**Landesbeauftragte
für Datenschutz und Informationsfreiheit
des Landes Nordrhein-Westfalen**

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/1736

Alle Abgeordneten

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

Datum: 2. September 2024

Geschäftszeichen

Landtag NRW
- Rechtsausschuss -
Platz des Landtags 1
40221 Düsseldorf

Telefon 0211 38424-101/103

- Übermittlung erfolgt ausschließlich elektronisch -

Antrag der Fraktion der FDP, Drucksache 18/7759 - Datenschutzrecht in Deutschland entbürokratisieren und Rechtssicherheit schaffen – den Beschlüssen der Datenschutzkonferenz muss eine rechtsverbindliche Wirkung zukommen.

**Anhörung von Sachverständigen
im Rechtsausschuss des Landtags von Nordrhein-Westfalen am 17.9.2024**

Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen

Sehr geehrter Herr Landtagspräsident,
sehr geehrte Damen und Herren Abgeordnete,

ich danke Ihnen für die Einladung zur Anhörung und nehme dazu wie folgt vorab schriftlich Stellung:

Ich begrüße die mit dem Antrag verbundene Intention, die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu stärken und ihr eine wichtige Rolle in der national einheitlichen Anwendung der Datenschutz-Grundverordnung (DS-GVO) im Sinne des Art. 51 Abs. 2 DS-GVO zuzuweisen. Diese Rolle entspricht dem Selbstverständnis der DSK, wie sich bereits aus dem in ihrer Geschäftsordnung niedergelegten Zweck der DSK ergibt[1]. Der Bedeutung einer einheitlichen Auslegung des Datenschutzrechts für die Funktionsfähigkeit von Wirtschaft und Verwaltung in einer digitalisierten Welt ist sich die DSK sehr bewusst.

Ich möchte im Zusammenhang mit dem Antrag auf folgende Punkte näher eingehen:

I. Feststellungen zur Ausgangslage
II. Maßnahmen zur einheitlichen Anwendung der DS-GVO

Kavalleriestraße 2-4
40213 Düsseldorf
Telefon 0211 38424-0
poststelle@ldi.nrw.de

[1] Siehe unter II. https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_Stand_Februar-2024.pdf

I. Feststellungen zur Ausgangslage:

Nicht nur im Antrag sondern auch in Politik, Wirtschaft und Verwaltung wird eine heterogene Anwendung der DS-GVO durch die Datenschutzaufsichtsbehörden kritisiert. Auch im zweiten Bericht der Europäischen Kommission zur Umsetzung der DS-GVO vom 25.7.2024 nimmt dieses Thema einigen Raum ein[2]. In dem Bericht wird unter anderem angeführt, die Wirtschaft beklage, dass die Aufsichtsbehörden den risikobasierten Ansatz der DS-GVO nicht ausreichend berücksichtigten. Dies zeige sich etwa bei der Beurteilung von Anonymisierung, bei den Rechtsgrundlagen der Einwilligung oder des berechtigten Interesses oder bei den Ausnahmen von der automatisierten Einzelentscheidung[3].
Dabei bleibt die Kritik oberflächlich und befasst sich nicht mit den Ursachen vermeintlich heterogener Entscheidungen der Datenschutzaufsicht. Ohne die Ursachen zu betrachten, ist eine Einschätzung nur schwerlich möglich, ob eine Grundgesetzänderung geeignet ist, eine Lösung anzubieten.

Zunächst sind **Datenverarbeitungen selbst heterogen** und in der Regel auf die Bedürfnisse der Verarbeiter ausgerichtet. Selbst wenn standardisierte Software eingesetzt wird, nutzen die Anwender vorhandene Einstellungen zur Verarbeitung nach ihren individuellen Bedarfen. In der Folge scheinen Entscheidungen der Aufsichtsbehörden oft unterschiedlich. Tatsächlich sind aber die Verfahren nur ähnlich. Im Detail weisen sie aber erhebliche Unterschiede auf. Man kann eben nicht Äpfel mit Birnen vergleichen, auch wenn die Früchte von außen betrachtet ähnlich aussehen. Datenschutzbehörden müssen bei ihren Entscheidungen die Verarbeitung im konkreten Fall beurteilen und kommen deswegen notwendigerweise zu unterschiedlichen Entscheidungen, wenn es bei zwei ähnlichen Verarbeitungen aber im Detail signifikante Unterschiede gibt.

Das **Datenschutzrecht ist nicht eindeutig.** Es nutzt unbestimmte Rechtsbegriffe, die erst durch die Praxis an Kontur gewinnen. Üblicherweise bildet sich bei unbestimmten Rechtsbegriffen erst mit der Zeit eine Kasuistik der Verwaltung und Rechtsprechung heraus, die sich verfestigt und dann einheitlich angewendet werden kann. Nicht anders kann dies in der Datenschutzaufsicht funktionieren.

Als Beispiel soll eine zentrale Rechtsgrundlage dienen, auf die sehr viele Verarbeitungsprozesse der Wirtschaft gestützt werden, nämlich Art.6 Abs. 1, UAbs. 1 Buchstabe f DS-GVO. Nach dieser Vorschrift ergeben sich drei auszulegende Prüfpunkte: Ist das Interesse des Verarbeiters (oder anderer) an der Datenverarbeitung berechtigt? Ist die Verarbeitung genau dieser Daten für dieses Interesse erforderlich? Gibt es überwiegende berechtigte Interessen der

---

[2] Siehe Nrn. 2.5.3, 3.1, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52024DC0357
[3] aaO, 2.5.3

Betroffenen, die die Verarbeitung ausschließen? In der Regel sind die Antworten auf diese Fragen für jede Branche, jeden Fachbereich und jeden Verarbeitungsprozess andere. Will ein Verantwortlicher etwa ein kreditorisches Risiko einschätzen oder Daten von Mieter*innen an eine andere Stelle übermitteln, will er Werbung betreiben oder Daten über seine Beschäftigten erheben, in diesen und ganz vielen anderen Konstellationen sind es immer wieder unterschiedliche Datensätze, unterschiedliche Interessenlagen und unterschiedliche Grenzen, was erforderlich ist und was nicht. Es ist ein ständiger Prozess, hier Schritt für Schritt zu allgemeingültigen Lösungen für einzelne Bereiche zu kommen. Diese Arbeit läuft zwischen den Datenschutzaufsichtsbehörden ständig, sie wird teils auch durch die Rechtsprechung beeinflusst und wird laufend fortgesetzt werden müssen, weil sich auch Datenverarbeitung immer wieder verändert.

Auch in der Rechtsprechung sind sich Gerichte zu vergleichbaren Sachverhalten in der Anwendung des Datenschutzrechts teils Jahre lang bis zur Klärung durch alle Instanzen uneinig. Hier soll nur exemplarisch auf die heterogene Rechtsprechung zum datenschutzrechtlichen Auskunftsrecht hingewiesen werden[4]. Dem gegenüber dürfte der Einigungsgrad über die Anwendung des Datenschutzrechts bei den Aufsichtsbehörden sehr hoch und fortgeschritten sein. Einzelne Aufsichtsbehörden sind allerdings in ihren Entscheidungsmöglichkeiten auch an die Rechtsprechung der für sie jeweils relevanten Gerichte gebunden, wenn ihre Entscheidungen nicht ständig aufgehoben werden sollen. Auch dies kann dazu führen, dass Aufsichtsbehörden unterschiedliche Entscheidungen treffen, weil die Gerichte in einzelnen Ländern das Datenschutzrecht unterschiedlich auslegen.

Datenverarbeitung ist allgegenwärtig. Die bloße Masse an potentiell zu kontrollierenden Verfahren erfordert, dass die Bildung einheitlicher Rechtsauffassungen auf wichtige hervorgehobene Fälle konzentriert wird. In kleinteiligen oder individuell fallbezogenen Fragen sind angesichts von Masse und Vielfalt von Datenverarbeitungen gewisse Abweichungen bei Entscheidung nicht vermeidbar.

Einheitliche Entscheidungen setzen einen gefestigten Sachverhalt voraus. Der Antrag thematisiert die Entscheidungsfindung in Bezug auf den Einsatz von MS 365 innerhalb der DSK. Korrekterweise beschreibt er die zunächst heterogene Einschätzung der Datenschutzaufsichten in dieser Frage, die durch die Schwierigkeit bei der Sachverhaltsfeststellung entstanden ist. Die meisten Aufsichten haben von vornherein darauf hingewiesen, dass die Anwender von MS 365 ihrer datenschutzrechtlichen Rechenschaftspflicht nicht nachkommen können, solange Microsoft nicht offenlegt, welche personenbezogenen Daten durch Microsoft für eigene Zwecke genutzt werden, die aus der Anwendung der Produkte bei anderen Verantwortlichen stammen. Einige Aufsichten haben hingegen eine solche Bewertung nicht von vornherein abgegeben, weil sie davon ausgingen, dass die Probleme lösbar seien. Allen voran hat sich der vormalige LfDI Baden-Württemberg verdienstvoll darum bemüht, technische Lösungen zu finden. Er hat aber nach intensiven Bemühungen

[4] Siehe dazu die Übersicht bei https://dejure.org/dienste/lex/DSGVO/15/1.html

leider am Ende auch feststellen müssen, dass es zu ungeklärten Datenübermittlungen zwischen den Anwendern der Programmgruppe MS 365 und Microsoft kommt. Er hat daraufhin ebenfalls von der Anwendung abgeraten[5]. In diesem Fall ging es für einige Aufsichten noch darum, eine Lösung zu finden, während andere zunächst den Status quo beurteilt haben. In der Sache bestand aber im Grunde keine Uneinigkeit. Bis heute konnte der Sachverhalt bezüglich der Verarbeitung durch Microsoft nicht geklärt werden. Die Datenschutzaufsichtsbehörden äußern sich dazu seit 2022 einheitlich.

Hinter Kritik an vermeintlich uneinheitlichen Rechtsauffassungen verbirgt sich mitunter der **Wunsch von Verantwortlichen auf Dispens vom geltenden Datenschutzrecht.** Die Verantwortung für die rechtmäßige Datenverarbeitung liegt primär bei den Verarbeitern selbst. Auch wenn Verarbeiter erkennen, wie sie sich rechtskonform verhalten müssen, wünschen sie sich etwa beim Einsatz innovativer Techniken von den Aufsichtsbehörden Nachsicht bei der „strengen" Einhaltung von Vorschriften, auch in Fallkonstellationen, in denen die DS-GVO den Aufsichten dazu gar keine Handlungsspielräume eröffnet. Dies tritt zum Beispiel in der oben zitierten Kritik der Wirtschaft am vermeintlich mangelnden risikobasierten Ansatz der Datenschutzaufsicht zu Tage. Ein risikobasierter Ansatz spielt aber keine Rolle, wo einzelne Tatbestandsmerkmale belegt werden müssen, wie beispielsweise bei Art. 6 Abs. 1, lit. f DS-GVO (siehe oben Nr. 2) oder bei der Frage, ob eine wirksame Einwilligung vorliegt. Der Hinweis auf einen risikobasierten Ansatz der Aufsichten erweckt insoweit den Eindruck, dass die Datenschutzaufsicht bei der Bewertung von Tatbestandsmerkmalen fünfe gerade sein lassen möge.

Der Wunsch von Verantwortlichen auf Ermöglichung von mehr Datennutzung wird durch die in Art. 1 Abs. 1 DS-GVO angesprochenen Vorschriften zum freien Datenverkehr und die EU-Datenstrategie bestärkt. Die **europäischen Rechtsetzungsakte** dazu **lassen** indessen **viele Fragen offen,** wie der Schutz von Persönlichkeitsrechten in einer digitalisierten Gesellschaft realisiert werden kann. Ein Beispiel bietet die Digitale-Inhalte-Richtlinie[6]. Die Richtlinie thematisiert den möglichen Einsatz von personenbezogenen Daten als Zahlungsmittel für bestimmte Dienstleistungen (Erwägungsgrund 24). Sie beschränkt sich auf die Feststellung, dass bestimmte nach der Richtlinie vorgesehene Schutzvorschriften für Verbraucher*innen anwendbar seien, wenn solche Verträge abgeschlossen würden. Sie beobachtet hier eine Praxis, überlässt aber die Frage, ob und in welchem Umfang solche Verträge zulässig sind, den nationalen Gesetzgebern. Die auch im Datenschutz sehr zentrale Frage, ob man Dienstleistungen mir personenbezogenen Daten bezahlen kann, wird damit auf der europäischen Gesetzgebungsebene bewusst nicht beantwortet. Im Übrigen gilt das auch auf der nationalen Ebene.

Ein anderes Beispiel sind die strikt geregelten Datenschutzrechte der Betroffenen, die sich in KI-Anwendungen gar nicht realisieren lassen, weil auch die Anbieter und Anwender von KI selbst nicht ohne Weiteres nachvollziehen

[5] https://www.baden-wuerttemberg.datenschutz.de/nutzung-von-ms-365-an-schulen/

[6] RICHTLINIE (EU) 2019/770 vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen

können, wie das einzelne KI-Modell bestimmte Ergebnisse produziert. Weder kann das Auskunftsrecht der Betroffenen vollumfänglich beantwortet werden, noch können individuelle Daten Einzelner, die über das Training in Modelle eingeflossen sind, durch Löschung im Modell beseitigt werden. Hier hat der europäische Gesetzgeber das Datenschutzrecht unberührt gelassen und stellt die Datenschutzaufsichtsbehörden damit vor die Aufgabe, Betroffenenrechte durchzusetzen, die in diesem Technikbereich nicht sicher durchsetzbar sind, anstatt in der KI-VO modifizierte Schutzvorschriften für die Persönlichkeitsrechte der Betroffenen anzubieten, die der neuen Technik gerecht werden.

Die EU-Datenstrategie will gleichermaßen Datennutzung fördern und Grundrechte einschließlich des Datenschutzes schützen. Sie gibt damit teils widerstreitende Ziele vor, oft ohne klare Lösungsansätze aufzuzeigen. Wenn die Lösung der offenen Fragen den Aufsichtsbehörden überlassen bleiben soll, sind diese nicht weiser als der Gesetzgeber selbst und benötigen vor einer Entscheidung eine Phase der Meinungsbildung. Eine solche Meinungsbildung darf nicht mit heterogenen Entscheidungen von Aufsichtsbehörden verwechselt werden.

Selbst das Instrumentarium der **DS-GVO** sieht **kein verbindliches Verfahren für die Harmonisierung von Einzelentscheidungen der Aufsichtsbehörden** vor**, die unterschiedliche Verantwortliche betreffen.** Mit dem Instrumentarium der DS-GVO werden Entscheidungen bezüglich eines Verantwortlichen oder eines Auftragsverarbeiters harmonisiert, wenn seine Verarbeitung grenzüberschreitend ist[7]. Es steht hingegen kein Harmonisierungsverfahren zur Verfügung, das einheitliche oder gleichmäßige Entscheidungen sicherstellt, die verschiedene Verarbeiter betreffen. Die DS-GVO lässt hier eine Varianz zu. Die Annäherung der Entscheidungen wird durch Leitlinien des Europäischen Datenschutzausschusses angestrebt, die aber in Bezug auf einzelne Entscheidungen formell nicht verbindlich sind. Die Leitlinien entfalten zwar eine große faktische Harmonisierung auch in Einzelfallentscheidungen, können aber mit ihrem generalisierenden Ansatz schon von vorne herein nicht selbst alle Einzelfallvarianten abdecken.

II. Maßnahmen zur einheitlichen Anwendung der DS-GVO in Deutschland

Ich habe bewusst ausführlich auf Umstände aufmerksam gemacht, die die Schwierigkeiten bei der Bildung einheitlicher Rechtsauffassungen sichtbar machen sollen, mit denen sich die Datenschutzaufsichten in der Praxis konfrontiert sehen. Gleichwohl bin ich der Auffassung, dass die Datenschutzaufsichtsbehörden in Deutschland sich ihrer Rolle bei der harmonisierten Anwendung der DS-GVO sehr bewusst sind und im Rahmen ihrer Selbstorganisation ein hohes Maß an einheitlichen Bewertungen rechtlich drängender Sachverhalte erreichen:

---

[7] Verfahren der Zusammenarbeit und Kohärenz nach Art. 60 ff. DS-GVO im konkreten Einzelfall. „Grenzüberschreitend" bedeutet, dass die Verarbeitung im Rahmen der Tätigkeit von Niederlassungen in der Union in mehr als einem Mitgliedstaat erfolgt oder erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann (Art. 4 Nr. 23 DS-GVO).

1. Bei Leitlinien des Europäischen Datenschutzausschusses und in grenzüberschreitenden Fällen haben die deutschen Datenschutzaufsichtsbehörden eine gut koordinierte Zusammenarbeit und bereiten mit gemeinsamer Expertise die Stellungnahmen der deutschen Vertretung im Europäischen Datenschutzausschuss vor. Die dort getroffenen Entscheidungen sind für alle Aufsichtsbehörden in Deutschland gleichermaßen maßgebend. Die §§ 17 und 18 BDSG legen hier bereits klare Regeln für die Zusammenarbeit und das Bilden gemeinsamer Standpunkte fest.

2. Darüber hinaus erarbeitet die DSK aus eigenem Antrieb Festlegungen zur Anwendung der DSGVO in wichtigen Bereichen. Das belegen die Veröffentlichungen in der Infothek der Internetseite der DSK[8]. zu verschiedenen zentralen Fragestellungen des Datenschutzes.
Neben den veröffentlichten Entscheidungen findet in den zahlreichen Arbeitskreisen der DSK[9] ein fachspezifischer Austausch über die jeweils relevanten Rechtsvorschriften für bestimmte Sachverhalte statt, mit dem Ziel auf Arbeitsebene auch in Detailfragen eine gleiche Rechtsanwendung zu erreichen.

3. Die DSK hat in ihrer Geschäftsordnung zudem Regelungen getroffen, die eine hohe Bindungswirkung ihrer Entscheidungen erzeugen[10]. Die Geschäftsordnung sieht unter Ziff. IV.3.grundsätzlich vor, dass eine in der Abstimmung unterlegene Minderheit, den Mehrheitsbeschluss akzeptiert. Nur zur Wahrung der Unabhängigkeit können abweichende Minderheitsmeinungen kenntlich gemacht und begründet werden. Hierbei geht es vor allem um Fälle mit Abweichungen in einzelnen Ländern aufgrund einer besonderen Sach- oder Rechtslage. Soweit keine Abweichung kenntlich gemacht wird, ist die Mehrheitsmeinung akzeptiert. Die Bindung der Aufsichtsbehörden an die einzelnen Beschlüsse entsteht durch die Selbstbindung der Verwaltung im Rahmen der Anwendung in der Praxis und durch das Rechtsinstrument des Ausschlusses eines „venire contra factum proprium".

4. Aufgrund des Erfordernisses zur einheitlichen Rechtsanwendung der DSGVO gemäß Art. 51 Abs. 2 DS-GVO hat sich der fachliche Austausch der Leitungen der Datenschutzaufsichtsbehörden erheblich verstärkt. Neben den üblichen zwei Hauptkonferenzen, werden Themen in ganztägigen Zwischen- oder Sonderkonferenzen (ca. 3 pro Jahr) geklärt. Eine regelmäßige einstündige Videokonferenz pro Woche dient der gegenseitigen Information über laufende Aktivitäten und dem Identifizieren von Themen, die gemeinsam geklärt werden müssen. Komplexe Thematiken werden in einer jährlichen Wochenendklausurtagung der Leitungen erörtert, um gemeinsame Positionen zu erreichen. Daneben werden Positionen schriftlich in Umlaufverfahren abgestimmt.

5. Eine Vertretung der DSK führt regelmäßig Gespräche mit Datenschutzverbänden, u.a. um Hinweise auf konkrete Problemlagen in der Wirtschaft zu

---

[8] https://www.datenschutzkonferenz-online.de/
[9] https://datenschutzkonferenz-online.de/ak.html
[10] A.IV.3 der Geschäftsordnung (https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_Stand_Februar-2024.pdf)

erhalten, die im Interesse einer einheitlichen Rechtsanwendung geklärt werden sollten.

6. Verbände und andere Vereinigungen haben die Möglichkeit, Verhaltensregeln gemäß Art. 40, 41 DS-GVO für ihre Branche zur Genehmigung vorzulegen. Vor der Genehmigung durch die zuständige Datenschutzaufsichtsbehörde findet eine Abstimmung in der DSK statt, um sicherzustellen, dass die in den Verhaltensregeln beschriebenen Datenverarbeitungsprozesse durch alle Aufsichtsbehörden akzeptiert sind. Dies bietet den Unternehmen, die sich den Regelungen unterwerfen, Rechtssicherheit für ihre Verfahren – deutschlandweit oder auf Wunsch auch in mehreren oder allen EU-Mitgliedstaaten.

III. Notwendige weitere Schritte und mögliche Änderung des Grundgesetzes

1. Änderungen im BDSG
Aktuell befindet sich das BDSG in Überarbeitung. Die DSK soll als Gremium im Gesetz verankert werden Der vorliegende Gesetzentwurf ist im Interesse einer einheitlichen Rechtsanwendung verbesserungsbedürftig. Nicht nur die Institution DSK sollte gesetzlich verankert werden, sondern auch ihre Zielsetzung, zur einheitlichen Rechtsanwendung beizutragen, sollte im Gesetz beschrieben sein. Unter anderem darauf hat die DSK in ihrer Stellungnahme vom 12.4.24[11] hingewiesen.

Zudem sollte die Arbeitsfähigkeit der DSK durch eine Geschäftsstelle unterstützt werden. Die oben beschriebene Koordinierungsarbeit, die inzwischen in der DSK stattfindet, ist allein durch den jährlich wechselnden Vorsitz kaum mehr leistbar. Auch kann eine Geschäftsstelle als Ansprechstelle für die Wirtschaft wichtige Themen in die Arbeitsgremien der DSK einspeisen.

Weitere Verbesserungen im Hinblick auf eine einheitliche Beurteilung von länderübergreifenden Datenverarbeitungsverfahren sollen durch eine Änderung von Zuständigkeitsregelungen im BDSG erreicht werden. Die Zielsetzung hier ist ähnlich dem „Einer für alle-Prinzip", das aus der Verwaltungsdigitalisierung bekannt ist, eine allein oder federführend zuständige Behörde festzulegen. Dieser Ansatz ist gut und wird von der DSK in der Praxis schon jetzt verfolgt. Im Detail weist der vorliegende Gesetzentwurf für die Änderung des BDSG aber an dieser Stelle noch handwerkliche Probleme auf, auf die die DSK in ihrer Stellungnahme ebenfalls hinweist[12].

2. Das durch unbestimmte Rechtsbegriffe geprägte Datenschutzrecht kann durch bereichsspezifische Regelungen auf europäischer und teils auch nationaler Ebene geschärft werden. Dies schafft Rechtsklarheit und mindert die Gefahr widersprüchlicher Entscheidungen in gleichgelagerten Fällen. Beispielsweise ein Beschäftigtendatenschutzgesetz könnte für die Praxis in den

---

[11] https://www.datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdf
[12] aaO, Nr. II.5.

Unternehmen erheblich zur Beseitigung von Rechtsunsicherheiten in datenschutzrechtlichen Fragen beitragen. Auch im Rahmen der Gesetzgebungskompetenz der Länder, gibt es teils Regelungen, die durch eine Harmonisierung in datenschutzrechtlichen Fragen eine einheitliche Beurteilung von gleichen Sachverhalten befördern würden. Dies betrifft zum Beispiel landesrechtlich unterschiedliche Regelungen zur medizinischen Forschung.

3. Geschäftsstelle für die DSK
Da die Regelung einer Geschäftsstelle der DSK im BDSG nicht mehr realistisch erscheint, könnte eine solche für die Verbesserung der Zusammenarbeit in der DSK außerordentlich hilfreiche Einrichtung auch auf anderem Wege realisiert werden. Eine Geschäftsstelle könnte durch Staatsvertrag vereinbart werden. Sie könnte personell bei einer der Datenschutzbehörden beheimatet werden und den jeweiligen Vorsitz nach Maßgabe von Festlegungen der DSK unterstützen. Die Kosten könnten über den modifizierten Königsteiner Schlüssel umgelegt werden.

4. Änderung des Grundgesetzes
Soweit der Antrag eine Änderung des Grundgesetzes anregt, um eine Verbindlichkeit von Entscheidungen der Datenschutzkonferenz zu erzielen, bleibt noch sehr vage, für welche Art von Beschlüssen dies gelten soll. Prof. Roßnagel, dessen Stellungnahme für die Anhörung mir bei der Fertigstellung dieser Stellungnahme bereits vorlag, hat die verschiedenen Formen von Stellungnahmen der DSK erläutert. Hierauf möchte ich verweisen und das nicht im Einzelnen wiederholen.

Wesentlich ist, dass eine Bindungswirkung von Beschlüssen die Unabhängigkeit der Datenschutzaufsichtsbehörden, die durch Art. 16 Abs. 2 Satz 2 AEUV, Art. 8 Abs 3 der Grundrechtscharte der EU; durch Art. 52 DS-GVO und in Nordrhein-Westfalen auch durch Art. 77a (2) LVerf NRW garantierte ist, nicht tangiert. Die durch höherrangiges EU-Recht garantierte Unabhängigkeit kann durch Recht eines Mitgliedstaates nicht eingeschränkt werden.

Dementsprechend können Festlegungen der Datenschutzkonferenz nicht Einzelentscheidungen der jeweiligen Aufsichtsbehörden beeinflussen, da die Aufsichtsbehörden gem. Art. 52 Abs. 1 DS-GVO bei der Erfüllung ihrer Aufgaben und Ausübung ihrer Befugnisse völlig weisungsfrei bleiben müssen. Eine Bindungswirkung bei abstrakten Festlegungen zur Interpretation des Datenschutzrechts würde nicht unmittelbar in die Unabhängigkeit der Aufsichtsbehörden eingreifen, wenn sie vergleichbar ausgestaltet sind, wie die Leitlinien des europäischen Datenschutzausschusses. Solche abstrakten Festlegungen würden aber ebenso nur begrenzte Wirkung für die Entscheidungen der Aufsichtsbehörden entfalten können, die immer die Besonderheiten im Einzelfall würdigen müssen. Unabhängig davon, erfüllen die Leitlinien des Europäischen Datenschutzausschusses nach Art. 70 Abs. 1, Buchstabe e DS-GVO diese Aufgabe der abstrakten Rechtsauslegung bereits. In diese Arbeiten bringen sich die deutschen Aufsichtsbehörden ein. Es erscheint sinnvoller, diesen Weg einer europäischen Abstimmung zu beschreiten, als rein nationale Festlegungen zu treffen, die möglicherweise im europäischen Abstimmungsprozess überholt werden.

Ähnliches gilt für abstrakte Festlegungen zu bestimmten typischen Verarbeitungsformen. Solche Festlegungen können nur Hinweise auf bekannte Rechtsprobleme im Zusammenhang mit einem bestimmten Verarbeitungstyp beschreiben. Die Besonderheiten im Einzelfall können durch abstrakte Regelungen kaum gelöst werden. Die Aufsichtsbehörden würden ihre Aufgabe nicht mehr verantwortlich wahrnehmen können, wenn sie durch abstrakte Festlegungen daran gehindert wären, auf die Bedürfnisse der für die Datenverarbeitung Verantwortlichen reagieren zu können.

Ausblick

Ein offensichtlicher Nutzen einer Verankerung verbindlicher Entscheidungen der DSK im Grundgesetz ist für mich derzeit nicht erkennbar. Die Ursachen (I.), die zu (vermeintlich) heterogenen Entscheidungen der Datenschutzaufsicht führen, sind vielfältig und es stehen eine Reihe von möglichen Lösungsansätzen (II. und III.) zur Verfügung. Soweit Verbesserungen durch die DSK selbst erzielt werden können, hat sie wichtige Schritte eingeleitet und arbeitet fortgesetzt daran, hier noch weitere Verbesserungen zu erzielen. Wenn sie dabei durch eine Geschäftsstelle unterstützt würde, würde dies die DSK weitaus mehr stärken, als eine Grundgesetzänderung, deren Effekte auf eine einheitliche Rechtsanwendung eher gering sein dürften.

Bettina Gayk

(Bettina Gayk)
Landesbeauftragte für Datenschutz und Informationsfreiheit
des Landes Nordrhein-Westfalen