Datenschutz-Grundverordnung VO (EU) 2016/679, Bundesdatenschutzgesetz: DS-GVO / BDSG

Gola / Heckmann / Rost

4. Auflage 2026
ISBN 978-3-406-83135-5
C.H.BECK

C.H.BECK und Franz Vahlen.
beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

bleibt. Für die Stellen, denen ein Entpixeln nicht möglich ist, sind die Daten anonymisiert.

Mittels **kryptographischer Verfahren** können alle Informationen, die in Textform dargestellt werden können (also alle digitalen Dateien wie Texte, Bilder oder Tonaufnahmen), **unleserlich gemacht werden.** Dementsprechend sind **verschlüsselte Daten** für diejenigen pseudonym, die keinen Zugang zu dem gesondert geführten Schlüssel haben.[122] Auch das Bilden von Hash-Werten ist eine Form der Pseudonymisierung.[123] **56**

Die einer Pseudonymisierung unterzogenen personenbezogenen Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, behalten für diejenigen, die Zugang zu diesen Informationen bekommen können, ihren **Personenbezug** (Erwgr. 26). Ansonsten liegt der Tatbestand anonymisierter Daten vor. Insoweit können Daten für die einen „nur" pseudonyme und für andere anonyme sein.[124] Um festzustellen, ob Pseudonymisierung oder Anonymisierung vorliegt, dh, ob eine natürliche Person identifizierbar ist, sind alle Mittel in Betracht zu ziehen, die von dem **Verantwortlichen** oder einer **anderen Person** (→ Rn. 9) nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Hierbei sind alle objektiven Faktoren heranzuziehen, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (Erwgr. 26 S. 2 und 3), mag auch ein Restrisiko verbleiben. Somit hängt die Frage der Anonymität immer auch vom Verarbeitungskontext ab.[125] **57**

3. Aufhebung des Personenbezugs (Anonymisierung). Zu trennen sind pseudonymisierte Daten von **anonymen Informationen**. Die DS-GVO definiert den Begriff nicht. Erwgr. 26 S. 5 erläutert ihn dahin gehend, dass es um Informationen geht, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Auch wenn die Verordnung den Vorgang der **Anonymisierung** nicht beschreibt, gilt nach dem zuvor Gesagten die in § 3 Abs. 6 BDSG aF enthaltene Definition weiterhin. Das Anonymisieren von Daten kann dadurch geschehen, dass die Daten **„verändert"** werden, indem sie aus einem Bestand personenbezogener Daten ohne Personenbezug und ohne Rückführbarmöglichkeit per entsprechender Auswertung herausgefiltert und zB für planerische oder statistische Zwecke[126] oder auch zum Testen und Trainieren von **künstlicher Intelligenz**[127] genutzt werden, wobei jedenfalls die nachfolgende **58**

[122] Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Mühlenbeck DS-GVO Art. 4 Rn. 96.

[123] Simitis/Hornung/Spiecker gen. Döhmann/Hansen DS-GVO Art. 4 Rn. 39; vgl. auch VGH München Beschl. v. 26.9.2018 – 5 CS 18.1157, ZD 2019, 43.

[124] Roßnagel ZD 2018, 243 (245), Gierschmann ZD 2021, 483; siehe hierzu nun auch EuGH Urt. v. 4.9.2025 – C-413/23 P, ECLI:EU:C:2025:645 – EDSB/SRB; pointiert: „Schrödingers Daten" Schemmel ZD-Aktuell 2025, 01404.

[125] Gierschmann ZD 2021, 482.

[126] Vgl. zur Personenbeziehbarkeit und Möglichkeit der Re-Identifikation bei statistischen Daten BVerwG Urt. v. 29.8.2019 – 7 C 33.17, NVwZ 2020, 1114 Rn. 25.

[127] Roßnagel/Geminn ZD 2021, 487.

Nutzung oder Verarbeitung mangels Personenbeziehbarkeit der Daten nicht mehr den Regeln der Verordnung unterliegt. Im Zusammenhang von KI-Systemen sind sog. **synthetische Daten** von Relevanz. Hierbei handelt es sich um anonymisierte Daten, die ihren Personenbezug verloren haben, jedoch weiterhin die gleichen statistischen Merkmale aufweisen und so für KI-Training geeignet sind.[128]

59 Eine **Re-Identifizierung** anonymisierter Daten – die besonders bei Gesundheitsdaten zu besorgen ist[129] – stellt einen Personenbezug wieder her. Ob eine den Anwendungsbereich der DS-GVO ausschließende Anonymisierung nur eine **absolute Anonymisierung** ohne Möglichkeit der Re-Identifizierung sein kann, ist bisher nicht geklärt. Angesichts der dynamischen Entwicklung der Technik im Bereich der Big-Data-Analyse mittels Maschine Learning kann Anonymisierung technisch gar nicht absolut gelingen. Es spricht daher vieles dafür, den **relativen** Ansatz (→ Rn. 21) auch auf die Anforderungen an eine Anonymisierung anzuwenden.[130]

60 Ob auch das eigentliche **Anonymisieren,** dh das Ausfiltern der keinen Personenbezug aufweisenden Daten aus einer personenbezogene Daten enthaltenden Datei, eine Verarbeitung nach Art. 4 Nr. 2 ist,[131] wurde bisher unterschiedlich beantwortet und ua auch von Aufsichtsbehörden verneint.[132] Gleichwohl muss das Anonymisieren als Verändern oder als eine sonstige Art der „Verwendung" von Daten verstanden werden, das einer Erlaubnis bedarf, um von dem **Gebot der Zweckbindung** nach Art. 5 Abs. 1 lit. b abzuweichen: Die Erlaubnis liegt vor, wenn nach Art. 6 Abs. 4 der Sekundärzweck mit dem Primärzweck vereinbar ist, wobei dann die Unterrichtungspflichten gem. Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 infrage stehen. Daneben wird auch auf Art. 6 Abs. 1 lit. f[133] als Erlaubnisnorm zurückgegriffen, wobei hier bei der Erhebung auf diese Zweckbestimmung hätte hingewiesen worden müssen. Auch Art. 6 Abs. 1 lit. c[134] iVm dem die Löschung gestattenden Art. 17 Abs. 1 lit. a[135] wird herangezogen. So soll das Anonymisieren mit einem **Löschen** gleichgesetzt werden können, wenn das Ergebnis vergleichbare geringe Risiken der De-Identifikation aufweist.[136] Schließlich bedarf es besonderer Argumentation, um die anonyme Auswertung besonderer Arten personenbezogener Daten, die nach Art. 9 Abs. 1 lit. a regelmäßig der Einwilligung bedarf, zu rechtfertigen.[137]

61 Die Gewinnung der anonymen Daten kann dadurch geschehen, dass der Personenbezug insgesamt durch **Löschung der Identifikationsmerkmale** entfällt, wobei die DS-GVO hinsichtlich der **Löschung**, nicht jedoch hinsichtlich der weiteren nicht mehr personenbezogenen Verarbeitung Anwendung findet. Sie

---

[128] Raji DuD 2021, 303 (305); Paal ZfDR 2024, 129 (139).

[129] Appenzeller/Orak DuD 2024, 277 ff.

[130] So auch Schwartmann/Jaspers/Lepperhoff/Weiss RDV 2023, 40 (41); Stummer DuD 2023, 354 (358); BeckOK DatenschutzR/Schild Rn. 15a.

[131] So ua Hornung/Wagner ZD 2020, 223; Roßnagel ZD 2021, 188.

[132] Zum derzeitigen Meinungsstand ausf. Gierschmann ZD 2021, 482 (484).

[133] Vgl. Roßnagel/Geminn ZD 2021, 487 mwN.

[134] Hierzu ausf. Gierschmann ZD 2021, 482 (484).

[135] Stürmer ZD 2020, 626 (630); gegen eine Gleichsetzung von Anonymisieren und Löschen ua Roßnagel ZD 2021, 188.

[136] So Gierschmann ZD 2021, 482 (485).

[137] Vgl. bei Hornung/Wagner ZD 2020, 223 (228).

kann durch das Ausfiltern der Daten ohne Personenbezug geschehen. Auch hierbei handelt es sich um einen Verarbeitungsschritt.[138]

Werden **Daten ohne Personenbezug** erhoben und gespeichert, so findet die Verordnung mangels Verarbeitung und Nutzung personenbezogener Daten von vornherein keine Anwendung. **62**

4. Gesetzlicher Auftrag zur Pseudonymisierung. Die Verordnung gibt Verantwortlichen und Auftragsverarbeitern zumindest einen allgemeinen Auftrag zur **Minimierung von Risiken** (Erwgr. 28) für die betroffene Person, die Pseudonymisierung der Daten in die Erwägungen über die Gestaltung einer Datenverarbeitung mit einzubeziehen, wobei deutlich gemacht wird, dass durch die ausdrückliche Einführung der „Pseudonymisierung" in dieser Verordnung nicht beabsichtigt sei, andere Datenschutzmaßnahmen auszuschließen (Erwgr. 26). Eine Privilegierung pseudonymisierter Daten sieht die DS-GVO nicht vor. Es gibt jedoch Anreize dafür.[139] Um einem Verantwortlichen einerseits die „Risikominimierung" durch pseudonymisierte Verarbeitungen zu ermöglichen, ihm andererseits jedoch die Möglichkeit allgemeiner Analysen der Datenbestände nicht zu nehmen, gestattet Erwgr. 29 derartige Verarbeitungen, wenn die erforderlichen technischen und organisatorischen Maßnahmen getroffen wurden, um – für die jeweilige Verarbeitung – die Umsetzung dieser Verordnung zu gewährleisten. **63**

VI. „Dateisystem" (Nr. 6)

1. Datensammlung. Die Speicherung der personenbezogenen Daten in einem **Dateisystem** ist Mindestvoraussetzung für die Anwendung der Verordnung bei **manueller Verarbeitung.** Der Begriff findet ausschließlich in Art. 2 Verwendung (→ Art. 2 Rn. 12). Unter einem solchen Dateisystem versteht Art. 4 Nr. 6 jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zwecks leichter Wiederauffindbarkeit und Auswertungsmöglichkeit zugänglich ist,[140] unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geführt wird. **64**

Eine **Sammlung von Daten** liegt vor, wenn Daten, die zueinander in einem inneren Zusammenhang stehen, auf einem oder auf mehreren zusammengehörenden Datenträgern gespeichert sind. Erforderlich ist ein **gleichartiger Aufbau,** der einen leichten Zugriff auf die Daten ermöglicht. Abgestellt wird auf die Auswertbarkeit der Sammlung nach bestimmten Kriterien, dh die den gesammelten Daten gemeinsamen, den aufgezeigten Sinnzusammenhang herstellenden personenbezogenen **Merkmalen.**[141] Als Zugangskriterien sind nur solche anzusehen, die für eine sinnvolle Ordnung der Datei notwendig sind. Dazu zählen sowohl die **„Anschrift"** als auch der die Anschrift ausmachende Wohnort, die Straße und Hausnummer; es ist also auch möglich, die Datei nach diesen Einzelmerkmalen zu ordnen bzw. auszuwerten. Dennoch bildet das Merkmal „Anschrift" ein einziges Merkmal, sofern die Datei nach der Anschrift geordnet oder ausgewertet wird. Soll die Datei hingegen eine Unterscheidung innerhalb **65**

[138] Zu Datenlöschung und Anonymisierung Roßnagel ZD 2021, 188.

[139] Siehe hierzu bei Kühling/Buchner/Klar/Kühling DS-GVO Art. 4 Rn. 13 f.

[140] EuGH Urt. v. 10.7.2018 – C-25/17, ECLI:EU:C:2018:551 = ZD 2018, 469 – Zeugen Jehovas mAnm Hoeren; EuGH Urt. v. 7.3.2024 – C-740/22, ECLI:EU:C:2024:216 = NVwZ 2024, 653 Rn. 37 – Endemol Shine Finland mAnm Gerhold/Lauenstein.

[141] BeckOK DatenschutzR/Schild Rn. 84.

der Anschrift ermöglichen (zB Suchmerkmal: alle Bewohner der X-Straße), dann bilden die Bestandteile der Anschrift selbstständige Kriterien.

66 In der Sammlung brauchen nicht Daten von mehreren Personen enthalten zu sein. Auch wenn über eine **Einzelperson** mehrere Daten gespeichert werden, liegt eine Sammlung personenbezogener Daten vor. Eine Untergrenze enthält das Gesetz nicht, sodass bereits zwei an den Betroffenen gerichtete und in einer Textverarbeitungsanlage **abgespeicherte Briefe** den Tatbestand der automatisierten Datei erfüllen. Auch eine einen einzelnen Beschäftigten betreffende **Gehaltsliste** erfüllt insoweit den Dateibegriff.[142]

67 **Bild- und Tonträger** können Gegenstand automatisierter Verarbeitung oder Inhalt einer strukturierten Datei sein, sofern die aufgezeichneten Personen bekannt oder zumindest identifizierbar sind.

68 Nach Erwgr. 15 S. 3 fallen **Akten oder Aktensammlungen,** wenn sie nicht nach bestimmten Kriterien geordnet und auswertbar sind, nicht in den Anwendungsbereich der DS-GVO:[143] Werden derartige Datenbestände **digitalisiert**, kommt die DS-GVO zur Anwendung, wenn die Vorgänge nicht nur eingescannt, sondern auch nach bestimmten Kriterien abrufbar bzw. auswertbar gemacht werden.

69 **2. Auswertungsmöglichkeiten.** Die Sammlung bzw. die in ihr enthaltenen Daten müssen nach bestimmten, dh zumindest zwei Kriterien zugänglich sein. Da zwei ermöglichende Merkmale für eine Sortierung oder Auswertung genügen, können an sich auch **Akten** oder **Aktensammlungen** hierunter fallen, wenn sie unter den Begriff der nichtautomatisierten Datei subsumierbar sind, so zB wenn sie nach Aktenzeichen geordnet und nach der Betreffsangabe bzw. dem Namen umgeordnet werden können. Akten und Aktensammlungen sowie die Deckblätter dazu fallen nur dann nicht unter den Dateibegriff, wenn ihr Inhalt nicht in der Art einer Datei strukturiert ist.

70 Dementsprechend sind Prüfungsarbeiten in einem „Dateisystem" gespeichert, wenn sie zwei Kriterien haben, nämlich den persönlichen Teil der Kennziffer als Pseudonym und das Jahr, in dem die Arbeiten angefertigt worden sind,[144] und unterliegen damit der Auskunftspflicht.

VII. „Verantwortlicher" (Nr. 7)

71 **1. Allgemeines. Normadressat** der Verordnung ist nach Art. 4 Nr. 7 die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Werden personenbezogene Daten im Bereich einer juristischen Person verarbeitet, ist grundsätzlich die juristische Person als **Rechtsträger der betroffenen Einrichtung** oder des betroffenen Unternehmens Verantwortlicher und nicht die jeweils handelnde natürliche Person.[145] Die DSRL machte den gleichlautend definierten Begriff mit der Bezeichnung als

---

[142] BlnDSB, Materialien zum Datenschutz Nr. 30, § 7.

[143] Zu Akten der Sozialverwaltung BSG Urt. v. 14.5.2020 – B 14 AS 7/19 R, ZD 2021, 101.

[144] BVerwG Urt. v. 30.11.2022 – 6 C 10.21, NVwZ 2023, 346 Rn. 20.

[145] EDSA, Leitlinien 07/2020, Version 2.0, Rn. 17 f.; aA OLG Dresden Urt. v. 30.11.2021 – 4 U 1158/21, ZD 2022, 159 Rn. 5.

„für die Verarbeitung Verantwortlichen“[146] noch deutlicher, während das BDSG aF den Begriff der „verantwortlichen Stelle“ (§ 3 Abs. 7 BDSG aF) verwendete, ohne den Aspekt der Möglichkeit der Kooperation mehrerer Verantwortlicher anzusprechen. Letztlich bleibt es auch nach der DS-GVO bei der verantwortlichen Stelle, der „Verantwortliche“ handelt nicht nur durch den Betriebsinhaber selbst, sondern durch alle ihm entscheidungsbefugt Zuarbeitenden.[147]

Beginnend mit der Google-Spain-Entscheidung[148] betont der EuGH immer wieder, dass der Begriff der Verantwortlichkeit weit auszulegen sei.[149] Das galt zwar für die DSRL, kann aber auch für Art. 4 Nr. 7 wohl erwartet werden.[150] Verantwortlicher kann auch eine **Einzelperson** sein, dies aber nur bei eigenständigem wirtschaftlichem Handeln. Ungeklärt ist bisher, ob auch beim sog. **Mitarbeiterexzess** eine Verantwortlichkeit iSv Art. 4 Nr. 7 vorliegen kann. Der Generalanwalt Campos Sánchez-Bordona hat diese Möglichkeit angedeutet.[151] Während die Rechtsprechung[152] bisher zur Anerkennung tendiert, ist die Literatur gespalten.[153] Richtig ist es, dass der handelnde Mitarbeiter für die von ihm vorgenommene Verarbeitung sowohl Zweck als auch Mittel bestimmt und daher Verantwortlicher iSd Art. 4 Nr. 7 ist.[154] **72**

2. Umfang der Verantwortlichkeit. Seine Ausgestaltung erfährt der Begriff des Verantwortlichen in Art. 24. Er hat im Rahmen eines risikobasierten Ansatzes einzustehen für die Sicherstellung der zulässigen Datenverarbeitung durch den Einsatz von technischen und organisatorischen Maßnahmen (→ Art. 24 Rn. 1 ff.), die regelmäßigen Überprüfungen unterliegen. Dabei gilt das Verhältnismäßigkeitsprinzip. **73**

Der in Art. 24 für die Umsetzung der Verordnung insgesamt zum Maßstab gemachte **risikobasierte Ansatz** soll es ermöglichen, die Pflichten des Verantwortlichen entsprechend dem im Vorfeld zu ermittelnden Risiko der von ihnen vorgenommenen Datenverarbeitung anzupassen. Die Pflicht zur Vornahme einer solchen Risikoprüfung ergibt sich für den Verantwortlichen direkt aus Art. 24 Abs. 1. In vielen weiteren Artikeln der DS-GVO wird zudem für spezielle Pflichten oder auch für eine Ausnahme von gesetzlichen Verpflichtungen eine Risikoprüfung sowohl von dem Verantwortlichen als auch von dem Auftragsverarbeiter (Art. 30 Abs. 5) und auch dem **Datenschutzbeauftragten** (Art. 39 Abs. 2) verlangt. **74**

3. Gemeinsam für die Verarbeitung Verantwortliche. Die DS-GVO gibt verarbeitenden Stellen die Möglichkeit, in **gemeinsamer Verantwortung** eine **75**

---

[146] Monreal ZD 2014, 428.

[147] Schantz/Wolff Neues DatenschutzR/Schantz Rn. 359 ff.

[148] EuGH Urt. v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317 = NJW 2014, 2257 – Google Spain.

[149] Zuletzt EuGH Urt. v. 4.10.2024 – C-200/23, ECLI:EU:C:2024:827 = ZD 2025, 87 Rn. 72 – Agentsia po vpisvaniyata; EuGH Urt. v. 11.1.2024 – C-231/22, ECLI:EU:C:2024:7 = ZD 2024, 274 Rn. 28 – Belgischer Staat.

[150] Abl. Kühling/Buchner/Hornung DS-GVO Art. 26 Rn. 42 ff.; Lee/Cross MMR 2019, 559.

[151] GA Campos Sánchez-Bordona, Schlussantrag v. 15.12.2022 – C-579/21 Rn. 65.

[152] Zuletzt OLG Stuttgart Beschl. v. 25.2.2025 – 2 ORbs 16 Ss 336/24, ZD 2025, 405; bezugnehmend auf ÖBVwG Erkenntnis v. 21.12.2021 – W258 2238615-1/16E, ZD 2022, 439.

[153] Für einen umfassenden Überblick zur Lit. siehe Dieterle ZD 2025, 405 (406).

[154] So überzeugend Reif RDV 2024, 286 (288); aA Dieterle ZD 2020, 135 (137 f.).

Verarbeitung zu betreiben. Einzelheiten der hierzu zu vereinbarenden Kooperation regelt Art. 26. Nach Art. 26 Abs. 1 S. 1 sind zwei oder mehr Verantwortliche dann gemeinsam verantwortlich, wenn sie die Zwecke und Mittel der Verarbeitung gemeinsam festlegen. Entsprechende Regelungen haben die Landesdatenschutzgesetze (vgl. zB § 58 Abs. 2 HDSIG). Fehlt eine förmliche Vereinbarung der gemeinsamen Verantwortlichen über die Zwecke und Mittel der Verarbeitung, hebt das die gemeinsame Verantwortlichkeit nicht auf.[155]

76 Eine gemeinsame Verantwortlichkeit ist danach nicht gegeben, wenn zwei Verantwortliche gemeinsam etwa nur die Mittel festlegen, also zB gemeinsam ein Rechenzentrum betreiben (Erwgr. 79). Gleiches gilt, wenn die Zusammenarbeit sich als Auftragsdatenverarbeitung darstellt.[156] Jeder der gemeinsamen Verantwortlichen muss die Voraussetzungen des Art. 4 Nr. 7 für sich erfüllen.[157]

77 In der Vereinbarung ist insbesondere festzulegen, welcher der beteiligten Verantwortlichen für die Wahrnehmung der **Rechte der betroffenen Personen** zuständig ist.

78 Die Mitgliedstaaten dürfen die gesetzlichen Verantwortlichkeiten der kooperierenden Verantwortlichen regeln. Sie können Aufgaben der Verantwortlichen einer bestimmten Person zuweisen und damit die diesbezüglichen Dispositionsbefugnisse ausschließen. Die **Öffnungsklausel** umfasst alle Aufgaben, die Verantwortliche nach der Verordnung treffen und nicht nur die Informationspflichten nach Art. 13 und 14.[158]

79 Auch sog. Verbundverfahren, also wenn mehrere Stellen speicherberechtigt sind, oder gemeinsame Abrufverfahren[159] sind unter den Vorgaben des Art. 26 zu betrachten. Solche „gemeinsam nutzbaren Datenverarbeitungsverfahren" werden zB bei konzernverbundenen Unternehmen zum Zweck der zentralisierten Bearbeitung bestimmter Vorgänge (zB Postein- und -ausgang, Inkasso) betrieben. Für das Versicherungsgewerbe findet sich eine Regelung in Art. 9 Abs. 1 CoC.

80 **4. Gesetzliche Regelung des Verantwortlichen.** Sind die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können dort auch der Verantwortliche bzw. die bestimmten Kriterien seiner Benennung vorgesehen werden. Der Mitgliedstaat kann sowohl konkrete Verantwortliche bestimmen als auch Kriterien für deren Bestimmung festlegen. Voraussetzung ist jedoch, dass die Verordnung derartige **Öffnungsklauseln** für die Bestimmung der Zwecke und Mittel der Verarbeitung vorgibt, die etwa in Art. 6 Abs. 1 S. 1 lit. c oder e iVm Art. 6 Abs. 3 gefunden werden können.[160]

81 **5. Einordnung des Betriebsrats.** Die Definition des Verantwortlichen gab Anlass, auch die Einordnung des **Betriebsrats** zu überdenken.[161] Nach überwiegender Ansicht wurde dieser auch unter der DS-GVO gleichwohl nicht als Dritter

[155] EuGH Urt. v. 5.12.2023 – C-683/21, ECLI:EU:C:2023:949 = ZD 2024, 209 Rn. 43 f. – Nacionalinis visuomenes sveikatos centras.

[156] Zur diesbzgl. Situation bei Arbeitnehmerüberlassungen vgl. Schuster RDV 2021, 141.

[157] EuGH Urt. v. 7.3.2024 – C-604/22, ECLI:EU:C:2024:214 = ZD 2024, 328 Rn. 58 – IAB Europe.

[158] Kühling/Martini DS-GVO S. 6.

[159] Vgl. Gola/Schomerus, 12. Aufl. 2015, BDSG § 10 Rn. 9 f.

[160] Kühling/Martini DS-GVO S. 26.

[161] Kort ZD 2017, 319 (322); Möhle, Die datenschutzrechtliche Verantwortlichkeit des Betriebsrats, 2022.

und damit eigenständiger Verantwortlicher, sondern als **Teil der verantwortlichen Stelle** und demgemäß als interner Empfänger bzw. Nutzer der ihm vom Arbeitgeber zugeleiteten Personaldaten angesehen.[162] Gleichwohl gab es auch fundierte gegenläufige Stimmen[163] und zumindest eine abweichende Regelung für Personalvertretungen in Thüringen.[164]

Der Bundesgesetzgeber hat zur Beendigung dieser bislang offenen Fragen schließlich eine nach der Gesetzesbegründung „klarstellende" gesetzliche Regelung in dem als Bestandteil eines **Betriebsrätemodernisierungsgesetzes**[165] in Kraft getretenen § 79a BetrVG[166] für den Betriebsrat getroffen und gleichermaßen für den Personalrat in § 69 des 2021 grundlegend novellierten BPersVG[167] entsprechend beschlossen.[168] **82**

Festgeschrieben wird unter Nutzung der Regelungsbefugnis des Art. 4 Nr. 7 Hs. 2 DS-DVO, dass für Datenverarbeitungen des Betriebsrats der Arbeitgeber der für die Verarbeitung Verantwortliche – und damit der **betriebliche DSB** auch insoweit Kontrollorgan – im Sinne der datenschutzrechtlichen Vorschriften ist.[169] Die vormals vom BAG verneinte[170] bzw. offengelassene[171] Kontrollbefugnis des **betrieblichen Datenschutzbeauftragten** gegenüber dem Betriebsrat ist damit – wenn auch mit Einschränkungen – zwar positiv entschieden (§ 79a S. 2 BetrVG); andererseits steht die datenschutzrechtliche Verantwortlichkeit des Arbeitgebers in Konflikt mit der **innerorganisatorischen Selbstständigkeit** und Weisungsfreiheit des Betriebsrats. So entscheidet der Betriebsrat innerhalb seines Zuständigkeitsbereichs eigenverantwortlich über die Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit iSd Art. 24 und 32. Hier bedarf es der Kooperation und gegenseitiger Unterstützung.[172] **83**

Um den fortbestehenden Konflikt zwischen der Eigenverantwortung der Mitarbeitervertretung, datenschutzrechtlicher Verantwortlichkeit des Arbeitgebers und den Betroffenenrechten der Mitarbeiter zu beheben, bietet es sich an, unternehmensintern die Verantwortung des Vertretungsorgans für bestimmte Vorgaben des Datenschutzrechts festzulegen (zB mit Blick auf die Betroffenenrechte oder das Verarbeitungsverzeichnis) oder Prozesse zu etablieren, die eine hinreichende Kooperation bei der Umsetzung der DS-GVO gewährleisten. Entsprechende Regelungen sollten im Interesse klarer Verfahrensabläufe in einer **Betriebsvereinbarung**[173] abgesichert werden. **84**

Hinsichtlich der Zulässigkeit des Personaldatenflusses vom Arbeitgeber zum Betriebsrat und der **vom Betriebsrat durchgeführten Datenverarbeitungen** ergab sich dadurch keine Änderung der Rechtssituation, da diese nach § 26 Abs. 1 **85**

---

[162] Gola/Schomerus, 12. Aufl. 2015, BDSG § 3 Rn. 49; so Kühling/Buchner/Hartung DS-GVO Rn. 11 unter Anwendung der DS-GVO.
[163] Vgl. Brink/Joos NZA 2019, 1395; Kort ZD 2017, 319.
[164] Siehe Gola RDV 2021, 181.
[165] BGBl. 2021 I 1762.
[166] Vgl. Gola RDV 2021, 181; krit. Brink/Joos RDV 2021, 116.
[167] BGBl. 2021 I 1614.
[168] Baden PersR 6/2021, 16.
[169] Gesetzesbegründung, BT-Drs. 19/29819, 17.
[170] BAG Beschl. v. 11.11.1997 – 1 ABR 21/97, NJW 1998, 2466.
[171] BAG Beschl. v. 9.4.2019 – 1 ABR 51/17, NZA 2019, 1055.
[172] Gola RDV 2021, 181 (182).
[173] Gola RDV 2021, 181 (183).

S. 1 Zulässigkeitsalt. 2 BDSG entweder durch das BetrVG oder das BDSG gestattet sein müssen.[174]

86 Das **BPersVG**[175] enthält eine der Regelung des § 79a BetrVG in etwa entsprechende, jedoch im Detail noch weniger aussagekräftige Bestimmung in § 69 BPersVG. Geregelt wird zunächst die Selbstverständlichkeit, dass der Personalrat bei der Verarbeitung personenbezogener Daten die Vorschriften über den Datenschutz einzuhalten hat. Soweit der Personalrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, wird sodann die Dienststelle als der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften festgelegt, was aber nichts daran ändert, dass die „Datenverarbeitungshoheit" bei der Mitarbeitervertretung liegt. Abgeschlossen wird die Norm durch ein **gegenseitiges Unterstützungsgebot** bei der Einhaltung der datenschutzrechtlichen Vorschriften.

87 **6. Betriebliche und behördliche Datenschutzbeauftragte.** Nicht eindeutig gesetzlich geklärt ist hingegen weiterhin, ob und gegebenenfalls mit welchen Funktionen ein **interner Datenschutzbeauftragter „Verantwortlicher"** für die von ihm vorgenommen Datenverarbeitungen sein kann. Einiges spricht dafür, dass dies jedenfalls zutrifft, wenn er in der Funktion des **„Anwalts von Betroffenen"** tätig wird, da hier der Verantwortliche selbst keinen Datenzugang hat, da ihm die Informationen über die Beschäftigten nicht nur aus Geheimhaltungsgründen, sondern auch prozessual vorzuenthalten sind. Literatur[176] und wohl einhellig die Aufsichtsbehörden sehen das anders. Dementsprechend stellt der Sächsische Datenschutzbeauftragte[177] ohne nähere Argumentation wie folgt fest: „Den internen Datenschutzbeauftragten behandelt meine Behörde als einen dem Verantwortlichen zuzuordnenden Funktionsträger, auch wenn dieser weisungsfrei agiert und einem Berufsgeheimnisträger gleichgestellt wird. Im Falle von in Rede stehenden Geheimhaltungspflichten müsse der interne Datenschutzbeauftragte aber selbst auskunftserfüllend tätig werden."

88 Anders zu beurteilen sind aber eigene Datenverarbeitungen des gewerblich tätigen – externen – Datenschutzbeauftragten.[178]

89 **7. Betriebsärzte.** Auch für **interne Betriebsärzte,** die unabhängig und der Schweigepflicht unterliegend im Betrieb arbeiten, wird – sofern das Thema problematisiert wird – die **Stellung als Verantwortlicher** iSd Art. 4 Nr. 7 verneint.[179] Betriebsärzte seien funktionale Stellen innerhalb des Verantwortlichen. Dies gelte auch, wenn die Betriebsärzte als Berufsgeheimnisträger agieren. Zwar unterliegen sie einer besonderen Geheimhaltungspflicht, die dazu führt, dass sie innerhalb der datenverarbeitenden Stelle **informationell abgeschottet** agieren und innerhalb ihres geheimhaltungspflichtigen Wirkungsbereichs auch fachlich-inhaltlich keiner

---

[174] Vgl. zur damaligen Rechtslage Gola/Schomerus, 12. Aufl. 2015, BDSG § 32 Rn. 37 f.; vgl. Gola/Pötters RDV 2017, 111.

[175] Vgl. zur Übersicht Baden PersR 6/2021, 16.

[176] Kühling/Buchner/Hartung DS-GVO Art. 4 Rn. 11; Simitis/Hornung/Spiecker gen. Döhmann/Drewes DS-GVO Art. 39 Rn. 27 f.

[177] SächsLfD, TB 2020, Abschn. 8.

[178] Jedoch → BDSG § 5 Rn. 3.

[179] Schuler/Weichert, Die Datenverarbeitung des Betriebsarztes Hinweise zum datenschutzgerechten Umgang mit Patientendaten durch Betriebsärzte und betriebsärztliche Dienste, Stand 22.9.2020 Version 1.0.