# Stellungnahme

**14.10.2025**
**Philipp Hagen**, Director Legal Affairs & Data Privacy, hagen@bvdw.org
**Janek Kuberzig**, Public Affairs Manager Data & Technology, kuberzig@bvdw.org

## Bundesverband Digitale Wirtschaft (BVDW) e.V. – Stellungnahme zum Vorschlag eines Digitalpaket und –omnibus der Europäischen Kommission

### Übersicht

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. begrüßt die Initiative der Europäischen Kommission, mit den Omnibusvorschriften für den Digitalbereich einen konkreten Beitrag zur sofortigen Vereinfachung des regulatorischen Rahmens für digitale Geschäftsmodelle zu leisten. Der Ansatz, die Einhaltungskosten für Unternehmen spürbar zu senken, ohne die grundlegenden Schutzstandards für Bürger*innen zu schwächen, ist richtig und notwendig. Besonders hervorzuheben ist die geplante Eignungsprüfung, mit der die Kohärenz und die kumulativen Anforderungen des bestehenden EU-Rechts im digitalen Bereich überprüft werden sollen. Eine solche Gesamtschau ist überfällig, da sich in den vergangenen Jahren durch eine Vielzahl horizontaler und sektorspezifischer Regelungen erhebliche Komplexität, Fragmentierung und Rechtsunsicherheit aufgebaut haben.

### Digital Omnibus

Im Bereich der Datengesetzgebung zeigt sich diese Problematik besonders deutlich. Das Dokument der Europäischen Kommission weist zu Recht darauf hin, dass die geltenden Vorschriften oftmals auf mehrere Instrumente verteilt sind und für kleine und mittlere Unternehmen erhebliche Belastungen darstellen. Die im Rahmen der Data Union Strategy vorgesehene Vereinfachung und Zusammenführung der relevanten Rechtsakte ist deshalb von zentraler Bedeutung.

Aus Sicht des BVDW darf es dabei jedoch nicht bei einer bloßen Konsolidierung bleiben. Vielmehr muss die europäische Datenpolitik einen klaren Perspektivwechsel vollziehen: Weg von einer rein risikoorientierten Regulierung hin zu einem stärkeren Fokus auf die Chancen der Datennutzung. Daten sind der Treibstoff für Innovation und Wettbewerbsfähigkeit in nahezu allen Branchen. Ein regulatorischer Rahmen, der diese Nutzung erleichtert, schafft die Grundlage für Wertschöpfung und gesellschaftlichen Fortschritt. Entscheidend ist daher, Doppelregelungen abzubauen, unklare Schnittstellen zu präzisieren und insbesondere KMU von unverhältnismäßigen Belastungen zu entlasten, ohne dabei den Schutz berechtigter Interessen zu vernachlässigen.

# Stellungnahme

**AI Act**

Als besonders entscheidend bewertet der BVDW die angesprochenen Herausforderungen rund um die Anwendung der KI-Verordnung. Die Kommission hebt hervor, dass es bei der Umsetzung darum gehen muss, Rechtssicherheit zu gewährleisten und die Unternehmen – gerade kleinere und mittelgroße – nicht durch überbordende Anforderungen zu überfordern. Wir teilen diese Einschätzung ausdrücklich. Gleichzeitig möchten wir davor warnen, das Primärrecht oder zentrale Grundlagen der Verordnung erneut aufzuschnüren. Ein solches Vorgehen würde zwangsläufig zu Rechts- und Planungsunsicherheit führen, mit gravierenden Folgen insbesondere für innovative Unternehmen im Mittelstand.

Auch die zurzeit laufende Debatte zum „Stop-the-clock"-Mechanismus muss mit Bedacht geführt werden. Eine Verschiebung der Fristen hat zur Folge, dass bereits geleistete Investitionen von Unternehmen in Compliance sich, wenn überhaupt, erst später auszahlen. Stattdessen sollten gezielte Nachschärfungen bei unklaren Begrifflichkeiten vorgenommen werden, um die Anwendbarkeit in der Praxis zu verbessern. Ergänzend dazu ist es notwendig, Unternehmen durch konkrete Compliance-Instrumente zu unterstützen – etwa durch leicht zugängliche, verständliche und aussagekräftige Leitlinien. Außerdem können standardisierte Prüfverfahren oder digitale Tools eine große Hilfe sein. Nur so kann die Apply AI Strategy tatsächlich zu einem Innovationsmotor für den europäischen Markt werden, anstatt Verunsicherung und Investitionshemmnisse zu erzeugen.

**ePrivacy Richtlinie** [1]

Ein weiteres wichtiges Feld betrifft die Datenschutzrichtlinie für elektronische Kommunikation, insbesondere die Vorschriften zu Cookies und Tracking-Technologien. Die Kommission benennt zutreffend die Problematik der „Einwilligungsmüdigkeit" bei Nutzer*innen.

Der BVDW sieht hier erheblichen Handlungsbedarf und unterstützt ausdrücklich die Absicht, die Anforderungen an Cookie-Einwilligungen zu senken. Verarbeitungen, die nur ein geringes Risiko für die Rechte und Freiheiten der Betroffenen bergen, sollten von der Einwilligungspflicht ausgenommen werden. Dies würde nicht nur die Belastung der Unternehmen reduzieren, sondern auch die Akzeptanz und Wirksamkeit der Einwilligungsmechanismen verbessern. Eine Reduzierung der „Einwilligungsmüdigkeit" ist sowohl im Interesse der Verbraucher*innen als auch der Unternehmen, die auf verlässliche und rechtssichere Daten angewiesen sind.

[1] Für eine tiefergehende Position sehen Sie bitte Anlage I

**DSGVO** [2]

Neben der Anpassung der oben angesprochenen Richtlinie bedarf es auch einer tiefgehenden Analyse der Datenschutz-Grundverordnung (DSGVO) und deren Zusammenspiel mit den weiteren Rechtsakten.

Die DSGVO ist die zentrale Grundlage des europäischen Daten- und Digitalrechts. Nach mehr als sieben Jahren ihrer Anwendung zeigt sich jedoch, dass wesentliche Elemente der Verordnung in ihrer jetzigen Form weder die notwendige Rechtssicherheit noch die erforderliche Praxistauglichkeit bieten. Die Digitale Wirtschaft ist durch überbordende Nachweispflichten, unklare Begriffsbestimmungen und eine fragmentierte Aufsichtsarchitektur erheblich belastet. Ziel einer Reform muss es daher sein, die DSGVO risikobasiert weiterzuentwickeln, unnötige bürokratische Hürden abzubauen und zugleich ein hohes Datenschutzniveau für die betroffenen Personen sicherzustellen.

**Fazit**

Zusammenfassend unterstützt der BVDW die Ziele der Kommission, durch die Omnibusvorschriften und die anschließende Eignungsprüfung eine spürbare Entlastung für Unternehmen zu schaffen, ohne die relevanten Schutzstandards der Bürger*innen zu schwächen. Dabei ist es entscheidend,

- die Datengesetzgebung konsequent zu vereinfachen und stärker chancenorientiert auszurichten,
- die KI-Verordnung nicht erneut grundsätzlich zu öffnen, sondern gezielt zu präzisieren und durch praktische Hilfen für Unternehmen flankierend abzusichern,
- die Datenschutzrichtlinie durch eine Absenkung der Einwilligungsanforderungen nutzerfreundlich und innovationsfördernd zu modernisieren sowie
- im Bereich Cybersicherheit und digitaler Identität Doppelstrukturen abzubauen und Klarheit zu schaffen.

Auf diese Weise kann ein regulatorisches Umfeld entstehen, das Rechtssicherheit, Wettbewerbsfähigkeit und gesellschaftlichen Fortschritt gleichermaßen gewährleistet.

[2] Für eine tiefergehende Position nutzen Sie bitte den Short Brief for the Implementation Dialogue on the application of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) on 16 July

# Stellungnahme

**Anlage I**

**Vorschläge für eine Anpassung der ePrivacy-Richtlinie**

## 1. Ausgangslage und Problemstellung

Artikel 5(3) der ePrivacy-Richtlinie verlangt eine vorherige Einwilligung für jede Form des Zugriffs auf oder der Speicherung von Informationen in Endgeräten von Nutzer*innen. Die Norm ist technologieoffen und gilt unabhängig davon, ob es sich um Cookies, SDKs, Caches oder andere Speichermechanismen handelt. Das hat drei wesentliche Folgen:

1. **Einwilligungsinflation:** Praktisch jede digitale Dienstleistung muss Einwilligungsbanner implementieren, selbst für geringfügige Vorgänge wie Reichweitenmessung oder Betrugsprävention.
2. **Rechtsunsicherheit:** Der Anwendungsbereich von „Speicherung" und „Zugriff" wird durch Aufsichtsbehörden sehr weit ausgelegt. Nationale Behörden bewerten dieselben Szenarien unterschiedlich, was Fragmentierung und zusätzliche Compliance-Kosten verursacht.
3. **Nutzerunfreundlichkeit:** „Consent Fatigue" führt dazu, dass Einwilligungen pauschal erteilt werden und nicht mehr Ausdruck einer informierten Entscheidung sind.

Damit ist Artikel 5(3) in seiner jetzigen Form nicht zweckgerecht. Er konterkariert die Zielsetzung des Datenschutzrechts, nämlich ein hohes Schutzniveau bei gleichzeitiger Wahrung von Praktikabilität, Rechtsklarheit und Nutzerautonomie.

## 2. Verhältnis zur DSGVO

Die DSGVO sieht einen risikobasierten Ansatz vor. Artikel 5(3) der ePrivacy-Richtlinie steht quer zu diesem System:

- **Formale Doppelprüfung:** Erst ist zwingend eine Einwilligung erforderlich, dann folgt zusätzlich die DSGVO-Prüfung für die weitere Verarbeitung.
- **Fehlende Risikodifferenzierung:** Vorgänge mit sehr geringem Eingriffsrisiko (z. B. Frequenz-Capping, Security oder Measurement) oder die Nutzung von datenschutzfreundlichen Lösungen (PETs) unterliegen denselben Anforderungen wie Profiling.
- **Fragmentierung:** Während die DSGVO auf unionsweite Kohärenz angelegt ist (One-Stop-Shop), gilt dies für die ePrivacy-Richtlinie nicht. Die Folge: unterschiedliche Maßstäbe in verschiedenen Mitgliedstaaten.

## 3. Praktische Herausforderungen für Unternehmen

- **Hohe Implementierungskosten:** Insbesondere KMU tragen erhebliche Lasten durch CMPs, Consent-Management-Systeme und laufende Anpassungen an wechselnde Behördenleitlinien.
- **Rechtliche Instabilität:** Durch unterschiedliche Auslegungen entstehen unklare Compliance-Anforderungen.
- **Markteintrittsbarrieren:** Start-ups und Nischenanbieter haben durch die regulatorische Komplexität erhöhte Markteintrittsbarrieren, selbst in den EU-Ländern.
- **Benachteiligung des europäischen Marktes:** In internationalen Vergleichen wirken die Regeln übermäßig streng, ohne dass ein Gewinn für Nutzer*innen erkennbar wäre

## 4. Vorschläge zur Reform von Artikel 5(3)

Aus Sicht der Digitalen Wirtschaft ist Artikel 5(3) aus der ePrivacy-Richtlinie zu streichen und die gesamte Cookie-bezogene Datenverarbeitung dem modernen, risikobasierten Rahmen der DSGVO zu unterstellen. Dadurch wird eine rechtliche Kohärenz und einen verhältnismäßigen Ansatz gewährleistet.

Sollte Artikel 5(3) beibehalten werden, ist er unbedingt zu reformieren. Es braucht eine Modernisierung der Cookie-Regeln durch Einbeziehung aller Rechtsgrundlagen der DSGVO sowie die Nichtanwendung von Artikel 5(3) in Fällen, in denen die DSGVO bereits die Verarbeitung personenbezogener Daten (Cookies) regelt. Zudem sollte die Speicherung von Informationen oder der Zugriff darauf ohne Einwilligung für ein breiteres Spektrum von risikoarmen und wesentlichen Zwecken nach Rechtsgrundlagen aus Art. 6 DSGVO gestattet werden. Diese Liste der zulässigen risikoarmen Verarbeitungszwecke sollte mindestens umfassen:

- Sicherheit, Cybersecurity und Betrugsprävention
- Reichweitenmessung und First-Party-Analytics
- Frequenzbegrenzung, Ad-Delivery und Billing
- Kontextuelle Werbung
- Speicherung von Opt-outs und Nutzerpräferenzen
- Produktentwicklung
- Profilbildung mit pseudonymen Daten

## 5. Auswirkungen auf Innovation und Markt

Eine vereinfachte, risikobasierte Ausgestaltung würde:

- Investitionen in PETs fördern (da deren Nutzung keine Einwilligungen voraussetzt),
- KMU entlasten (geringere Implementierungskosten, weniger Rechtsunsicherheit),

- Nutzer*innen stärken (Einwilligung nur dort, wo es wirklich zählt),
- Fragmentierung eindämmen (EU-weit einheitliche Definitionen von zulässigen Zwecken).

## 6. Fazit

Artikel 5(3) in seiner heutigen Form ist überholt, unverhältnismäßig und ineffizient. Die Reform muss folgende Ziele erreichen:

1. Einwilligungspflicht auf Vorgänge mit höherem Risiko begrenzen,
2. Klare und unionsweit einheitliche Anwendung für die Verarbeitung mit geringer Eingriffsintensität auf Basis aller Rechtsgrundlagen von Art. 6 DSGVO schaffen,
3. Anreize für Investition in datenschutzfreundliche Technologien (PETs) durch Rechtssicherheit erhöhen,
4. Nutzerfreundlichkeit wiederherstellen und das Konzept der informierten Einwilligung stärken.

Nur mit einer solchen Modernisierung kann die ePrivacy-Richtlinie ihrem Anspruch gerecht werden: Schutz der Privatsphäre, Förderung von Innovation und Stärkung der digitalen Souveränität in Europa.

# Stellungnahme

**Anlage II**

**8. July 2025**
**Philipp Hagen**, Director Legal Affairs & Data Privacy, hagen@bvdw.org

**Short Brief for the Implementation Dialogue on the application of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) on 16 July**

Dear Sir or Madam,
The BVDW would like to focus on two topics. Further simplification/reduction of administrative burden and increasing legal certainty, reducing fragmentation and further harmonising enforcement.

Should the GDPR be reopened through an omnibus instrument, it is imperative that this does not result in a de facto tightening of the regulatory framework but rather delivers genuine simplification and enhanced legal certainty. The BVDW considers the following reform elements indispensable to achieve those objectives.

## 1. Further Simplification and Reduction of Administrative Burden

- Article 5(2) – The accountability requirement must be fundamentally revised, particularly in its linkage to Article 83(5)(a); the current record-keeping obligation imposes disproportionate burdens while providing little demonstrable benefit to data subjects or supervisory authorities.
- Article 15(3) – The notion of a "copy" requires precise definition; access should be restricted where the data subject already possesses the information (mirroring Article 13(4)). Abuse clauses must be introduced, and the burden of showing that a request is manifestly unfounded or excessive should lie with the data subject.
- Pseudonymisation – Pseudonymised data should enjoy a privileged regime with lighter obligations, thereby enabling data-driven innovation while keeping re-identification risks low.
- Codes of conduct and certification – Accelerated procedures and a rebuttable presumption of compliance should be established, giving controllers—especially SMEs—ready-made compliance "toolkits" that materially lower administrative costs.

## 2. Increasing Legal Certainty, Reducing Fragmentation and Harmonising Enforcement

- Article 6 – The Regulation must explicitly confirm the equal standing of all legal bases, eliminating any perceived primacy of consent.
- Article 9 – The regime for special-category data should be thoroughly overhauled—or, failing that, repealed—because it engenders frequent practical deadlocks that disproportionately burden companies and research institutions.

- The European Data Protection Board should be recast as an advisory (WP29-style) body.
- International transfers – The present whitelist (adequacy) model should be replaced by a blacklist system and Article 44(2) repealed. All transfers would be lawful unless the Commission designates a third country as offering inadequate protection, thereby increasing predictability and correctly allocating political responsibility.
- Core definitions and terminology – A clearer definition of "personal data" is required, again granting privileged status to pseudonymisation. Moreover, the GDPR's central legal terms currently appear in up to 21 variations —sometimes synonymous, sometimes hierarchical, occasionally contradictory. Harmonising this terminology would provide users with the semantic precision needed for consistent application across the Union.