ARBEITSGEMEINSCHAFT MITTELSTAND

WWW.ARBEITSGEMEINSCHAFT-MITTELSTAND.DE

Uneinheitlichkeit der Datenschutzaufsicht – Kein Mythos, sondern Realität

Stellungnahme zu den Stuttgarter Impulsen der unabhängigen Datenschutzaufsichtsbehörden der Länder

BGA BVR DEHOGA BUNDESVERBAND DIHK drv HDE Handelsverband Deutschland ZDH Bundesverband Kooperierender Mittelstand

Die unabhängigen Datenschutzaufsichtsbehörden der Länder haben am 19. Juni 2026 das Eckpunktepapier „Stuttgarter Impulse“ veröffentlicht. Vor dem Hintergrund der im Koalitionsvertrag der aktuellen Bundesregierung vereinbarten Bündelung der Datenschutzaufsicht bei der/dem BfDI werden dort Vorschläge für eine Reform der Datenschutzaufsicht unter Erhalt der föderalistischen Struktur gemacht.

Zu dem seit Jahren kritisierten Problem der uneinheitlichen Auslegung und Anwendung des Datenschutzrechts durch die Aufsichtsbehörden des Bundes und der Länder wird dort ausgeführt, dass es sich um einen „Mythos“ handele, welcher ungeprüft zum Anlass einer Modernisierung der Datenschutzaufsicht herangezogen werde.

Als Vertreter der Interessen zahlreicher mittelständischer Unternehmen, die seit Jahren die Kosten, Verzögerung und Rechtsunsicherheit einer uneinheitlichen und inkohärenten Rechtsanwendung und -auslegung des Datenschutzrechts tragen müssen, können wir diese Ausführungen nicht unerwidert lassen. Die Uneinheitlichkeit der Datenschutzaufsichten ist kein Mythos, sondern eine dokumentierte Realität mit spürbaren realen, praktischen und wirtschaftlichen Folgen.

Für konkrete Belege genügt ein Blick in die Veröffentlichungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) selbst. Daraus gehen zahlreiche Fälle nicht einheitlich zustande gekommener Beschlüsse, Anwendungshinweise, Orientierungshilfen und Entschließungen hervor, z.B.

- Orientierungshilfe für Online-Lernplattformen v. 26.04.2018[1] (eine Gegenstimme),
- Entschließung zur Haftung von Datenschutzverstößen durch Beschäftigte v. 03.04.2019[2] (zwei Gegenstimmen),
- Beschluss zu datenschutzrechtlichen Aspekten bei sog. Asset-Deals v. 24.05.2019[3] (zwei Gegenstimmen),

[1] https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf.
[2] https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf
[3] https://www.datenschutzkonferenz-online.de/media/dskb/20190524_dskb_asset_deal.pdf

- Datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Microsoft Office 365, Beschluss v. 29.09.2020[4] (acht Gegenstimmen),
- Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail v. 27.05.2021[5] (eine Gegenstimme),
- Beschluss zur Möglichkeit der Nichtanwendung von TOMs auf Wunsch der betroffenen Person v. 24.11.2021[6] (zwei Gegenstimmen),
- Beschluss zur Task Force Facebook-Fanpages v. 23.03.2022[7] (eine Gegenstimme),
- Anwendungshinweis zum EU-US Data Privacy Framework v. 10.07.2023[8] (eine Gegenstimme),
- Entschließung zur Sicherstellung menschenzentrierter Digitalisierung in der Daseinsvorsorge v. 19.12.2024[9] (zwei Gegenstimmen).

Daneben existieren Pressemitteilungen einzelner Landesdatenschutzbehörden, in denen diese sich explizit von DSK-Positionen distanzieren:

- Gemeinsame Presseerklärung des LfDI BaWü, HBDI, UDZ Saarland, BayLDA, BayLfD v. 01.10.2020[10],
- Pressemitteilungen des TlfDI zum EU – US Data privacy framework v. 05.09.2023[11].

Ein weiteres Beispiel für praxisrelevante Unterschiede bei der Rechtsauslegung sind die unterschiedlichen Anforderungen der Aufsichtsbehörden an die Meldung von Datenschutzverletzungen nach Art. 33 DSGVO im Zusammenhang mit den sog. Hafnium Hack-Angriffen auf Microsoft-Exchange-Server.

---

[4] https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf
[5] https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.
[6] https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf
[7] https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf
[8] https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf
[9] https://www.datenschutzkonferenz-online.de/media/en/2024-12-19_DSK-Entschliessung_Menschenzentrierte-Digitalisierung.pdf.
[10] https://www.datenschutz-bayern.de/presse/20201002_365.pdf.
[11] https://tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen_2023/230904_PM_DPF.pdf.

Schließlich finden sich auch in den Tätigkeitsberichten der Aufsichtsbehörden nicht miteinander in Einklang zu bringende rechtliche Einschätzungen zu identischen Sachverhalten. So führt bspw. das LDI NRW in seinem 30. Tätigkeitsbericht aus, dass sich die Volksbanken und Raiffeisenbanken bei der Durchführung sog. Smart Data Verfahren auf der Grundlage einer entsprechenden Einwilligungserklärung „an alle Regeln halten[12]“, während das LfD Niedersachsen dieselbe Einwilligung in seinem 29. Tätigkeitsbericht als „problematisch“ einstuft[13]. Daher mussten unter enormem Aufwand trotz langwieriger Abstimmungen in der DSK zwei unterschiedliche Einwilligungserklärungen für identische Verfahren ausgerollt werden.

Die vorstehenden Beispiele stammen nicht aus anekdotischen Einzelbeobachtungen, sondern aus Veröffentlichungen der Datenschutzaufsichtsbehörden selbst. Die tatsächlich auftretenden Unterschiede dürften nur die Spitze des Eisbergs darstellen. Die Mehrzahl der aufsichtsbehördlichen Abstimmungen erfolgt im Rahmen informeller Konsultationen, Beratungen oder laufender Verfahren, ohne dass die Öffentlichkeit davon Kenntnis erlangt.

Nicht nur bei der Rechtslauslegung, sondern auch bei der Erfüllung von Meldepflichten bestehen Unterschiede zwischen den Aufsichtsbehörden, die einen hohen administrativen Aufwand für Unternehmen verursachen. Ein Beispiel hierfür sind die Anforderungen an die Meldungen von Datenschutzbeauftragten. Hier bestehen unterschiedliche Vorgaben in Bezug auf die meldebefugte(n) Person(en) im Unternehmen und die Zulässigkeit von Sammelmeldungen.

Auch die Formulare der Behörden zur Meldung von Datenschutzverletzungen fallen unterschiedlich aus. Bei Meldungen für mehrere Gesellschaften sind die Anforderungen unterschiedlich: Teilweise wird ein ausgefülltes Formular pro Gesellschaft verlangt, teilweise reicht – was mit deutlich weniger Aufwand verbunden ist – ein einziges Formular mit einer beigefügten Liste aller betroffenen Gesellschaften aus.

---

[12] https://www.ldi.nrw.de/system/files/media/document/file/30.-bericht.pdf, siehe dort S. 113.
[13] https://www.lfd.niedersachsen.de/2023, siehe dort S. 73.

Dies zeigt: die Uneinheitlichkeit der Datenschutzaufsicht lässt sich nicht wegdiskutieren. Die Folgen für die mittelständische Wirtschaft sind massiv. Werden identische Sachverhalte von verschiedenen Aufsichtsbehörden unterschiedlich bewertet, entsteht Rechtsunsicherheit. Dies führt zu mehrfachen Abstimmungsschleifen mit unterschiedlichen Datenschutzbehörden, aufwendigen Anpassungen von Prozessen und Dokumentationen, erhöhten Compliance-Kosten, Verzögerung bei Projekten und Wettbewerbsnachteilen gegenüber international tätigen Unternehmen in stärker harmonisierten Rechtsräumen. Unternehmensgruppen mit mehreren rechtlich selbstständigen Standorten sehen sich teilweise gezwungen, unterschiedliche Lösungen für den selben Sachverhalt vorzuhalten, um regionalen Anforderungen Rechnung zu tragen.

Über geeignete Lösungsansätze kann man unterschiedlicher Auffassung sein. Sowohl für eine Zentralisierung als auch für die Beibehaltung der föderalistischen Struktur der Datenschutzaufsicht gibt es nachvollziehbare Argumente. Wer bestehende Inkohärenz in der Aufsichtspraxis nicht anerkennt, wird die Ursachen der bestehenden Probleme kaum wirksam adressieren können.