Sitzung der Vollversammlung am 21. November 2019

Verabschiedung des IHK-Positionspapiers zur Datenschutzgrundverordnung

Einleitung

Die EU-Verordnung 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) 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.

Die Industrie- und Handelskammer Nord Westfalen (IHK NW) will sich mit ihrem Forderungspapier an der Diskussion über die Umsetzung der Verordnung beteiligen. Darum hat sie zusammen mit der Handwerkskammer (HWK) Münster eine Umfrage bei den Mitgliedern der regionalen Wirtschaft durchgeführt, an der sich Unternehmen aller Branchen und Größenordnungen beteiligt haben.

Ausgehend von den Ergebnissen unserer Umfrage hat eine gemeinsame Arbeitsgruppe der IHK NW und der HWK Münster dieses Positionspapier erarbeitet.

Die Kommission sollte folgende Punkte bei der Evaluierung der DSGVO berücksichtigen:

Forderungen

1. Es bedarf einer gesetzlichen Klarstellung, wonach Vorschriften zum Datenschutz nicht vom Anwendungsbereich des Gesetzes gegen den unlauteren Wettbewerb (UWG) erfasst werden.

2. Die Verpflichtung zur Information der von einer Datenverarbeitung betroffenen Person nach den Artikeln 13, 14 DSGVO entfällt, wenn zwischen den Parteien keine vertragliche Vereinbarung zustande kommt. Alternativ wird es als ausreichend für die Erfüllung einer Informationspflicht angesehen, wenn die erforderliche Information durch den Verweis auf eine andere Stelle im Rahmen der Erhebung der Daten erfolgt – sog. Medienbruch.

3. Die Kriterien, wann ein Vertrag zur sog. Auftragsdatenverarbeitung nach Art. 28 DSGVO abzuschließen ist, sind zu konkretisieren oder durch eine harmonisierte Rechtsauslegung der Aufsichtsbehörden sicherzustellen.

4. Die Erstellung von Verarbeitungsverzeichnissen kann anhand von einfachen Musterverarbeitungsverzeichnissen erfolgen, die von den jeweiligen Aufsichtsbehörden vorausgefüllt zur Verfügung gestellt werden.

5. Die Kriterien für ein IT-Sicherheitskonzept nach Art. 32 DSGVO sind gesetzlich zu konkretisieren oder durch eine harmonisierte Rechtsauslegung der Aufsichtsbehörden sicherzustellen.
6. Die Erfahrungen mit der Umsetzung der DSGVO sollten für die Gesetzgebung zur E-Privacy-Verordnung beachtet werden. Es ist zu befürchten, dass die E-Privacy-VO ähnliche Konsequenzen bei der konkreten Umsetzung wie die DSGVO haben wird. Darum sollte die E-Privacy-VO die Bedürfnisse und die Praxisrealität der KMU stärker berücksichtigen und Erleichterungen bzw. Ausnahmen für KMU vorsehen.

Allgemeines

Durch die DSGVO ist erstmals ein einheitliches europäisches Datenschutzrecht geschaffen worden. Zusammen mit den nationalen Datenschutzgesetzen etabliert die DSGVO erhebliche administrative Anforderungen an Unternehmen bei gleichzeitiger Gewährung von vielfältigen Betroffenenrechten zur Durchsetzung des Rechts auf informationelle Selbstbestimmung. Diese Zielrichtung ist sicherlich der richtige Ansatz, wenn es darum geht, der Digitalbranche einen Rechtsrahmen zu setzen, der einen ausgewogenen Ausgleich zwischen dem Erwerbsinteresse der Digitalbranche und dem Schutzbedürfnis von natürlichen Personen darstellt. Er greift aber zu weit, wenn er die für diesen Rechtsrahmen sicherlich richtige Zielsetzung auch auf „analoge Unternehmen“ ausweitet. Die fehlende Unterscheidung zwischen Unternehmen, deren Hauptgeschäftszweck die Verarbeitung und wirtschaftliche Verwertung von personenbezogenen Daten ist und klein- und mittenständischen Unternehmen, die personenbezogene Daten nur als Nebenzweck zur ihrer eigentlichen wirtschaftlichen Betätigung verarbeiten, erfordert auch eine Trennung der für diese Bereiche geltenden Rechtsrahmen.

Aus diesem Grunde muss es eine Freistellung von Unternehmen für verschiedene Regelungsbereiche geben, in denen die Datenverarbeitung nur einen Nebenzweck zur eigentlichen wirtschaftlichen Betätigung darstellt. Die DSGVO verfolgt diesen Ansatz bereits an wichtiger Stelle, wenn sie von der Verpflichtung zum Führen eines Verfahrensverzeichnisses in Art. 30 Abs. 5 DSGVO Unternehmen ausnimmt, die weniger als 250 Mitarbeiter beschäftigen. Dieser absolut richtige Ansatzpunkt wird allerdings in der Praxis vollständig durch die Rückausnahme in Art. 30 Abs. 5 DSGVO entwertet, wonach die Verarbeitung der personenbezogenen Daten in diesen Fällen

nicht nur gelegentlich erfolgen darf. Eine „nicht nur gelegentliche“ Verarbeitung personenbezogener Daten ist allerdings selbst bei Unternehmen, die Daten nur als Nebenzweck zu ihrer eigentlichen Tätigkeit verarbeiten, nur schwer bis überhaupt nicht vorstellbar.

Richtigerweise muss die Bereichsausnahme des Art. 30 Abs. 5 DSGVO daher um die Rückausnahme „nicht nur gelegentliche Verarbeitung“ bereinigt werden und der in Art. 30 Abs. 5 DSGVO niedergelegte Rechtsgedanken ist auf folgende Regelungsbereiche auszudehnen:

- Informationspflichten nach den Artikeln 13 und 14 DSGVO
- Datenschutz-Folgenabschätzung nach Art. 35 DSGVO
- Auftragsverarbeitung nach Art. 28 DSGVO
- Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen nach Art. 25 DSGVO

Darüber hinaus besteht ein erhebliches Interesse der Wirtschaft an einheitlichen rechtlichen Rahmenbedingungen, die nicht davon abhängen, wo sich der jeweilige Unternehmenssitz oder Sitz einer Zweigstelle befindet. Insbesondere bei Unternehmen, die über mehrere Zweigniederlassungen verfügen, die sich ggf. auch über mehrere Bundesländer erstrecken, besteht ein Bedürfnis nach einer einheitlichen Rechtsauslegung der Aufsichtsbehörden. Diese gemeinsame Auslegung der Aufsichtsbehörden ist aktuell in zentralen Rechtspunkten fraglich. Beispielsweise wird die Frage, wann eine ständige Beschäftigung mit automatisierter Datenverarbeitung vorliegt, die ab einer bestimmten Anzahl von derartigen Beschäftigten zur Benennungspflicht eines Datenschutzbeauftragten führt, je nach Bundesland unterschiedlich beantwortet.

Diese unklare Rechtsauslegung ist insbesondere wegen der damit verbundenen Sanktionsmöglichkeiten für Unternehmen nicht hinnehmbar. Aus diesem Grunde spricht viel dafür, die Datenschutzaufsicht über Materien, die dem BDSG unterfallen, zentral dem Bundesbeauftragten für Datenschutz zuzuweisen.

Im Übrigen haben die von den Regelungen des Datenschutzrechts betroffenen Unternehmen ein dringendes Interesse daran, dass ihnen von den zuständigen Aufsichtsbehörden bundeseinheitlich abgesprochene Formulare bzw. Vordrucke zur Verfügung gestellt werden.

Unabhängig von diesen Kernthesen besteht hinsichtlich der DSGVO auch in folgenden Regelungsbereichen Handlungsbedarf:

Im Einzelnen

- Abmahnfähigkeit von Verstößen gegen die DSGVO

Auf der Grundlage der aktuellen Rechtsprechung besteht große Verunsicherung, ob und ggf. in welchem Umfang Verstöße gegen die DSGVO nach dem Gesetz gegen unlauteren Wettbewerb

abgemahnt werden können. Während ein Landgericht ohne erkennbare sachliche Begründung eine Abmahnung auf der Grundlage der DSGVO zugelassen hat, halten andere Instanzgerichte im Einklang mit der überwiegenden Meinung in der Literatur das Sanktionsregime der DSGVO für abschließend und verneinen dementsprechend die Möglichkeit einer Abmahnung auf der Grundlage der DSGVO.

Diese unklare und nicht prognostizierbare Auslegung führt zu einer großen Verunsicherung insbesondere bei klein- und mittelständischen Unternehmen, die befürchten müssen, schon für geringfügige Verstöße gegen die DSGVO von sog. “Abmahnfabriken“ kostenpflichtig abgemahnt zu werden. Darüber hinaus sind die Bestimmungen der DSGVO Ausfluss des Rechtes auf informationelle Selbstbestimmung und dienen nicht der Regelung des Marktverhaltens zwischen Unternehmen. Den zuständigen Aufsichtsbehörden stehen durch das Sanktionsregime der DSGVO und den nationalen Datenschutzgesetzen ausreichende Möglichkeiten zur Verfügung, einen effektiven Schutz dieses Grundrechts sicherzustellen. Die Klarstellung, dass Verstöße gegen Vorschriften der Datenschutzgesetze nicht abmahnfähig sind, sollte gesetzgeberisch geklärt werden.

- Informationspflichten nach den Artikeln 13 und 14 DSGVO

Auf der Grundlage der Artikel 13, 14 DSGVO ist der Verantwortliche im Zeitpunkt der Datenerhebung verpflichtet, den Betroffenen über die Datenverarbeitung zu informieren. In der Praxis bestehen auch hier erhebliche Auslegungsschwierigkeiten, da von den Aufsichtsbehörden teilweise vertreten wird, dass die z. B. im Rahmen eines Vertragsabschlusses zu erteilende Information nicht durch den Verweis auf einen anderen Ort (z.B. auf der Homepage), an dem die Information bereitgestellt wird, erfolgen kann (sog. Medienbruch).

Die vom Grunde her bereits zeitlich weit vor den eigentlichen Vertragsabschluss nach vorne verlagerte Informationspflicht hat sicherlich ihre Berechtigung, wenn zwischen den Parteien tatsächlich ein Vertragsverhältnis entsteht, in dessen Verlauf notwendige Daten verarbeitet werden und gesetzliche Aufbewahrungspflichten an den verarbeiteten Daten entstehen. Etwas anderes muss aber dann gelten, wenn ein Unternehmen, dessen Unternehmenszweck nicht in der wirtschaftlichen Verwertung von Daten besteht, Daten lediglich für Vertragsverhandlungen verarbeitet. In diesen Fällen werden die verarbeiteten Daten nach kurzer Frist wieder gelöscht, falls es zwischen den Parteien zu keinen aufbauenden rechtlichen Beziehungen mehr kommt. Nach der derzeitigen strengen Gesetzesauslegung würde eine Information der von einer Datenverarbeitung betroffenen Person zu einem erheblichen bürokratischen Aufwand führen, der wegen der kurzen Löschfristen in keinem vertretbaren Verhältnis zu den Anforderungen des Datenschutzrechts steht.

Alternativ könnte eine Verminderung des bürokratischen Aufwands auch darin gesehen werden, dass es grundsätzlich als ausreichend für die Erfüllung einer Informationspflicht angesehen wird, wenn die erforderliche Information für den Betroffenen beispielsweise auf einer Webseite mit einem entsprechenden Verweis bei der Datenerhebung abrufbar ist. Auch bei dieser Variante ist

sichergestellt, dass der Bearbeitungsaufwand sich bei dem verarbeitenden Unternehmen in überschaubaren Grenzen hält.

- Auftragsverarbeitung nach Art. 28 DSGVO

Eine der grundlegenden Problematiken im Bereich der DSGVO ist die Frage, wann ein Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen werden muss. In der Praxis werden immer wieder Unternehmen aufgefordert, derartige Verträge abzuschließen, obwohl deutlich erkennbar ist, dass die gesetzlichen Voraus-setzungen nicht vorliegen. Diese Vorgehensweise ist insbesondere dem Umstand geschuldet, dass die Verwender derartiger Vertragsformulare nicht Gefahr laufen wollen, vom Sanktionsregime der DSGVO erfasst zu werden. Auch hier wäre es wünschenswert, wenn klargestellt würde, dass Auftragsverarbeitung im daten-schutzrechtlichen Sinne nur in den Fällen vorliegt, in denen eine Stelle von einer anderen Stelle weisungsgebunden im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird. Neben dieser gesetzgeberischen Klarstellung bedarf es auch einer eindeutigen Auslegung der entsprechenden Vorschrift durch die Aufsichtsbehörden, die durch die Datenschutzkonferenz des Bundes und der Länder sicherzustellen ist.

- Verarbeitungsverzeichnisse nach Art. 30 DSGVO

Insbesondere die Erstellung von Verarbeitungsverzeichnissen erfordert einen erheblichen administrativen Aufwand bei den Daten verarbeitenden Unternehmen. Neben der ständigen Aktualisierung und Pflege der einzelnen Verzeichnisse besteht ein weiteres Problem darin, dass in jedem Unternehmen eine ungezählte Fülle von einzelnen Datenverarbeitungsvorgängen vorliegen, die eine eingehenden Beschäftigung mit dieser administrativen Aufgabe erfordern. Diese nicht unerheblichen Anforderungen bereiten insbesondere Kleinstbetrieben ohne Beschäftigte erhebliche Probleme, da deren Geschäftsbetrieb in der Regel nicht auf die Ausarbeitung derartig komplexer Verzeichnisse ausgerichtet ist. Wenn man die bisherige strenge Regelung beibehalten möchte, wonach auch Kleinstbetriebe von der Vorschrift erfasst werden, wäre es angezeigt, die Unternehmen durch einfache Handreichungen (wie z.B. vorausgefüllte Muster) und zurückhaltende Auslegung von Vorschriften zu entlasten.

- Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Darüber hinaus bereitet die Frage, welche konkreten technischen und organisatorischen Maßnahmen im speziellen Einzelfall umzusetzen sind, den Unternehmen Umsetzungsprobleme. Die einschlägige Vorschrift des Art. 32 DSGVO enthält eine Vielzahl von unbestimmten Rechtsbegriffen, die es dem nicht täglich mit Fragen zu Datenverarbeitungsvorgängen beschäftigten Unternehmer beinahe unmöglich machen, das für sein Unternehmen einschlägige Niveau der Datensicherheit zu bestimmen. Auch diese Schwierigkeiten begegnen unter Betrachtung der mit einer Verletzung dieser Vorschriften einhergehenden Sanktionsmöglichkeiten erheblichen Bedenken.

Die Anforderungen an die technischen und organisatorischen Maßnahmen bereiten wiederum insbesondere Kleinstbetrieben ohne Beschäftigte erhebliche Probleme, da deren Geschäftsbetrieb in der Regel nicht auf die Einrichtung einer komplexen Sicherheitsstruktur ausgerichtet ist. Wenn man die bisherige strenge Regelung beibehalten möchte, wonach auch Kleinstbetriebe von der Vorschrift erfasst werden, wäre es auch hier angezeigt, die Unternehmen durch einfache Handreichungen und zurückhaltende Auslegung von Vorschriften zu entlasten.

Verabschiedet von der Vollversammlung am 21. November 2019.