Medienimpulse
ISSN 2307-3187
Jg. 56, Nr. 2, 2018

Hoch geschätzt und viel gescholten: Plädoyer für die Datenschutz-Grundverordnung der EU

Herbert Gnauer

Die Datenschutz-Grundverordnung der EU reguliert Fragen des Datenschutzes. Der Beitrag widmet sich Herausforderungen und Problemstellungen, die durch Digitalisierung, Big Data und Machine Learning für den Datenschutz entstanden sind und geht der Frage nach, inwiefern die DSGVO eine Antwort darauf ist …

The Central Data Protection Regulation of the EU governs issues related to data protection. This article discusses the challenges and problems that have arisen for data protection from digitalization, big data and machine learning, and addresses the question of the extent to which the GDPR provides a solution …

I. Wie es begann - die lange Vorgeschichte

Laut Duden sind Daten durch Beobachtung, Messung oder (statistische) Erhebung gewonnene Werte. Dergleichen geschah wohl schon in prähistorischen Zeiten: Wechsel von Tag und Nacht, Mondphasen und Jahreszeiten waren seit jeher von großer Bedeutung, aufbauend auf ihrer Beobachtung dürften bereits steinzeitliche Kulturen erste Kalender entwickelt haben. Spätestens mit dem Aufkommen eines geldbasierten Handels wurde die Erfassung und Auswertung von Daten zur alltäglich geübten Praxis: Listen wurden geführt, Register angelegt, Werte berechnet und miteinander verglichen. Erste Ansätze einer Buchführung finden sich mehrere Jahrtausende vor unserer Zeitrechnung in Mesopotamien. Ab dem Mittelalter trat die doppelte Buchführung von Italien ausgehend ihren Siegeszug an, ein System, das seinem Prinzip nach bis heute mehr oder minder unverändert im Einsatz ist [1].

Ein markanter Punkt in der Entwicklung war die Entstehung von Adressbüros und sogenannten Fragämtern zu Beginn des 17. Jahrhunderts [2]. Die ersten wurden in Paris und London eingerichtet. Zunächst dauerte es einige Jahrzehnte, bis sich die Idee, vorerst noch etwas zögerlich, dann immer rascher über den europäischen Kontinent zu verbreiten begann. Ab diesem Zeitpunkt war der Handel mit Daten verschiedenster Art zum institutionalisierten Geschäftsfeld geworden. Personenbezogene Daten waren dabei stets von besonderem Interesse. Schon früh wurden nicht nur Geburt und Tod von Menschen verzeichnet, sondern auch ihre Vermögensverhältnisse, Wohnorte, familiäre Verbindungen und vieles mehr. Doch solange die Aufzeichnungen auf physischen Medien wie Tontafeln oder später Pergament und Papier erfolgten, hielten sich die Möglichkeiten des Austausches und der Auswertung in engen Grenzen. Auch die Aktualisierung vorhandener Datenbestände bereitete Mühe, oft hinkten die Aufzeichnungen der Realität hoffnungslos hinterher.

Doch all diese Beschränkungen fielen mit Anbrechen des sogenannten digitalen Wandels praktisch über Nacht weg. In atemberaubendem Tempo schritt die technologische Entwicklung in den Jahren ab 1990 voran. Speichermedien und Computer wurden immer kleiner und erreichten bald Geschwindigkeiten, von denen selbst kühnste Geister kurz zuvor nicht einmal zu träumen wagten. Neue Kommunikationswege und -formen entstanden, mit einem Mal eröffnete sich eine Fülle ungeahnter Einsatzmöglichkeiten. Big Data und Machine Learning lassen leicht vergessen, dass Computer im Grunde unverändert auf Konzepten basieren, die vor rund 70 Jahren erdacht wurden [3], [4]. Dessen ungeachtet ist längst noch kein Ende abzusehen. Doch mit den Möglichkeiten wuchsen auch die Herausforderungen und Problemstellungen. Bald wurde klar, dass Regulierung nottut.

II. Um welche Daten geht es hier?

Insbesondere personenbezogene Daten wurden zu Recht als schutzwürdig erkannt. Darunter werden Informationen verstanden, die mit einer konkreten Person verbunden sind. Geläufige Beispiele sind Name, Geburtsdatum, Adresse, Sozialversicherungsnummer, E-Mail-Adresse oder Telefonnummer. Aber auch KFZ-Kennzeichen, IP-Adressen, Fotos, Stimmaufnahmen oder Kontonummern können dazu zählen, sofern sie auf konkrete Personen rückführbar sind. Das gilt selbstverständlich ebenso für zahlreiche höchst sensible Informationen, etwa medizinische Befunde, Strafregistereinträge, Angaben zur religiösen Ausrichtung, sexuellen Orientierung, politischen Überzeugung, nicht zu vergessen biometrische oder genetische Daten, die Liste ist fast beliebig erweiterbar. Das Kriterium ist stets die Verknüpfung mit konkreten Personen.

Durch Anonymisierung können persönliche Daten in 'normale' Daten umgewandelt werden, die keinem besonderen Schutz mehr unterliegen. Von echter Anonymisierung (Löschen aller Angaben, die eine Rückführung erlauben) wäre noch die häufig vorgenommene

Pseudonymisierung zu unterscheiden. Hier werden z.B. Namen durch Kennzahlen ersetzt, die aber zu einem späteren Zeitpunkt problemlos wieder mit den ursprünglichen Namen in Verbindung gebracht werden können. Diese Methode wird häufig angewandt und soll auch in Zusammenhang mit der Weitergabe von Daten aus dem österreichischen Gesundheitsbereich zum Einsatz kommen, betroffen sind unter anderem Daten der Elektronischen Gesundheitsakte ELGA.

Ganz ohne Zweifel ist es wünschenswert, dass (nicht nur) von öffentlichen Stellen generierte Datenbestände für Wissenschaft und Forschung zugänglich gemacht werden. Doch dessen ungeachtet hätte man immerhin erwarten dürfen, dass zumindest die einfachsten Erfordernisse zum Schutz persönlicher Daten der Bevölkerung erfüllt werden, was aber leider nicht der Fall ist.

In den Stellungnahmen zum Entwurf des Datenschutz-Anpassungsgesetzes 2018 – Wissenschaft und Forschung [5] findet sich die Stellungnahme der Bayer Austria Gesellschaft m.b.H. [6], in der unumwunden gefordert wird, die gesamte Pharmabranche als solche explizit in die Liste potenzieller Empfänger von Datentransfers aufzunehmen (§2 Z 14 'Wissenschaftliche Einrichtungen') und in den Erläuterungen die Einschränkung 'akademisches Wissen' auf 'Wissen' zu erweitern (§ 2 Z 13 'Technologietransfer'). Ganz offenkundig möchte man den direkten Zugriff auf die Gesundheitsdaten beizeiten sicherstellen. Wird dem stattgegeben, wäre ihre Verwendung für kommerzielle Zwecke nicht mehr auszuschließen.

Doch der Reihe nach: November 1978, vor bald 40 Jahren, bekam Österreich ein Datenschutzgesetz, das 1999 zum DSG 2000 ausgebaut und 2005 abermals grundlegend überarbeitet wurde [7]. Mit der Novelle 2013 wurde die ursprünglich als Dienststelle des Bundesministeriums für Inneres (BMI) konzipierte Datenschutzkommission ausgelagert und zur eigenständigen, weisungsfreien Datenschutzbehörde (DSB) [8] umgeformt.

III. Von der Richtlinie zur Verordnung

Die Wege der Daten kennen heute keine Grenzen mehr, weshalb nationale Regelungen nur beschränkt wirksam bzw. sinnvoll sind. Schon ab Mitte der 1970er Jahren wurde nachgedacht, wie die BürgerInnen der damaligen Europäischen Gemeinschaft (EG) vor Missbrauch bei Speicherung und Verarbeitung persönlicher Informationen geschützt werden könnten. Doch vorläufig war das Bewusstsein in vielen Mitgliedsländern noch recht schwach ausgeprägt, ein erstes Datenschutzübereinkommen wurde vielerorts nicht oder nur mangelhaft umgesetzt. So kam es erst 1995, rund 20 Jahre später, nach mehreren Zwischenschritten zur Richtlinie der EG zum Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten [9]. In ihr wurden erstmals Mindeststandards festgelegt, die von allen Staaten der EG einzuhalten waren und 2009 bei der Umformung zur Europäischen Union (EU) übernommen wurden. Zweifellos zumindest ein Fortschritt auf dem langen Weg zu einem vernünftigen Umgang mit Information.

Angesichts der rasanten technischen Entwicklung sind Regelwerke stets in Gefahr, von der Realität überholt zu werden und bedürfen laufender Anpassung an immer neue Gegebenheiten. Daran hat sich bis heute nichts geändert und es wird auch noch längere Zeit dabei bleiben, womöglich für mehrere Generationen. Daher wäre es keine Option, auf das Eintreten eines Status Quo zu hoffen, um die Dinge dann ein für alle Mal zu regeln. Das ist im Grunde nichts Neues, sondern verhält sich in sehr vielen Rechtsbereichen so. Die Datenschutzrichtlinie machte hier, wenig überraschend, keine Ausnahme.

Im nächsten Anlauf wollte man sinnvollerweise einen Schritt weitergehen und die Richtlinie, die in den einzelnen Ländern mitunter sehr unterschiedlich umgesetzt worden war, durch eine EU-weit gültige Verordnung ersetzen. Gleichzeitig wurde durchaus mit bestem Willen versucht, auf die laufende technologische Entwicklung einzugehen und

zeitgemäße Regelungen zu finden. Doch wenn es um hohe Gewinne geht, kommen schnell äußerst divergente Interessen ins Spiel. Und hohe Gewinne sind hier zu erwarten, immerhin stellt der Handel mit Daten derzeit eines der lukrativsten Geschäftsfelder dar. Ein zu strenger, bzw. aus Sicht vieler Konzerne zu sehr am Schutz der Person orientierter Datenschutz könnte hinderlich wirken, das augenblicklich gepflogene 'Anything goes' ein jähes Ende finden. Denn so manche Big Data Anwendung wäre wohl schneller von Verboten bedroht, als die Investition sich rentieren kann. Von der laufenden Entwicklung mit all ihren renditeversprechenden Zwischenerfolgen ganz zu schweigen.

So kam es nach längeren Verhandlungen Ende April 2016 zu einem Kompromiss, der einigen zu weit ging, anderen zu wenig weit: Die Datenschutz-Grundverordnung (DSGVO) [10], [11] wurde beschlossen, trat wenige Wochen später am 24. Mai desselben Jahres in Kraft und mit 25. Mai 2018 in Geltung. Was nichts anderes heißt, als dass sie nach einer zweijährigen Übergangsfrist nun anzuwenden ist. Im Gegensatz zu einer Richtlinie bedarf eine Verordnung keiner nationalen Umsetzung, sondern ist ab dem Stichtag automatisch in allen Mitgliedsländern der EU gültig (vielmehr müssen vorhandene nationale Gesetze ggf. angepasst werden, wenn sie der Verordnung nicht entsprechen). Außerdem geben sogenannte Öffnungsklauseln den Ländern Spielraum für Ausgestaltung. Diese Freiräume wurden in Österreich zunächst kaum genutzt, im Datenschutz-Anpassungsgesetz 2018 wird in der Fassung von Juli 2017 [12]) wenig Gebrauch davon gemacht. Erst ein Jahr später sollten die Dinge hierzulande eine überraschende Wende erfahren, auf die noch näher einzugehen sein wird.

IV. Was ist nun neu daran?

Aus österreichischer Sicht hat sich mit Inkrafttreten der DSGVO eigentlich nicht allzu viel geändert. Die meisten Bestimmungen waren schon seit Jahren im DSG 2000 enthalten und sind seit geraumer Zeit in Geltung.

Das gilt insbesondere auch für die verlangte aktive Zustimmung zur Speicherung von E-Mail-Adressen, die zuletzt für viel Aufregung sorgte. Unerwünschte Zusendung von Werbung ist hierzulande schon seit vielen Jahren verboten, nur wurde bislang darauf wenig bis gar nicht geachtet. Bereits vor dem 25. Mai 2018 erteilte Einwilligungen behalten übrigens weiterhin ihre Gültigkeit, sofern sie dokumentiert sind.

So waren auch die zahllosen Mails, die schon seit April so manche Mailbox täglich aufs Neue füllten, teils unnötig, teils falsch. Ersteres, wenn eine Einwilligung bereits gegeben und selbige belegbar war. Diese Mails machten vermutlich den geringsten Anteil aus. Zumeist wurde man in Kenntnis gesetzt, Mitglied irgendeines E-Mail-Verteilers zu sein und belehrt, dass man nichts weiter zu tun habe, falls man es dabei belassen wolle. Das war natürlich völlig falsch, denn die DSGVO fordert aktive Zustimmung, nicht passive Duldung. Die allerwenigsten taten dem Genüge und versandten ein Link mit der Bitte, man möge die Subskription per Klick bestätigen. Diese wenigen Braven wurden von mir, ungeachtet ihrer Relevanz, durchwegs mit solidarischer Zustimmung belohnt, was aber nur drei oder viermal der Fall war.

Jene Mails, die DSGVO-Konformität bloß heuchelten, verfügten oftmals über ein Link, das vorgab, unerwünschte Mitgliedschaften unverzüglich zu beenden. Doch fast immer trog die Hoffnung, wer darauf klickte, wird meist bis heute unverändert mit allerlei obskuren Informationen versorgt. Man sollte sich hier keine allzu romantischen Vorstellungen machen. Sollte es je gelingen, das Phänomen Spam aus der Welt zu schaffen, wird es jedenfalls noch Jahre dauern. Bis dahin können Spamfilter gute Dienste tun.

Doch ungeachtet solcher Misslichkeiten ist die DSGVO als wichtiger Schritt in die richtige Richtung zu sehen, wenn auch in mancher Hinsicht nicht weitgehend genug.

Neu sind vor allem die hohen Strafrahmen, mit denen dem Datenschutz tatsächlich zum Durchbruch verholfen werden könnte: 10 Millionen Euro (oder 2% Prozent des globalen Umsatzes) Höchststrafe für Vergehen bei

administrativen Tätigkeiten, bis zu 20 Millionen Euro (oder 4% des globalen Umsatzes) bei grundsätzlichen ethischen Vergehen. Das klingt dramatisch und ist es auch. Allerdings sind es nicht KMUs und Kulturvereine, die hier im Fokus stehen, sondern finanzkräftige, meist international tätige Konzerne. Wie anders wäre Unternehmen dieser Liga beizukommen, als durch Strafdrohungen in einer für sie ernstzunehmenden Höhe? Überdies handelt es sich um das obere Limit des Strafrahmens, der nur ausgeschöpft wird, wenn es auch angemessen scheint.

Davon abgesehen sind die Datenschutzbehörden und sonstigen Kontrollinstanzen nicht nur in Österreich mit eher dürftigen Kapazitäten ausgestattet. Jedem Verdachtsfall nachzugehen und eine Prüfung einzuleiten bleibt bis auf Weiteres weit jenseits der Möglichkeiten. Vorerst wird man sich damit begnügen müssen, streng nach Priorität vorzugehen. Wobei wohl auch damit zu rechnen ist, dass dabei in einigen Ländern mehr, in anderen weniger Eifer an den Tag gelegt wird.

Eine weitere wichtige Neuerung besteht darin, dass im Fall von Beschwerden nun die Datenschutzbehörde frei gewählt werden kann. Max Schrems wird daher künftig nicht mehr nach Irland pilgern müssen, wenn er mit seiner Datenschutz-Plattform NOYB ("none of your business") [13] gegen Facebook zu Felde zieht. Ein großer Fortschritt angesichts des Umstandes, dass die irische DSB erfahrungsgemäß ausgesprochen konzernfreundlich agiert. Bislang wurde dort den Anliegen von NutzerInnen jedenfalls keine allzu große Bedeutung beigemessen. NOYB hat von dieser Möglichkeit bereits Gebrauch gemacht und am 25. Mai, nur wenige Minuten nach Mitternacht, zeitgleich bei vier Behörden Beschwerden gegen Google, Instagram, WhatsApp und Facebook eingebracht. Dem Vernehmen nach dürfte er zumindest in Wien durchaus auf offene Ohren gestoßen sein.

Neu eingeführt wurde auch die Position der Datenschutzbeauftragten. Behörden und öffentliche Stellen sind, mit Ausnahme von Gerichten die im Rahmen ihrer justiziellen Tätigkeit handeln, zur Benennung von Datenschutzbeauftragten verpflichtet. Die Verpflichtung besteht unter

anderem, wenn die Kerntätigkeit eines Unternehmens oder einer Institution die Überwachung von Personen erforderlich macht. Das gilt insbesondere, wenn sensible Informationen, etwa über strafrechtliche Verurteilungen, rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten zur Identifizierung einer Person im Spiel sind. Solche Daten dürfen nur unter bestimmten Umständen verarbeitet werden, etwa zu medizinischen Zwecken, zum Schutz lebenswichtiger Interessen Dritter oder zur Geltendmachung von Rechtsansprüchen. Auch wenn das explizite Einverständnis der betroffenen Person vorliegt, dürfen Daten dieser besonderen Kategorien verarbeitet werden. Datenschutzbeauftragte können entweder Angestellte des betreffenden Betriebes oder externe MitarbeiterInnen sein. Sie haben sowohl beratende (z.B. in Zusammenhang mit Datenschutz-Folgenabschätzungen) als auch kontrollierende Funktion. Im Fall von Fragen oder Prüfungen fungieren sie als Anlaufstellen der zuständigen Datenschutzbehörde.

V. Wer ist betroffen und was ist zu tun?

Grundsätzlich regelt die DSGVO den Umgang mit personenbezogenen Daten vor allem in professionellem bzw. gewerblichem Zusammenhang. Private Nutzungen sind außer Obligo, solange nicht missbräuchliche Weitergabe bzw. Verwendung oder Veröffentlichung im Spiel sind. Adressverzeichnisse privat genutzter E-Mail-Programme, Gästelisten, Notizen, Tagebücher und dergleichen sind weiterhin unproblematisch, sofern nicht einer der eben genannten Fälle vorliegt. Selbst dann wird oftmals eher das Recht auf das eigene Bild oder auf Wahrung der Privatsphäre schlagend als die DSGVO.

Inwieweit BetreiberInnen von Internetmedien wie Blogs oder Youtube-Channels den Status als Privatperson für sich in Anspruch nehmen können, wird im Einzelfall zu entscheiden sein. Wird zu Spenden oder Crowdfunding aufgerufen, sind Gegenstände oder Leistungen gegen Geld angeboten, ist daran zu zweifeln. Auch Sponsoring oder Monetarisierung

von Youtube-Videos dürfte sich als problematisch erweisen, selbst wenn dabei bloß geringe Beträge lukriert werden sollten. Die Gewinnabsicht wird bei der Beurteilung sicher eine Rolle spielen.

EinzelunternehmerInnen, Vereine, ARGEs und andere kleine Körperschaften sind von der DSGVO in jedem Fall betroffen. Allerdings ist der Aufwand für EPUs und kleinere Institutionenbei weitem nicht so hoch, wie vielfach angenommen wird [14]. Entgegen einem weit verbreiteten Irrglauben sind auch keine teuren IT-Lösungen nötig, der Dokumentationspflicht kann ebenso gut auch mittels Bleistift und Papier nachgekommen werden. Auch hier gab es eigentlich keine Änderung, alle Lösungen, die seit dem 25. Mai 2018 als nicht DSGVO-konform gelten, waren in Österreich schon seit Jahren illegal.

Zur Beurteilung der eigenen Situation ist es wichtig, sich klarzumachen, welche Daten gespeichert sind, woher sie stammen und für welche Zwecke sie verwendet werden sollen. Daraus lässt sich die vorgeschriebene Datenschutz-Folgenabschätzung ableiten. Bezüglich der Herkunft von Daten ist es von Bedeutung, dass die betroffenen Personen davon wissen und damit einverstanden sind. Im Rahmen von Geschäftsverhältnissen ergibt sich das oftmals implizit. Im Zweifel sollte man betroffene Personen sicherheitshalber informieren, welche Informationen man über sie zu welchem Zweck gespeichert hat und ihre Zustimmung einholen.

Nebstbei bemerkt fallen auch Aufzeichnungen auf Papier unter die DSGVO, sofern sie systematisch erfasst und strukturiert, beispielsweise in der Art von Akten abgelegt sind. Weitere Details sind dem Leitfaden der österreichischen Datenschutzbehörde [15] sowie den Informationen der österreichischen Wirtschaftskammer zur DSGVO [16] zu entnehmen.

VI. Kritikpunkte

Die DSGVO ist keineswegs ein monströses Ungetüm, wie vielfach behauptet wird. Ganz im Gegenteil ist sie gemessen an der komplexen Thematik sogar sehr schlank gehalten. Zu schlank, wie viele JuristInnen

meinen, denen einige Punkte nicht genau genug definiert erscheinen. So wäre es beispielsweise sinnvoll gewesen, die verpflichtende Datenschutz-Folgenabschätzung mit Vorgaben auszustatten. Wohl aufgrund der Vielzahl höchst unterschiedlicher Anwendungsfälle, die jeweils andere Erfordernisse mit sich bringen, wurde das bewusst offen gehalten. Dennoch hätten einige Eckpunkte genauer bestimmt und festgelegt werden können.

Vieles ist vage und unklar, die genauere Ausdeutung wird der Judikatur überlassen. Das schafft Unsicherheit. Andrerseits bringt es die Möglichkeit, sich unter Berücksichtigung laufender Erfahrungen Schritt für Schritt voran zu tasten. Vielleicht kann so jene Flexibilität erhalten werden, die nötig ist, um mit dem schnelllebigen Umfeld technologischer Entwicklung mitzuhalten. Künftige Innovationen sind unvorhersehbar, vielleicht tritt schon morgen ein sogenannter 'Game Changer' auf den Plan? In den letzten Jahrzehnten waren wir nicht selten mit Veränderungen konfrontiert, die völlig unerwartet eintraten und den Dingen eine jähe Wendung gaben. Nicht selten wurde der Vorwurf erhoben, die Justiz reagiere zu langsam auf den digitalen Wandel. In diesem Zusammenhang könnten Freiräume von Vorteil sein. Bei aller gebotenen Vorsicht scheint Gerichten doch höhere Beweglichkeit gegeben als Gremien der EU.

Ein klares Versäumnis sehen Viele darin, das die Möglichkeit der Verbandsklage nicht in der DSGVO selbst festgelegt ist, sondern zu den erwähnten Öffnungsklauseln zählt. In Deutschland wurde dieser Spielraum genützt, um das Verbandsklagerecht in Zusammenhang mit Verstößen gegen die DSGVO einzuführen [17], in Österreich leider nicht [18]. Das ist ein herber Schlag für den KonsumentInnenschutz und alle, die sich ihm verschrieben haben. Hier ruhten große Hoffnungen im Kampf um die Rechte von NutzerInnen. Nun ist ihre Position Konzernen gegenüber in vielfacher Hinsicht empfindlich geschwächt.

Manche fragen sich auch ob es der Weisheit letzter Schluß sei, wenn über Behörden und öffentlichen Stellen bei Verfehlungen von anderen staatlichen Stellen Geldbußen verhängt werden, die der Staat dann quasi

an sich selber zahlt. Möglicherweise wären hier andere Sanktionsmöglichkeiten sinnvoller gewesen. Österreich hat hier einen besonders originellen Ausweg gefunden, über den gleich noch zu lesen sein wird.

VII. Österreichs Sonderweg in die Sackgasse

Nachdem in der Juli 2017 verabschiedeten Fassung des Datenschutz-Anpassungsgesetzes [5] von den besagten Öffnungsklauseln kein nennenswerter Gebrauch gemacht wurde und die Angelegenheit bereits erledigt schien, folgte März 2018 ein Knalleffekt. Völlig überraschend brachte die Bundesregierung per Initiativantrag das Datenschutz-Deregulierungs-Gesetz 2018 [19] im Nationalrat ein.

In diesem werden sämtliche Strafen ausgesetzt, lediglich Verwarnungen sollen an ihrer statt ausgesprochen werden. Womit die vielleicht wichtigste Errungenschaft der DSGVO zunichte gemacht wäre: Die Möglichkeit, bei Verstößen angemessene Sanktionen zu setzen, die ggf. auch für finanzkräftige Konzerne spürbar sind.

Ohne sie bliebe die gesamte Verordnung zahnlos, ihre Wirkung wäre grundsätzlich in Frage gestellt. Doch dieser österreichische Sonderweg ist von keiner Öffnungsklausel gedeckt und widerspricht ganz klar dem geltenden EU-Recht [20], [21]. Aus welchem Grund man diese Schritte für opportun hielt, bleibt völlig rätselhaft. Andrea Jelinek [22], Leiterin der österreichischen Datenschutzbehörde und seit kurzem auch Vorsitzende des EU-Datenschutzausschusses [23], läßt keinen Zweifel daran, dass in Zusammenhang mit der DSGVO einheitlich EU-Recht anzuwenden ist.

Nach Vorstellung der Bundesregierung sollen Behörden und Institutionen mit hoheitsrechtlichen Aufgaben mit Strafen grundsätzlich nicht behelligt werden können. Das mag vielleicht wie eine elegante Lösung des oben skizzierten Paradoxons staatlicher Selbstbestrafung erscheinen, steht aber ebenfalls gegen EU-Recht und wird wohl früher oder später fallen müssen. Von der demokratiepolitischen Bedenklichkeit ganz zu schweigen. Etliche österreichische Behörden haben sich bei der

Beantwortung von Auskunftsbegehren schon bisher nicht eben mit Ruhm bekleckert. Trotz gesetzlicher Verpflichtung blieb man so manche Antwort schuldig. Ohne Sanktionsmöglichkeit wird sich daran kaum etwas ändern. Zu allem Überdruss wurde nun auch die Auskunftspflicht von Behörden empfindlich eingeschränkt ("Die Presse", Print-Ausgabe, 03.05.2018). Kein gutes Zeichen im einzigen Land Europas mit in der Verfassung verankertem Amtsgeheimnis. Allen Lippenbekenntnissen zum Trotz, die baldige Abschaffung dieses reichlich anachronistisch anmutenden Zustandes versprachen, ist die amtierende Bundesregierung die erste seit langem, in deren Regierungsprogramm dieses Vorhaben fehlt.

Diese Aufweichungen werden vollends unverständlich, wenn man sich vor Augen hält, dass Österreich 2016 als einziges Land im Rat der EU, also jenem Gremium, das direkt von den Regierungen der Mitgliedstaaten mit VertreterInnen beschickt wird, gegen die DSGVO stimmte. Die Begründung lautete damals, dass sie in der vorliegenden Form nicht weit genug ginge.

Ungeachtet all dieser Problempunkte wurde das Datenschutz-Deregulierungs-Gesetz am 20.04.2018 im Nationalrat beschlossen und trat mit 25. Mai in Kraft [24]. Daneben wurden zwischen 7. März und 25. Mai 2018 nicht weniger als 13 Entwürfe für Datenschutz-Anpassungsgesetze im Nationalrat eingebracht, die bislang erst zum Teil beschlossen wurden.

VIII. Conclusio: Fürchtet euch nicht!

Trotz mancher Schwäche stellt die DSGVO unbestreitbar einen wichtigen Meilenstein auf dem Weg ins digitale Zeitalter dar. Erstmals existiert nun eine EU-weit gültige Regulierung im Bereich des Datenschutzes. Damit ist das Thema jedoch nicht abgeschlossen, wir befinden uns vielmehr am Anfang einer Entwicklung, deren Fortgang oder gar Ende nicht abzusehen ist. Voraussichtlich wird der Bereich noch lange nicht zur Ruhe kommen. Viel eher ist anzunehmen, dass diese Auseinandersetzung künftig dauerhaft zu führen sein wird. Umso bedeutsamer ist es, dass hier eine

Weichenstellung in Richtung eines starken Datenschutzes vorgenommen wurde.

Denn schlussendlich sind wir alle betroffen, sowohl als einzelne BürgerInnen als auch als gesamte Gesellschaft. Die digitalen Technologien bergen neben ihrem hohen positiven Potenzial auch immense Gefahren. Ihr Missbrauch kann wohlerworbene Freiheiten und Rechte aushebeln, letztlich stehen zahlreiche demokratische Errungenschaften auf dem Spiel. Die jüngst bekanntgewordenen Vorgänge um Facebook und Cambridge Analytica sind nur die sprichwörtliche Spitze eines Eisberges, und beileibe nicht des einzigen.

So ist die DSGVO in Summe durchaus positiv zu bewerten, mit ihr wurde zweifellos ein enorm wichtiger Schritt gesetzt. Eine detaillierte Analyse ist dem Blogpost von Angelika Adensamer auf dem Website von epicenter.works zu entnehmen [25]. Wie es weitergeht, muss sich erst weisen, doch die eingeschlagene Richtung stimmt unbestreitbar. Der Ball wurde bereits aufgenommen, die ersten Beschwerden liegen vor, weitere sind zu erwarten [26] [27].

Quellen und weiterführende Links, zuletzt abgerufen am 13. Juni 2018

[1] Wikipedia: Buchführung
https://de.wikipedia.org/wiki/Buchf%C3%BChrung

[2] Anton Tantner: Die ersten Suchmaschinen
http://tantner.net/publikationen/DieErstenSuchmaschinen_toc.html

[3] Wikipedia: Von Neumann Architektur
https://de.wikipedia.org/wiki/Von-Neumann-Architektur

[4] Wikipedia: Harvard Architektur
https://de.wikipedia.org/wiki/Harvard-Architektur

[5] Datenschutz-Anpassungsgesetz 2018 – Wissenschaft und Forschung –

WFDSAG 2018
https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00010/index.shtml

[6] Stellungnahme der Fa. Bayer zum Datenschutz-Anpassungsgesetz 2018
https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_00327/imfname_684667.pdf

[7] Wikipedia: Datenschutzgesetz (Österreich)
https://de.wikipedia.org/wiki/Datenschutzgesetz_(%C3%96sterreich)

[8] Datenschutzbehörde der Republik Österreich
https://www.dsb.gv.at

[9] Wikipedia: Datenschutzrichtlinie der EG
https://de.wikipedia.org/wiki/Richtlinie_95/46/EG_(Datenschutzrichtlinie)

[10] Datenschutz-Grundverordnung (EU) 2016/679 auf EUR-Lex
http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679

[11] Text der Datenschutz-Grundverordnung 2016/679
http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE

[12] Datenschutz-Anpassungsgesetz 2018, Fassung von Juli 2017
https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.html

[13] Website NOYB
https://noyb.eu

[14] WKO: FAQs zur EU-Datenschutz-Grundverordnung

https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-bin-ich-betroffen-faq.html

[15] Leitfaden der österreichischen Datenschutzbehörde zur DSGVO
https://www.dsb.gv.at/documents/22758/116802/DSGVO-Leitfaden-2018.pdf/01c18811-eb9e-4293-a9f1-0464d5e22b8f

[16] Informationen der österreichischen Wirtschaftskammer zur DSGVO
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html

[17] Website der Deutschen Bundesregierung – Verbandsklagerecht in Kraft
https://www.bundesregierung.de/Content/DE/Artikel/2015/12/2015-12-17-bmjv-verbandsklagerecht-bei-datenschutzverstoessen.html

[18] Website Kleine Zeitung: Wiener Datenschutzaktivist kritisiert Nein zu Verbandsklagen
https://www.kleinezeitung.at/politik/innenpolitik/5425467/Datenschutz_Schrems_Oesterreichs-Regierung-schuetzt-Google-und

[19] Datenschutz-Deregulierungs-Gesetz 2018 (189/A)
https://www.parlament.gv.at/PAKT/VHG/XXVI/A/A_00189/index.shtml#tab-Uebersicht

[20] Website heise online: Keine Strafen: Österreich zieht neuem Datenschutz die Zähne
https://www.heise.de/newsticker/meldung/Keine-Strafen-Oesterreich-zieht-neuem-Datenschutz-die-Zaehne-4031217.html?seite=all

[21] Website netzpolitik.org: Österreich verwässert die EU-Datenschutzgrundverordnung
https://netzpolitik.org/2018/oesterreich-verwaessert-die-eu-

datenschutzgrundverordnung

[22] Website Trend: Interview Andrea Jelinek
https://www.trend.at/branchen/digital/datenschutz-geldbussen-9251275

[23] Youtube-Channel phoenix: Pressekonferenz mit Andrea Jelinek am 25.05.2018
https://www.youtube.com/watch?v=_gWyNk5V8FI

[24] Bundesgesetzblatt I Nr. 24/2018 - Datenschutz-Deregulierungs-Gesetz
https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_I_24/BGBLA_2018_I_24.html

[25] Website epicenter.works: Du hast Rechte, nutze sie!
https://epicenter.works/content/dsgvo-du-hast-rechte-nutze-sie

[26] Website orf.at: Welle von Abmahnungen erwartet
http://orf.at/stories/2439995/2439994

[27] Website futurezone.at: Bereits 81 Verfahren wegen neuer EU-Datenschutzregeln
https://futurezone.at/netzpolitik/bereits-81-verfahren-wegen-neuer-eu-datenschutzregeln/400050185