Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Tischrede

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Bedeutung der DSGVO für die Versicherungswirtschaft“

Gesamtverband der Versicherungswirtschaft (GdV)

Weinhaus Habel am Reichstag, Luisenstraße 19, Berlin

17. September 2019

18 Uhr (Dauer 15-20 Minuten)

Es gilt das gesprochene Wort

I. Einleitung

Sehr geehrter Herr Dr. Wiener,

Sehr geehrter Herr Junge,

Sehr geehrte Damen und Herren,

ich danke für die Gelegenheit, Ihnen zwischen Suppe und Hauptgericht – vielleicht gibt es ja sogar Kartoffeln – einen Gruß aus der Küche des BfDI servieren zu dürfen.
Es gehört zu meinen Aufgaben, mit den öffentlichen- und nicht-öffentlichen Einrichtungen die optimale Umsetzung des Datenschutzes in den unterschiedlichsten Bereichen zu besprechen.

Diese Gespräche dürfen keine Eintagsfliegen sein, bei denen man sich guten Tag sagt, die eigene Position möglichst ausführlich darstellt und dann wieder auseinandergeht. Da haben wir bereits gut vorgelegt: Ende August hatten wir ein

ausführliches Vorgespräch. Insofern markiert die heutige Begegnung auch nur einen Zwischenstand.

II. Kontrollzuständigkeit liegt bei den Ländern

Wie Ihnen sicher bekannt ist, liegt die Kontrollzuständigkeit für die Versicherungswirtschaft bei den Datenschutzaufsichtsbehörden der Bundesländer.
Daher fehlen mir bei vielen der für Sie spezifisch interessanten Themen die praktischen Erfahrungen. Das gilt beispielsweise für den Umgang mit den Rechten der Betroffenen in der Versicherungsbranche nach § 15 DSGVO oder auch für den Umgang mit Datenpannen und die Verhängung von Sanktionen.

Ich kann Ihnen aber versichern, dass die Aufsichtsbehörden im Rahmen der DSK und ihren Arbeitsgremien sehr intensiv über diese verschiedenen datenschutzrechtlichen Fragen beraten. **Der deutsche Föderalismus prägt eben auch die Aufsicht über den Datenschutz.**

Beim Datenschutz in der Versicherungswirtschaft hat auch der der Europäische Datenschutzausschuss ein wichtiges Wörtchen mitzureden. Diesem Gremium gehöre ich an. Insofern trage ich für die Anwendung der europäischen Datenschutzrechts in der Versicherungswirtschaft in bestimmtem Umfang doch auch eine gewisse Mitverantwortung.

Der EDSA trifft seine Entscheidungen mit Mehrheit – da kann es - wie geschehen und Ihnen sicherlich bekannt - auch passieren, dass man sich nicht durchsetzt. Gleichwohl sehe ich mich durch Mehrheitsbeschlüsse in diesem Gremium gebunden und ich werde sie auch dann vertreten, wenn ich eine andere Meinung habe.

III. Herausforderungen der DSGVO an die Versicherungswirtschaft

Mit der DSGVO wird der Datenschutz neu und erstmals und auch verbindlich für alle Staaten der EU geregelt. Von den Regelungen sind auch Versicherungsunternehmen betroffen.

Trotz Code of Conduct (CoC), der bereits zuvor einen weitreichenden Datenschutz gewährleistet hat, gibt es einiges zu verändern.

Bitte sehen Sie die Anforderungen der DSGVO aber nicht **– nur -** als bürokratischen Ballast an, sondern betrachten den Mehraufwand auch als Chance im Wettbewerb. Ein sorgfältiger, regelbasierter und transparenter Umgang mit den Daten der Versicherten bietet Ihnen auch eine Chance, das Vertrauen in die Branche zu stärken.

Das ist nicht anders als bei ökologisch nachhaltigen Produkten. Wer hier nichts anzubieten hat, wird vom Markt abgestraft!

Versicherungsunternehmen sind nun einmal keine Randfiguren, wenn es um den Schutz persönlicher Daten geht. In ihren Akten und Dateien schlummert seit eh und je eine Vielzahl von Kundendaten. Diese werden für sehr unterschiedliche Zwecke verwendet, Abrechnungen, Kundeninformationen, Schadensregulierungen oder interne Statistiken: das ist Alltag. Die technologische Entwicklung bietet zwischenzeitlich vielfältige Möglichkeiten, Daten zusammenzufassen und durch – unter Umständen auch selbstlernende – Werkzeuge auszuwerten und daraus Schlussfolgerungen zu ziehen oder Vorhersagen zu verfeinern. Für die Versicherungsbranche durchaus verlockende Möglichkeiten.

Datenschutzrechtlich stehen dem die Gebot der Datenminimierung und der Zweckbindung – die in Ihrer Branche partiell durch die Spartentrennung unterstützt wird – der Fairness und der Transparenz gegenüber, die umso wichtiger werden, wie die technologische Entwicklung fortschreitet.

Die seit dem 25. Mai 2018 wirksamen Vorschriften der DSGVO wollen hier – auch für die Versicherungswirtschaft – einen Ausgleich zwischen all diesen Interessen herstellen. Hat die DSGVO naheliegenderweise vor allem den Grundrechtsschutz des Einzelnen im Blick, erkennt sie den freien Datenverkehr ebenfalls als Interesse an. Neuland ist der Datenschutz für Sie natürlich nicht. Die Verarbeitung persönlicher Daten war schon immer zentraler Bestandteil Ihres Geschäfts

Lassen Sie mich ein paar Stichpunkte benennen:

- **Informationspflichten**

Informationspflichten nach Artikel 12 bis 14 DSGVO sowie zur Aufklärung über die nach der DSGVO bestehenden Betroffenenrechte gemäß Artikeln 15 bis 22 und Artikel 34 DSGVO. Das sind nicht immer einfach umzusetzende Vorschriften. Hier ist nicht zuletzt auch Ihre Phantasie gefragt, wie etwa mit abgestuften Prozessen – von der allgemeineren Information für alle zur spezifischen Information für speziell

Interessierte – eine den datenschutzrechtlichen Anforderungen genügende Transparenz auch effizient und wirksam umgesetzt werden kann. Die Informationstechnik kann auch in diesem Kontext eine gute Hilfe sein.

- **Verarbeitung versicherungstechnischer Daten**

Hier stellt sich grundsätzlich bereits die Frage, ob überhaupt und mit welcher Begründung die DSGVO eine Erhebung und Verarbeitung personenbezogener Daten für Durchführung eines Versicherungsvertrages zulässt.

Eine Zustimmung der betroffenen Person in die Verarbeitung ihrer Daten kann jederzeit widerrufen werden.

Es wird also darauf ankommen, ob das Versicherungsunternehmen die Verarbeitung der Daten mit der Notwendigkeit für die Erfüllung des Vertrages begründen kann.

Bei der weitergehenden Verarbeitung etwa für Bilanzierung wird zu prüfen sein, ob diese Verarbeitung tatsächlich für die Erfüllung einer rechtlichen Verpflichtung notwendig ist oder nicht.

Das gilt auch für die Verarbeitung personenbezogener Daten beispielsweise bei der Erkennung von Versicherungsbetrug. Auch hier werden ganz sicher die Gerichte darüber zu entscheiden haben, ob es sich hier um eine von der Grundverordnung gedeckte Wahrnehmung berechtigter Interessen handelt – oder eben nicht.

- **Rechtmäßigkeit der Verarbeitung**

Artikel 6 der DSGVO verbietet im Grundsatz die Verarbeitung personenbezogener Daten. Ausnahmen sind nur dann zulässig, wenn eine ausdrückliche Zustimmung der betroffenen Person vorliegt es oder es hierfür eine Rechtsgrundlage gibt.

Verarbeitungsgründe sind beispielsweise

- die Verarbeitung zur Erfüllung eines Vertrages,
- die Erforderlichkeit Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten; **die Interessen oder Grundrechte der jeweils betroffenen Personen dürfen hier aber nicht überwiegen.**

- **Datenschutz durch Privacy by Design**

In den Prozessen der Datenverarbeitung verlangt die DSGVO in jedem Fall eine ganz besondere Sorgfalt. So müssen auch die Versicherungsunternehmen geeignete technische und organisatorische Maßnahmen treffen, um den datenschutzrechtlichen Anforderungen zu genügen.

Datenschutz durch Technikgestaltung **(Privacy by Design)** ist eine Verpflichtung nach Artikel 25 Absatz 1 DSGVO, bei deren Verletzung Sanktionen drohen. Bereits bei der Planung und Konzeption eines technologischen Systems sind die Erfordernisse des Datenschutzes zu beachten.

Darüber hinaus verlangt Privacy by Design ausreichend sichere Verarbeitungsverfahren, die auch vor Hackerangriffen schützen.

- **Code of Conduct der Versicherungswirtschaft**

Mit dem *Code of Conduct* (CoC) Datenschutz hat die Versicherungsbranche unter der Federführung des GDV schon seit 2012 einen beachtlichen Standard erreicht. Rechtsgrundlage war der damalige § 38a BDSG.

Die meisten der in Deutschland ansässigen Versicherungsunternehmen haben den CoC unterschrieben und ihre Arbeit nach diesen Vorgaben ausgerichtet. Ich habe mit Freude auf Ihrer Webseite gelesen, dass diese Unternehmen einen Marktanteil von 95 Prozent haben.

Die DSGVO brachte allerdings einige Veränderungen. Mit einem „Weiter so“ war es daher nicht getan. Daher erfolgte 2018 eine Überarbeitung der CoCs in Kooperation mit der DSK, die erfreulicherweise dazu führte, dass die materiellen

Bestimmungen des überarbeiteten CoC als vereinbar mit der DSGVO angesehen worden sind. Schon damals stand in der Diskussion allerdings auch die Frage eines **sog. Monitoring Body (MB) im** Mittelpunkt, der die Einhaltung der CoC überwachen sollte.

Die DSK hat sich auf den Standpunkt gestellt, dass ein solcher MB nicht eingerichtet werden muss. Allerdings müsse das Verfahren zur Kontrolle des CoCs im CoC selbst geregelt werden.

Diese deutsche Auffassung hat sich allerdings auf europäischer Ebene nicht durchgesetzt. Die erst kürzlich angenommenen europäischen Leitlinien CoC und die Opinion des Europäischen Datenschutzausschusses zu einem Entwurf von Kriterien für die Akkreditierung einen MBs verlangen, dass ein akkreditierter MB eingerichtet werden muss.

Das ist die Lage in Brüssel und wir sollten davon ausgehen, dass sich daran auch nichts mehr ändern wird.

Ich gehe davon aus, dass die deutschen Datenschutzaufsichtsbehörden die Verbindlichkeit dieses Votums der EDSA nicht in Frage stellen werden.

IV. Evaluierung der DSGVO

Die DSGVO hat sich seit ihrem Inkrafttreten bewährt. Ihren Zielen, den Grundrechtsschutz zu verbessern und einen einheitlichen europäischen digitalen Binnenmarkt zu schaffen, ist sie ein gutes Stück näher gekommen. Ihr Wirksamwerden im Mai 2018 hat in Deutschland das seit den 70er Jahren geltende Datenschutzrecht nach langer Zeit wieder gesamtgesellschaftlich in Erinnerung gerufen. Alle Beteiligten mussten – nicht immer freiwillig und mit Freuden – auf die Neuregelungen reagieren und ihre eingefahrenen Verarbeitungsprozesse kritisch überprüfen.

Für die öffentliche Wahrnehmung und die Berichterstattung waren in diesem Zusammenhang das neue Sanktionssystem

von ausschlaggebender Bedeutung. Sie wissen, dass von diesen scharfen Sanktionen wie schon bisher natürlich nur im Rahmen der Verhältnismäßigkeit Gebrauch gemacht wird.

Die Grundverordnung hält selbst hält sich im Übrigen keineswegs für allwissend. Deshalb haben ihre Erbauer in Art. 97 DSGVO vorgeschrieben, dass bis zum 25. Mai 2020 von der Europäischen Kommission ein „Bericht über die Bewertung und Überprüfung“ der DSGVO erfolgen soll. Dieser Zeitraum von 2 Jahren genügt m.E. auch, die ersten Defizite zu erkennen um entsprechende Verbesserungen in die Wege zu leiten.

Ich sehe die eine oder andere allzu bürokratisch geratene Regelung durchaus kritisch. Bürokratische Regelungen lassen sich nicht immer vermeiden. Wo sie aber für die Betroffenen selbst keinen erkennbaren Nutzen bringen, sollten sie auf den Prüfstand kommen.

Ich bereite gerade mit meinen Kolleginnen und Kollegen in der DSK eine entsprechende Stellungnahme zur Evaluation vor.

Ganz besonders am Herzen liegen mir in dem anstehenden Evaluierungsprozess die Bereiche **Profiling und Scoring am Herzen.**

Moderne Datenverarbeitung ermöglicht die Bildung von persönlichen Profilen und deren kommerzielle und politische Auswertung und schafft damit eine der zentralen datenschutzpolitischen Herausforderungen unserer Zeit. Trotz vorhandener Begriffsdefinition wird die Profilbildung von den meisten dieser Normen nicht hinreichend erfasst, sodass eine Beurteilung meist nur über den Umweg der allgemeinen Tatbestände des Art. 6 DSGVO erfolgt.

Ein Hauptanwendungsfall von Profiling im Sinne der Begriffsbestimmung des Art. 4 Nr. 4 ist die Erstellung von Profilen auf der Grundlage von Internet–

Kommunikationsinhalten sowie Metadaten. Die werden dann für Werbezwecke, für personalisierte Preisangebote sowie für personalisierte Informationsanzeigen veredelt.

Leider bietet Artikel 22 DSGVO nur einen recht überschaubaren Regelungsgehalt. Ich plädiere hier für eine klare gesetzliche Regelung automatisierter Entscheidungen im Einzelfall einschließlich Profiling. Ob die Regelung an dieser Stelle überhaupt einschlägig ist, wird teilweise mit dem Hinweis bestritten, es handele sich hier nicht um „automatisierte Entscheidungen."

Nach meiner Auffassung riskieren wir aber doch Eingriffe in die Persönlichkeitsrechte der Betroffenen. Die Gefahr gezielter individueller Manipulationen und Diskriminierungen ist nicht von der Hand zu weisen.

Wir sollten daher über eine rechtliche Klarstellung mit dem Ziel nachdenken, alle Formen eines umfassenden und komplexen

Profilings einer grundsätzlichen Vorschrift zum Verbot von automatisierten Einzelfallentscheidungen zu unterwerfen.

Der zitierte Artikel 22 ist die einzige Regelung der DSGVO zu automatisierten Auswertungsprozessen auf der Basis von Algorithmen. Die Komplexität der Algorithmen nimmt aber stetig zu; ihre Transparenz und ihre Kontrollierbarkeit durch die Aufsichtsbehörden drohen dabei auf der Strecke zu bleiben. **Auch hier mahne ich für den Prozess der Evaluation gesetzlichen Klarstellungsbedarf an.**

Eine wirksame und verantwortungsvolle Kontrolle ist in diesem Zusammenhang aber nur dann möglich, wenn sich der Algorithmus nicht länger hinter Betriebs- und Geschäftsgeheimnissen verbergen darf.

V. Abschluss

Ich hoffe sehr, dass ich Ihnen mit meinen Anmerkungen nicht den Appetit verdorben habe. Aber bei Wein und gutem Essen werden wir noch genügen Gelegenheit haben, die aufgeworfenen Fragen zu vertiefen.

Ich freue mich auf diesen Abend und danke Ihnen für Ihre Aufmerksamkeit.