



Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die
Informationsfreiheit

Ulrich Kelber

Ein zukunftsfähiger Exportschlager!

Datentag Berlin 1 Jahr DSGVO

Stiftung Datenschutz

Hertie School of Governance

Friedrichstraße 180
10117 Berlin

Berlin, 24 Mai 2019
Einlass und Registrierung: ab 9.00 Uhr

Begrüßung: 9.30 Uhr

Redezeit: 9.45 – 10.05 Uhr

Ende der Tagung: 16.00 Uhr

Es gilt das gesprochene Wort

Sehr geehrter Herr Wanderwitz,
Sehr geehrter Herr Richter,
Liebe Kolleginnen und Kollegen,
Sehr geehrte Damen und Herren,

Ich freue mich sehr, als (fast) neuer Bundesdatenschutzbeauftragter bei dieser Tagung der Stiftung Datenschutz ein paar Worte sagen zu dürfen.

Ich danke Ihnen, Herr Richter, für die Vorbereitung dieser Veranstaltung, in der u. a. beleuchtet werden soll, inwieweit die DSGVO ein zukunftsfähiger Exportschlager ist.

Bemerkenswert finde ich, dass Sie meinen Vortrag insoweit mit einem Ausrufezeichen versehen haben, während der Titel des Vortrages von Herrn Prof. Detzermann hier eine deutlich skeptisches Fragezeichen ziert.

Diese selbstbewusste Zeichensetzung ermutigt mich, nicht zurückzuschauen, sondern zuversichtlich nach vorne zu blicken.

Herr Richter hat mich heute ordentlich in die Pflicht genommen.

Neben diesem Impulsreferat müssen Sie mich heute noch auf zwei Podien ertragen.

Ich hoffe aber doch, dass meine Überlegungen die Diskussion beleben – und nicht den Umsatz beim Caterer.

Vorbemerkung

Bevor ich mich dem Exportschlager DSGVO widme, müssen wir aber doch noch kurz eine erste Bilanz ihres ersten Jahres ziehen. Die Krabbelphase neigt sich ihrem Ende zu – das Kind lernt laufen.

Sein Start war – mit dieser Feststellung trage ich in diesem Kreis Eulen nach Athen – recht holprig.

Der schwierige Start lag nicht nur an der bei der Umsetzung jeder großen Reform üblichen Unsicherheit. Er war auch verursacht durch ein mitunter schwer erträgliches Übermaß gezielt verbreiteter Verängstigung und glatten Fehlinformationen.

So wurden im Vorfeld eine Abmahnwelle und die massenweise Verhängung von Bußgeldern auch gegen kleine und mittlere Unternehmen sowie Vereine und Verbände befürchtet. Diese Besorgnisse haben sich als unbegründet herausgestellt.

Vieles konnte durch sehr aktive Aufklärungsarbeit der Aufsichtsbehörden gerade gerückt werden. Ich möchte hier auch den Kolleginnen und Kollegen aus den Ländern meine besondere Anerkennung aussprechen. Sie haben mit wenig Personal und knappen Ressourcen diese schwierige und zeitaufwendige Aufgabe gestemmt.

Nationale und internationale Fortschritte durch die DSGVO

Die DSGVO ist wahrlich nicht perfekt. Darauf werde ich noch zu sprechen kommen.

Aber sie schafft erstmals eine gemeinsame Grundlage für ein – weitgehend – einheitliches europäisches Datenschutzrecht.

Wir müssen Öffentlichkeit, Regierungen und Parlamenten immer daran erinnern, dass erst auf der Grundlage der DSGVO die Betroffenen

- mehr Kontrolle
- und Transparenz bei der Datenverarbeitung erlangt haben,

und wie wichtig dies gerade im digitalen Zeitalter ist.

Die DSGVO hat sich mittlerweile allen Unkenrufen zum Trotz zu einem internationalen **Standard entwickelt. Daran orientieren sich auch andere Weltregionen.** Die Entwicklungen in Japan, aber auch das hohe Interesse weiterer Staaten in Lateinamerika und Asien belegen dies eindrucksvoll.

Hoffnungsfroh stimmt mich auch die Entwicklung des Datenschutzes im Bundesstaat Kalifornien.

Dort wurde als Reaktion auf den Facebook-Skandal nach dem Vorbild der DSGVO der "California Consumer Privacy Act" verabschiedet. Unternehmen müssen dann ab dem 1. Januar 2020 offenlegen, welche Kunden- und Nutzerdaten sie speichern. Die Nutzer wiederum erhalten das Recht, die Verwendung ihrer persönlichen Daten zu kommerziellen Zwecken zu unterbinden. Die Internetfirmen werden verpflichtet, einen Link anzubieten, der es den Nutzern erlaubt, ohne Papierkrieg den Weiterverkauf ihrer Daten zu verhindern.

Es sind zwar keine Zwangsmaßnahmen und keine Bußgelder vorgesehen, die Verbraucher können aber gerichtlich ihre Rechte gegenüber den Unternehmen geltend machen.

Kalifornien ist der Sitz zahlreicher Technologiekonzerne, Von daher hat das neue Gesetz eine wichtige Pilotfunktion. .

Wir sehen also: Die USA sind nicht nur Trump!

Aber nicht allein in anderen Ländern, auch hierzulande hat die DSGVO einen Paradigmenwechsel eingeleitet. Der Datenschutz ist wieder stärker in das Bewusstsein der Bürgerinnen und Bürgerinnen gerückt. In meinem Haus hat sich die Anzahl der Beschwerden über Datenschutzverstöße gegenüber Vor-DSGVO-Zeiten mehr als verdoppelt. Auch bei den Datenschutzaufsichtsbehörden der Länder haben die **Beschwerden, allgemeinen Anfragen und Meldungen von Datenschutzverstößen** erheblich zugenommen.

Wenn ich über die DSGVO als Exportschlager spreche, möchte ich bei allen Überschneidungen doch zwischen drei Bereichen differenzieren.

- Räumlicher Geltungsbereich der DSGVO
- Datenschutz als Wettbewerbsvorteil
- Schutz der individuellen Rechte der Menschen weltweit

Zu 1

Räumlicher Geltungsbereich der DSGVO

Die DSGVO gilt nicht nur innerhalb der EU. Sie gilt in vielen Fällen auch für Datenverarbeitungen, die anderswo stattfinden, beispielsweise in der Schweiz oder den USA. Sie stellt nicht mehr allein auf eine Niederlassung in der EU und auch nicht auf den Ort ab, an dem technisch die Datenverarbeitung erfolgt.

Artikel 3 enthält in Bezug auf den territorialen Anwendungsbereich der DSGVO zwei Prinzipien

- **Niederlassungsprinzip (Abs. 1)**
- **Marktortprinzip (Abs. 2)**

Den Ausschlag ergibt entweder die Niederlassung des Verantwortlichen oder Auftragsverarbeiters in der EU – oder der Aufenthaltsort des Betroffenen in der EU. Gibt es von dort aus einen tatsächlichen Zusammenhang zur Verarbeitung von personenbezogenen Daten, ist die DSGVO gültig – auch für Unternehmen, die außerhalb der EU ihren Sitz haben.

Auch Unternehmen, die zwar nicht in der EU niedergelassen sind, aber auf dem europäischen Markt tätig sind müssen für alle Aktivitäten, die damit in Zusammenhang stehen, die DSGVO anwenden und befolgen. Drittstaatliche Unternehmen müssen sich also unter Umständen an höhere Anforderungen halten, als es ihre nationalen Gesetze möglicherweise vorsehen.

Das Ziel des europäischen Gesetzgebers, den Anwendungsbereich der DSGVO möglichst breit zu gestalten, ist damit erfolgreich umgesetzt.

Sie sehen, meine Damen und Herren, die DSGVO ist allein durch den erweiterten räumlichen Anwendungsbereich in einem bestimmten Umfang „Weltrecht“ geworden.

Der Vollständigkeit halber weise ich außerdem darauf hin, dass die DSGVO – ebenso wie das vorherige Recht – auch dadurch weit über die EU hinauswirkt, dass eine Übermittlung personenbezogener Daten in Länder außerhalb der EU bzw. des EWR weiterhin nur erlaubt ist, wenn beim Empfänger ein angemessenes Datenschutzniveau besteht. Dieses kann auch nach der DSGVO auf verschiedenen Wegen hergestellt werden.

Zu 2

Datenschutz als Wettbewerbsvorteil

Gelingt es, so mein zweiter Punkt, europäische Produkte so datenschutzfreundlich zu gestalten, dass sie darauf auf den internationalen Märkten einen Wettbewerbsvorteil erreichen?

Viele Unternehmen erkennen an, dass es nun einheitliche Regeln für ganz Europa gibt, an die nicht nur kleine und mittlere Unternehmen gebunden sind, sondern gerade auch die internationalen Großkonzerne wie Amazon u.a. Die größeren dieser Unternehmen sind häufig international aufgestellt und haben die zweijährige Übergangszeit intensiv genutzt, um sich entsprechend aufzustellen.

Durch die DSGVO haben es Unternehmen ebenso wie Bürgerinnen und Bürger bei den Aufsichtsbehörden jeweils nur noch mit einem Ansprech-

partner zu tun, was vor allem für grenzüberschreitend in Europa tätige Unternehmen und für die hier betroffenen Personen ein großer Vorteil ist.

Zu den Vorzügen der DSGVO gehören die erweiterten Betroffenenrechte – wie etwa das Recht auf Datenübertragbarkeit oder das Recht auf Vergessenwerden – ebenso wie die Verpflichtungen, die Datenverarbeitung datenschutzfreundlich zu gestalten („**Privacy by Design**“ und „**Privacy by Default**“). Gerade der letzte Punkt kann nicht genug betont werden. Denn hier kann ein entscheidender Vorteil auch für die europäische Digitalwirtschaft liegen: Warum sollen nicht gerade IT-Verfahren und -Produkte „made in Europe“ diejenigen sein, die eine vertrauenswürdige – am Grundsatz des Datenschutzes und der Datensicherheit orientierte – Digitalisierung ermöglichen? Hier wünsche ich mir auch deutlich mehr Unterstützung auf europäischer, aber auch nationaler Ebene, um die Entwicklung solcher Produkte nachhaltig zu fördern.

Es werden sicher auch weiterhin von Seiten der Unternehmen Vorbehalte gegen Regelungen der DSGVO fortbestehen, die mit einem größeren Arbeitsaufwand verbunden sind. Dennoch wären die Unternehmen gut beraten, die Chancen der DSGVO zu nutzen, um so Wettbewerbsvorteile zu erreichen. Mit der Erfüllung der datenschutzrechtlichen Verantwortung lassen sich durch Werbung alte und neue Kunden überzeugen.

Zu 3.

Schutz der individuellen Rechte der Menschen weltweit

Die Grundverordnung leistet einen wichtigen Beitrag, die Menschen vor einer Verletzung ihrer Privatsphäre zu schützen – gerade auch durch Unternehmen, die außerhalb der EU ihren Hauptsitz haben, wie z. B. Amazon, Google, Microsoft und Facebook.

Das europäische Datenschutzrecht macht erfreulicherweise deutlicher denn je, dass Datenschutz ein Grundrecht, ein Freiheitsrecht ist und stellt somit das Persönlichkeitsrecht des Menschen in den Mittelpunkt.

Die DSGVO schafft kein Elysium – sondern bleibt eine Baustelle

Wenn ich die großen Fortschritte der Grundverordnung hervorhebe, stelle ich mich aber nicht taub und blind gegenüber bestimmten Schwächen der DSGVO.

Der europäische Gesetzgeber war vorausschauend genug, den Evaluierungsprozess als Grundlage für ihre Weiterentwicklung in der Verordnung festzuschreiben. Ich hoffe sehr, dass die aus diesem Prozess entwickelten Reformvorschläge nicht auf taube Ohren stoßen.

Dies gilt zum einen natürlich für eine Verbesserung des Datenschutzes an Stellen, die aus meiner Sicht noch nicht zufriedenstellend gelöst sind. Auch die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder befassen sich zurzeit intensiv mit der anstehenden Evaluierung und haben eine Reihe von Themen bestimmt, die insofern der näheren Betrachtung bedürfen. Mit Blick auf die Zeit möchte ich hier vor allem zwei Punkte herausgreifen:

- Die Bildung von Profilen und deren Auswertung ist eines der zentralen Themen der Zeit. Die Werkzeuge der Datenverarbeitung ermöglichen das Anlegen, die Auswertung und Analyse ungeheurer Datenmengen aus verschiedensten Kontexten. Verbunden mit immer weiter verfeinerten Möglichkeiten des Einsatzes selbstlernender Mechanismen eröffnet dies vielfältige Möglichkeiten, Verhalten von Einzelnen (vermeintlich) vorherzusagen und ggf. zu steuern. Obwohl diese Entwicklung diverse datenschutzrechtliche Grundprinzipien herausfordert – z. B. das Gebot der Datenminimierung oder die Zweckbindung – bleibt die DSGVO gerade in diesem Punkt vage und weitgehend auf dem Stand von 1995. Bei den Verhandlungen zur Schaffung der DSGVO war es nicht gelungen, die Bildung von Profilen und das Scoring einer modernen europäischen Regelung zuzuführen. Stattdessen wurde die seit 1995 bestehende Rechtslage im Wesentlichen beibehalten, die das Treffen automatisierter Entscheidungen im Einzelfall nur unter engen Voraussetzungen zulässt. Die vorgelagerte Bildung von Profilen wird aber nicht adressiert und es fehlen auch konkrete Regelungen zu den Voraussetzungen und zur Transparenz des Scorings. Hier sollten wir die Evaluierung für einen neuen Anlauf nutzen.
- Der zweite Punkt betrifft die bereits angesprochene Verpflichtung zum Einsatz datenschutzfreundlicher Technologie. Warum setzt diese erst beim datenschutzrechtlich Verantwortlichen, d. h. dem Unternehmen oder der Behörde ein, die die Technologie einsetzt? Sie haben in manchen Fällen gar keine oder nur eine geringe Auswahl, welche IT sie verwenden. Wäre es deshalb nicht eher

zielführend, hier viel früher, nämlich bei den Herstellern von IT-Verfahren und -Produkten anzusetzen? Auch hierzu hatte es bereits bei den Verhandlungen zur DSGVO Vorschläge gegeben, die ich gern wieder aufgreifen würde.

Auf der anderen Seite will ich aber auch nicht verhehlen, dass es vielleicht auch den einen oder anderen Punkt gibt, bei dem vor allem der mit der Umsetzung der DSGVO verbundene bürokratische Aufwand keinen datenschutzrechtlichen Mehrwert bringt. Schon kurz nach der Einführung der DSGVO erreichten mich Eingaben, in denen die Nutzer oder die privaten Betreiber mir mitteilten, dass sie aus Überforderung den Betrieb ihrer kleinen Webseiten der Foren eingestellt haben. Sie sahen sich nicht in der Lage, den neuen Anforderungen der DSGVO gerecht zu werden.

Eine solche Haltung ist gerade in ehrenamtlichen Bereichen wie Vereinen und Verbänden misslich.

Die Betreiber sind vielfach Privatleute, die in ihrer Freizeit etwas auf die Beine stellen und sich dann über Bürokratie ärgern. Nach meiner Überzeugung ist da manche Flinte zu früh ins Korn geworfen worden. Bei genauerem Hinsehen ist die eine oder andere Sorge unbegründet oder zumindest überzogen.

Datenschutzrechtlich bleibt vieles möglich, was unter der Ägide des alten Rechts auch schon zulässig war. Einige Besorgnisse sind auf unzureichendes Wissen und auf manche Fehlinformationen aus der Übergangsphase zurückzuführen. Hier sind die Aufsichtsbehörden gefordert,

zu helfen und Ängste zu nehmen. Das tun sie auch mit hohem Einsatz. Sie arbeiten weiter an Hilfestellungen und bemühen sich um eine pragmatische Rechtsauslegung.

Es ergibt aber auch keinen Sinn, Regelungen zu verteidigen, die nur Arbeit machen und dem Datenschutz nicht von Nutzen sind. Ich sehe es auch als Aufgabe der Aufsichtsbehörden an, hier zwischen dem europäischen und dem nationalen Gesetzgeber zu vermitteln und an bestimmten Stellen auch Reformbedarf anzuzeigen.

Im Rahmen der in der DSGVO ohnehin vorgesehenen Evaluierung werden wir konkrete Vorschläge für eine Optimierung des geltenden Rechts vorlegen. Dies gilt gerade für die umfangreichen Nebenpflichten, die ein Verantwortlicher hat, ganz gleich welche Größe er hat. Wo der Aufwand zum Selbstzweck wird, ohne für den Schutz der Daten etwas zu erreichen, sind Korrekturen angebracht. Diese wären z. B. denkbar bei der Erfüllung der Informationspflichten, bei der Verpflichtung, ein Verzeichnis der Verarbeitungstätigkeiten zu führen oder bei den Voraussetzungen für eine Meldung von Datenschutzverstößen an eine Aufsichtsbehörde.

Die ewig Unvollendete: ePrivacy-Verordnung

Meine Damen und Herren,

Hauptziel der DSGVO ist es, natürliche Personen bei der Verarbeitung personenbezogener Daten zu schützen.

Bei der ePrivacy-Verordnung wiederum geht es um den speziellen Schutz des Privatlebens und den Schutz personenbezogener Daten in

der elektronischen Kommunikation. Beide überschneiden sich von daher vielfach in ihren Schutzzielen.

Eigentlich sollten beide Verordnung zugleich in Kraft treten. Das hat nicht geklappt. Es hakt und klemmt heftig.

Die ePrivacy-Verordnung ist wie eine Operndiva, die im Aufzug stecken geblieben ist. Man hört laut ihre Stimme, kann aber den Stand der Dinge nur sehr schwer feststellen.

Die ePrivacy-Verordnung enthält bereichsspezifische Sonderregelungen für den Datenschutz in der elektronischen Kommunikation. Ziel ist die Gewährleistung eines hohen Schutzniveaus und die Schaffung gleicher Wettbewerbsbedingungen für alle Marktteilnehmer, auch Messenger-Dienste wie WhatsApp.

Am 10. Januar 2017 legte die KOM den Entwurf der ePrivacy-Verordnung vor. Das EP hat am 26. Oktober 2017 den Berichtsentwurf des federführenden LIBE-Ausschusses als Verhandlungsgrundlage angenommen. Das Trilogverfahren selbst wird aber erst nach der Europawahl am kommenden Sonntag, dem 26. Mai 2019 stattfinden können. Mit dem Inkrafttreten der ePrivacy-Verordnung ist daher nicht vor 2020 zu rechnen. Anzuwenden wäre die Verordnung dann erst nach einer zweijährigen Übergangsfrist im Jahr 2022.

Ich werde mich in den anstehenden Beratungen dafür einsetzen, dass die **Vorschriften zum Tracking** nicht zu Lasten der betroffenen Nutzer verwässert werden. So darf die Einwilligung in die mit der Setzung von Cookies verbundene Datenverarbeitung nicht zur Bedingung für die Nutzung eines Kommunikationsdienstes gemacht werden.

Kinderpornographie und Terrorismus müssen entschieden bekämpft werden. Dazu bedarf es aber wirkungsvoller Schutzkonzepte, die zugleich rechtsstaatlichen Grundsätze wahren.

Der Vorschlag, die Verarbeitung elektronischer Kommunikationsdaten zum Zweck der Identifizierung kinderpornographischer oder terroristischer Inhalte zu erlauben, wirft mehr Fragen auf, als er zu lösen verspricht.

Ich bemängele insbesondere, dass keine ausreichenden Sicherheitsvorkehrungen vorgesehen sind, die verhindern können, dass die einmal gespeicherten Daten nicht zu anderen Zwecken verarbeitet werden. Damit meine ich etwa urheberrechtliche Abmahnungen, die nichts mit dem ursprünglichen Zweck der Datenerhebung zu tun haben.

Schlussbemerkungen:

bei der DSGVO sind wir bereits in der ersten Phase der Evaluierung angelangt.

Bei der geplanten e-Privacy-Verordnung hakt es noch gewaltig. Ich bin aber zuversichtlich, dass ihre Verabschiedung eine grundlegende Weichenstellung sein wird für den Schutz personenbezogener Daten in der elektronischen Kommunikation bringen wird.

Auf dem Spiel steht nicht weniger als die Zukunft der digitalen Gesellschaft.

Wollen wir in einer Gesellschaft leben, in der jeder die Vorteile der digitalen Technik selbstbestimmt nutzen kann? Oder wollen wir es zulassen, dass jeder von uns unweigerlich zum Objekt der „Datensammelei“ verkommt?

Es ist jetzt an der Zeit, einen angemessenen Schutzstandard für die Vertraulichkeit der elektronischen Kommunikation in den nächsten Jahren und Jahrzehnten zu etablieren und die vorhandenen Rechtsunsicherheiten zu beseitigen.

Wie bei der Datenschutz-Grundverordnung gilt es, auch hier einen datenschutzfreundlichen Rechtsrahmen zu schaffen, auf den wir Europäer stolz sein können.

Vielleicht können wir dann auf einer der nächsten Tagungen der Stiftung Datenschutz auch vom Exportschlager e-Privacy-Verordnung sprechen.

Ich danke Ihnen für Ihre Aufmerksamkeit.