DATENSCHUTZGRUPPE NACH ARTIKEL 29

17/DE

WP 248 Rev. 01

Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“

angenommen am 4. April 2017

zuletzt überarbeitet und angenommen am 4. Oktober 2017

Die Gruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingerichtet. Sie ist ein unabhängiges europäisches Beratungsgremium für den Schutz personenbezogener Daten und der Privatsphäre. Ihre Aufgaben werden in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG beschrieben.

Die Sekretariatsgeschäfte werden von der Europäischen Kommission, Generaldirektion Justiz, Direktorat C (Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro MO-59 03/075, wahrgenommen.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

DIE ARBEITSGRUPPE FÜR DEN SCHUTZ DER RECHTE VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und 30 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung -

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN:

Inhaltsverzeichnis

I. Einleitung

Die Verordnung 2016/679[1] (Datenschutz-Grundverordnung, DSGVO) wird ab dem 25. Mai 2018 gelten. Artikel 35 der DSGVO führt, ebenso wie die Richtlinie 2016/680[2], das Konzept einer Datenschutz-Folgenabschätzung (DSFA)[3] ein.

Eine Datenschutz-Folgenabschätzung ist ein Verfahren, anhand dessen die Verarbeitung beschrieben, ihre Notwendigkeit und Verhältnismäßigkeit bewertet und die Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung personenbezogener Daten[4] mit sich bringt, durch eine entsprechende Risikoabschätzung und die Ermittlung von Gegenmaßnahmen besser kontrolliert werden sollen. Datenschutz-Folgenabschätzungen sind bedeutende Rechenschaftsinstrumente: Für die Verarbeitung Verantwortliche können damit nicht nur die DSGVO-Anforderungen besser erfüllen, sondern auch nachweisen, dass geeignete Maßnahmen zur Einhaltung der Verordnung (siehe auch

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[2] Nach Artikel 27 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr wird eine Datenschutz-Folgenabschätzung benötigt, da die „*Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge*“ hat.

[3] Auch in anderen Zusammenhängen ist häufig die Rede von einer Datenschutz-Folgenabschätzung, dann jedoch im Sinne der englischen Bezeichnung „Privacy Impact Assessment“ (PIA) (im Gegensatz zu der den Gegenstand dieser Leitlinien bildenden „Data Protection Impact Assessment“ (DPIA)).

[4] Zwar enthält die DSGVO keine offizielle Definition des Konzepts einer Datenschutz-Folgenabschätzung an sich, aber

- in Artikel 35 Absatz 7 ist festgehalten, was sie mindestens umfassen muss:
    - „*a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;*
    - *b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;*
    - *c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und*
    - *d) 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 berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“*
- in Erwägungsgrund 84 sind ihre Bedeutung und Rolle wie folgt erläutert: „*Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, besser eingehalten wird, sollte der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich sein.“*

Artikel 24)[5] ergriffen wurden. Das heißt also, dass **eine Datenschutz-Folgenabschätzung ein Verfahren zur Sicherstellung und zum Nachweis der Einhaltung gesetzlicher Anforderungen** ist.

Gemäß der DSGVO können bei Nichteinhaltung der DSFA-Anforderungen von der zuständigen Aufsichtsbehörde Bußgelder verhängt werden. Für den Fall, dass keine DSFA durchgeführt wird, obwohl für die Verarbeitung eine solche erforderlich ist (Artikel 35 Absätze 1, 3 und 4), dass eine DSFA nicht ordnungsgemäß durchgeführt wird (Artikel 35 Absätze 2 und 7 bis 9) oder dass die zuständige Aufsichtsbehörde – obwohl vorgeschrieben – nicht konsultiert wird (Artikel 36 Absatz 3 Buchstabe e), kann ein Bußgeld von bis zu 10 Mio. EUR oder, bei einem Unternehmen, von bis zu 2 % des jährlichen weltweiten Gesamtumsatzes des abgelaufenen Geschäftsjahrs verhängt werden, wobei der höhere der beiden Beträge maßgeblich ist.

II. Anwendungsbereich der Leitlinien

Mit diesen Leitlinien wird Folgendem Rechnung getragen:

- Erklärung der Datenschutzgruppe nach Artikel 29 (WP29): 14/EN WP 218[6];
- WP29-Leitlinien für Datenschutzbeauftragte: 16/EN WP 243[7];
- WP29-Stellungnahme zur Zweckbindung: 13/EN WP 203[8];
- internationalen Normen[9].

Entsprechend dem risikobasierten Ansatz der DSGVO ist eine DSFA nicht für alle Verarbeitungsvorgänge obligatorisch. Eine DSFA ist nur dann erforderlich, wenn die Verarbeitung „*wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt*“ (Artikel 35 Absatz 1). Mit Blick auf eine einheitliche Auslegung der Umstände, unter denen eine DSFA obligatorisch ist (Artikel 35 Absatz 3), zielen diese Leitlinien insbesondere darauf ab, dieses Konzept zu präzisieren und Kriterien für die Listen vorzugeben, die von den Datenschutzbehörden gemäß Artikel 35 Absatz 4 anzunehmen sind.

---

[5] Siehe auch Erwägungsgrund 84: „*Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht.*“

[6] Erklärung 14/EN WP 218 der Datenschutzgruppe über die Rolle eines risikobasierten Ansatzes zu den am 30. Mai 2014 angenommenen Rechtsformen des Datenschutzes, angenommen am 30. Mai 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Am 13. Dezember 2016 von der Datenschutzgruppe angenommene Leitlinien für Datenschutzbeauftragte (16/EN WP 243). http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Stellungnahme 3/2013 der Datenschutzgruppe zur Zweckbindung (13/EN WP 203), angenommen am 2. April 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] z. B. ISO 31000:2009, *Risikomanagement – Allgemeine Anleitung zu den Grundsätzen und zur Implementierung eines Risikomanagements*, Internationale Organisation für Normung (ISO); ISO/IEC 29134, *Informationstechnologie – Sicherheitsverfahren – Datenschutz-Folgenabschätzung – Leitfaden*, Internationale Organisation für Normung (ISO).

Nach Artikel 70 Absatz 1 Buchstabe e wird der Europäische Datenschutzausschuss Leitlinien, Empfehlungen und bewährte Verfahren bereitstellen können, mit deren Hilfe eine einheitliche Anwendung der DSGVO gefördert werden soll. Mit diesem Dokument soll die künftige Arbeit dieses Ausschusses erleichtert werden, indem die entsprechenden DSGVO-Bestimmungen erläutert werden, damit die für die Verarbeitung Verantwortlichen gesetzeskonform handeln können und Rechtssicherheit für diejenigen für die Verarbeitung Verantwortlichen geschaffen wird, die eine DSFA durchführen müssen.

Darüber hinaus soll mit diesen Leitlinien die Entwicklung von Folgendem gefördert werden:

- einer unionsweit geltenden Liste der Verarbeitungsvorgänge, für die eine DSFA erforderlich ist (Artikel 35 Absatz 4);
- einer unionsweit geltenden Liste der Verarbeitungsvorgänge, für die keine DSFA erforderlich ist (Artikel 35 Absatz 5);
- gemeinsame Kriterien für die Methodik einer DSFA (Artikel 35 Absatz 5);
- gemeinsame Kriterien für die Festlegung der Umstände, unter denen die Aufsichtsbehörde konsultiert werden muss (Artikel 36 Absatz 1);
- mögliche Empfehlungen auf der Grundlage von in EU-Mitgliedstaaten gesammelten Erfahrungen.

III. Datenschutz-Folgenabschätzung: Erläuterungen zur Verordnung

Nach der DSGVO müssen für die Verarbeitung Verantwortliche geeignete Maßnahmen ergreifen, um sicherzustellen und den Nachweis dafür zu erbringen, dass die Verarbeitung gemäß der DSGVO erfolgt, wobei sie unter anderem die „unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“ (Artikel 24 Absatz 1) berücksichtigen. Die Vorgabe, dass für die Verarbeitung Verantwortliche unter bestimmten Voraussetzungen eine DSFA durchführen müssen, ist vor dem Hintergrund ihrer allgemeinen Pflicht zu verstehen, ein geeignetes Management der Risiken zu betreiben[10], die die Verarbeitung personenbezogener Daten birgt.

Ein „Risiko“ ist ein Szenario mit einem Ereignis und dessen Konsequenzen, das bezüglich seiner Schwere und seiner Eintrittswahrscheinlichkeit beurteilt wird. „Risikomanagement“ lässt sich hingegen als koordinierte Maßnahmen zur Leitung und Kontrolle einer Organisation unter besonderer Berücksichtigung von Risiken definieren.

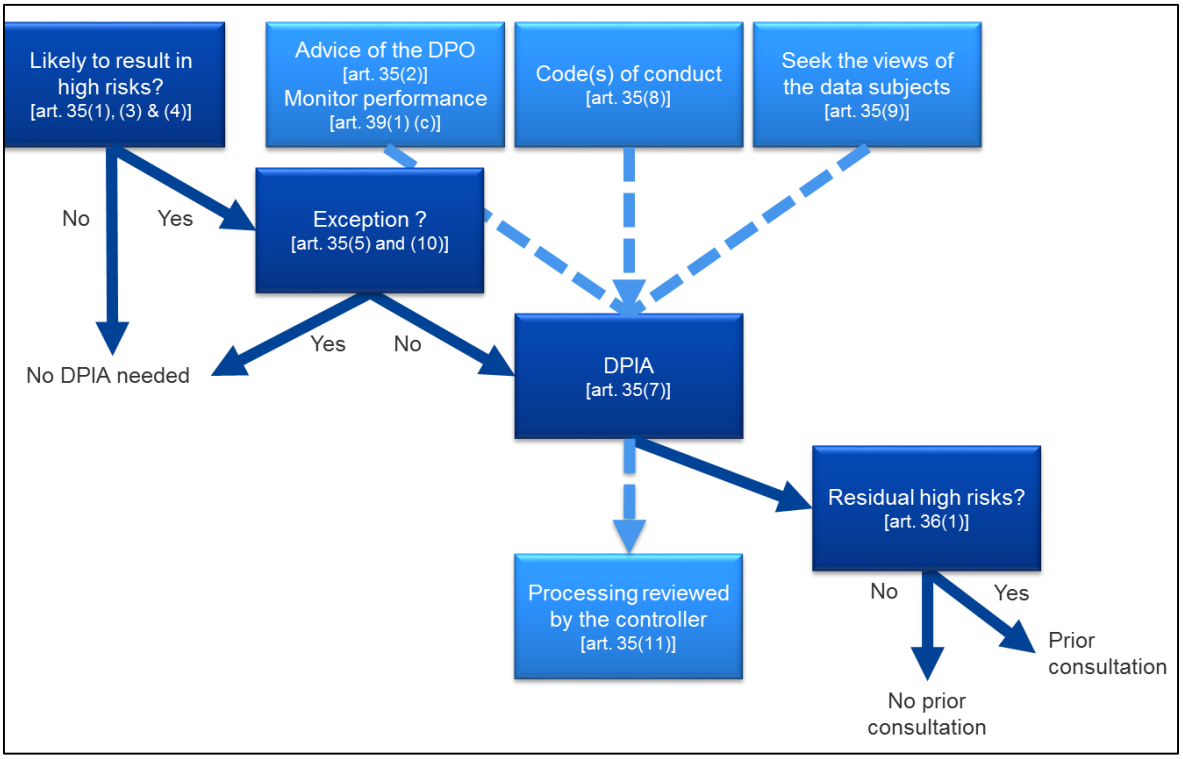
In Artikel 35 ist von einem wahrscheinlich hohen Risiko „für die Rechte und Freiheiten von Personen“ die Rede. Im Sinne der Erklärung der Artikel-29-Datenschutzgruppe zur Rolle eines risikobasierten Ansatzes in rechtlichen Datenschutzrahmenbedingungen beziehen sich „die Rechte und Freiheiten“ von Betroffenen hauptsächlich auf das Recht auf Datenschutz, können sich aber auch auf andere

[10] An dieser Stelle sei darauf hingewiesen, dass zum Management der Risiken für die Rechte und Freiheiten natürlicher Personen gehört, dass diese Risiken ermittelt, analysiert, beurteilt, bewertet und bearbeitet (z. B. gemindert) sowie regelmäßig überprüft werden. Für die Verarbeitung Verantwortliche können sich ihrer Pflicht nicht entziehen, indem sie für diese Risiken Versicherungen abschließen.

Grundrechte wie Rede- und Gedankenfreiheit, Freizügigkeit, Benachteiligungsverbot, Recht auf Freiheit, Gewissens- und Religionsfreiheit erstrecken.

Entsprechend dem risikobasierten Ansatz der DSGVO ist eine DSFA nicht für alle Verarbeitungsvorgänge obligatorisch. Eine DSFA ist nur dann erforderlich, wenn eine Form der Verarbeitung „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“ (Artikel 35 Absatz 1). Dennoch besteht weiter die allgemeine Pflicht der für die Verarbeitung Verantwortlichen zur Durchführung von Maßnahmen, mit denen ein geeignetes Management der Risiken für die Rechte und Freiheiten von Betroffenen möglich ist, selbst wenn keiner der Umstände, unter denen eine DSFA erforderlich ist, vorliegt. In der Praxis bedeutet das, dass für die Verarbeitung Verantwortliche fortlaufend die Risiken bewerten müssen, die ihre Verarbeitungsvorgängen bergen, um erkennen zu können, ob eine Form der Verarbeitung „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“.

In der nachstehenden Grafik sind die Grundsätze der DSFA laut DSGVO veranschaulicht:



A. Was ist Gegenstand einer DSFA? Ein einzelner Verarbeitungsvorgang oder mehrere ähnliche Verarbeitungsvorgänge.

Eine DSFA kann für einen einzelnen Datenverarbeitungsvorgang durchgeführt werden. Nach Artikel 35 Absatz 1 kann jedoch „*für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken [...] eine einzige Abschätzung vorgenommen werden*“. Laut den näheren Ausführungen in Erwägungsgrund 92 kann es „*unter bestimmten Umständen [...] vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen — beispielsweise wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform*

schaffen möchten oder wenn mehrere Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten".

Mit einer einzigen DSFA können zugleich mehrere ähnliche Verarbeitungsvorgänge im Hinblick auf die Art, den Umfang, die Umstände, den Zweck und die Risiken bewertet werden. Da es das Ziel von Datenschutz-Folgenabschätzungen ist, systematisch neue Situationen zu untersuchen, von denen ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen ausgehen könnte, ist eine DSFA für bereits untersuchte Fälle (d. h. für in einem bestimmten Zusammenhang und zu einem bestimmten Zweck durchgeführte Verarbeitungsvorgänge) nicht mehr erforderlich. Dies kann der Fall sein, wenn zur Erfassung derselben Art von Daten zum gleichen Zweck eine ähnliche Technologie zum Einsatz kommt. Beispiel: Verschiedene Gemeindebehörden, die alle eine ähnliche Videoüberwachungsanlage einrichten, könnten eine einzelne DSFA durchführen, mit der dann die Verarbeitung durch die einzelnen Verantwortlichen in allen diesen Behörden abgedeckt ist; oder ein Bahnbetreiber (ein einziger für die Verarbeitung Verantwortlicher) könnte für die Videoüberwachung all seiner Bahnhöfe eine einzige DSFA durchführen. Dies gilt unter Umständen auch für ähnliche Verarbeitungsvorgänge, die von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt werden. In diesen Fällen ist es ratsam, eine Referenz-DSFA gemeinsam zu nutzen bzw. öffentlich zugänglich zu machen; zudem müssen die in der DSFA beschriebenen Maßnahmen umgesetzt und eine Begründung vorgelegt werden, warum eine einzige DSFA ausreichend ist.

Sollten für den fraglichen Verarbeitungsvorgang mehrere Verantwortliche gemeinsam für die Verarbeitung zuständig sein, müssen deren jeweilige Aufgaben genau festgelegt sein. In ihrer DSFA müssen sie angeben, welcher Beteiligte für die verschiedenen Maßnahmen zuständig ist, mit denen die Risiken bearbeitet und die Rechte und Freiheiten der Betroffenen geschützt werden. Jeder für die Datenverarbeitung Verantwortliche muss angeben, was er benötigt, und den anderen Beteiligten hilfreiche Informationen bereitstellen, ohne Geheimnisse (z. B.: Schutz von Betriebsgeheimnissen, von geistigem Eigentum, von vertraulichen Geschäftsinformationen) oder Schwachstellen preiszugeben.

Eine DSFA kann auch von Nutzen sein, wenn die Auswirkungen eines Technologieprodukts auf den Datenschutz untersucht werden sollen, was z. B. der Fall sein kann, wenn ein Hardware- oder Softwareprodukt aller Wahrscheinlichkeit nach von mehreren für die Datenverarbeitung Verantwortlichen für verschiedene Verarbeitungsvorgänge eingesetzt wird. Natürlich ist derjenige für die Datenverarbeitung Verantwortliche, der das Produkt einsetzt, weiterhin zur Durchführung seiner eigenen DSFA unter Berücksichtigung seiner konkreten Umsetzung verpflichtet; dafür können jedoch gegebenenfalls Angaben aus einer vom Produktlieferanten erarbeiteten DSFA verwendet werden. Dieses Szenario wäre beispielsweise bei der Geschäftsbeziehung zwischen einem Hersteller von intelligenten Zählern und Versorgungsunternehmen denkbar. Jeder Produktlieferant und jeder Auftragsverarbeiter sollte den anderen Beteiligten hilfreiche Informationen bereitstellen, ohne Geheimnisse preiszugeben oder durch die Offenlegung von Schwachstellen Sicherheitsrisiken zu verursachen.

B. Welche Verarbeitungsvorgänge werden bei einer Datenschutz-Folgenabschätzung untersucht? (Abgesehen von Ausnahmen, die „*wahrscheinlich ein hohes Risiko mit sich bringen*“.)

Dieser Abschnitt enthält eine Beschreibung der Umstände, unter denen eine DSFA obligatorisch ist, und solche, unter denen auf eine DSFA verzichtet werden kann.

Sofern für den fraglichen Verarbeitungsvorgang keine Ausnahme gilt (III.B.a), muss eine DSFA immer dann durchgeführt werden, wenn ein Verarbeitungsvorgang „*wahrscheinlich ein hohes Risiko mit sich bringt*“ (III.B.b).

a) Wann ist eine DSFA obligatorisch? Wenn die Verarbeitung „*wahrscheinlich ein hohes Risiko mit sich bringt*“.

Datenschutz-Folgenabschätzungen sind laut der DSGVO nicht für alle Verarbeitungsvorgänge vorgeschrieben, bei denen die Möglichkeit eines Risikos für die Rechte und Freiheiten natürlicher Personen besteht. Die Durchführung einer DSFA ist nur dann obligatorisch, wenn die Verarbeitung „*wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt*“ (Artikel 35 Absatz 1), verdeutlicht in Artikel 35 Absatz 3 und ergänzt durch Artikel 35 Absatz 4). Dies gilt insbesondere dann, wenn eine neue Datenverarbeitungstechnologie eingeführt wird[11].

Für den Fall, dass unklar ist, ob eine DSFA erforderlich ist, empfiehlt die WP29-Gruppe dennoch die Durchführung einer DSFA, weil den für die Verarbeitung Verantwortlichen damit ein hilfreiches Instrument für die Einhaltung der Datenschutzgesetze zur Verfügung steht.

Zwar könnte eine DSFA auch in anderen Fällen erforderlich sein, in Artikel 35 Absatz 3 sind jedoch exemplarisch einige Situationen aufgeführt, in denen ein Verarbeitungsvorgang „*wahrscheinlich ein hohes Risiko mit sich bringt*“:

- „*a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen*[12]**;**
- *b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10*[13] *oder*
- *c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche*.“

[11] Weitere Beispiele siehe Erwägungsgründe 89 und 91 sowie Artikel 35 Absätze 1 und 3.

[12] Siehe Erwägungsgrund 71: „*insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen*“.

[13] Siehe Erwägungsgrund 75: „*wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden*“.

Wie aus dem Wort „*insbesondere*“ im Einleitungssatz von Artikel 35 Absatz 3 der DSGVO hervorgeht, ist diese Liste nicht als erschöpfende Aufzählung zu verstehen. Bestimmte Verarbeitungsvorgängen mit „hohen Risiken“, die unter Umständen nicht in der Liste aufgeführt sind, können dennoch ähnlich hohe Risiken bergen. Auch für diese Verarbeitungsvorgänge ist eine DSFA obligatorisch. Aus diesem Grunde gehen die nachstehend dargelegten Kriterien bisweilen über eine einfache Erläuterung dessen hinaus, was unter den drei in Artikel 35 Absatz 3 der DSGVO angeführten Beispielen zu verstehen ist.

Um unter Berücksichtigung der in Artikel 35 Absatz 1 und Artikel 35 Absatz 3 Buchstaben a bis c genannten Elemente, der gemäß Artikel 35 Absatz 4 und den Erwägungsgründen 71, 75 und 91 auf einzelstaatlicher Ebene festzulegenden Liste sowie anderer Bezugnahmen in der DSGVO auf Verarbeitungsvorgänge, die *„wahrscheinlich ein hohes Risiko mit sich bringen“*[14], eine konkretere Menge von Verarbeitungsvorgängen zu ermitteln, für die aufgrund ihres hohen Risikos eine DSFA erforderlich ist, müssen folgende neun Kriterien berücksichtigt werden:

1. Bewerten oder Einstufen, darunter das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von *„Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen“* (Erwägungsgründe 71 und 91). Hierfür seien zur Veranschaulichung folgende drei Beispiele genannt: 1) ein Finanzinstitut, das eine von Kreditauskunfteien betriebene Datenbank, eine im Sinne der Verfahren für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (AML/CTF) eingerichtete Datenbank oder eine Betrugsdatenbank nach seinen Kunden durchsucht, 2) ein Biotechnologie-Unternehmen, das sich zwecks genetischer Tests direkt an Verbraucher wendet, um die Erkrankungs-/Gesundheitsrisiken abschätzen bzw. prognostizieren zu können, 3) ein Unternehmen, das anhand der Nutzung seiner Website bzw. der Navigation der Website durch die Nutzer Verhaltens- oder Marketingprofile erstellt.
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung: Verarbeitung, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „*die Rechtswirkung gegenüber natürlichen Personen entfalten*“ oder diese „*in ähnlich erheblicher Weise beeinträchtigen*“ (Artikel 35 Absatz 3 Buchstabe a). So kann die Verarbeitung beispielsweise zum Ausschluss oder zur Benachteiligung von Personen führen. Verarbeitungsvorgänge, die keine oder wenige Auswirkungen auf Personen haben, erfüllen nicht dieses spezielle Kriterium. Weiterführende Erläuterungen zu diesen Konzepten werden die künftigen WP29-Leitlinien zur Erstellung von Profilen enthalten.
3. Systematische Überwachung: Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und auf beispielsweise über Netzwerke erfasste Daten oder auf „*eine systematische [...] Überwachung öffentlich zugänglicher Bereiche*“ (Artikel 35 Absatz 3 Buchstabe c[15]) zurückgreifen. Diese Form der Überwachung

[14] Siehe z. B. Erwägungsgründe 75, 76, 92, 116.

[15] Die WP29 verwendet „*systematisch*“ in einer oder mehreren der folgenden Bedeutungen (siehe WP29-Leitlinien für Datenschutzbeauftragte: 16/EN WP 243):

- im Rahmen eines Systems stattfindend;
- vorab festgelegt, organisiert oder methodisch;

stellt ein Kriterium dar, weil die personenbezogenen Daten möglicherweise in Situationen erfasst werden, in denen die Betroffenen unter Umständen nicht wissen, wer ihre Daten erfasst und wie die Daten verwendet werden. Darüber hinaus kann es vorkommen, dass die Betroffenen keine Möglichkeit haben, eine solche Verarbeitung ihrer in der Öffentlichkeit (oder in öffentlich zugänglichen Bereichen) erfassten Daten zu verhindern.

4. Vertrauliche Daten oder höchst persönliche Daten: Hierzu zählen besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 (z. B. Informationen über die politischen Meinungen von Einzelpersonen) sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten im Sinne von Artikel 10. Hierfür seien als Beispiele ein allgemeines Krankenhaus genannt, das die Krankenakten seiner Patienten archiviert, oder ein Privatdetektiv, der Akten zu Straftätern führt. Darüber hinaus gibt es weitere Datenkategorien, die zwar nicht in den DSGVO-Bestimmungen aufgeführt sind, jedoch die möglichen Risiken für die Rechte und Freiheiten von Personen erhöhen können. Diese personenbezogenen Daten gelten als vertraulich (im gängigen Sinne des Wortes), da sie mit häuslichen und privaten Aktivitäten verknüpft sind (wie etwa die elektronische Kommunikation, deren Vertraulichkeit geschützt werden muss), sich auf die Ausübung eines der Grundrechte auswirken (wie etwa Standortdaten, deren Erfassung die Freizügigkeit in Frage stellt) oder die Verletzung derselben mit ernsthaften Konsequenzen für den Alltag des Betroffenen einhergeht (wie etwa Finanzdaten, die für den Zahlungsbetrug missbraucht werden könnten). In diesem Zusammenhang kann es von Bedeutung sein, ob die Daten durch den Betroffenen oder durch Dritte bereits öffentlich zugänglich gemacht worden sind. Die öffentliche Zugänglichkeit personenbezogener Daten kann als bestimmender Faktor gelten, wenn beurteilt werden soll, ob eine weitere Nutzung der Daten für bestimmte Zwecke vorgesehen war. In dieses Kriterium können auch Daten wie persönliche Dokumente, E-Mails, Tagebücher, Notizen aus E-Readern mit Notizfunktion sowie über Lifelogging-Anwendungen erfasste, sehr persönliche Informationen fallen.
5. Datenverarbeitung in großem Umfang: Zwar ist „in großem Umfang" in der DSGVO nicht definiert, aber Erwägungsgrund 91 liefert einige Hinweise. In jedem Fall empfiehlt die WP29 die Berücksichtigung speziell folgender Faktoren, wenn ermittelt werden soll, ob die fragliche Verarbeitung in großem Umfang durchgeführt wird[16]:
    a. Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;
    b. verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
    c. Dauer oder Dauerhaftigkeit der Datenverarbeitung;
    d. geografisches Ausmaß der Datenverarbeitung.

- als Teil eines Gesamtplans zur Datenerfassung stattfindend;
- als Teil einer Strategie durchgeführt.

Die WP29 verwendet „*öffentlich zugänglicher Bereich*" in der Bedeutung als Bereich, der jedem Bürger offensteht, wie z. B. ein öffentlicher Platz, ein Einkaufszentrum, eine Straße, ein Marktplatz, ein Bahnhof oder eine öffentliche Bibliothek.

[16] Siehe WP29-Leitlinien für Datenschutzbeauftragte: 16/EN WP 243.

6. Abgleichen oder Zusammenführen von Datensätzen, z. B. solcher Datensätze, die aus zwei oder mehreren Datenverarbeitungsvorgängen stammen, die zu unterschiedlichen Zwecken und/oder von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgeht[17].
7. Daten zu schutzbedürftigen Betroffenen (Erwägungsgrund 75): Die Verarbeitung dieser Art von Daten stellt ein Kriterium dar, weil zwischen den Betroffenen und dem für die Datenverarbeitung Verantwortlichen ein größeres Machtungleichgewicht vorliegt; d. h. den Personen ist es unter Umständen nicht ohne Weiteres möglich, der Verarbeitung ihrer Daten zuzustimmen bzw. zu widersprechen oder ihre Rechte auszuüben. Als schutzbedürftige Betroffene gelten beispielsweise folgende Bevölkerungsgruppen: Kinder (bei ihnen kann nicht davon ausgegangen werden, dass sie in der Lage sind, der Verarbeitung ihrer Daten wissentlich und überlegt zu widersprechen bzw. zuzustimmen), Arbeitnehmer, Teile der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber, Senioren, Patienten *usw*.) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des für die Verarbeitung Verantwortlichen vorliegt.
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen, wie etwa die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle *usw*. Aus der DSGVO (Artikel 35 Absatz 1 und Erwägungsgründe 89 und 91) wird deutlich, dass der Einsatz einer neuen Technologie, die „*entsprechend dem jeweils aktuellen Stand der Technik*“ (Erwägungsgrund 91) als solche einzuordnen ist, der Grund für die Notwendigkeit einer DSFA sein kann. Das liegt daran, dass der Einsatz einer solchen Technologie mit neuartigen Formen der Datenerfassung und -nutzung einhergehen kann, was möglicherweise ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringt. Schließlich sind die persönlichen und gesellschaftlichen Folgen, die der Einsatz einer neuen Technologie haben kann, kaum absehbar. Kann ein für die Datenverarbeitung Verantwortlicher auf eine DSFA zurückgreifen, kann er diese Risiken besser verstehen und bearbeiten. Beispielsweise könnten sich einige Anwendungen des „Internet der Dinge“ erheblich auf den Alltag und das Privatleben von Personen auswirken und somit eine DSFA obligatorisch machen.
9. Fälle, in denen die Verarbeitung an sich *„die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“* (Artikel 22 und Erwägungsgrund 91). Hierzu zählen Verarbeitungsvorgänge, mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrags gestattet, geändert oder verwehrt werden soll. Hierfür sei als Beispiel eine Bank genannt, die eine von Kreditauskunfteien betriebene Datenbank nach ihren Kunden durchsucht, um über Kreditvergaben zu entscheiden.

Erfüllt ein Verarbeitungsvorgang zwei dieser Kriterien, muss der für die Datenverarbeitung Verantwortliche in den meisten Fällen zu dem Schluss kommen, dass eine DSFA obligatorisch ist. Nach Auffassung der WP29 nimmt die Wahrscheinlichkeit, dass ein Verarbeitungsvorgang ein hohes Risiko für die Rechte und Freiheiten von Betroffenen mit sich bringt und somit eine DSFA

[17] Siehe Erläuterungen in der WP29-Stellungnahme zur Zweckbindung: 13/EN WP 203, S. 24;

erforderlich ist (und zwar unabhängig von den Maßnahmen, die der für die Verarbeitung Verantwortliche ins Auge fasst), im Allgemeinen immer weiter zu, je mehr Kriterien dieser Vorgang erfüllt.

In einigen Fällen kann es jedoch vorkommen, dass **ein für die Datenverarbeitung Verantwortlicher von der Notwendigkeit einer DSFA ausgehen muss, obwohl der fragliche Verarbeitungsvorgang nur eines dieser Kriterien erfüllt.**

Die folgenden Beispiele sollen veranschaulichen, wie die Kriterien zu verwenden sind, wenn es darum geht, die Notwendigkeit einer DSFA für einen bestimmten Verarbeitungsvorgang zu ermitteln:

Beispiele für Verarbeitungsvorgänge	**Ggf. maßgebliche Kriterien**	**Notwendigkeit einer DSFA wahrscheinlich?**
Ein Krankenhaus verarbeitet die genetischen und medizinischen Daten seiner Patienten (Krankenhausinformationssystem).	- vertrauliche Daten oder höchst persönliche Daten - Daten zu schutzbedürftigen Betroffenen - Datenverarbeitung in großem Umfang	Ja
Ein Kamerasystem wird zur Überwachung des Fahrverhaltens auf Schnellstraßen eingesetzt. Zur Identifizierung einzelner Fahrzeuge und automatischen Erkennung von Nummernschildern plant der für die Verarbeitung Verantwortliche den Einsatz eines intelligenten Videoanalysesystems.	- systematische Überwachung - innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen	
Ein Unternehmen überwacht systematisch die Tätigkeiten seiner Angestellten, so auch deren Arbeitsplatzrechner, ihre Internetnutzung *usw*.	- systematische Überwachung - Daten zu schutzbedürftigen Betroffenen	
Aus sozialen Netzwerken werden öffentlich zugängliche Daten erfasst, um daraus Profile zu erstellen.	- Bewerten oder Einstufen - Datenverarbeitung in großem Umfang - Abgleichen oder Zusammenführen von Datensätzen - vertrauliche Daten oder höchst persönliche Daten	
Ein Institut erstellt eine Bonitäts- oder Betrugsdatenbank auf nationaler Ebene.	- Bewerten oder Einstufen - automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung - Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert. - vertrauliche Daten oder höchst persönliche Daten	
Zu Archivierungszwecken werden	- vertrauliche Daten	

Beispiele für Verarbeitungsvorgänge	Ggf. maßgebliche Kriterien	Notwendigkeit einer DSFA wahrscheinlich?
pseudonymisierte personenbezogene vertrauliche Daten zu schutzbedürftigen Betroffenen gespeichert, die an Forschungsprojekten bzw. klinischen Studien teilgenommen haben	- Daten zu schutzbedürftigen Betroffenen - Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert.	
Es werden „personenbezogene Daten von Patienten oder von Mandanten [verarbeitet, wobei die Verarbeitung] durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt“ (Erwägungsgrund 91).	- vertrauliche Daten oder höchst persönliche Daten - Daten zu schutzbedürftigen Betroffenen	Nein
Ein Online-Magazin verwendet eine Verteilerliste, um seinen Abonnenten eine tägliche allgemeine Übersicht zu schicken.	- Datenverarbeitung in großem Umfang	
Ein Online-Händler schaltet auf seiner Website Werbeanzeigen für Oldtimer-Ersatzteile, für die eine Profilerstellung auf der Grundlage von Produkten zum Einsatz kommt, die der Nutzer auf der Website des Online-Händlers angesehen oder gekauft hat.	- Bewerten oder Einstufen	

Andererseits kann es vorkommen, dass ein für die Verarbeitung Verantwortlicher einen Verarbeitungsvorgang, der den vorgenannten Fällen entspricht, nicht als Vorgang bewertet, der „wahrscheinlich ein hohes Risiko mit sich bringt“. In einem solchen Fall muss der für die Verarbeitung Verantwortliche begründen und dokumentieren, warum er keine DSFA durchführt, und den Standpunkt des Datenschutzbeauftragten mit einbeziehen bzw. festhalten.

Darüber hinaus muss jeder für die Datenverarbeitung Verantwortliche im Rahmen des Grundsatzes der Rechenschaftspflicht „*ein Verzeichnis aller Verarbeitungstätigkeiten [führen], die [seiner] Zuständigkeit unterliegen*“, wobei ein solches Verzeichnis unter anderem die Zwecke der Verarbeitung, eine Beschreibung der Datenkategorien und die Empfänger der Daten und „*wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1*“ enthalten muss (Artikel 30 Absatz 1), und beurteilen, ob ein hohes Risiko wahrscheinlich ist, selbst wenn letztlich gegen die Durchführung einer DSFA entschieden wird.

Anmerkung: Aufsichtsbehörden müssen eine Liste der Verarbeitungsvorgänge erstellen, für die eine DSFA durchzuführen ist, diese Liste veröffentlichen und dem Europäischen Datenschutzausschuss übermitteln (Artikel 35 Absatz 4)[18]. Die oben genannten Kriterien können den Aufsichtsbehörden bei

[18] In diesem Zusammenhang „*wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren*

der Erstellung einer solchen Liste als Orientierungshilfe dienen, wobei mit der Zeit ggf. weitere Einzelheiten hinzugefügt werden. So könnte beispielsweise auch die Verarbeitung jeder Art von biometrischen Daten oder von Daten über Kinder für die Erstellung einer Liste nach Artikel 35 Absatz 4 von Bedeutung sein.

b) Wann ist keine Datenschutz-Folgenabschätzung erforderlich? Wenn die Verarbeitung „*wahrscheinlich kein hohes Risiko mit sich bringt*" oder eine ähnliche DSFA bereits vorhanden ist oder wenn die Verarbeitung vor Mai 2018 genehmigt wurde, auf einer Rechtsgrundlage beruht oder in der Liste der Verarbeitungsvorgänge aufgeführt ist, für die keine DSFA erforderlich ist.

Nach Ansicht der WP29 ist in folgenden Fällen keine DSFA erforderlich:

- **wenn die Verarbeitung „*wahrscheinlich [kein] hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt*"** (Artikel 35 Absatz 1);
- **wenn sich die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung von denen einer anderen Verarbeitung, für die bereits eine DSFA durchgeführt wurde, nur in geringem Maße unterscheiden**. In diesen Fällen können die DSFA-Ergebnisse einer solchen ähnlichen Verarbeitung verwendet werden (Artikel 35 Absatz 1[19]);
- wenn die Verarbeitungsvorgänge vor Mai 2018 von einer Aufsichtsbehörde unter bestimmten Bedingungen geprüft worden sind, die sich nicht geändert haben[20] (siehe III.C);
- **falls ein Verarbeitungsvorgang** gemäß Artikel 6 Absatz 1 Buchstabe c oder e **auf einer Rechtsgrundlage** im Unionsrecht oder im Recht der Mitgliedstaaten beruht und diese Rechtsvorschrift den konkreten Verarbeitungsvorgang regelt **und falls bereits im Rahmen der Schaffung dieser Rechtsgrundlage eine DSFA erfolgte** (Artikel 35 Absatz 10)[21], es sei denn, ein Mitgliedstaat erklärt, dass es notwendig ist, vor den fraglichen Verarbeitungstätigkeiten eine DSFA durchzuführen;
- **falls der Verarbeitungsvorgang auf einer (von der Aufsichtsbehörde erstellten) optionalen Liste der Verarbeitungsvorgänge aufgeführt ist**, für die keine DSFA erforderlich ist (Artikel 35 Absatz 5). Eine solche Liste kann Verarbeitungstätigkeiten enthalten, die die Voraussetzungen dieser Behörde erfüllen, die sie insbesondere in Form von Leitlinien, besonderen Beschlüssen oder Genehmigungen, Konformitätsvorschriften *usw*. festgelegt haben (z. B. in Frankreich, Genehmigungen, Befreiungen, vereinfachte

---

Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten" (Artikel 35 Absatz 6).

[19] „*Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.*"

[20] „*Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden*" (Erwägungsgrund 171).

[21] Wird zum Zeitpunkt der Ausarbeitung der Rechtsvorschrift, die eine Rechtsgrundlage für einen Verarbeitungsvorgang liefert, eine DSFA durchgeführt, muss vor der Umsetzung wahrscheinlich eine erneute Prüfung erfolgen, da die erlassene Rechtsvorschrift hinsichtlich der Datenschutzfragen vom eingereichten Antrag abweichen kann. Darüber hinaus ist es möglich, dass zum Zeitpunkt des Erlassens der Rechtsvorschrift nicht genügend technische Einzelheiten bezüglich der tatsächlichen Verarbeitung zur Verfügung standen, selbst wenn eine DSFA beigefügt wurde. In einem solchen Fall kann vor der Durchführung der eigentlichen Verarbeitungstätigkeiten dennoch eine DSFA erforderlich sein.

Vorschriften, Konformitätspakete…). In solchen Fällen, die einer Überprüfung durch die zuständige Aufsichtsbehörde unterliegen, ist nur dann keine DSFA erforderlich, wenn die Verarbeitung genau einem Geltungsbereich des jeweils in der Liste aufgeführten Verfahrens entspricht und weiterhin ausnahmslos alle zutreffenden Voraussetzungen der DSGVO erfüllt.

C. Wie ist der Sachverhalt bei schon laufenden Verarbeitungsvorgängen? Unter bestimmten Umständen ist auch dafür eine DSFA erforderlich.

Eine DSFA muss für bereits laufende Verarbeitungsvorgänge durchgeführt werden, wenn diese wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen und wenn sich deren Risiken im Hinblick auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung geändert haben.

Für Verarbeitungsvorgänge, die von einer Aufsichtsbehörde oder dem Datenschutzbeauftragten gemäß Artikel 20 der Richtlinie 95/46/EG geprüft wurden und noch immer auf dieselbe Art durchgeführt werden wie bei der Vorabkontrolle, ist keine DSFA erforderlich. So bleiben „*auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden [...] in Kraft, bis sie geändert, ersetzt oder aufgehoben werden*“ (Erwägungsgrund 171).

Umgekehrt bedeutet das aber auch, dass jede Datenverarbeitung, deren Durchführungsbedingungen (Umfang, Zweck, erfasste personenbezogene Daten, Identität der für die Verarbeitung Verantwortlichen oder der Empfänger, Datenspeicherfrist, technische und organisatorische Maßnahmen usw.) sich seit der Vorabkontrolle durch die Aufsichtsbehörde oder den Datenschutzbeauftragten geändert haben und die wahrscheinlich ein hohes Risiko mit sich bringen, einer DSFA unterzogen werden muss.

Zudem könnte eine DSFA erforderlich werden, wenn sich die Risiken aus den Verarbeitungsvorgängen geändert haben[22], z. B. weil inzwischen eine neue Technologie zum Einsatz gekommen ist oder weil die Verwendung personenbezogener Daten zu einem anderen Zweck erfolgt. Datenverarbeitungsvorgänge können einer raschen Weiterentwicklung unterliegen, auch können neue Sicherheitslücken entstehen. Aus diesem Grunde sei darauf hingewiesen, dass die Überprüfung einer DSFA nicht nur für die kontinuierliche Verbesserung von Vorteil ist, sondern auch entscheidend dazu beitragen kann, das Datenschutzniveau in einem sich wandelnden Umfeld langfristig aufrechtzuerhalten. Ein weiterer Anlass für die Notwendigkeit einer DSFA können auch Veränderungen des für die Verarbeitung geltenden organisatorischen oder gesellschaftlichen Rahmens sein, z. B. weil die Auswirkungen bestimmter automatisierter Entscheidungen eine größere Tragweite erlangt haben oder weil für neue Kategorien betroffener Personen das Risiko für Benachteiligungen gestiegen ist. Jedes dieser Beispiele könnte einen Sachverhalt darstellen, der eine Veränderung des Risikos nach sich zieht, das von der fraglichen Verarbeitungstätigkeit ausgeht.

[22] Je nach Kontext die erfassten Daten, Zwecke, Funktionalitäten, verarbeitete personenbezogene Daten, Empfänger, Datenkombinationen, Risiken (stützende Sachvermögen, Risikoquellen, mögliche Folgen, Bedrohungen *usw.*), Sicherheitsmaßnahmen und internationaler Datenverkehr.

Umgekehrt könnte das Risiko durch andere Arten von Veränderungen auch gesenkt werden. So könnte ein Verarbeitungsvorgang beispielsweise einer Weiterentwicklung unterzogen werden, so dass Entscheidungen nicht länger automatisiert erfolgen oder dass ein Überwachungsvorgang nicht länger systematischer Natur ist. In einem solchen Fall kann die Überprüfung der Risikoanalyse ergeben, dass die Durchführung einer DSFA nicht mehr erforderlich ist.

Im Sinne einer guten Praxis **sollte eine DSFA kontinuierlich überprüft und regelmäßig erneuert werden.** Aus diesem Grunde sollte ein für die Verarbeitung Verantwortlicher im Rahmen seiner allgemeinen Rechenschaftspflichten zu gegebener Zeit auch dann eine DSFA durchführen, wenn eine solche ab dem 25. Mai 2018 nicht obligatorisch ist.

D. Wie wird eine Datenschutz-Folgenabschätzung durchgeführt?

a) Zu welchem Zeitpunkt sollte eine Datenschutz-Folgenabschätzung durchgeführt werden? Vor der fraglichen Verarbeitung.

Die DSFA ist „*vor den betreffenden Verarbeitungstätigkeiten*“ durchzuführen (Artikel 35 Absatz 1 und Artikel 35 Absatz 10, Erwägungsgründe 90 und 93)[23]. Dies steht im Einklang mit den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 und Erwägungsgrund 78). Die DSFA sollte als Instrument angesehen werden, mit dem die Entscheidungsfindung in Fragen der Verarbeitung vereinfacht wird.

Die DSFA muss zum frühestmöglichen Zeitpunkt bereits in der Entwicklungsphase der Verarbeitungstätigkeiten begonnen werden, selbst wenn einige der Verarbeitungsvorgänge noch nicht bekannt sind. Durch die ständige Aktualisierung der DSFA über den gesamten Lebenszyklus des Projekts hinweg wird nicht nur gewährleistet, dass der Datenschutz die gebührende Beachtung findet, sondern auch angeregt, dass Lösungen zur Einhaltung geltender Vorschriften entwickelt werden. Im Verlauf der Entwicklung kann es auch erforderlich werden, dass einzelne Schritte der Datenschutz-Folgenabschätzung wiederholt werden müssen, da die Schwere bzw. Eintrittswahrscheinlichkeit der Risiken, die die Verarbeitung mit sich bringen, unter Umständen durch die Wahl bestimmter technischer oder organisatorischer Maßnahmen beeinflusst werden.

Die Möglichkeit, dass die DSFA nach erfolgreichem Start der Verarbeitung aktualisiert werden muss, stellt keinen triftigen Grund dar, die betreffende DSFA zu verschieben oder nicht durchzuführen. Bei der DSFA handelt es sich um einen fortlaufenden Prozess, was umso mehr für den Fall gilt, dass der fragliche Verarbeitungsvorgang dynamisch ist und ständigen Veränderungen unterliegt. **Die Durchführung einer DSFA ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess**.

[23] Eine Ausnahme hierzu stellen bereits laufende Verarbeitungsvorgänge dar, die vorab von der Aufsichtsbehörde geprüft wurden. In diesem Fall muss eine DSFA nur dann durchgeführt werden, wenn maßgebliche Veränderungen geplant sind.

b) Wer muss eine Datenschutz-Folgenabschätzung durchführen? Der für die Verarbeitung Verantwortliche in Zusammenarbeit mit dem Datenschutzbeauftragten und den Auftragsverarbeitern.

Der für die Verarbeitung Verantwortliche muss dafür sorgen, dass die DSFA durchgeführt wird (Artikel 35 Absatz 2). Die eigentliche Durchführung der DSFA kann durch eine andere Person erfolgen, entweder unternehmensintern oder per Auslagerung; der für die Verarbeitung Verantwortliche ist jedoch derjenige, der letztlich zur Rechenschaft verpflichtet ist.

Der für die Verarbeitung Verantwortliche muss darüber hinaus den Rat des Datenschutzbeauftragten einholen, sofern ein solcher benannt wurde (Artikel 35 Absatz 2). Dieser Rat und auch die Entscheidungen, die von dem für die Verarbeitung Verantwortlichen getroffen werden, müssen in der DSFA dokumentiert werden. Der Datenschutzbeauftragte ist außerdem für die Überwachung der Durchführung der DSFA zuständig (Artikel 39 Absatz 1 Buchstabe c). Nähere Erläuterungen hierzu enthalten die WP29-Leitlinien für Datenschutzbeauftragte: 16/EN WP 243.

Erfolgt die Verarbeitung ganz oder teilweise durch einen Auftragsverarbeiter, **muss dieser den für die Datenverarbeitung Verantwortlichen bei der Durchführung der DSFA unterstützen** und erforderliche Informationen zur Verfügung stellen (im Sinne von Artikel 28 Absatz 3 Buchstabe f).

„***Gegebenenfalls***" **holt der für die Verarbeitung Verantwortliche „*den Standpunkt der betroffenen Personen oder ihrer Vertreter*" ein (Artikel 35 Absatz 9)**. Die WP29-Gruppe ist der Auffassung, dass:

- die Einholung dieses Standpunkts auf verschiedensten Wegen erfolgen kann – und zwar je nachdem, welcher Kontext vorliegt (z. B. eine generische Studie zu Zweck und Mitteln der Verarbeitung, eine Frage an die Arbeitnehmervertreter oder gewöhnliche Umfragen, die an die potenziellen Kunden des für die Datenverarbeitung Verantwortlichen gesendet werden) und ob sich der Verantwortliche auf eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen einer solchen Kommunikation stützen kann. Es sei jedoch darauf hingewiesen, dass die Zustimmung zur Verarbeitung offenkundig keinen dieser Wege zur Einholung des Standpunkts der Betroffenen darstellt;
- sofern die endgültige Entscheidung des für die Datenverarbeitung Verantwortlichen vom Standpunkt der Betroffenen abweichen sollte, müssen die Gründe für das weitere Fortfahren dokumentiert werden;
- der für die Verarbeitung Verantwortliche muss zudem seine Begründung für den Verzicht auf die Einholung des Standpunkts der Betroffenen dokumentieren, nämlich wenn er eine solche Einholung für nicht angemessen hält, weil sie z. B. eine Verletzung der Geheimhaltungspflichten bezüglich der Geschäftspläne des Unternehmens darstellen würde oder unverhältnismäßig bzw. impraktikable wäre.

Schließlich hat es sich bewährt, je nach unternehmensinternen Richtlinien, Verfahren und Regeln weitere spezielle Rollen und Zuständigkeiten festzulegen und zu dokumentieren. Im Folgenden seien einige Beispiele genannt:

- Wenn bestimmte Abteilungen die Durchführung einer DSFA vorschlagen, müssen diese Abteilungen Informationen bereitstellen, die für die DSFA erforderlich sind, und sich am DSFA-Validierungsverfahren beteiligen.

- Gegebenenfalls empfiehlt es sich, den Rat unabhängiger Spezialisten verschiedener Berufsgruppen einzuholen[24] (Anwälte, IT-Experten, Sicherheitsexperten, Soziologen, Ethiker *usw*.).
- Die Rollen und Zuständigkeiten der Auftragsverarbeiter müssen vertraglich festgehalten werden. Die DSFA muss mit Unterstützung des Auftragsverarbeiters unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen durchgeführt werden (Artikel 28 Absatz 3 Buchstabe f).
- Der leitende Beauftragte für Informationssicherheit, sofern ein solcher benannt ist, und der Datenschutzbeauftragte könnten den Vorschlag unterbreiten, dass der für die Verarbeitung Verantwortliche eine DSFA für einen bestimmten Verarbeitungsvorgang durchführt und den Beteiligten bezüglich der Methodik zur Seite steht, zudem bei der Qualitätsbewertung der Risikoabschätzung und bei der Beantwortung der Frage hilft, ob das Restrisiko hinnehmbar ist, sich aber auch bei der Erarbeitung von Wissen einbringt, das speziell den Bereich des für die Datenverarbeitung Verantwortlichen betrifft.
- Der leitende Beauftragte für Informationssicherheit, sofern ein solcher benannt ist, und/oder die IT-Abteilung sollten den für die Datenverarbeitung Verantwortlichen unterstützen und könnten, je nach Sicherheits- oder Betriebserfordernissen, die Durchführung einer DSFA für einen bestimmten Verarbeitungsvorgang vorschlagen.

c) Welche Methodik liegt einer Datenschutz-Folgenabschätzung zugrunde? Verschiedene Methodiken, aber gemeinsame Kriterien.

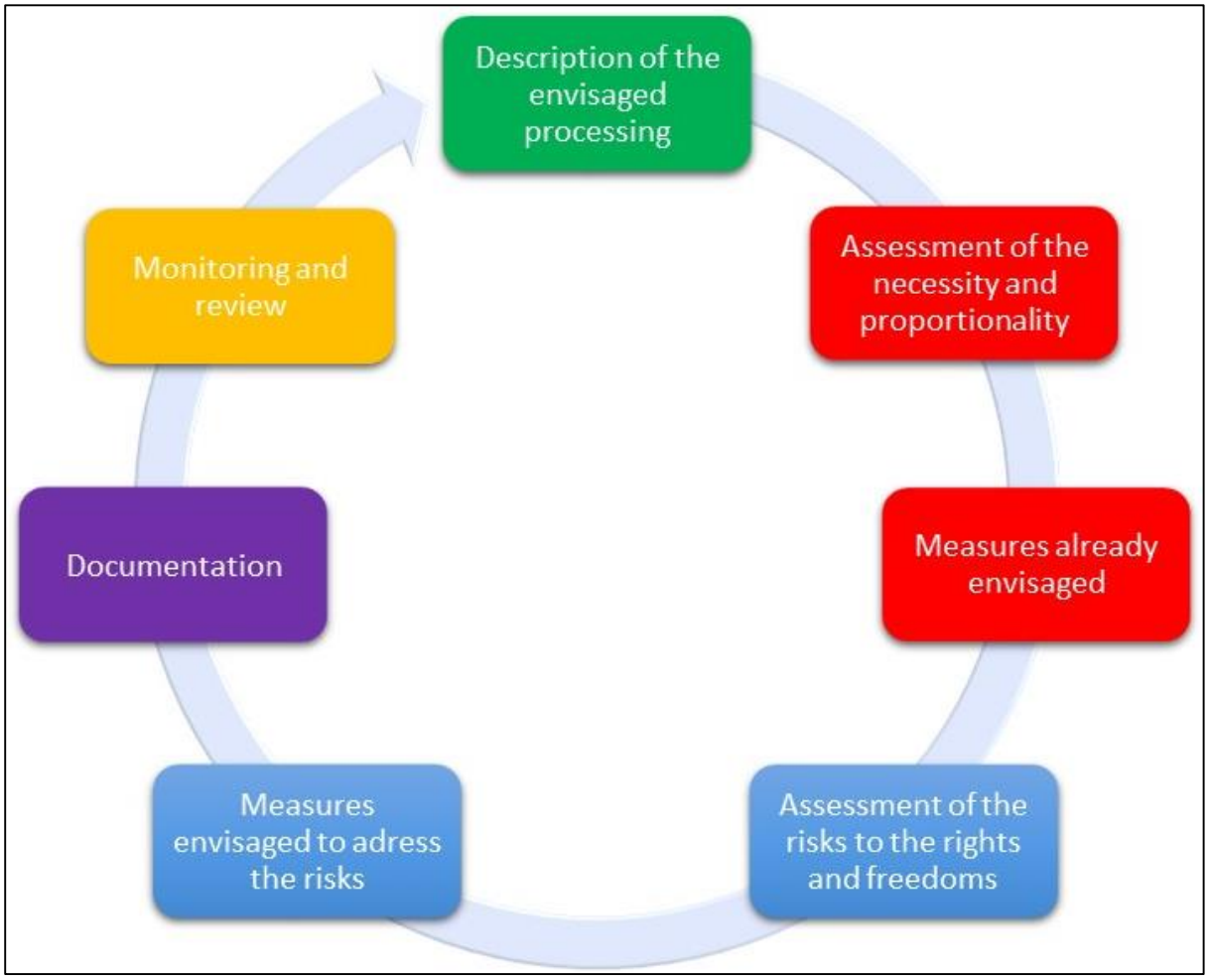
In der DSGVO sind die Elemente festgelegt, die in einer DSFA mindestens enthalten sein müssen (Artikel 35 Absatz 7 und Erwägungsgründe 84 und 90):

- „*eine Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung*“;
- „*eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge*“;
- „*eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen*“;
- *die Maßnahmen, mit denen Folgendes erreicht werden soll:*
    - „*Bewältigung der Risiken*“*;*
    - „*Nachweis dafür [...], dass diese Verordnung eingehalten wird*“.

In der nachstehenden Grafik ist das generische Iterationsverfahren für die Durchführung einer DSFA veranschaulicht[25]:

[24] *Empfehlungen für einen Rahmen für Datenschutz-Folgenabschätzungen für die Europäische Union, Ergebnis D3:*
http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

[25] Das hier dargestellte Verfahren ist iterativ: In der Praxis werden die einzelnen Phasen sicherlich mehrere Male durchlaufen, bevor die DSFA abgeschlossen werden kann.



Bei der Folgenabschätzung für einen Datenverarbeitungsvorgang ist die Einhaltung von Verhaltensregeln (Artikel 40) zu berücksichtigen (Artikel 35 Absatz 8). Dies kann bei der Erbringung eines Nachweises darüber hilfreich sein, dass geeignete Maßnahmen beschlossen oder umgesetzt wurden, vorausgesetzt, dass die Verhaltensregeln für den Verarbeitungsvorgang zweckmäßig sind. Auch sollten Zertifizierungen, Siegel und Prüfzeichen Berücksichtigung finden, die dem Nachweis darüber dienen, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird (Artikel 42), ebenso wie verbindliche interne Datenschutzvorschriften.

Die Gesamtheit aller einschlägigen Vorschriften der DSGVO bildet einen umfassenden Allgemeinrahmen für die Entwicklung und Durchführung einer DSFA. Für die eigentliche Durchführung einer DSFA gelten die Vorschriften der DSGVO, die gegebenenfalls um eine weitere Einzelheiten umfassende praktische Orientierungshilfe ergänzt werden können. Das heißt also, dass die DSFA-Durchführung skalierbar ist. Somit kann auch der Auftragsverarbeiter einer kleinen Organisation eine für die jeweiligen Verarbeitungsvorgänge geeignete DSFA erarbeiten und durchführen.

In Erwägungsgrund 90 der DSGVO sind einige Komponenten der DSFA aufgezeigt, die sich mit den genau abgegrenzten Komponenten des Risikomanagements (z. B. laut ISO 31000[26]) überschneiden. Im Sinne des Risikomanagements wird mit einer DSFA das Ziel verfolgt, unter Anwendung folgender Prozesse „Risiken zu steuern", die für die Rechte und Freiheiten natürlicher Personen bestehen:

- Ermitteln der Rahmenbedingungen: „*unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos*";
- Abschätzen der Risiken: „*die spezifische Eintrittswahrscheinlichkeit und die Schwere des hohen Risikos bewerten*";
- Behandeln der Risiken: durch die „*dieses Risiko eingedämmt*" und „*der Schutz personenbezogener Daten sichergestellt*" und „*die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen*" werden soll.

Anmerkung: Die DSFA im Sinne der DSGVO ist ein Instrument für das Management von Risiken, die für die Rechte der betroffenen Personen bestehen, und wird demnach in bestimmten Bereichen aus deren Perspektive behandelt (z. B. gesellschaftliche Sicherheit). In anderen Bereichen wiederum (z. B. Informationssicherheit) liegt der Schwerpunkt des Risikomanagements auf der Organisation.

Die DSGVO lässt den für die Datenverarbeitung Verantwortlichen die nötige Flexibilität zur Festlegung der genauen Struktur und Form der DSFA, damit sie möglichst nahtlos in die bestehenden Arbeitsabläufe integriert werden kann. Auf Ebene der EU und auf internationaler Ebene wurde eine Vielzahl verschiedener Prozesse erarbeitet, die den in Erwägungsgrund 90 beschriebenen Komponenten Rechnung tragen. Unabhängig von ihrer Form muss es sich bei einer DSFA jedoch um eine echte Risikoabschätzung handeln, auf deren Grundlage die für die Verarbeitung Verantwortlichen Abhilfemaßnahmen ergreifen können.

Zur Erfüllung der Grundvoraussetzungen gemäß DSGVO könnten verschiedene Methodiken zur Anwendung kommen (Beispiele zu Methodiken für die Datenschutz-Folgenabschätzung siehe Anhang 1). Damit diese verschiedenen Ansätze parallel bestehen können und es den für die Verarbeitung Verantwortlichen dennoch möglich ist, der DSGVO zu entsprechen, wurden allgemeine Kriterien aufgestellt (siehe Anhang 2). Einerseits sind darin die Grundvoraussetzungen der Verordnung klar umrissen, andererseits lassen sie jedoch auch genügend Spielraum für verschiedene Formen der Durchführung. Anhand der Kriterien lässt sich nachweisen, dass eine bestimmte DSFA-Methodik die Standards laut DSGVO-Anforderungen erfüllt. **Zwar ist die Wahl einer Methodik Sache des für die Verarbeitung Verantwortlichen, dieser muss jedoch beachten, dass die Kriterien gemäß Anhang 2 erfüllt sind**.

Die WP29-Gruppe spricht sich für die Erarbeitung branchenspezifischer DSFA-Rahmenbedingungen aus. Grund dafür ist, dass so auf Branchenkenntnisse zurückgegriffen und in der DSFA auf die Besonderheiten einer bestimmten Art von Verarbeitungsvorgängen eingegangen werden kann (z. B.: bestimmte Datentypen, Gesellschaftsvermögen, potenzielle Folgen, Bedrohungen, Maßnahmen). Das bedeutet, dass in der DSFA die Fragen behandelt werden können, die in einem bestimmten

[26] Risikomanagementprozesse: Mitteilung und Abstimmung, Ermittlung der Rahmenbedingungen, Risikoabschätzung, Risikobehandlung, Überwachung und Überprüfung (siehe Begriffe und Definitionen sowie das Inhaltsverzeichnis der ISO 31000 als Vorschau: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

Wirtschaftssektor, bei der Nutzung bestimmter Technologien oder bei der Durchführung bestimmter Arten von Verarbeitungsvorgängen auftreten.

Erforderlichenfalls *„führt der Verantwortliche eine [abschließende] Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind"* (Artikel 35 Absatz 11[27]).

d) Ist die Veröffentlichung der Datenschutz-Folgenabschätzung obligatorisch? Nein, aber mit der Veröffentlichung einer Zusammenfassung könnte das Vertrauen gestärkt werden. Zudem muss der Aufsichtsbehörde im Falle einer vorherigen Konsultation oder auf Verlangen der Datenschutzbehörde die vollständige DSFA übermittelt werden.

Laut DSGVO ist die Veröffentlichung einer DSFA kein rechtliches Erfordernis, sondern liegt in der Entscheidung des für die Verarbeitung Verantwortlichen. Dieser sollte jedoch zumindest die Veröffentlichung von Teilen der DSFA, wie etwa einer Zusammenfassung oder der Ergebnisse, in Betracht ziehen.

Ziel eines solchen Prozesses wäre es, das Vertrauen in die Verarbeitungsvorgänge des für die Verarbeitung Verantwortlichen zu stärken, die Übernahme von Verantwortung zu demonstrieren und Transparenz zu schaffen. Besonders bewährt hat sich eine Veröffentlichung der DSFA in Fällen, in denen Bürger von der Verarbeitung betroffen sind. Dies würde beispielsweise zutreffen, wenn eine staatliche Behörde eine DSFA durchführt.

Die veröffentlichte DSFA muss nicht die gesamte Folgenabschätzung umfassen, besonders wenn die DSFA bestimmte Informationen über Sicherheitsrisiken für den für die Datenverarbeitung Verantwortlichen oder Betriebsgeheimnisse bzw. vertrauliche Geschäftsinformationen enthalten könnte. In einem solchen Fall könnte die veröffentlichte Fassung nur aus einer Zusammenfassung der zentralen Ergebnisse der DSFA oder sogar nur aus einer Erklärung darüber bestehen, dass eine DSFA durchgeführt wurde.

Darüber hinaus muss der für die Datenverarbeitung Verantwortliche, sofern eine DSFA hohe Restrisiken birgt, vor der Verarbeitung die Aufsichtsbehörde konsultieren (Artikel 36 Absatz 1). Im Rahmen dessen muss die DSFA in ihrer Gesamtheit vorgelegt werden (Artikel 36 Absatz 3 Buchstabe e). Die Aufsichtsbehörde bietet gegebenenfalls ihre Beratungsdienste an[28], gibt aber gemäß den Grundsätzen, die in den einzelnen Mitgliedstaaten hinsichtlich des Zugangs der Öffentlichkeit zu offiziellen Dokumenten gelten, weder Betriebsgeheimnisse noch Sicherheitsrisiken preis.

[27] Nach Artikel 35 Absatz 10 wird ausdrücklich nur die Anwendung von Artikel 35 Absätze 1 bis 7 ausgeschlossen.

[28] Empfehlungen für den für die Verarbeitung Verantwortlichen in Schriftform sind nur dann erforderlich, wenn die geplante Verarbeitung nach Auffassung der Aufsichtsbehörde nicht mit der Verordnung gemäß Artikel 36 Absatz 2 im Einklang steht.

E. Wann muss die Aufsichtsbehörde konsultiert werden? Bei hohen Restrisiken.

Wie bereits zuvor erwähnt,

- ist eine DSFA erforderlich, wenn ein Verarbeitungsvorgang „*wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt*“ (Artikel 35 Absatz 1, siehe III.B.a). So gilt etwa die Verarbeitung von Gesundheitsdaten in großem Umfang als ein Vorgang, der wahrscheinlich ein hohes Risiko mit sich bringt und demnach eine DSFA erfordert;
- ist es anschließend Aufgabe des für die Datenverarbeitung Verantwortlichen, die Risiken für die Rechte und Freiheiten von Betroffenen abzuschätzen und Maßnahmen zu bestimmen[29], mit deren Hilfe diese Risiken auf ein vertretbares Maß reduziert werden sollen und der Nachweis für die Einhaltung der DSGVO erbracht werden kann (Artikel 35 Absatz 7, siehe III.C.c). Als Beispiel sei hier die Speicherung personenbezogener Daten auf Laptops genannt, für die geeignete technische und organisatorische Sicherheitsmaßnahmen (wirksame Festplattenverschlüsselung, sicheres Schlüsselmanagement, geeignete Zugangskontrolle, zuverlässige Datensicherung *usw*.) neben den vorhandenen Richtlinien (Hinweis, Zustimmung, Zugangsrecht, Widerspruchsrecht *usw*.) zur Anwendung kommen.

Im vorstehenden Laptop-Beispiel kann die Verarbeitung, sofern die Risiken von dem für die Datenverarbeitung Verantwortlichen und im Sinne von Artikel 36 Absatz 1 und der Erwägungsgründe 84 und 94 hinreichend gemindert worden sind, ohne Konsultation der Aufsichtsbehörde stattfinden. Nur in denjenigen Fällen, in denen es dem für die Datenverarbeitung Verantwortlichen nicht gelingt, die ermittelten Risiken hinreichend zu bewältigen (d. h. die Restrisiken bleiben hoch), muss der Verantwortliche die Aufsichtsbehörde konsultieren.

Ein unzulässig hohes Restrisiko wäre beispielsweise eine Situation, in der die Betroffenen erheblichen oder gar unumkehrbaren und nicht zu bewältigenden Folgen ausgesetzt sind (z. B.: unrechtmäßiger Datenzugriff, durch den das Leben der Betroffenen bedroht ist oder der eine Gefahr für ihre Arbeitsstelle oder ihre finanzielle Situation darstellt) und/oder in der das Eintreten eines Risikos unausweichlich scheint (z. B.: weil aufgrund des Weitergabe-, Nutzungs- oder Verteilmodus keine Möglichkeit besteht, die Zahl derjenigen zu verringern, die auf die Daten zugreifen, oder weil eine bekannte Sicherheitslücke nicht behoben wird).

In Fällen, in denen der für die Datenverarbeitung Verantwortliche keine hinreichenden Maßnahmen bestimmen kann, mit denen sich die Risiken auf ein vertretbares Maß reduzieren lassen (d. h. es bestehen weiterhin hohe Restrisiken), ist eine Konsultation der Aufsichtsbehörde erforderlich[30].

---

[29] Hierzu gehört u. a. auch die Berücksichtigung vorhandener Leitlinien des Europäischen Datenschutzausschusses und der Aufsichtsbehörden sowie des Stands der Technik und der Implementierungskosten gemäß Artikel 35 Absatz 1.

[30] Anmerkung: „*Die Pseudonymisierung und Verschlüsselung personenbezogener Daten*“ (sowie Datensparsamkeit, Kontrollmechanismen usw.) stellen nicht zwingend geeignete Maßnahmen dar. Sie sollen nur als Beispiel dienen. Welche Maßnahmen geeignet sind, hängt von den Umständen und Risiken ab, die für die jeweiligen Verarbeitungsvorgänge gelten.

Darüber hinaus muss der für die Verarbeitung Verantwortliche die Aufsichtsbehörde konsultieren, wenn er durch das Recht der Mitgliedstaaten verpflichtet wird, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen (Artikel 36 Absatz 5).

In diesem Zusammenhang sei jedoch darauf hingewiesen, dass unabhängig davon, ob die Aufsichtsbehörde aufgrund der Höhe der Restrisiken konsultiert werden muss, die Pflicht zur Aufzeichnung und rechtzeitigen Aktualisierung einer DSFA dennoch bestehen bleibt.

IV. Schlussfolgerungen und Empfehlungen

Mit den Datenschutz-Folgenabschätzungen steht den für die Datenverarbeitung Verantwortlichen eine nützliche Methode zur Verfügung, mit der sie Datenverarbeitungssysteme implementieren können, die im Einklang mit der DSGVO stehen und für einige Arten von Verarbeitungsvorgängen obligatorisch sind. Zwar sind die Datenschutz-Folgenabschätzungen skalierbar und können von unterschiedlicher Form sein, aber die Grundvoraussetzungen für ihre Konformität sind in der DSGVO vorgegeben. Für die Datenverarbeitung Verantwortliche sollten die Durchführung einer DSFA als nützliche und positive Tätigkeit sehen, die die Einhaltung gesetzlicher Vorgaben erleichtert.

In Artikel 24 Absatz 1 sind die wesentlichen Pflichten eines für die Verarbeitung Verantwortlichen aufgeführt, was die Einhaltung der DSGVO anbelangt: „*Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.*“

In Fällen, in denen eine mit hohen Risiken verbundene Datenverarbeitung geplant ist oder bereits durchgeführt wird, stellt die DSFA ein zentrales Element bei der Einhaltung der Verordnung dar. Das bedeutet, dass die für die Datenverarbeitung Verantwortlichen anhand der in diesem Dokument aufgeführten Kriterien ermitteln sollten, ob eine DSFA durchzuführen ist. Diese Kriterienliste könnte noch einige Ergänzungen erfahren, wenn die unternehmensinternen Richtlinien für die Datenverarbeitung über die rechtlichen Vorgaben gemäß DSGVO hinausgehen. Dies sollte das Vertrauen der Betroffenen und anderer für die Datenverarbeitung Verantwortlicher weiter stärken.

In Fällen, in denen eine Verarbeitung geplant ist, die wahrscheinlich hohe Risiken mit sich bringt, muss der für die Datenverarbeitung Verantwortliche:

- eine DSFA-Methodik wählen (Beispiele hierfür sind in Anhang 1 zu finden), bei der die Kriterien gemäß Anhang 2 erfüllt sind, oder ein systematisches DSFA-Verfahren bestimmen und umsetzen, das:
  - die Kriterien gemäß Anhang 2 erfüllt;
  - in die vorhandenen Prüfverfahren für die Bereiche Auslegung, Entwicklung, Änderung, Risiken und Betriebsabläufe integriert wird und dabei mit unternehmensinternen Prozessen, mit dem Kontext und der Kultur im Einklang steht;
  - die jeweiligen betroffenen Parteien mit einbezieht und deren Zuständigkeiten genau festlegt (für die Verarbeitung Verantwortlicher, Datenschutzbeauftragter, betroffene

Personen bzw. deren Vertreter, Geschäftsbetrieb, technischer Dienst, Auftragsverarbeiter, Beauftragter für Informationssicherheit usw.);

- der zuständigen Aufsichtsbehörde auf Verlangen den DSFA-Bericht vorlegen;
- die Aufsichtsbehörde konsultieren, wenn es ihm nicht gelungen ist, hinreichende Maßnahmen zur Bewältigung der hohen Risiken zu bestimmen;
- die DSFA sowie die darin bewertete Verarbeitung in regelmäßigen Abständen bzw. spätestens dann überprüfen, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind;
- die getroffenen Entscheidungen dokumentieren.

Anhang 1 – Beispiele für EU-weit geltende Rahmenbestimmungen für Datenschutz-Folgenabschätzungen

Mit der DSGVO wird den für die Datenverarbeitung Verantwortlichen kein konkretes DSFA-Verfahren vorgeschrieben, sondern vielmehr die Möglichkeit gegeben, eigene Rahmenbestimmungen in Ergänzung der bestehenden Arbeitsmethoden einzuführen, jedoch unter der Voraussetzung, dass die in Artikel 35 Absatz 7 beschriebenen Komponenten darin Berücksichtigung finden. Solche Rahmenbestimmungen können speziell auf den für die Datenverarbeitung Verantwortlichen zugeschnitten sein oder für eine gesamte Branche gelten. Im Folgenden finden Sie eine Liste mit Rahmenbestimmungen, die von Datenschutzbehörden der EU bereits erarbeitet und veröffentlicht wurden, sowie EU-weite branchenspezifische Rahmenbestimmungen. Hierzu gehören unter anderem:

Beispiele für EU-weite allgemeine Rahmenbestimmungen:

- DE: Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung, 2016[31].
  https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V_1_1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact 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-weite branchenspezifische Rahmenbestimmungen:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications[32].[Rahmenvertrag für RFID-Anwendungen für die Datenschutz-Folgenabschätzung zu Methodiken.]
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

[31] Von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig und zustimmend (bei Enthaltung von Bayern) zur Kenntnis genommen.

[32] Siehe auch:

- Empfehlung der Kommission vom 12. Mai 2009 zur Umsetzung der Grundsätze der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Stellungnahme 9/2011 zu dem überarbeiteten Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_de.pdf

- Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme[33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Auch eine internationale Norm liefert Leitlinien für Methodiken zur Durchführung einer DSFA (ISO/IEC 29134[34]).

[33] Siehe auch Stellungnahme 7/2013 zum Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme, erstellt durch die Sachverständigengruppe 2 der Taskforce der Kommission für intelligente Netze. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_de.pdf

[34] ISO/IEC 29134, *Informationstechnologie – Sicherheitsverfahren – Datenschutz-Folgenabschätzung – Leitfaden*, Internationale Organisation für Normung (ISO).

Anhang 2 – Kriterien für eine zulässige Datenschutz-Folgenabschätzung

Die WP29-Gruppe empfiehlt die folgenden Kriterien, anhand derer die für die Verarbeitung Verantwortlichen ermitteln können, ob eine DSFA oder eine Methodik zur Durchführung einer DSFA umfassend genug ist, dass den Vorschriften gemäß DSGVO entsprochen wird:

- ☐ eine systematische Beschreibung der Verarbeitungsvorgänge ist enthalten (Artikel 35 Absatz 7 Buchstabe a):
  - ☐ die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sind berücksichtigt (Erwägungsgrund 90);
  - ☐ die personenbezogenen Daten, die Empfänger und die Speicherfrist für die personenbezogenen Daten sind festgehalten;
  - ☐ eine funktionale Beschreibung der Verarbeitungsvorgänge ist enthalten;
  - ☐ die Wirtschaftsgüter, auf die sich die personenbezogenen Daten stützen (Hardware, Software, Netzwerke, Personen, Papiere oder Übertragungsmedien für Papiere), wurden ermittelt;
  - ☐ die Einhaltung genehmigter Verhaltensregeln ist berücksichtigt (Artikel 35 Absatz 8);
- ☐ die Notwendigkeit und Verhältnismäßigkeit wurden bewertet (Artikel 35 Absatz 7 Buchstabe b):
  - ☐ Maßnahmen zur Einhaltung der Verordnung wurden bestimmt (Artikel 35 Absatz 7 Buchstabe d und Erwägungsgrund 90), wobei Folgendes berücksichtigt wurde:
    - ☐ Maßnahmen im Sinne der Verhältnismäßigkeit und Notwendigkeit der Verarbeitung, und zwar auf folgender Grundlage:
      - ☐ festgelegte, eindeutige und legitime Zwecke (Artikel 5 Absatz 1 Buchstabe b);
      - ☐ Rechtmäßigkeit der Verarbeitung (Artikel 6);
      - ☐ Daten, die dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sind (Artikel 5 Absatz 1 Buchstabe c);
      - ☐ begrenzte Speicherfrist (Artikel 5 Absatz 1 Buchstabe e);
    - ☐ Maßnahmen im Sinne der Rechte der Betroffenen:
      - ☐ Informationspflicht gegenüber den Betroffenen (Artikel 12, 13 und 14);
      - ☐ Auskunftsrecht und Recht auf Datenübertragbarkeit (Artikel 15 und 20);
      - ☐ Recht auf Berichtigung und Löschung (Artikel 16, 17 und 19);
      - ☐ Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (Artikel 18, 19 und 21);
      - ☐ Verhältnis zu Auftragsverarbeitern (Artikel 28);
      - ☐ Garantien in Bezug auf die internationale Übermittlung von Daten (Kapitel V);
      - ☐ vorherige Konsultation (Artikel 36).
- ☐ die Risiken für die Rechte und Freiheiten der betroffenen Personen werden kontrolliert (Artikel 35 Absatz 7 Buchstabe c):
  - ☐ Ursache, Art, Besonderheit und Schwere der Risiken (vgl. Erwägungsgrund 84) wurden aus Sicht der Betroffenen bewertet, und zwar genau genommen für jedes einzelne Risiko (unrechtmäßiger Datenzugriff, unerwünschte Änderung und Verschwinden von Daten):
    - ☐ Risikoquellen wurden berücksichtigt (Erwägungsgrund 90);
    - ☐ potenzielle Auswirkungen auf die Rechte und Freiheiten von Betroffenen wurden ermittelt, die bei Ereignissen wie z. B. einem unrechtmäßigen

Datenzugriff, einer unerwünschten Änderung und dem Verschwinden von Daten bestehen könnten;

- ☐ Bedrohungen wurden ermittelt, die einen unrechtmäßigen Datenzugriff, eine unerwünschte Änderung und das Verschwinden von Daten nach sich ziehen könnten;
- ☐ Eintrittswahrscheinlichkeit und Schwere wurden bewertet (Erwägungsgrund 90);

☐ Maßnahmen zur Bewältigung dieser Risiken wurden ermittelt (Artikel 35 Absatz 7 Buchstabe d und Erwägungsgrund 90);

☐ betroffene Parteien wurden einbezogen:

- ☐ der Rat des Datenschutzbeauftragten wurde eingeholt (Artikel 35 Absatz 2);
- ☐ gegebenenfalls wurde der Standpunkt der betroffenen Personen oder ihrer Vertreter eingeholt (Artikel 35 Absatz 9).