POSITIONSPAPIER

Berlin, 2. Juli 2019

Deutscher Industrie- und Handelskammertag

Evaluierung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO)

Wer wir sind:

Unter dem Dach des Deutschen Industrie- und Handelskammertags (DIHK) haben sich die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich der DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Darüber hinaus koordiniert der DIHK das Netzwerk der 140 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 92 Ländern.

Er ist im Register der Interessenvertreter der Europäischen Kommission registriert (Nr. 22400601191-42).

Vertretung des DIHK | Deutscher Industrie- und Handelskammertag e.V. bei der EU
B19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Internet: http://www.dihk.de

I. Anlass

Die Verordnung (DSGVO) sieht in Art. 97 vor, dass die EU-Kommission im Jahre 2020 dem Europäischen Parlament einen Bericht „über die Bewertung und Überprüfung dieser Verordnung“ vorlegen muss. Der Deutsche Industrie- und Handelskammertag e. V. will sich mit seinem Positionspapier an der Diskussion über die Umsetzung der Verordnung beteiligen. Dazu hat er mit Unterstützung der Industrie- und Handelskammern eine Umfrage bei ca. 4.500 Unternehmen aller Branchen und Größenordnungen durchgeführt. Dabei zählten über 80 % der Unternehmen, der Mitarbeiterzahl nach, zu den KMUs nach der Definition der Europäischen Kommission. Aber auch Unternehmen, die zwischen 250 bis über 1.000 Mitarbeiter beschäftigen, haben sich an der Umfrage beteiligt.

II. Forderungen

Ausgehend von den Ergebnissen unserer Umfrage, sollte die Kommission folgende Punkte bei der Evaluierung der DSGVO berücksichtigen:

- Das ursprüngliche Ziel der Harmonisierung und Rechtsvereinheitlichung sollte stringenter verfolgt werden. Die Möglichkeit der Öffnungsklauseln führen in der Praxis zu einer Rechtszersplitterung, die wiederum zu unterschiedlichen Marktbedingungen innerhalb der EU für die Unternehmen führt. In Deutschland zeigt sich das insbesondere anhand der Regelungen für die Bestellung des betrieblichen Datenschutzbeauftragten sowie für den Beschäftigtendatenschutz.
- Es gibt ein enormes Bedürfnis nach Rechtssicherheit. Die Sorge vor Abmahnungen besteht. Rechtsunsicherheit könnte unter anderem durch verbindliche Muster und Standardverträge vermieden werden. Zudem sind einheitliche Leitlinien der Aufsichtsbehörde geeignet, mehr Rechtssicherheit zu schaffen. Insgesamt besteht der Wunsch nach einer einheitlichen Rechtsauslegung und auch Interpretation durch die Aufsichtsbehörden.
- Erleichterungen für KMU sind dringend erforderlich, etwa durch vereinfachte Vorschriften oder Ausnahmeregelungen, denn die Umsetzung der DSGVO belastet KMU überproportional stark. Erwägungsgrund 13 sollte als Auftrag zum gesetzgeberischen Handeln verstanden werden.
- Allgemein wird die Dokumentations- und Nachweispflicht als zu streng und nicht verhältnismäßig erachtet. Erleichterungen könnten hier eingeführt werden, wenn bspw. die Verarbeitung der Daten nicht den Schwerpunkt der unternehmerischen Tätigkeit darstellt. So wird angeregt, für den gesamten B2B-Bereich im Rahmen der Art. 12 ff. DSGVO Erleichterungen zu schaffen.
- In diesem Zusammenhang wird auch der Mangel des Konzernprivilegs gerügt. Für Unternehmen einer Unternehmensgruppe sollten Privilegierungen vorgesehen werden.
- Die Erfahrungen mit der Umsetzung der DSGVO sollten für die Gesetzgebung zur E-Privacy-Verordnung beachtet werden:

Vertretung des DIHK | Deutscher Industrie- und Handelskammertag e.V. bei der EU
B19 A-D, Avenue des Arts | B–1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Internet: http://www.dihk.de

- Gesetzliche Anforderungen, die Unternehmen nur unter einem hohen finanziellen und personellen Aufwand umsetzen können, mindern die Akzeptanz der Regelung erheblich und führen letztendlich nicht zum Ziel. Zu nennen wäre hier das Erfordernis der Einwilligung als durchgehende Rechtsgrundlage in der E-Privacy-VO.
- Da zu befürchten steht, dass die E-Privacy-VO ähnliche Konsequenzen bei der konkreten Umsetzung wie die DSGVO haben wird, sollte die E-Privacy-VO die Bedürfnisse und die Praxisrealität der KMU stärker berücksichtigen und Erleichterungen bzw. Ausnahmen für KMU vorsehen.
- Die Gesetzgebung muss flankiert werden von erklärenden und beratenden Maßnahmen, um die Regelungen auch für KMU umsetzbar zu machen. Das gilt insbesondere auch für den Aspekt der technischen Umsetzung.
- Die E-Privacy-VO und die DSGVO sollten konsistent und kohärent sein.

III. Allgemeines

Datenschutz ist ein Grundrecht nach Art. 16 AEUV. Die EU ist daher verpflichtet, dieses Grundrecht auszugestalten. Dieser Pflicht ist sie durch die Verabschiedung der Verordnung nachgekommen.

Datenschutz ist angesichts einer rasant fortschreitenden Digitalisierung des privaten und öffentlichen Lebens ein wesentliches und wichtiges Element des europäischen Binnenmarkts. Regelungen dazu können wegen der globalen Datenströme nicht mehr von einzelnen Nationalstaaten beschlossen werden, sondern es bedarf Staaten-übergreifender Vorschriften. Die DSGVO kann aber nur ein Mosaikstein auf dem Wege zu internationalen Regelungen sein.

Solange es keine verbindlichen internationalen Vereinbarungen gibt, muss die EU mit dem Instrument der Angemessenheitsbeschlüsse schneller agieren, als das bisher der Fall war. Zudem müssen die Beschlüsse auch dauerhaft und belastbar sein, was im Falle des Privacy Shield fraglich ist.

So dürfen bei einem Austritt Großbritanniens ohne eine Vereinbarung zur Fortgeltung der DSGVO keine zu hohen Ansprüche an einen Angemessenheitsbeschluss gestellt werden, wenn die EU gleichzeitig über eine E-Evidence-Verordnung entscheiden wird.

Fraglich bleibt, ob die DSGVO ausreichend zukunftsorientiert ist und den Anforderungen z. B. von Künstlicher Intelligenz genügen kann.

IV. Auswirkungen des Inkrafttretens

Bereits nach dem Inkrafttreten der DSGVO am 24.05.2016 begann die Diskussion über ihre Umsetzung. Ende 2017/Anfang 2018 – also mit Blick auf das Gültigkeitsdatum der DSGVO am 25.05.2018 – nahm die Auseinandersetzung mit der DSGVO einen immer größeren Raum bei den Unternehmen ein. Das galt für alle Größenklassen und Branchen. Industrie- und Handelskammern nahmen einen umfangreichen Bedarf an Informationen und Beratungen bei den Unternehmen wahr.

Viele Veranstaltungen wurden durchgeführt, um sowohl allgemein über die Anforderungen der DSGVO zu informieren, aber auch zu konkreten Umsetzungsschritten zu beraten. Eine Roadshow mit Unterstützung des Bundesministeriums für Wirtschaft und Energie trug ebenfalls zur Information der Unternehmen bei. Dabei zeigte sich, dass auch größere Unternehmen einen erheblichen Personal- und Kostenaufwand betreiben mussten, um die DSGVO umzusetzen, insbesondere wenn sie grenzüberschreitend tätig sind. Kleine und mittlere Unternehmen haben bis heute Schwierigkeiten, die DSGVO umzusetzen, weil sie nicht über das notwendige Know-how verfügen und der Markt den Bedarf an kompetenten Beratern kaum befriedigt. Die Datenschutzaufsichtsbehörden können den Beratungsbedarf ebenfalls nicht decken.

Damit verbunden gibt es ein weiteres Problem: die Rechtsunsicherheit, die mit der Interpretationsfähigkeit der DSGVO verbunden ist. Einerseits ergeben sich daraus Spielräume für die Unternehmen, wie sie konkret die Umsetzung gestalten. Andererseits zeigt sich, dass Datenschutzaufsichtsbehörden, Gerichte und Berater zu unterschiedlichen Ergebnissen kommen, z. B. beim Thema der gemeinsamen Verantwortung. Dies trägt zur Verwirrung der Unternehmen und ihrer Sorge bei, bei Aufsichtsmaßnahmen Sanktionen ausgeliefert zu sein.

V. Ziele der DSGVO

1. Harmonisierung

Eines der wichtigsten Argumente zur Schaffung der DSGVO war die Vollharmonisierung des Datenschutzrechts in der EU – ein grundsätzlich zu unterstützender Ansatz. Dies belegt auch das Ergebnis der Umfrage. Aufgrund der Öffnungsklauseln besteht aber für die Mitgliedstaaten ein Spielraum für nationale Regelungen, der zu Goldplating führen kann – zu denken ist hier an den Beschäftigtendatenschutz. Zudem sind auch die Aufsichtsbehörden in den einzelnen Mitgliedstaaten bei Entscheidungen im nationalen Rahmen frei in der Interpretation der DSGVO, was zu unterschiedlichem Vorgehen in den Mitgliedstaaten führt.
Nicht für alles wird der Europäische Datenschutzausschuss eine EU-weit geltende Auslegung finden können. Hinzu kommt, dass der Ausschuss nach dem Prinzip des kleinsten gemeinsamen Nenners vorgehen muss, wenn er Beschlüsse fasst.

Die Aufsichtsbehörden in den Mitgliedstaaten sind ferner weiterhin unterschiedlich personell und sachlich ausgestattet, so dass sich allein schon daraus Unterschiede in der Rechtsdurchsetzung ergeben.

Insofern ist zu hoffen, dass das Kohärenzverfahren zu einer stärkeren Vereinheitlichung von Rechtsauffassungen beitragen wird.

Aus der Umfrage ergibt sich, dass die Öffnungsklauseln der DSGVO von knapp einem Drittel der Befragten positiv gesehen werden; etwa die Hälfte der Unternehmen sieht sich jedoch davon nicht betroffen. Kritisch sehen Unternehmen, die die Öffnungsklauseln negativ beurteilen, die Gefahr der Rechtszersplitterung und den damit einhergehenden Wettbewerbsnachteil durch meist strengere Regelungen in Deutschland (Wettbewerbsverzerrung) an.
Folgen sind ein erhöhter Aufwand, um z. B. einen Überblick über die nationalen Regelungen zu erhalten und sie zu befolgen; das gilt z. B. für die Bestellung eines geeigneten

Datenschutzbeauftragten oder die Regelungen des Beschäftigtendatenschutzes. Als Nachteil wird aber auch die unterschiedliche Rechtsauslegung sowie die Vorgehensweise/Strenge der Aufsichtsbehörden gesehen. Eine Mehrheit derer, die Erfahrungen mit datenschutzrechtlichen Regelungen in anderen
EU- Mitgliedstaaten gemacht haben, gaben an, dass diese dort weniger streng sind. Der Wunsch nach Rechtsharmonisierung und einem einheitlichen Rechtsrahmen innerhalb der EU ist bei den befragten Unternehmen sehr hoch. Denn zusätzliche Regelungen zur DSGVO erhöhen die Rechtsunsicherheit und den Regelungsaufwand für grenzüberschreitend tätige Unternehmen.

2. Marktortprinzip

Das Marktortprinzip wird von großen Unternehmen als Schaffung eines level playing field begrüßt. Dennoch zeigt sich, dass die Möglichkeiten, große Unternehmen aus Drittländern zur Einhaltung der DSGVO zu verpflichten, eine Herausforderung ist. Dies muss auf europäischer Ebene zeitnah angegangen werden, um nicht den Eindruck zu erwecken, dass nur KMU Sanktionen unterworfen sind.

3. Interessenausgleich zwischen Bürgern und Wirtschaft

Die DSGVO enthält zwei Aspekte: zum einen den Schutz der Privatsphäre der EU-Bürger, zum anderen den freien Datenverkehr, also die Möglichkeit für Unternehmen, Daten zu verarbeiten und grenzüberschreitend zu nutzen. Die Auflösung der widerstreitenden Interessen zwischen der wirtschaftlichen Nutzung von Daten und ihrem Schutz ist in der DSGVO eher zugunsten der Bürger entschieden worden. Anwendungen wie Big Data oder auch im Rahmen von Künstlicher Intelligenz bereiten insbesondere Unternehmen, deren Geschäftsmodelle allein in der Verarbeitung von Daten besteht, erhebliche Schwierigkeiten.
Die Umfrage zeigt, dass unabhängig von der Beschäftigtenzahl des Unternehmens der Großteil der Teilnehmer den Datenschutz als ein wichtiges Thema für ihr Unternehmen einstuft.

4. Risikobasierter Ansatz

Die DSGVO geht von einem risikobasierten Ansatz aus, also einem flexiblen Reagieren auf die jeweiligen Datenschutzanforderungen. So ist die stärkere Verknüpfung von Datenschutz und Informationssicherheit ein positiver Aspekt. Allerdings wird der risikobasierte Ansatz nicht konsequent durchgehalten. Denn lediglich in Art. 37 wird darauf Bezug genommen, dass eine Managementaufgabe wie die Bestellung eines betrieblichen Datenschutzbeauftragten davon abhängig ist, ob das Unternehmen die Datenverarbeitung als „Kerntätigkeit“ betreibt. Ansonsten gilt der Grundsatz „one size fits all”. Das trifft jedoch weder die Unternehmenswirklichkeit, noch verbessert es den Datenschutz. Sämtliche anderen Pflichten gelten unabhängig von Unternehmensgröße oder Geschäftsgegenstand.
Der Verbesserung des Datenschutzes dient der risikobasierte Ansatz insofern nicht, als er die vielen bürokratisch zu erfüllenden Pflichten wie z. B. die Informationspflicht nach Art. 13, 14 auch dann vorsieht, wenn es sich um vertragliche Beziehungen handelt, beide Seiten also wissen, welche Daten für welchen Zweck verarbeitet werden.

VI. Auswirkungen auf die Unternehmenswirklichkeit

1. Positive und negative Aspekte

Die Umfrage ergibt, dass je größer ein Unternehmen ist, desto mehr positive Aspekte werden gesehen. Die DSGVO schafft höhere Transparenz für die Verarbeitung personenbezogener Daten. Das Inkrafttreten der DSGVO wurde zum Anlass genommen, die eigenen Prozesse und Strukturen zu überprüfen und zu optimieren sowie zu professionalisieren. Daten wurden minimiert und bereinigt, Verfahren standardisiert. Ferner hat die DSGVO zu einem erhöhten Bewusstsein und einer Sensibilisierung für Datenschutz bei den Mitarbeitern und der Geschäftsleitung, aber auch bei Kunden geführt. Die stärkere Verknüpfung von Datenschutz und Datensicherheit wird ebenfalls positiv bewertet.

Mehr als die Hälfte der Unternehmen sehen für ihr Unternehmen jedoch gar keine positiven Aspekte. Zahlreiche Unternehmen sehen die Bedeutsamkeit eines funktionierenden Datenschutzes, bewerten die DSGVO aber als über das Ziel hinausschießend. Insbesondere der mit der Einführung der DSGVO einhergehende enorm erhöhte Bürokratieaufwand wird von der überwiegenden Mehrheit (fast 90 %) der befragten Unternehmen bemängelt, ca. 70 % geben eine hohen bis sehr hohen finanziellen, ca. 60 % einen hohen bis sehr hohen personellen Aufwand an.

Der größte Aufwand entstand bei der Erstellung der Verarbeitungsverzeichnisse, den Informationspflichten/der Datenschutzerklärung und den technisch-organisatorischen Maßnahmen sowie der Auftragsverarbeitung. Genannt wurden daneben die Einführung eines Datenschutzmanagements, insbesondere die Erstellung und Umsetzung eines Löschkonzept, und bei größeren Unternehmen der internationale Datentransfer.
Bemängelt wurde auch die kurze Frist für die Meldung von Datenverstößen, die in der Praxis kaum eingehalten werden kann.

Unternehmen sehen sich bereits jetzt mit umfangreichen Auskunftsansprüchen konfrontiert. Besondere Relevanz kommt dieser Frage z. B. in Fällen zu, in denen ein ehemaliger Mitarbeiter um Aushändigung bestimmter E-Mails bittet oder ein Angestellter sämtliche interne Unternehmenskommunikation herausverlangt.

2. Auswirkungen auf geschäftliches Handeln

Einige Unternehmen gaben an, dass sie aufgrund der gesteigerten Erfordernisse, aber auch wegen der entstandenen Rechtsunsicherheit und dadurch gestiegener Abmahngefährdung Geschäftsmodelle eingeschränkt oder gar aufgegeben haben. Dies betraf vor allem die Bereiche Fotografie, Werbung, Web- und Social-Media-Marketing sowie allgemein datenbetriebene Geschäftsmodelle etwa im Gesundheitsbereich. Selbst die Verwendung von E-Mails z. B. für Werbung wurde aufgegeben.

3. Resonanz der Kunden und Geschäftspartner

Die DSGVO ist u. a. mit dem Hinweis angepriesen worden, dass sie den Unternehmen in der EU einen Wettbewerbsvorteil gegenüber Konkurrenten erbringt. Dazu muss aber der Datenschutz bei Kunden und Geschäftspartnern positiv wahrgenommen werden. Laut Umfrage

sehen jedoch 70 % der Teilnehmer weder einen Wettbewerbsvorteil noch einen Imagegewinn darin. Insbesondere beschweren sich Kunden häufig über die Informationsflut.

Die Usability der Kommunikation ist den Kunden häufig wichtiger (z. B. WhatsApp).

4. Besondere Situation der kleineren und mittleren Unternehmen

Kleinst-, kleine und mittlere Unternehmen erleben die Umsetzung der DSGVO als noch belastender als größere Unternehmen. Ihnen fehlt Personal, das sich um die Implementierung kümmern könnte, und externe Berater sind teuer bzw. gar nicht mehr zu verpflichten. In den Beratungen der IHKs hat sich bereits gezeigt, was durch die Umfrage bestätigt wird, dass daher KMU ein großes Interesse an Musterdokumenten, Leitfäden, Checklisten oder Standardvorgaben haben, die sie – wenn überhaupt – schnell an ihre Unternehmenswirklichkeit anpassen können, um damit auch sicher sein zu können, die Vorschriften einzuhalten.

Unabhängig von der konkreten Unterstützung bei der Umsetzung fordern die KMU aber generell Entlastungen von den gesetzlichen Pflichten. Die für KMU geregelte Ausnahme in Art. 30 Abs. 5 entpuppt sich als faktisch nicht geltend. Der Aussage des Erwägungsrunds 13, der „besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen“ Rechnung tragen zu wollen, kommt die DSGVO nicht nach. So wäre z. B. zu prüfen, ob als Kriterium für die Prüfung der Verhängung von Bußgeldern nach Art. 83 DSGVO kleine und mittlere Unternehmen im Rahmen des Abs. 2 explizit vorgesehen werden könnten.
Auch bei der Erstellung des Verarbeitungsverzeichnisses und bei den Informationspflichten erhoffen sich die Unternehmen Erleichterungen. Hierbei sollte nach Geschäftsmodellen abgestuft werden: So sollten z. B. kleine Industrieunternehmen, die keine Endverbraucher als Kunden haben, aufgrund des risikobasierten Ansatzes von Informationsplichten befreit werden.

Ansprechpartner:

Annette Karstedt-Meierrieks
Bereich Recht
Leiterin des Referats Wirtschaftsverwaltungsrecht, Öffentliches Auftragswesen, Datenschutz

DIHK – Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29, 10178 Berlin
Tel.: (030) 20308-2706
Fax: (030) 20308-5-2706
mailto: karstedt-meierrieks.annette@dihk.de
http://www.dihk.de

Kei-Lin Ting-Winarto
Bereich Recht
Leiterin des Referats Datenschutz

DIHK - Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29, 10178 Berlin
Tel.: (030) 20308-2717
Fax: (030) 20308-5-2717
mailto: ting-winarto.kei-lin@dihk.de
http://www.dihk.de