Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

zum Vorschlag der Europäischen Kommission vom 19. November 2025 für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 und der Richtlinien 2002/58/EG, (EU) 2022/2555 und (EU) 2022/2557 hinsichtlich der Vereinfachung des digitalen Rechtsrahmens und zur Aufhebung der Verordnungen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 und der Richtlinie (EU) 2019/1024 (Digital-Omnibus-Verordnung) – COM(2025) 837 final

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Kontakt:

Berlin, 23. Februar 2026

Federführer:
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
https://die-dk.de/

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Stellungnahme zum Vorschlag für eine „Digital-Omnibus-Verordnung"

Inhaltsverzeichnis

I. Allgemein

Die Deutsche Kreditwirtschaft (DK) nimmt die Gelegenheit wahr, zu dem am 19. November 2025 von der Europäischen Kommission (EU-Kommission) veröffentlichten Vorschlag für eine „**Digital-Omnibus-Verordnung**"[1] Stellung zu nehmen. Dabei fokussieren sich die Anmerkungen der DK auf die Vorschläge

- zur **Änderung der EU-Datenschutzgrundverordnung** (DSGVO) in Art. 3 (siehe Abschnitt II der Stellungnahme) und
- zur **Zusammenfassung der Meldepflichten von Cybersicherheitsvorfällen** in einem einheitlichen Meldemechanismus (siehe Abschnitt III. der Stellungnahme).

Allgemein unterstützt die DK den Ansatz der EU-Kommission den EU-Digitalrechtsrahmen zu modernisieren, kohärenter zu gestalten und zu vereinfachen, um die Wettbewerbsfähigkeit der EU zu fördern und übermäßige bürokratische Lasten abzubauen:

- **Wir begrüßen das Ziel der EU-Kommission, mit Art. 3 des Verordnungsvorschlags durch Änderung der DSGVO einen „innovationsfreundlichen Datenschutzrahmen" zu fördern**. Denn die DSGVO ist mittlerweile über 9 Jahre alt und aufgrund der fortschreitenden technischen Entwicklungen und der bislang in der Praxis gesammelten Erfahrungen verbesserungsbedürftig. Die Vorschläge der EU-Kommission zur Änderung der DSGVO können ein wichtiger Beitrag zur Schaffung von mehr Rechtssicherheit und zur Entbürokratisierung sein. **Gleichwohl besteht bei einigen Vorschlägen der EU-Kommission noch Klärungs- und Verbesserungsbedarf (siehe Abschnitt II.1 bis II.8). Überdies sollten auch weitere Punkte in der DSGVO verbessert und vereinfacht werden (siehe Abschnitt II.9).**

- **Wir begrüßen die Zielsetzung des Digital-Omnibus, das Vorfallsmeldewesen effizienter und konsistenter zu gestalten**. Eine Harmonisierung von Reporting-Anforderungen kann Unternehmen entlasten und Prozesse vereinfachen. Dieses Ziel teilen wir ausdrücklich. **Entscheidend ist jedoch, dass Vereinfachung tatsächlich erreicht wird und nicht durch zusätzliche Komplexität unterlaufen wird (siehe Abschnitt III.).**

Zu den ebenfalls am 19. November 2025 von der EU-Kommission vorgeschlagenen

- Änderungen der Verordnung (EU) 2024/1689 über künstliche Intelligenz[2] und
- Verordnung für die europäischen Unternehmensbrieftaschen[3]

nimmt die DK gesondert Stellung.

---

[1] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 und der Richtlinien 2002/58/EG, (EU) 2022/2555 und (EU) 2022/2557 hinsichtlich der Vereinfachung des digitalen Rechtsrahmens und zur Aufhebung der Verordnungen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 und der Richtlinie (EU) 2019/1024 (Digital-Omnibus-Verordnung)

[2] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Verordnungen (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI) COM/2025/836 final

[3] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Einrichtung europäischer Unternehmensbrieftaschen COM/2025/838 final

II. Zu den DSGVO-Änderungsvorschlägen der EU-Kommission in Art. 3

1. Präzisierung des Anwendungsbereichs des Datenschutzrechts in Bezug auf die Personenbezogenheit von Daten

a. Allgemein

Eine verstärkte innovative und zugleich verantwortungsvolle Datennutzung erfordert einheitliche und rechtssichere Standards für eine wirksame Anonymisierung personenbezogener Daten. Die rechtssichere Anonymisierung personenbezogener Daten ist eine Kernvoraussetzung für datengetriebene Geschäftsmodelle (u.a. bei KI-Anwendungen) und für die Verfügbarkeit qualitativ hochwertiger Daten. Zugleich werden hierdurch ein hohes Datenschutzniveau und das Vertrauen der Betroffenen in den Schutz ihrer personenbezogenen Daten gewährleistet. In der Praxis stehen die Kreditinstitute jedoch vor der Herausforderung, dass weder klare rechtliche Vorgaben noch einheitliche technische Standards und Methoden für eine De-Personalisierung von Daten existieren. Die DSGVO enthält weder eine Legaldefinition von „Anonymisierung" noch einen Mindeststandard, ab wann die Identifizierbarkeit einer Person ausgeschlossen ist. Ebenso fehlen praxistaugliche Vorgaben für eine dauerhafte Pseudonymisierung, insbesondere bei älteren Bestandsdaten, für die keine Einwilligung nach heutigen Standards vorliegt. Dies erschwert nicht nur die Nutzung bestehender Datenbestände (u.a. bei KI-Anwendungen), sondern auch die vertragliche Ausgestaltung von Auftragsverarbeitungen. Erforderlich sind klare Regelungen, wann eine Anonymisierung vorliegt. Auch sollte gesetzlich unterstrichen werden, dass sowohl die Anonymisierung als auch die Pseudonymisierung von Daten durch die verantwortliche Stelle in der Regel zulässig ist und eine gesonderte Erfüllung der Erlaubnistatbestände nach Art. 6 DSGVO nicht erforderlich ist. Dies ließe sich beispielsweise systematisch umsetzen, indem man Art. 6 Abs. 4 DSGVO zur Zweckänderung dahingehend erweitert, dass Anonymisierung und Pseudonymisierung als ausdrücklich erlaubte Weiterverarbeitung stets von der Rechtsgrundlage der ursprünglichen Verarbeitung gedeckt sind.

b. Art. 3 Nr. 1 des Verordnungsvorschlags - Ergänzung der Definition „personenbezogene Daten" in Art. 4 DSGVO

Die EU-Kommission schlägt vor, vor allem aufgrund des EuGH-Urteils vom 4. September 2025 in der Rechtssache C-413/23 P (EDSB / SRB), den Begriff „personenbezogene Daten" als zentralen Anknüpfungspunkt für den Anwendungsbereich der DSGVO zu präzisieren. Die vorgeschlagene Ergänzung zu Art. 4 Nr. 1 DSGVO regelt, dass pseudonymisierte Daten für den Datenempfänger nicht allein deshalb personenbezogen sind, weil sie für den Verantwortlichen Personenbezug haben. Entscheidend soll ausschließlich sein, ob der konkrete Dateninhaber über Mittel verfügt, die „vernünftigerweise wahrscheinlich" zu einer Identifikation führen würden. Erwägungsgrund 27 des Verordnungsvorschlags unterstreicht, dass das Vorhandensein zusätzlicher Informationen bei Dritten die Daten nicht automatisch für alle Beteiligten zu personenbezogenen Daten macht.

Der Vorschlag der EU-Kommission ist zu unterstützen, da damit der Begriff „personenbezogene Daten" unter Berücksichtigung der EuGH-Rechtsprechung im Gesetzestext der DSGVO selbst genauer gefasst wird. Zudem geht damit für die Datenschutzpraxis eine deutliche Stärkung pseudonymisierter und kontextabhängiger (identifikationsarmer) Datenverarbeitung einher. Denn hat der Empfänger von pseudonymisierten Daten selbst keine realistische Möglichkeit zur Re-Identifizierung, fällt die Überlassung von pseudonymisierten Daten an den Empfänger grundsätzlich nicht mehr unter die DSGVO (vgl. auch Erwägungsgrund 27). Dies kann auch die Rahmenbedingungen für KI-Anwendungen vereinfachen.

Klarstellungsbedarf in Bezug auf Auftragsdatenverarbeitungen

Allerdings besteht bei Auftragsdatenverarbeitungen zu folgenden Punkten noch weiterer Klarstellungsbedarf:

- **Entscheidungsrecht der verantwortlichen Stelle als Auftraggeber wahren**
  In der Praxis ist bereits zu beobachten, dass Dienstleister mit Hinweis auf das o.g. EuGH-Urteil den Abschluss eines Vertrags zur Auftragsdatenverarbeitung mit der Begründung ablehnen, dass er als Dienstleister keine personenbezogenen Daten empfange. Deshalb sollte in geeigneter Weise klargestellt werden, dass allein der verantwortlichen Stelle die Bewertung und Entscheidung obliegt, ob die Bereitstellung von pseudonymisierten Daten an einen Dienstleister eines Vertrages zur Auftragsdatenverarbeitung nach Art. 28 DSGVO bedarf oder nicht. Denn letztendlich trägt der Auftraggeber die datenschutzrechtliche Verantwortung für die Daten, die aufgrund seines Wissens für ihn personenbezogen sind. Ist er sich nicht sicher, ob der Dienstleister aufgrund seines aktuellen oder späteren Zusatzwissens die zur Verfügung gestellten Daten einer natürlichen Person zuordnen könnte, dann muss er die Möglichkeit haben, auf den Abschluss eines Auftragsdatenverarbeitungsvertrages bestehen zu können. Dies würde auch eine vertragliche Regelung erlauben, wonach der Dienstleister/Auftragnehmer Mitteilungspflichten hat, wenn er später über Zusatzwissen verfügt, das einen Personenbezug der pseudonymisierten Daten ermöglicht.

- **Verfügungs- und Weisungsrechte des Auftraggebers wahren**
  Stellt der Auftraggeber dem Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung pseudonymisierte Daten zur Verfügung, sollte der Vorschlag der EU-Kommission nicht dazu führen, dass der Auftragnehmer die Daten entgegen der Vorgaben des Auftragsdatenverarbeitungsvertrages für eigene Zwecke nutzen kann, weil dieser meint, es handele sich nicht um personenbezogene Daten. Es muss weiter das Prinzip in der Auftragsdatenverarbeitung gelten, dass der Auftragnehmer an den ihm zur Verfügung gestellten Daten keine eigenen Rechte erhält, sondern in Bezug auf die ihm überlassenen Daten in jedem Fall den Weisungen des Auftraggebers unterliegt. Dies würde sich im Bereich der Kreditwirtschaft auch mit bankaufsichtsrechtlichen Grundsätzen decken, wonach bei der Auslagerung einer Tätigkeit in jedem Fall die Weisungsrechte des Kreditinstituts (Outsourcing-Geber) gegenüber dem Dienstleister (Outsourcing-Nehmer) gelten müssen.

Klarstellungsbedarf für den Fall des späteren Zusatzwissens beim Datenempfänger

Es stellt sich die Frage, wie mit solchen Fällen zu verfahren ist, in denen der Empfänger bei zunächst nicht auf eine bestimmte Person beziehbare pseudonyme Daten später ein Zusatzwissen erhält, mit dem die Daten wieder als personenbezogen gelten würden. Eine Pflicht der verantwortlichen Stelle, die Datenempfänger diesbezüglich regelmäßig zu prüfen, wäre nicht praktikabel. Vielmehr müsste dann der Datenempfänger die datenschutzrechtliche Verantwortung übernehmen. Sollte ein Auftragsdatenverarbeitungsvertrag nach Art. 28 DSGVO abgeschlossen worden sein, könnten dort Meldepflichten des Auftragnehmers an den Auftraggeber bei späterer Personenbeziehbarkeit geregelt werden (s.o.).

c. Art. 3 Nr. 10 des Verordnungsvorschlags - Ermächtigung der EU-Kommission zur Konkretisierung der Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten (Art. 41a DSGVO-neu)

Ergänzend zur Änderung in Art. 4 Nr. 1 DSGVO soll ein neuer Art. 41a DSGVO die EU-Kommission ermächtigen, technische Standards zu definieren, die die Wiederherstellung des Personenbezugs so weit wie möglich ausschließen.

Dieser Vorschlag wird unterstützt, da damit für die Datenschutzpraxis eine wichtige Hilfestellung gegeben werden kann, in welchen Fällen die DSGVO aufgrund Personenbezugs der Daten gilt und in welchen Fällen aufgrund fehlenden Personenbezugs der Daten die DSGVO nicht relevant ist (vgl. dazu auch die Ausführungen oben unter Abschnitt II.1.a). Dies dürfte die Rechtssicherheit bei der Abgrenzung erhöhen.

2. Verarbeitung von personenbezogenen Daten für Entwicklung und -Betrieb von Technologien der Künstliche Intelligenz (KI)

a. Allgemein

Die zunehmende Verbreitung und Relevanz von Technologien der Künstlichen Intelligenz (KI) stellt das bestehende Datenschutzrecht vor strukturelle und normative Herausforderungen. Die DSGVO bietet zwar einen europaweit einheitlichen Rahmen für den Schutz personenbezogener Daten, ist jedoch aufgrund ihrer Entstehung vor einem Jahrzehnt bislang nicht in allen Aspekten auf die besonderen technischen und funktionalen Eigenheiten von KI-Systemen ausgerichtet. Im Zusammenspiel mit der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung) stellen sich in der Praxis eine Vielzahl von Einzelfragen, insbesondere zur Anonymisierung und Pseudonymisierung von Daten, zu einschlägigen Rechtsgrundlagen, zu Zweckänderungsgesichtspunkten, zur Verarbeitung von sensiblen personenbezogenen Daten und zur automatisierten Entscheidungsfindung mit Hilfe von KI. Es besteht daher ein erhöhter Bedarf an klarstellenden Regelungen und an einer kohärenten Verzahnung der datenschutzrechtlichen Anforderungen mit den regulatorischen Vorgaben der KI-Verordnung.

b. Art. 3 Nr. 15 des Verordnungsvorschlags - Spezifische Zulässigkeitsregelung für KI-Entwicklung und -Betrieb in Art. 88c DSGVO-neu

In den Erwägungsgründen 30 und 31 des Verordnungsvorschlags und mit einem neuen Art. 88c DSGVO-neu stellt die EU-Kommission klar, dass die Verarbeitung personenbezogener Daten für die Entwicklung und den Betrieb von KI-Systemen oder von KI-Modellen auf das berechtigte Interesse der verantwortlichen Stelle gestützt werden kann, sofern kein Gesetz eine Einwilligung verlangt und die Interessen oder Grundrechte der Betroffenen nicht überwiegen.

Dieser Ansatz ist zu begrüßen, da damit die wirtschaftliche und technische Bedeutung von KI-Technologien für die Allgemeinheit auch im Datenschutzrecht ausdrücklich anerkannt und damit ein wichtiges Signal gesetzt wird. Mit Art. 88c Abs. 1 DSGVO-neu wird unterstrichen, dass der Erlaubnistatbestand der Interessenabwägung in Art. 6 Abs. 1 f DSGVO regelmäßig für die Verarbeitung personenbezogener Daten im Rahmen der KI-Entwicklung und des KI-Betriebs herangezogen werden kann. Damit dürfte mehr Rechtssicherheit geschaffen werden. Für die Datenschutzpraxis könnte ein Leitfaden mit Beispielsfällen zur Interessenabwägung hilfreich sein.

Allerdings erscheinen die dann folgenden Anforderungen in Art. 88c Abs. 2 DSGVO-neu als zu restriktiv:

- Zum einen werden Prinzipien aus der DSGVO (z.B. in Art. 5 DSGVO) wiederholt, die allgemein gelten. Dies führt nur zu unnötigen rechtlichen Diskussionen, ob damit diese Prinzipien eine andere Bedeutung bekommen sollen.
- Zudem stellt sich die Frage, was mit „enhanced transparency to data subjects" gemeint ist. Besser wäre es, bei den Informationspflichten die Anforderungen in der DSGVO einerseits und in der KI-VO andererseits kohärent zu gestalten. Zusätzlicher Informationspflichten bedarf es nicht.
- Abzulehnen ist das am Ende von Art. 88c Abs. 2 DSGVO vorgesehene unbedingte Widerspruchsrecht des Betroffenen. Denn dieser Ansatz ist deutlich strenger als Art. 21 Abs. 1 DSGVO, wonach die Begründetheit des Widerspruchs im Einzelfall zu prüfen ist, aber der Widerspruch nicht automatisch greift. Auch wird verkannt, dass eine aus dem Widerspruch folgende Löschung von personenbezogenen Daten in KI-Modellen - wenn überhaupt - nur mit einem enorm hohen Aufwand möglich wäre.
- Um die mit Art. 88c Abs. 1 DSGVO-neu bezweckte Rechtssicherheit tatsächlich für alle betroffenen Verantwortlichen zu gewährleisten, sollte klargestellt werden, dass die Vorschrift sektorübergreifend und ohne Regelungslücken anwendbar ist. Dies kann beispielsweise dadurch erreicht werden, dass für öffentliche Stellen bei Wahrnehmung von Aufgaben im öffentlichen Interesse ausdrücklich eine Stützung auf Art. 6 Abs. 1 lit. e DSGVO vorgesehen wird und Art. 6 Abs. 1 UA 1 Satz 2 DSGVO insoweit einer Anwendung von Art. 88c DSGVO-neu nicht entgegensteht.

Insgesamt wäre es besser, in der DSGVO zusätzlich eine spezifische Zulässigkeitsregelung für KI-Entwicklung und -Betrieb aufzustellen, bei der es nicht auf eine Interessenabwägung durch die verantwortliche Stelle ankommt.

c. Art. 3 Nr. 3 des Verordnungsvorschlags - Nutzung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO für KI-Entwicklung und -Betrieb (Art. 9 Abs. 2 (k) und Abs. 5 DSGVO-neu)

Art. 9 DSGVO soll in Abs. 2 mit einem neuen Unterabsatz (k) um eine Ausnahme vom Verarbeitungsverbot ergänzt werden, wenn besondere Kategorien personenbezogener Daten für die Entwicklung und den Betrieb eines KI-Systems genutzt werden sollen. Zusätzlich verpflichtet der neue Art. 9 Abs. 5 Verantwortliche, besonders sensible und persönliche Daten im Sinne von Art. 9 Abs. 1 in KI-Datensätzen möglichst zu verhindern bzw. nachträglich zu entfernen oder zumindest wirksam vor Nutzung und Weitergabe zu schützen.

Der neue Ausnahmebestand für KI-Anwendungen in Art. 9 Abs. 2 (k) DSGVO ist grundsätzlich zu begrüßen, da dieser für mehr Rechtssicherheit bei Nutzung sensiblen Daten in KI-Anwendungen sorgen dürfte. Allerdings sind die zusätzlichen Anforderungen in Art. 9 Abs. 5 DSGVO zur Prüfungs- und Entfernungspflicht in Bezug auf sensible Daten nicht ganz verständlich. Wenn in der KI-Anwendung tatsächlich die sensiblen Daten herausgefiltert werden könnten, dann wäre Art. 9 DSGVO eigentlich nicht mehr relevant. Lassen sich sensible Daten nicht herausfiltern, dann dürfte eigentlich nur die Schutzvorkehrung im letzten Satz von Art. 9 Abs. 5 Bedeutung haben.

3. Art. 3 Nr. 3 des Verordnungsvorschlags - Verarbeitung biometrischer Daten zur Identifizierung des Betroffenen (Art. 9 Abs. 2 (l) DSGVO-neu)

Art. 9 DSGVO soll in Abs. 2 mit einem neuen Unterabsatz (l) um eine Ausnahme vom Verarbeitungsverbot für biometrische Identitätsbestätigung unter alleiniger Kontrolle der betroffenen Person ergänzt werden. Auch diese

Änderung ist grundsätzlich zu unterstützen, da sie für mehr Rechtssicherheit bei Identifizierungsvorgängen sorgen kann.

Weitergehender Verbesserungsbedarf in Art. 9 DSGVO:

- *Verarbeitung zur Erfüllung vertraglicher Pflichten*

Zusätzlich sollte in Art. 9 Abs. 2 DSGVO als neuen Erlaubnistatbestand die für den Abschluss und die Erfüllung eines Vertrags erforderlichen Verarbeitungen sensibler Daten aufgenommen werden. Denn ist die Verarbeitung sensibler Daten für die Vertragsanbahnung und -erfüllung erforderlich, bedarf es nicht einer gesonderten Einwilligung des Betroffenen. Vielmehr ist dann der jeweilige Vertrag zugleich Rechtsgrundlage als auch Verbotsausnahme. Als Beispiel aus der Praxis ist die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person zu nennen. Nach der EU-Zahlungsdiensterichtlinie (2015/2366) ist für Online-Transaktionen eine starke Kundenauthentifizierung vorzusehen, bei der auch biometrische Daten eingesetzt werden können. Haben Kunde und Kreditinstitut sich auf die Authentifizierung mittels biometrischer Daten vertraglich geeinigt, sollte dies sogleich auch nach Art. 9 DSGVO legitimiert sein.

- *Mischdatensätze*

Der Anwendungsbereich von Art. 9 Abs. 1 DSGVO wird vom EuGH regelmäßig sehr weit ausgelegt, was zur Folge hat, dass auch Daten, aus denen lediglich mittelbar Rückschlüsse auf sensible personenbezogene Daten gezogen werden können, als Daten i. S. v. Art. 9 Abs. 1 DSGVO betrachtet werden. Im Zahlungsverkehr betrifft dies häufig Umsatzdaten, die als sog. Mischdatensätze aufgrund ihres Empfängers oder Verwendungszwecks Rückschlüsse zulassen auf z. B. den Gesundheitszustand oder die Partei- oder Gewerkschaftszugehörigkeit des Zahlenden. Dies hat zur Folge, dass Datenverarbeitungen sich regelmäßig an den strengeren Anforderungen von Art. 9 DSGVO messen lassen müssen und viele Rechtsgrundlagen aus Art. 6 DSGVO unanwendbar sind. Wir regen daher an, Art. 9 Abs. 1 DSGVO sachgerecht einzuschränken. Bei Mischdatensätzen, die lediglich mittelbar Rückschlüsse auf sensible personenbezogene Daten zulassen, die nicht den Schwerpunkt der Verarbeitungstätigkeit bilden, ist eine kontextabhängige Betrachtung erforderlich, welche sich (wie vielfach in der datenschutzrechtlichen Literatur vertreten) an der Auswertungsabsicht des Verantwortlichen oder an einem Zu-Nutze-Machen des sensiblen Informationsgehalts durch den Verantwortlichen orientieren sollte.

- *Unaufgefordert zur Verfügung gestellte Daten*

In den täglichen Geschäftsbeziehungen zwischen Kunde und Bank kommt es zudem immer wieder vor, dass sensible personenbezogene Daten vom Betroffenen unaufgefordert an das Kreditinstitut übermittelt werden („aufgedrängte Daten"). Da Art. 9 Abs. 2 lit. a DSGVO jedoch keine konkludente Einwilligung gelten lässt und die Daten aufgrund des begrenzten Empfängerkreises auch nicht „offensichtlich öffentlich gemacht" wurden, dürfen sie nach derzeitiger Rechtslage nicht verarbeitet werden. Um den Kundeninteressen in solchen Fällen stärker Rechnung zu tragen, wird angeregt, die in Art. 9 Abs. 2 lit. e DSGVO normierte Verbotsausnahme tatbestandlich um personenbezogene Daten zu erweitern, die von der betroffenen Person unaufgefordert bereitgestellt wurde.

4. Beschränkung von Informations- und Auskunftspflichten

a. Art. 3 Nr. 4 des Verordnungsvorschlags - Rechte der betroffenen Person (Art. 12 Abs. 5 DSGVO-neu)

Durch die Neufassung von Art. 12 Abs. 5 DSGVO soll die verantwortliche Stelle die Möglichkeit haben, bei offensichtlich unbegründeten oder exzessiven Anfragen sowie bei missbräuchlichen Auskunftsersuchen nach Art. 15 DSGVO, eine angemessene Gebühr zu verlangen oder den Antrag abzulehnen. Diese Änderung ist sehr zu begrüßen, da sie helfen kann, exzessive oder missbräuchliche Auskunftsersuchen zu beschränken.

Weitergehender Verbesserungsbedarf in Art. 15 DSGVO:

Die Regelung zum Auskunftsrecht nach Art. 15 DSGVO bedarf noch weiterer Verbesserungen:

- *Zweckbegrenzung*

Das Auskunftsrecht des Betroffenen nach Art. 15 DSGVO ist ein Grundpfeiler des Datenschutzrechts, wie auch die Rechtsprechung des EuGH belegt. Doch zeigen die Praxis und die Rechtsprechung (vgl. EuGH, Urt. v. 26. Oktober 2023 - C 307/22, BGH, Urt. vom 5. März 2024 - VI ZR 330/21), dass dieses Recht auch für datenschutzfremde Zwecke zum Teil auch sehr exzessiv instrumentalisiert wird (z. B. in arbeitsrechtlichen Beendigungsstreitigkeiten im Rahmen von Verhandlungen über Abfindungen). Deshalb sollte in Art. 15 DSGVO selbst im Sinne des Erwägungsgrundes 63 S. 1 DSGVO klargestellt werden, dass das Auskunftsrecht ausschließlich dazu dienen darf, dass der Betroffene damit seine Datenschutzrechte und keine anderweitigen Zwecke verfolgt.

- *Konkretisierung des Auskunftsersuchens*

Die Bearbeitung von Auskunftsersuchen durch die verantwortliche Stelle sollte dahin gehend erleichtert werden, dass der Betroffene grundsätzlich darlegen sollte, auf welche konkreten Bereiche sich sein Auskunftsersuchen erstreckt. Dies wird zwar in Erwägungsgrund 35 des Verordnungsvorschlags bereits berücksichtigt, jedoch sollte dieser Erwägungsgrund aus dem Verordnungsvorschlag und dem Erwägungsgrund 63 S. 7 DSGVO in der Vorschrift des Art. 15 DSGVO selbst berücksichtigt werden.

- *Bereits erfolgte Auskünfte und Archivdaten*

Vom Auskunftsrecht sollten solche Daten ausgenommen sein, die der Verantwortliche dem Betroffenen in der Vergangenheit nachweislich bereits zur Verfügung gestellt hat oder die lediglich zur Erfüllung gesetzlicher Aufbewahrungspflichten vorgehalten werden, also nur noch zu Archivzwecken gespeichert sind.

- *Begriff der Kopie*

Der Begriff der Kopie in Art. 15 Abs. 3 S. 1 DSGVO sollte klarer definiert werden. Zudem wäre es gut, wenn deutlicher als bisher dargestellt würde, dass das Recht auf Erhalt einer Kopie Betroffenen kein Wahlrecht hinsichtlich der Form der Datenwiedergabe gewährt.

b. Art. 3 Nr. 5 des Verordnungsvorschlags – Beschränkung von Informationspflichten (Art. 13 Abs. 4 DSGVO-neu)

Durch den neugefassten Abs. 4 in Art. 13 DSGVO sollen die Informationspflichten des Verantwortlichen bei „geringer Datenintensität" eingeschränkt werden, wenn Daten in einer „klaren und beschriebenen Beziehung zwischen betroffener Person und einem Verantwortlichen" erhoben werden und davon auszugehen ist, dass die betroffene Person bereits allgemein informiert ist. Ausgenommen von dieser Erleichterung der Informationspflicht: Bei Weitergabe der Daten, Transfer der Daten in Drittstaaten, automatisierten Entscheidungen oder hohem Risiko der Datenverarbeitung.

Grundsätzlich ist dieser Ansatz zu unterstützen, da bei Datenverarbeitungen mit geringem Umfang eine Informationsüberflutung des Betroffenen vermieden werden kann und weniger Aufwand bei der verantwortlichen Stelle anfällt.

Zusätzliche Möglichkeit der Vermeidung einer Informationsüberflutung

Aus Sicht der Kreditwirtschaft besteht zusätzlicher Verbesserungsbedarf: Die Informationspflichten für die verantwortliche Stelle in Art. 13 und 14 DSGVO sind zu detailliert und überbordend. Sie sollten auf ein vernünftiges Maß beschränkt werden, um Betroffene nicht mit Informationen zu überfluten – weniger ist mehr. Vorzugswürdig wäre ein zweistufiger Ansatz, d.h. ein Überblick über wesentliche Aspekte der Datenverarbeitung bei der verantwortlichen Stelle auf erster Stufe und Detailinformationen zum Abruf/auf Nachfrage des Betroffenen auf zweiter Stufe. Dies würde Unternehmen und Betroffene entlasten und im Ergebnis für mehr Transparenz gegenüber den Betroffenen sorgen, da hinsichtlich wirklich relevanter Informationen fokussiert informiert werden würde. Auch ist es unverhältnismäßig, dass bereits ein vergleichsweise kleines Informationsdefizit zu Sanktionen führen oder als Wettbewerbsverstoß eingeordnet werden kann (vgl. die zu weite Auslegung im Urteil des BGH v. 27.3.2025 – I ZR 186/17).

5. Art. 3 Nr. 7 des Verordnungsvorschlags - Vereinfachung der Zulässigkeit automatisierter Einzelentscheidungen (Art. 22 DSGVO-neu)

Bislang sind automatisierte Einzelentscheidungen mit negativen Folgen für den Betroffenen verboten, außer es greift einer der Ausnahmegründe in Art. 22 Abs. 2 DSGVO. Durch die von der EU-Kommission vorgeschlagene Neuformulierung des Art. 22 Abs. 1 und Abs. 2 DSGVO wird das Verbot gestrichen und es werden nur noch die Bedingungen definiert, die erfüllt sein müssen, damit eine automatisierte Einzelentscheidung zulässig ist. Dabei wird mit Abs. 1 (a) die Zulässigkeit einer automatisierten Einzelentscheidung zur Begründung und Durchführung eines Vertrages erweitert, weil es für die Erforderlichkeit nicht darauf ankommen soll, dass alternativ eine nicht-automatisierte Entscheidung möglich wäre.

Der Änderungsvorschlag ist zu unterstützen. Zum einen wird die Vorschrift vereinfacht und verständlicher. Zudem wird klargestellt, dass die Nutzung automatisierter Einzelentscheidungen in Vertragssituationen auch zulässig ist, wenn es die Alternative einer nicht-automatisierten Entscheidung geben würde.

6. Art. 3 Nr. 8 des Verordnungsvorschlags - Erleichterungen bei der Meldung von Datenschutzverletzungen (Art. 33 Abs. 1 DSGVO)

Die von der EU-Kommission vorgeschlagene Beschränkung der Meldepflicht in Art. 33 Abs. 1 DSGVO-neu auf Fälle mit hohen Risiken ist als organisatorische Erleichterung zu begrüßen und trägt dem Grundsatz der Verhältnismäßigkeit Rechnung.

Auch die Erweiterung der Meldefrist von 72 auf 96 Stunden ist zu begrüßen, um der verantwortlichen Stelle mehr Zeit zur Prüfung des Vorfalls einzuräumen. Der aktuelle Zeitrahmen für Meldungen ist zu knapp, insbesondere bei Vorfällen vor Feiertagen oder an Freitagen. Zum Teil nehmen die Sachverhaltsermittlung und nötige Aufklärungen mehr Zeit in Anspruch, was an Freitagen oder vor Feiertagen in der Praxis oft zu Schwierigkeiten und ggf. zu unvollständigen oder voreiligen Meldungen führt, nur um die 72-Stunden-Frist einhalten zu können. Zudem sollten bei der Fristberechnung Sonntage und gesetzliche Feiertage nicht mitzählen, da dann grundsätzlich weder die Unternehmen noch die Datenschutzbehörden aktiv sind. Als Lösung bietet sich in Anlehnung an den „Arbeitstag"-Ansatz in Art. 3 Abs. 3 und 5 der „Verordnung Nr. 1182/71 des Rates zur Festlegung der Regeln für die Fristen, Daten und Termine" an, die Fristbemessung in Art. 33 Abs. 1 S. 2 DSGVO statt der von der EU-Kommission vorgeschlagenen 96 Stunden auf „vier Arbeitstage" umzustellen.

Die Entwicklung eines einheitliches Meldeformulars durch den EU-Datenschutzausschuss ist zu unterstützen. Ein solcher Standard dürfte für organisatorische Erleichterungen sorgen. Gleichwohl wird darauf zu achten sein, dass das Standardmeldeformular praxistauglich ausgestaltet wird und sich auf das Wesentliche beschränkt.

7. Art. 3 Nr. 9 des Verordnungsvorschlags - Erleichterung der Datenschutzfolgenabschätzung (Art. 35 Abs. 4 ff. DSGVO-neu)

Die EU-Kommission schlägt vor, dass der EU-Datenschutzausschuss eine Liste von Fällen veröffentlicht, in denen eine Datenschutzfolgenabschätzung erforderlich ist. Bisher ist dies eine Aufgabe der nationalen Datenschutzaufsichtsbehörden. Eine EU-weite Einheitlichkeit der Liste wird positiv bewertet.

Datenschutzfolgenabschätzung nach DSGVO und Grundrechtsfolgenabschätzung nach KI-Verordnung synchronisieren

Die Datenschutzfolgenabschätzung nach Art. 35 DSGVO sowie die Grundrechtsfolgenabschätzung für Hochrisiko-KI-Systeme nach Art. 27 KI-Verordnung verfolgen übereinstimmend das Ziel, potenzielle Risiken für die Rechte und Freiheiten natürlicher Personen im Vorfeld technischer Systementwicklungen systematisch zu identifizieren, zu bewerten und – soweit möglich – zu minimieren. Beide Instrumente beruhen auf dem präventiven Risikomanagementansatz des europäischen Grundrechtsschutzes, sind bislang jedoch weder inhaltlich noch methodisch aufeinander abgestimmt.

Vor diesem Hintergrund erscheint eine systematische Koordinierung beider Prüfregime geboten. Die gegenwärtige Parallelität der Anforderungen birgt das Risiko redundanter Prüfprozesse auch in ggf. unterschiedlichen Fachbereichen aufgrund Zuständigkeitsverteilungen sowie potenziell widersprüchlicher Wertungen in Bezug auf die Schutzbedürftigkeit betroffener Rechtsgüter. Zur Vermeidung doppelten Verwaltungsaufwands und zur Steigerung der rechtspraktischen Kohärenz ist eine stärkere inhaltliche und strukturelle Verzahnung von Datenschutzfolgenabschätzung und Grundrechtsfolgenabschätzung erforderlich.

8. Art. 3 Nr. 10 des Verordnungsvorschlags - Modernisierung der „Cookie-Vorschriften" (Art. 88a und Art. 88b DSGVO-neu)

Eine Überarbeitung der bislang in der ePrivacy-Richtlinie (Richtlinie 2002/58/EG in der Fassung der Richtlinie 2009/136/EG) verorteten „Cookie-Regeln" ist zu begrüßen, um der Ermüdung durch „Cookie-Banner" („cookie-fatigue") zu begegnen. Jedoch sollten folgende Punkte berücksichtigt werden:

- Mit Schaffung spezieller „Cookie-Vorschriften" in der DSGVO müsste die Regelung in Art. 5 Abs. 3 ePrivacy-Richtlinie insgesamt gestrichen werden, um Doppelregulierungen zu vermeiden. Nach Art. 5 Nr. 2 des Verordnungsvorschlags soll zwar der Anwendungsbereich von Art. 5 Abs. 3 ePrivacy-Richtlinie auf Fälle beschränkt werden, in denen keine personenbezogenen Daten verarbeitet werden. Doch ist nicht klar, warum es überhaupt noch dieser Regelung in der ePrivacy-Richtlinie bedarf, wenn der Datenschutz durch die neue Art. 88a und 88b DSGVO gewahrt werden soll.

- In dem Ausnahmetatbestand des Art. 88c Abs. 3 (d) DSGVO-neu, wonach keine Zustimmung des Betroffenen erforderlich ist, wenn der „Cookie" der Wahrung der Verarbeitungssicherheit dient, sollte zusätzlich auch der Zweck der Vermeidung von missbräuchlicher Nutzung des Online-Dienstes aufgenommen werden *(„(d) maintaining or restoring the security **or misuse** of a service…."*). Denn auch bei der Missbrauchs- und Betrugsabwehr kann der Einsatz von „Cookies" ein wichtiges Instrument sein. Der Einsatz dieser technischen Verfahren zur Missbrauchs- und Betrugsprävention sollte weiter ohne Einwilligung möglich sein.

- Das sechsmonatige Wiederholungsverbot einer Einwilligungsanfrage in Art. 88 Abs. 4 (c) DSGVO-neu ist nicht sachgerecht. Denn es müssten bei der verantwortlichen Stelle hierfür spezielle technische Rahmenbedingungen geschaffen werden, um personenbezogen die Einhaltung der Frist kontrollieren und steuern zu können. Damit würde eine Menge von personenbezogener Daten gespeichert, was im Widerspruch zum Grundsatz der Datenminimierung steht.

9. Zusätzlicher Verbesserungsbedarf in der DSGVO

a. Art. 5 Abs. 2 DSGVO - Nachweispflichten nach dem Verhältnismäßigkeitsgrundsatz aussteuern

Die sehr allgemein und abstrakt gefasste Nachweispflicht (accountability) in Art. 5 Abs. 2 DSGVO in Kombination mit dem übermäßigen Sanktionsregime in Art. 83 DSGVO hat zu einer enormen Bürokratisierung der unternehmensinternen Datenschutzkontrolle und zu einem gewaltigen Ausufern der Dokumentationspflichten in den Unternehmen geführt. Gewiss ist eine ordnungsgemäße Dokumentation der Umsetzung der DSGVO sinnvoll, doch sollte diese sich auf das Erforderliche beschränken. Auch der Grad der Datenschutzrisiken sollte ausschlaggebend für den Umfang von Nachweispflichten sein. Eine automatische Verknüpfung eines etwaigen Dokumentationsdefizits mit dem strengen Sanktionsregime ist unverhältnismäßig. Es sollte hier ein stärkerer risikobasierter Ansatz betont werden. Wünschenswert wäre außerdem die Möglichkeit der Bezugnahme auf und der gegenseitigen Anerkennung von gesetzlich geforderten Dokumentationen (DSGVO, bankaufsichtsrechtlichen Regelungen zur Risikosteuerung [MaRisk], Digital Operational Resilience Act [DORA], bankaufsichtlichen Anforderungen an die IT [BAIT], gemeinsames Cybersicherheitsniveau [NIS2], ISO-Standards).

b. Art. 6 Abs. 1 lit. c, Abs. 2 und 3 DSGVO – DSGVO sollte Vorrang von Spezialgesetzen mit Datenschutzrelevanz deutlicher akzeptieren

Das Verhältnis der DSGVO zu anderen Rechtsvorschriften bereitet immer wieder Probleme in der Praxis. Gerade Kreditinstitute unterliegen vielen spezialgesetzlichen und bankaufsichtsbehördlichen Anforderungen zur Datenverarbeitung (in Deutschland z.B. MaRisk, BAIT, DORA). Diese spezialgesetzlichen Regelungen müssen die Leitlinie bilden und auch die damit verbundene Verarbeitung personenbezogener Daten rechtfertigen. Ein Unternehmen wäre völlig überfordert, die Kompatibilität der spezialgesetzlichen Regelungen mit der DSGVO

eigenständig überprüfen zu müssen. Dies ist allein Aufgabe des Gesetzgebers. Die DSGVO sollte daher deutlicher den sektorspezifischen Regelungen nachgeordnet werden, um Widersprüche zu vermeiden.

c. Art. 25 DSGVO – Einbeziehung von Herstellern

Der Adressatenkreis von Art. 25 DSGVO zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sollte auf Hersteller von Datenverarbeitungsprodukten ausgedehnt werden, denn diese sind die Produktverantwortlichen. Derzeit sind die Produktanwender gezwungen, von Herstellern erworbene Produkte vor deren Einsatz auf Datenschutzschwachstellen zu prüfen, was erheblichen Aufwand verursacht und bei der Nutzung komplexer Software wie bspw. KI-Anwendungen (technisch) nicht zu leisten ist. Auch lassen sich Produkte vom Anwender oft nicht anpassen. Die laufende Debatte über die datenschutzkonforme Nutzung von Microsoft 365-Produkten verdeutlicht dieses Problem. Hersteller sollten verpflichtet sein, datenschutzrechtliche Vorgaben bereits in der Produktentwicklung zu berücksichtigen und sich am Stand der Technik zu orientieren, um den Verantwortlichen bei Einsatz des Produkts die Erfüllung ihrer Verpflichtungen zu ermöglichen. Da Hersteller von Diensten, Produkten und Anwendungen gerade in Zeiten immer schnellerer technologischer Weiterentwicklung eine Schlüsselfunktion sowohl für Datenschutz als auch Datensicherheit einnehmen, sollte ihnen unter der DSGVO eine gesonderte Rolle (bspw. „produktverantwortliche Stelle") mit eigenständigen Pflichten (und Sanktionierungsmöglichkeiten) zugewiesen werden. Insbesondere sollten Hersteller in die Pflicht genommen werden, die Datenschutzkonformität ihrer Produkte entsprechend der Einsatzzwecke zu gewährleisten, wozu auch eine datenschutzkonforme Grundeinstellung für die öffentlich beworbene Standardnutzung gehören sollte.

d. Art. 26 DSGVO – Ansatz der gemeinsamen Verantwortung bedarf Überarbeitung

Das Merkmal der „gemeinsamen Bestimmung über die Mittel und Zwecke" zur Einstufung als „gemeinsame Verantwortung" in Art. 26 DSGVO ist sehr generisch. Es wird daher vorgeschlagen, die Fallgruppen der gemeinsamen Verarbeitung klarer zu definieren, indem man über das allgemeine Merkmal der gemeinsamen Bestimmung über die Mittel und Zwecke hinausgeht. Der Aufwand für die Ausgestaltung der gemeinsamen Verarbeitung im horizontalen Verhältnis zwischen den Verarbeitern und im vertikalen Verhältnis zu den Betroffenen steht in vielen Fällen nicht in einem angemessenen Verhältnis zum datenschutzrechtlichen Mehrwert für die Betroffenen. Die gesamtschuldnerische Haftung ist in der Praxis oft unverhältnismäßig, selbst unter Berücksichtigung des Einblicks und der Einflussnahme auf die Datenverarbeitung der jeweils anderen Partei. Daher wird eine angemessene Begrenzung der gemeinsamen Haftung im Außenverhältnis empfohlen. Außerdem sollte allein die sachnächste Aufsichtsbehörde zuständig sein, um widersprüchliche aufsichtsbehördliche Entscheidungen zu vermeiden.

III. „Single-entry point for incident reporting" in Art. 6 und 8

Wir begrüßen die Zielsetzung in Art. 6 und 8 der Digital-Omnibus-Verordnung, das Vorfallsmeldewesen effizienter und konsistenter zu gestalten. Eine Harmonisierung von Reporting-Anforderungen kann Unternehmen entlasten und Prozesse vereinfachen. Dieses Ziel teilen wir ausdrücklich. Entscheidend ist jedoch, dass Vereinfachung tatsächlich erreicht wird und nicht durch zusätzliche Komplexität unterlaufen wird.

Ein Single-Entry-Point kann für Unternehmen, die in mehreren Mitgliedstaaten oder nach mehreren Rechtsakten meldepflichtig sind, grundsätzlich Vorteile haben. Gleichzeitig birgt ein zentraler Meldeweg erhebliche Risiken. Er schafft eine Abhängigkeit von einer einzigen Infrastruktur. Fällt diese aus oder weist sie Sicherheitslücken auf, sind sämtliche Meldungen betroffen. Eine zentrale Plattform wird zudem zu einem besonders attraktiven

Angriffsziel. Diese Risiken müssen bei der Bewertung des erwartbaren Nutzens angemessen berücksichtigt werden.

Im Finanzsektor besteht bereits heute eine weitgehende Harmonisierung des Vorfallsmeldewesens. Meldungen erfolgen einheitlich nach DORA. DORA gilt als lex specialis gegenüber NIS2 und CER. Die zuständigen Behörden-strukturen sind etabliert. Meldungen werden zentral entgegengenommen und an relevante nationale und europäische Stellen weitergeleitet. Ein ersetzender Single-Entry-Point würde diese funktionierenden Strukturen aufbrechen, erhebliche Transformationskosten verursachen und klare Zuständigkeiten verwischen. Er würde neue Koordinationsbedarfe schaffen, ohne einen erkennbaren Mehrwert zu liefern. Aus Sicht der empfangenden Behörden kann eine weitere inhaltliche Harmonisierung der bestehenden Meldungen nach DORA und NIS2 jedoch sinnvoll sein.

Vorfallsmeldungen nach DSGVO und KI-Verordnung unterscheiden sich hingegen deutlich in Zielrichtung, Inhalt und Systematik, sowohl untereinander als auch im Vergleich zu Meldungen nach DORA, NIS2 und CER. Eine inhaltliche Harmonisierung ist hier nur eingeschränkt möglich.

Besondere Risiken sehen wir zudem bei Verantwortlichkeiten und Haftungsfragen. Bei einem zentralen Meldeweg ist unklar, wer für Entgegennahme, Bearbeitung und fristgerechte Weiterleitung verantwortlich ist. Es besteht das Risiko, dass Meldungen verzögert werden oder Rückfragen ungeklärt bleiben. Haftungsfragen bei technischen Störungen oder Fristversäumnissen sind bislang nicht eindeutig geregelt. Unterschiedliche nationale Zusatzanfor-derungen und Fristen erhöhen dieses Risiko weiter. Ein komplexes Meldeformular, das alle Fallkonstellationen abbilden soll, würde die Fehleranfälligkeit zusätzlich steigern.

Hinzu kommt, dass der interne Abstimmungsaufwand in den Unternehmen bestehen bleibt. Die Frage, wer welchen Sachverhalt meldet und welche Frist gilt, lässt sich nicht allein durch ein Portal lösen. Ohne ausreichend bemesse-ne Übergangsfristen und klare technische Vorgaben drohen erhebliche Umsetzungsprobleme. Die Kosten für An-passungen von Prozessen, IKT-Systemen und Schulungen sind erheblich und müssen realistisch berücksichtigt werden.

Vor diesem Hintergrund sprechen wir uns für einen differenzierten Ansatz aus. Das etablierte Meldewesen nach DORA sollte beibehalten werden. Aufgrund der inhaltlichen Nähe kann geprüft werden, DORA- und CRA-Meldungen stärker zu verzahnen und Meldefristen zu harmonisieren. Meldungen nach DSGVO und KI-Verordnung sollten weiterhin separat erfolgen, um ihrer jeweiligen Zielrichtung und Praxis gerecht zu werden. Vorrangig sollte die Vereinfachung und Vereinheitlichung der Meldeanforderungen selbst verfolgt werden, etwa durch praxisgerechtere Daten-felder und Schwellen, einheitliche Definitionen und abgestimmte Fristen.

Daher sollte auf die Ersetzung funktionierender sektoraler Meldewege durch einen zentralen Meldeweg verzichtet werden. Erforderlich sind klare Zuständigkeiten, eindeutige Haftungsregelungen und hohe Sicherheitsstandards, bevor weitere Zentralisierungsschritte erfolgen. Ebenso notwendig sind ausreichend lange Übergangsfristen und frühzeitige Transparenz zur Architektur und technischer Umsetzung. Harmonisierung sollte vorrangig bei den Inhalten ansetzen und nicht allein bei der technischen Plattform. Nur so kann der Digital-Omnibus sein Ziel erreichen, das Vorfallsmeldewesen tatsächlich einfacher, sicherer und effizienter zu gestalten.

***