonster, das ihren Alltag überkompliziert, den Aufwand massiv erhöht und in keiner Beziehung zum Kosten-Nutzen-Verhältnis steht. Darüber hinaus gibt es die begründete grundrechtliche Kritik, dass die DSGVO die bürgerlichen Freiheiten beeinträchtigt und wichtige rechtsstaatliche Standards untergräbt.

Als ich 2011 als Berichterstatter des Europäischen Parlaments den Initiativbericht für ein "Gesamtkonzept für den Datenschutz in der Europäischen Union " (aus dem die spätere DSGVO hervorging) schrieb, war ich ein starker Befürworter gesetzgeberischer Maßnahmen. Alarmiert durch ständige Datenschutzskandale sah ich es als unsere demokratische Pflicht an, die zersplitterten nationalen Systeme zu harmonisieren und das Recht unserer Bürger auf Privatsphäre deutlich zu stärken. In diesem Sinne würde ich die DSGVO immer noch als Erfolg betrachten. Doch schon während der politischen Verhandlungen über die DSGVO als Schattenberichterstatter wurde mir klar, dass das Gesetz auch zahlreiche Mängel aufweist. Mit der Zeit wurde ich immer kritischer gegenüber diesen Punkten und schließlich wurde ein Großteil meiner Kritik durch den öffentlichen Aufschrei,

nachdem die DSGVO im Jahr 2018 Anwendung fand, bestätigt. Die Europäische Union hat zwar ein Gesetz geschaffen, das in der Theorie hervorragend sein mag und die Standards für den Datenschutz in vielen Bereichen verbessert hat, jedoch in anderen Bereichen für rechtliches und praktisches Chaos gesorgt hat.

Egal wie gut die Absichten des Gesetzgebers sind, Gesetze sind nie perfekt. Fehlentscheidungen sind Teil der Politik und wir sind dafür verantwortlich, sie zu korrigieren. Was mich daher schockiert hat, waren die Reaktionen bestimmter Entscheidungsträger in Brüssel und der Datenschutzbehörden, die den öffentlichen Aufschrei bis heute ignorieren und immer noch nicht bereit sind, anzuerkennen, dass es Probleme gibt. Für sie ist die DSGVO „das perfekte Gesetz" oder sogar „die Datenschutzbibel". Für sie sind die bestehenden Probleme allein die Schuld der Mitgliedstaaten, die das Gesetz falsch umsetzen; unserer Unternehmen und Bürger, die es nicht richtig verstehen; der Rechtsberater, die es nicht richtig erklären; der Aufsichtsbehörden, die es nicht richtig durchsetzen; und der Gegner des Gesetzes, die absichtlich Verwirrung stiften.

Nachdem ich dieselbe Argumentationslinie Anfang des Jahres im LIBE-Ausschuss wieder gehört habe, als ich als Schattenberichterstatter die neue DSGVO-Resolution verhandelte, habe ich beschlossen, etwas Neues zu versuchen. Am 16. Februar 2021 habe ich meine eigene öffentliche Konsultation gestartet, um Ihre Meinung über die DSGVO zu erfahren. Mit mehr als 180 Antworten haben Sie meine Zweifel bestärkt und beschrieben, wie die DSGVO zu zahlreichen Problemen in Ihrem täglichen Leben führt. Auffallend war, dass nur etwa 1/3 der Antworten von Unternehmen und Wirtschaftsverbänden kam, während die große Mehrheit von Bürgern, Forschern, Wissenschaftlern, Krankenpflegern, Datenschutzbeauftragten, Anwälten, gemeinnützigen Vereinen, Sportvereinen und vielen mehr stammte. Die folgende Liste kategorisiert und fasst Ihr Feedback zusammen.

Während sich diese Liste ausschließlich auf konzeptionelle Fehler, rechtliche Lücken und praktische Probleme konzentriert, die seit dem Inkrafttreten der DSGVO im Jahr 2018 aufgetreten sind, argumentiert dieses Dokument nicht dafür, dass das Gesetz selbst zurückgezogen werden sollte oder dass seine Verabschiedung per se ein Fehler war. Datenschutz ist und muss immer ein wesentliches Element unseres demokratischen Systems bleiben. Darüber hinaus steht die DSGVO für eine wesentliche Verbesserung des Rechts auf Privatsphäre. Weder ich noch andere Kritiker wollen die hohen Datenschutzstandards der EU absenken. Die Liste zeigt aber deutlich, dass das Gesetz in seiner jetzigen Form gleichzeitig andere Grundrechte in den Hintergrund stellt, zu einer Kostenexplosion bei der Einhaltung führt und die digitale Transformation Europas massiv behindert. Wir sind es unseren Bürgern schuldig, diese

Tatsachen anzuerkennen und damit zu beginnen, die mit der DSGVO zusammenhängenden Probleme durch rechtliche Anpassungen sowie eine bessere Anleitung zu beheben. Was wir brauchen, ist eine neue Denkweise, wenn es um die Nutzung von Daten geht. In unserer digitalen Welt bieten Daten vielfältige Chancen, den Lebensstandard zu verbessern und aktuelle Probleme wie den Klimawandel oder eine Pandemie anzugehen. Erst im zweiten Schritt sollten wir uns auf die Risiken konzentrieren und wirksame Schutzmechanismen aufbauen, um möglichen Missbrauch zu verhindern. Die Digitalisierung ist eine große Chance für die EU. Lassen Sie uns damit beginnen, die DSGVO zu einem ausgewogeneren Gesetz zu machen.

Überblick:

I. Konzeptionelle Schwächen der DSGVO.....5

II. Aufkommende Technologien.....10

III. KMUs & Start-Ups vs. digitale Gatekeeper.....14

IV. Privatpersonen und gemeinnützige Einrichtungen.....17

V. Die Wächter: EDSA & DSB.....19

VI. Fragmentierung.....23

VII. Schwachstellen und Lücken im Gesetzestext.....25

VIII. Datenschutz im Gesundheitsbereich.....30

IX. Praktische Probleme.....32

X. Internationale personenbezogene Datenströme.....34

I. Konzeptionelle Schwächen der DSGVO

„One-size-fits-all"-Ansatz

Das Gesetz differenziert nicht zwischen verschiedenen Unternehmen (zB. zwischen globalen Konzernen/digitalen Gatekeepern und lokalen KMU/Start-ups), und berücksichtigt damit nicht die unterschiedlichen Fähigkeiten zur Einhaltung der Datenschutzregeln. Außerdem unterscheidet es nicht zwischen der Verarbeitung personenbezogener Daten durch Privatpersonen und durch staatliche Behörden.

Sektorale Unterschiede

Das Gesetz unterscheidet auch nicht zwischen verschiedenen Sektoren (z.B. Gesundheit und Finanzen) oder verschiedenen Technologien (z.B. KI oder Blockchain) und versäumt es, beides klar zu definieren. Anstatt sich auf grundlegende und gut gestaltete Regeln mit klaren Definitionen, Prinzipien und Methoden zu konzentrieren, die dann durch zusätzliche Richtlinien für verschiedene Sektoren und Technologien ergänzt werden (= normative Spezifizierung), strebt die DSGVO danach, alles gleichzeitig zu schützen.

Risikobasierter Ansatz

Obwohl das Konzept des risikobasierten Ansatzes allgemein behandelt wird, wird es im Gesetzestext nicht konsequent umgesetzt. Die DSGVO differenziert nicht ausreichend zwischen Anwendungen mit geringem und hohem Risiko und legt - mit einigen Ausnahmen wie der vorherigen Konsultation der Datenschutzbehörden bei Anwendungen mit hohem Risiko - weitgehend die gleichen Pflichten für jede Art der Datenverarbeitung fest. Die in der DSGVO vorgesehene Möglichkeit, unterschiedliche Risikoklassen der Datenverarbeitung zu definieren, die unterschiedliche Rechtsgrundlagen erfordern, wird nicht genutzt. Zudem sind die Aufsichtsbehörden oft nicht bereit, Datenverarbeitungsvorgänge mit geringem Risiko als solche zu bezeichnen und erhöhen so den Einhaltungsaufwand.

Komplexität

Die Bestimmungen sind zu zahlreich, komplex und schwierig, so dass nur wenige ausgewiesene Experten wirklich den Überblick behalten und alle rechtlichen Konsequenzen verstehen können.

Veraltete Konzepte

Die DSGVO verwendet Bestimmungen und Ansätze aus früheren Gesetzen, von denen einige sogar bis in die 80er Jahre zurückreichen. Zunächst einmal geht das Gesetz von der Verarbeitung einzelner Daten aus (und ignoriert damit Big Data) sowie von der Verarbeitung durch

einen einzelnen Verantwortlichen (und ignoriert damit Cloud Computing, das Internet der Dinge, Plattformen oder andere komplexe Netzwerke). Die DSGVO geht auch davon aus, dass Daten an einem bestimmten Ort auf einer festen Festplatte verarbeitet werden (und berücksichtigt damit nicht, dass Daten nicht mehr auf einer physischen Ressource gespeichert werden, sondern sich stattdessen global von Server zu Server in globalen Netzwerken, miteinander verbundenen Clouds und Blockchains bewegen). Der Grundsatz der Zweckbindung schließt zufällige Entdeckungen im Bereich der Wissenschaft (z. B. Korrelationen zwischen Befunden) aus. Zusammenfassend lässt die DSGVO unberücksichtigt, dass aktuelle Technologien (z.B. KI) völlig anders funktionieren. Die alten Datenschutzideen (z.B. Datenminimierung) - auf denen die DSGVO basiert - sind daher nicht mehr tragfähig.

Dateninstitutionen

Das Gesetz bietet nicht die Möglichkeit, vertrauenswürdigen Drittanbietern wie Datentreuhändlern oder einer neuen europäischen Datenagentur mehr Flexibilität für einen vereinbarten Zweck einzuräumen. Diese Institutionen könnten dazu beitragen, Datensilos für KMU und Forscher zu öffnen, den Austausch vertraulicher und persönlicher Daten zu erleichtern und den Zugang zu Daten zu verbessern. Die Schenkung von Daten ist auch unter den Bestimmungen der DSGVO zu kompliziert, wenn nicht sogar unmöglich. Da der Data Governance Act einige dieser Probleme anspricht, müssen legislative Überschneidungen mit der DSGVO vermieden werden.

Umfang des Schutzes

Im Gegensatz zur Datenschutzrichtlinie 95/46, die den Schutz der Privatsphäre natürlicher Personen als Hauptinteresse herausstellte, postuliert die DSGVO in Art. 1(2), dass sie die "Grundrechte und Grundfreiheiten" natürlicher Personen schützt. Wenn das Gesetz jedoch alle Rechte und Freiheiten schützen will, führt dies zu einer Überforderung der für die Verarbeitung Verantwortlichen, da sie theoretisch alle Grundrechte und Freiheiten berücksichtigen müssten, und zwar in allen 68 Pflichten und in allen 82 Abwägungsprüfungen der DSGVO. Dies kann in der Praxis niemals erfüllt werden.

Unverhältnismäßigkeit mit anderen Grundrechten

Die DSGVO stellt nicht klar, dass Datenschutz kein absolutes Grundrecht ist, sondern mit anderen Grundrechten oder Interessen wie dem Recht auf Leben, auf Freiheit und Sicherheit, der unternehmerischen Freiheit oder der Pressefreiheit abgewogen werden muss. In Kollision mit der ständigen Rechtsprechung zu Art. 8 der EU-Grundrechtscharta oder Art. 16 AEUV unterstützen jedoch immer mehr Entscheidungsträger und Regulierer diese radikale Auslegung. Außerdem berücksichtigt die DSGVO nicht, dass die Verarbeitung

personenbezogener Daten durch den Verantwortlichen an sich auch durch Grundrechte (z.B. die Wissenschaftsfreiheit oder die unternehmerische Freiheit) geschützt ist.

Rechtfertigung der Verarbeitung

Da jede Art der Verarbeitung personenbezogener Daten das Recht auf Datenschutz einschränkt, bedarf jede dieser Einschränkungen einer Rechtfertigung auf der Grundlage des Gesetzes. Rechtfertigungen können sich aus den Rechten und Interessen des für die Verarbeitung Verantwortlichen, aus den Rechten und Interessen eines Dritten oder aus dem öffentlichen Interesse ergeben. Die DSGVO enthält jedoch kein kohärentes Konzept, wie und wann das Datenschutzrecht rechtmäßig eingeschränkt wird. Die Rechte und Interessen, die mit dem Datenschutzrecht kollidieren, sind eher bruchstückhaft und sprunghaft aufgelistet. Auch zusätzliche Schwierigkeiten während der COVID-19-Pandemie haben ein Licht auf diese Problematik geworfen.

Paradigmenwechsel

Das Datenschutzrecht war ursprünglich als Abwehrrecht des Bürgers gegenüber dem Staat konzipiert. Dieser Ansatz wurde, wenn auch meist unbemerkt, geändert. Regeln, die früher nur für den Staat gemacht wurden, gelten nun auch im Verhältnis zwischen einzelnen Bürgern, im Verhältnis zwischen Unternehmen und Bürgern, aber auch zwischen Unternehmen untereinander. Die Gleichsetzung von Datenverarbeitung im öffentlichen und nichtöffentlichen Bereich ist rechtstheoretisch höchst problematisch und einer der Hauptgründe für die mangelnde Flexibilität der DSGVO.

Verbotsprinzip

Die DSGVO sieht jede Verarbeitung personenbezogener Daten als potenzielles Risiko und verbietet sie grundsätzlich. Sie erlaubt sie nur, wenn ein Rechtsgrund erfüllt ist. Ein solcher Anti-Verarbeitungs- und Anti-Weitergabe-Ansatz macht in unserer datengetriebenen Wirtschaft wenig Sinn und steht im Widerspruch zum allgemeinen Ziel in Art. 1(3) DSGVO, das den freien Datenverkehr fördert. Die Verlagerung von Maßnahmen zur Gefahrenabwehr in ein sehr frühes Stadium, in dem die Risiken noch sehr abstrakt sind, führt zudem zu einem rechtsstaatlichen Problem. Eine Vollstreckung erfordert nicht mehr eine konkrete Gefahr für ein hinreichend bestimmtes Rechtsgut, wie dies im Polizeigewohnheitsrecht der Fall ist. Folglich gehen auch die Eingriffsbefugnisse der Datenschutzbehörden weit über die üblichen Standards für Behörden hinaus. Das Gesetz als solches zielt darauf ab, das Internet und seine Nutzer so umfassend wie möglich zu kontrollieren. Es will auch die Auffassung

durchsetzen, dass die Verarbeitung personenbezogener Daten generell als gesellschaftlich unerwünschtes Verhalten angesehen wird. Dieser Ansatz ist nicht nur fortschrittsfeindlich. Es führt dazu, dass selbst die grundrechtlich geschützte oder zur Wahrung des öffentlichen Interesses gesellschaftlich erwünschte Verarbeitung personenbezogener Daten unter ständigen Rechtfertigungsdruck gerät (z. B. die Weitergabe der Daten potenzieller Impfstoffempfänger oder zur Nutzung der COVID-19-Tracing-Apps).

Überforderung der für die Verarbeitung Verantwortlichen

Die DSGVO bürdet dem zuständigen Verantwortlichen („controller“) zahlreiche Pflichten auf (z.B. Rechtsgrundlage, Interessenabwägung, Informations- und Nachweispflicht, Rechtsbehelfsbelehrung), was zu unverhältnismäßigen Compliance-Kosten führt, die den tatsächlichen Nutzen bei weitem übersteigen. Was in der Theorie gut erscheint, führt in der Praxis dazu, dass Pflichten nur schematisch erfüllt oder sogar ignoriert werden.

Vorrang der Einwilligung

Obwohl die DSGVO sechs gleichermaßen gülitge Rechtsgrundlagen für die Verarbeitung personenbezogener Daten enthält, sehen viele Datenschutzbehörden und politische Entscheidungsträger die Einwilligung als Eckpfeiler des Datenschutzes. Damit wird dem Nutzer die Illusion von Kontrolle gegeben und der Verantwortliche kann die Verantwortung in komplexen und seitenlangen Datenschutzerklärungen auf den Nutzer abwälzen. Aufgeschreckt durch ein weiteres Datenschutz-Banner, stimmen viele Nutzer übermäßig allem zu, um endlich den gewünschten Service zu bekommen, oft ohne zu wissen, wozu sie eigentlich zugestimmt haben. Diese Fokussierung auf Einwilligungen hat die dominante Position einiger weniger großer Unternehmen weiter gestärkt, die aufgrund ihrer verbrauchernahen Position einen Wettbewerbsvorteil haben, wenn sie solche Einwilligungen zentral für alle ihre Dienste oder als Teil ihrer Allgemeinen Geschäftsbedingungen einholen. In der Folge können sie die Datenerhebung für Innovation und Produktentwicklung auf Kosten von KMU oder Start-ups nutzen. Darüber hinaus gehen die extremen Auslegungen des Grundsatzes der freien Einwilligung tendenziell an der Realität vieler datenbasierter Geschäftsmodelle vorbei, wodurch solche Geschäftsmodelle in starke Rechtsunsicherheit geraten, mit Folgen für KMU und für Inhalte/Dienste, die Einzelpersonen online angeboten werden.

E-Privacy-Verordnung

Obwohl die in der Richtlinie von 2002 festgelegten Regeln zur Vertraulichkeit der Kommunikation dringend aktualisiert werden müssen, versäumen es die Pläne der Europäischen Kommission für einen

Verordnungsentwurf sowie die Position des Europäischen Parlaments in erster Lesung, die alten Regeln an die DSGVO anzugleichen. Stattdessen schaffen sie eine eigene Schiene des Datenschutzrechts, die die gesamte EU-Datenschutzpolitik in Frage stellen würde. Inhaltlich gibt es keinen Grund, warum elektronische Kommunikationsdaten außerhalb der DSGVO geregelt werden sollten. Definitionen, Rechtsgrundlage und Bestimmungen zum Profiling sind dort bereits aufgeführt. Warum sollte die DSGVO für Dateien gelten, die auf einer Website veröffentlicht werden, während die neue E-Privacy-Verordnung gilt, wenn die Datei per E-Mail verschickt wird?

Auswirkungen auf andere Gesetze

Aufgrund des umfangreichen und horizontalen rechtlichen Geltungsbereichs wird sich die DSGVO mit bestehenden und zukünftigen Gesetzen überschneiden und diesen widersprechen. Besonders besorgniserregend ist das Verhältnis zum Data Governance Act, der Datenbankrichtlinie und dem Data Act. Mit diesen Paketen verfolgt die EU das wichtige Ziel, eine globale Führungsrolle in der Datenwirtschaft zu übernehmen. Sie will sowohl die Datenverarbeitung als auch den Datenaustausch beschleunigen. Gleichzeitig verbietet die DSGVO aber generell die Weitergabe von privaten Daten, wie oben beschrieben. In der Realität ist dies höchst problematisch, da die Trennung von privaten und nicht-privaten Daten nicht immer machbar (gemischte Daten) und zumindest ein teurer Prozess ist. Daher werden die Datenschutzregeln und die daraus resultierende Rechtsunsicherheit zu einer geringeren Qualität der Datensätze in den europäischen Datenräumen und einer größeren Zurückhaltung der Unternehmen bei der Weitergabe von Daten führen.

Komplizierte internationale Datenflüsse

Obwohl die DSGVO mehrere Mechanismen für internationale Datenflüsse vorsieht (die für europäische Unternehmen mit Tochtergesellschaften, Kunden, Verkäufern oder Lieferanten in Drittländern von entscheidender Bedeutung sind), können nur drei von ihnen von Unternehmen effektiv genutzt werden. Infolgedessen sind die internationalen Datenströme derzeit bedroht, wodurch die Gefahr besteht, dass die Europäische Union vom Rest der Welt isoliert wird.

II. Aufkommende Technologien

Obwohl die DSGVO technologieneutral sein soll, sind das Gesetz und seine Konzepte mit vielen neuen technologischen Entwicklungen nicht kompatibel. Mit den Grundsätzen der Datenminimierung sowie der Zweck- und Speicherbegrenzung in Art. 5 ist die Fokussierung der DSGVO auf die Verarbeitung einzelner Daten durch einen einzigen Verantwortlichen in Art. 4 oder die Beschränkung der Sekundärnutzung von Daten nicht mehr problemadäquat. Diese Konzepte verhindern, dass neue Technologien ihr volles Potenzial ausschöpfen können. Die Folge ist, dass europäische Unternehmen nicht so viel erfinden, wie sie könnten, ihre Prototypen nicht weiterentwickeln oder sogar die EU ganz verlassen, wie es bei vielen Start-ups der Fall ist. Die Rechtsunsicherheit ist einfach zu groß, zumal die nationalen Datenschutzbehörden (DSB) sowie der Europäische Datenschutzausschuss (EDSA) viele Bestimmungen der DSGVO zu restriktiv auslegen. Nachfolgend einige der betroffenen Technologien und Prozesse:

Künstliche Intelligenz

In Europa ist es schwierig, Algorithmen mit ausreichenden Mengen an personenbezogenen Daten zu trainieren (z. B. um KI bei Diagnosen oder der Entwicklung von Medikamenten zu nutzen), da dafür riesige Mengen an hochwertigen Datensätzen benötigt würden. Die Bestimmungen der DSGVO zur Zweckbindung und Datenminimierung sowie die Beschränkungen der Sekundärnutzung können als die größten Hindernisse für KI angesehen werden. Zum Beispiel verlangt die Zweckbindung, dass Forscher und Unternehmen die Erlaubnis jeder betroffenen Person einholen müssen, bevor sie etwas Neues mit ihren Daten machen. Dies macht es schwieriger, die Zustimmung aufrechtzuerhalten, und hindert Forscher und Unternehmen daran, mit ihren Algorithmen zu experimentieren, selbst in Fällen, in denen eine Weiterverwendung keine Auswirkungen auf das Wohl der Verbraucher oder die Privatsphäre hätte. Das Fehlen von Anonymisierungsverfahren und die Tatsache, dass das Training von Algorithmen nicht als statistischer oder wissenschaftlicher Zweck anerkannt wird (Erwägungsgrund 162), sind weitere Gründe. Eine Rechtsgrundlage für die Verarbeitung von Daten bei autonomem Verhalten und für die Einhaltung der Informationspflichten sowie der Transparenz-, Rechenschafts- und Erklärbarkeitsprinzipien der DSGVO zu finden, ist auch für Entwickler und Betreiber von KI-Systemen eine entscheidende Herausforderung. Die Erklärbarkeit kann aufgrund aller am Aufbau und der Nutzung eines KI-Systems beteiligten Stakeholder eine besondere Herausforderung darstellen, da nicht jeder einen ausreichenden Kenntnisstand über

die beteiligten Prozesse hat. Infolgedessen ist unklar, was realistisch, machbar und praktisch ist, wenn es darum geht, Erklärbarkeit zu bieten. Wenn es um Transparenz geht, müssen möglicherweise externe Effekte wie Risiken für die Sicherheit, die Privatsphäre und Geschäftsgeheimnisse berücksichtigt werden.

Internet der Dinge

Die Erlangung einer DSGVO/ePrivacy-konformen Rechtsgrundlage für solche Systeme könnte sich in Szenarien, in denen personenbezogene Daten für einen oder mehrere spezifische Zwecke verarbeitet werden, erneut als schwierig erweisen - etwa bei der hochfrequenten Kommunikation zwischen mehreren Akteuren in der Machine-to-Machine- (M2M) oder Vehicle-to-Everything- (V2X) Kommunikation. Die Einhaltung einer gültigen Einwilligung kann sich bei vernetzten Systemen als unmöglich erweisen, da die Personen in diesen Systemen nicht immer aktive Nutzer sind, die Einwilligungserklärungen akzeptieren können. Die DSGVO-Prinzipien der Speicher- und Zweckbindung und insbesondere der Datenminimierung sind ebenfalls schwer umzusetzen. Das Internet der Dinge hingegen basiert auf „Datenmaximalismus", was die Sammlung riesiger Mengen personenbezogener Daten, die Erstellung spezifischer Nutzerprofile und das Scannen von Geräten bedeutet.

Blockchain und andere Distributed-Ledger-Technologien

Eine Schlüsseleigenschaft der Blockchain-Technologie ist, dass alte Daten gegen Änderungen gesichert werden können, was sie zu einer "Append-Only"-Struktur macht, bei der neue Daten hinzugefügt, aber niemals entfernt werden können. Somit entspricht Blockchain nicht dem DSGVO „Recht auf Vergessenwerden". Sobald personenbezogene Daten in einem dezentralen Block aufgezeichnet sind, ist es nicht mehr möglich, diese Informationen zu löschen. Diese historischen Daten können dann analysiert werden, um Identitäten aufzudecken. Während die DSGVO ihre Regeln gegen mindestens eine bestimmte Person durchsetzt, sind an Blockchains zahlreiche Akteure beteiligt, was die Zuordnung von Verantwortung/Zurechenbarkeit sehr schwierig, wenn nicht gar unmöglich macht. Die Konzepte der DSGVO (Verantwortlicher, gemeinsamer Verantwortlicher und Auftragsverarbeiter) können dies kaum abbilden. Da Blockchains ständig wachsen, können auch die Prinzipien der Datenminimierung und der Zweckbindung nicht erfüllt werden. Schließlich ist oft unklar, ob Daten, die auf einem verteilten Ledger gespeichert oder verschlüsselt oder gehasht sind, noch als personenbezogene Daten gelten.

Biometrische Daten

Anwendungen, die z. B. auf Gesichts- oder Stimmerkennung basieren, oder personenbezogene Daten, die von tragbaren Geräten generiert werden, erfüllen regelmäßig nicht die bestehenden Datenschutzregeln. In vielen Bereichen führen die mit biometrischen Daten verbundenen Risiken sogar zu einem generellen Verbot jeglicher Form der Verarbeitung. Die DSGVO unterscheidet auch nicht zwischen biometrischen Eins-zu-Eins-Vergleichen (z. B. Verifizierung) und Eins-zu-Vielen-Vergleichen (z. B. Identifizierung). Die rechtlichen und technischen Definitionen gehen ebenfalls auseinander und es besteht Unsicherheit darüber, welche Art von Daten als „sensibel" eingestuft wird. Wenn dieser Bereich durch einen neuen KI-Rahmen geregelt wird, müssen Überschneidungen in der Gesetzgebung vermieden werden.

Virtuelle Realität

Hier verbinden sich die bereits aufgeführten Probleme bei der Verarbeitung biometrischer Daten mit der Frage, ob die Einwilligung wirklich frei gegeben wurde, d. h. es ist unklar, ob die betroffene Person eine echte Wahl hatte, die Verarbeitung personenbezogener Daten abzulehnen.

Text- und Data-Mining

Die Verwendung von Text- und Data-Mining ist nicht konform mit der DSGVO, da man nicht sicher sein kann, dass die Methode nicht auch personenbezogene Daten verarbeitet. Der für die Verarbeitung Verantwortliche wird Schwierigkeiten haben, die Transparenzpflichten zu erfüllen, da Text- und Data-Mining per Definition zur Verarbeitung unbekannter Daten führt. Es ist außerdem sehr schwierig, die betroffenen Personen zu benachrichtigen und eine informierte Zustimmung zu erhalten. Es ist auch wichtig, zwischen Text- und Data-Mining zu wissenschaftlichen und zu kommerziellen Zwecken zu unterscheiden, da beide Ansätze unterschiedliche Auswirkungen auf den Datenschutz haben und unterschiedliche Transparenzanforderungen haben sollten.

Profiling und Micro-Targeting

Es fehlt eine Unterscheidung zwischen automatisierter Verarbeitung, einschließlich Profiling, die von Einzelpersonen erwartet wird und die zu effektiveren Diensten für Einzelpersonen und relevanteren Inhalten beiträgt, und Profiling, das Schaden anrichtet, wie z. B. politische Manipulation oder einen kommerziellen Sperreffekt, für den besondere Schutzmaßnahmen vorgesehen werden sollten. Falls letzteres durch neue Gesetze wie das Gesetz über digitale Dienste geregelt wird, sollten Überschneidungen mit bestehenden DSGVO- / E-Privacy-Bestimmungen vermieden werden.

Cloud Computing

Die DSGVO knüpft die Verarbeitung von Daten entweder an einen einzelnen Verantwortlichen (Art. 4 Nr. 7 DSGVO) oder bestimmt Sonderregelungen für Situationen mit mehreren Personen (Art. 26 oder 28 DSGVO). Beide Ansätze sind für Cloud Computing nicht ausreichend. Dieses Problem wird dadurch verschärft, dass mehrere Parteien ohne klar zugewiesene Qualifikationen involviert sind und dass sich die Daten ständig innerhalb miteinander verbundener Clouds bewegen, während sie vorübergehend an verschiedenen physischen Standorten in verschiedenen Ländern gespeichert werden. Die in Kapitel X dieses Papiers aufgeführten Probleme erschweren den Einsatz dieser Technologie zusätzlich.

Home-Office

Mitarbeiter verfügen oft nicht über echtes Datenschutzwissen und werden daher in einer Situation, in der sowohl private als auch geschäftliche Daten zusammengeführt werden, mit widersprüchlichen Verantwortlichkeiten und vielen neuen Pflichten allein gelassen. Infolgedessen verstoßen sie oft ungewollt gegen die DSGVO-Bestimmungen. Viele Arbeitgeber schreiten nicht ein, da sie Kosten sparen wollen oder ihre Mitarbeiter nicht mit neuen Regeln, Verfahren und Pflichten überfordern wollen.

III. KMUs & Start-Ups vs. digitale Gatekeeper

In Kombination mit der ePrivacy-Richtlinie und der ständigen Rechtsprechung führte die DSGVO zu einer **Ausbreitung von Cookie-Bannern** und vielen verschiedenen Arten von Benutzereinwilligungsschnittstellen, während die anderen fünf Rechtsgrundlagen für die Datenverarbeitung häufig nicht verwendet werden. Infolgedessen wurde der bereits bestehende **Vendor Lock-in** in der digitalen Wirtschaft weiter verfestigt. Dieser zustimmungsbasierte Ansatz hat zu einer **hohen regulatorischen Belastung für KMU und Start-ups** geführt und stellt einen erheblichen **Wettbewerbsnachteil** gegenüber großen, verbraucherorientierten Konzernen dar. Diese digitalen Gatekeeper sind in der Lage, mehrere integrierte Online-Dienste anzubieten und damit ein besseres und reibungsloseres Erlebnis für die Nutzer zu schaffen, die im Gegenzug eher bereit sind, ihre Zustimmung zu geben, wenn sie einen ihrer Dienste nutzen wollen.

Digitale Gatekeeper haben viele externe Berater sowie große Rechtsabteilungen mit Datenschutzexperten. KMU und Start-ups hingegen **fehlt oft Wissen, Erfahrung und die finanziellen Ressourcen**, um die DSGVO-Regeln adäquat umzusetzen oder wegen potenziell nicht konformer Dienste vor Gericht zu gehen. Folglich sind sie einem viel **größeren Risiko von Sanktionen** ausgesetzt als ihre großen Konkurrenten, während die Bußgelder gleichzeitig ein **existenzielles Risiko** für ihre Unternehmen darstellen. Ein weiterer Nebeneffekt, der KMU und Start-ups benachteiligt, ist, dass sie sich möglicherweise dafür entscheiden, Ressourcen für die Einstellung externer Rechtsexperten zu verwenden, um die Einhaltung der Verordnung sicherzustellen, anstatt diese Ressourcen in die Einstellung von Datenwissenschaftlern zu investieren, um ihre Produkte und Dienstleistungen zu erneuern/verbessern.

Die **hohen Compliance-Kosten** sowie Rechtsunsicherheit behindern effektiv die Innovation für KMU und Start-ups. Studien haben gezeigt, dass die DSGVO Geschäftsmodelle und das Vertrauen von Investoren stark beeinträchtigt hat, was zu **unternehmerischer Entmutigung** und der Aufgabe von Produkten geführt hat.[1]

Die **Ausnahmeregelung** zur Aufbewahrung von Aufzeichnungen in Art. 30(5) DSGVO für KMU mit weniger als 250 Mitarbeitern ist **praktisch unwirksam**, da jedes Unternehmen mit einer IT-Infrastruktur nicht nur gelegentlich

[1] Im Google Play Store mussten ca. 1/3 aller verfügbaren Apps entfernt werden. Der Eintrag neuer Apps sank um 50%.http://conference.nber.org/conf_papers/f146409.pdf. Siehe auch, wie sich die DSGVO auf Start-up-Innovationen auswirkte, unter https://link.springer.com/article/10.1007/s10796-019-09974-2.

personenbezogene Daten verarbeiten wird. „Nicht gelegentlich" ist sehr weit gefasst, sodass bereits E-Mails, Gehaltsabrechnungen, Kundenverwaltung oder die Ereignisprotokollierung des Betriebssystems darunterfallen. Darüber hinaus muss jedes Unternehmen mit Mitarbeitern regelmäßig besondere Kategorien personenbezogener Daten verarbeiten, wie z.B. Gesundheitsdaten im Rahmen der Lohnfortzahlung oder Angaben zur Religionszugehörigkeit im Rahmen der Lohnsteuerabrechnung. Da die Ausnahmeregelung in diesen Fällen nicht anwendbar ist, tritt die beabsichtigte Entlastung für KMU in der Praxis nicht ein. Für die zahlreichen anderen Pflichten neben Art. 30 Abs. 5 DSGVO gibt es überhaupt keine KMU-Ausnahmen. Schwer nachvollziehbar ist auch das Fehlen einer Erheblichkeitsschwelle, die zwischen den verschiedenen Arten von Risiken und dem Umfang der Verarbeitung personenbezogener Daten sowie der Art des Unternehmens differenziert.

Die herausgegebenen Leitlinien des EDSA und der Datenschutzbehörden zur Ausnahmeregelung in Art 30(5) DSGVO und zu anderen Fragen sind für KMU und Start-ups nicht immer hilfreich. Die Ausarbeitung geeigneter Analyserahmen für jeden Technologietyp zwingt KMU und Start-ups dazu, nach der Lektüre von mehr als 60 Seiten Leitlinien ihre eigenen Folgenabschätzungen durchzuführen, was weder machbar noch pragmatisch ist. Es fehlen vereinfachte und besser strukturierte Rahmen.

Das Fehlen von Interoperabilitätsmechanismen und einer effektiven Umsetzung der Datenportabilitätsrechte hindert KMU und Start-ups daran, Datensilos aufzubrechen, um die eigene Wettbewerbsfähigkeit zu steigern. Die wirtschaftsweiten Datenportabilitätsregeln der DSGVO verlangen, dass personenbezogene Daten über alle Sektoren hinweg in einem „strukturierten, allgemein verwendeten und maschinenlesbaren Format" vorliegen müssen. Dies stellt eine regulatorische Belastung dar, da sektorspezifische Regeln für den Datenaustausch wesentlich besser geeignet wären. Gleichzeitig könnte auch der angedachte Spielraum für Datenportabilität in der Praxis nicht realisierbar sein. Ursprünglich dazu gedacht, den Wechsel zwischen sozialen Netzwerken zu erleichtern, wurde sie über diesen speziellen Anwendungsbereich hinaus ausgedehnt, ohne dass sie dazu beiträgt, den Einzelnen zu stärken. Das Konzept der Datenportabilität wird nur funktionieren, wenn es eine Verpflichtung sowohl für den Export als auch für den Import von personenbezogenen Daten gibt. Selbst die Übertragung personenbezogener Daten außerhalb der EU innerhalb eines

Unternehmensnetzwerks ist kompliziert, da sie die gleichen vertraglichen Anforderungen erfordert wie eine externe Datenübertragung an eine andere Einheit.

Der DSGVO fehlt ein Mechanismus, der es KMU und Start-ups ermöglicht, die Compliance-Last auf Dritte zu verlagern, die dann Daten speichern und verarbeiten. Anbieter von IT-Lösungen könnten die Verantwortung von KMU und Start-ups übernehmen und ihnen so ermöglichen, die Compliance allein durch die Bezahlung und Nutzung ihrer Dienste zu übernehmen. Derzeit führt die Nutzung solcher Dienste zu einem komplexen Haftungsgeflecht, was bedeutet, dass KMU und Start-ups oft noch die Last der Compliance tragen müssten.

IV. Privatpersonen und gemeinnützige Einrichtungen

Zahlreiche neue Pflichten und die Notwendigkeit, viel Zeit und Geld zu investieren, um die DSGVO-Compliance zu gewährleisten, bedeuten eine **hohe regulatorische Belastung für Vereine, Verbände und Privatpersonen**. Diese Anforderungen stehen in keinem Verhältnis zueinander, da diese Einrichtungen und Personen personenbezogene Daten nicht kommerziell verarbeiten sondern ihre Freizeit **als Freiwillige für einen guten Zweck** aufwenden.

Trotz des Mangels an adäquaten Ressourcen und Kenntnissen sowie des geringeren Risikos müssen diese Akteure **zahlreiche Prüfungen** durchführen, wie z. B. Angemessenheitsprüfungen, Interessenabwägungen, Vereinbarkeitsprüfungen, Erforderlichkeitsprüfungen, Angemessenheitstests oder Risikoprüfungen. Dies zeigt erneut, dass einige rechtliche Anforderungen, die durch die DSGVO festgelegt wurden, die praktischen Realitäten völlig aus den Augen verloren haben.

Da Art. 13 und 14 DSGVO allgemein anwendbar sind, müssen auf den Websites von Privatpersonen und freiwilligen Einrichtungen **umfangreiche Informationen offengelegt** werden, was die Länge der Datenschutzrichtlinien erhöht, aber nicht unbedingt die Lesbarkeit und Verständlichkeit der Datenschutzbestimmungen für Einzelpersonen.

Um professionelle Hilfe zu erhalten, beauftragen gemeinnützige Einrichtungen und Privatpersonen oft **Datenschutzberater oder spezialisierte Anwaltskanzleien gegen hohe Gebühren**. Anstatt kostenlose Vorlagen für Datenschutzrichtlinien anzubieten, die die Einhaltung der DSGVO garantieren, hat die EU damit ein **neues Geschäftsmodell** geschaffen, das auf einer **Überfrachtung von Verpflichtungen** für normale Bürger und freiwillige Einrichtungen basiert. Auch die von den Datenschutzbehörden veröffentlichten **Hilfestellungen sind nicht wirklich hilfreich**, da den angesprochenen Akteuren Zeit und Fachwissen fehlt, um diese komplexen Dokumente vollständig zu verstehen und umzusetzen.

Die **Ausnahmeregelung für Haushalte** (Verarbeitung personenbezogener Daten „durch eine natürliche Person im Rahmen einer rein persönlichen oder häuslichen Tätigkeit") ist zu eng gefasst, da nach der Rechtsprechung des EuGHs eine **Veröffentlichung im Internet keine rein persönliche Tätigkeit** darstellen kann. Die relevantere Frage, ob die personenbezogenen

Daten nur zu nicht-kommerziellen Zwecken verarbeitet werden, wird nicht berücksichtigt.

Da jeder Informationsaustausch personenbezogene Daten sowohl des Senders als auch des Empfängers enthält, betrifft die DSGVO (zusammen mit der ePrivacy-Richtlinie) die Kommunikation im Internet per se. Dabei hat der Datenschutz oft sogar Vorrang vor der Meinungsfreiheit. Ausnahmen in Form von Öffnungsklauseln zu Gunsten der Kommunikationsfreiheit (Artikel 85(2) DSGVO) wurden von den Mitgliedstaaten nur für die traditionelle Presse genutzt, nicht aber für die Verarbeitung privater Daten durch Blogger, Hobbyfotografen, Öffentlichkeitsarbeit und andere private Nutzer.

V. Die Wächter: EDSA & DSB

Datenschutzbehörden sind **zu einseitig** und zu sehr auf den Schutz persönlicher Daten fokussiert. Obwohl dies natürlich ihre Hauptaufgabe ist, sollten sie verpflichtet werden, auch andere Elemente wie Fairness, Gleichheit, Gesundheit, Sicherheit, Wettbewerb, Wohlstand und Innovation zu berücksichtigen.

Einerseits erwies sich das Prinzip der „einzigen Anlaufstelle" als entscheidend für die Schaffung von Rechtssicherheit und die Verringerung des Verwaltungsaufwands für Unternehmen und Bürger gleichermaßen. Andererseits half es großen Unternehmen, sich der **Haftung zu entziehen**, weil bestimmte Datenschutzbehörden aus Angst vor dem Verlust von Investitionen in ihren Ländern nicht bereit waren, Ermittlungen durchzuführen und Sanktionen zu verhängen, und/oder weil ihre Arbeitsbelastung unverhältnismäßig hoch war. Wie der Generalanwalt des EuGHs argumentierte, sollte es auch anderen betroffenen Datenschutzbehörden erlaubt sein, eine aktive Rolle bei der Überprüfung der Einhaltung der DSGVO durch die Unternehmen zu spielen und somit die führende Datenschutzbehörde des Landes, in dem das Unternehmen seinen Sitz hat, zu unterstützen. Es ist wichtig zu betonen, dass das beschriebene Problem nicht mit Mängeln im Gesetz zusammenhängt, sondern mit einem **Mangel an konsequenter Anwendung**. Das **Kooperations- und Kohärenzverfahren** - festgelegt in Kapitel VII der DSGVO - bietet Verfahren, die helfen würden, Forum Shopping zu verhindern und Datenschutzbehörden aus anderen Ländern einzubeziehen. Der EDSA und die Datenschutzbehörden nutzen dieses wichtige Instrument bisher jedoch nur selten.

Ein weiterer Grund für die **uneinheitliche und schwache Durchsetzung der DSGVO** - in einigen Mitgliedsstaaten werden nur 0,15 % der Beschwerden über Datenschutzverletzungen untersucht - ist die Tatsache, dass viele nationale **Datenschutzbehörden unterfinanziert und personell unterbesetzt** sind[2]. Sie sind oft nicht in der Lage, den massiven Aufgabenzuwachs zu bewältigen und vor allem Datenschutzverstöße sinnvoll durchzusetzen, zu verfolgen und zu bestrafen. Um europaweit gleiche Wettbewerbsbedingungen zu gewährleisten und Unternehmen vor existenzbedrohenden

[2] Im Februar 2020 veröffentlichte der EDSA die Beiträge der EU-Datenschutzbehörden zu einem Fragebogen zur Bewertung der DSGVO, in dem 14 Datenschutzbehörden erklärten, dass sie nicht angemessen ausgestattet seien, um zu den Kooperations- und Kohärenzmechanismen beizutragen. Siehe auch: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

Wartezeiten zu bewahren, sollte jede Datenschutzbehörde über eine ausreichende und angemessene personelle, technische und finanzielle Ausstattung, Räumlichkeiten und Infrastruktur verfügen. Außerdem sollten sie ihre Ressourcen auf wichtige Fälle konzentrieren.

Kommt es zu einem Ermittlungsverfahren, sind die rechtlichen Möglichkeiten und Dimensionen der **Strafen jedoch nicht angemessen und rechtsstaatlich bedenklich**. Die Eingriffsbefugnisse der DSB sind nämlich im Vergleich zu anderen Ordnungswidrigkeiten beispiellos. Sie übersteigen sogar die höchstmöglichen Bußgelder im Strafrecht. Darüber hinaus haben die Datenschutzbehörden **Zugang zu allen Informationen und personenbezogenen Daten** sowie zu allen Räumlichkeiten und Datenverarbeitungsanlagen des für die Verarbeitung Verantwortlichen, was es ihnen ermöglicht, **Unternehmen effektiv stillzulegen**, indem sie die Datenverarbeitung verbieten oder langwierige Ermittlungs- und Compliance-Verfahren auferlegen, was für ein Unternehmen einen Nachteil auf dem Markt bedeuten kann. All diese Befugnisse sind kaum gesetzlich begrenzt oder spezifiziert, während vieles nach dem Ermessen der Verwaltung entschieden wird. Außerdem ist die Leitung einer Datenschutzbehörde eine politische Position, die mit einer Person mit politischem Hintergrund besetzt ist. Diese Person ist jedoch oft ohne jegliche Erfahrung im Datenschutz, da **keine spezifischen Kenntnisse** wie in vielen anderen öffentlichen Positionen gefordert werden. Vor diesem Hintergrund ist es umso erstaunlicher, dass DSB weder einer fachlichen noch einer rechtlichen Aufsicht unterliegen, wie es bei Regulierungsbehörden üblich ist. Stattdessen genießen sie **völlige Unabhängigkeit**. Ähnliches gilt für den EDSA, da seine Stellungnahmen erheblichen Einfluss auf die europäische Datenverarbeitung haben, ohne demokratisch rechenschaftspflichtig und legitimiert zu sein. Obwohl die Stellungnahmen des EDSA nicht bindend sind, haben sie den Zweck, eine harmonisierte Auslegung der DSGVO in der gesamten EU zu steuern, und werden oft direkt in den Richtlinien der Datenschutzbehörden zitiert, wodurch sie de facto zu Gesetzen werden, die von den Datenschutzbehörden durchgesetzt werden. Daher ist es höchst bedenklich, dass es derzeit **keine Möglichkeit gibt, gegen eine EDSA-Stellungnahme vorzugehen**, da sie nicht bindend ist.

Angetrieben von politischen Meinungen und Motiven einiger Mitarbeiter veröffentlichten der EDSA und mehrere Datenschutzbehörden einige **sehr strenge Auslegungen** der DSGVO, die eindeutig **gegen den Willen des Gesetzgebers** und gegen den Grundsatz der Neutralität verstießen. Auffallend ist die Tatsache, dass der EDSA zwar theoretisch alle Interessengruppen für die Ausarbeitung seiner Stellungnahme konsultieren sollte, in der Praxis aber **sehr wenig auf die Interessengruppen** aus Forschung, Industrie oder Zivilgesellschaft und deren Forderungen nach

einer ausgewogenen Auslegung reagiert hat, selten deren Feedback berücksichtigt oder eine Konsultation durchgeführt hat, nachdem er die Stellungnahme bereits verabschiedet hatte. Um den EDSA, der sich als einseitig erwiesen hat, auszugleichen, sollte ein **European Data Innovation Board** eingerichtet werden. Es sollte mit Vertretern aus Forschung und Industrie besetzt sein und einen gesetzlichen Auftrag haben, Kommentare, Interpretationen und Richtlinien herauszugeben, wie das Grundrecht auf Privatsphäre mit den Rechten auf Leben, Freiheit, Sicherheit und der Freiheit, in Europa Geschäfte zu machen, abgewogen werden kann.
Außerdem besteht bei einigen Datenschutzbehörden die Tendenz, Leitlinien und Konsultationen zu ähnlichen Themen (z. B. zu Cookies) separat zu veröffentlichen, was kein innovationsförderndes Umfeld schafft. Bis Gerichte diese Auslegungen zurückweisen können, haben Unternehmen die kritisierte Verarbeitung personenbezogener Daten bereits angepasst oder sogar eingestellt. In der Praxis halten sich die Datenschutzbehörden oft auch nicht an das Gesetz, das regelt, unter welchen Bedingungen sich öffentliche Stellen äußern dürfen. Es gibt viele Fälle, in denen Unternehmen, die zu einer Geldstrafe verurteilt wurden, **namentlich angeprangert** wurden. Einige Unternehmen wurden sogar öffentlich abgemahnt, ohne dass ihnen ein Verstoß gegen die Datenschutzbestimmungen nachgewiesen werden konnte.

Besonders wenn es um KMU und Start-ups geht oder wenn ein Verstoß zum ersten Mal auftritt, sollten die Datenschutzbehörden **serviceorientierter arbeiten** und **Warnungen, Erklärungen und Hilfe** anbieten, wie man DSGVO-konform wird. Ebenso ist nicht jeder Vorfall ein Datenschutzverstoß. Aus Angst vor Sanktionen neigen Unternehmen dazu, die Meldevorschriften streng auszulegen und „zu viel zu melden" (wodurch die Ressourcen der Datenschutzbehörden weiter belastet werden). Problematisch ist auch, dass Bußgelder von DSB für Datenschutzverletzungen immer häufiger mit **zivilrechtlichen Schadensersatzansprüchen** einhergehen, insbesondere in Form von Sammelklagen. Nicht jede kleine Datenschutzverletzung sollte ein Ziel für eine Schadensersatzklage sein, insbesondere dann nicht, wenn diese Klagen von kommerziellen Akteuren geführt werden, die hoffen, auf dem Rücken der betroffenen Personen Profit zu machen. Der Anwendungsbereich von Art. 82 DSGVO hat sich als zu vage erwiesen.

Die Rollen und Pflichten der Datenschutzbehörden, ihre mangelnden Ressourcen, um Unternehmen anzuleiten, und die komplexen Verfahren erschweren die

Zusammenarbeit zwischen Datenschutzbehörden und der Industrie. Erstens bedeutet die **Doppelrolle der Datenschutzbehörden als Durchsetzer und Berater** der Industrie, dass sie mit Ermittlungs- und Korrekturbefugnissen ausgestattet sind, um die DSGVO durchzusetzen, während sie gleichzeitig eine beratende Funktion haben. Audits oder Bewertungen, die als Anleitung und Unterstützung gedacht sind, können stattdessen zur Identifizierung von Fällen der Nichteinhaltung führen, gefolgt von Durchsetzungsmaßnahmen, die wahrscheinlich zur Verhängung von Geldstrafen führen. Dies kann das Vertrauen in die Beziehung zwischen Datenschutzbehörden und Unternehmen in Frage stellen. Zweitens sind unterfinanzierte Datenschutzbehörden möglicherweise nicht in der Lage, effiziente Beratung zu leisten, da sie ihre Ressourcen vorrangig auf die Bearbeitung von Beschwerden und weniger auf den konstruktiven Dialog mit Unternehmen konzentrieren könnten. Infolgedessen kann es bei Unternehmen, die nicht schnell Antworten erhalten, zu Verzögerungen in den Entwicklungszyklen kommen.

VI. Fragmentierung

Zunächst steht die Europäische Union, wie bei vielen anderen Gesetzgebungen auch, vor Herausforderungen aufgrund von **Sprachbarrieren, kulturellen Unterschieden, veralteten Informationsaustauschsystemen, divergierenden nationalen Rechtssystemen und unterschiedlichen Methoden**, z. B. für Datenschutz-Folgenabschätzungen in den Mitgliedstaaten.

Bei der weiteren Spezifizierung der Anwendung der DSGVO in bestimmten Bereichen (z. B. das Einwilligungsalter von Kindern für Online-Dienste) haben viele Mitgliedstaaten in ihren nationalen sektoralen Gesetzen **rechtliche Anforderungen zusätzlich zu den Vorschriften der DSGVO** eingeführt. Dies steht einer echten Harmonisierung der Datenschutzvorschriften im Wege. Es führt auch zu noch mehr Rechtsunsicherheit, insbesondere für Unternehmen, die Produkte und Dienstleistungen in verschiedenen Mitgliedstaaten anbieten.

Neben der **unterschiedlichen Auslegung** der Gesetze unterscheiden sich auch die **Durchsetzung und die Höhe der verhängten Bußgelder** erheblich zwischen den Mitgliedsstaaten. Diese Situation ermöglicht es Unternehmen, sich in den Ländern niederzulassen, die die nachlässigste DSGVO-Umsetzung in Kombination mit den niedrigsten Bußgeldern haben.

Die **Bußgelder** aufgrund von DSGVO-Verstößen sind oft **nicht angemessen**. Während die gegen einige multinationale Unternehmen verhängten Bußgelder manchmal zu niedrig sind, um als wirksame Abschreckung zu dienen, kann bereits die Androhung eines Bußgeldes für ein KMU existenziell sein und es dazu zwingen, seine Geschäftsidee aufzugeben. Was fehlt, sind klare Kriterien, um zu definieren, wann ein Verstoß stattgefunden hat und wie die genaue Höhe des Bußgeldes festgelegt werden kann.

Viele Bestimmungen der DSGVO (z.B. Art. 15, 20, 24, 25, 26, 32 DSGVO) genügen nicht den Anforderungen an ausreichende Klarheit und Bestimmtheit und lassen verschiedene **widersprüchliche Interpretationen** zu, die zu **Rechtsunsicherheit** führen. Dies ist ein erheblicher Nachteil nicht nur für den Rechtsanwender, sondern auch für die Aufsichtsbehörden. In anderen Fällen wurden die **Begriffe nicht ausreichend harmonisiert**. Nachfolgend einige der dringlichsten Beispiele:

- Es gibt sehr unterschiedliche Auslegungen der nationalen Datenschutzbehörden darüber, was eine gültige „Einwilligung" ist, wobei diese zum Teil stark von europäischen Rechtstraditionen und zivilrechtlichen Grundsätzen abweichen.
- Einige Datenschutzbehörden legen den Begriff des „berechtigten Interesses" sehr restriktiv aus und schließen beispielsweise die Datenverarbeitung für rein kommerzielle Interessen aus (obwohl Erwägungsgrund 47 der DSGVO Direktmarketing als Beispiel für eine gültige Verwendung des Begriffs „berechtigtes Interesse" aufführt[3]) oder behindern die Videoüberwachung von Einzelhändlern zum Schutz der Kunden vor Taschendiebstahl.
- Die Leitlinien der Datenschutzbehörde zu Cookies und Datenschutz-Folgenabschätzungen sind ebenfalls nicht einheitlich, was dazu führt, dass Unternehmen in den einzelnen Mitgliedstaaten unterschiedliche Dokumentationspflichten haben.
- Die Fragmentierung zeigt sich auch in der fehlenden technischen Standardisierung der Rechte der betroffenen Person (z.B. durch die Bereitstellung von APIs auf Basis von Art. 21 (5) DSGVO), bei den Verpflichtungen zu Datenschutzrichtlinien für Websites oder bei den Formalitäten für Formulare zur Meldung von Datenschutzverletzungen.

[3] In diesem Fall wurde die Auslegung des niederländischen Datenschutzgesetzes später von einem niederländischen Gericht aufgehoben und für ungültig erklärt. In seinem Urteil erklärte das Gericht, dass das Vorliegen eines kommerziellen Interesses nicht automatisch ein berechtigtes Interesse als rechtmäßigen Verarbeitungsgrund ausschließt.

VII. Schwachstellen und Lücken im Gesetzestext

Anonymisierung

Obwohl die Depersonalisierung von personenbezogenen Daten in großer Zahl ein entscheidendes Mittel sein könnte, um sowohl den Datenschutz als auch eine florierende Datenwirtschaft zu gewährleisten, bietet die DSGVO dazu nicht viel Anleitung. Erwägungsgrund 26 besagt lediglich, dass das Gesetz nicht auf anonymisierte Daten anwendbar ist[4]. Weitere gesetzgeberische Klarstellungen sind erforderlich:

- Es bedarf einheitlicher Definitionen von absoluter und relativer Anonymisierung und einer weiteren Abgrenzung zur Pseudonymisierung. Es sollte auch klargestellt werden, dass das Gesetz für einen DSGVO-konformen Depersonalisierungsprozess nur eine relative Anonymisierung verlangt, wie es bereits in Erwägungsgrund 26 steht.
- Die Definition des Begriffs "personenbezogene Daten" in Art. 4(1) DSGVO ist nach wie vor extrem weit gefasst und unklar, unter welchen Bedingungen Datensätze, die personenbezogene Daten enthalten, als anonymisiert gelten können.
- Einige Entscheidungsträger und Datenschutzbehörden betrachten den Prozess der Anonymisierung personenbezogener Daten auch als „Verarbeitung" im Sinne von Art. 4(2) DSGVO[5]. Dies würde bedeuten, dass auch für die Anonymisierung eine Rechtsgrundlage erforderlich wäre, was den gesamten Prozess unnötig verkomplizieren würde.
- Die Anonymisierung ist zudem eine zweckändernde Weiterverarbeitung. Das bedeutet, dass die Verarbeitung gemäß Art. 6(4) DSGVO mit dem ursprünglichen Zweck, basierend auf der ursprünglichen Rechtsgrundlage, vereinbar sein muss.
- Zusätzlich zu diesen vier gesetzgeberischen Punkten sollte der EDSA auch praktische Leitlinien herausgeben, welche spezifischen standardisierten

[4] Insbesondere die fehlende Spezifizierung im Gesetz sowie die fehlende Anleitung zum folgenden Teil in Erwägungsgrund 26 führt in der Praxis zu Rechtsunsicherheit: "Um festzustellen, ob eine natürliche Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die nach vernünftigem Ermessen verwendet werden können."

[5] Dieses Verständnis von Erwägungsgrund 26 hat beispielsweise der deutsche Bundesdatenschutzbeauftragte in seinem jüngsten Positionspapier zur Anonymisierung in der DSGVO vom 26. Juni 2020 dargelegt.

Anonymisierungsmethoden verwendet werden können, um Daten nach der DSGVO zu anonymisieren. Die WP216 der Artikel-29-Datenschutzgruppe hat sich in der Praxis als unzureichend erwiesen. Spezifische Anwendungsfälle und relevante Situationen für verschiedene Arten von Datenverarbeitungen und eine Checkliste mit allen Anforderungen, die erfüllt werden müssen, um Daten zu anonymisieren, sollten enthalten sein. Regelmäßige Aktualisierungen scheinen notwendig zu sein, da die technischen Entwicklungen in diesem Bereich rasant sind.

Gemischte Daten

Aufgrund der großen Rechtsunsicherheit, ob personenbezogene Daten ausreichend depersonalisiert sind, entscheiden sich Unternehmen oft dafür, keine ihrer kommerziellen Datensätze zu teilen, da sie gemischte Daten enthalten. Die DSGVO legt fest, dass ihre Bestimmungen gelten, wenn personenbezogene und nicht-personenbezogene Daten „untrennbar miteinander verbunden" sind. Trotz neuer Leitlinien ist es in der Praxis jedoch sehr schwierig, klar zwischen personenbezogenen und nicht-personenbezogenen Daten zu unterscheiden oder beide voneinander zu trennen.

Sekundärnutzung

Gerade in Zeiten von COVID-19 und der Verwendung von Daten im Gesundheitswesen, aber auch für Bereiche der Cybersicherheit und der Künstlichen Intelligenz, erweisen sich Erwägungsgrund 50 und Art 6(4) DSGVO als höchst problematisch. In der Praxis ist oft unklar, ob eine neue Rechtsgrundlage für Fälle erforderlich ist, in denen die betroffene Person zunächst eine Einwilligung erteilt hat, die personenbezogenen Daten aber für einen anderen, mit dem Zweck der ursprünglichen Erhebung vereinbarten Zweck weiterverarbeitet werden. Die enge Auslegung der Einwilligung sowie die vagen Kriterien für die Vereinbarkeitsprüfung (durch den für die Verarbeitung Verantwortlichen) führen zu zahlreichen Situationen, in denen äußerst nützliche Daten für das Wohl der Gesellschaft nicht verwendet werden können. Schlimmer noch, viele Datenschutzbehörden ignorierten sogar die Tatsache, dass eine kompatible Weiterverarbeitung nach den DSGVO-Bestimmungen zulässig ist.

Rechte des Datenschutzobjekts

Mehrere Bestimmungen in Kapitel 3 führten nicht zu einer verbesserten Rechtslage für das Datensubjekt, sondern überfordern den Verantwortlichen. Daher scheinen gesetzliche Änderungen sinnvoll zu sein:

- Die Informationspflicht in Art. 13 und 14 sollte entfallen, wenn sich der Zweck der Verarbeitung personenbezogener Daten

aus dem Erhebungszusammenhang ergibt (z.B. Verteilen von Visitenkarten auf einer Messe oder erstes Telefonat mit Kunden), wenn die betroffene Person bereits über die entsprechenden Informationen verfügt oder wenn das Interesse an der Information nach den Umständen als gering anzusehen ist.

- Die derzeitigen Anforderungen in beiden Artikeln führen zudem zu sehr komplexen und meist unübersichtlichen Datenschutzerklärungen auf Webseiten, die den Betroffenen in Sachen Transparenz und Vertrauen nicht weiterhelfen. Studien zeigen, dass die Bereitschaft, Datenschutzerklärungen zu lesen, seit der Anwendung der DSGVO sinkt[6].
- Es ist auch nicht nachvollziehbar, warum es - insbesondere in risikoarmen Verarbeitungsszenarien oder wenn KMU, Start-ups, nicht-kommerzielle Einrichtungen oder Privatpersonen verantwortlich sind - keine Ausnahmeregelungen (wie in Art. 14(5) DSGVO) in Art. 13 gibt. Insbesondere Informations- und Beratungsstellen (z.B. Sucht, sexuelle Gewalt) und deren Klienten leiden unter dem Fehlen ausreichender Ausnahmen.
- Es fehlen generell Bestimmungen, die die Rechte des für die Verarbeitung Verantwortlichen und Dritter schützen (z. B. Geschäfts- und Betriebsgeheimnisse oder Geheimhaltungspflichten). Ausnahmeregelungen, um einen unverhältnismäßigen Aufwand zu vermeiden, fehlen daher auch in Art. 15 - 18. In der Praxis führt vor allem der große Umfang von Art. 15 (Auskunftsrecht) zu Problemen, da auch bloße Sicherungskopien, personenbezogene Daten, auf die die betroffene Person jederzeit zugreifen kann (z.B. Kontobewegungen, Vertragsdetails) oder personenbezogene Daten, die nicht direkt im System gespeichert sind (z.B. Name der betroffenen Person wurde in einer E-Mail genannt), von diesem Artikel erfasst werden.

Verantwortlicher und Auftragsverarbeiter

In der Praxis führt die unklare Unterscheidung in Kapitel 4 der DSGVO zwischen für die Verarbeitung Verantwortlichem, gemeinsamem

[6] Siehe Eurobarometer vom Mai 2019: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86881

Verantwortlichen und Auftragsverarbeitern zu vielen Problemen.

- Die Definitionen in Art. 4 Nr. 7 und 8 DSGVO sind zu vage und es fehlen Leitlinien mit Fallgruppen.
- In Fällen gemeinsamer Verantwortlichkeit werden die Marktmacht der für die Verarbeitung Verantwortlichen, ihre Fähigkeit, die Verarbeitung zu beeinflussen, und die Vereinbarungen auf praktischer Ebene kaum berücksichtigt, während die rechtlichen Verpflichtungen und Bedingungen für eine solche Zusammenarbeit unklar bleiben. Insbesondere die Marktmacht hat es großen Technologieunternehmen ermöglicht, kleineren Marktteilnehmern die gemeinsame Kontrolle mit kommerziellen Bedingungen aufzuzwingen.
- Bei komplexen Projekten, an denen mehrere Unternehmen beteiligt sind, ist die Abgrenzung zwischen gemeinsamer Kontrolle und Bearbeitung unscharf. Hier fehlen einheitliche Richtlinien. Die vertraglichen Anforderungen an die Verarbeitung in Art. 28(3) DSGVO unterscheiden zudem nicht zwischen den spezifischen Risiken der verschiedenen Arten der Verarbeitung. Ausnahmeregelungen für risikoarme Verarbeitungen (z.B. IT-Wartung) sind in der DSGVO ebenfalls nicht vorgesehen. Die Aufzeichnungspflichten des Auftragsverarbeiters in Art. 30(2) DSGVO erscheinen überflüssig, da die erforderlichen Informationen bereits im Verarbeitungsvertrag enthalten sind.
- Die Anforderungen des Art. 25 DSGVO bleiben unklar und werden der Realität der Softwareentwicklung und digitaler Dienste nicht gerecht. Obwohl diese oft von außereuropäischen Unternehmen entwickelt oder angeboten werden (wie z.B. "Google Analytics"), werden sie kaum von der DSGVO erfasst. Das bedeutet, dass Akteure oft ihre Haftung auf europäische Unternehmen abwälzen, die die Software einsetzen oder die Dienste nutzen, ohne dass sie irgendeine Kontrolle über den Datenschutz durch Design und Voreinstellung haben. Außerdem werden in Erwägungsgrund 78 nur Datenminimierung und Pseudonymisierung als angemessene Mittel genannt. Der Bereich der „Privacy Enhancing Technologies" hat jedoch viele Alternativen geschaffen, von synthetischen/augmentierten Daten über Anonymisierung bis hin zu föderiertem Lernen.

Benachrichtigung bei Datenschutzverletzungen

Die Bestimmungen zu Datenschutzverletzungen lassen viele Fragen offen. Das Verhältnis zwischen der Pflicht zur Meldung von Datenschutzverletzungen und der

Selbstbelastungsfreiheit sowie die Verwendung von Informationen für spätere Ermittlungen bleiben unklar. Weiterhin fehlen in den Artikeln klare materielle Schwellenwerte (z.B. Berufsgeheimnis, Verdacht auf Straftaten, Kreditkartenkonten oder Passwörter), um eine meldepflichtige Verletzung des Schutzes personenbezogener Daten zu bejahen; sie verfolgen keinen risikobasierten Ansatz, indem sie auch bei geringfügigen Verletzungen eine sofortige Meldung verlangen; und sie bieten keine mildernden Umstände als Anreiz für Unternehmen, Datenverletzungen zu melden. Darüber hinaus sind die Formulare für die Meldung von Datenschutzverletzungen, die Art und Weise, wie die Betroffenen zu informieren sind, und die Art und Weise, wie Abhilfe zu schaffen ist, sehr uneinheitlich, was zu unfairen Ergebnissen führt und grenzüberschreitende Fälle sehr schwierig zu lösen macht. Schließlich ist die 72-Stunden-Frist für die Meldung von Datenschutzverletzungen höchst unpraktisch und bindet Ressourcen, die ein Unternehmen für die Analyse und Behebung des Schadens nutzen könnte. Bevor das Unternehmen der Pflicht zur Benachrichtigung der Behörden nachkommt, sollte es die Behebung der Datenverletzung zur Priorität machen.

VIII. Datenschutz im Gesundheitsbereich

Medizinische Diagnosen und Behandlungen sind in hohem Maße von genetischen und medizinischen Faktoren abhängig. So reagieren Frauen beispielsweise anders auf Medikamente als Männer. Vorerkrankungen sowie bestimmte genetische und medizinische Faktoren haben einen großen Einfluss, wenn nicht auf eine Diagnose, so doch auf die Reaktion auf eine Behandlung. Deshalb ist gerade der Gesundheitssektor **auf große Mengen an persönlichen Daten angewiesen**. Ein Medikament oder ein Impfstoff muss an Menschen mit z.B. Vorerkrankungen genauso getestet werden wie an solchen ohne, um seine Sicherheit für alle zu prüfen. Da die meisten Gesundheitsdaten pseudonymisiert sind, wurden mit der DSGVO viele zusätzliche rechtliche Schritte, Prüfungen sowie Zeit- und Zweckbeschränkungen eingeführt. Die Auswirkungen liegen auf der Hand: Der gesamte Gesundheitssektor leidet unter **Rechtsunsicherheit** und wird in seiner wichtigen Arbeit stark eingeschränkt. Die sinnvollsten Lösungen wären, ein **eigenes neues Kapitel zum Thema Gesundheit** in der DSGVO zu schaffen oder die medizinische Forschung sowie die Angehörigen der Heil- und Gesundheitsberufe komplett von der DSGVO auszunehmen und ein **sektorspezifisches Datenschutzgesetz** für diesen Bereich zu erarbeiten. Es scheint ein ziemlich unmögliches Unterfangen zu sein, alle Probleme - von denen einige im Folgenden aufgeführt sind - zu lösen und gleichzeitig die Anwendbarkeit der DSGVO zu gewährleisten.

Während Art. 9(1) die Verarbeitung besonderer Datenkategorien, einschließlich Gesundheitsdaten, verbietet, sind die **Ausnahmeklauseln** in Absatz (2h) und (2i) sehr vage und überlassen die genaue Ausgestaltung den Mitgliedsstaaten. Das Ergebnis ist eine **rechtliche Zersplitterung** in der EU. Forscher und Krankenhäuser wissen oft nicht, welche Regeln in einem Mitgliedsstaat gelten, insbesondere wenn dieser ein föderales System hat.

Die Verarbeitung von Gesundheitsdaten - basierend auf einem Vertragsverhältnis schafft viele neue Probleme für die Ärzte, da sie nach Art. 9(2) in den meisten Fällen eine **zusätzliche Einwilligung** der betroffenen Person einholen müssen. Neue Forschungsprojekte werden dadurch regelmäßig verzögert, da erst zusätzliche vertragliche Regelungen ausgehandelt werden müssen. Da Forscher dies nicht selbst tun können, müssen sie (oft teure) Anwälte beauftragen, um die notwendigen Absicherungen zu platzieren.

Die **rechtliche Situation** für eine wissenschaftliche Entdeckung (mit persönlichen Daten), die Auswirkungen auf eine andere Krankheit, ein

Medikament oder eine Behandlung haben kann, ist unsicher. Die ursprüngliche Einwilligung wurde nicht für diesen Zweck erteilt und kann daher nicht erneut als Rechtsgrundlage verwendet werden. Müssen Forscher wegen der unvorhergesehenen Verwendung von personenbezogenen Daten erneut die Zustimmung aller Anbieter einholen oder können sie das öffentliche oder berechtigte Interesse als Rechtsgrundlage verwenden? Was passiert mit Daten, die vor der DSGVO erhoben wurden; insbesondere, wenn die Forscher nicht in der Lage sind, die betroffenen Patienten zurückzuverfolgen?

An medizinischen Forschungsprojekten ist der Sponsor der Studie (z. B. ein Unternehmen) beteiligt, der für die Überwachung und Verwaltung der Studie verantwortlich ist. Aber auch andere Beteiligte (Kollaborateure) sowie externe Kliniken wickeln die klinischen Studien vor Ort ab. In der Praxis bleibt oft unklar, welcher Akteur in diesem Netzwerk für die Vereinbarungen zur gemeinsamen Datennutzung verantwortlich ist und in welcher der zahlreichen parallelen vertraglichen Vereinbarungen zwischen diesen Akteuren er zu verorten ist.

Daten von Patienten mit einer chronischen Erkrankung, die ein Medizinprodukt besitzen, werden nicht automatisch pseudonymisiert. Allerdings bitten immer mehr Krankenhäuser ihre Patienten, die Daten zu pseudonymisieren, um einen Verstoß gegen die DSGVO auszuschließen. Viele Patienten wären jedoch bereit, ihre persönlichen Daten ohne jegliche Depersonalisierung zur Verfügung zu stellen, wenn dies für sie oder die Patientengemeinschaft von Vorteil ist. Andererseits ist dem Patienten nicht immer klar, auf welcher Datenbereitstellungsvereinbarung das Medizinprodukt verwendet wird und ob die personenbezogenen Daten kommerziell und/oder mit Drittländern geteilt werden. Dieser Punkt ist insbesondere dann relevant, wenn außereuropäische Cloud-Anbieter genutzt werden, die wiederum mit weiteren Drittanbietern kooperieren.

Schließlich ist auch rechtlich unklar, ob gewinnorientierte Unternehmen, die wichtige wissenschaftliche Forschung betreiben, unter die Kategorie „wissenschaftliche Forschung" im Sinne von Erwägungsgrund 159 DSGVO fallen.

IX. Praktische Probleme

Zertifikate

Obwohl die DSGVO den Rahmen für Unternehmen bietet, ihre DSGVO-Konformität nachzuweisen (Art. 42/43), gibt es noch kein allgemein akzeptiertes Zertifikat. Auch Verhaltenskodizes als alternative Option werden aufgrund ihres langwierigen und kostspieligen Annahmeverfahrens sowie des höchst ungewissen Ausgangs eines solchen Unterfangens nicht häufig genutzt. Während Unternehmen ihre hohen Datenschutzstandards kaum als Wettbewerbsvorteil nutzen können, sind Kunden gezwungen, umfangreiche Überprüfungen auf eigene Faust vorzunehmen und fallen häufig auf Betrüger herein. Eine vertrauenswürdige Zertifizierung, basierend auf internationalen Zertifizierungsstandards (ISO 17024), sollte auch die Qualifikation des DSB umfassen.

Ausbildung und Rolle der DSB

Es fehlt eine standardisierte Grundausbildung, die mit einer zentralen Prüfung abschließt. Auch gibt es nur begrenzte Voraussetzungen, um Datenschutzbeauftragter in einem Unternehmen zu werden, sowie zu vage Klarstellungen in Art 39 DSGVO zu den genauen Aufgaben und Verantwortlichkeiten des DSB. In der Praxis kann der DSB die Aufgabe der Kontrolle und Pflege der Aufzeichnungen von Verarbeitungstätigkeiten oft nicht erfüllen, da die notwendigen inhaltlichen Aussagen fehlen.

Datenschutz-Folgenabschätzungen (DSFA)

Nach der DSGVO ist es das Unternehmen selbst, das die DSFA durchführt, während die DSB nur das Ergebnis bewertet. Die Unternehmensleitung ist sich oft nicht bewusst, welche Vorteile es hätte, der DSB eine unterstützende Rolle im gesamten Prozess zu geben. Die DSB könnte z. B. helfen, die Risiken für die betroffenen Personen zu bewerten und Hinweise zur Schaffung von Schutzmaßnahmen geben.

Werbung

Die Verarbeitung personenbezogener Daten im Rahmen von Online-Werbung muss sich fast ausschließlich auf die Einwilligung stützen und ignoriert die anderen Rechtsgrundlagen der DSGVO. Dieser Ansatz ignoriert alle Unterscheidungen zwischen Erst- und Drittparteien, die Daten verarbeiten, und deren Beziehung zu den Nutzern (oder deren Fehlen). Darüber hinaus können große Tech-Player, die leichter eine Einwilligung einholen können, oder durch erzwungene gemeinsame Kontrolle mit kleineren, aber verbrauchernahen Partnern, die Daten zum eigenen Wettbewerbsvorteil oft unter einer anderen Rechtsgrundlage weiterverarbeiten.

Datenportabilität im Finanzsektor

Das von der Zahlungsdiensterichtlinie (PSD 2) eingeräumte Recht der Nutzer, zu verlangen, dass ihre bereitgestellten und gespeicherten Daten direkt und in Echtzeit von einem Dateninhaber zu einem anderen übertragen werden, funktioniert in der Praxis noch nicht vollständig. Es fehlen ausreichende technische Schnittstellen, die die Portabilität von Daten in Echtzeit ermöglichen.

Löschung von Daten

Die Forderung, Daten zu „löschen", ist aus praktischer Sicht teilweise unmöglich. Zusammen mit der begrenzten Anleitung, die in Erwägungsgrund 66 und Art. 17 DSGVO gegeben wird, was „angemessen" sein kann, bedeutet dies eine große administrative und operative Belastung für Unternehmen, die entweder nicht in der Lage sind, personenbezogene Daten zu löschen, weil dies ihre Systeme "kaputt" machen würde, oder die unverhältnismäßig teure neue Systeme aufbauen müssen, um irgendeine Art von Anonymisierung zu ermöglichen.

Unfairer Wettbewerbsvorteil

Bestimmte Unternehmen, die im europäischen Binnenmarkt tätig sind, nutzen die Tatsache aus, dass einige Drittländer kein hohes Datenschutzniveau haben. Sie bauen in diesen Ländern Forschungszentren auf, um ihre KI zu trainieren oder ihre neuen datengesteuerten Geschäftsmodelle ohne Einschränkungen zu testen. Dadurch sind sie in der Lage, technisch stark voranzukommen und diese Technologien schließlich in der EU einzuführen, um bedeutende Marktanteile im Binnenmarkt zu erobern.

Missbrauch des Rechts auf Information

Einige professionelle Anbieter verfolgen ihr kommerzielles Eigeninteresse, indem sie Anreize für Betroffene schaffen, ihr Auskunftsrecht gegen unerwünschte Konkurrenten auszuüben. Diese Form der Selbstjustiz ist aufgrund der fehlenden formalen Voraussetzungen für die Ausübung dieses Rechts (z. B. über Social-Media-Plattformen) sowie des unbestimmten Anwendungsbereichs (z. B. unklar, ob handschriftliche Notizen eingeschlossen sind) möglich.

X. Internationale personenbezogene Datenströme

Um ihre DSGVO-Compliance zu zeigen, geben viele Unternehmen an, dass personenbezogene Daten nicht außerhalb der EU übertragen werden, obwohl ihr Datenverkehr durch Drittländer läuft oder in globalen Cloud-Diensten gespeichert wird. Das **Verstehen und Überwachen** solcher Prozesse ist vor allem für KMUs sehr kompliziert und teuer. Erschwerend kommt hinzu, dass die Datenschutzbehörden argumentieren, dass der **risikobasierte Ansatz** nicht auf internationale personenbezogene Datenströme anwendbar ist (Kapitel 5), sowie das jüngste **Schrems-II-Urteil** des EuGHs. In der Praxis bedeutet diese umstrittene Auslegung, dass Unternehmen bei den meisten Übermittlungen personenbezogener Daten in Drittländer eine umfassende Risikoanalyse und Angemessenheitsprüfung durchführen müssen[7].

Angemessenheitsbeschlüsse wären ein hervorragendes Mittel zur Vereinfachung internationaler Datenströme, da sie Datentransfers nicht an zusätzliche Bedingungen oder Genehmigungen knüpfen. Dennoch hat die Europäische Union sie bisher nur mit zwölf Ländern abgeschlossen, obwohl viele weitere Drittländer kürzlich neue Datenschutzgesetze mit ähnlichen Regeln und Prinzipien wie die DSGVO verabschiedet haben. Dies liegt auch an dem langwierigen und komplexen Prozess der Angemessenheitsprüfungen und der anschließenden Verhandlungen, der Länder davon abhalten könnte, überhaupt ein Beitrittskandidat werden zu wollen. Ein weiteres Problem ist die **Inkonsistenz**, wenn es um die Bewertungen oder die Überprüfungen geht. Während die EU nach Bekanntwerden von nicht-DSGVO-konformer Datenverarbeitung in einigen Ländern nicht reagierte, wurden andere mit ähnlichen oder sogar weniger problematischen Handlungen von Datenschutzbehörden und Politikern öffentlich an den Pranger gestellt.

Transatlantische Datentransfers sind entscheidend für viele Unternehmen sowie für digitale Dienste und Anwendungen, die Menschen täglich nutzen. Angesichts **fehlender wettbewerbsfähiger Alternativen** aus der EU zu dominanten Diensten aus Drittländern (z.B. Google Ads, YouTube Video Hosting) hat das Schrems II-Urteil des EuGHs **große Unsicherheit über solche Transfers** gebracht und viele europäische KMUs, Start-ups, Universitäten und Forschungsinstitute, die sich auf diese spezielle Angemessenheitsentscheidung verlassen hatten, in einen rechtlichen Schwebezustand versetzt. Auch europäische multinationale Unternehmen leiden unter der erhöhten Unsicherheit in Bezug

[7] Diese sind jedoch nicht erforderlich, wenn ein Angemessenheitsbeschluss vorliegt oder eine Ausnahmeregelung auf der Grundlage von Art. 49 DSGVO gilt.

auf Transfers mit ihren US-Tochtergesellschaften und Geschäftspartnern.

In Ermangelung von Angemessenheitsentscheidungen sind **Standardvertragsklauseln** (SCC) das am weitesten verbreitete Instrument für internationale Datenübermittlungen. Die EDSA-Empfehlungen zu ergänzenden Maßnahmen missachten jedoch den risikobasierten Ansatz der DSGVO für Sicherheitsmaßnahmen (Art. 25(1) und 32(1) DSGVO) und verlangen **Verschlüsselung und vollständige Unlesbarkeit** personenbezogener Daten auf jeder Stufe der Datenverarbeitung außerhalb der EU. In Kombination mit der Schrems II-Entscheidung des EuGHs sind Unternehmen nun verpflichtet, für jeden ihrer Datentransfers eine „**Mini-Angemessenheitsprüfung**" vorzunehmen (da sie die Gesetze des Ziellandes selbst bewerten und auf dieser Grundlage entscheiden müssen, welche Schutzmaßnahmen am besten geeignet wären). Dies ist in der Praxis einfach nicht machbar.

Verhaltenskodizes, Binding Corporate Rules (BCR) und Zertifizierungsmechanismen[8] werden kaum als mögliche Alternativen zu Angemessenheitsentscheidungen genutzt. Im Falle von Codes of Conducts und Zertifikaten sind **fehlende Leitlinien** und **politische Motive** als Hauptgründe zu nennen. Der EDPB hat bisher noch nicht einmal einen genehmigt. Bei BCRs ist die Messlatte für die Erstellung und Umsetzung - wie sie in den Arbeitspapieren der Datenschutzbehörden festgelegt ist - zu streng, komplex und eng für die Realitäten einer digitalen Wirtschaft.

Das Verständnis der Ausnahmeregelungen in Art 49 DSGVO ist ein weiterer Fall, in dem die **Auslegung des EDSA über den Willen des Gesetzgebers hinausgeht**. So erlaubt Art. 49(1a) Datenübermittlungen auf der Grundlage der ausdrücklichen Einwilligung der betroffenen Person, nachdem sie über die möglichen Risiken solcher Übermittlungen in Drittländer mit unzureichendem Datenschutzniveau informiert wurde. Dem Ausnahmecharakter dieser Vorschrift wird bereits durch die erhöhten Informationspflichten gegenüber der Einwilligung nach Art. 6 und 9 DSGVO Rechnung getragen. Obwohl es weder im Wortlaut des Art. 49 Abs. 1a noch in den zugehörigen Erwägungsgründen eine Einschränkung der Einwilligungsmöglichkeit gibt,

[8] Ausreichend für internationale Übermittlungen, wenn sie durch verbindliche und durchsetzbare Verpflichtungen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters im Drittland ergänzt werden, die garantieren, dass sie die entsprechenden Schutzmaßnahmen anwenden werden.

lassen die EDSA-Leitlinien eine Einwilligung nur in Ausnahmefällen zu.