Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.

AWV e.V. | Düsseldorfer Straße 40 | 65760 Eschborn

per E-Mail an VII4@bmi.bund.de

An das
Bundesministerium des Innern und für Heimat

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Ihr Zeichen, Ihre Nachricht vom	Unsere Zeichen	Datum
VII4.20108/9#10		05.09.2023

Verbändebeteiligung BDSG
Stellungnahme zu dem Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

Sehr geehrte Damen und Herren,

wir bedanken uns für die Möglichkeit, uns an der Verbändeanhörung zum „Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes“ zu beteiligen und bitten Sie, die anliegende Stellungnahme unseres AWV-Arbeitskreises 4.3 „Datenschutz und Informationssicherheit“ bei den weiteren Beratungen zu berücksichtigen.

Mit freundlichen Grüßen

Rudi Kramer
Leiter des AWV-Arbeitskreises 4.3

Dr. Ulrich Naujokat
AWV-Geschäftsführer

Anlage
Stellungnahme der Arbeitsgemeinschaft für Wirtschaftliche Verwaltung e.V. im Rahmen der Verbändeanhörung zu Änderungen im BDSG

Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
Düsseldorfer Straße 40
65760 Eschborn
Tel. 06196 777 26-0
Fax 06196 777 26-51
info@awv-net.de
www.awv-net.de

5. September 2023

Stellungnahme des AWV-Arbeitskreises 4.3 „Datenschutz und Informationssicherheit“ zu dem Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

Die Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV) ist das zentrale Forum in Deutschland, in dem Wirtschaft und Verwaltung zusammenarbeiten, um zukunftswirksame Regeln und Verfahren zu entwickeln, Verwaltungskosten zu reduzieren und den Nutzen für Wirtschaft und Verwaltung zu optimieren. Die AWV - gefördert durch das Bundesministerium für Wirtschaft und Klimaschutz - versteht sich dabei als unabhängige Mittlerin und stellt eine Plattform für die Zusammenarbeit bereit, um die Kommunikation und Kooperation zwischen öffentlicher Verwaltung, Wirtschaft und Drittem Sektor zu fördern.

Die Mitglieder unserer Fachgremien repräsentieren nahezu alle Wirtschaftsbereiche und sind Spezialistinnen und Spezialisten aus Verwaltung, Unternehmen, Beratung und Verbänden. Im Rahmen der AWV-Fachgremien besteht die Möglichkeit, den direkten und unkomplizierten Austausch zu pflegen und das gegenseitige Verständnis für die Belange des anderen zu wecken, um letztlich praktikable und für alle Beteiligten zufriedenstellende Regelungen zu erarbeiten.

Im Mittelpunkt der Tätigkeit unseres Expertengremiums „Datenschutz und Informationssicherheit“ steht das Ziel, Unternehmen (insbesondere KMU), Behörden sowie sonstige Organisationen bei rechtlichen Fragestellungen zum Datenschutz und zur Informationssicherheit zu unterstützen und zum Beispiel über Broschüren oder Handlungsempfehlungen Hilfestellungen zu erarbeiten. Der Arbeitskreis beschäftigt sich intensiv mit Gesetzesentwürfen und Stellungnahmen, die den Datenschutz und die Informationssicherheit berühren.

Einleitende Hinweise

In Anbetracht der relativ kurzen Rückmeldefrist und der Notwendigkeit, die Rückmeldungen innerhalb des Arbeitskreises zu konsolidieren, kann der AWV-Arbeitskreis 4.3 nur auf ausgewählte Punkte des Gesetzentwurfs Bezug nehmen. Eine tiefgehende Stellungnahme zum Inhalt des Gesetzentwurfs kann daher nicht bereitgestellt werden.

Aus Gründen der leichteren Lesbarkeit wird in dieser Stellungnahme nicht durchgängig ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung in der Regel für alle Geschlechter.

1. Zu Teil 1, Kapitel 2 § 4 Absatz 1 des Referentenentwurfes eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

„Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) durch öffentliche Stellen ist nur zulässig, soweit sie zu ihrer Aufgabenerfüllung, einschließlich der Wahrnehmung ihres Hausrechts, erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen."

Grundsätzlich bewertet der Arbeitskreis eine Berücksichtigung der Aussagen aus dem Urteil des BVerwG positiv, weil damit eine Klarstellung zur Anwendbarkeit des § 4 BDSG einhergeht. Es ist allerdings darauf hinzuweisen, dass das Urteil des BVerwG sich ausschließlich auf den ersten Satz von § 4 Abs. 1 BDSG bezog. Mit dem nun vorliegenden Referentenentwurf soll jedoch auch der bisherige zweite Satz von § 4 Abs. 1 BDSG aufgehoben werden. Dabei wird durch diese Regelung zu öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs klargestellt, dass die Videoüberwachung solcher Bereiche zwecks Prävention und Aufklärung von Straftaten gegen Leben, Gesundheit oder Freiheit von dort aufhältigen Personen, wie insbesondere Gewaltverbrechen, in besonderem Maße im öffentlichen Interesse liegt. Die Zulässigkeit entsprechender Videoüberwachungen wird von einzelnen Datenschutzaufsichtsbehörden gelegentlich in Zweifel gezogen.

Eine von uns daher angeregte Beibehaltung des bisherigen zweiten Satzes von § 4 Abs. 1 BDSG etwa als Abs. 2 des neuen § 4 BDSG ist u.E. dem deutschen Gesetzgeber aufgrund der Öffnungsklausel des Art. 6 Abs. 1 lit. e DSGVO erlaubt.

2. Zu Teil 1, Kapitel 4a. § 16a des Referentenentwurfes eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

„Die oder der Bundesbeauftragte im Sinne des § 8 sowie die Aufsichtsbehörden der Länder im Sinne des § 40 bilden die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Die Datenschutzkonferenz gibt sich eine Geschäftsordnung."

Wir begrüßen eine Regelung zur Einrichtung einer Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Dabei regen wir an,

bereits im BDSG eine Aufnahme bzw. Berücksichtigung der sektorspezifischen Datenschutzaufsichtsbehörden nicht von vornherein auszuschließen.

Zudem sind wir der Ansicht, dass diese Regelung alleine an sich keine zufriedenstellende Effizienz schaffen kann, solange keine entsprechende organisatorische Infrastruktur bereitgestellt wird. Dies könnte durch die Anbindung an bestehende Einheiten zur Koordinierung der gemeinsamen Aufgaben der Länder oder auch durch die Schaffung einer neuen Geschäftsstelle mit entsprechender Ausstattung erreicht werden.

3. Zu Teil 2, Kapitel 2 § 34 Absatz 1 des Referentenentwurfes eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

Absatz 1 wird wie folgt geändert:
In Nummer 2 Buchstabe a wird das Wort *„satzungsmäßiger“* durch die Wörter *„von in öffentlich-rechtlichen Satzungen vorgesehenen“* ersetzt.

Folgender Satz wird angefügt:
„Das Recht auf Auskunft besteht auch insoweit nicht, als der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt.“

Diese Regelungsabsicht hinsichtlich der Berücksichtigung von Geschäftsgeheimnissen des Verantwortlichen wird auch durch das Urteil des OLG Karlsruhe vom 26.05.2023 – 10 U 24/22 aus der DSGVO abgeleitet (dort RN 276).

Wir empfehlen in der Begründung zu dieser Klarstellung die Aussagen aus dem Erwägungsgrund 4 der DSGVO miteinfließen zu lassen, wonach datenschutzrechtliche Ansprüche im Hinblick auf die gesellschaftliche Funktion betrachtet und deren Umsetzung unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden müssen.

4. Zu Teil 2, Kapitel 4. § 40a des Referentenentwurfes eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes

„Aufsichtsbehörde gemeinsam verantwortlicher Unternehmen

Sind Unternehmen gemeinsam Verantwortliche gemäß Artikel 26 der Verordnung (EU) 2016/679 und mehrere Aufsichtsbehörden für sie zuständig, können die Unternehmen gemeinsam anzeigen, dass sie gemeinsam verantwortliche Unternehmen sind und deshalb für die von ihnen gemeinsam verantwortete Datenverarbeitung allein die Aufsichtsbehörde zuständig sein soll, in deren Zuständigkeitsbereich das Unternehmen fällt, das in dem der Antragstellung vorangegangenen Geschäftsjahr den größten Jahresumsatz erzielt hat. Die gemeinsame Anzeige ist an alle Aufsichtsbehörden zu richten, die für die gemeinsam verantwortlichen Unternehmen zuständig sind, und muss die das umsatzstärkste Unternehmen nachweisenden Unterlagen enthalten. Ab dem Zeitpunkt, zu dem die Anzeige im Sinne der Sätze 1 und 2 bei der für das umsatzstärkste Unternehmen zuständigen Behörde eingegangen ist, wird diese die allein zuständige Aufsichtsbehörde. § 3 Absatz 3 und 4 des Verwaltungsverfahrensgesetzes findet entsprechende Anwendung.“

Wir begrüßen das Bemühen, im Rahmen der föderalen Rahmenbedingungen zentrale Zuständigkeiten zu ermöglichen. Dazu empfehlen wir bei der angedachten Regelung klarzustellen, ob dies dann für alle Verarbeitungen der beteiligten Entitäten gilt oder nur für diejenige, die in gemeinsamer Verantwortlichkeit erbracht werden. Auch empfehlen wir von vornherein zu entscheiden, ob diese Zuständigkeitsreglung auch zusammen mit sektoralen Aufsichten (Kirchen, Rundfunkanstalten) zur Anwendung kommen kann, wenn diese auch entsprechende Formulierungen bezüglich der Zuständigkeit deren Aufsichten aufnehmen.

Diese Regelung könnte erweitert werden um eine Wahlmöglichkeit für Verarbeitungen innerhalb eines Konzerns, innerhalb des Geltungsbereichs der DSGVO auch losgelöst von einer gemeinsamen Verantwortung. Entgegen der in der Gesetzesbegründung aufgeführten Beispiele „Stammdatenverwaltung im Unternehmensverbund, konzernweites Customer-Relationship-Management“ werden diese oft nach dem Konstrukt der Auftragsverarbeitung durchgeführt. Das Ziel einer „besseren Durchsetzung und Kohärenz des Datenschutzes“ kann u.E. nur durch eine Erweiterung der Wahlmöglichkeit innerhalb von Konzernen unter Einbeziehung der Auftragsverarbeitung erreicht werden. Zur Vereinheitlichung sollte dabei die Begrifflichkeit der „Unternehmensgruppe“ aus der DSGVO verwendet werden (vgl. ErwGr. 37). In Bezug auf eine Unternehmensgruppe empfiehlt es sich, als relevanten Parameter für die Auswahl der zuständigen Aufsichtsbehörde die Hauptniederlassung in Analogie zu Art. 56 DSGVO zugrunde zu legen.

5. Vorschlag für neue Regelungen innerhalb des Abschnitts 2 „Besondere Verarbeitungssituationen“ in Teil 2, Kapitel 1

„Verarbeitungen für IT-Sicherheitszwecke“

Erläuterung:

Angriffe auf die IT-Sicherheit bei Unternehmen und Behörden nehmen in dramatischem Ausmaß zu. Dabei spielt die Motivation der Täter zunächst keine Rolle, ob der Angriff nun durch Kriminelle zur Erpressung von Finanzmitteln oder ausländischen Diensten zur Destabilisierung einer Volkswirtschaft erfolgt. Maßnahmen aus Unternehmenssicht stellen sich hier oftmals als Verarbeitung personenbezogener Daten (z.B. Zugangsdaten) dar, deren Verarbeitung zu Sicherheitszwecken einer Rechtsgrundlage bedarf (vgl. beispielsweise die Empfehlungen des BayLDA zu Good Practice bei Art. 32, Stand Oktober 2020).

Art. 6 Abs. 1 lit. c DSGVO i.V.m. Art. 32 DSGVO wird bislang als nicht überzeugende Befugnisnormkette anerkannt, so dass in der Regel auf die Grundlage der „Wahrung berechtigter Interessen“ zurückgegriffen werden muss. Dies stößt dann auf folgende Bürokratieerfordernisse und Probleme in der Praxis: Durchzuführende Abwägung, deren Dokumentation und vorherige Information mit Hinweis auf Widerspruchsmöglichkeit. Zudem steht die Befugnisnorm des Art. 6 Abs. 1 lit. f DSGVO zu Sicherheitszwecken (vgl. Erwägungsgrund 49 der DSGVO) nur dem Verantwortlichen zu. Berücksichtigt man dann noch die weite Auslegung des EuGH zu den besonderen Kategorien personenbezogener Daten (C-184/20), wäre die Anwendbarkeit der Grundlage „Wahrung berechtigter Interessen“ dann auch nicht bei Verarbeitung zu IT-Sicherheitszwecken von Zugangsdaten zu Gesundheitsplattformen wie Selbsthilfegruppen möglich, weil Art. 9 Abs. 2 DSGVO eine Grundlage auf Basis einer Interessensabwägung nicht vorsieht. Auch die Grundlage zur Vertragserfüllung aus Art. 6 Abs. 1 lit. b DSGVO erscheint fraglich, weil der EuGH hierzu in seinem Urteil C-252/21 (Meta/BKartA) (ab RN 98) eine enge Auslegung einfordert.

Erschwerend kommt hinzu, dass Aufsichtsbehörden bei der Umsetzung der Informationspflichten eine möglichst konkrete Angabe der Maßnahme fordern. So reiche z.B. in der Orientierungshilfe für Telemedienanbieter:innen, Stand Dez. 2022, die Angabe „zu IT-Sicherheitszwecken“ nicht aus, um für die Einholung einer rechtskonformen Einwilligung zu entsprechenden Verarbeitungen ausreichend zu informieren (RN 49). Auch genüge die pauschale Bezeichnung von „Sicherheitscookies“ nicht den Anforderungen, selbst wenn „Sicherheitscookies“ in der Variante der nutzerorientierten Sicherheitscookies als unbedingt erforderlich akzeptiert werden (RN 81).

Im Ergebnis unterliegen damit Verarbeitungen für IT-Sicherheitszwecke – sei es präventiv oder forensisch – erschwerenden Anforderungen, die erfolgreiche Sicherheitsmaßnahmen beeinträchtigten.

Bei Bundesbehörden hat der Gesetzgeber bereits eine Lösung in § 5 BSIG und § 5a BSIG gefunden. Es wäre zu begrüßen, diese Regelungen in angepasster

Formulierung für Verarbeitungen zu IT-Sicherheitszwecken auch im BDSG zugunsten anderer Verantwortlicher und Auftragsverarbeiter zu übernehmen. Die jeweilige Definition konkreter Verarbeitungen, die im Rahmen von IT-Sicherheitszwecken erfolgen können, könnte dem BSI übertragen werden. Damit bliebe das BDSG weiterhin technikneutral ausgestaltet, über die fachliche Kompetenz des BSI können aber jeweilige Maßnahmen konkreten Gefährdungen angepasst werden.

Diese gesamte Thematik könnte auch in einem Evaluierungsverfahren zur DSGVO eingebracht werden, um über Art. 32 in Verbindung mit Art. 6 Abs. 1 lit. c DSGVO und Art. 9 Abs. 2 lit. g DSGVO nationale allgemeine Regelungen zu IT-Sicherheitszwecken obsolet zu machen.