D3 Risiken und Schutzbedarf

Die DS-GVO knüpft die Anforderungen an technische und organisatorische Maßnahmen an das mit der Verarbeitung der personenbezogenen Daten verbundene Risiko für die Rechte und Freiheiten betroffener Personen.

Im Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen“ [1)] der Datenschutzkonferenz wird der Begriff des Risikos im Kontext der DS-GVO erläutert und in allgemeiner Form aufgezeigt, wie Risiken für die Rechte und Freiheiten natürlicher Personen bestimmt und in Bezug auf ihre Rechtsfolgen bewertet werden können. Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das einen Schaden für die Rechte und Freiheiten natürlicher Personen (einschließlich ungerechtfertigter Beeinträchtigung der Rechte und Freiheiten) darstellt oder zu einem Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens für die Rechte und Freiheiten der betroffenen Personen und zweitens die Wahrscheinlichkeit, dass das Ereignis und der Schaden eintreten. Gemäß ErwGr 75 sind unter die möglichen Schäden für die Rechte und Freiheiten natürlicher Personen physische, materielle und immaterielle Schäden einzuordnen. Im Folgenden wird allgemein von Schadensereignissen gesprochen. Ein Schadensereignis kann verschiedene Rechte und Freiheiten schädigen oder beeinträchtigen und möglicherweise weitere Schadensereignisse nach sich ziehen. Unrechtmäßige Verarbeitungstätigkeiten, insbesondere solche die nicht den Grundsätzen des Art. 5 DS-GVO entsprechen, sind in sich Beeinträchtigungen des Grundrechts auf Datenschutz und stellen daher bereits ein Schadensereignis dar. Sie können zusätzliche Schäden wie bspw. die Diskriminierung natürlicher Personen nach sich ziehen. [2)]

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden.

Aufgabe des Verantwortlichen ist, diese Risiken zu identifizieren, zu analysieren und einzustufen und Maßnahmen zu deren Eindämmung zu treffen (siehe Kapitel D4 Datenschutzmanagement mit dem SDM).

Dieses Kapitel D3 gibt Hilfestellungen, um das Datenschutz-Risiko einer Verarbeitungstätigkeit zu bestimmen. Es stellt außerdem den Zusammenhang her zwischen den Risiken durch eine Verarbeitungstätigkeit und dem durch sie hervorgerufenen Schutzbedarf natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 1 DS-GVO) einerseits und dem durch die implementierten Maßnahmen erreichten Schutzniveau bzw. dem Restrisiko einer Verarbeitungstätigkeit andererseits, mit dem Ziel, die Bestimmung geeigneter und angemessener Maßnahmen zu ermöglichen. Die Bestimmung der Höhe des Risikos ist die Voraussetzung dafür, technische und organisatorische Maßnahmen und den notwendigen Grad ihrer Wirksamkeit festlegen zu können, mit denen sich Risiken eliminieren oder zumindest reduzieren lassen und eine Verarbeitung datenschutzkonform erfolgen kann. Grundsätzlich gilt die Regel: Je höher das Risiko, desto umsichtiger muss die Verarbeitungstätigkeit gestaltet sein und desto wirksamer müssen die entsprechenden, konkreten technischen und organisatorische Maßnahmen betrieben, kontrolliert und ggf. verbessert werden.

D3.1 Risiken für Betroffene

a) Ausgangspunkt von Überlegungen zum Risiko ist die Verarbeitungstätigkeit, die aus einem oder mehreren Verarbeitungsvorgängen besteht. Es wird der in Art. 30 DS-GVO eingeführte Begriff „Verarbeitungstätigkeit“ verwendet, denn nach der Definition in Art. 4 Nr. 2 DS-GVO sind Verarbeitungen einzelne Vorgänge oder Vorgangsreihen. Für jede Verarbeitungstätigkeit müssen die in Art. 5 DS-GVO formulierten Grundsätze der Verarbeitung personenbezogener Daten beachtet werden. Das SDM „verdichtet“ diese Grundsätze zu Gewährleistungszielen, die weitere operative Anforderungen der DS-GVO aufnehmen. Jede Verarbeitungstätigkeit erzeugt grundsätzlich Risiken für betroffene Personen durch den Umstand der Verarbeitung personenbezogener Daten allein. Im Unterschied zum allgemeinen Risikomanagement und auch zum Risikomanagement in der Informationssicherheit besteht dabei im Bereich des Datenschutzes grundsätzlich die Pflicht, die durch die Verarbeitung personenbezogener Daten entstehenden Risiken mit geeigneten und angemessenen technischen und organisatorischen Maßnahmen auf ein angemessenes Schutzniveau zu reduzieren. Nach der DS-GVO ist es nicht zulässig, auf die Behandlung von Anforderungen insbesondere der Umsetzung der Grundsätze aus Art. 5 DS-GVO gänzlich zu verzichten und die daraus resultierenden Risiken in Kauf zu nehmen. Die aus dem Bereich der Informationssicherheit bekannten Instrumente der Risikoakzeptanz oder des Risikotransfers stehen im datenschutzrechtlichen Kontext dem Verantwortlichen nicht zur Verfügung. Spielraum besteht bei der Auswahl und der Art und Weise der Umsetzung von Anforderungen mit Hilfe von technischen und organisatorischen Maßnahmen, die in einen angemessenen Umfang gefordert werden (Artikel 5 Nr. 1 lit. d „angemessene Maßnahmen“, lit. f „angemessene Sicherheit“). Hier ist es geboten, bestehende Risiken für die Rechte und Freiheiten natürlicher Personen genauer zu analysieren. Erst wenn ein angemessenes Schutzniveau erreicht wurde und somit die Interessen der Betroffenen angemessen berücksichtigt wurden, können die verbleibenden Restrisiken durch den Verantwortlichen akzeptiert werden.

b) Art. 35 DS-GVO verlangt vom Verantwortlichen, bei einem „voraussichtlich hohen Risiko“ für die Rechte und Freiheiten natürlicher Personen eine Datenschutz- Folgenabschätzung für die vorgesehene Verarbeitung durchzuführen. Zur Bestimmung der Höhe des Risikos muss der Verantwortliche daher zunächst eine „Schwellwert- Analyse“ durchführen. Diese Analyse muss für jede Verarbeitungstätigkeit, bestehend aus einem oder mehreren Verarbeitungsvorgängen, durchgeführt werden, um die Entscheidung für die Einstufung einer Verarbeitungstätigkeit gegenüber einer zuständigen Datenschutzaufsichtsbehörde begründen zu können (Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO).

Wenn das Ergebnis der Schwellwert-Analyse ein „voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ ist, dann muss das eine Auswirkung auf die Gestaltung der Verarbeitungstätigkeit sowie deren Prüfbarkeit haben. Die methodisch zentrale Frage zur Gestaltung einer Verarbeitungstätigkeit besteht deshalb darin, wie für eine Verarbeitungstätigkeit die Höhe des Risikos zu bestimmen ist.

D3.2 Risikobetrachtung

D3.2.1 Schwellwert-Analyse

Ziel der Schwellwert-Analyse ist es festzustellen, ob eine Verarbeitungstätigkeit voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat und somit eine DSFA erfordert. Zur Identifikation eines voraussichtlich „hohen Risikos“ durch eine Verarbeitungstätigkeit wird folgendes Vorgehen vorgeschlagen, wobei die Reihenfolge nicht zwingend eingehalten werden muss:

1. Prüfen, ob die Verarbeitungstätigkeit, für welche das Risiko zu bestimmen ist, in der „Muss-Liste“ gemäß Art. 35 Abs. 4 DS-GVO der Datenschutzaufsichtsbehörden enthalten ist. Wenn ja, dann besteht ein voraussichtlich hohes Risiko. (Für den nicht-öffentlichen Bereich: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf, Stand: 17.10.2018, letzter Aufruf: 01.04.2019).

2. Prüfen, ob die betrachtete Verarbeitungstätigkeit zu den besonders riskanten Verarbeitungstätigkeiten gem. Art. 35 Abs. 3 DS-GVO zählt. Wenn dies zutrifft, besteht ein voraussichtlich hohes Risiko.

3. Prüfen, ob auf die Verarbeitungstätigkeit Eigenschaften zutreffen, die in der Auflistung von Verarbeitungstätigkeiten mit „voraussichtlich hohem Risiko“ des Working Paper 248 rev. 01 [3)] des Europäischen Datenschutzausschusses enthalten sind. Wenn mindestens zwei der Einträge zutreffen ist in den meisten Fällen davon auszugehen, dass ein voraussichtlich hohes Risiko besteht. Ein hohes Risiko kann allerdings auch bereits dann vorliegen, wenn nur eines der Kriterien erfüllt ist.

1. Bewerten oder Einstufen (Scoring)
   („Evaluation or scoring“)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
   („Automated-decicion making with legal or similar significant effect“)
3. Systematische Überwachung
   („Systematic monitoring“)
4. Vertrauliche Daten oder höchst persönliche Daten
   („Sensitive data or data of a highly personal nature“)
5. Datenverarbeitung in großem Umfang
   („Data processed in a large scale“)
6. Abgleichen oder Zusammenführen von Datensätzen
   („Matching or combining datasets“)
7. Daten zu schutzbedürftigen Betroffenen
   (Data concerning vulnerable data subjects“)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
   („Innovative use or applying new technological or organisational solutions“)
9. Betroffene werden an der Ausübung ihres Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages gehindert
   („When the processing in itself prevents data subjects from exercising a right or using a service or a contract“)

4. Prüfen, ob Art, Umfang, Umstände oder Zwecke (ErwG 76 DS-GVO) der Verarbeitungstätigkeit das Risiko für betroffene Personen erhöhen. Hierfür ist es ratsam, entsprechende Praxiserfahrungen und konkretisierende Gerichtsurteile in die Prüfung eines eventuell bestehenden hohen Risikos einzubeziehen.

D3.2.2 Risiko-Identifikation

Zur Identifikation konkreter Risiken für die Rechte und Freiheiten der betroffenen Personen, die auch durch spezifische Besonderheiten der Verarbeitungstätigkeit entstehen können, bietet es sich an, die folgenden Fragen zu stellen:

a) Welche Schäden können für betroffene Personen auf der Grundlage der zu verarbeitenden Daten auftreten?

b) Wodurch, d. h. durch welche Ereignisse kann es zu dem Schaden kommen?
c) Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

Insbesondere bei diesem Schritt kann es vorkommen, dass in Ausnahmefällen Risiken identifiziert werden, die zu sehr schwerwiegenden Auswirkungen für betroffene Personen führen können, etwa zu einer Gefahr für Leib und Leben. In solchen Fällen ist es sinnvoll, einen sehr hohen Schutzbedarf anzunehmen. Die durch das SDM vorgeschlagenen technischen und organisatorischen Maßnahmen sind dafür jedoch nicht ausgelegt, so dass in einem solchen Fall, wie auch bereits bei hohem Schutzbedarf, stets eine individuelle Betrachtung der möglichen Maßnahmen erfolgen muss, um ein entsprechendes angemessenes Schutzniveau herzustellen. Die Maßnahmen des SDM können jedoch als Ausgangspunkt für diese allgemeine Betrachtung dienen.

Neben den spezifischen Datenschutz-Risiken einer Verarbeitungstätigkeit selbst sind auch die Risiken der Informationssicherheit zu betrachten. Diese Risiken beziehen sich auf den Schutz der Geschäftsprozesse der Organisation. Zur Bearbeitung dieser Risiken hat sich der IT-Grundschutz des BSI bewährt (https://www.bsi.de). Wesentliche Aspekte von Grundschutz-Maßnahmen betreffen einen geordneten Betrieb, die Sicherstellung der Verfügbarkeit und Integrität der Daten, Systeme und Dienste sowie die Verhinderung eines unbefugten Zugriffs auf Geschäfts-, Produktions- und Personendaten, also die Sicherstellung der Vertraulichkeit. Diese sind Voraussetzungen auch für einen wirksamen Datenschutz. Sehr wichtig ist es, dabei darauf zu achten, dass bei der Abstimmung von Maßnahmen für die Informationssicherheit und den operativen Datenschutz insbesondere jene Schutzmaßnahmen, welche für die IT-Sicherheit betrieben werden, ihrerseits datenschutzkonform eingerichtet sind (z. B. Videoüberwachung zur Objektsicherung, Cloud- Lösungen zum Malwareschutz oder Protokollierung). Hierbei müssen etwaige Konflikte zwischen den Anforderungen des Datenschutzes und der Informationssicherheit aufgelöst werden.

D3.2.3 Risikobewertung

Es ist die Aufgabe des Verantwortlichen und ggfs. des Auftragsverarbeiters, die identifizierten Risiken für die betroffenen Personen zu analysieren und einzustufen. Dabei muss der Verantwortliche bzw. der Auftragsverarbeiter die Schwere und die Eintrittswahrscheinlichkeit der identifizierten Risiken nach objektiven Maßstäben bestimmen und dokumentieren. Aus dieser Bewertung folgt auf Basis einer Risikofunktion (bspw. in Form einer Risikomatrix) die jeweilige Höhe der Risiken (vgl. Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen“ [4)]).

D3.3 Risikohöhe, Schutzbedarfsstufe, Schutzniveau und Restrisiko

Der Schutzbedarf einer natürlichen Person bei der Verarbeitung personenbezogener Daten in Bezug auf ihre Rechte und Freiheiten ergibt sich aus dem Risiko, das von der Verarbeitungstätigkeit und deren Eingriffsintensität ausgeht. Die DS-GVO kennt nur die Begriffe „Risiko“ und „hohes Risiko“, wobei „Risiko“ hier als „normales Risiko“ bezeichnet wird. Daneben verwendet die DS-GVO die Formulierung „voraussichtlich nicht zu einem Risiko“ führend (Art. 27 Abs. 2 lit. a und Art. 33 Abs. 1 DS-GVO). Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko“ führend verstanden. Erfahrungen aus der Praxis zeigen, dass es solche geringen Risiken gibt, die in der DS-GVO keine gesonderte Erwähnung finden, für die jedoch ebenfalls Maßnahmen zu ergreifen sind. Die Maßnahmen für den normalen Schutzbedarf decken auch solche geringen Risiken ab.

Der Schutzbedarf ergibt sich aus dem Risiko der Verarbeitungstätigkeit, bevor technische und

organisatorische Maßnahmen bestimmt und umgesetzt wurden. Insofern gilt der folgende Zusammenhang zwischen Risiko(höhe), im Sinne eines Ausgangsrisikos, und Schutzbedarf(sstufe):

- **kein oder geringes Risiko** der Verarbeitung → **normaler Schutzbedarf** für von der Verarbeitung betroffene Personen
- **normales Risiko** der Verarbeitung → **normaler Schutzbedarf** für von der Verarbeitung betroffene Personen
- **hohes Risiko** der Verarbeitung → **hoher Schutzbedarf** für von der Verarbeitung betroffene Personen

Während der durch das Ausgangsrisiko definierte Schutzbedarf betroffener Personen bzgl. der Verarbeitungstätigkeit konstant bleibt, können die Risiken der Verarbeitung für die betroffenen Personen durch technische und organisatorische Maßnahmen verringert werden. Diese Maßnahmen verändern nicht den Schutzbedarf, sondern reduzieren das Risiko der Verarbeitungstätigkeit. Die zunächst vorhandenen Risiken – die Ausgangsrisiken – müssen durch Verfahrensgestaltung und technische und organisatorische Maßnahmen so weit verringert werden, bis ein dem Risiko angemessenes (Art. 32 Abs. 1 DS-GVO) und somit verantwortbares Schutzniveau für die Verarbeitungstätigkeit gewährleistet wird. Oder anders ausgedrückt: Das Schutzniveau muss so hoch sein, dass die verbleibenden Restrisiken einer Verarbeitung durch den Verantwortlichen nachweislich berechtigt verantwortet werden können. Wenn kein angemessenes Restrisiko vorliegt, darf die Verarbeitungstätigkeit aufgrund mangelnder Rechtskonformität nicht aufgenommen werden. Verbleibt ein „hohes Risiko“ und darüber hinaus, dann sieht Art. 36 DS-GVO vor, dass der Verantwortliche die zuständige Datenschutzaufsichtsbehörde konsultieren muss.

Die Methodik des IT-Grundschutz des BSI nutzt zur Gewährleistung der Informationssicherheit ebenfalls das Konzept der Schutzbedarfseinstufungen, um die Wirkungen technischer und organisatorischer Maßnahmen skalieren zu können.

Wegen der unterschiedlichen Zielrichtungen von IT-Grundschutz des BSI (Gewährleistung der Informationssicherheit einer Organisation) und „operativem Datenschutz“ mit Hilfe des SDM (Gewährleistung der Rechte und Freiheiten natürlicher Personen) kann nicht ausgeschlossen werden, dass die Schutzbedarfsfeststellungen nach Grundschutz und nach SDM für dieselbe Verarbeitung unterschiedlich ausfallen. Kommt es zu unterschiedlichen Bewertungen, dann sollten entweder die jeweiligen Maßnahmen für den höheren Schutzbedarf umgesetzt werden, oder es sollte im Rahmen einer genaueren Analyse festgestellt werden, was der Grund für die unterschiedlichen Bewertungen ist und wie in diesem Fall ein angemessenes Schutzniveau erzielt werden kann. Die datenschutzrechtlichen Anforderungen sind maßgeblich. Diese Analyse- und Entscheidungsprozesse mit ihrer dazugehörigen Bewertung sind zu dokumentieren. Sowohl bei einer unternehmens- oder organisationsinternen Evaluation bzw. Revision oder während einer datenschutzrechtlichen Prüfung mussnachvollziehbar sein, welche konkreten technischen und organisatorischen Maßnahmen zur Erlangung des erforderlichen Schutzniveaus in Bezug auf die jeweilige Verarbeitungstätigkeit ergriffen wurden.

D3.4 Bestimmung technischer und organisatorischer Maßnahmen insbesondere bei hohem Risiko

Grundsätzlich sind Datenverarbeitungsprozesse und damit die Spezifikation der Datenverarbeitung so zu gestalten, dass, wenn möglich, die Verarbeitung ohne Personenbezug erfolgt oder zumindest die Risiken gemindert werden. Wurde beispielsweise als Risiko identifiziert, dass in automatisierten Abrufverfahren hohe Risiken für die Rechte und Freiheiten natürlicher Personen bestehen, weil nicht erforderliche Abrufe nicht technisch unterbunden werden können oder der Datenumfang von Abrufen

nicht vom Abrufenden angemessen eingeschränkt werden kann, so besteht eine weitere Möglichkeit zur Risikobeschränkung im Verzicht auf das automatisierte Abrufverfahren und eine ersatzweise Implementierung einer Übermittlung im Einzelfall. Beim Treffen geeigneter technischer und organisatorischer Maßnahmen ist der Stand der Technik zu berücksichtigen. Die in Abschnitt “D1 Generische Maßnahmen“ vorgeschlagenen technischen und organisatorischen Maßnahmen sind eine gute Grundlage, um angemessene Maßnahmen für normalen Schutzbedarf zu entwickeln. Zukünftig werden diese generischen Maßnahmen um den Referenzmaßnahmen-Katalog ergänzt. Im Fall eines hohen oder sehr hohen Schutzbedarfs wird die folgende standardisierte Strategie zur wirksamen Minderung der Risiken empfohlen.

1. Es sind die Maßnahmen des Referenzmaßnahmen-Katalogs umzusetzen, die bei normalem Ausgangsrisiko bzw. normalem Schutzbedarf zu ergreifen sind.
2. Zusätzliche Maßnahmen aus dem Referenzmaßnahmen-Katalog sind umzusetzen.
3. Zusätzlich sind individuelle Maßnahmen auszuwählen. Ein Beispiel für eine individuelle Maßnahme könnte darin bestehen, bestimmte Vorgänge einer Verarbeitungstätigkeit nur auf Antrag bzw. nach einer Prüfung freizugeben und diese Tätigkeit dann im Betrieb zu überwachen, so dass bei Abweichungen ein Abbruch oder die Korrekturmaßnahme ausgelöst wird.
4. Die Wirkung einer Maßnahme kann erhöht wird, indem Skalierungsmöglichkeiten genutzt werden.
   Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel. Ein anderes Beispiel wäre die Sicherung von Protokolldaten, der Betrieb dedizierter Protokolleserver für die Verarbeitung von Protokolldaten, der an zentraler Stelle sämtliche Protokolldaten speichert und sie dem Zugriff von den Produktionsmaschinen aus und durch deren Administratoren entzieht.
5. Auf alle schon getroffenen Maßnahmen sind ihrerseits technische und organisatorische Maßnahmen anzuwenden, um die Wirksamkeit, die Zuverlässigkeit, die Robustheit, die Belastbarkeit und die Evaluierbarkeit der Maßnahmen zu verbessern und ihre Rechtmäßigkeit sicherzustellen.
   Das folgende Beispiel verdeutlicht die Strategie der Selbstanwendung der Maßnahmen auf sich selbst. Transparenz bedeutet, dass eine Verarbeitungstätigkeit anhand von Soll-Ist-Bilanzen prüfbar sein muss. Prüfbarkeit im Nachhinein bedeutet, dass Protokolldaten erzeugt, gespeichert und verarbeitet werden müssen. Die Protokolldaten müssen dann durch zusätzliche Maßnahmen revisionsfest gespeichert und deren Vertraulichkeit gewährleistet sein, indem sie signiert und verschlüsselt übertragen und gespeichert werden.

Zu beachten ist, dass neue Risiken durch ergriffene technische und organisatorische Maßnahmen entstehen können. Diese Risiken sind zu bewerten und angemessen zu reduzieren. Als Beispiel kann eine Vollprotokollierung von Mitarbeiter-Handlungen gefordert sein, die zugleich das Risiko birgt, dass durch Auswertungen dieses Protokolls eine unzulässige Leistungs- und Verhaltenskontrolle stattfindet. Wird in diesem Schritt eine Verarbeitung so verändert, dass die getroffenen Maßnahmen zu neuen Risiken, die höher sind als das Ausgangsrisiko, und somit zu einer Erhöhung des Schutzbedarfs führen, muss die Ausgestaltung der Maßnahmen erneut evaluiert werden. Die oben genannten Strategiensind in einem iterativen Prozess so lange anzuwenden, bis die Ausgestaltung der Maßnahmen ein angemessenes Schutzniveau gewährleistet.

---

1) https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, Stand: 26.04.2018, letzter Aufruf: 29.07.2019.

2) Diese Definition des Risikos kann aus den ErwGr 75 DS-GVO hergeleitet werden.

3)

Dieses Arbeitspapier wurde ursprünglich durch die Vorgängerinstitution des EDSA, die Artikel-29-Arbeitsgruppe, und später durch den EDSA mit Bestätigung 1/2018 angenommen. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, Stand: 13.10.2017 (Revision 0.1; letzter Aufruf: 01.04.2019) (aus: WP 248 der Art. 29 Gruppe, ab Seite 10 f)
[4)]
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, Stand: 26.04.2018, letzter Aufruf: 01.04.2019.