Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO X

Voraussetzungen der Datenschutz-Folgenabschätzung

INHALT

Voraussetzungen der Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) soll gem. Art. 35 DS-GVO eine umfassende Risikobewertung von Datenverarbeitungsvorgängen ermöglichen. Sie ersetzt die bisherige Vorabkontrolle nach § 4d Abs. 5 BDSG a.F., wobei beide Instrumente nicht in allen Teilen vollständig deckungsgleich sind.

Enthalten sind nach Art. 35 Abs. 7 DS-GVO zumindest folgende Aspekte:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen (lit. a);
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck (lit. b);
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 (lit. c) und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und bechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird (lit d).

Die vorliegende Praxishilfe widmet sich zunächst der vorgelagerten Frage, unter welchen Voraussetzungen und zu welchem Zeitpunkt eine DSFA durchzuführen ist.

1. Voraussetzungen der DSFA

1.1 Tatbestand

Schon nach dem BDSG war es erforderlich, in bestimmten Fällen eine Vorabkontrolle durchzuführen, nämlich dann, wenn sich aus der automatisierten Verarbeitung personenbezogener Daten besondere Risiken für die Betroffenen ergeben (§ 4d Abs. 5 BDSG a.F.).

Im alten BDSG war von „besonderen Risiken“ die Rede, Art. 35 Abs. 1 DS-GVO knüpft an ein „hohes Risiko“ an. Beide Begrifflichkeiten sind nicht notwendigerweise deckungsgleich.

Als Beispiele nennt das BDSG die Verarbeitung besonderer Arten personenbezogener Daten sowie die Verarbeitung personenbezogener Daten zur Bewertung einer Person. Ähnlich formuliert es Art. 35 DS-GVO, ohne jedoch ausdrücklich zu definieren, wann eine Verarbeitung ein hohes Risiko für den Betroffenen zur Folge hat. Allerdings werden in Abs. 3 Anwendungsfälle aufgeführt, die im Wesentlichen den bisherigen Beispielen des BDSG entsprechen. Ergänzt werden diese Anwendungsfälle durch die Erwägungsgründe 89 bis 91, die zusätzlich auf den Umfang der Verarbeitung und den Einsatz neuer Technologien abstellen.

Anwendungsfälle	Beispiele
Automatisierte systematische und umfassende Bewertung persönlicher Aspekte, die als Grundlage einer Entscheidung mit Rechtswirkung dient.	Persönlichkeitstest oder Scorewertberechnungen. Keine DSFA bspw. bei reinen Mitarbeiterbefragungen, die keine unmittelbaren Rückschlüsse auf konkrete Beschäftigte zulassen.
Umfangreiche Verarbeitung von Daten besonderer Kategorien nach Art. 9 Abs. 1 DS-GVO	Daten zur rassischen und ethnischen Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur eindeutigen Identifikation, Gesundheitsdaten und Daten zum Sexualleben oder sexueller Orientierung; insb. Gesundheitsdaten sind häufig Bestandteil in Personalprozessen wie Arbeitsmedizin und Gesundheitsvorsorge (BEM) oder Tauglichkeitsprüfungen.
Umfangreiche Daten über strafrechtliche Verurteilungen und Straftaten.	Z.B. Führungszeugnisse und Sicherheitsüberprüfungen.
Systematische umfangreiche Überwachung (öffentlich) zugänglicher Bereiche.	Videoüberwachung in Gebäuden wie Einkaufszenten, Bahnhöfen, aber Zügen oder Bussen, systematische Erfassung von Autokennzeichen auf Autobahnen zur Identifikation.

Nach Erwägungsgrund 91 handele es sich nicht um eine umfangreiche Verarbeitung von Patienten- und Mandantendaten, wenn sie durch einen einzelnen Arzt oder Anwalt erfolgt. Es ist jedoch fraglich, ob Art. 35 DS-GVO überhaupt einen Interpretationsspielraum belässt, der durch den Erwägungsgrund ausgefüllt werden könnte.[1]

1 Zum Problem überschießender Erwägungsgründe vgl. Gola, K&R 2017, 145 ff.

Unterdessen hat die Artikel-29-Gruppe ein WP veröffentlicht, die diese gesetzlichen Vorgaben mit weiteren Beispielen konkretisiert.[2] Unter anderem wird als Anwendungsfall der Einsatz von Monitoringsystemen zur Überwachung von Mitarbeitern (einschließlich der Nutzung des Internets) genannt. Die Aufsichtsbehörden haben gem. Art. 35 Abs. 4 S. 1 DS-GVO den gesetzlichen Auftrag, sog. „Blacklists" derjenigen Verarbeitungsvorgänge zu erstellen, für die stets eine DSFA durchzuführen ist. Ferner haben die Behörden die Möglichkeit, gem. Art. 35 Abs. 5 DS-GVO spezifische Ausnahmen von der DSFA in „Whitelists" zu erfassen. Noch existieren diese Listen nicht. Stattdessen hat die DSK ein erstes Kurzpapier zur DSFA verabschiedet.[3]

1.2 Prüfungsschema

Beim Verantwortlichen muss jederzeit klar sein, wie mit neuen oder geänderten Verfahren umzugehen ist. Insbesondere ist bei neuen oder geänderten Verfahren sicherzustellen, dass jemandem die Entscheidung obliegt, ob eine DSFA durchzuführen ist. Nach der Vorstellung des Verordnungsgebers trifft diese Entscheidung der Verantwortliche, während der DSB hierbei berät (vgl. Art. 35 Abs. 2 & Art. 39 Abs. 1 lit c DS-GVO). Auslösendes Ereignis für die Prüfung ist das Bekanntwerden oder die Bekanntgabe einer Neuerung, z.B. im Rahmen eines Projektantrages oder im Austausch zwischen Fachbereich und DSB.

Erster Schritt: Rechtmäßigkeit

>> Findet sich ein Erlaubnistatbestand für die geplante Verarbeitung? Wenn nein: Prüfung beendet.

Zweiter Schritt: Pflicht zur DSFA

>> Ist die Verarbeitung gewhitelistet gem. Art. 35 Abs. 5 DS-GVO?
Wenn ja: keine DSFA notwendig, Prüfung beendet.

>> Liegt bereits eine vorweggenommene Folgenabschätzung im Sinne des Art. 35 Abs. 10 DS-GVO vor und hat der Mitgliedsstaat keine darüber hinausgehende DSFA angeordnet? Wenn ja: keine DSFA notwendig, Prüfung beendet.

>> Liegt bereits eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohem Risiko im Sinne von Art. 35 Abs. 1 Satz 2 DS-GVO vor? Wenn ja: keine DSFA notwendig, Prüfung beendet.

>> Ist die Verarbeitung geblacklistet gem. Art. 35 Abs. 4 DS-GVO? Wenn ja: DSFA notwendig, weiter mit Schritt Drei

>> Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen?
> Ist eine der Fallgruppen des Art. 35 Abs. 3 litt. a bis c DS-GVO erfüllt? Wenn ja: DSFA notwendig, weiter mit Schritt Drei.
> Ist ein sonstiges hohes Risiko im Sinne des Art. 35 Abs. 1 DS-GVO erkennbar? (Mögliche Anknüpfungspunkte: eigene Checkliste des DSB, eigene Checkliste des

2 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
3 https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

Fachbereichs, Checkliste nach WP 248 der Artikel-29-Gruppe.[4]) Wenn ja: DSFA notwendig, weiter mit Schritt Drei

Dritter Schritt: Durchführung der DSFA

Die DSFA besteht zumindest aus den in Art. 35 Abs. 7 litt a bis d DS-GVO niedergelegten Punkten. Derzeit sind mehrere Modelle in der Diskussion, wie bei einer DSFA am besten vorzugehen sei.

Deutschland: Standard Datenschutzmodell, V.1.0 –Testversion, 2016[5]. (https://www.datenschutzzentrum.de/Uploads/SDM-Methodology_V1_EN1.PDF)

Spanien: Guía Para Una Evaluación de Impacto de la Protección de Datos Personales (EIPD), Agencia Española de Protección de Datos (AEPD), 2014. (https://www.agpd.es/portalwebAGPD/canaldocumentacion/Publicaciones/Common/guias/Guia_EIPD.PDF)

Frankreich: Privacy Impact Assessment (PIA), Commission Nationale de l'Informatique et des Libertés (CNIL), 2015. (https://www.CNIL.fr/FR/Node/15798)

Großbritannien: Conducting privacyimpact assessments code of practice, Information Commissioner's Office (ICO), 2014. (https://ICO.org.UK/Media/for-Organisations/Documents/1595/Pia-Code-of-Practice.PDF)

Beispiele für EU branchenspezifische Rahmenbedingungen:

Privacy and Data Protection Impact Assessment Framework for RFID Applications. (http://ec.Europa.EU/Justice/Data-Protection/article-29/Documentation/Opinion-Recommendation/Files/2011/wp180_annex_en.PDF)

Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems. (http://ec.Europa.EU/Energy/Sites/Ener/Files/Documents/2014_dpia_smart_grids_forces.PDF)

ISO: Ein internationaler Standard wird auch der ISO-Standard zu Methoden für die Durchführung einer DSFA (ISO/IEC 29134) sein.

1.3 Einzelfall vs. Standardverfahren

Wie bereits erwähnt, besteht die Möglichkeit, mehrere ähnliche Verarbeitungsvorgänge mit ähnlichen Risiken in einer Datenschutz-Folgenabschätzung zu beurteilen. So kann es ausreichen, bei der Videoüberwachung gleichgelagerte Überwachungsanlagen – z.B. die Videoüberwachung verschiedener Filialen oder Niederlassungen eines Unternehmens nach einem feststehenden Konzept - nur einer Datenschutzfolgenabschätzung zu unterziehen. Demgegenüber wäre eine solche stationäre Videoüberwachung nicht vergleichbar mit dem Einsatz

4 Artikel-29-Datenschutzgruppe, WP 248 – „Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679", vom 4.10.2017, S. 9 f. mit insgesamt neun Kriterien.
5 Die Durchführung einer DSFA als Planspiel am Beispiel eines Pay-as-you-drive-Tarifs finden Sie unter https://datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf.

mobiler Videosysteme, wie z.B. beim Einsatz von Drohnen oder Bodycams bzw. intelligenter Videosysteme zum Tracking mit Personen- oder Gesichtserkennung.

In jedem Falle ist eine kursorische Prüfung erforderlich, ob die in Rede stehenden Fälle wirklich „gleichgelagert" sind.

Sofern der Verantwortliche zu dem Ergebnis kommt, dass kein hohes Risiko für den Betroffenen zu erwarten ist und eine DSFA demzufolge nicht erforderlich ist, ist dieses Ergebnis zu dokumentieren (Rechenschaftspflicht).

Zu den Accountability-Pflichten siehe GDD-Praxishilfe DS-GVO IX.

Da aber ungeachtet einer etwa erforderlichen DSFA in jedem Fall angemessene Maßnahmen zum Schutz personenbezogener Daten zu treffen sind (u.a. nach Artt. 5, 32), sollte dieser Schritt (Prüfung und Dokumentation der Erforderlichkeit) keinen besonderen Zusatzaufwand darstellen. Denkbar ist, diesen Prüfschritt in der Dokumentation der Verarbeitungstätigkeiten zu verankern.

1.4. Gewohnte Ausnahmen entfallen weitestgehend

Die bisher im BDSG a.F. vorgesehenen Ausnahmen (gesetzliche Verpflichtung oder Einwilligung des Betroffenen oder Erfüllung eines Vertrages mit dem Betroffenen) fallen im Wesentlichen weg. Nur wenn die Verarbeitung auf Art. 6 Abs. 1 lit. c oder e DS-GVO beruht (also zu Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt, oder die Verarbeitung erforderlich ist zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde) kann eine DSFA entfallen, wenn die Rechtsvorschrift den konkreten Verarbeitungsvorgang regelt und bereits im Rahmen der allgemeinen Folgenabschätzung bei Erlass der Vorschrift eine DSFA erfolgte.

2. Nachträgliche DSFA

2.1 Risikoänderung

Art. 35 Abs. 11 DS-GVO regelt die Überprüfung, ob die Verarbeitung (noch) nach der ursprünglichen DSFA durchgeführt wird. Dies bedeutete eine permanente Kontrolle, ob die einst zu Grunde gelegten Vorstellungen weiterhin Geltung beanspruchen.

>> In Art. 35 Abs. 11 Hs. 2 DS-GVO ist die anlassbezogene Kontrolle geregelt. So könnte z.B. nach einem Hinweis oder einer Beschwerde offenkundig sein, dass vormals festgelegte Abhilfemaßnahmen nicht eingehalten werden oder sich die rechtlichen bzw. tatsächliche Rahmenbedingungen der Verarbeitung geändert haben.

>> Art. 35 Abs. 11 Hs. 1 DS-GVO befasst sich demgegenüber mit der turnusmäßigen, anlassunabhängigen Kontrolle. Hier ist zumindest eine kursorische Prüfung notwendig, um zu beurteilen, ob sich eine Änderung des Risikos ergeben haben könnte.

Für die turnusmäßige Kontrolle bietet sich ein Jahresrhythmus an. Maßgebliches Kriterium sollte jedoch nicht die zeitliche Komponente, sondern die tatsächliche Risikoeinschätzung sein.

2.2 Nachgeschobene Blacklist

Da in der Verordnung kein bestimmter Zeitpunkt für die Aufsichtsbehörde geregelt ist, bis wann die Listen nach Art. 35 Abs. 4 und 5 DS-GVO veröffentlicht sein müssen, bleibt abzuwarten, wie die Listen genau aussehen werden. Es ist auch nicht ausgeschlossen, dass veröffentlichte Listen nachträglich überarbeitet werden. Möglicherweise wird eine Liste von DSFA-pflichtigen Verarbeitungen gem. Art. 35 Abs. 4 S. 1 DS-GVO daher auch solche Verarbeitungsvorgänge enthalten, die nicht unmittelbar und offenkundig einen Tatbestand des Art. 35 Abs. 3 litt. a bis c DS-GVO erfüllen.

Hierdurch kann die Situation entstehen, dass Verantwortliche zunächst auf eine DSFA verzichten dürfen, um dann von der nachgeschobenen Blacklist eingeholt zu werden. Hierbei handelt es sich um einen Anwendungsfall des Art. 35 Abs. 11 DS-GVO, da sich in der Tat die rechtlichen Rahmenbedingungen der Verarbeitung geändert haben. Eine nachträgliche DSFA gem. Art. 35 Abs. 11 DS-GVO ist daher angezeigt.

2.3 Nachholen einer pflichtwidrig unterlassenen DSFA

Unterbleibt trotz gesetzlicher Verpflichtung die Durchführung einer DSFA, ist dies ein Verstoß gem. Art. 83 Abs. 4 lit. a i.V.m. Art. 35 Abs. 1 DS-GVO. Es ist allerdings davon auszugehen, dass die nachträgliche Durchführung eines der DSFA entsprechenden Verfahrens gem. Art. 83 Abs. 2 Satz 2 litt. c oder f DS-GVO (Schadensminderung; Zusammenarbeit mit der Aufsichtsbehörde) die Verhängung einer Geldbuße entbehrlich macht. Dies gilt jedenfalls dann, wenn die verspätete Prüfung tatsächlich Rechte von Betroffenen stärkt, die Sicherheit der Verarbeitung erhöht oder eine bestehende Beeinträchtigung abmildert.

2.4 Altverfahren

Die Artikel-29-Datenschutzgruppe geht im kürzlich überarbeiteten WP 248 davon aus, dass die DSFA auch für bestehende Verarbeitungen durchzuführen ist, soweit ein hohes Risiko für die Betroffenen besteht. Hiervon könne lediglich abgewichen werden, wenn eine Vorabkontrolle nach altem Recht durchgeführt worden sei und sich die die Umstände seitdem nicht verändert hätten.[6]

Die Auffassung der Artikel-29-Gruppe findet keine Stütze im Gesetz!

6 Artikel-29-Datenschutzgruppe, WP 248 – „Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679“, S. 13 vom 4.10.2017.

Nach dem Wortlaut des Art. 35 Abs. 1 DS-GVO soll die DSFA präventiv wirken. ErwGr 171 S. 1 DS-GVO sieht vor, dass laufende Verarbeitungsvorgänge materiellrechtlich mit der DS-GVO in Einklang gebracht werden, die DSFA hat jedoch eine reine Ordnungsfunktion.

Die Artikel-29-Gruppe berücksichtigt insb. nicht, dass nach § 4d Abs. 5 Satz 2, Hs. 2 BDSG a.F. befugtermaßen von einer Vorabkontrolle abgesehen werden durfte, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorlag oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich war.

Es wäre höchst widersprüchlich, wenn Verarbeitungsvorgänge, die nach altem Recht ordnungsgemäß implementiert wurden, seit Jahren beanstandungsfrei laufen und nach neuem Recht materiell vollkommen rechtmäßig sind, mangels nachträglicher DSFA plötzlich ein erhebliches Haftungsrisiko bedeuten würden. Verarbeitungen, die nach altem Datenschutzrecht aufgenommen worden sind und gleichbleibend fortgeführt werden, können daher nicht dem Art. 35 Abs. 1 DS-GVO unterliegen.

3. Tätigkeit des Datenschutzbeauftragten bei der DSFA

Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer DSFA unterliegen, haben sie gem. § 38 Abs. 1 Satz 2 BDSG 2018 unabhängig von der Anzahl ihrer Beschäftigten einen DSB zu benennen.

Die Bestellpflicht gem. § 38 Abs. 1 Satz 2 BDSG 2018 deckt sich mit derjenigen bei der Vorabkontrolle nach § 4f Abs. 1 Satz 6 BDSG a.F. Die Öffnungsklausel hierfür findet sich in Art. 37 Abs. 4 Satz 1 Hs. 2 DS-GVO.

Welche Rolle hat nun der DSB bei der Durchführung einer DSFA? Art 35 Abs. 2 DS-GVO ist recht eindeutig: „Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten […] ein." Art. 39 DS-GVO, der die Aufgaben des DSB beschreibt, wiederholt: „Dem DSB obliegen zumindest folgende Aufgaben: … c) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung". Damit scheint die Rollenverteilung klar. Der Verantwortliche führt die DSFA durch und der DSB berät und überwacht.

Dass es in der Praxis so nicht funktionieren kann, weiß zumindest jeder, der sich in der Vergangenheit mit dem Vorgängerprozess, der Vorabkontrolle, beschäftigt hat. Hier muss es ein Miteinander des für den Verarbeitungsvorgang Verantwortlichen und dem DSB geben, wobei allerdings die datenschutzrechtliche Verantwortung zur ordnungsgemä-

ßen Durchführung der DSFA gem. Art. 35 Abs. 1 DS-GVO bei der verantwortlichen Stelle liegt.

Ob eine DSFA durchzuführen ist, ergibt sich aus dem Prüfschema unter 1.2.

Der Verantwortliche hat zunächst die Pflicht, den geplanten Verarbeitungsvorgang systematisch zu beschreiben. Für die Bewertungsphase, das heißt für die Einschätzung der Risiken, sollte er sich mit dem DSB beraten, bzw. ihn so früh wie möglich einbeziehen. Beide Funktionen sollten gemeinsam überlegen, welche Maßnahmen geeignet sind, die ermittelten Risiken einzudämmen.

Den Verantwortlichen mit diesen Aufgaben alleine zu lassen, hieße ihn zu überfordern. Andererseits wäre es aber auch abwegig, die Durchführung einer DSFA insgesamt auf den DSB zu delegieren. Abgesehen davon, dass der DSB zwingend auf Informationen zu dem geplanten Verarbeitungsvorgang angewiesen wäre, bedeutete eine Aufgabendelegierung einen Interessenkonflikt. Denn ein DSB kann seine gesetzliche Überwachungspflicht nicht interessenfrei wahrnehmen bei einer DSFA, die er selbst und alleine durchgeführt hat. Zudem würde eine Delegierung der Durchführung der DSFA auf den DSB der gesetzlich in Art. 35 Abs. 1 DS-GVO festgelegten Rollenverteilung widersprechen, die insoweit dem Verantwortlichen als Aufgabe auferlegt ist. Mit Verantwortlicher ist nach Art. 4 Nr. 7 DS-GVO die jeweilige natürliche oder juristische Person gemeint, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Das kann nicht der DSB sein, dessen Aufgaben in Art. 39 DS-GVO klar umrissen sind. Hier sind also Verantwortlicher und DSB aufgerufen, in einer abgestimmten und kooperativen Vorgehensweise den Prozess der DSFA zu beginnen und iterativ durchzuführen. Dabei sind gegebenenfalls und idealerweise auch die Meinungen der betroffenen Personen oder ihrer Vertreter, z. B. Gremien der Mitbestimmung, einzuholen.

4. Anhörung von Betroffenen oder Vertretern

Nach Art. 35 Abs. 9 DS-GVO holt der Verantwortliche ggf. den Standpunkt der Betroffenen oder gegegenenfalls ihrer Vertreter ein. Wann und wie dies zu erfolgen hat, ist weder in Art. 35 DS-GVO noch in den ErwGr näher ausgeführt. Nach Auffassung der DSK umfasst dies beispielsweise die Einbindung der Mitbestimmungsgremien.[7] Diese erfolgt bei der Einführung neuer IT-Systeme im Beschäftigtenkontext regelmäßig ohnehin im Rahmen der Mitbestimmung nach § 87 BetrVG. So wäre im Beispiel der Artikel-29-Gruppe (Einführung eines umfassenden MA-Monitoring-Systems) der Betriebsrat zu beteiligen und der Abschluss einer Betriebsvereinbarung empfehlenswert. Sofern ein Unternehmen über einen Kundenbeirat[8] verfügt, könnte dieser in eine DSFA eingebunden werden. Darüber hinaus ist auch denkbar, eine abstrakte Beteiligung Betroffener durch die Berücksichtigung von vorangegangenen Studien oder Umfragen sicherzustellen.

7 https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf
8 https://de.wikipedia.org/wiki/Kundenbeirat

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.0 (November 2017)