Wie die EU ihre Digitalstrategie vorantreibt

Im Regulierungsrausch

Nationale Regierungen müssen sich daran gewöhnen: Relevante Gesetze werden zunehmend in Brüssel geschrieben. Gerade in der Digitalpolitik schleudert die Kommission einen Verordnungsvorschlag nach dem anderen heraus, um Versäumnisse aufzuholen und Zukunftstechnologien frühzeitig zu regulieren. Das kl…

Wie die EU ihre Digitalstrategie vorantreibt

Nationale Regierungen müssen sich daran gewöhnen: Relevante Gesetze werden zunehmend in Brüssel geschrieben. Gerade in der Digitalpolitik schleudert die Kommission einen Verordnungsvorschlag nach dem anderen heraus, um Versäumnisse

aufzuholen und Zukunftstechnologien frühzeitig zu regulieren. Das klappt manchmal, ist aber auch oft widersprüchlich.

Von Falk Steiner

kompakt

- Die EU zieht im digitalen Bereich immer mehr Kompetenzen an sich und übernimmt auch Aufsichtsfunktionen.
- Insbesondere zu den USA ist die Beziehung kompliziert, weil sich die großen Tech-Konzerne nur ungern an die Regeln der lukrativen europäischen Märkte anpassen.
- Einige Pläne, vor allem der CSAM-Act, schießen deutlich über das Ziel hinaus und werden 2023 für heftige Konflikte zwischen den Mitgliedsstaaten sorgen.

Das dritte Jahrzehnt des 21. Jahrhunderts müsse zur „digitalen Dekade“ werden. Dies hatte EU-Kommissionspräsidentin Ursula von der Leyen in ihrer „Rede zur Lage der Europäischen Union“ im September 2020 angekündigt – und direkt Taten folgen lassen. Bereits ein Jahr später war ein Konzept erkennbar, inklusive neu entwickelter Instrumente, um den digitalen Fortschritt zu messen.

Beispielsweise hat die Kommission den „Index für die digitale Wirtschaft und Gesellschaft“ (DESI) geschaffen, der Fortschritte bei den Zielmarken für 2030 in jedem EU-Mitgliedsstand abbildet und damit Wettbewerb der Staaten untereinander anfacht. In einem jährlichen Bericht über den „Stand der digitalen Dekade“ bewertet die Kommission außerdem die Fortschritte, beispielsweise bei der Digitalisierung von Verwaltungsakten.

Vor allem aber hat die Kommission, die als einziges EU-Organ Gesetze entwerfen und vorschlagen darf, ein wahres Feuerwerk an neuen Regelwerken fürs Digitale auf die Schiene gesetzt [1]. Einige der Gesetzentwürfe stehen bereits davor, umgesetzt

zu werden, bei anderen suchen Kommission, EU-Parlament und Europäischer Rat noch Kompromisse. Und die Lust auf mehr Regulierung ist in Brüssel noch lange nicht verflogen – auch fragwürdige Ideen sind auf dem Weg.

Der Brüssel-Effekt

Den Startschuss für die digitale Dekade gab die EU eigentlich schon im Mai 2018: Damals wurde die EU-Datenschutz-Grundverordnung (DSGVO) wirksam. Sie setzt bis heute die Grenzen dafür, wie Unternehmen und Behörden Daten von EU-Bürgern nutzen dürfen – auch für alle nachfolgenden Gesetze. Die EU-Kommission hatte darauf gesetzt, mit der DSGVO nationale Datenschutzgesetze abzulösen und einheitliche Regelungen für den gesamten Binnenmarkt zu schaffen. Dies gilt mittlerweile als Erfolgsmodell, weshalb viele neue Vorhaben als für alle 27 Mitgliedsstaaten verbindliche Verordnungen daherkommen statt als schwächere Richtlinien.

Denn die DSGVO hat gezeigt: Als Absatzmarkt ist die EU mit ihren fast 450 Millionen kaufkräftigen Einwohnern für viele Unternehmen zu wichtig, um sie zu ignorieren – unter anderem auch für Amazon, Apple, Meta, Google und die anderen großen Akteure. Wer in Europa Profite machen will, muss sich ihren Regeln unterwerfen. Ob bei Anschlussbuchsen, Ladegeräten, im Daten-, Wettbewerbs- und Kartellrecht, bei der Plattformgesetzgebung, IT-Sicherheit oder KI-Regulierung: Nationale Regeln sind an vielen Stellen mittlerweile schlicht zu unbedeutend.

Dieser sogenannte Brüssel-Effekt führt dazu, dass Europa immer mehr Kompetenzen an sich zieht – und das mit Unterstützung der Mitgliedstaaten. Die meisten davon haben begriffen, dass sie alleinstehend wenig ausrichten können. Mit der Kraft der EU lockt eine mächtige Verhandlungsposition.

Komplizierte Beziehung

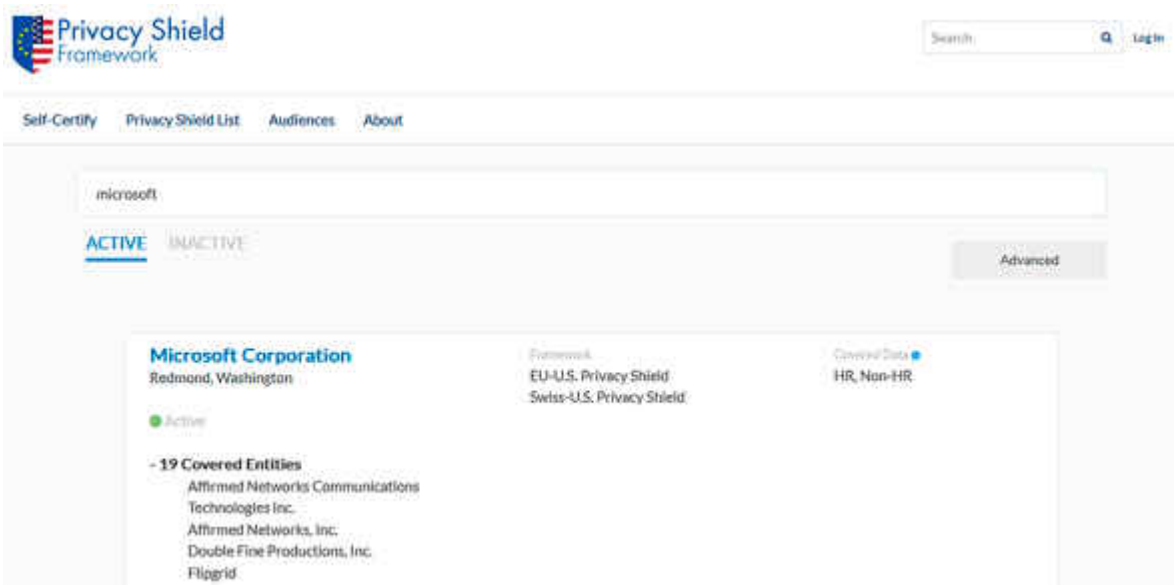
Seit dem Amtsantritt Joe Bidens in den USA und dem Angriff Russlands auf die Ukraine sind weitere Einflüsse auf künftige Regulierung maßgeblich geworden. Vor allem eine Frage treibt Politiker in Brüssel um: Auf wen wird man sich in Zukunft verlassen können? Ihre naheliegende Antwort: Auf als stabil erachtete Demokratien überall in der Welt. Seit Monaten führen EU-Politiker auf vielen Ebenen Gespräche und loten aus, wie sich „die Guten“ dieser Welt untereinander besser vernetzen können, um resilienter gegen böswillige Akteure zu werden.

Handelsabkommen wie CETA mit Kanada, das lange auf Eis lag, sollen nun doch kommen. Vorteilhaft: Auch in den USA gibt es durchaus Lust auf mehr Regulierung. Das ist nicht zuletzt der wachsenden Macht chinesischer Staatsunternehmen, aber auch der einheimischen Kritik am Gebaren einiger US-Konzerne geschuldet.

Aber nicht nur mit Investitionen, auch regulatorisch versucht die EU den Schulterschluss mit den USA. Der eigentliche Lackmustest für die neu belebten transatlantischen Beziehungen steht noch bevor: Im Frühjahr 2023 wird die EU-Kommission über den Transfer personenbezogener Daten in die USA entscheiden. Der erwartete Angemessenheitsbeschluss als Nachfolgeregelung des gescheiterten Privacy Shields ist elementar für Wirtschaft und Nutzer auf beiden Seiten des Atlantiks. Denn wenn keine neue, sichere Rechtsgrundlage geschaffen wird, dürfen viele US-Unternehmen nicht mehr mit den persönlichen Daten von EU-Bürgern arbeiten.

Salesforce, Amazon, Google, Apple, Meta und Microsoft könnten für EU-Daten zur Tabuzone werden. Meta etwa warnt immer wieder davor, dass möglicherweise das EU-Geschäft eingestellt werden müsste – ein Milliardenmarkt würde dem Konzern verloren gehen. Damit das nicht passiert, müssten die USA die Sicherheit von EU-Daten auch gegenüber den US-Nachrichtendiensten verbessern und die Hürden für Zugriffe höher legen. Bislang liegt aber

lediglich ein Vorschlag seitens der US-Regierung vor, der bessere Beschwerdemöglichkeiten vorsieht. Dafür hat US-Präsident Biden Anfang Oktober ein Dekret unterzeichnet, und die EU-Kommission muss nun entscheiden, ob das ausreicht [2].



Auf Eis: Viele US-Konzerne wie Microsoft haben sich zwar selbst für den EU-US-Datentransfer zertifiziert, dürfen sich aber derzeit nicht darauf berufen.

Parallel dazu ist die EU bemüht, sich US-Unternehmen als Spielfeld für die sogenannten Zukunftsmärkte im IT-Sektor zu präsentieren. Das ist kein leichtes Unterfangen, denn gerade hier reguliert sie exzessiv herum: Um die KI-Verordnung (AI-Act), die zumindest besonders kritische KI-Anwendungen mit strikteren Regeln versehen soll, wird seit dem Amtsantritt Ursula von der Leyens 2020 gerungen. Bereits seit Frühjahr 2021 liegen die Vorschläge der Kommission auf dem Tisch. Es geht nur zäh voran: Das Parlament und die Mitgliedstaaten suchen nach Lösungen, während KI-Anwendungen in immer mehr Endgeräte und Anwendungen Einzug halten.

Die strittige Haftung für automatisierte Entscheidungen hat man nun aus der Verordnung herausgenommen: Für KI im engeren Sinne und für den Einsatz im Rahmen marktgängiger Produkte und Dienstleistungen hat die Kommission Ende September neue Regelungsvorschläge unterbreitet. Sie sollen gewährleisten, dass von KI-Entscheidungen unrechtmäßig Benachteiligte ihre

Betroffenheit auch nachweisen können. Bei der begründeten Annahme, dass ein Unternehmen nicht alle Regeln eingehalten hat, soll in einigen Fällen eine „Vermutungsregel“ zugunsten der Betroffenen greifen – für Anwälte könnte da ein weiteres interessantes Geschäftsfeld entstehen.

Alles für die Kinder?

Wo sogenannte KI nach dem Willen der Kommission entgegen aller Bedenken intensiv zum Einsatz kommen soll, ist beim Kampf gegen Missbrauchsdarstellungen von Kindern im Internet. Als Sammelbegriff für dieses Material hat sich auch hierzulande das US-amerikanische Akronym CSAM (Child Sexual Abuse Material) etabliert. Ein im Mai 2022 vorgestellter Gesetzentwurf wird deshalb auch kurz CSAM-Verordnung genannt. Dieses Vorhaben der EU-Innenkommissarin steht inhaltlich stark in der Kritik: Mit dem Gesetz könnten Plattformanbieter wie Apple, Meta, Microsoft und Google dazu verpflichtet werden, automatisiert nach CSAM-Inhalten zu fahnden und mutmaßliche Treffer an ein europäisches Zentrum zur Bekämpfung derartiger Inhalte zu melden. Bislang tun das einige auf Grundlage einer befristeten Erlaubnis bereits heute. Microsoft etwa durchforstet seinen Cloud-Speicher OneDrive auf CSAM-Material hin und sperrt deshalb bisweilen unberechtigt Nutzerkonten [3].

Bürgerrechtler stellen denn auch immer wieder infrage, dass die KI-gestützten Filter CSAM-Abbildungen ausreichend zuverlässig erkennen. Sie sehen die Gefahr von Falschverdächtigungen für größer an als den Nutzen, zumal die Pflicht nach den Plänen der Kommission auch Anbieter verschlüsselter Chats träfe – was zu einem heftigen Eingriff ins Grundrecht auf vertrauliche Kommunikation führen würde [4]. Zudem könnten Strafverfolgungsbehörden laut Kommissionsvorschlag Zugangsanbieter dazu verpflichten, Sperren gegen Websites einzurichten, die nicht genug gegen derartige Inhalte unternehmen. Da der Vorschlag technikneutral

formuliert ist, bezieht er sich nicht nur auf klassische Webseiten: auch Betreiber anderer digitaler Kommunikationswege, etwa Tor-Hoster, könnten davon betroffen sein.

Gegenwind aus Deutschland: Bürgerrechtsorganisationen sammeln gemeinsam auf der Petitionsplattform Campact Unterschriften gegen die geplante CSAM-Verordnung der EU-Kommission.
Das Vorhaben gilt insbesondere in Deutschland als politisch heißes Eisen. In der Bundesregierung hat sich Bundesinnenministerin Nancy Faeser (SPD) grundsätzlich dafür ausgesprochen, die FDP-geführten Digital- und Justizministerien dagegen. Auch im Europaparlament gibt es Widerstand vor allem aus Reihen von FDP, Grünen und Piraten gegen die dort unter dem Begriff Chatkontrolle laufenden Pläne der Kommission. Ob das Parlament den Plan im Gesetzgebungsprozess stoppen oder doch nur abmildern kann, wird sich frühestens 2023 entscheiden.

Sicherheit vor allzu wilden Politikerideen lässt sich nicht verordnen – sehr wohl aber mehr Cybersicherheit für Endgeräte und kritische Infrastruktur: Für beide Themen liegen Vorschläge auf dem Tisch. Die überarbeitete Netzwerk- und Informationssicherheits-Richtlinie NIS ist bereits unter Dach und Fach – die Mitgliedstaaten müssen sie nun in nationales Recht umsetzen. Für Deutschland bringt sie vergleichsweise wenig Änderungen mit sich, dennoch werden 2023 einige Änderungen am IT-Sicherheitsgesetz fällig, um dem genauen

Wortlaut der Revision zu entsprechen.

Anders sieht es mit dem Cyber Resilience Act (CRA) genannten Kommissionsvorschlag vom Herbst 2022 aus – es stehen harte Verhandlungen zwischen Kommission, Parlament und Rat an. Unter anderem geht es um Anforderungen an netzwerkfähige Endgeräte, die nicht von Spezialregeln (etwa für kritische Infrastruktur) umfasst sind. Die Kommission begreift ihren Vorschlag als Antwort etwa auf die Erfahrungen mit dem Mirai-Botnetz, das eine große Zahl nicht gesicherter Webcams für DDoS-Attacken missbrauchte. Mit dem CRA sollen Anbieter von derlei Produkten von Betroffenen in die Pflicht genommen werden können. Halten sie sich nicht an definierte Sicherheitskriterien, haften sie für Schäden – so zumindest der Plan der EU, der im kommenden Jahr verabschiedet werden soll.

Notdürftige Reparaturen

Die Eile, mit der die Kommission einige der Gesetzeswerke derzeit unkoordiniert durch die Institutionen peitscht, führt zu jeder Menge neuer Probleme. Zum Beispiel die Cookie-Problematik: Sie ist bis heute auf EU-Ebene nicht abschließend gelöst – ein echtes Ärgernis für alle Beteiligten, sowohl Unternehmen als auch Verbraucher. Die Kommission hatte geplant, dass die sogenannte E-Privacy-Verordnung eindeutige Regeln vorgibt. Doch die steckt seit über vier Jahren im Prozess fest und wurde von der DSGVO überholt, aus der nun Datenschutzbehörden notgedrungen Regeln ableiten müssen, die nicht drinstehen. Die Gemengelage aus DSGVO und noch gültiger, überalterter E-Privacy-Richtlinie lässt zu viel Interpretationspielraum – eine umfassende Lösung gibt es bislang nicht, nur notdürftige Reparaturen [5].

Gegen irreführende Techniken bei Einwilligungsbannern („Dark Patterns“) hat die EU zuletzt auf Drängen der Europaparlamentarier in den ab April 2024 wirksamen Digital Services Act (DSA) eine Regelung aufgenommen. Das deutsche Digitalministerium erarbeitet parallel auf Grundlage des

deutschen Telemedien-Teledienste-Datenschutzgesetzes (TTDSG) eine Regelung für die zentralisierte Einwilligungsverwaltung. Von der erhofft sich die Ampelregierung, einen großen Knoten in der Debatte um die E-Privacy-Verordnung vorbildhaft durchschlagen zu können, sodass sie irgendwann doch noch kommen kann – mit einem halben Jahrzehnt Verspätung [6].

Viele der zuletzt verabschiedeten oder derzeit im Beratungsprozess steckenden Gesetzgebungen zeigen aber auch, dass die EU dazulernt: Während mit der DSGVO noch versucht wurde, starke und unabhängige Aufsichtsbehörden in den Mitgliedstaaten zu schaffen, plant die Kommission neuere Vorschläge deutlich zentralistischer – und das teils auf ausdrücklichen Wunsch der EU-Staaten, vertreten durch den Europäischen Rat. Denn wenn im Binnenmarkt eine der Behörden nicht mitspielt, entsteht ein exekutiver Flaschenhals, wie die irische Datenschutz-Aufsichtsbehörde DPC mit ihrer laxen Verfolgung von Datenschutzverstößen immer wieder belegt.

Mit dem DSA und dem Digital Markets Act (DMA) hat die EU nun bereits zwei Gesetze verabschiedet, bei denen die Kommission im kommenden Jahr das Aufsichtsregime zusammensetzt. Geplant ist ein Zusammenspiel nationaler und europäischer Aufsichtsbehörden. Für die extrem großen Player am Markt wird die EU-Kommission selbst als Aufsicht fungieren.

Bei der Plattformaufsicht im DSA muss sich insbesondere Deutschland umsortieren. Das umfangreiche Gesetzeswerk verändert unter anderem den Mechanismus, wann und wie Plattformbetreiber im Netz bei rechtswidrigen Inhalten eingreifen müssen. Was in Deutschland bislang über das Netzwerkdurchsetzungsgesetz (NetzDG) geregelt war, wird ab 2024 vom DSA überschrieben. Und der geht in Teilen sogar über das hinaus, was das umstrittene NetzDG vorgibt. Damit werden im kommenden Jahr Änderungen am deutschen Recht nötig, die auch die Nutzer von sozialen Medien betreffen.

Zankapfel Traffic-Kosten

Überrascht waren im Mai 2022 Beobachter und Regulierungsbehörden, als Kommissionsvizepräsidentin Margrete Vestager und der Binnenmarktkommissar Thierry Breton einen neuen Vorstoß unternahmen, einige Anbieter im Netz künftig mehr für die Infrastruktur zahlen zu lassen. Kern der Debatte: Sehr wenige Akteure verursachen einen Großteil des Datenverkehrs im Netz – tragen in der Wahrnehmung der ausbauenden Telekommunikationsunternehmen und der EU-Kommission aber zu wenig der entstehenden Kosten. Insbesondere geht es um den Breitbandausbau in der Fläche, den viele Mitgliedstaaten teuer subventionieren.

Wer soll das bezahlen? Nach Wünschen zweier EU-Kommissare sollen Streaminganbieter wie Netflix an den Kosten für den Glasfaserausbau in der Fläche beteiligt werden. *Bild: Deutsche Telekom*

Zwei unvereinbare Positionen prallen aufeinander: Die Anbieter von Streamingdiensten wie Netflix oder Amazon, deren hochauflösende Videos statistisch große Teile des Verkehrs verursachen, argumentieren damit, dass erst ihre Angebote teure Netzzugänge und den weiteren Ausbau attraktiv machen

würden. Einige der Telekommunikationsanbieter wiederum argumentieren, dass diese ohne die Breitbandzugänge keine Umsätze generieren könnten.

Derzeit überarbeitet die EU die Richtlinie zur Reduzierung der Breitbandkosten. Im Laufe des Jahres 2022 rückten Vestager und Breton von ihrem Plan zwar nicht ab – von einem schnellen Abschluss der Revision ist seit dem Herbst aber nicht mehr die Rede. Stattdessen soll nun in einem geregelten Prozess ermittelt werden, ob tatsächlich finanzielle Ungleichgewichte bestehen und ob sich daraus Handlungsbedarf ergibt. Dieses Vorgehen hatten auch die nationalen Regulierungsbehörden verlangt.

Eine breite Koalition aus Mitgliedstaaten, Verbraucherschützern und Europaparlamentariern hatte davor gewarnt, mit dieser Debatte ein altes Fass wieder aufzumachen: Sollten nicht doch einzelne Dienste gegen Bezahlung bevorzugt werden? Dies würde einen Eingriff in die eigentlich garantierte Netzneutralität bedeuten. Danach sieht es politisch derzeit zumindest nicht aus, doch ein Streit im kommenden Jahr scheint vorprogrammiert.

Bilanz

Im Frühjahr 2024 wählen die EU-Bürger ihr Parlament neu. Offen ist, ob die Von-der-Leyen-Kommission danach die „Digitale Dekade“ weiter umsetzen darf. Einen großen Teil der EU-Digitalstrategie hat sie tatsächlich bereits 2022 auf den Weg gebracht – doch viele der Puzzlestücke sind entweder noch in Arbeit oder werden bereits von neueren Entwicklungen überrollt.

Bei einigen Gesetzgebungsvorhaben ist unklar, ob sie tatsächlich den gewünschten, großen Unterschied machen können. Zugleich lauern auch in den Brüsseler Schubladen der Kommissare immer wieder Ideen, die nicht unbedingt von tieferem Verständnis für die digitalpolitischen Debatten der

vergangenen Jahrzehnte zeugen. Und je stärker der außenpolitische Druck wird, desto größer ist die Gefahr, dass auch sicherheitspolitische Ideen wie die Vorratsdatenspeicherung, automatische Inhaltsfilterungen und Websperren in Brüssel Anklang finden.

Bislang ist die Bilanz der aktuellen EU-Kommission durchwachsen. Während sie mit ihrer KI-Gesetzgebung und im Datenrecht vor vielen anderen Initiativen in der Welt liegt und Standards setzt, bei der IT-Sicherheit endlich auch wenig smarte Endgeräte und deren Hersteller in den Blick nimmt, droht in anderen Bereichen Chaos: Neue Regeln allein machen die digitale Welt noch kein bisschen besser. *(hob@ct.de)*

1. Literatur

2. Joerg Heidrich, Europäisches Trommelfeuer, Wie die EU den Umgang mit Daten revolutionieren will, c’t 18/2022, S. 168
3. Holger Bleich, Privacy Shield 2.0, Neues EU-US-Datentransfer-Abkommen nimmt erste Hürde, c’t 23/2022, S. 32
4. Greta Friedrich, Ein Foto – und alles ist weg, Microsoft sperrt Kunden unangekündigt für immer aus, c’t 24/2022, S. 104
5. Holger Bleich, Massenüberwachung durch die Hintertür, Wie ein EU-Kinderschutzgesetz die Presse- und Meinungsfreiheit massiv einschränken könnte, c’t 13/2022, S. 144
6. Holger Bleich, Löcher stopfen per Verordnung, Die bizarre Tracking-Regulierung in Deutschland, c’t 16/2022, S. 34
7. Holger Bleich, Cookie-Banner adieu?, Eine Rechtsverordnung soll Cookie-Abfragen eindämmen, c’t 20/2022, S. 38

Disable and Remove Google Fonts

Disable and Remove Google Fonts

Von Fonts Plugin

Beschreibung

Verbessert die Leistung der Website, indem Google Fonts deaktiviert werden, die von Themes oder Plugins geladen werden.

While this plugin removes Google Fonts from as many themes and plugins as possible, some require additional steps, we have detailed those here: Remove Google Fonts from WordPress

Plugin-Kompatibilität

Dieses Plugin funktioniert mit allen WordPress-Themes. Speziell getestet wurde es für folgende Themes:

- Twenty Twelve
- Twenty Thirteen
- Twenty Fourteen
- Twenty Fifteen
- Twenty Sixteen
- Twenty Seventeen
- Twenty Nineteen

- Twenty Twenty
- Avada
- Enfold
- Sydney
- Hestia
- Hueman
- Vantage
- ColorMag
- Shapely
- OnePress
- JupiterX
- Storefront
- Divi Extra
- Zerif Lite

Es entfernt auch Google Fonts, die von den folgenden Plugins geladen werden:

- Divi
- MailPoet
- Elementor
- Beaver Builder
- Revolution Slider
- WPBakery (Visual Composer)

Neben der Verbesserung der Ladezeit kann das Entfernen der Google Fonts auch dazu beitragen, die Bestimmungen der DSGVO einzuhalten.

Fehler

Wenn du ein Problem mit diesem Plugin feststellst, melde dich bitte hier!

Mitwirkende

Jeder ist willkommen, zu diesem Plugin beizutragen.

Es gibt verschiedene Arten, wie du dich beteiligen kannst:

1. Melde uns Fehler, die du feststellst.
2. Übersetze „Disable and Remove Google Fonts“ in verschiedene Sprachen
3. Gib uns Feedback und mache Vorschläge für Verbesserungen

FAQ

Wird mein Theme mit „Disable and Remove Google Fonts“ funktionieren?

Das sollte man bei der E-Mail-Signatur beachten

entwickler.de – entwickler.de Deine Wissensplattform

[…]Weiterlesen…

Das sollte man bei der E-Mail-Signatur beachten

Mit freundlichen Grüßen …

von Michael Rohrlich

Auch wenn die „E-Mail-Unterschrift“ eine Art Schattendasein fristet – juristisch gibt es dabei einiges zu beachten.

Für die meisten Privatpersonen ist sie Platzhalter für Grußfloskeln, für Unternehmen stellt sie hingegen oftmals ein Marketinginstrument dar: die E-Mail-Signatur. Hierbei ist nicht die Rede von der digitalen Signatur – also dem Äquivalent zur händischen Unterschrift – die an Dateien oder eben auch an E-Mails angehängt werden kann, um eine rechtsverbindliche Erklärung abzugeben. Stattdessen geht es im folgenden Artikel um den textlichen Abschluss einer E-Mail, in deren Rahmen in aller Regel der Name des Absenders nebst etwaigen Zusatzangaben angegeben wird.

Ausgangssituation

Zwar ist es schon eine ganze Weile in Kraft und doch gibt es nach wie vor zahlreiche Verstöße gegen das Gesetz über elektronische Handels- und Genossenschaftsregister sowie das Unternehmensregister (EHUG) – und das jeden Tag. Denn mit dem Inkrafttreten des EHUG zum 01.01.2007 wurden zahlreiche Gesetze geändert. Zwar ist die Realisierung der für alle kostenfreien Abrufbarkeit von veröffentlichungspflichtigen Unternehmensdaten wie Bilanzen oder Jahresabschlüsse im Internet (www.unternehmensregister.de) das primäre Ziel des EHUG. Allerdings wurden u. a. auch im Handelsgesetzbuch (HGB) diverse Normen neu hinzugefügt, die wiederum für unterschiedliche Unternehmensarten bestimmte Vorschriften enthalten. Unter anderem sind folgende Organisationsformen von Unternehmen betroffen:

- eingetragener Kaufmann (e. K./e. Kfr.)
- offene Handelsgesellschaft (oHG)
- Kommanditgesellschaft (KG)
- Gesellschaft mit beschränkter Haftung (GmbH)

Gegenüber Freiberuflern entfaltet das EHUG hingegen keine Wirkung, sodass sie von den verschiedenen Informationspflichten ausgenommen sind.

Exemplarisch sei an dieser Stelle die entscheidende Vorschrift

für eine GmbH angeführt (§ 35a GmbHG):

„Angaben auf Geschäftsbriefen

(1) Auf allen Geschäftsbriefen gleichviel welcher Form, die an einen bestimmten Empfänger gerichtet werden, müssen die Rechtsform und der Sitz der Gesellschaft, das Registergericht des Sitzes der Gesellschaft und die Nummer, unter der die Gesellschaft in das Handelsregister eingetragen ist, sowie alle Geschäftsführer und, sofern die Gesellschaft einen Aufsichtsrat gebildet und dieser einen Vorsitzenden hat, der Vorsitzende des Aufsichtsrats mit dem Familiennamen und mindestens einem ausgeschriebenen Vornamen angegeben werden. Werden Angaben über das Kapital der Gesellschaft gemacht, so müssen in jedem Falle das Stammkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen angegeben werden.

(2) Der Angaben nach Absatz 1 Satz 1 bedarf es nicht bei Mitteilungen oder Berichten, die im Rahmen einer bestehenden Geschäftsverbindung ergehen und für die üblicherweise Vordrucke verwendet werden, in denen lediglich die im Einzelfall erforderlichen besonderen Angaben eingefügt zu werden brauchen.

(3) Bestellscheine gelten als Geschäftsbriefe im Sinne des Absatzes 1. Absatz 2 ist auf sie nicht anzuwenden.

(4) Auf allen Geschäftsbriefen und Bestellscheinen, die von einer Zweigniederlassung einer Gesellschaft mit beschränkter Haftung mit Sitz im Ausland verwendet werden, müssen das Register, bei dem die Zweigniederlassung geführt wird, und die Nummer des Registereintrags angegeben werden; im Übrigen gelten die Vorschriften der Absätze 1 bis 3 für die Angaben bezüglich der Haupt- und der Zweigniederlassung, soweit nicht das ausländische Recht Abweichungen nötig macht. Befindet sich die ausländische Gesellschaft in Liquidation, so sind auch diese Tatsache sowie alle Liquidatoren anzugeben.“

Diese Regelung ist für ein Gesetz vergleichsweise klar formuliert und verdeutlicht auch dem juristischen Laien, was wobei anzugeben ist und wann Ausnahmen bestehen. Durch das EHUG wurden, wie § 35a GmbHG zeigt, vor allem auch neue Vorschriften im Hinblick auf bestimmte Pflichtinformationen in Geschäftsbriefen eingeführt. Als „Geschäftsbrief“ im Sinne des EHUG werden auch geschäftliche E-Mails eingestuft. Das EHUG basiert auf europäischem Recht, nämlich auf der Publizitätsrichtlinie und auf der Transparenzrichtlinie. Folglich gelten dem EHUG entsprechende Regelungen auch in den anderen Mitgliedsstaaten der Europäischen Union.

Informationspflichten

Die einzelnen Normen, die für die jeweiligen Gesellschaftsformen gelten, bestimmen alle in etwa das Gleiche wie § 35a GmbHG. Den betroffenen Unternehmen werden folgende Pflichtangaben abverlangt:

- Name des eingetragenen Kaufmanns/der eingetragenen Kauffrau bzw. Bezeichnung des Unternehmens inkl. Rechtsformzusatz
- Sitz des eingetragenen Kaufmanns/der eingetragenen Kauffrau bzw. des Unternehmens
- Vor- und Nachnamen des/der Vertretungsberechtigten (z. B. bei einer GmbH der/die Geschäftsführer, bei einer AG der/die Vorstandsvorsitzenden)
- Registerangaben (Registergericht und -nummer)
- bei Bestehen eines Aufsichtsrats zusätzlich die Vor- und Nachnamen des bzw. der Aufsichtsratsvorsitzenden
- wenn Angaben zum Stammkapital gemacht werden sollen, dann muss jedenfalls das Stammkapital aufgeführt werden (z. B. bei einer GmbH oder einer AG)

Über diese verpflichtenden Angaben hinaus können noch weitere Informationen in die E-Mail-Signatur eingebunden werden, zum Beispiel die vollständigen Kontaktdaten, Servicezeiten oder

auch die Bankverbindung.

Praktische Umsetzung

Die aufgezeigten Pflichtinformationen sind auf jeden Fall in geschäftlichen E-Mails zu nennen. An welcher Stelle genau, dazu findet sich im Gesetz kein Anhaltspunkt. In aller Regel werden sie in einem für die E-Mail-Korrespondenz erstellten Briefbogen eingefügt oder eben im Rahmen der E-Mail-Signatur angegeben. Eine musterhaft formulierte, juristisch korrekte E-Mail-Signatur könnte so aussehen:

„Mustermann GmbH
Musterstr. 123
12345 Musterhausen
Geschäftsführer: Max Mustermann
Registerangaben: AG Musterhausen, HRB 12345“

In den meisten Fällen kommen zumindest noch die Kontaktdaten hinzu, wozu aber, wie gesagt, nach dem EHUG keine Pflicht besteht. Alle darüber hinausgehenden Inhalte, insbesondere Werbung, sind hierbei tabu.

Die Pflichtangaben sind idealerweise als Text direkt in der E-Mail zu platzieren. Eine an die E-Mail gehängte „digitale Visitenkarte“ (z. B. VCF-Datei zur Einbindung in Outlook etc.) oder PDF-Datei sollte dagegen vermieden werden, denn dabei ist nicht gewährleistet, dass der Empfänger den E-Mail-Anhang öffnen und die darin enthaltenen Informationen auch zur Kenntnis nehmen kann.

Für etwaige Versäumnisse der Pflichten sind im EHUG generell vergleichsweise empfindliche Sanktionen vorgesehen. Die Höhe der drohenden Geldbuße kann bei 2 500 Euro und höher liegen. Zusätzlich sind – unter Umständen – im Hinblick auf fehlende Pflichtangaben in Geschäftskorrespondenz auch Abmahnungen der Konkurrenz oder von Verbraucherschutzorganisationen wegen eines Wettbewerbsverstoßes möglich.

Geschäftliche Korrespondenz

Letztlich stellt sich noch die Frage, was genau als Geschäftsbrief im Sinne des EHUG zu verstehen ist, denn heutzutage gibt es ja die unterschiedlichsten Formen von Korrespondenz, sowohl inhaltlich als auch in Bezug auf das Übermittlungsmedium. Nach der Vorstellung des Gesetzgebers sind gemäß EHUG alle Briefe, Faxe und E-Mails als Geschäftsbrief anzusehen, die an einen bestimmten, externen Empfänger gerichtet sind. Da möglichst viele geschäftliche Schreiben von den gesetzlichen Informationspflichten erfasst werden sollen, ist der Begriff „Geschäftsbrief“ im Zweifel sehr weit auszulegen, sodass die Eintrittshürde für das EHUG vergleichsweise gering ist.

Ausgenommen sind lediglich interne Kurzmitteilungen, Telefonnotizen oder sonstige Vermerke und vergleichbare Inhalte. Reine Werbeschreiben, die sich an einen nicht individuell bestimmten Personenkreis richten, sollen ebenfalls nicht durch das EHUG erfasst werden.

Im Einzelfall kann es vorkommen, dass sich ein Schriftstück nicht eindeutig einstufen lässt. Im Zweifel gilt: lieber einmal zu viel Angaben geleistet, als einmal zu wenig.

Praxistipp

Unter den Begriff „Geschäftsbrief“ fallen nicht nur, aber insbesondere folgende Schreiben:

- Angebote
- Auftragsbestätigungen
- Empfangsbestätigungen
- Quittungen
- Rechnungen
- Mahnungen

Michael Rohrlich hat als Rechtsanwalt und Fachautor seinen Kanzleisitz in Würselen, Nähe Aachen. Seine beruflichen Schwerpunkte liegen auf dem Gebiet des Onlinerechts sowie des gewerblichen Rechtsschutzes. Weitere Infos zu den Themen aus den Rechtsbeiträgen sowie Gesetze und Gerichtsentscheidungen bietet er unter http://www.rechtssicher.info an.

Links & Literatur

[1] Homepage des Autors: http://www.ra-rohrlich.de

[2] Blog des Autors zum Thema Onlinerecht für Webmaster: http://bit.ly/1W46GHD

[3] Blog des Autors zum Thema Onlinerechte von Verbrauchern: http://www.verbraucherrechte-online.de

[4] Weitergehende Infos zum Thema E-Commerce: http://bit.ly/1jAI1yt

[5] Videotrainings des Autors: http://bit.ly/1OI5ivc

Allgemeine

Informationspflichten für kommerzielle Websites

Allgemeine Informationspflichten für kommerzielle Websites

Eine Online-Shop-Betreiberin/ein Online-Shop-Betreiber muss neben der Informationspflichten, die nur zwischen Unternehmerinnen/Unternehmern und Verbraucherinnen/Verbrauchern zu beachten ist, auch allgemeine Informationen auf der Website zur Verfügung stellen. Diese Informationen müssen leicht und unmittelbar zugänglich sein und betreffen

- den Namen der Online-Shop-Betreiberin/des Online-Shop-Betreibers oder ihre/seine Firma,
- die geografische Anschrift, unter der das Unternehmen niedergelassen ist,
- Angaben, aufgrund deren die Nutzerinnen/Nutzer mit der Online-Shop-Betreiberin/dem Online-Shop-Betreiber rasch und unmittelbar in Verbindung treten können und ihre/seine E-Mail-Adresse,
- wenn vorhanden, die Firmenbuchnummer und das Firmenbuchgericht,
- wenn die Tätigkeit einer behördlichen Aufsicht unterliegt, die zuständige Aufsichtsbehörde,
- bei Online-Shop-Betreiberinnen/Online-Shop-Betreibern, die gewerbe- oder berufsrechtlichen Vorschriften unterliegen, die Kammer, den Berufsverband oder ähnliche Einrichtungen, der die Online-Shop-Betreiberin/der Online-Shop-Betreiber angehört,
- die Berufsbezeichnung und den Mitgliedstaat, in dem die Berufsbezeichnung verliehen worden ist,
- den Hinweis auf die anwendbaren gewerbe- oder

berufsrechtlichen Vorschriften und auch einen Zugang zu diesen Vorschriften,
- wenn vorhanden, Umsatzsteuer-Identifikationsnummer,
- den Standort der Gewerbeberechtigung, wenn das Unternehmen nicht im Firmenbuch eingetragen ist.

Zusätzlich müssen Online-Shop-Betreiberinnen/Online-Shop-Betreiber, deren Unternehmen im Firmenbuch eingetragen ist, weitere Informationspflichten beachten. Diese finden sich unter Geschäftspapiere und Bestellscheine ebenfalls auf USP.gv.at.

Impressum und Offenlegung

Die Online-Shop-Betreiberin/der Online-Shop-Betreiber unterliegt der Offenlegungspflicht nach dem Mediengesetz. Diese reicht in ihrem Umfang weiter als ein Impressum. Die Impressumspflicht gilt für elektronische Medien, die wenigstens viermal im Kalenderjahr in vergleichbarer Gestaltung verbreitet werden, z.B. elektronische Newsletter.

Hinweis

- Umgangssprachlich werden die Offenlegungspflichten nach dem Mediengesetz häufig als Impressum bezeichnet.
- Nähere Informationen zur „Impressumspflicht“ finden sich ebenfalls auf USP.gv.at. Die Wirtschaftskammer Österreich bietet Unternehmerinnen/Unternehmern auf Ihrer Homepage an, die gesetzlichen Auflagen durch Eintragung ihrer Firmendaten und Verlinkung darauf zu erfüllen.

Bei der Offenlegungspflicht wird zwischen „großen“ und „kleinen“ Websites unterschieden. Wenn eine Website keine über die Darstellung des persönlichen Lebensbereichs oder die Präsentation der Medieninhaberin/des Medieninhabers hinausgehenden Informationsgehalt aufweist, der geeignet ist,

die öffentliche Meinungsbildung zu beeinflussen, handelt es sich um eine „kleine Website“. Die Offenlegungspflicht beschränkt sich in diesem Fall auf

- Name oder Firma der Medieninhaberin/des Medieninhabers,
- Unternehmensgegenstand,
- Wohnort oder Sitz (Niederlassung) der Medieninhaberin/des Medieninhabers.

Daher sind Websites, die sich auf die Präsentation des Unternehmens oder auf Produkte oder Dienstleistungen des Unternehmens beschränken, „kleine Websites“. Ein Online-Shop ohne redaktionelle Beiträge gilt somit als „kleine Website“.

Die Angaben zur Offenlegung können gemeinsam mit den allgemeinen Informationspflichten für kommerzielle Websites zur Verfügung gestellt werden. Ist die Medieninhaberin/der Medieninhaber mit der Online-Shop-Betreiberin/dem Online-Shop-Betreiber ident, muss nur der Unternehmensgegenstand offen gelegt werden, weil die weiteren Informationen bereits durch die allgemeinen Informationspflichten für kommerzielle Websites abgedeckt werden.

Ein Online-Shop gilt als „große Website“, wenn auch redaktionelle bzw. meinungsbildende Beiträge auf der Website enthalten sind. Zu den oben genannten Offenlegungspflichten müssen für „große Websites“ zusätzlich folgende Angaben getätigt werden:

- Namen der vertretungsbefugten Organe der Medieninhaberin/des Medieninhabers (z.B. Geschäftsführerinnen/Geschäftsführer)
- Im Falle des Bestehens eines Aufsichtsrates auch dessen Mitglieder
- Für sämtliche der an einer Medieninhaberin/einem Medieninhaber direkt oder indirekt beteiligten Personen die jeweiligen Eigentums-, Beteiligungs-, Anteils- und Stimmrechtsverhältnisse

- Allfällige stille Beteiligungen an der Medieninhaberin/dem Medieninhaber
- Treuhandverhältnisse für jede Stufe
- Im Falle der Beteiligung von Stiftungen die Stifterin/der Stifter und die jeweiligen Begünstigten
- Im Falle eines Vereins der Vorstand und der Vereinszweck
- Erklärung über die grundlegende Richtung des Mediums bzw. der Website, die sogenannte Blattlinie

Nähere Informationen zur Offenlegungspflicht der „großen Website“ finden sich ebenfalls auf USP.gv.at. Zusätzliche Informationspflichten der Online-Shop-Betreiberin/des Online-Shop-Betreibers finden sich unter Informationspflichten ebenfalls auf USP.gv.at.

Neue Vorschriften für Online-Shops – Geoblocking-Verordnung

Seit 3. Dezember 2018 darf der Zugriff auf einen Online-Shop wegen der Herkunft der Userin/des Users (Staatsangehörigkeit, gewöhnlicher Aufenthalt, Lieferadresse, IP-Adresse) nicht verweigert werden. Automatische Umleitungen sind nur dann erlaubt, wenn die Besucherin/der Besucher ihnen ausdrücklich zugestimmt hat, z.B. durch aktives Anklicken eines Feldes, und diese Auswahl jederzeit wieder aufgehoben werden kann.

Die Händlerin/der Händler darf jedoch das Liefergebiet selbst frei bestimmen und ist nicht verpflichtet, die Waren in jedes Land zu versenden. Das Liefergebiet sollte auf der Website klar erkenntlich gemacht werden.

Im Streitfall mit einer Verbraucherin/einem Verbraucher gilt der Gerichtsstand jenes Landes, auf das der Online-Shop ausgerichtet ist. Gibt es keine spezifische Ausrichtung auf ein einzelnes Land der Europäischen Union, gelten für eine österreichische Händlerin/einen österreichischen Händler das österreichische Recht und der österreichische Gerichtsstand.

Eine Unterscheidung bei Preisen aufgrund von Staatsangehörigkeit, Wohnsitz oder gewöhnlichem Aufenthalt ist verboten, außer es gibt dafür eine sachliche Rechtfertigung. Eine sachliche Rechtfertigung besteht etwa bei unterschiedlichen Umsatzsteuersätzen.

Auch bei den möglichen Zahlungsmitteln darf es grundsätzlich keine Unterscheidungen aufgrund von Staatsangehörigkeit, Wohnsitz oder gewöhnlichem Aufenthalt geben, außer es besteht eine sachliche Rechtfertigung.

Im Bereich zwischen zwei Unternehmen gelten diese Vorschriften nur, wenn die Käuferin/der Käufer keine Wiederverkäuferin/kein Wiederverkäufer ist.

Weiterführende Links

- Wirtschaftskammer Österreich (→ WKO)
- Website ECG– und mediengesetzkonform gestalten (→ WKO)
- Recht im Internet (→ onlinesicherheit.at)
- → NIC.at

Rechtsgrundlagen

- E-Commerce-Gesetz (ECG)
- Mediengesetz (MedienG)
- Gewerbeordnung (GewO)
- Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG

Letzte Aktualisierung: 16. Februar 2021

Für den Inhalt verantwortlich: Bundesministerium für Justiz

Eine Rechtsverordnung soll Cookie-Abfragen eindämmen

Cookie-Banner adieu?

Eine Rechtsverordnung soll Cookie-Abfragen eindämmen

Die Bundesregierung will zentral verwaltete Cookie-Einstellungen ermöglichen. Nutzer könnten sogar pauschal alle Cookies ablehnen. Allerdings würden sie dann wohl mit Hinweisbannern zu kostenpflichtigen Angeboten überschwemmt.

Von Holger Bleich

Die Datenschutz-Grundverordnung (DSGVO) lässt derzeit keinen Ausweg: Website-Betreiber müssen ihre Besucher um Erlaubnis fragen, bevor sie Tracking- oder Analyse-Cookies auf deren Rechner setzen. Diese Einwilligung muss informiert erfolgen, weshalb nahezu jede werbefinanzierte Website Pop-up-Banner vorschaltet, die viel Text enthalten. Und viele Banner stupsen Nutzer mit Design-Tricks zum „Ja“.

Das im Dezember 2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) sieht in seinem Paragrafen 26 einen deutschen Sonderweg vor, der die nervigen Banner überflüssig machen soll: In „anerkannten Diensten zur Einwilligungsverwaltung“ hinterlegen demnach Nutzer ihre

Cookie-Präferenzen zentral. Websites fragen dann nicht mehr direkt den User, sondern holen sich Einwilligung oder Ablehnung bei dem Dienst ab [1].

Nun hat das von Volker Wissing (FDP) geführte Bundesministerium für Digitales und Verkehr (BMDV) den Entwurf zu einer Verordnung erarbeitet, die den nach TTDSG erforderlichen Rechtsrahmen für die Einwilligungsdienste definieren soll. Nutzer können dem Entwurfstext zufolge „generelle Einwilligungen geordnet nach Kategorien für bestimmte Zugriffe auf Endeinrichtungen und Gruppen von Telemedienanbietern erteilen“. Die Dienste müssen gut erklären und informieren, außerdem sollen sie den Nutzer nicht mit Voreinstellungen beeinflussen.

Im BMDV glaubt man, im Entwurf die „richtige Balance“ zwischen den Interessen von Nutzern und kommerziellen Anbietern getroffen zu haben. Es gebe „keinen Anspruch auf kostenlosen Content“, war aus dem Ministerium zu hören. Diese Prämisse spiegelt sich im Entwurf wider: Zwar dürfen Nutzer im externen Einwilligungsdienst das Setzen von Cookies generell ablehnen. Doch gestattet es der Verordnungsentwurf Anbietern in diesem Fall, Nutzer mit vorgeschalteten Bannern darauf hinzuweisen, dass sie Tracking-Cookies benötigen, um die Site über Werbung zu finanzieren. Außerdem dürfen sie auf ein „kostenpflichtiges Alternativangebot“ (auf Medien-Websites die sogenannten „Pur-Abos“) verweisen oder den Nutzer „zur Änderung seiner Voreinstellungen beim Dienst zur Einwilligungsverwaltung“ auffordern.

Wie Websites die Nutzerpräferenzen beim Einwilligungsdienst abfragen sollen, lässt der Entwurf offen. In der Begründung zum Text, die c’t vorliegt, spricht das BMDV von „technikneutral“. Der Browser könne etwa einen HTTP-Request schicken, der die Zusatzinformation enthalte, dass der Endnutzer einen Dienst zur Einwilligungsverwaltung verwendet.

Auch wie die Dienste selbst funktionieren, will das BMDV dem

Markt überlassen. Sie dürfen „kein wirtschaftliches Eigeninteresse“ daran haben, dass Nutzer möglichst viele Einwilligungen erteilen. Wohl aber dürfen sie kommerziell agieren und auch Geld für ihre Services verlangen. Sie müssen ein Sicherheitskonzept vorweisen und sich anschließend von der Bundesdatenschutzbehörde prüfen und zertifizieren lassen.

Den ersten Entwurf hat das BMDV Ende August mit Bitte um Stellungnahmen an Wirtschaftsverbände geschickt. Er ist noch nicht mit anderen Bundesministerien abgestimmt. Bis er im Bundestag landet, werden noch viele Änderungen folgen – und Monate vergehen. Sollte der Bundestag die Rechtsverordnung durchwinken, muss die EU im sogenannten Notifizierungsverfahren prüfen, ob der Text europarechtskonform ist.

„Handwerkliche Fehler“

Daran regen sich bereits Zweifel. In einer ersten Stellungnahme kritisiert der Bundesverband Digitale Wirtschaft (BVDW) „handwerkliche Fehler“ im Text und moniert, dass der „aktuelle europäische Rechtsrahmen nicht hinreichend gewürdigt“ werde. Der Gesetzgeber habe „in den letzten Jahren zunehmend darauf hingewirkt“, die Einwilligung als Rechtsgrundlage für Datenverarbeitung zu forcieren, und nun wolle er „deren Einholung quasi untersagen“. Dies sei „aus Sicht der Datenökonomie und besonders aus Sicht der informationellen Selbstbestimmung der Nutzerinnen und Nutzer nicht der große Wurf, sondern ein großer Rückschritt“.

Das BMDV hat seinen Entwurf genau in einer Zeit vorgelegt, in der die EU dabei ist, ohnehin Cookie-Vorgaben und Einwilligungserfordernisse neu zu regeln: In Brüssel arbeiten Rat, EU-Parlament und Kommission gerade an einem Kompromiss zur E-Privacy-Verordnung. Weil diese EU-Verordnung über dem deutschen Recht stehen wird, könnte die deutsche Rechtsverordnung je nach Verhandlungsergebnis also schon in zwei bis drei Jahren wieder obsolet sein. (*hob@ct.de*)

1. Literatur
2. Holger Bleich, Löcher stopfen per Verordnung, Die bizarre Tracking-Regulierung in Deutschland, c’t 16/2022, S. 34

Datenschutzrechtliches für die Videoüberwachung

Vorsicht, Kamera!

Datenschutzrechtliche Schranken für die Videoüberwachung

Vor Eingängen oder auf Grundstücken, private Überwachungskameras sind allgegenwärtig. Und allzu oft verstößt deren Einsatz gegen den Datenschutz, wie eine große Zahl von Beschwerden und Bußgeldern belegt. Was gilt es zu beachten?

Von Holger Bleich und Joerg Heidrich

kompakt

- Kameras, die in den öffentlichen Raum gerichtet sind, erfassen personenbezogene Daten im DSGVO-Sinn.
- Betreiber müssen eine ausreichende Rechtsgrundlage vorweisen können und Transparenzpflichten erfüllen.
- Auch für den Betrieb von Türklingeln und

Gegensprechanlagen mit Kamera gilt die DSGVO, weshalb sie schwer rechtskonform zu betreiben sind.

Als Dashcam, im Smartphone oder an Hauswänden zur Überwachung: Kameras sind im öffentlichen Raum allgegenwärtig. Sie lösen Bewegtbilder so gut auf, dass man Personen auch noch erkennen kann, wenn sie weit entfernt sind. Dabei sind die Kameras bisweilen so winzig, dass Hersteller sie nahezu unsichtbar in beliebige Geräte verbauen können.

Geraten Unbeteiligte unwissentlich ins Blickfeld einer Kamera, kann dies Rechte verletzen. Zum einen geht es ums Persönlichkeitsrecht, also den Anspruch auf Kontrolle übers eigene Bild. Zum anderen handelt es sich bei jeder Aufnahme von Menschen, die man auf den Bildern anhand beliebiger Merkmale identifizieren kann, um eine Erhebung personenbezogener Daten im datenschutzrechtlichen Sinn.

Die europäischen Datenschutz-Aufsichtsbehörden fassen deshalb den Begriff „Videoüberwachung“ sehr weit. In einer Orientierungshilfe (siehe ct.de/yq1q) definierte es die Datenschutzkonferenz (DSK) als gemeinsames Gremium der deutschen Behörden folgendermaßen: „Eine Videoüberwachung liegt vor, wenn mithilfe optisch-elektronischer Einrichtungen personenbezogene Daten verarbeitet werden. Von diesem Begriff werden nicht nur handelsübliche Überwachungskameras erfasst, sondern jegliche Geräte, die zur längerfristigen Beobachtung und somit für einen Überwachungszweck eingesetzt werden.“

Aus den Tätigkeitsberichten der Aufsichtsbehörden geht hervor, dass es in keinem anderen Bereich so viele Beschwerden von Privatleuten gibt wie dem der Videoüberwachung von öffentlichen Räumen. Und in diesem Bereich wurden europaweit seit Einführung der DSGVO auch mit großem Abstand die meisten Bußgelder verhängt.

Dabei kennt die DSGVO nicht einmal eine explizite Regelung für die Videoüberwachung. In den meisten Fällen greifen die

Aufseher daher als potenzielle Rechtsgrundlage auf das sogenannte „berechtigte Interesse“ aus Art. 6 Abs. 1 f DSGVO zurück. Dessen Prüfung ist dreistufig aufgebaut.

Interesse berechtigt?

Zunächst muss eben dieses berechtigte Interesse auf der Seite des Kamerabetreibers vorliegen. Dies kann der Wunsch sein, das eigene Grundstück oder das Auto vor Diebstahl zu sichern, das Aufzeichnen von Straßenszenen bei Unfällen oder der Sichtkontakt zur klingelnden Person vor der Wohnungstür.

Der geplante Einsatz muss zudem erforderlich sein, um den beabsichtigten Zweck zu erreichen. Insbesondere darf es keine andere, zumutbare Maßnahme geben, die erwartbar weniger stark in die Rechte der betroffenen Personen eingreift. So mag es im Interesse des Betreibers eines Supermarkts liegen, durch Videoüberwachung zu verhindern, dass nachts auf seinem Parkplatz geparkt wird. Erforderlich wäre dies aber nicht, da er auch eine Schranke anbringen könnte und damit weniger in die Rechte von Personen eingreifen würde.

Ein berechtigtes Interesse allein reicht allerdings nicht aus. Vielmehr ist nach DSGVO im dritten Schritt eine Abwägung zwischen dem Interesse des Kamerabetreibers mit den „Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen“ notwendig. Und deren Interessen überwiegen in vielen Fällen, wenn für die Videoüberwachung nicht sehr gute Gründe vorliegen. Diese können zum Beispiel bei der Überwachung besonders gefährlicher Anlagen oder gefährdeter Bereiche in Bankfilialen angenommen werden.

In den meisten Fällen wird die Abwägung aber nicht so eindeutig ausfallen. So stehen beispielsweise die Interessen eines Unternehmens, jenen Eingangsbereich zu überwachen, in dem es wiederholt zu Diebstählen kam, denen der Mitarbeiter gegenüber, nicht beim Kommen und Gehen überwacht zu werden.

In solchen Fällen kommt es dann auch darauf an, wie die Überwachung konkret gestaltet wird. Hierzu kann der Aufnahmewinkel und -bereich gehören, den die Kamera erfasst. Falls die Kamera nicht nur einen Livefeed liefert, sondern auch aufzeichnet, spielen außerdem Speicherfristen und Zugriffsbeschränkungen aufs Material eine Rolle.

Zudem ist rechtlich relevant, ob die Betroffenen eine Überwachung erwarten. Dies haben Aufsichtsbehörden und Gerichte in der Vergangenheit besonders für Orte wie Tankstellen, Banken, Kaufhäuser oder den öffentlichen Nahverkehr als gegeben angesehen. Dagegen überwiegen die schutzwürdigen Interessen der Betroffenen meist an Orten wie Schwimmbädern, Innenbereichen von Hotels oder Restaurants, Sitzecken in Bäckereien, Schulen und natürlich Sanitäranlagen.

Wie unangenehm es werden kann, wenn Vorgaben nicht eingehalten werden, musste Anfang 2021 der Computerhändler notebooksbilliger.de erfahren [1]. Das Unternehmen hatte über mindestens zwei Jahre seine Beschäftigten per Video überwacht, ohne dass dafür eine Rechtsgrundlage vorlag. Erfasst hat er unter anderem Arbeitsplätze, Verkaufsräume, Lager und Aufenthaltsbereiche. Auch Kunden von notebooksbilliger.de waren von der unzulässigen Videoüberwachung betroffen, da einige Kameras auf Sitzgelegenheiten im Verkaufsraum gerichtet waren.

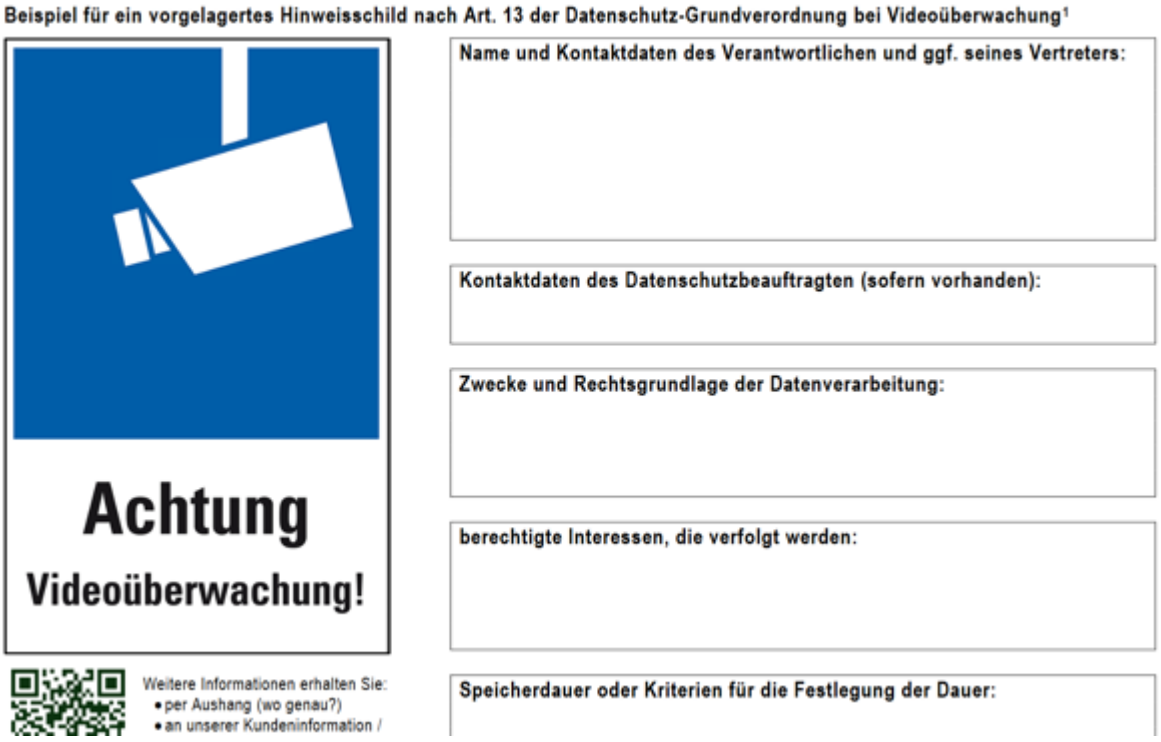
Die Argumentation des Händlers, dass es Ziel der installierten Videokameras gewesen sei, Straftaten zu verhindern und aufzuklären sowie den Warenfluss in den Lagern nachzuverfolgen, überzeugte die zuständige Datenschutzbehörde in Niedersachsen nicht. Allerdings ist der Fall noch vor Gericht und es ist offen, ob das hohe Bußgeld von 10,4 Millionen Euro für den Fall tatsächlich angemessen ist.

Transparenzanforderungen

Selbst wenn er eine valide Rechtsgrundlage für eine

Videoüberwachung vorhält, kann der Verantwortliche immer noch viel falsch machen. Denn neben der Rechtmäßigkeit fordert die DSGVO auch die Transparenz der Verarbeitung: Aus Art. 12 und den nachfolgenden Vorschriften ergeben sich weitgehende Informationspflichten in Richtung der potenziell Betroffenen.

Der Verantwortliche muss ein Informationsschild anbringen, das bildlich durch ein Kamerasymbol auf die Beobachtung hinweist. Zusätzlich ist viel Text erforderlich: Es muss die Identität des Verantwortlichen angegeben sein, außerdem seine Kontaktdaten und im Fall eines Unternehmens die des Datenschutzbeauftragten. Betroffene müssen über Zwecke und Rechtsgrundlagen der Videoüberwachung sowie die maximale Speicherdauer der Aufzeichnungen hingewiesen werden. All dies gehört schließlich auf ein möglichst großes Schild gedruckt und gut sichtbar ausgehängt.



Ein editierbares Muster der Datenschutzbehörden zeigt, wie ein rechtskonformer Hinweis auf Videoüberwachung aussehen muss (siehe ct.de/yq1q). *Quelle: LfDI Niedersachsen*

Noch weitergehende Informationspflichten, etwa obligatorische Angaben zu den Rechten auf Auskunft, Widerspruch, Löschung der Aufnahmen sowie auf die Beschwerdemöglichkeit bei der

Datenschutzaufsichtsbehörde, dürfen ins Web ausgelagert werden. Es genügt, einen Link oder einen QR-Code anzugeben. Immerhin: Die Datenschutzbehörden bieten hierfür Vorlagen als PDF- oder Word-Dateien, die Sie für den eigenen Gebrauch anpassen können (siehe ct.de/yq1q).

Datenschutzfolgenabschätzung

Besteht durch einen technischen Prozess ein besonders hohes Risiko für die Privatsphäre von potenziell davon Betroffenen, so hat der Verantwortliche laut DSGVO vorab eine sogenannte Datenschutzfolgenabschätzung durchzuführen. Es geht um eine verschriftlichte Risikoabschätzung unter datenschutzrechtlichen Gesichtspunkten. Eine solche Pflicht besteht nach Ansicht der DSK auch bei der Videoüberwachung, und zwar explizit dann, wenn die Verarbeitung ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge hat (Art. 35 Abs. 1 DSGVO).

Das umfasst insbesondere Systeme, die unzählige Personen in einem öffentlichen Bereich erfassen. Hierzu zählen der DSK zufolge etwa Kameras in Sport-, Versammlungs- und Vergnügungsstätten, Bahnhöfen, Einkaufszentren und Parkräumen. Ausgenommen ist die Überwachung von privaten Bereichen, die nicht öffentlich zugänglich sind. Das gilt sowohl für Unternehmen als auch für Privatpersonen, die ihr eigenes Grundstück überwachen wollen.

Sofern letztere es schaffen, nur ihren eigenen privaten Bereich zu erfassen – und nicht den öffentlichen Raum oder den Garten des Nachbarn – findet die DSGVO ohnehin keine Anwendung. Denn das Gesetz gilt grundsätzlich nicht für die „Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“. Allerdings wird diese Schwelle schnell gedankenlos überschritten, etwa bei der „Überwachung“ des öffentlichen Verkehrsraums mit Auto- oder Fahrrad-Dashcams – hier tangiert man immer die Rechte Dritter.

Videoüberwachung bei Autos

Vor allem Teslas „Wächtermodus“ hat dazu geführt, dass derzeit viel über 360-Grad-Kameraüberwachung moderner Fahrzeuge diskutiert wird. Diese geht weit über die Dashcam-Aufnahmeproblematik hinaus, zu der mittlerweile gefestigte Rechtssprechung existiert [2].

Aufsehen hat zuletzt ein Bußgeld erregt, das die niedersächsische Landesdatenschutzaufsicht Ende Juli dieses Jahres verhängt hat: 1,1 Millionen Euro muss Volkswagen für Datenschutzverstöße während einiger Forschungsfahrten zahlen, bei denen Techniker die Funktionsfähigkeit eines Fahrassistenzsystems zur Vermeidung von Verkehrsunfällen getestet hatten. Kameras hatten das Verkehrsgeschehen rund um den Wagen zur Analyse von Fehlern aufgezeichnet.

Der Behörde fehlte eine Datenschutzfolgenabschätzung für das Vorhaben. Vor allem aber monierte sie, dass keine Magnetschilder mit einem Kamerasymbol und die weiteren vorgeschriebenen Informationen für alle Verkehrsteilnehmer vorhanden waren. Diese hätten darüber aufgeklärt werden müssen, wer die Verarbeitung zu welchem Zweck durchführt und wie lange die Daten gespeichert werden. Wie Betroffene die Informationen während einer Autobahnfahrt dem Schild am Testfahrzeug hätten entnehmen können, sagte die Behörde nicht. Volkswagen hat das Bußgeld akzeptiert.

Doorbell-Cams

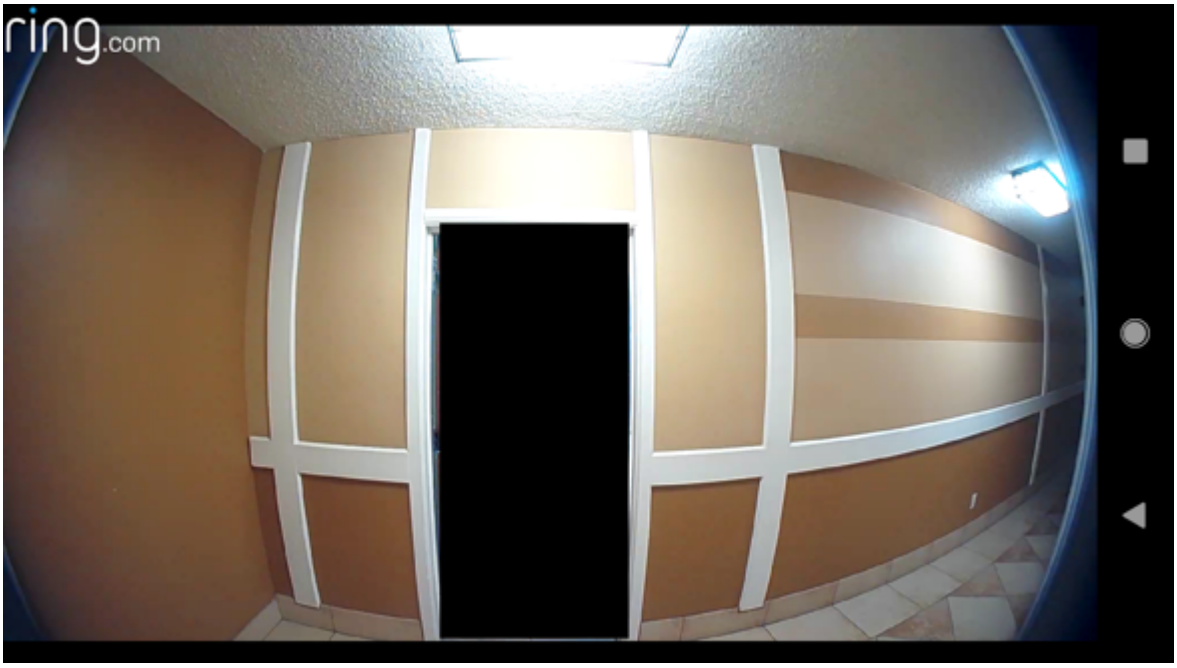
Ein weiteres datenschutzrechtliches Problem, das vor allem Privatleute betrifft, bilden vernetzte Wohnungs- und Haustürklingeln, die außerdem eine HD-Kamera enthalten. Weil diese Geräte insbesondere von Amazons Tochterfirma Ring bereits für unter 100 Euro zu haben und extrem leicht zu installieren sind, finden sie sich mittlerweile neben vielen Eingangstüren. Das eigentlich obligatorische Hinweisschild mit Kamerasymbol sucht man meist vergebens. Hier besteht akute

Bußgeldgefahr, falls sich Nachbarn oder Passanten bei der zuständigen Datenschutzaufsicht beschweren.

Die Vorgaben der DSK sind unmissverständlich: Unbedenklich seien die Systeme nur dann, wenn sie keinen öffentlichen Raum erfassen und „eine Bildübertragung erst nach Betätigung der Klingel ermöglichen, eine dauerhafte Speicherung der Bildaufnahmen ausschließen, räumlich nicht mehr abbilden, als ein Blick durch einen Türspion gewähren würde, und wenn die Übertragung nach einigen Sekunden automatisch unterbricht“.

Fast alle Funktionen, die Ring in seinen Prospekten bewirbt, muss man demnach unbedingt abschalten – etwa die Aktivierung durch Bewegungsmelder oder via App und die dauerhafte Speicherung der Aufnahmen in der Amazon-Cloud. Ring beziehungsweise Amazon machen darauf an keiner Stelle aufmerksam, weshalb dies kaum einem begeisterten Anwender bewusst sein dürfte.

Immerhin findet sich in der Ring-App die Möglichkeit, zwei rechteckige „Privatsphärenbereiche“ im Blickfeld der Kamera definieren zu können. Diese Felder bleiben schwarz, und Ring garantiert, dass darin keine Aufzeichnung stattfindet. So kann man beispielsweise die Wohnungstür des Nachbarn oder den erfassten Teil des Gehwegs vorm Haus maskieren.



In der Ring-App lassen sich rechteckige Bereiche im Blickfeld von der Aufnahme ausschließen, etwa der Wohnungseingang gegenüber. *Bild: ring.com*

Während deutsche Datenschutzbehörden bislang nur vereinzelt Bußgelder wegen Video-Türklingeln an Privatleute aussprechen, sieht das etwa in Spanien ganz anders aus: Agencia Española de Protección de Datos verhängt jeden Monat derlei Bußgelder, meist zwischen 300 und 600 Euro. Es scheint nur eine Frage der Zeit, bis dieser Trend auch andere EU-Behörden erreicht. (*hob@ct.de*)

1. Literatur
2. Holger Bleich, Joerg Heidrich, Teure Überwachung, notebooksbilliger.de soll 10,4 Millionen Euro Bußgeld zahlen, c’t 4/2021, S. 164
3. Dr. Michael Koch, Vorsicht Datenschleudern!, Was beim Datenschutz im Auto zu beachten ist, c’t 1/2022, S. 28

DSK-Infos und editierbare Vorlagen: ct.de/yq1q

Datenschutz Europa und USA

Prekärer Datenfluss

Was sich die USA beim Datenschutz von Europa abschauen

In den USA hatten Datenkraken lange Zeit leichtes Spiel. Doch nun droht der Datenfluss zu versiegen. Joe Biden hat den Datenverkehr mit Europa zur Chefsache erklärt, gleichzeitig arbeiten Demokraten und Republikaner fieberhaft an einem bundesweiten Datenschutzgesetz. Das hat aber seine Tücken, wie unser Überblick zeigt.

Von Falk Steiner

kompakt

- Bislang gelten in den US-Bundesstaaten unterschiedliche Datenschutzgesetze.
- Ein einheitliches Datenschutzgesetz ist in greifbare Nähe gerückt, lässt den Zugriff der Behörden aber außen vor.
- Präsident Biden will darüber hinaus den Datenaustausch zwischen der EU und den USA mit einem neuen Datenschutzrahmen absichern, der EU-Bürgern ein Klagerecht einräumt.

Mit der Datenschutz-Grundverordnung (DSGVO) hat die EU 2016 einen Standard gesetzt, an dem sich Anbieter und Gesetzgeber aus aller Welt orientieren müssen, wenn sie mit dem Recht des 27-Staaten-Bundes in Europa kompatibel sein wollen. Dabei

prallen immer wieder Welten aufeinander – insbesondere transatlantische. Die USA gelten mit ihren staatlichen und privatwirtschaftlichen Akteuren immer noch als Land der Datensammler. Dort existiert bis heute kein bundesweites Datenschutzrecht. Stattdessen kocht jeder US-Bundesstaat sein eigenes Süppchen. Weil die transatlantischen Datenflüsse aus Europa zu versiegen drohen, muss die US-Regierung dringend eine Lösung finden.

Das fehlende Datenschutzrecht auf Bundesebene ist eine von mehreren Hürden: Die DSGVO erlaubt den Export von personenbezogenen EU-Daten nur, wenn im Zielland der Schutz dieser Daten auf einem vergleichbaren Niveau wie in Europa gewährleistet ist. Die EU-Kommission als zuständige Behörde muss dies prüfen und dann eine sogenannte Angemessenheitsentscheidung treffen.

Derartige „Adequacy Decisions“ wurden bislang für 14 Staaten getroffen, darunter Südkorea, Japan, Israel, Uruguay, Kanada und die Färöer-Inseln. Der US-Rechtsrahmen ist hingegen nicht ausreichend. Daher suchten die USA in den vergangenen 20 Jahren immer wieder nach Alternativen, um die Datentransfers rechtlich abzusichern.

Doch sowohl die sogenannte Safe-Harbor-Vereinbarung zwischen EU und US-Regierung aus dem Jahr 2000 als auch die Nachfolgeregelung Privacy Shield von 2016 wurden vom Europäischen Gerichtshof (EuGH) kassiert: Die Absprachen, die keine Verträge im Sinne des Völkerrechts sind, konnten in der EU erhobene Daten nicht ausreichend sichern, befanden die Richter in Luxemburg nach zwei Klagen des österreichischen Aktivisten Max Schrems.

Nach Privacy Shield

Lange ist danach wenig passiert. Doch nun läuft den Unternehmen die Zeit davon: Nach und nach fallen die verbliebenen rechtlichen Möglichkeiten weg, doch noch

irgendwie legal personenbezogene Daten in die USA zu transferieren. Die irische Datenschutzaufsichtsbehörde DPC Ireland bearbeitet dabei den wichtigsten Fall: Sie könnte Facebook untersagen, personenbezogene Daten von seinem EU-Hauptsitz auf der Insel in die USA zu transferieren. Das steht in einem Entscheidungsentwurf, den die Iren Anfang Juli an ihre Kollegen der übrigen europäischen Datenschutzaufsichtsbehörden verschickt haben. Obwohl die DPC unter Datenschützern als sehr zurückhaltend gilt, könnte ihr Vorhaben das Aus für datengetriebene US-Unternehmen in Europa bedeuten. Die Facebook-Mutter Meta hat ihre Aktionäre schon mehrfach gewarnt, dass sie aufgrund der dann drohenden empfindlichen DSGVO-Bußgelder womöglich Teile ihres Europageschäfts aufgeben müsste – und damit Milliarden an Umsatz verlöre.

Mark Zuckerberg hat Aktionäre von Meta bereits gewarnt, dass sein Konzern womöglich bald keine personenenbezogenen Daten aus Europa mehr in die USA übertragen darf. *Bild: Eric Risberg/AP/dpa*

Sammelklagen statt Aufsichtsbehörden

Parallel dazu bewegt sich der Datenschutz in den USA: Viele US-Bundesstaaten bereiten Gesetze vor oder haben bereits welche erlassen, die die Privatsphäre besser schützen sollen. Zwei Staaten stehen im Zentrum der Aufmerksamkeit: Kalifornien schärft im Januar 2023 seinen fünf Jahre alten California Consumer Privacy Act (CCPA) mit dem Californian Privacy Rights Act (CPRA) nach. In Illinois gilt seit 2008 der Biometric Information Privacy Act (BIPA). Das Schutzgesetz für biometrische Daten hatte nach Sammelklagen mehrere Vergleiche mit bemerkenswerten Summen zur Folge: McDonalds zahlte 50 Millionen Dollar, Google 100 Millionen Dollar und Facebook sogar 650 Millionen Dollar an Kläger aus Illinois, weil sie deren biometrische Daten unerlaubt verarbeitet und gegen den BIPA verstoßen hatten. Fast im Monatstakt kommen neue Millionenvergleiche hinzu, der Druck auf die Unternehmen steigt.

Während in Europa Aufsichtsbehörden die Strafen für Verstöße verhängen, schließen sich in den USA Betroffene vor allem in Sammelklagen zusammen. Organisationen sammeln die Rechtsansprüche vieler Bürger und reichen vor Gericht Klage gegen ein Unternehmen ein. In den seltensten Fällen enden diese Verfahren mit einem Urteil. Stattdessen schließen Kläger und Beklagte einen Vergleich. Das kann für die Firmen mitunter teurer sein als ein Gerichtsurteil.

Aufsichtsbehörden haben in den USA deutlich weniger Möglichkeiten, Bußgelder zu verhängen als in Europa. Nur in wenigen Fällen nutzt etwa die Handelsaufsicht, die Federal Trade Commission (FTC), ihre rechtlich begrenzten Möglichkeiten: Zuletzt etwa, weil sich ein Unternehmen nicht an seine Selbstverpflichtung hielt, die es im Zuge der Privacy-Shield-Vereinbarung abgegeben hatte. Auch wenn der EuGH die Privacy-Shield-Angemessenheitsentscheidung inzwischen annulliert hat, behalten die damit verbundenen

Selbstverpflichtungen von Firmen in den USA weiterhin ihre Gültigkeit.

Flickenteppich

Für in- und ausländische Unternehmen sind die in einzelnen Bundesstaaten der USA aufploppenden neuen Datenschutzgesetze ein Problem: Statt an einem einzelnen Rechtsrahmen müssten sie sich eigentlich an den Vorgaben jedes Staates einzeln ausrichten und somit Nutzer in Maine anders als in Illinois oder Kalifornien behandeln. Kein Wunder, dass sich viele der großen Technologiekonzerne ein einheitliches US-Datenschutzrecht wünschen.

Einige der Datenschutzgesetze der Bundesstaaten definieren den Begriff „personenbezogene Daten“ äußerst weitreichend, erläutert Jan Sebisch von der Gesellschaft für Außenwirtschaft und Standortmarketing (GTAI): „Sie räumen den Verbrauchern in Bezug auf ihre Daten durchaus mit EU-Niveau vergleichbare Betroffenenrechte ein, zum Beispiel das Recht auf Löschung, und in bestimmten Konstellationen sogar ein privates Klagerecht.“ Mangels US-Bundesdatenschutzgesetz gebe es für Unternehmen jedoch keine allgemeinen Leitlinien oder Faustformeln, wann sie „auf der sicheren Seite sind“. Es komme stets auf die konkrete Fallkonstellation und das entsprechende einzelstaatliche Recht an, sagt Sebisch.

Neues Bundesdatenschutzrecht

Ein Vorschlag, das zu ändern, liegt derzeit in den beiden Kammern des US-Kongresses: der American Data Privacy and Protection Act (ADPPA). Er wurde von Vertretern der Republikaner und Demokraten initiiert und schließlich von einflussreichen Mitgliedern des Repräsentantenhauses und des Senats eingebracht. Aus Sicht von Sebisch ist ein solch parteiübergreifender Vorschlag sehr beachtlich, weil Demokraten und Republikaner in puncto Datenschutzrecht zuvor nicht auf einen Nenner gekommen seien.

Der ADPPA könnte ein Bundesdatenschutzrecht schaffen, das in einigen Teilen dem EU-Recht ähnelt. Er betrachtet nicht nur unmittelbar personenbezogene Daten als regulierbar, sondern auch solche Daten, die einen Personenbezug herstellen können, wenn man sie mit weiteren Angaben koppelt. Dazu zählen auch sogenannte Identifier, denen sich Personen eindeutig zuordnen lassen.

Zudem schreibt er vor, das Erheben, Verarbeiten und Weitergeben von Daten auf das Nötige zu beschränken und fordert damit eine ähnliche Datensparsamkeit wie die DSGVO. Laut ADPPA dürfen Daten nur noch erhoben werden, wenn dies „vernünftigerweise notwendig und verhältnismäßig“ ist. Darunter fallen Daten für Produktion und Dienstleistungen, Kundenkommunikation, Rechnungswesen und IT-Sicherheit.

An einigen Stellen geht der ADPPA-Vorschlag sogar über den Text der DSGVO hinaus: etwa beim Verbot irreführender Oberflächengestaltungen, die Betroffene zu ungewollten Einwilligungen verleiten. Hier folgt der ADPPA dem neuen Digital Services Act (DSA) der EU und formuliert darüber hinaus restriktive Regelungen zur algorithmischen Verarbeitung biometrischer Daten. „Er hat mehr Momentum als jede Vorgängerinitiative“, erläutert Tyson Barker, der für die Deutsche Gesellschaft für Auswärtige Politik (DGAP) in Berlin die transatlantische Technologiepolitik beobachtet. „Der Vorschlag beschränkt Sammelklagen, verdrängt stärkere Einzelstaatengesetze, macht bei den Betroffenenrechten viele Anleihen bei der DSGVO und integriert Elemente des DSA, etwa zu datenbasierter Werbung“, zählt Barker auf.

Derzeit hält er es jedoch für unwahrscheinlich, dass der ADPPA in dieser Form verabschiedet werde, weil ihn die wichtigste Person nicht unterstützt: Maria Cantwell, die demokratische Vorsitzende im Wirtschaftsausschuss des Senats. An Cantwell führt laut Barker kein Weg vorbei. Sie fordert wesentlich weiter gehende Regelungen zum Schutz der Privatsphäre, als sie der ADPPA derzeit vorsieht. Auf jeden Fall will sie eines

verhindern: dass ein schwaches Bundesgesetz stärkere Regelungen in einzelnen Bundesstaaten aushebelt.

US-Senatorin Maria Cantwell möchte verhindern, dass ein zu laxes bundesweites Datenschutzgesetz künftig rigidere Vorgaben in einzelnen Bundesstaaten blockiert. *Bild: Maria Cantwell / U. S. Senate*

Bundesrecht und Landesrecht

Der Streit um den ADPPA und Cantwells Auffassung ähnelt der Subsidiaritätsdebatte in Europa: Was soll auf der obersten Ebene rechtlich geregelt werden, was sollen untere Ebenen beschließen? Die vollständige Vereinheitlichung auf Bundesebene zu Lasten der Gesetzgebung der Mitgliedstaaten wird in den USA als „preemption“ bezeichnet. Dies ist im ADPPA zumindest für bestehende Gesetze nicht vorgesehen. Er führt eine lange Liste von strengeren Gesetzen auf Bundes- und Einzelstaatsebene auf, die ausdrücklich nicht ausgehebelt werden sollen – etwa der Biometric Privacy Act aus Illinois. Cantwell befürchtet jedoch, dass der ADPPA künftige strengere Datenschutzregelungen in einzelnen Bundesstaaten ausschließt und somit landesweit einen zu laxen Datenschutz zementiert.

Der ADPPA regelt laut Sebisch auch den Zusammenhang zwischen behördlichen und privatrechtlichen Klagen. So sollen

geschädigte Personen vier Jahre nach Inkrafttreten des Gesetzes private Klagen vor dem Bundesgericht einreichen dürfen. Bei Datenschutzverletzungen von Unternehmen könnten sie Schadenersatz, Unterlassung, Prozesskosten und Anwaltsgebühren geltend machen, erläutert Sebisch.

Bevor sie eine Klage einreichen, müssten Betroffene dem ADPPA-Entwurf zufolge aber die Federal Trade Commission (FTC) und den Generalstaatsanwalt ihres Bundesstaates informieren. Eröffnet eine der beiden Institutionen ein Verfahren, wären Sammelklagen für dessen Dauer erst einmal ausgeschlossen. Die FTC könnte die Regelungen ähnlich wie die Datenschutzaufsichtsbehörden in Europa von sich aus durchsetzen. In diesen Tagen diskutiert der Ausschuss für Energie und Wirtschaft des US-Repräsentantenhauses sehr intensiv über den ADPPA-Entwurf. Damit er schließlich Gesetz wird, müssen seine Befürworter aber noch Maria Cantwell überzeugen. Jan Sebisch von der GTAI erwartet deshalb noch einige Änderungen, bevor der ADPPA das erste in den gesamten USA gültige Datenschutzgesetz überhaupt werden kann.

Mit dem ADPPA würden sich die USA der europäischen Vorstellung von Datenschutz deutlich annähern. Das wäre für transatlantische Datenübertragungen eine Verbesserung – dürfte aber noch lange nicht den Ansprüchen europäischer Datenschützer genügen. Dennoch begrüßt der Landesdatenschutzbeauftragte von Baden-Württemberg, Stefan Brink, die Initiative für das Gesetz: „Die Strahlkraft der Datenschutzgrundverordnung reicht ganz offensichtlich bis in die USA“, freut sich Brink angesichts vieler konzeptioneller Übernahmen im US-Vorschlag. „Inwiefern ein US-Datenschutzrecht die Beratung und Prüfung von Datenverarbeitungen mit Übermittlung in die USA verändert, hängt jedoch von der genauen Ausgestaltung des Gesetzes ab.“

Geheimdienste bleiben unberührt

Bei aller Euphorie enthält der ADPPA noch einige Lücken. Denn er soll grundsätzlich nur die Rechte von Personen mit einer US-Aufenthaltserlaubnis schützen. Darunter fallen auch viele in den USA lebende Ausländer. Doch selbst US-Bürger, die im Ausland leben, könnten sich dem Entwurf nach nicht auf ihn berufen, betont Calli Schroeder von der US-Bürgerrechtsorganisation EPIC. Zugleich wären Ansprüche aus den Vorschriften nicht von Personen außerhalb der USA einklagbar – also auch nicht von Europäern.

Einen Aspekt klammert der ADPPA zudem vollständig aus, da er als Verbraucherschutznorm konzipiert ist: den Datenzugriff von US-Behörden, darunter Strafverfolgern und Geheimdiensten wie der NSA. Genau hier liegt seit dem Urteil des EuGH zum Privacy Shield 2020 aber ein großer Stolperstein. Infolge der Snowden-Affäre prüfte der EuGH, unter welchen Umständen US-Behörden auf personenbezogene Daten zugreifen dürfen, die in den USA oder aber von US-Unternehmen außerhalb der USA gespeichert sind. In seinem Urteil bemängelte der EuGH sowohl die umfangreichen Zugriffsmöglichkeiten der US-Geheimdienste als auch das Fehlen von Rechtsmitteln, die EU-Bürger dagegen einlegen können. Dieses Urteil fordert das politische Washington gleich auf mehreren Ebenen heraus.

Auf der einen Seite ist es aus Sicht vieler US-amerikanischer Politiker ein Unding, dass ein europäisches Gericht amerikanischen Behörden und Gesetzgebern Vorschriften machen möchte. Auf der anderen Seite steht die enorme wirtschaftliche Bedeutung, die der EU-Markt für die meisten US-Tech-Konzerne hat. Und ein Szenario, in dem US-Firmen vom Datenstrom aus Europa abgeschnitten werden, ist mit der kommenden Entscheidung der irischen Datenschutzaufsichtsbehörde DPC nur noch Monate statt Jahre entfernt.

US-Präsident Joe Biden hat den Datenaustausch mit Europa zur Chefsache erklärt. Er möchte die EU mit Präsidialverfügungen zufriedenstellen. *Bild: Evan Vucci/AP/dpa*

TADPF soll Datenverkehr sichern

Damit EU-US-Datentransfers in Zukunft rechtssicher sind, soll daher eine neue Vereinbarung zwischen den USA und der EU her. Damit sie nicht ebenfalls vor dem Europäischen Gerichtshof scheitert, soll sie Daten von EU-Bürgern besser schützen als Safe Harbor und Privacy Shield.

US-Präsident Joe Biden erklärte dies zur Chefsache und kündigte bei seinem Besuch in Brüssel im Frühjahr einen neuen transatlantischen Datenschutzrahmen an: Die US-Regierung bietet der EU-Kommission ein Transatlantic Data Privacy Framework (TADPF) an. Die Vorarbeiten dafür laufen seit Anfang vorigen Jahres. Doch bis Redaktionsschluss fehlte das wohl wichtigste Element: der Rechtstext, mit dem die US-Regierung den Einwänden des EuGH künftig begegnen will.

Bislang gibt es nur mündliche Ankündigungen von Präsident Biden. So wollen die USA künftig weniger Daten über EU-Bürger

sammeln und ihre Behörden strenger prüfen. EU-Bürger sollen sich zudem rechtlich gegen eine Erfassung durch US-Geheimdienste wehren können – vor einer dafür zuständigen Gerichtsinstanz.

Solange die Präsidialverfügungen aber nicht vorhanden sind, kann die EU-Kommission mit dem in der DSGVO vorgesehenen Prozess für eine Angemessenheitsentscheidung nicht beginnen. Offen ist zudem, ob die EU-Kommission eine solche Entscheidung auf Basis von US-Präsidialverfügungen überhaupt treffen kann. Denn ein künftiger Präsident könnte eine Executive Order jederzeit mit einem Federstrich ändern.

Landesdatenschützer Stefan Brink wünscht sich deshalb einen anderen Weg: „Ein – parlamentarischer – Rechtsakt würde mehr Beständigkeit und damit auch Rechtssicherheit versprechen." Seine Behörde hätte bei der Angemessenheitsentscheidung der EU-Kommission zwar ein Recht zur Mitsprache, allerdings nicht zum Veto.

Klagen mit Ansage

„Europas Sorgen im Fall einer Wiederkehr Trumps könnten Überlegungen nötig machen, wie der Kongress die Präsidialverfügungen in Gesetzen kodifizieren könnte", sagt Tyson Barker von der DGAP. 2024 muss der US-Kongress den Abschnitt 702 des für die Überwachungsbefugnisse der Behörden wichtigsten Gesetzes, dem Foreign Intelligence Surveillance Act (FISA), erneut beschließen. „Das könnte eine Gelegenheit sein, das Gesetz so anzupassen, dass es die Inhalte der Präsidialverfügungen widerspiegelt", erklärt Barker.

Es bewegt sich also etwas beim Datenschutz in den USA, wenn auch aus europäischer Sicht zu wenig. Bei der Ankündigung des TADPF meinte Datenschutzvorkämpfer Max Schrems, er wolle die Vereinbarung prüfen. Er geht davon aus, dass nach einer eventuellen Angemessenheitsentscheidung der EU-Kommission zum TADPF Klagen beim EuGH eingereicht werden. Falls nicht von ihm

selbst, dann von anderen Datenschutzaktivisten. (*hag@ct.de*)

Datenschutzaktivist Max Schrems hat mit seinen Klagen bereits Safe Harbor und Privacy Shield gekippt. Die Geschichte könnte sich mit dem TADPF wiederholen. *Bild: Hans Punz/APA/dpa*

1. Literatur
2. Holger Bleich, FAQ: Das Ende des Privacy Shields, c’t 21/2020, S. 178

EU – Umgang mit Daten

Europäisches Trommelfeuer

Wie die EU den Umgang mit Daten revolutionieren will

Europa soll zum Vorbild für die digitale Gesellschaft werden. Dazu zündet die EU ein wahres Feuerwerk an Gesetzen. Sie sollen die Dominanz der US-Unternehmen brechen und europäischen Firmen einen besseren Zugang zu Daten verschaffen. Die geplanten Regulierungen stellen sogar die DSGVO in den Schatten, wie unsere Übersicht zeigt, und werden die Gesellschaft wohl nachhaltig verändern.

Von Joerg Heidrich

kompakt

- Ab Mitte 2023 reguliert der Digital Markets Act europaweit die Geschäftspraktiken von Onlineplattformen, ab 2024 greift der Digital Services Act.
- Der Data Governance Act und der Data Act sollen vor allem den Umgang mit nicht personenbezogenen Daten regeln, die nicht unter die DSGVO fallen.
- Firmen sollen ihre Daten künftig mit Treuhändern teilen, ein AI Act verbietet KI-Systeme in besonders risikoreichen Einsatzgebieten.

Mit viel Pathos kündigte die EU-Kommission Anfang 2020 in einer Art Manifest ihre neue Datenstrategie an. Die EU könne zu einem Vorbild für eine Gesellschaft werden, die „dank Daten in der Lage ist, in der Wirtschaft wie im öffentlichen Sektor bessere Entscheidungen zu treffen“. Um eine weltweit führende Rolle in der Datenwirtschaft zu übernehmen, müsse man unverzüglich handeln und die vielfältigen Probleme regulatorisch angehen, die von der Konnektivität über die Datenverarbeitung und -speicherung bis hin zur Cybersicherheit reichen.

Hierfür sei es nötig, die Voraussetzungen für den Umgang mit

Daten zu verbessern und für die Gesellschaft „Pools mit hochwertigen Daten“ aufzubauen. Diese sollen nicht nur die Produktivität von Firmen steigern und deren Wettbewerbsfähigkeit verbessern, sondern auch den Bereichen Gesundheit, Umwelt und öffentliche Dienste zugutekommen. Zugleich will man die digitale Wirtschaft fördern, damit sie mit Firmen aus den USA und China mithalten kann.

Um diese ambitionierten Ziele zu erreichen, hat die Kommission seit der Ankündigung ein ganzes Bündel aus Gesetzen auf den Weg gebracht. Juristen erwarten gar ein neues Rechtsgebiet, das Datenrecht. Im Fokus der Diskussion steht etwa ein halbes Dutzend dieser Vorhaben. Sie haben das Potenzial, die Gesellschaft nachhaltig zu verändern.

Digital Services Act

Dies gilt insbesondere für den Digital Markets Act (DMA) und den Digital Services Act (DSA). „Acts“ sind Verordnungen, die – wie beispielsweise die DSGVO – unmittelbar als europäisches Recht gelten. Im Gegensatz zu Richtlinien müssen Gesetzgeber in den einzelnen europäischen Ländern sie nicht erst in nationales Recht umsetzen.

EU-Binnenmarktkommissar Thierry Breton kündigte mit den neuen EU-Verordnungen „das Ende des Wilden Westens" im Internet an. *Bild: Virginia Mayo/Pool AP/dpa*

Der DSA tritt ab 2024 in Kraft und wendet sich insbesondere an Anbieter von Onlinediensten und sozialen Medien. Er verpflichtet diese, in kurzer Zeit gegen rechtswidrige Inhalte vorzugehen. Besonders strenge Anforderungen gibt es für jene großen Onlineplattformen und Suchmaschinen, die im Monat von mehr als 45 Millionen Menschen genutzt werden. Aufgrund ihrer Reichweite sollen deren Anbieter „systemische Risiken" eindämmen, die sich etwa aus der Verbreitung rechtswidriger Inhalte ergeben. Dazu zählen Desinformation oder Wahlmanipulation, Cybergewalt gegen Frauen sowie jugendgefährdende Inhalte. Die EU-Kommission sieht darin einen wichtigen Schritt „zur Verteidigung europäischer Werte wie Demokratie und Rechtsstaatlichkeit" im virtuellen Raum. Der DSA wird damit zum EU-weiten Nachfolger des deutschen Netzwerkdurchsetzungsgesetzes (NetzDG), welches bereits jetzt Social-Media-Angebote reguliert.

In die Pflicht nimmt der DSA auch Onlinemarktplätze. Sie haben dafür zu sorgen, dass über ihre Plattformen keine gefährlichen

oder illegalen Produkte wie Markenfälschungen angeboten werden. Das Gesetz sieht dazu neue Mechanismen vor, die es Usern ermöglichen, illegale Inhalte zu melden. Die Plattformen müssen zudem mit „vertrauenswürdigen Hinweisgebern“ zusammenarbeiten, die ihnen helfen sollen, verbotene Inhalte zu ermitteln und zu entfernen.

Der DSA regelt ferner bestimmte Formen der Werbung. Hier war sogar ein grundsätzliches Verbot von Werbetracking in der Diskussion, der Ansatz konnte sich jedoch nicht durchsetzen. Das Gesetz enthält allerdings ein Verbot irreführender Werbepraktiken, zum Beispiel gezielt auf Kinder ausgerichtete Werbung oder solche, die auf sensiblen Daten wie Religionszugehörigkeit, sexueller Ausrichtung oder politischer Meinung basiert. Dies wird die werbetreibende Industrie vor große Herausforderungen stellen.

Nach den neuen Vorschriften sind auch sogenannte Dark Patterns verboten. Onlineplattformen dürfen Nutzer nicht mehr täuschen oder manipulieren beziehungsweise „ihre Fähigkeit, freie und fundierte Entscheidungen zu treffen“ beeinträchtigen oder behindern.

Digital Markets Act

Der DMA kommt etwas früher und gilt bereits ab der zweiten Jahreshälfte 2023. Seine Vorschriften ergänzen das Wettbewerbsrecht und sollen die Macht der marktbeherrschenden Digitalkonzerne einschränken. Auf deren Plattformen, den sogenannten Gatekeepern, soll es zukünftig durch gesetzliche Regulierung fairer zugehen.

Welche Unternehmen unter diese Einstufung fallen, legt die Kommission explizit fest. Erfasst werden mit hoher Sicherheit Unternehmen wie Airbnb, Alphabet, Apple, Amazon, Meta und Microsoft. Dass es sich dabei um amerikanische Konzerne handelt, ist kein Zufall. Die gesamte Digitalstrategie der EU beruht darauf, es amerikanischen Unternehmen schwerer zu

machen und so die digitale Wirtschaft im europäischen Raum zu stärken. Aber auch die Verbraucher sollen geschützt werden, indem Firmen ihre Nutzerdaten nicht mehr über Plattformgrenzen hinweg zusammenführen dürfen.

Den Gatekeepern ist es zukünftig untersagt, ihre eigenen Dienste oder Produkte höher zu gewichten als die von anderen geschäftlichen Nutzern ihrer Plattform. Dies dürfte etwa Amazon oder Alphabet treffen, denen Kritiker häufig vorhalten, eigene Angebote gegenüber Dritten zu bevorzugen.

Weitere Regelungen sollen sogenannte Lock-In-Effekte verhindern. Die als Gatekeeper eingestuften Plattformen müssen ihre Angebote kompatibel zu denen von Wettbewerbern gestalten. In der Vergangenheit musste etwa Microsoft bereits hohe Strafen zahlen, weil es unter Windows seinen Edge-Browser gegenüber anderen Browser bevorzugt hatte.

Verstößt ein Gatekeeper gegen die Vorschriften des DMA, so kann dies für ihn sehr teuer werden. Die neue Vorschrift sieht Geldstrafen vor, die bis zu 10 Prozent Gesamtumsatzes betragen, die das Unternehmen im vorhergehenden Geschäftsjahr weltweit erzielt hat. Bei wiederholten Verstößen können die Strafen sogar bis zu 20 Prozent des Umsatzes betragen. Im Fall von Amazon wären das aktuell bis zu 94 Milliarden US-Dollar.

Die dänische EU-Kommissarin für Wettbewerb, Margrethe Vestager, gilt als treibende Kraft hinter dem Digital Markets Act, der wettbewerbswidrige Praktiken der großen US-Konzerne eindämmen soll. *Bild: Oliver Berg/dpa*

Umstrittene Interoperabilität

Die geplante Regulierung von Messenger-Diensten trifft bei kleineren Anbietern eher auf Ablehnung. Künftig müssen sich Platzhirsche wie WhatsApp und iMessage dafür öffnen, auch Nachrichten von Wettbewerbern zu empfangen. Kleinere Anbieter wie Signal oder Threema sperren sich jedoch gegen das Vorhaben. Die Firmen sehen nämlich durch die Pläne der EU die vertrauliche und sichere Kommunikation über ihre Apps bedroht. So fürchtet der Betreiber von Signal, dass die Zusammenarbeit mit den dominanten Messengern letztlich die Privatsphäre des eigenen Angebots verschlechtert. Die Mitbewerber hätten dann Zugriff auf Metadaten und könnten diese für ihre Zwecke nutzen. Daher haben beide Anbieter bereits angekündigt, auf eine Zusammenschaltung mit WhatsApp & Co. zu verzichten.

Laut Digital Markets Act müssen Gatekeeper wie WhatsApp sich für Konkurrenten öffnen, wenn diese das fordern. Anbieter wie Threema und Signal wollen davon jedoch keinen Gebrauch machen. *Bild: Threema*

Trainingsdaten für KI

Während der DMA und der DSA primär Plattformen und größere Onlinedienste regulieren, betrifft der zweite wichtige Teil der EU-Strategie den Umgang mit Daten. Für personenbezogene Daten gilt die Datenschutz-Grundverordnung (DSGVO) bereits seit 2018. Allerdings gibt es eine Vielzahl von Daten, die nicht unter die DSGVO fallen, insbesondere solche, die von Maschinen stammen und für das Training neuronaler Netze genutzt werden. Hier setzen zwei weitere Gesetzesvorhaben der EU an: der Data Governance Act (DGA) und der Data Act (DA).

Den DGA verabschiedeten die EU-Gremien bereits im Mai 2022. Er soll im September 2023 in Kraft treten. Ziel des Gesetzes ist es, dem öffentlichen Sektor den Zugang zu Daten zu erleichtern und ein „vertrauenswürdiges Umfeld“ für die Forschung sowie für innovative Dienste und neue Produkte zu schaffen.

Der DGA geht bei der Weitergabe von Daten an den öffentlichen Sektor sehr weit. Der Regelung liegt der Gedanke zugrunde, dass auch geschützte Daten der Gesellschaft zugutekommen sollen, wenn sie beispielsweise durch öffentliche Förderung generiert oder gesammelt wurden. Firmen sollen beispielsweise Geschäftsgeheimnisse, personenbezogene Daten und durch Rechte des geistigen Eigentums geschützte Werke übertragen. Dies gilt allerdings nur für Daten, die sich bereits „im Besitz öffentlicher Stellen“ befinden. Dort vorhandene Daten können etwa für Forschungszwecke im öffentlichen Interesse weiterverarbeitet werden.

Faire Datenbroker

Der DGA soll darüber hinaus ein neues und potenziell revolutionäres Geschäftsmodell etablieren: Es sollen Datenvermittlungsdienste entstehen, die eine sichere Umgebung bieten, in der Unternehmen oder Einzelpersonen Daten austauschen. Unternehmen sollen ihre Daten teilen können, ohne Missbrauch oder einen Wettbewerbsnachteil befürchten zu müssen.

Die Vermittlungsdienste bieten nur eine Plattform an und sind ansonsten neutrale Akteure. Die von ihnen vorgehaltenen Daten dürfen sie nicht zu eigenen Zwecken nutzen. Erstaunlicherweise müssen sie aber keinen Sitz innerhalb der EU haben, sondern dürfen sich auch außerhalb der EU niederlassen.

Auf Basis der neuen Regulierung sollen Dienste entstehen, die einen Handel mit persönlichen Daten ermöglichen. Der Gesetzgeber sieht solche Datainteremediären als Schlüssel für eine neu entstehende Datenwirtschaft. Genannt werden als Beispiel Daten-Wallets, also Apps, mit deren Hilfe der Einzelne in die Nutzung seiner Daten einwilligt und dadurch auch Geld verdienen oder sonstige Vorteile erlangen kann.

Daten für alle

Der dritte Bereich des Data Governance Acts bildet das Konzept des Datenaltruismus ab. Die EU will es Privatpersonen und Unternehmen erleichtern, der Gesellschaft Informationen für Ziele im allgemeinen Interesse zur Verfügung zu stellen. Hierzu zählen beispielsweise Daten für Forschungszwecke im Bereich der Medizin, des Klimawandels oder um öffentliche Dienstleistungen zu verbessern.

Allerdings ist es gar nicht so einfach, eine datenaltruistische Organisation zu werden. Die Stellen müssen neben hohen Anforderungen an ihre technische Ausstattung und Transparenz auch umfangreiche Berichtspflichten erfüllen, sobald sie in ein Verzeichnis aufgenommen wurden.

Den wohl radikalsten Ansatz hinsichtlich des Umgangs mit Daten verfolgt die Europäische Kommission derzeit mit dem Data Act (DA). Dieser befindet sich allerdings noch in einer recht frühen Phase des Gesetzgebungsverfahrens und wird nicht vor 2024 in Kraft treten. Der Grundgedanke des Data Act liegt darin, bislang weitgehend ungenutzte Potenziale von Daten auszuschöpfen und dadurch die europäische Wirtschaft zu fördern.

Zu diesem Zweck verpflichtet der DA Unternehmen dazu, ihre eigenen Daten zugänglich zu machen und Dritten zur Verfügung zu stellen. Dabei geht es in erster Linie nicht um personenbezogene Informationen, sondern um Maschinendaten, insbesondere aus Industrieanlagen, medizinischen Geräten, IoT- oder Smart-Home-Prozessen. Gerade kleine und mittlere Unternehmen (KMU) können auf solche Daten bislang nicht zugreifen oder sie zusammenführen, wodurch ihnen erhebliche Wettbewerbsnachteile bei der Entwicklung innovativer Geschäftsfelder entstehen.

Daten vergesellschaften

Der Data Act regelt zahlreiche, noch nicht abschließend diskutierte Voraussetzungen, unter denen Unternehmen verpflichtet werden können, ihre Informationen zu teilen. Zugleich soll er festlegen, wer unter welchen Umständen auf diese Daten zugreifen darf. Das können auch öffentliche Stellen sein, sofern sie ein erhebliches Interesse nachweisen, etwa im Rahmen der Bekämpfung einer Pandemie. Der DA soll so eine Art „freien Datenmarkt“ für nicht-personenbezogene Nutzungsdaten schaffen, auf dem diese gehandelt und weitergeben werden. Unter bestimmten Voraussetzungen sollen auch Vergütungen fließen.

Die Unternehmen, bei denen die begehrten Daten entstehen und in deren Rechte eingegriffen werden soll, reagieren nicht gerade begeistert auf den Vorstoß der EU-Kommission. So kritisiert beispielsweise der Bundesverband der Deutschen Industrie (BDI) in einer Stellungnahme bereits den Ansatz der Regulierung im DA. Man zweifele an der „Notwendigkeit eines solchen breit gelagerten Eingriffs in die Grundprinzipien der Datenwirtschaft in noch jungen Märkten”.

Die Kommission hält den Eingriff jedoch für notwendig, damit die europäische Wirtschaft mithilfe eines solchen Datenbinnenmarkts wettbewerbsfähig gegen eine sich rasant entwickelnde internationale Konkurrenz bleibt. Wie weit der Data Act jedoch in seiner finalen Form gehen wird, ist angesichts des langen Weges durch die Mühlen der europäischen Gesetzgebung noch offen.

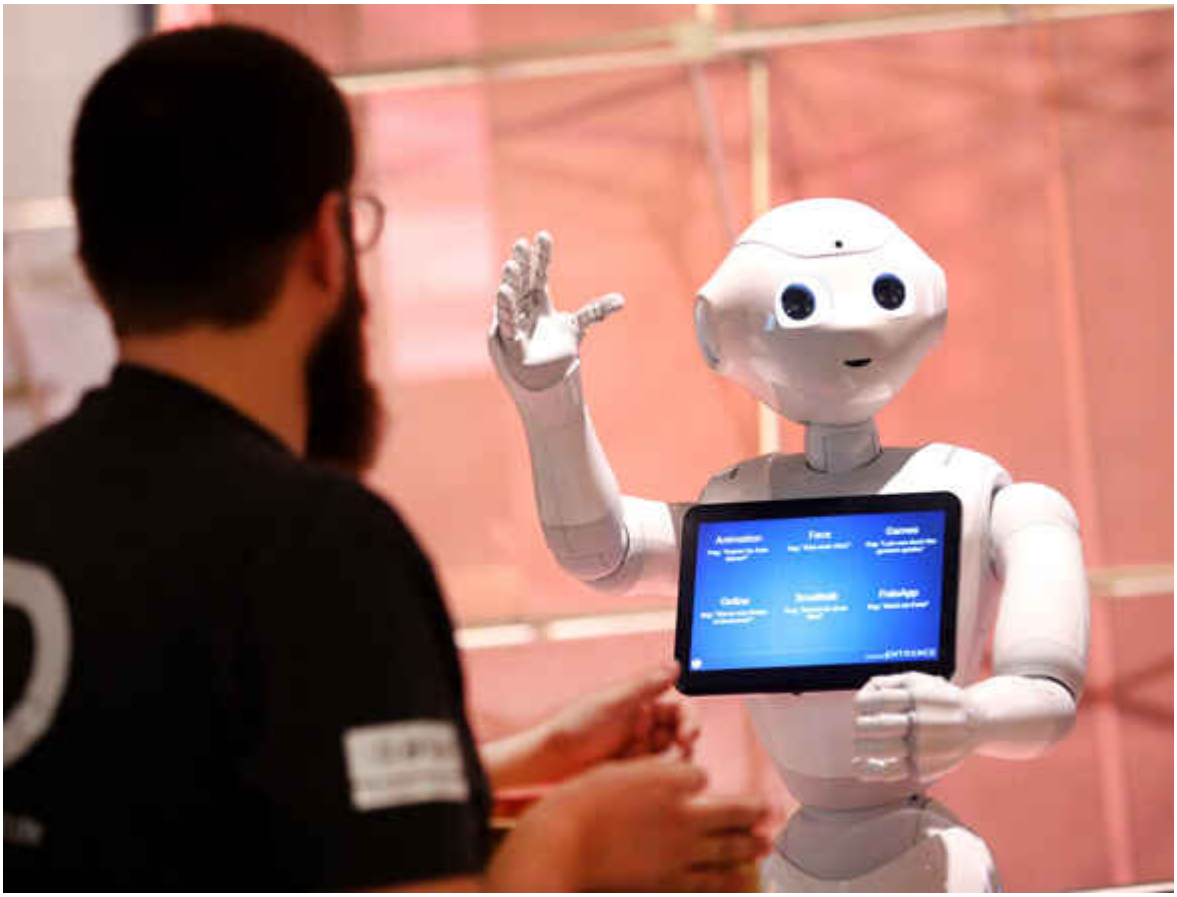
KI im Zaum halten

Erwähnenswert ist in diesem Zusammenhang auch der Artifical Intelligence Act, der ebenfalls noch in einer sehr frühen Phase der Gesetzgebung hängt und nicht vor 2024 zu erwarten ist. Der AI Act soll einen europaweit einheitlichen rechtlichen Rahmen schaffen, in dem Unternehmen und

Institutionen sichere und vertrauenswürdige Systeme mit künstlicher Intelligenz entwickeln und einsetzen.

Im Kern der vorliegenden Fassung steht dabei ein Stufensystem, das die KI-Anwendungen in verschiedene Risikoklassen mit daraus resultierenden Vorgaben einteilt. In die strengste Kategorie des „Inakzeptablen Risikos“ fallen vier Praktiken, die der Gesetzgeber als klare Bedrohung bewertet und grundsätzlich verbietet.

Hierzu gehören Social Scoring, also die „Klassifizierung der Vertrauenswürdigkeit natürlicher Personen auf der Grundlage ihres sozialen Verhaltens“ ebenso wie das sogenannte Nudging, die unterschwellige Beeinflussung einer Person außerhalb des Bewusstseins. Ebenfalls verbieten wollen die Initiatoren das „Ausnutzen der Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund ihres Alters oder ihrer Behinderung“. Zumindest teilweise wollen sie außerdem untersagen, biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zur Strafverfolgung zu nutzen. Erstaunlicherweise nicht in dieser Gruppe finden sich naheliegende Bedrohungen durch autonome Waffensysteme, die ihre Ziele mithilfe von künstlicher Intelligenz auswählen.



Der AI Act teilt KI-Systeme in Risikostufen ein und verbietet künftig beispielsweise deren Einsatz beim Social Scoring. *Bild: Roland Weihrauch/dpa*

Anwendungen, die als potenziell bedrohlich eingestuft werden, fallen in die Kategorie „Hohes Risiko“. Nutzt jemand Algorithmen für derartige Bereiche, so muss er zahlreiche Voraussetzungen erfüllen und die Sicherheit der Anwendung nachweisen. Hierzu zählt etwa, natürliche Personen biometrisch zu identifizieren und zu kategorisieren, ferner die Strafverfolgung, die Rechtspflege sowie die Verwaltung und der Betrieb kritischer Infrastrukturen.

Für Angebote im Bereich des „begrenzten Risikos“ gelten vor allem Transparenzverpflichtungen. Hierunter fallen zum Beispiel Chatbots, die dann als solche gekennzeichnet werden müssen. Nutzer sollen informierte Entscheidungen treffen können, ob sie diese Angebote nutzen wollen. Nicht reguliert werden KI-gestützte Prozesse mit „minimalem Risiko“ wie KI-gestützte Videospiele oder Spamfilter, da von ihnen nur eine geringe Gefahr für die Sicherheit und Rechte der Nutzer

ausgehe.

Der AI Act sieht in seinem derzeitigen Stadium weiterhin vor, dass die von einer KI getroffenen Entscheidungen „transparent und fair“ sein müssen. Das könnte in einigen Bereichen, in denen etwa Deep Neural Networks zum Zuge kommen, sehr schwierig werden, weil die trainierten Netzwerke zum Teil Tausende Variablen einbeziehen. Aber auch bei diesem Entwurf kann es noch zu erheblichen Änderungen im Rahmen des Gesetzgebungsverfahrens kommen.

Fazit

Die Grundgedanken der ambitionierten Datenstrategie der EU-Kommission sind nachvollziehbar und im Grundsatz auch sinnvoll. Die Liste von geplanten oder bereits umgesetzten Gesetzen ist sogar noch weitaus länger als hier dargestellt.

Es ist allerdings fraglich, ob man ein hochgradig disruptives und dynamisches Umfeld tatsächlich einer so weitgehenden staatlichen Regulierung unterwerfen und diese mit den Rechten von Bürgern und Unternehmen in Einklang bringen kann. Ungeklärt ist beispielsweise das Verhältnis der DSGVO zu den vielen neuen Acts, denen ein allzu rigider Datenschutz in vielen Bereichen im Weg stehen wird. Schließlich ist es ja ein Ziel der Regulierungen, die internationale Wettbewerbsfähigkeit der europäischen Wirtschaft zu verbessern, indem man ihr den Zugang zu Daten erleichtert. Zudem überschneiden sich viele der neuen Grundverordnungen in zahlreichen Punkten. Zu befürchten ist daher, dass ein regulatorisches Dickicht entsteht, welches auf Jahre zu einer großen Rechtsunsicherheit führt. *(hag@ct.de)*

Die wichtigsten EU-Gesetzesinitiativen	
Name	Wichtigste Regelungen
Digital Markets Act (DMA)	– reguliert den Wettbewerb und insbesondere große Unternehmen – verpflichtet Gatekeeper zu fairem Wettbewerb – fordert Interoperabilität zwischen Anbietern (Messenger)
Digital Services Act (DSA)	– verlangt sicheren digitalen Raum ohne rechtswidrige Inhalte – fordert von Onlinemarktplätzen eine Überwachung der Angebote – verbietet bestimmte Werbepraktiken, etwa gezielte Ansprache von Kindern
Data Governance Act (DGA)	– reguliert Verfügbarkeit von Daten für den öffentlichen Sektor – schafft Basis für Datenvermittlungsdienste und Datenaltruismus
Data Act (DA)	– fördert die Wirtschaft durch stärkere Datennutzung – regelt Voraussetzungen, unter denen Firmen ihre Daten teilen müssen – strebt einen freien Datenmarkt für nicht-personenbezogene Daten an
Artificial Intelligence Act (AIA)	– reguliert den Rahmen und die Entwicklung künstlicher Intelligenz – teilt KI-Anwendungen in Risikoklassen mit bestimmten Beschränkungen ein

Datenstrategie der EU-Kommission: ct.de/ynr9

Widersprüchliche Ratschläge zur Google-Fonts-Einbindung

Markt + Trends | IT-Recht & Datenschutz

Widersprüchliche Ratschläge zur Google-Fonts-Einbindung

Zur aktuellen Abmahnwelle wegen der datenschutzrechtswidrigen Einbindung dynamischer Google Fonts auf Webseiten hat sich

jüngst die Datenschutzbehörde aus Niedersachsen zu Wort gemeldet. Sie empfiehlt auf die dynamische Einbindung zu verzichten, die benötigten Schrifttypen (Fonts) herunterzuladen und auf dem eigenen Server zum Abruf vorzuhalten. Hierdurch wird eine Übermittlung personenbezogener Daten von Internetnutzern in die USA, etwa deren IP-Adresse, vermieden.

Google hat unterdessen ein FAQ zur Verarbeitung von Nutzerdaten im Zusammenhang mit dem Bezug von Schriftarten von Google-Servern veröffentlicht. Der Konzern vertritt die Ansicht, dass die übermittelten Daten bei dynamischer Fonts-Einbindung ausschließlich für die Bereitstellung der Schriften verarbeitet werden. Eine Verarbeitung für Zwecke der Analyse oder Werbung erfolge nicht. Ob dies allerdings helfen könne, sich gegen Abmahnungen erfolgreich zu verteidigen, wie Google schreibt, ist unsicher. Im Januar 2022 hatte das Landgericht München I einem Kläger Schadenersatz wegen der datenschutzrechtswidrigen Google-Fonts-Einbindung zugesprochen und so die Abmahnwelle losgetreten. *Tobias Haar* (ur@ix.de)

Abmahnwelle wegen Google Fonts

Bettelbriefe

Abmahnwelle wegen Google

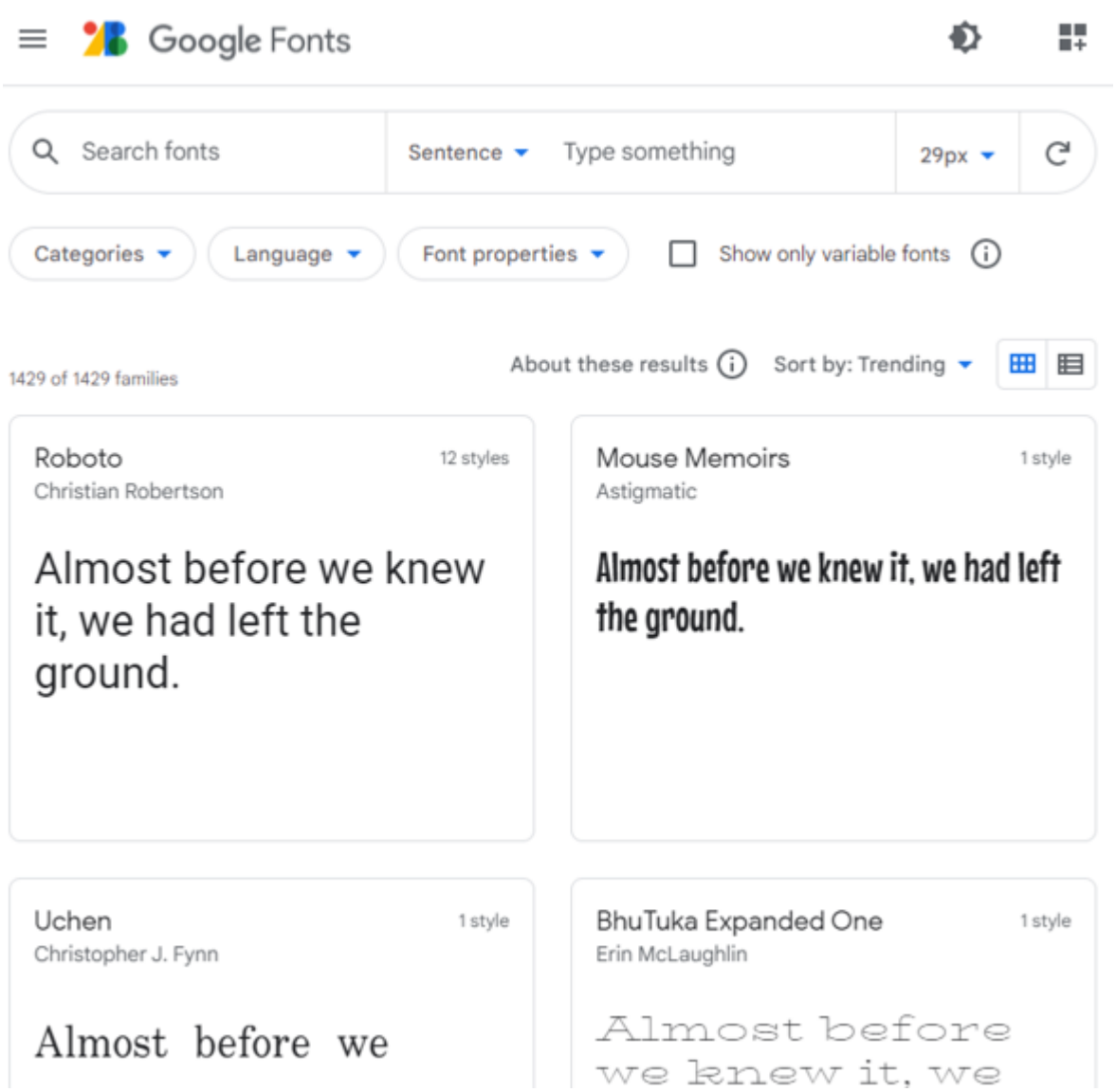
Fonts

Tausende von Empfängern staunen derzeit über Forderungsschreiben, die sie im E-Mail-Postfach oder im Briefkasten vorfinden. Weil sie Googles kostenlose Fonts in ihre Websites eingebettet haben, sollen sie 100 bis knapp 500 Euro berappen. Was steckt hinter diesen Schreiben und wie wehrt man sich dagegen?

Von Joerg Heidrich

Adressaten der Schreiben sind allesamt Website-Betreiber. Die Abmahnungen werfen ihnen einen „unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht“ und einen Verstoß gegen die Datenschutz-Grundverordung (DSGVO) vor. Ihr Vergehen: Sie nutzen auf ihrer Webseite Fonts, die Google kostenlos anbietet.

Dabei handelt es sich um ein Verzeichnis von mehreren Hundert frei verwendbarer Schriftarten. Website-Betreiber können die Schriftarten herunterladen und lokal auf dem eigenen Webserver bereitstellen. Alternativ dazu können sie die Schriften auch online einbinden. Dies führt dann dazu, dass der Browser des Besuchers sie beim Aufruf einer Seite von den Servern des US-Konzerns lädt. Und das ist ein Problem.



Google Fonts hält viele kostenlose Schriftarten bereit – die aber lokal eingebunden werden sollten.
Das Landgericht (LG) München hatte im Januar 2022 die Online-Nutzung von Google Fonts mit der Begründung verboten, dass dabei unerlaubt personenbezogene Daten an Google in die USA weitergegeben werden (Az. 3 O 17493/20). Diese Entscheidung bildet die Grundlage für die versandten Abmahnungen und Forderungsschreiben.

Es handele sich bei den übermittelten dynamischen IP-Adressen um Informationen, so die Münchener Richter, die in den Schutzbereich des Datenschutzes fallen. Der Seitenbetreiber habe das Recht des Klägers auf informationelle Selbstbestimmung verletzt, indem er die dynamische IP-Adresse des Besuchers beim Aufruf der Seite an Google weiterleitete. Hierfür habe es keine Rechtsgrundlage in Form einer

Einwilligung oder eines berechtigten Interesses gegeben. Dem Kläger stehe somit ein Unterlassungsanspruch zu.

Doch damit nicht genug hatte das LG München dem Besucher der Website noch einen Schadensersatzanspruch in Höhe von 100 Euro zugebilligt. Ein solcher Anspruch kann sich aus Artikel 82 der DSGVO ergeben und steht jeder Person zu, „der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist“. Hoch umstritten ist dabei die Frage, welche Intensität ein solcher Eingriff haben muss, um ein Schmerzensgeld auszulösen. In der juristischen Diskussion wird die Entscheidung aus München überwiegend als überzogen kritisiert.

„Individuelles Unwohlsein“

Die Richter sahen im vorliegenden Fall bereits durch die Übermittlung an Google einen „Kontrollverlust“ des Betroffenen und ein „individuelles Unwohlsein“. Denn Google sei bekannt dafür, Daten über seine Nutzer zu sammeln. Zudem sei es unstreitig, dass die IP-Adresse an einen Server in den USA übermittelt werde, wo kein angemessenes Datenschutzniveau gewährleistet sei.

Diese Argumentation machen sich jetzt die Schreiber der fordernden Briefe zu eigen. Man habe die Website des Empfängers besucht, dieser verwende die Online-Version der Google Fonts und solle daher wegen des dadurch verursachten individuellen Unwohlseins schnellstens 100 Euro an den Versender überweisen.

Etwas komplizierter wird es, wenn das Schreiben von einem Anwalt kommt. Offenbar haben juristische Veteranen vergangener Massenabmahnungen ein neues Tätigkeitsfeld gefunden. Sie fordern nicht nur, dass die Empfänger den Schaden ihrer Mandanten begleichen. Sie sollen zudem eine Unterlassungserklärung für die Nutzung der Google-Fonts abgeben – und die Anwaltsgebühren zahlen, meist in Höhe von

367,23 Euro.

Gerade gegen die anwaltlichen Abmahnungen gibt es allerdings eine ganze Reihe von potenziellen Einwendungen, sodass es sich dabei keinesfalls um „sichere Fälle“ für die Abmahner handelt. Es spricht bereits einiges dafür, dass die Anwaltsschreiben rechtsmissbräuchlich sind, da die angeblichen Betroffenen die Websites vorsätzlich angesteuert haben dürften. Trotzdem sollten zumindest juristische Laien in diesen Fällen vorsichtshalber einen IT-Anwalt ins Boot holen.

Weniger riskant ist dagegen die Abwehr von Aufforderungsschreiben, die nicht von einem Anwalt kommen. Denn nach derzeitigem Stand ist es eher unwahrscheinlich, dass die Mehrheit der Gerichte den Ansichten des LG München hinsichtlich der Zahlung einer Geldentschädigung folgen. Es spricht daher einiges dafür, dass man derartige Schreiben ignorieren darf. Allerdings sollte jeder Website-Betreiber auf die lokal gehostete Version von Google Fonts umsteigen. (*jo@ct.de*)

Urteil des LG München: ct.de/yjub

https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-B-2022-N-612?hl=true