Bundesverband E-Commerce und
Versandhandel Deutschland e.V.
www.bevh.org

- Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) -

Stellungnahme zum

Template for Data Protection Impact Assessment ('DPIA')

Berlin, den 09.06.2026

Der **Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)** repräsentiert als die Interessenvertretung der Branche der in Deutschland aktiven Online- und Versandhändler Unternehmen aller Größen und aller denkbaren Handelsformen (Online, Multichannel, Katalog, TV-Shopping, Plattformhändler und -betreiber). Die Mitglieder des bevh stehen für mehr als 75% des gesamten Branchenumsatzes. Darüber hinaus sind dem Verband mehr als 130 Dienstleister aus dem Umfeld der E-Commerce-Branche angeschlossen.

I. Allgemeine Anmerkungen

Wir begrüßen das Ziel des Europäischen Datenschutzausschusses (EDSA), die Einheitlichkeit bei der Durchführung von Datenschutz-Folgenabschätzungen (DSFA) innerhalb der Europäischen Union zu fördern und Verantwortlichen eine Orientierung hinsichtlich des Umfangs und des erforderlichen Detailgrads einer DSFA zu geben. Einheitliche Erwartungen der Aufsichtsbehörden können zur Rechtssicherheit beitragen und die Qualität von DSFA verbessern.

Der vorgelegte Entwurf geht jedoch in wesentlichen Punkten über die Anforderungen der DSGVO hinaus. Zudem enthält das Template zwar zahlreiche Dokumentationsanforderungen, bietet jedoch nur begrenzte praktische Orientierung für die tatsächliche Durchführung einer risikobasierten Bewertung. Insbesondere für kleinere und mittlere Unternehmen fehlen konkrete Hilfestellungen, Anwendungsbeispiele und methodische Leitlinien.

Die Einführung eines europaweit einheitlichen Templates für sämtliche Branchen und Verarbeitungskontexte sehen wir kritisch. DSFA sind nach Art. 35 DSGVO bewusst risikobasiert ausgestaltet und sollen an die jeweilige Verarbeitung angepasst werden können. Ein starrer, für alle Verantwortlichen gleichermaßen geltender Standard birgt die Gefahr, die Aufmerksamkeit von der inhaltlichen Analyse konkreter Risiken auf die formale Vervollständigung eines umfangreichen Dokumentationsschemas zu verlagern. Dies würde den administrativen Aufwand erhöhen, ohne notwendigerweise zu besseren Ergebnissen für den Schutz der betroffenen Personen zu führen.

II. Die Vorlage geht über die Anforderungen von Art. 35 DSGVO hinaus

Die Vorlage verlangt Angaben, die über die gesetzlichen Vorgaben des Art. 35 Abs. 7 DSGVO hinausgehen. Dadurch wird die DSFA faktisch von dem vom Gesetzgeber vorgesehenen risikoorientierten Instrument zu einer Mischung aus Risikobewertung, Compliance-Dokumentation und Best-Practice-Katalog erweitert.

Art. 35 Abs. 7 DSGVO nennt vier Kernelemente einer DSFA:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung,
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie
4. die zur Bewältigung dieser Risiken vorgesehenen Maßnahmen.

Die Vorlage enthält demgegenüber zusätzliche Anforderungen, für die sich keine ausdrückliche Grundlage in Art. 35 DSGVO findet. Hierzu zählen insbesondere:

- die Kennzeichnung des Umsetzungsstatus einzelner Compliance-Maßnahmen in mehreren Unterabschnitten,
- die prinzipienbezogene Zuordnung von Maßnahmen zu sämtlichen Grundsätzen des Art. 5 Abs. 1 DSGVO einschließlich einer Bewertung ihrer Angemessenheit und Wirksamkeit,
- die verpflichtende Unterscheidung zwischen inhärenten Risiken und Restrisiken in einer zweistufigen Risikobewertung.
-

Insbesondere die verpflichtende Dokumentation des Umsetzungsstatus ("geplant", "teilweise umgesetzt", "umgesetzt") bewertet nicht das Risiko für die Rechte und Freiheiten betroffener Personen, sondern den Reifegrad eines Compliance-Management-Systems. Dies liegt außerhalb des Regelungszwecks des Art. 35 DSGVO.
Darüber hinaus werden an verschiedenen Stellen Anforderungen aus nicht bindenden Leitlinien des EDPB, des EDPS oder anderen Soft-Law-Instrumenten in das Template integriert, ohne diese klar von den gesetzlichen Mindestanforderungen abzugrenzen. Für Verantwortliche entsteht dadurch der Eindruck, dass sämtliche Elemente zwingende Bestandteile einer DSFA seien.
Wir regen daher an, klar zwischen den gesetzlichen Mindestanforderungen nach Art. 35 Abs. 7 DSGVO und zusätzlichen Empfehlungen oder Best Practices zu unterscheiden. Sofern das Template künftig als Referenzmaßstab für die Bewertung der Angemessenheit einer DSFA dienen soll, sollte es sich auf die gesetzlichen Anforderungen beschränken oder fakultative Elemente ausdrücklich als solche kennzeichnen.

III. Verhältnismäßigkeit und Praxistauglichkeit wahren

Auch dort, wo die Vorlage Themen behandelt, die grundsätzlich von Art. 35 Abs. 7 DSGVO erfasst sind, verlangt sie ein Maß an Detailtiefe, das in keinem angemessenen Verhältnis zum Zweck einer DSFA steht.

Der vorgeschriebene Detaillierungsgrad führt dazu, dass Verantwortliche umfangreiche Dokumentationen erstellen müssen, deren Mehrwert für die eigentliche Risikobewertung begrenzt erscheint. Dies betrifft insbesondere die detaillierte Zuordnung von Maßnahmen zu Datenschutzgrundsätzen, die Nachverfolgung von Umsetzungsständen, die Dokumentation unterstützender Ressourcen oder die formalisierte Bewertung verschiedener Risikostufen.
Für kleinere und mittlere Unternehmen ohne spezialisierte Datenschutzabteilungen oder dedizierte Governance-Tools stellt dies eine erhebliche Belastung dar. Aber auch größere Unternehmen mit komplexen Lieferketten, Cloud-Infrastrukturen oder arbeitsteiligen Organisationsstrukturen werden erhebliche Ressourcen auf die Dokumentation verwenden müssen.
Die Gefahr besteht, dass Verantwortliche künftig entweder unverhältnismäßig viel Zeit in die Erstellung formaler Dokumentation investieren oder aber primär darauf abzielen, sämtliche Felder des Templates auszufüllen, ohne dass dadurch die Qualität der eigentlichen Risikobewertung verbessert wird. Beides läuft dem Zweck einer DSFA zuwider.

Fehlende Risikoorientierung des Templates
Das Template verfolgt den Anspruch, die für eine DSFA erforderlichen Informationen vollständig, zeitsparend und fehlerfrei zusammenzuführen. Diesen Anspruch erfüllt es jedoch nur eingeschränkt.
Statt die Risikobetrachtung in den Mittelpunkt zu stellen, orientiert sich die Struktur weitgehend an Compliance-Anforderungen und Dokumentationspflichten. Aus Sicht der Praxis wäre eine risikoorientierte Struktur hilfreicher.
Eine solche Struktur könnte beispielsweise zwischen:

- Risiken aus der beabsichtigten Verarbeitung (z. B. Überwachungsdruck, Profilbildung, Manipulation, Bewertungswirkungen, Transparenzdefizite) und
- Risiken aus unbeabsichtigten Ereignissen (z. B. Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit)

unterscheiden.

Anschließend könnten die jeweiligen Schutzmaßnahmen unmittelbar den relevanten Risikokategorien z.B. Überwachungsdruck wird reduziert durch Pseudonymisierung, Maskierung von Daten und kurze Speicherfristen) zugeordnet werden. Dies würde die eigentliche Funktion der DSFA – die Bewertung und Reduzierung konkreter Risiken – deutlich besser unterstützen.

Fehlende Praxisbeispiele

Der Leitfaden erläutert zwar, welche Informationen einzutragen sind. Es fehlen jedoch konkrete Mustereinträge oder ausgefüllte Beispiel-DSFA.
Insbesondere für weniger erfahrene Anwender wären vollständig ausgefüllte Muster – beispielsweise für einen typischen Personal- oder Kundenprozess – eine erhebliche praktische Unterstützung. Aufgrund der unterschiedlichen Branchen und Verarbeitungskontexte halten wir es für sinnvoll, mehrere Muster für unterschiedliche Verarbeitungskontexte zur Verfügung zu stellen.

Fehlende Hinweise zur Beteiligung Betroffener
Art. 35 Abs. 9 DSGVO sieht vor, dass die Ansichten der betroffenen Personen oder ihrer Vertreter eingeholt werden, sofern dies angemessen ist.
Das Template fragt entsprechende Informationen ab, enthält jedoch keine Hinweise dazu, wie diese Anforderung praktisch umgesetzt werden kann. Eine Orientierung anhand typischer Beispiele – etwa Mitarbeiterbefragungen, Einbindung von Betriebsräten, Fokusgruppen oder Nutzerbefragungen – wäre hilfreich.

IV. Eine Einheitslösung passt nicht für alle – die Vorlage muss eine Anpassung an den Einzelfall ermöglichen

Die Vorlage geht von einer einheitlichen Struktur und einem einheitlichen Detaillierungsgrad aus, unabhängig von Art, Umfang, Kontext oder Risiko der jeweiligen Verarbeitung.
Dies steht im Spannungsverhältnis zum risikobasierten Ansatz des Art. 35 DSGVO. Eine DSFA sollte stets verhältnismäßig sein und die konkreten Umstände der jeweiligen Verarbeitung berücksichtigen.
Ein groß angelegtes KI-System mit umfangreicher Profilbildung und der Verarbeitung besonderer Kategorien personenbezogener Daten sollte nicht denselben Dokumentationsanforderungen unterliegen wie ein internes Mitarbeiterverzeichnis oder eine begrenzte Geschäftsanwendung.
Zudem enthält die Vorlage Abschnitte, die für zahlreiche Verarbeitungsvorgänge nicht relevant sind. So verlangt Abschnitt 2.3.b die Dokumentation von Schutzmaßnahmen im Zusammenhang mit automatisierten Entscheidungen gemäß Art. 22 DSGVO, unabhängig davon, ob solche Entscheidungen überhaupt stattfinden.
Darüber hinaus reduziert die stark strukturierte Tabellenlogik komplexe rechtliche und tatsächliche Abwägungsprozesse auf einzelne Felder und Einträge. Der eigentliche Mehrwert einer DSFA liegt jedoch gerade in der kontextbezogenen Bewertung und Gewichtung verschiedener Interessen und Risiken.

Wir regen daher an, die Vorlage flexibler auszugestalten. Nicht einschlägige Abschnitte sollten ausdrücklich als optional gekennzeichnet werden. Zudem sollte den Verantwortlichen mehr Raum für erläuternde Freitextdarstellungen eingeräumt werden.

Schließlich sollte die Vorlage anerkennen, dass Art. 35 DSGVO keine bestimmte Dokumentationsform vorgibt. Verantwortliche sollten weiterhin die Möglichkeit haben, die Risikobewertung in bestehende Compliance- und Governance-Strukturen zu integrieren.

V. Die Vorlage vermischt die Risikobewertung mit der allgemeinen Compliance-Dokumentation

Die Vorlage behandelt die DSFA teilweise als umfassendes Compliance-Instrument und verlangt die Wiederholung von Informationen, die bereits an anderer Stelle innerhalb des Datenschutz-Managementsystems dokumentiert werden.
Dies betrifft insbesondere Informationen, die typischerweise:

- im Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO,
- in Vereinbarungen zur Auftragsverarbeitung nach Art. 28 DSGVO,
- in Zertifizierungen nach Art. 42 DSGVO oder
- in Verhaltenskodizes nach Art. 40 DSGVO

abgebildet werden.

Die DSFA dient der Bewertung von Risiken für die Rechte und Freiheiten betroffener Personen. Sie ist weder ein vollständiges Verzeichnis der Verarbeitung noch ein umfassendes Compliance-Audit. Besonders deutlich wird dies in Abschnitt 2.3, der umfangreiche Nachweise zur Einhaltung der Datenschutzgrundsätze, zu Betroffenenrechten, zu Auftragsverarbeitern, zu Übermittlungen und zu technischen und organisatorischen Maßnahmen verlangt.

Abschnitt 0: Unklare Festlegung des Bewertungsgegenstands der DSFA
Die Vorlage knüpft die DSFA faktisch an einzelne „Verarbeitungstätigkeiten“ („processing activities“) und geht damit von einer 1:1-Beziehung zwischen Verarbeitungstätigkeit und DSFA aus. Art. 35 DSGVO stellt hingegen auf „Verarbeitungsvorgänge“ („processing operations“) ab und sieht ausdrücklich vor, dass eine einzige DSFA mehrere ähnliche Verarbeitungsvorgänge mit vergleichbaren Risiken erfassen kann.

Die vom EDSA gewählte Verknüpfung kann zwar in vielen Fällen praktikabel sein, da sich Risiken häufig an Verarbeitungszwecken und Geschäftsprozessen orientieren. Sie sollte jedoch nicht als zwingendes Modell vorgegeben werden. Die starre Kopplung einer DSFA an eine einzelne Verarbeitungstätigkeit schränkt den vom Gesetzgeber bewusst eröffneten Spielraum ein und kann zu unnötigem Dokumentationsaufwand führen.
Wir regen daher an, klarzustellen, dass das Template auch für die gemeinsame Bewertung mehrerer ähnlicher Verarbeitungsvorgänge genutzt werden kann und Verantwortliche den Zuschnitt einer DSFA weiterhin risikobasiert festlegen dürfen.

Abschnitt 1: zu detaillierte Reihe von Unterkategorien

Abschnitt 1 unterteilt die Beschreibung der Verarbeitung in eine unnötig detaillierte Reihe von Unterkategorien (Kategorien personenbezogener Daten, Zwecke, Vorgänge, Umfang, Kontext, funktionale Beschreibung, Datenlebenszyklus, technische Mittel, unterstützende Ressourcen) – was eher einer RoP-Struktur entspricht als den Anforderungen von Art. 35 Abs. 7 DSGVO Buchstabe a an eine „systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke".

Abschnitt 2.2.b: Datenqualitätskennzahlen pro Datenkategorie

Abschnitt 2.2.b geht über die rechtlichen Vorgaben einer DSFA hinaus, da hier die Angabe von Datenqualitätskennzahlen pro Datenkategorie verlangt wird – ein operatives Data-Governance-Anliegen, das für die meisten Verarbeitungsaktivitäten nichts mit der Risikobewertung zu tun hat.

Abschnitt 2.3: Rechenschaftspflicht und Umsetzungsstatus

Der Abschnitt 2.3 verlangt die Dokumentation von Compliance-Maßnahmen in Bezug auf die Grundsätze des Art. 5 DSGVO, die Rechte der betroffenen Personen, die Pflichten des Auftragsverarbeiters/der Übermittler, den Datenschutz durch Technikgestaltung und die Sicherheit – jeweils mit einer Erörterung der Angemessenheit und Wirksamkeit. Dies ist eine Dokumentation der Rechenschaftspflicht, keine Risikobewertung.

Die in Abschnitt 2.3 vorgeschriebene Kennzeichnung des Umsetzungsstatus (Geplant / Teilweise umgesetzt / Umgesetzt) ist eine Funktion zur Bewertung der Compliance-Reife – sie gibt Auskunft darüber, ob eine Maßnahme umgesetzt wurde, nicht aber darüber, ob die Verarbeitung ein inakzeptables Risiko für die betroffenen Personen darstellt.

Abschnitte 1.3 und Abschnitt 2.3: Besonderheiten cloudbasierter Infrastrukturen

Die Anforderungen benachteiligen zudem Verantwortliche, die moderne Cloud-Infrastrukturen nutzen.

Abschnitt 1.3 und Abschnitt 2.3 setzen voraus, dass detaillierte Informationen zu Servern, Rechenzentren, Speichermedien und Sicherheitsmaßnahmen dokumentiert werden. In cloudbasierten Umgebungen werden diese Funktionen jedoch typischerweise von spezialisierten Anbietern erbracht.

Die Vorlage sollte daher ausdrücklich anerkennen, dass Zertifizierungen, Auditberichte, vertragliche Verpflichtungen und sonstige Nachweise von Cloud-Anbietern als geeignete Nachweise berücksichtigt werden können.

Abschnitte 3.2 und 3.3: Notwendigkeit und Verhältnismäßigkeit

Die Abschnitte 3.2 und 3.3 verlangen umfangreiche Begründungen zur Notwendigkeit und Verhältnismäßigkeit der Verarbeitung.

Hierbei handelt es sich um komplexe rechtliche Bewertungsfragen. Das Template verweist zwar auf verschiedene Hilfsmaterialien, enthält jedoch keine konkreten Prüffragen oder methodischen Hilfestellungen.

Aus unserer Sicht sollte zudem die Prüfung von Notwendigkeit und Verhältnismäßigkeit nicht isoliert erfolgen, sondern als Bestandteil einer integrierten rechtlichen Würdigung der jeweiligen Verarbeitung.

Abschnitt 4.1.2: Risikobewertungsmethodik
Positiv hervorzuheben ist, dass der EDSA keine bestimmte Risikobewertungsmethodik vorschreibt. Gleichzeitig führt dies in der Praxis zu Unsicherheiten hinsichtlich der anzuwendenden Bewertungsmaßstäbe. Zusätzliche Orientierungshilfen oder optionale Musteransätze oder ein konkreter Methodenvorschlag (z. B. wie bei der CNIL PIA-Methodik) könnten hier die Vergleichbarkeit verbessern, ohne die notwendige Flexibilität einzuschränken.

Abschnitt 4.2.c: Maßnahmenpläne und Governance-Anforderungen
Abschnitt 4.2.c verlangt einen detaillierten Maßnahmenplan einschließlich Zuständigkeiten, Zeitplänen und Überwachungsmechanismen. Art. 35 Abs. 7 Buchstabe d verlangt „die zur Bewältigung der Risiken vorgesehenen Maßnahmen“, nicht einen Projektmanagementplan.

Abschnitt 5: Einbindung des Datenschutzbeauftragten (DSB)
Art. 35 Abs. 7 lit. d DSGVO verlangt hingegen lediglich die Darstellung der vorgesehenen Maßnahmen zur Risikominimierung. Die operative Umsetzung und Überwachung erfolgt in der Regel bereits über bestehende Governance- und Compliance-Prozesse.
Auch die vorgesehene Genehmigung jeder DSFA durch ein Mitglied der Unternehmensleitung geht über die gesetzlichen Anforderungen hinaus. Dies kann erhebliche organisatorische Reibungsverluste verursachen, ohne die Qualität der Risikobewertung zu verbessern.
Ebenso sollte auf eine Differenzierung zwischen Maßnahmen verzichtet werden, die aufgrund einer Empfehlung des Datenschutzbeauftragten ergriffen wurden, und solchen, die der Verantwortliche eigenständig vorgesehen hat. Eine solche Unterscheidung ist gesetzlich nicht vorgesehen und birgt Konfliktpotenzial.

VI. Die Vorlage verpasst die Gelegenheit, sich an überlappende Rechtsrahmen anzupassen

Schließlich berücksichtigt die Vorlage nicht ausreichend die zunehmende Überschneidung zwischen DSFA nach Art. 35 DSGVO und anderen regulatorischen Bewertungsverfahren.
Besonders relevant ist hierbei die Folgenabschätzung für Grundrechte nach Art. 27 KI-Verordnung für Betreiber von Hochrisiko-KI-Systemen.

Beide Instrumente verfolgen ähnliche Ziele, verlangen vergleichbare Informationen und befassen sich mit ähnlichen Risiken für die Grundrechte betroffener Personen.
Vor diesem Hintergrund wäre es wünschenswert, die Kompatibilität beider Verfahren stärker zu fördern und Doppelarbeit zu vermeiden. Die Vorlage könnte hierzu zumindest klarstellen, inwieweit Informationen aus einer DSFA für die Erfüllung von Verpflichtungen nach dem AI Act genutzt werden können.

Gerade vor dem Hintergrund der europäischen Bemühungen um regulatorische Vereinfachung stellt die fehlende Abstimmung mit benachbarten Rechtsrahmen eine verpasste Gelegenheit dar. Eine stärkere Harmonisierung würde sowohl die Rechtssicherheit erhöhen als auch die praktische Umsetzung für Verantwortliche erleichtern, ohne das Datenschutzniveau zu beeinträchtigen.