

Leitlinie 1/2026 nach DADG

„Personenbezug“

zur Unterstützung der Bundesnetzagentur gemäß § 3 Absatz 2 Satz 2 DADG
bei der Feststellung,

ob ihre **Kapitel II DA (Datenweitergabe B2C oder B2B)**
betreffende Entscheidung oder sonstige Handlung gemäß § 3 Absatz 4 DADG,

die **Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten**
durch die/den BfDI
und damit deren oder dessen Beteiligung im Verfahren erfordert.

Version 1.0 vom 12. Oktober 2026

Inhaltsverzeichnis

A)	Einleitung	3
I.	Zur rechtlichen Einordnung	3
II.	Zur inhaltlichen Gliederung	4
B)	Formale Prüfung	5
I.	Beteiligung – verfahrensimmanente Indikatoren	5
II.	Keine Beteiligung – fehlende Entscheidungserheblichkeit	5
1.	Fallgruppe – Entscheidungsgegenstand ohne Bezug zur Rechtmäßigkeit einer Verarbeitung personenbezogener Daten	5
2.	Fallgruppe – Entscheidung oder Verfahrensbeendigung ohne Betroffenheit einer datenschutzrechtlichen Frage	6
C)	Materielle Prüfung	6
I.	Beteiligung – Personenbezug	7
1.	Konstellation: Nutzer ist natürliche Person	7
2.	Konstellation: Nutzer ist juristische Person	8
II.	Keine Beteiligung – kein Personenbezug	9
1.	Kein Personenbezug für Dateninhaber	9
a)	Konstellation: Nutzer ist anonym	9
b)	Konstellation: Nutzer ist juristische Person ohne weitere Zuordnungsmöglichkeit	9
2.	Kein Personenbezug für Nutzer und ggf. Dritten	10
D)	Konsultation der/des BfDI	11

A) Einleitung

Die vorliegende Leitlinie dient der Unterstützung der Bundesnetzagentur (BNetzA) im Rahmen ihrer Tätigkeiten als für die Verordnung (EU) 2023/2854 (Datenverordnung, englisch Data Act – im Folgenden „DA“) zuständige Aufsichtsbehörde.

Die Leitlinie bietet eine Hilfestellung bei der initial von der BNetzA vorzunehmenden Prüfung, ob eine Entscheidung oder sonstige Handlung der BNetzA bezüglich Datenweitergaben nach Kapitel II DA von Unternehmen an Verbraucher (B2C) und zwischen Unternehmen (B2B) die Prüfung und Bewertung des Datenschutzrechts durch die/den BfDI und damit deren oder dessen Beteiligung erfordert. Die Beteiligung der/des BfDI erfolgt entweder im Rahmen eines „verzahnten Verfahrens“ oder im „vereinfachten Verfahren“, siehe [Dokument zur Zusammenarbeit BNetzA und BfDI](#). Tragender Gedanke der Leitlinie ist, für die BNetzA und die BfDI die Verfahrensführung zu erleichtern, um zugunsten der Beteiligten und im Sinne der Rechtsklarheit möglichst effizient und zügig zu verfahrensabschließenden Entscheidungen zu gelangen.

Um die Verwaltungsverfahren möglichst effizient und transparent zu gestalten, wird die Leitlinie fortlaufend unter Berücksichtigung auftretender Praxisfälle ergänzt sowie an aktuelle nationale und internationale Entscheidungen im Datenschutzrecht angepasst.

I. Zur rechtlichen Einordnung

Die Regelungen des Kapitel II DA sehen vor, dass

- vernetzte Produkte und verbundene Dienste den direkten Zugang zu Produkt- und verbundenen Dienstdaten durch den Nutzer¹ ermöglichen (Artikel 3 Absatz 1 DA),
- Dateninhaber² auf Verlangen des Nutzers ohne Weiteres verfügbare Daten aus vernetzten Produkten und verbundenen Diensten bereitstellen (Artikel 4 Absatz 1 DA) und dass
- Dateninhaber auf Verlangen des Nutzers ohne Weiteres verfügbare Daten aus vernetzten Produkten und verbundenen Diensten Dritten³ weitergeben (Artikel 5 Absatz 1 DA).

Die Begriffe des Nutzers und des Dateninhabers sind im Data Act definiert:

- Nutzer im Sinne des Artikel 2 Nummer 12 DA ist eine natürliche oder juristische Person, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundene Dienste in Anspruch nimmt.

¹ Der in Artikel 2 Nummer 12 DA legaldefinierte Begriff des Nutzers schließt natürliche oder juristische Personen jeglichen Geschlechts ein.

² Der in Artikel 2 Nummer 13 DA legaldefinierte Begriff des Dateninhabers schließt natürliche oder juristische Personen jeglichen Geschlechts ein.

³ Dritte fallen unter den in Artikel 2 Nummer 14 DA legaldefinierten Begriff des Datenempfängers und schließen natürliche Personen jeglichen Geschlechts und juristische Personen ein.

- Dateninhaber im Sinne des Artikel 2 Nummer 13 DA ist eine natürliche oder juristische Person, die nach Data Act, nach geltendem Unionsrecht oder nach nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts berechtigt oder verpflichtet ist, Daten – soweit vertraglich vereinbart, auch Produktdaten oder verbundene Dienstdaten - zu nutzen und bereitzustellen, die sie während der Erbringung eines verbundenen Dienstes abgerufen oder generiert hat.

Das Gesetz zur Anwendung und Durchsetzung der Datenverordnung (Datenverordnung-Anwendungs-und-Durchsetzungs-Gesetz – DADG) regelt Zuständigkeiten und Verfahren. § 2 Absatz 1 DADG benennt die BNetzA als die nach Artikel 37 Absatz 1 DA zuständige Behörde für die Anwendung und Durchsetzung des DA. § 3 Absatz 1 DADG weist die Zuständigkeit für die Überwachung der Anwendung des DA bezüglich des Schutzes personenbezogener Daten nach Art. 37 Abs. 3 DA der/dem BfDI zu.

Die Zusammenarbeit von BNetzA und BfDI wird wie folgt adressiert:

- § 3 Absatz 2 Satz 1 DADG regelt eine kooperative und vertrauensvolle Zusammenarbeit und § 3 Absatz 2 Satz 2 DADG sieht vor, dass die/der BfDI die BNetzA in Fragen des Datenschutzes unterstützt
- § 3 Absatz 4 DADG fordert, dass die BNetzA die/den BfDI beteiligt, wenn ihre Entscheidung oder sonstige Handlung die Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten erfordert, weil eine Verarbeitung personenbezogener Daten Gegenstand des Verfahrens ist.

II. Zur inhaltlichen Gliederung

Zu Beginn der Prüfung, ob eine Entscheidung eine datenschutzrechtliche Bewertung der Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten betrifft, steht die Frage, ob verfahrensimmanente Indikatoren eine Beteiligung erfordern ([Abschnitt B I](#)) und, falls das nicht der Fall ist, ob Datenschutzaspekte im konkreten Fall nicht entscheidungserheblich sind ([Abschnitt B II](#)). Im Fall nicht gegebener Entscheidungserheblichkeit ist eine Beteiligung der /des BfDI nicht erforderlich.

Im Folgenden beschreibt die Leitlinie abstrakt Konstellationen, in denen die BNetzA grundsätzlich annehmen kann, dass personenbezogene Daten betroffen sind und ihre Entscheidung oder sonstige Handlung eine Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten und damit die Beteiligung der/des BfDI erfordert ([Abschnitt C I](#)) sowie Konstellationen, in denen sie das grundsätzlich nicht annehmen und folglich auf die Beteiligung verzichten kann ([Abschnitt C II](#)). Diese Prüfung ist für Fälle erforderlich, wenn kein Fall nach Abschnitt C I oder C II vorliegt.

Kann die BNetzA einen Sachverhalt nicht anhand dieser Leitlinie beurteilen, konsultiert die BNetzA die/den BfDI, damit sie oder er im Rahmen der vorgesehenen Unterstützung prüfen kann, ob Datenschutz betroffen ist ([Abschnitt D](#)).

B) Formale Prüfung

Eine datenschutzrechtliche Prüfung und Bewertung ist grundsätzlich erforderlich, wenn dem (Verwaltungs-)Verfahren immanente Indikatoren einen Bezug zu personenbezogenen Daten herstellen ([Abschnitt I](#)). Nicht erforderlich ist eine solche Prüfung, wenn das Datenschutzrecht nicht entscheidungserheblich ist ([Abschnitt II](#)).

I. Beteiligung – verfahrensimmanente Indikatoren

In folgenden Konstellationen kann von der Erforderlichkeit einer Beteiligung der/des BfDI ausgegangen werden:

- Ein Dateninhaber lehnt einen Anspruch auf Datenbereitstellung oder -weitergabe unter Berufung auf entgegenstehende Datenschutzrechte dritter Personen, also anderer als den Nutzer, (teilweise) ab.
- Im Fall einer Beschwerde beruft sich die/der Beschwerdeführer:in (zum Beispiel Nutzer oder Dritter) als betroffene Person auf eigene konkrete Datenschutzrechte.

II. Keine Beteiligung – fehlende Entscheidungserheblichkeit

Die folgenden Fallgruppen 1 und 2 betreffen Fälle, in denen das Datenschutzrecht nicht entscheidungserheblich und deswegen eine Beteiligung der/des BfDI nicht erforderlich ist.

1. Fallgruppe – Entscheidungsgegenstand ohne Bezug zur Rechtmäßigkeit einer Verarbeitung personenbezogener Daten

Der Gegenstand des Verfahrens betrifft Vorgaben nach dem Data Act, deren Erfüllung von der Rechtmäßigkeit einer Verarbeitung personenbezogener Daten unabhängig ist und die Entscheidung der BNetzA setzt keine datenschutzrechtliche Bewertung voraus. Das betrifft insbesondere:

- Informations- und Transparenzpflichten (z. B. Artikel 3 Absatz 2 und 3 DA – vorvertragliche Informationen; Artikel 26 DA – Informationen bei Vertragsschluss über Datenverarbeitungsdienste; Artikel 28 DA – Informationspflichten; Artikel 31 Absatz 3 DA – Unterrichtung des Kunden);
- technische, format- und schnittstellenbezogene Fragen der Umsetzung von Pflichten zur Datenweitergabe nach Kapitel II DA (z. B. Fragen das „wie“ der Bereitstellung betreffend), soweit nicht technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten betroffen sind (Artikel 25 und 32 DSGVO);
- Handlungen des Nutzers entgegen Artikel 4 Absatz 11 DA;
- Handlungen Dritter entgegen Artikel 5 Absatz 5 DA;
- Vorgaben zu Vertragsbedingungen und zum Verbot missbräuchlicher Vertragsklauseln (Kapitel IV; Artikel 25 DA – Wechsel zwischen Datenverarbeitungsdiensten);

- technische, format- und schnittstellenbezogene Pflichten bei Kapitel VI DA (z. B. Artikel 30 DA – Schnittstellen und Datenexport beim Wechsel);
- die Einhaltung von Fristen, Form- und Mitteilungspflichten.

2. Fallgruppe – Entscheidung oder Verfahrensbeendigung ohne Betroffenheit einer datenschutzrechtlichen Frage

Das Verfahren wird aus Gründen abgeschlossen, die keine datenschutzrechtliche Bewertung erfordern, insbesondere:

- Handlung/Entscheidung der BNetzA, ohne dass eine datenschutzrechtliche Frage entschieden werden muss (z.B. Ablehnung eines Zugangsverlangens auf Grundlage anderer rechtlicher Erwägungen wie Geheimnisschutz);
- Rücknahme der Beschwerde oder anderweitige Erledigung.



Hinweis

Nicht von der 2. Fallgruppe umfasst sind Fälle, in denen die Handlung der BNetzA die Zulässigkeit einer Verarbeitung personenbezogener Daten voraussetzt. Das ist zum Beispiel der Fall, wenn die BNetzA einen Datenzugang oder eine Datenbereitstellung anordnet und die streitgegenständlichen Daten personenbezogen sind oder sein könnten.

Exemplarisch: Der vom Hersteller eines vernetzten Produkts angebotene Datenzugang (u.a. Umfang, Qualität) entspricht aus Sicht des Nutzers nicht den Vorgaben des Data Act, beispielsweise gemäß Artikel 4. Der Hersteller begründet die eingeschränkte Datenbereitstellung mit Sicherheitsanforderungen. Ein Nutzer legt daraufhin Beschwerde ein und fordert die Herausgabe der Daten in einem bestimmten Umfang und in einem bestimmten Format. Lehnt die BNetzA diese Beschwerde als unbegründet ab, weil sie die Wertung des Herstellers stützt, beteiligt sie die/den BfDI unter Zugrundelegung der Wertung in dieser Leitlinie mangels Entscheidungserheblichkeit nicht. Ebenso erfolgt keine Beteiligung der/des BfDI, sofern die Entscheidung der BNetzA ausschließlich technische, format- und schnittstellenbezogene Fragen betreffend das "wie" der Datenbereitstellung beinhaltet und nicht technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten betroffen sind (Artikel 25 und 32 DSGVO; siehe oben 1. Fallgruppe). Eine Beteiligung der/des BfDI muss aber etwa stattfinden, wenn sich der Hersteller auf Datenschutz als weiteren Grund für die eingeschränkte Datenbereitstellung beruft oder die BNetzA den Hersteller zur Bereitstellung der Daten verpflichten möchte, die auch personenbezogene Daten einschließen. Denn dann bedarf es für die Bereitstellung der Daten einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO.

C) Materielle Prüfung

Kann der Sachverhalt nicht schon im Rahmen der formalen Prüfung unter [Abschnitt B](#) eindeutig einer Fallkonstellation bzw. -gruppe zugeordnet werden, muss geprüft werden, ob im Rahmen der Weitergabe von Daten im Sinne des Kapitel II DA personenbezogene Daten verarbeitet werden (dann Beteiligung, siehe [Abschnitt I](#)) oder nicht (dann keine Beteiligung, siehe Abschnitt II).

I. Beteiligung – Personenbezug

Eine Verarbeitung personenbezogener Daten kann jedenfalls angenommen werden, wenn festgestellt werden kann, dass der Dateninhaber die bereitgestellten oder weitergegebenen Daten einer natürlichen Person zuordnet oder zuordnen kann.

1. Konstellation: Nutzer ist natürliche Person



Praxishinweis (a)

Produktdaten und verbundene Dienstdaten können in vielen Fällen als personenbezogene Daten betrachtet werden, da sie sich auf den oder die Nutzer beziehen. Auch wenn die von vernetzten Produkten und verbundenen Diensten erhobenen oder generierten Daten nicht direkt mit einem Namen, sondern mit technischen Aspekten und Merkmalen eines Produktes und Dienstes verknüpft sind, können sie dem Nutzer bzw. den Nutzern zugeordnet werden. Solche technischen Daten werden von natürlichen Personen erzeugt und können ihre direkte oder indirekte Identifizierung durch die Person, die für die Verarbeitung der Daten verantwortlich ist, ermöglichen.

Ein Nutzer,

- der Daten generiert oder von dem Daten erhoben werden,
- ist für den Dateninhaber erkennbar eine natürliche Person und identifizierbar,
 - o wenn der Dateninhaber den Nutzer unmittelbar identifizieren kann,



Praxishinweis (b)

Der Dateninhaber ist zum Beispiel in der Lage, einen Nutzer unmittelbar zu identifizieren, wenn ein nutzerbezogener Account verwendet wird oder der Dateninhaber mit dem Nutzer einen Kauf-, Miet- oder Leasingvertrag für ein vernetztes Produkt abgeschlossen hat.

oder

- o wenn die Daten aus sich heraus Rückschlüsse auf eine identifizierte oder identifizierbare Person zulassen,



Praxishinweis (c)

Eine Identifizierbarkeit kann sich durch Aussondern („Singling Out“) i.S.d. Erwägungsgrund 26 Satz 3 DSGVO ergeben. Beispiel: Die Stromverbrauchsdaten von Smart Home-Geräten können ein individuelles Nutzungsmuster abbilden. Selbst wenn die Daten nur unter einer Geräte-ID laufen, können sie wie ein digitaler Fußabdruck wirken. Man kann einen Nutzer gegenüber anderen aussondern, da niemand sonst exakt dieses Nutzungsmuster hat.

oder

- o wenn der die Daten verlangende Nutzer in den Fällen der Art. 4 und 5 DA eine natürliche Person ist und der Dateninhaber die Daten dieser betroffenen Person zuordnet, um dem Verlangen auf Datenbereitstellung bzw. -weitergabe zu entsprechen,

oder

- o wenn der Dateninhaber über andere Mittel verfügt, die eine Identifizierung des Nutzers ermöglichen.

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren (EG 26 S. 3 DSGVO).

**Praxishinweis (d)**

(Andere) Mittel zur Bestimmung betroffener Personen können in den Händen des Verantwortlichen oder Dritter liegen und insbesondere Zusatzwissen oder rechtliche Ansprüche zur Erlangung von Zusatzinformationen sein.

Damit liegt etwa ein Personenbezug vor, wenn zwar die Produkt- oder Dienstdaten selbst keinen Aufschluss über betroffene Personen geben, der Dateninhaber aber Zusatzwissen hat, über das er individuelle Nutzungsmuster ableiten kann. Es geht also insbesondere um die Zusammenführung verschiedener Informationen mit der Folge, dass eine Identifizierung möglich wird. Beispiel: Ein Hersteller smarter Kassensysteme vertreibt zugleich Videoüberwachungssysteme für den Einzelhandel und wertet die Daten auf eigenen Servern aus. Sind Kameras auf die Kassen gerichtet, können mit einer Zusammenführung der Daten einzelne Kund:innen ausgesondert werden.

Ebenso liegt etwa Personenbezug etwa vor, wenn der Dateninhaber einen rechtlichen Anspruch gegen einen Dritten zur Erlangung von Informationen hat, die ihm eine Identifizierung betroffener Personen ermöglichen. Beispiel: Ein Hauseigentümer (Nutzer) aktiviert in der App der Herstellerin seiner vernetzten Wärmepumpe eine dort angebotene Anwendung eines Drittanbieters zur Effizienzsteigerung. Der Drittanbieter erhält über die Hersteller-API ausschließlich Geräte-ID, Sensor- und Nutzungsdaten. Identifikationsdaten des Nutzers verbleiben bei der Herstellerin und eine direkte Kommunikation zwischen Nutzer und Drittanbieter existiert nicht. Der nach Art. 8 Abs. 1 DA erforderliche Datenbereitstellungsvertrag enthält eine Klausel, wonach der Drittanbieter von der Herstellerin die Identifikationsdaten für Sicherheits-, Haftungs-, oder Streitbeilegungszwecke (Art. 10 DA) verlangen kann. Der Drittanbieter hat damit einen rechtlichen Anspruch auf Informationen, die ihm eine Identifizierung des Nutzers ermöglichen.

2. Konstellation: Nutzer ist juristische Person

Ein Nutzer,

- der Daten generiert oder von dem Daten erhoben werden,
- ist eine juristische Person, die einer natürlichen Person die tatsächliche Nutzung zuweist oder überlässt (sog. „betroffene Person“, die Daten generiert; unter den Voraussetzungen des Artikel 2 Nummer 12 DA auch als nachgelagerter Nutzer)

und

- der Dateninhaber kann die natürliche Person identifizieren; dabei kann die Zuordnung der Daten zu einer natürlichen Person beispielsweise auf einer Kennung oder einem eigenen Nutzungskonto basieren oder auf Singling Out.

 **Siehe zu Singling Out Praxishinweis (c)**

II. Keine Beteiligung – kein Personenbezug

Eine datenschutzrechtliche Prüfung und Bewertung ist nicht erforderlich, wenn festgestellt werden kann, dass die nach Kapitel II DA weitergegebenen Daten keine personenbezogenen Daten sind.

Für die Verarbeitung im Rahmen der Datenweitergabe nach Kapitel II DA kann ein Personenbezug jedenfalls dann ausgeschlossen werden, wenn keine der an einer Weitergabe beteiligten Parteien aus sich heraus oder durch Zusammenführung mit Informationen der beteiligten Parteien oder Dritter einen Personenbezug herstellen kann (also kumulativ nicht der Dateninhaber ([Abschnitt I](#)), nicht der Nutzer und in den Fällen des Artikel 5 Absatz 1 DA nicht der Dritte ([Abschnitt II](#)).

1. Kein Personenbezug für Dateninhaber

Die Daten sind für den Dateninhaber unter folgenden (kumulativen) Voraussetzungen grundsätzlich keine personenbezogenen Daten:

a) Konstellation: Nutzer ist anonym

Der Dateninhaber kann keinen Nutzer identifizieren; das ist der Fall,

- wenn das Produkt / der Dienst ohne Nutzerkonto oder –kennung genutzt wird und
- wenn die Daten nicht aus sich heraus Rückschlüsse auf eine identifizierte oder identifizierbare Person zulassen

 Praxishinweis (e)

Daten geben beispielsweise keinen Aufschluss über individuelle Personen, wenn sie ausschließlich sachbezogen sind (wie Wetterdaten oder Angaben über die Bodenbeschaffenheit) oder genügend viele natürliche Personen das Produkt / den Dienst nutzen, sodass keine individuellen Nutzungsmuster ausgemacht werden können. Ein weiteres Beispiel sind Maschinendaten vollautomatisierter und unbemannter Produktionsanlagen.

und

- wenn der Dateninhaber über keine (anderen) Mittel verfügt, die eine Identifizierung betroffener Personen ermöglichen.

 **Siehe zu (anderen) Mitteln Praxishinweis (d)**

b) Konstellation: Nutzer ist juristische Person ohne weitere Zuordnungsmöglichkeit

Der vom Dateninhaber identifizierte Nutzer ist erkennbar eine juristische Person

 **Praxishinweis (f)**

Eine juristische Person kann dem Dateninhaber beispielsweise bekannt sein, weil sie dessen Vertragspartnerin eines Kauf-, Miet- oder Leasingvertrages für ein vernetztes Produkt ist.

und

- o Nutzerkonto- oder -kennung bezieht sich ausschließlich auf eine juristische Person

oder

- o die Nutzung erfolgt durch ein einheitliches nutzerunabhängiges Konto / einen einheitlichen Weg ohne Differenzierung nach verschiedenen Nutzern



Praxishinweis (g)

Beispielsweise wird eine vernetzte Industriemaschine mit einem Account der Fabrik benutzt, auf den alle Mitarbeiter:innen zugreifen können.

oder

- o das Produkt / der Dienst wird ohne Nutzerkonto oder -kennung genutzt

und

- die Daten lassen für den Dateninhaber nicht aus sich heraus Rückschlüsse auf eine identifizierte oder identifizierbare Person zu



Siehe Praxishinweis (e)

und

- der Dateninhaber verfügt über keine anderen Mittel, die eine Identifizierung betroffener Personen ermöglichen



Siehe zu anderen Mitteln Praxishinweis (d)

2. Kein Personenbezug für Nutzer und ggf. Dritten

Wenn die Daten für den Dateninhaber nicht personenbezogen sind, muss weiter geprüft werden, ob sie für den Nutzer und ggf. Dritten personenbezogen sind.

Die Daten sind für den Nutzer und in den Fällen des Artikel 5 Absatz 1 DA für den Dritten grundsätzlich unter folgenden (kumulativen) Voraussetzungen keine personenbezogenen Daten:

- Die Daten lassen nicht aus sich heraus Rückschlüsse auf eine identifizierte oder identifizierbare Person zu



Praxishinweis (h)

Zusätzlich zu den in **Praxishinweis (e)** genannten Fällen kann eine Identifizierbarkeit beispielsweise ausgeschlossen sein, weil die Kennungen oder Accountzuordnungen von der Datenweitergabe vom Dateninhaber an den Nutzer oder Dritten ausgeschlossen sind.

und

- der Nutzer und ggf. der Dritte verfügt über keine (anderen) Mittel, die eine Identifizierung betroffener Personen ermöglichen.



Praxishinweis (i)

Entsprechend **Praxishinweis (d)** muss eine Identifizierbarkeit angenommen werden, wenn zwar die Produkt- oder Dienstdaten selbst keinen Aufschluss über betroffene Personen geben, der Nutzer und/oder ggf. Dritter aber Zusatzwissen hat/haben, über das sie individuelle Nutzungsmuster ableiten können. Beispiel: Der Nutzer oder Dritte erhält reine Maschinendaten, die aus sich heraus keinen Aufschluss über natürliche Personen geben, die die Maschine bedienen. Nutzer oder Dritter haben aber etwa Schicht- oder Arbeitspläne oder aber Videokameraaufnahmen der Produktionsfläche, die die Maschine und ihre Bediener:innen zeigen, sodass individuelle Nutzungsmuster durch Zusammenführung der Daten ausgemacht werden können.

D) Konsultation der/des BfDI

Kann weder festgestellt werden, dass eine Beteiligung der/des BfDI erforderlich ist ([Abschnitt B I](#) und [Abschnitt C I](#)), noch, dass eine Beteiligung nicht erforderlich ist ([Abschnitt B II](#) und [Abschnitt C II](#)), konsultiert die BNetzA die/den BfDI, damit sie oder er im Rahmen der vorgesehenen Unterstützung prüfen kann, ob Datenschutz betroffen ist.

Die Konsultation gewährleistet, dass die gemäß § 3 Absatz 3 DADG erforderliche Beteiligung der/des BfDI erfolgt, wenn eine Entscheidung oder sonstige Handlung der BNetzA die Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten erfordert.