05.19

PinG

Privacy in Germany

Datenschutz und Compliance

7. Jahrgang
September 2019
Seiten 193–240

www.PinGdigital.de

ESV ERICH SCHMIDT VERLAG

86118

PRIVACY NEWS

STIFTUNG DATENSCHUTZ

Aus Sicht der Stiftung Datenschutz

Nobody's perfect – not even the GDPR …

Frederick Richter, LL. M.

In manchen Datenschutzkreisen scheint es mittlerweile als Sakrileg zu gelten, die EU-Datenschutz-Grundverordnung in ihrer konkreten, Gesetz gewordenen Form zu kritisieren. Wir bei der Stiftung Datenschutz wollen auch zukünftig ein Forum für die Debatte bieten, auf dem auch Stimmen der Minderheit zu Wort kommen. Da DSGVO-Kritiker durchaus interessante Argumente haben können, sollte man sie nicht wie Klimawandel-Leugner behandeln, sondern durchaus einmal zu Wort kommen lassen. Nichts ist besser, als das eigene Argument – von dessen Güte und Schlagkraft man überzeugt ist – anhand des Gegenarguments abzuklopfen.

Wer hat Angst vor dem bösen Kritiker?

Angesichts des starken Signals, das von der DSGVO weltweit ausgeht, und der Wucht ihrer Wirkung auf die Welt der Unternehmens-Compliance verwundert es doch immer wieder, wie empfindlich manche Protagonisten in Brüssel reagieren, wenn das Gesetzeswerk kritisiert wird. Ich bin überzeugt: Die DSGVO hält Kritik aus. Die Fakten sind geschaffen, und niemand muss Angst haben, dass es ein Zurück zu einem nationalen Datenschutzrecht geben wird. Wohl aber muss ebenso gelten: Auch der größte Schritt ist meist nicht der letzte. Warum sollte die DSGVO das Ende des Weges markieren? Als Schlusspunkt der Rechtsentwicklung dürfte man sie wohl nur dann betrachten, wenn zugleich die technische Entwicklung zum Stillstand käme und wenn Verhalten und Alltagsleben der Datensubjekte keinem Wandel mehr unterlägen. Da beides natürlich nicht der Fall ist, war es konsequent vom europäischen Gesetzgeber, die Regelungen des vereinheitlichten Datenschutzrechts einer quasi dauerhaften Evaluierung zu unterwerfen. Alle vier Jahre soll die Verordnung bewertet und überprüft werden.[1] Der Startschuss für dieses Verfahren fällt im kommenden Frühjahr, vier Jahre nach der Verabschiedung des Gesetzes. Der Überprüfung müssen keine Reformschritte folgen, sie können es aber.

Dem Vernehmen nach ist der Reformeifer in Brüssel, was das Datenschutzrecht angeht, unter dem Eindruck der mehr als „intensiven" Verhandlungen im Gesetzgebungsverfahren zur DSGVO etwas erlahmt. Allen ist klar, was es bedeutete, dieses Paket wieder aufzuschnüren. Sollte im Rahmen der ersten Evaluation in 2020 jedoch handfestes Verbesserungspotential hervortreten, so wäre es rechtspolitisch fragwürdig, eine inhaltlich gebotene Modifizierung des Rechts mit einem „zu anstrengend" zu vertagen. Nicht zuletzt deshalb, weil eine enge Verwandte der EU-Datenschutz-Grundverordnung ihrer Geburt harrt.

1 Art. 97 Abs. 2 DSGVO.

Frederick Richter ist ständiger Autor bei „Privacy in Germany". Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz. *(Foto: Lorenz Becker)*

Zusammen regeln, was zusammengehört?

Der Entwurf der ePrivacy-Verordnung ließe sich mit guten Gründen parallel zur DSGVO-Überprüfung aufgreifen. Dies würde die Chance bieten, beide Regelwerke zu verzahnen. Die Bundesregierung betonte in diesem Sommer, dass die ePrivacy-VO „ein hohes, über die DSGVO hinausreichendes Schutzniveau gewährleisten müsse". Gleichzeitig stellte sie klar, dass eine der Telekommunikation nachfolgende Datenverarbeitung allein nach der Datenschutz-Grundverordnung zu beurteilen sei.[2] Eine

2 BT-Drs. 19/11351; Antwort der Bundesregierung auf Kleine Anfrage von Abgeordneten der FDP; S. 6; abrufbar unter: http://dipbt.bundestag.de/dip21/btd/19/113/1911351.pdf.

gewisse Abstimmung aufeinander scheint daher systematisch geboten. Es ist zu verhindern, dass zu den *Auslegungs*schwierigkeiten, die die DSGVO – wie jedes neue Gesetz in seinen ersten Anwendungsjahren – mit sich bringt, womöglich noch *Abstimmungs*schwierigkeiten mit dem „anderen" neuen Datenschutzrecht hinzukommen.

Unter den letzten Vorsitzen im Rat der Europäischen Union kamen zum ePrivacy-Vorhaben kaum mehr als sogenannte Fortschrittsberichte zustande – welche nicht von Fortschritten des gleichsam ruhenden Gesetzgebungsverfahrens berichten konnten.[3] Mit den Ergebnissen des Kommissionsberichts zur DSGVO-Praxis aus dem nächsten Mai könnte Deutschland seine Ratspräsidentschaft in der zweiten Hälfte von 2020 zu einem beherzten Neuaufschlag nutzen.

Wo hakt es?

Nicht nur systematisch und mit Blick auf die nach einheitlicher Orientierung suchende Rechtspraxis wäre eine Abstimmung von DSGVO und ePrivacy-VO wünschenswert. Der Prozess könnte auch für einen kritischen Blick auf grundsätzliche Probleme des Datenschutzes genutzt werden. So besteht offensichtlicher Verbesserungsbedarf im Bereich der datenschutzrechtlichen Einwilligung. Denn mit der vom Recht vorgesehenen Informiertheit der Einwilligenden ist es in den allermeisten Fällen nicht weit her. Eine Einwilligung ist eben nicht bereits dann „informiert", wenn ein Verantwortlicher seine datenschutzrechtlichen Informationspflichten erfüllt hat, sei es auch in textlicher Vollendung. Ein nicht gelesener ist Text für die betroffene Person ohne Wert, mag jener auch Datenschutzbehörden und Rechtsabteilungen wegen seiner inhaltlichen Güte noch so erfreuen. Compliance muss noch lange nicht Datensouveränität bedeuten. Bevor zu diesem Punkt nicht neue Lösungsansätze gesucht und gefunden wurden, erscheint es daher ein wenig unausgegoren, wenn mit der geplanten ePrivacy-VO ein Gesetz zum Datenschutz voll auf die – vermeintlich informierte – Einwilligung als Rechtsgrundlage setzt.

Risiken und Zumutungen

Als weiterer kritischer Punkt dürfte in der DSGVO-Evaluation seitens der Rechtsadressaten vor allem die Belastung mit bestimmten Nebenpflichten vorgebracht werden, der „Datenschutz auf dem Papier". Ich will hier nicht das Lied derer gelten lassen, die klagen, für ihre winzige Organisation wäre Konformität mit dem Datenschutzrecht unmöglich herzustellen. Unmöglich ist nichts, es ist allein eine Frage von Zeit und Kosten, eine Frage des Aufwandes, des Wollens und des Machens. Doch sollte Datenschutz nie als Selbstzweck erscheinen.

Es liegt auf der Hand, dass die Bürgerinnen und Bürger die wahren Gefahren für ihre Freiheit und Privatsphäre nicht aus Richtung von Sportclubs, Bäckereibetrieben oder Kindergärten wähnen, sondern aus Richtung mächtiger ausländischer Digitalunternehmen. Allen ist der Unterschied klar, der mit Blick auf die datenschutzbezogenen Risiken zwischen einem datenbasierten Weltkonzern und einem gemeinnützigen Kleingartenverein besteht. Diese Klarheit beim Risikounterschied mag den Unmut erklären, der entsteht, wenn allein im technisch-organisatorischen Bereich risikoadäquat abgestuft wird,[4] bei den Informations- und Dokumentationspflichten jedoch nicht.

Wo die Erfüllung der vielen Pflichten nachweislich dem großen Ganzen dient, nämlich dem konkreten und effektiven Schutz der einzelnen schützenswerten Person, dort kann man die ausgeweitete Datenschutzbürokratie mit dem früheren Bundesbeauftragten Peter Schaar durchaus treffend als eine „notwendige Zumutung" betrachten.[5] Dort aber, wo Effektivität und Effizienz der kosten- und vor allem zeitintensiven Bürokratielast im Zweifel stehen, könnten sich Handlungsfelder für einen Reformgesetzgeber auftun. Es erschiene rechtspolitisch unsauber, zur Abmilderung von Datenschutzbürokratie auf exekutives Unvermögen zu setzen – wissend, dass notorisch unterbesetzte Aufsichten keine Kapazitäten für Prüfungen sämtlicher KMU und Vereine haben. Gesetzliche Klarstellungen sind vorzuziehen. Diese können allein auf EU-Ebene Erfolg haben; Vorstöße auf nationaler oder gar Landesebene wären Kosmetik, auf welche der EuGH sich freute.

Mitnichten würde es jedenfalls das mit der DSGVO Erreichte in Frage stellen, nach einem intensiven Praxisjahr dezidiert Hand an kritische Stellen anzulegen. Kein Gesetz ist im ersten Wurf perfekt.

3 Eine anschauliche Übersicht zum Stand des Gesetzgebungsverfahrens findet sich beim Bundesverband der Digitalen Wirtschaft e. V., abrufbar unter: www.bvdw.org/themen/recht/kommunikationsrecht-eprivacy.

4 Art. 32 Abs. 1 DSGVO: „Berücksichtigung [...] der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen".

5 „Die notwendige Zumutung Datenschutz", Gastbeitrag bei *heise online* am 25. Mai 2018; abrufbar unter: www.heise.de/newsticker/meldung/Analyse-zur-DSGVO-von-Peter-Schaar-Die-notwendige-Zumutung-Datenschutz-4057260.html.