



BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Einleitungsvortrag

des Bundesbeauftragten für den Datenschutz und die
Informationsfreiheit

Ulrich Kelber

**Evaluation der Datenschutz-Grundverordnung: Was bleibt,
was muss sich ändern?**

bei EAID

Berlin, den 27.01.2020

Dauer: 10 Minuten / anschließende Podiumsdiskussion

Es gilt das gesprochene Wort

Lieber Herr Schaar,

Lieber Herr Büllesbach,

liebe Kolleginnen und Kollegen,

meine sehr geehrten Damen und Herren,

I. Einleitung

Nach allgemeiner Meinung feiert die DSGVO im Mai ihren zweiten Geburtstag.

Das ist aber so nicht richtig: Sie ist bekanntlich bereits am 24 Mai 2016 in Kraft getreten.

Lediglich scharf gestellt wurde sie - 2 Jahre später - am 25. Mai 2018. Statt sich rechtzeitig – und zwar vor vier Jahren - vorzubereiten, haben viele Verantwortliche geschlafen.

Als es dann im Mai 2018 ernst wurde, ging das Wehklagen über ruinöse Bußgelder und ausufernde Bürokratie los.

Ein Teil der Beratungsindustrie hat die allgemeine Verunsicherung noch angestachelt. Das Internet war vor und nach dem 25. Mai 2018 voll mit gezielt verbreiteter Verängstigung, aber auch glatten Fehlinformationen.

Eine Abmahnwelle wurde heraufbeschworen – ein Tsunami an Kostenbescheiden und Bußgeldern gegen kleine Unternehmen und Vereine zog am dunklen Horizont herauf.

Heute wissen wir: Diese Besorgnisse und Ängste waren unbegründet.

Trotzdem: Die Angst- und Miesmacherei ist noch längst nicht beendet. Gerade von Seiten der Industrie wird auch in diesen Tagen massiv gegen die DSGVO Stimmung gemacht.

In der Diskussion über die Evaluierung der DSGVO müssen wir angesichts dieser Vorbehalte immer wieder daran erinnern:

- Mit der DSGVO haben die Betroffenen mehr Kontrolle und Transparenz bei der Datenverarbeitung erlangt.
- Die Europäische Union hat endlich Schluss gemacht mit dem nationalstaatlichen und extrem löchrigen Flickenteppich beim Datenschutz.
- Das Datenschutzbewusstsein ist in dieser Zeit merklich gestiegen. Die Eingaben bei den Aufsichtsbehörden haben sich vervielfacht.

Angesichts dieser Fortschritte hätte ich mir in der Zeit vor und nach dem Wirksamwerden der DSGVO von Seiten der Medien und auch Teilen der Fachöffentlichkeit insgesamt doch etwas mehr Willkommenskultur gewünscht.

II. Erste Bilanz: DSGVO als Erfolgsmodell

Insgesamt ziehe ich eine positive Bilanz der DSGVO.

Dazu tragen auch die verbesserten Sanktionsmöglichkeiten der Aufsichtsbehörden bei, von denen diese - unter anderem - in Form von Bußgeldern auch mehr und mehr Gebrauch machen.

Die DSGVO hat darüber nicht nur in der EU selbst, sondern weltweit Maßstäbe gesetzt.

Über 100 Länder in aller Welt haben inzwischen Datenschutzgesetze eingeführt. Die Mehrzahl der Datenschutzgesetze wurde außerhalb von Europa verabschiedet – gerade in Afrika! Und bei vielen der neuen Datenschutzgesetze – zum Beispiel in Kalifornien oder Brasilien – wurde die DSGVO als Vorbild herangezogen.

IV. Der Evaluierungsprozess: Besseres als Feind des Guten

Ein Knackpunkt ist und bleibt die Durchsetzung des Datenschutzes insbesondere gegenüber den großen internationalen IT-Unternehmen.

Hier müssen alle europäischen Aufsichtsbehörden das in der DSGVO geregelte Verfahren der Zusammenarbeit im Europäischen Datenschutzausschuss so mit Leben zu füllen, dass die Konzerne hinreichend unter Druck gesetzt werden.

Die DSK hat ihren Bericht über die Erfahrungen auf der 98.

DSK verabschiedet und dem EDSA zugeleitet. Der wurde von der Kommission nach Art. 97 Abs. 3 DSGVO konsultiert.

Gut, dass wir uns in dem doch recht aufwändigen Verfahren auf eine anspruchsvolle Reformagenda verständigen konnten.

Gut auch, dass wir uns auf wesentliche Punkte konzentriert und nicht die alten Schlachten bei der Entwicklung der DSGVO nochmal geschlagen haben.

Lassen Sie mich zwei Reformbaustellen herausgreifen:

1. Kernthema: Profiling

Die Bildung persönlicher Profilen und deren kommerzielle oder politische Auswertung sind zentrale Herausforderungen.

Moderne Datenverarbeitung ermöglicht das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten.

Selbstlernende Algorithmen eröffnen immer neue Möglichkeiten, das Verhalten von Menschen vorherzusagen und sogar zu steuern.

Die Verarbeitung ihrer Daten kann Betroffenen nützen, aber auch erheblich schaden. Ich nenne hier als Stichwort die chinesische Überwachungsstrategie gegenüber der eigenen Bevölkerung. Aber auch die Vermessung der Bürger durch US-amerikanische Privatfirmen.

Die DSGVO enthält zwar eine Definition des Profilings in Art. 4 Nr. 4 und das Verbot der automatisierten Entscheidungsfindung in Art. 22. Sie bleibt aber letztlich vage und lückenhaft.

Rechtlich auf dem Stand von 1995. Technisch auf dem Stand der 1980er Jahre.

Wir müssen an dieser Stelle – wenn irgend möglich auf europäischer Ebene - nachbessern. Nationale Alleingänge sind der falsche Weg, rechtlich auch beinahe unmöglich.

Wir brauchen eine Verschärfung des geltenden Rechtsrahmens, um die Menschen vor Manipulation und Diskriminierung wirkungsvoll zu schützen.

Meine Haltung wird von der Konferenz der Datenschutzbeauftragten ebenso geteilt wie von der Datenethikkommission, in der ich mitgearbeitet habe.

Zum wirksameren Schutz der Bürgerinnen und Bürger sollten die vorhandenen Regelungen der DSGVO bereits auf die Bildung von Profilen erstreckt werden. Derzeit beschränken sie sich nur auf die automatisierte Entscheidungsfindung.

Die Schufa und in deren Schlepptau die übrigen Auskunftsteile beteuern stets:

- Wir treffen selbst ja gar keine automatisierten Entscheidungen.
- Wir stellen doch nur den Endkunden ein Profil, den Score, zur Verfügung.

Der Trick dabei: Bei den Banken verfehlen häufig die Schutzregelungen bei der automatisierten Entscheidungsfindung ihr Ziel: Sie können treuherzig immer noch auf eine menschliche Entscheidungsinstanz verweisen. Die ist zumindest auf dem Papier vor einer Kreditvergabe dazwischen geschaltet.

Diese klaffende Schutzlücke ließe sich schließen, wenn bereits das Profiling als solches dem Verbot mit Erlaubnisvorbehalt des Art. 22 DSGVO unterstellt wird.

Zudem sollte klargestellt werden, dass sich die Auskunftspflicht aus Art. 13 Abs. 2 lit f. nicht ausschließlich auf Profiling beschränken darf, wenn dieses als Verfahren unmittelbar Bestandteil einer automatisierten Entscheidung ist.

Die Betroffenen müssen grundsätzlich ein Recht auf aussagekräftige Informationen haben wenn Profilbildung stattfindet. Denn diese stellt immer ein Risiko für das Recht auf informelle Selbstbestimmung dar, egal auf welcher technischen Grundlage sie erfolgt.

Eine rechtstechnisch noch etwas größere Lösung empfiehlt die Datenethikkommission.

Danach sollen verschiedene Formen des Profilings und der algorithmenbasierten Entscheidung anhand ihres Risikopotentials, etwa nach dem Einsatzzweck und der Sensibilität der Daten, klassifiziert und reguliert werden.

Die Konsequenz ist einschneidend: Ergibt sich ein unvertretbares Risikopotential, kann es ggf. zum vollständigen Verbot kommen.

Sie sehen, wir müssen der ungehemmten Nutzung personenbezogener Daten zur Profilbildung effektive und in der Praxis durchsetzbare Grenzen setzen.

Hier müssen wir Datenschützer eng mit den Verbraucherverbänden kooperieren. Klaus Müller wird heute sicher einiges dazu sagen.

2. Entbürokratisierung - wo es dem Datenschutz nicht schadet.

Es gibt Bereiche, in denen sich der bürokratische Aufwand reduzieren lässt, ohne gleichzeitig den Datenschutz zu beschneiden.

Ich denke da an die Informationspflichten, die gerade für viele kleine Unternehmen und Vereine einen maßgeblichen Mehraufwand im Vergleich zum alten Datenschutzrecht bedeuten.

Ich bin froh darüber, dass wir Aufsichtsbehörden im Rahmen der DSK diese Problematik in den Blick genommen haben, ohne aber das Gejammer über angeblich unerträgliche bürokratische Lasten durch die DGSVO zu befördern.

Denn ohne Dokumentation ist auch keine Kontrolle möglich.

Wagen wir den Blick ins Detail: Die Informationspflichten der Art. 13 und 14 DSGVO sind ein Kernstück der DSGVO.

Transparenz ist zum einen die Voraussetzung für die Ausübung der Betroffenenrechte. Zum anderen ist das Wissen darüber, wer welche meiner Daten zu welchen Zwecken verarbeitet aber auch ein Wert für sich.

In einer digitalen Umgebung sind diese Informationspflichten regelmäßig gut erfüllbar. Gemäß Erwägungsgrund 58 Satz 2 können die Informationen grundsätzlich in elektronischer Form zum Zeitpunkt der Erhebung bereitgestellt werden. Sofern der Verantwortliche eine Webseite betreibt, kann er die erforderlichen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ anbieten.

Bei nicht digitalen Sachverhalten führt jedoch das Erfordernis der Information zum Zeitpunkt der Erhebung gemäß Art. 13 DSGVO zu praktischen Zweifelsfragen. Bei mündlichen oder telefonischen Kontakten im geschäftlichen Bereich ist es lebensfremd zu erwarten, dass der Verantwortliche umfassende Datenschutzinformationen erteilt. Bei Aufnahme einer Bestellung, der Entgegennahme einer Visitenkarte oder dem Notieren eines Termins wird er keine Rechtsgrundlage für diese Handlungen benennen oder über die zuständige Datenschutzaufsichtsbehörde, Auskunfts-, Beschwerde- und sonstige Betroffenenrechte informieren.

Eine solche Kaskade von Information würde vielfach auf das Unverständnis der Betroffenen stoßen. Mehr Akzeptanz für den Datenschutz im Alltag sieht anders aus.

Wir haben uns in der DSK erfreulicherweise auf einen recht weitgehenden Reformvorschlag verständigt: Die Informationspflichten sollen danach in bestimmten Fällen nur noch auf Verlangen der betroffenen Person erfüllt werden müssen.

Das gilt vor allem bei einer Datenverarbeitung, die der Betroffene erwarten muss und bei der keine besonderen Risikofaktoren vorliegen. Ausnahmen von diesem Grundsatz wären dann etwa die Weitergabe der erhobenen Daten an Dritte, oder die Verarbeitung besonders sensibler Daten nach Art. 9. Auch beim Profiling müsste weiterhin umfassend informiert werden.

Was die Informationspflichten angeht, möchte ich den sogenannten Mehrebenenansatz („layered approach“) erwähnen, der vom Europäischen Datenschutzausschuss in seinen Leitlinien zur Transparenz vorgesehen ist. Diese Möglichkeit einer stufenweisen Erfüllung der Informationspflichten über mehrere Ebenen ist zwar in der DSGVO nicht ausdrücklich erwähnt, aber sinnvoll und praxistauglich.

Ist es wirklich ein datenschutzrechtliches Problem, wenn bei einem telefonischen Erstkontakt mit einer betroffenen Person nicht die gesamte Datenschutzerklärung, sondern nur die wichtigsten Informationen zur Verfügung gestellt werden? Hier dürfte es doch genügen, auf die Abrufbarkeit der gesamten Erklärung im Internet oder eventuell auf eine separat vom Band abrufbare Datenschutzerklärung mit Hinweis auf die Betroffenenrechte zu verweisen.

Auch ein symbolhaftes Hinweisschild bei der Videoüberwachung mit Angabe eines Links zur ausführlichen Datenschutzerklärung fällt unter den Mehrebenenansatz.

VI. Schlussbemerkung

Ich möchte abschließend an diese Runde appellieren, die fundierten Vorschläge der DSK zu unterstützen; Ich konnte Ihnen hier nur zwei einfachere Beispiele davon vortragen. Wer die weiteren Punkte noch nicht kennt sich aber dafür interessiert, kann das Papier auf der Website der DSK oder des BfDI finden.

Ich bitte auch darum, die vielen Angriffe auf das neue europäische Gesetzeswerk

- energisch zurückzuweisen
- und auf deren nationale und internationalen Erfolge zu verweisen.

Wir sind auf einem guten Weg, den wir gemeinsam weiter gehen sollten.

Im Gegenteil: Wir sollten die Durchsetzung der gefundenen Rechtsgrundlagen noch stärken. Das gilt auch für die Zusammenarbeit der europäischen Datenschutzbehörden im Rahmen des One-Stop-Shop.

619 Tage nach der vollen Wirksamkeit der DSGVO wurde noch in keinem der großen Fälle der großen Internetkonzerne eine Entscheidung getroffen. Vor allem die irische Datenschutzbehörde legt keinen Vorschlag vor, wie offensichtliche Datenschutzverstöße geahndet werden sollen.

Von Tag zu Tag zweifele ich mehr daran, ob dieses System unverändert bleiben kann oder einer Reform bedarf. Ich habe der irischen Behörde angeboten, Fälle zu übernehmen, allerdings nach unserem eigenen Verfahren. Auf dieses Angebot wird nicht eingegangen.

Immer mehr spricht für eine europäische Datenschutzbehörde, die besonders wichtige Verfahren bei einer $\frac{3}{4}$ -Mehrheit im EDPB übernehmen kann und für die ein zu schaffendes europäisches Verwaltungsrecht besteht, das den Datenschutz nicht aushebelt.

Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich auf eine angeregte Diskussion