Rede der Berliner Datenschutzbeauftragten Meike Kamp auf der Veranstaltung der Datenschutzkonferenz zum Europäischen Datenschutztag am 28. Januar 2026 in Berlin.

- Es gilt das gesprochene Wort -

Sehr geehrte Kolleginnen und Kollegen Datenschutzbeauftragte des Bundes und der Länder,

sehr geehrte Damen und Herren,

liebe Gäste,

ich freue mich außerordentlich, dass ich mit meiner Behörde den Europäischen Datenschutztag würdigen und die diesjährige Veranstaltung ausrichten darf.

Im letzten Jahr hatte ich die ehrenvolle Aufgabe, den Vorsitz in der Datenschutzkonferenz zu führen. In diesem Zusammenhang haben wir ein Projekt der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (kurz DSK) zur Operationalisierung der Maßnahmen zur Anonymisierung und Pseudonymisierung initiiert. Die Idee ist, die Leitlinien des Europäischen Datenschutzausschusses, die gerade zu den beiden Themen erarbeitet werden, anhand von typisierten Fallgestaltungen für die Anwender:innen umsetzbar zu machen. Erste Erkenntnisse aus der Arbeit an dem Papier wird Herr Dr. Daldrop aus unserem Hause gleich vorstellen. Zudem freue ich mich auf eine spannende Diskussion mit den Fachleuten aus Wirtschaft und Wissenschaft, die sicherlich auch die Frage aufwerfen wird, ob Anonymisierung und Pseudonymisierung Risiken mindern können und gleichzeitig die Nutzbarkeit der Daten erhalten bleibt.

Mir ist bewusst, dass wir Ihnen heute ein bisschen was zumuten. Rechts- und technische Fragen rund um die Themen Anonymisierung und Pseudonymisierung sind keine leichte Kost. Über allem hängt die Frage, wann sind Daten (noch) personenbezogen und ist die Datenschutz-Grundverordnung anwendbar oder nicht (mehr).

Die Diskussion vom absoluten zum relativen Personenbezug und hin zu den Fragen, wer über Mittel zur Identifizierung verfügt, welche Perspektive für die Beurteilung des Personenbezugs relevant ist und wie hoch das Risiko der Re-Identifizierung sein darf, hat sich über viele Jahre fortentwickelt.

Auch im letzten Jahr haben neue Dynamiken diese langwährende Diskussion wieder ordentlich entfacht: Da wäre zum einen das Urteil des EuGH zum EDPS/SRB Verfahren vom 4. September 2025, das in der „Datenschutzszene“ mit Spannung erwartet worden war.

Der EuGH hat zunächst einmal klargestellt, dass pseudonymisierte Daten nicht zwangsläufig personenbezogen sein müssen. Soweit so klar. Allein die Existenz von identifizierenden Informationen kann nicht dazu führen, dass Daten in jedem Fall und für jede Person personenbezogen sind. Damit ist grundsätzlich zu prüfen, welche Mittel dem Verantwortlichen oder einer Stelle, die Daten empfängt, zur Verfügung stehen und ob diese Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden.

Unter bestimmten Bedingungen kommt es dabei nicht nur darauf an, welche Mittel etwa dem Verantwortlichen oder einer empfangenden Stelle selbst zur Verfügung stehen, sondern auch darauf, welche Identifizierungsmöglichkeiten in den Händen von Dritten liegen und inwieweit diese Mittel auch für die zu betrachtende Stelle Relevanz entfalten.

Nach der Rechtsprechung des EuGH – schon seit dem sog. Breyer-Urteil – gilt etwa, dass Zusatzinformationen in den Händen Dritter dann relevant sind, wenn der Verantwortliche über rechtliche Möglichkeiten verfügt, diese zusätzlichen Informationen, die eine Identifizierung erlauben, von Dritten zu erlangen.

Darüber hinausgehend hat der EuGH vor nicht allzu langer Zeit im sog. Scania-Urteil eine weitere Konstellation angesprochen, bei der es für die Beurteilung des Personenbezugs ebenfalls auf Informationen oder Identifizierungsmittel in den Händen Dritter ankommt. Auch in dieser Konstellation werden für den Verantwortlichen an sich nicht personenbezogene Daten zu personenbezogenen Daten. Dies ist dann der Fall, wenn ein Verantwortlicher die Daten anderen Personen überlässt, die über Mittel verfügen, die eine Identifizierung der betroffenen Person ermöglichen. In diesem Fall – so konstatiert der EuGH – sind die Daten im Zusammenhang mit einer solchen Überlassung personenbezogen und zwar sowohl für die empfangende Person als auch indirekt für den Verantwortlichen.

Die Scania-Rechtsprechung wird im SRB-Urteil fortgeführt: Es geht darum, dass der EuGH ein Argument entkräften möchte, nämlich das Argument, dass pseudonymisierte Daten immer personenbezogen sein müssen, weil es ansonsten möglich wäre, Daten in pseudonymisierter Form an einen Empfänger, der über keine Mittel zur Identifikation verfügt, quasi aus dem Anwendungsbereich der DSGVO „rauszuübermitteln“. Dieser Befürchtung tritt der EuGH im SRB-Urteil entgegen und sagt, dass diese Übermittlung an den „unwissenden“ Empfänger sich insbesondere im Zusammenhang mit einer etwaigen späteren Übermittlung an Dritte nicht auf die Beurteilung der Personenbezogenheit der Daten auswirkt.

Lassen Sie mich kurz das Szenario verdeutlichen:

Wir haben es mit drei unterschiedlichen Stellen zu tun

- Zum einen mit dem Verantwortlichen, der pseudonymisierte Daten an einen Empfänger übermittelt
- Zum zweiten mit dem Empfänger dieser Daten, dem selbst keine zusätzlichen Informationen zur Verfügung stehen, die Daten bestimmten Personen zuzuordnen und
- Zum dritten mit dem Dritten, dem der Empfänger die Daten überlässt (by the way, dass kann im Falle der Rückübermittlung der Daten natürlich auch der Verantwortliche sein),

So, nun sagt der EuGH, sofern nicht ausgeschlossen werden kann, dass dieser Dritte nach allgemeinem Ermessen in der Lage ist, die pseudonymisierten Daten der betroffenen Person zuzuordnen, sind die pseudonymisierten Daten (die der Verantwortliche an den Empfänger übermittelt hat) sowohl in Bezug auf die Übermittlung der Daten an den Dritten als auch in Bezug auf die spätere Verarbeitung dieser Daten durch den Dritten als identifizierbar anzusehen.

Dies führt dann nach Ansicht des Gerichts dazu, – um auf den Ausgangsumstand und die Befürchtung zurückzukommen, dass die DSGVO umgangen werden könnte – dass unter solchen Umständen die pseudonymisierten Daten als personenbezogene Daten betrachtet werden müssen; die Befürchtung mithin unbegründet ist.

In den vielen Diskussionen um das Urteil spielt diese Passage nach meiner Wahrnehmung kaum eine Rolle. Vielmehr habe ich den Eindruck, dass dieser Teil schlichtweg überlesen oder gar weggelassen wird.

So erklärt sich dann vielleicht auch ein zweites Ereignis im letzten Jahr, dass den Personenbezug erneut zum Gegenstand zahlreicher Fachdiskussionen gemacht hat. Ende November veröffentlichte die Europäische Kommission den Entwurf für einen Digitalen Omnibus, der auch Änderungsvorschläge zur DSGVO enthält.

Unter anderem werden der Definition des Personenbezugs in Art. 4 Nr. 1 DSGVO drei Sätze hinzugefügt. Der erste ist harmlos, der zweite nicht ganz so und der dritte gravierend!

Aufgrund der Kürze der Zeit möchte ich nur auf den dritten Satz eingehen. Die Kommission formuliert, vereinfacht gesprochen, dass Informationen nicht allein deshalb personenbezogen werden, weil ein potenzieller nachfolgender Empfänger über Mittel verfügt, die betroffene Person zu identifizieren. Mit dem Entwurf eines neuen Erwägungsgrundes wird erläutert, dass eine mögliche Weitergabe an „wissende“ Dritte, die Informationen nur für diejenigen Dritten zu personenbezogenen Daten machen.

Die Kommission deklariert diese Ergänzungen mehr oder weniger als Kodifikation der Rechtsprechung des EuGH. Wie wir gesehen haben, das Gegenteil ist der Fall!

Schauen wir uns das an einem Beispiel an: Werbeplätze auf einer Webseite werden in Sekundenbruchteilen meistbietend verkauft. Anlass für diese Vorgänge sind spezifische Nutzer:innen, die die Werbeseiten aufrufen. Die Möglichkeit, diese zielgenau zu bewerben, wird etwa in Real-Time-Bidding-Verfahren in Echtzeit versteigert. Die Grundlage für diese Verfahren, d. h. die vielen Informationen und Profile der spezifischen Nutzer:innen, liefern eine Vielzahl von Akteuren in einer verzweigten Datenverarbeitungskette. All diese Akteure arbeiten mit Cookies oder Werbe-IDs um die einzelnen Datensätze zu unterscheiden bzw.

Daten einer Nutzer:in zusammenzuführen. Verfügen diese Stellen nun über die Mittel die natürlichen Personen zu identifizieren, oder gilt das nur für die eine Stelle, die die Webseite betreibt und die Werbung ausspielt? Mit den Ergänzungen im digitalen Omnibus wird es schwer zu argumentieren, dass alle dazwischen liegenden Verarbeitungen, etwa das Zusammenführen von Informationen und das notwendige Anreichern der Profile für das Bieterverfahren weiterhin von der DSGVO erfasst sind. All diese Datenverarbeitungen zielen ihrem Wesen nach aber auf ein bestimmtes bzw. bestimmbares Individuum ab und entfalten ihre Wirkung gerade auf Ebene des Einzelnen. Hierfür ist es vollkommen irrelevant, ob es um die letzte Stelle in der Kette geht oder ob diese einzelne Person Hans, Thorsten oder Mareike im „real life“ heißt.

Die vorgeschlagenen Änderungen haben damit erhebliche Auswirkungen auf den Anwendungsbereich der DSGVO. Sie rütteln an den Grundpfeilern des Datenschutzes. Ich halte dies nicht für den richtigen Weg: Wir sollten den Anwendungsbereich der DSGVO erhalten und Compliance-Erleichterungen stärker ausbauen bei guter Pseudonymisierung und geringen Auswirkungen und Risiken für betroffene Personen. Gleichzeitig sollte aber auch bei geringem Risiko einer Re-Identifizierung ein Basis-Schutzprogramm zumindest nach Art. 32 DSGVO erhalten bleiben.

Das heißt, nicht nach dem Unerreichbarem streben oder die Begrifflichkeiten aufweichen, sondern solide Pseudonymisierung wagen!

In diesem Sinne freue ich mich jetzt ganz besonders, dass Frau Prof. Anja Lehmann heute bei uns ist. Frau Lehmann forscht am Hasso-Plattner Institut in Potsdam zu Cybersecurity, Identitätsmanagement, Kryptographie und Datenschutz und wird uns nun mitnehmen in die wundervolle Welt kryptographischer Pseudonyme!

Herzlichen Dank Ihnen allen für Ihre Aufmerksamkeit. Ich wünsche Ihnen einen erkenntnisreichen und anregenden Nachmittag! Viel Spaß!