Ist nach Art 35 eine DSFA erforderlich?
(Art 35 Abs 1, 3)

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Eine DSFA ist insbesondere in folgenden Fällen erforderlich:

(3) 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;

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 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Treffen zwei oder mehrere Kriterien der **Art 29-Datenschutzguppe** zu?
(Leitlinien zur DSFA, WP 248 Rev.01)

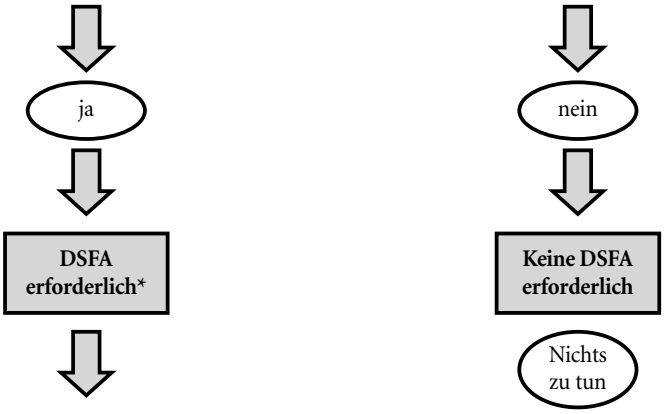
Generell ist die WP 29, die diese Kriterien aufgestellt hat der Auffassung, dass mit steigender Anzahl der erfüllten Kriterien eine Pflicht zur Durchführung umso wahrscheinlicher wird; in der Regel ist eine Pflicht ab zwei erfüllten Kriterien gegeben. Dies unabhängig von den Maßnahmen, die der für die Verarbeitung Verantwortliche vorsieht. In manchen Fällen kann eine DSFA auch dann durchzuführen sein, wenn nur eines der Kriterien erfüllt ist.

1 Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (Bewerten oder Einstufen, darunter das Erstellen von Profilen und Prognosen)

2 Automatisierte Entscheidungsfindung mit rechtlicher oder ähnlicher bedeutsamer Wirkung

3 Systematische Überwachung

4 Verarbeitung besonderer Kategorien von personenbezogenen Daten, strafrechtlich relevanten Daten oder vertraulichen oder höchstpersönlichen Daten
5 Datenverarbeitung in großem Umfang
6 Der Abgleich oder die Zusammenführung von Datensätzen
7 Daten von schutzbedürftigen Betroffenen
8 Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9 Die betroffene Person wird durch die Verarbeitung daran gehindert, ein Recht auszuüben oder eine Dienstleistung oder einen Vertrag in Anspruch zu nehmen
10 Anderes relevantes Kriterium – gegebenenfalls bitte anführen



***DSFA ist entsprechend Art 35 Abs 7 durchführen:**

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.

Abbildung 25: Schwellenwertprüfung

9783214010072
Praxishandbuch Datenschutzrecht | 4
Rainer Knyrim
MANZ Verlag Wien

D. Durchführung der Datenschutz-Folgenabschätzung

1. Allgemeines

12.71 Gelangt man nach dem im vorigen Unterkapitel erklärten Prüfschema zum Ergebnis, dass eine Datenschutz-Folgenabschätzung durchzuführen ist, so gibt Art 35 Abs 7 den **Mindestinhalt einer Datenschutz-Folgenabschätzung vor**, gleichzeitig aber auch eine Struktur für deren praktischen Aufbau. Wichtig ist, dass sowohl die Vorprüfung, ob eine Datenschutz-Folgenabschätzung durchzuführen ist (siehe das vorige Unterkapitel), als auch die Datenschutz-Folgenabschätzung selbst, **schriftlich dokumentiert** wird, damit der Verantwortliche seiner Rechenschaftspflicht nachkommen kann und belegen kann, dass er diese durchgeführt hat. Die **Nichterfüllung der Verpflichtungen**, die sich aus Art 35 ergeben, sind mit einer **Strafdrohung von bis zu EUR 10 Mio oder 2 % des gesamten weltweit erzielten Jahresumsatzes belegt.**[1193]

12.72 Art 35 Abs 7 DSGVO schreibt für die Durchführung der Datenschutz-Folgenabschätzung keine bestimmte Art und Weise der Durchführung vor, sondern gestaltet diese als **Prozess.**[1194] Solange die Mindestanforderungen erfüllt sind, entspricht die DSFA der DSGVO. Damit soll dem Verantwortlichen bewusst die nötige Flexibilität zur Integration der DSFA in bestehende Prozesse gelassen werden.[1195]

Es gibt verschiedene **Muster für die Durchführung einer Datenschutz-Folgenabschätzung**, die teilweise schon vor dem Inkrafttreten der DSGVO,[1196] teilweise erst danach ausgearbeitet und veröffentlicht wurden.[1197] Die Leitlinien der *Artikel-29-Datenschutzgruppe* nennen ebenfalls Muster.[1198]

2. Erstellung der Datenschutz-Folgenabschätzung

12.73 Die Erfahrung zeigt, dass die Abarbeitung der von Art 35 Abs 7 genannten Erfordernisse für eine Datenschutz-Folgenabschätzung für den Verantwortlichen[1199] in der Praxis zunächst eine entsprechende **Vorplanung** erfordert: Es ist zu klären, welche **internen Mitarbeiter** des

1193 Art 83 Abs 4 lit a DSGVO.

1194 *Jandt* in *Kühling/Buchner*, DS-GVO/BDSG[2] Art 35 Rz 31.

1195 Siehe *Trieb* in *Knyrim*, DatKomm Art 35 Rz 103 mit Verweis auf *Art-29-Datenschutzgruppe,* Leitlinien zu Datenschutz-Folgenabschätzung (WP248 rev.01) 21.

1196 *De Hert/Kloza/Wright*, PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf (abgefragt am 9. 3. 2020); EK, Privacy and Data Protection Impact Assessment Framework for RFID Applications (2011) https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications (abgefragt am 9. 3. 2020); EK, Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems (2014) https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf (abgefragt am 9. 3. 2020).

1197 Siehe CNIL, Privacy Impact Assessment (PIA), Methodology and Templates (2018), https://www.cnil.fr/en/PIA-privacy-impact-assessment-en (abgefragt am 9. 3. 2020); DSK, Standard-Datenschutzmodell (2018) https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_sdm.pdf (abgefragt am 9. 3. 2020). Eine detaillierte Beschreibung enthält auch die ISO/IEC 29134:2017.

1198 *Art-29-Datenschutzgruppe,* Datenschutz-Folgenabschätzung (WP248 rev.01) 26.

1199 Der Auftragsverarbeiter hat den Verantwortlichen auf Anfrage zu unterstützen, siehe dazu näher bei *Kastelitz/Hötzendorfer/Riedl* in *Jahnel*, Jahrbuch Datenschutzrecht 122.

Verantwortlichen über das erforderliche Know-how über die geplante Datenverarbeitung verfügen und ausreichende **Zeitressourcen** haben, um an der Erstellung der Datenschutz-Folgenabschätzung mitarbeiten zu können. Zunächst sind Mitarbeiter der jeweiligen **Fachabteilungen** erforderlich. Bei Kundendatenverarbeitungen zB die Marketingabteilung oder Presseabteilung; bei Mitarbeiterdatenverarbeitungen zB die Personal- und Recruitingabteilung; bei Lieferantendaten zB die Einkaufsabteilung. Typischerweise sind auch Mitarbeiter der **IT-Abteilung, der Rechtsabteilung, der Informationssicherheit** und des **Organisationsmanagements** hinzuzuziehen, um die Risiken der geplanten Datenverarbeitung und mögliche Abhilfemaßnahmen abschätzen zu können. Oft wird es dazu auch erforderlich sein, involvierte **Auftragsverarbeiter** in die Abarbeitung mit einzubeziehen und **externe Rechts- und IT-Beratung** hinzuzuziehen.[1200] Es muss also in der Praxis ein **Team aus den richtigen – wissenden und verfügbaren – Personen** gebildet werden, um die Datenschutz-Folgenabschätzung durchzuführen.

12.74 Zu beachten ist, dass Art 35 Abs 2 DSGVO vorschreibt, dass auch der **Rat des Datenschutzbeauftragten** bei der Durchführung einer Datenschutz-Folgenabschätzung **einzuholen** ist. Wenn somit beim Verantwortlichen ein Datenschutzbeauftragter bestellt ist, sollten diesem der Beschluss und die Gründe für die Durchführung der Datenschutz-Folgenabschätzung ehebaldigst mitgeteilt und ihm alle Unterlagen für die Erfüllung seiner Konsultationsaufgaben zur Verfügung gestellt werden.[1201]

12.75 Nach Art 35 Abs 9 DSGVO hat der Verantwortliche gegebenenfalls den **Standpunkt der betroffenen Personen** oder **ihrer Vertreter** zur beabsichtigten Verarbeitung einzuholen. Vor oder während der Durchführung der Datenschutz-Folgenabschätzung muss also überlegt werden, welche betroffenen Personen und Vertreter konsultiert werden können, und deren Standpunkte sollten in die Datenschutz-Folgenabschätzung einfließen. Ein typischer solcher „Stakeholder" ist der **Betriebsrat**, wenn es um Personaldatenverarbeitungen geht.[1202]

Da nach Art 35 Abs 9 der Verantwortliche den Standpunkt der betroffenen Personen oder ihrer Vertreter „gegebenenfalls" einholen soll, hat der Verantwortliche einen gewissen Spielraum, ob er diese einbezieht oder nicht. Sofern eine Einbeziehung nicht praktikabel oder etwa mit einem hohen wirtschaftlichen Aufwand verbunden wäre und er von dieser absieht, sind die Gründe dafür zu dokumentieren.[1203]

Vor Beginn der Datenschutz-Folgenabschätzung muss weiters geprüft werden, ob die geplante Datenverarbeitung Gegenstand **genehmigter Verhaltensregeln**[1204] ist. Art 35 Abs 8 DSGVO schreibt dem Verantwortlichen nämlich vor, die Vorgaben aus solchen Verhaltensregeln entsprechend zu berücksichtigen; diese können Auswirkungen auf alle nachstehend erläuterten Schritte einer Datenschutz-Folgenabschätzung haben.[1205]

1200 Siehe näher *Trieb* in *Knyrim*, DatKomm Art 35 Rz 106.

1201 *Trieb* in *Knyrim*, DatKomm Art 35 Rz 106, 120 ff. Nach *Hötzendorfer* in *Gantschachter/Jelinek/Schmidl/Spanberger*, DSGVO Art 35 Anm 5 kann die DSFA grundsätzlich durch interne oder externe Personen durchgeführt werden.

1202 Siehe zur – davon unabhängigen – Verpflichtung zum Abschluss von Betriebsvereinbarungen näher im Kapitel 16. Arbeitnehmerdatenverarbeitung.

1203 *Nolte/Werkmeister* in *Gola, DS-GVO*[2] Art 35 Rz 61 f.

1204 Zu Verhaltensregeln siehe Kapitel Zertifizierung und Verhaltensregeln.

1205 Siehe näher *Trieb* in *Knyrim*, DatKomm Art 35 Rz 106, 125 ff.

Art 35 Abs 7 lit a) DSGVO verlangt hinsichtlich der Datenschutz-Folgenabschätzung zunächst Folgendes:[1206] **12.76**

> a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

Es wird also die Beschreibung der verarbeiteten **Kategorien** personenbezogener Daten, des **Zweckes** der Verarbeitung, des **Umfangs** und der **Dauer** der Verarbeitung, sowie der **betroffenen Personengruppen** verlangt. Auch die verwendeten **IT-Systeme samt technischer und organisatorischer Maßnahmen** müssen beschrieben werden,[1207] was auch die Beschreibung der Betriebsmittel (Hard- und Software), mit denen die Datenverarbeitung betrieben wird, beinhaltet.

Praxistipp

Weiters sollte die Art der Verarbeitung inkl **Datenübermittlungen und Datenempfänger** verständlich beschrieben werden und allenfalls in Grafiken verdeutlicht werden. Auch eine **Darstellung** des **„Lebenszyklusses"** der Daten von deren ersten Erhebung bis zu ihrer finalen Löschung in Form einer Beschreibung oder von Flussdiagrammen kann eine hilfreiche Grundlage für die weitere Abarbeitung der Datenschutz-Folgenabschätzung sein.

Lit a) verlangt weiters, dass, wenn die **Rechtsgrundlage der Verarbeitung berechtigte Interessen** des Art 6 Abs 1 lit f DSGVO sind, diese berechtigten Interessen in der Datenschutz-Folgenabschätzung angegeben werden müssen. Es genügt dabei nicht, berechtigte Interessen bloß zu behaupten, diese müssen konkret angeführt werden.[1208] Überhaupt empfiehlt es sich, die Rechtsgrundlage(n) der Verarbeitung in der Datenschutz-Folgenabschätzung anzuführen, da eine Datenverarbeitung ohne, oder auf Grundlage einer falschen Rechtsgrundlage, unzulässig wäre. Wenn besondere Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO) verarbeitet werden, ist zu prüfen, ob ein Ausnahmetatbestand vom generellen Verarbeitungsverbot in Art 9 Abs 2 DSGVO anwendbar ist.

Art 35 Abs 7 lit b) DSGVO fordert als nächsten Schritt: **12.77**

> b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

Gem Art 35 Abs 7 lit b DSGVO muss die Datenschutz-Folgenaschätzung aufgrund der Datenschutzgrundsätze des Art 5, insbes der Grundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung[1209] sowie der Rechtmäßigkeitserfordernisse[1210] eine **Bewertung der Notwendigkeit und Verhältnismäßigkeit** der geplanten Verarbeitungsvor-

1206 Siehe auch die Übersichtsgrafik über den Verlauf einer DSFA bei *Nolde* in *Koreng/Lachenmann,* Formularhandbuch Datenschutzrecht[2] 166 und 169.
1207 *Baumgartner* in *Ehmann/Selmayr (Hrsg)*, DS-GVO[2] Art 35 Rz 50 f.
1208 Dies lässt sich aus der E „Allergie-Tagesklinik" der DSB-D213.692/0001-DSB/2018 vom 16. 11. 2018 ableiten, in der die DSB dies auch in der Information an die Betroffenen nach Art 13 gefordert hat.
1209 Art 5 Abs 1 lit b), c) und e).
1210 Art 6 ff.

gänge in Bezug auf ihren Zweck enthalten. Daraus soll sich ergeben, weshalb die Datenverarbeitung für den konkreten Zweck erforderlich, geeignet und verhältnismäßig ist.[1211]

Praxistipp

Die Datenschutz-Folgenabschätzung muss daher Ausführungen zu den **festgelegten, eindeutigen und legitimen Zwecken**, für die die personenbezogenen Daten erhoben wurden, enthalten (Art 5 Abs 1 lit b DSGVO), darlegen warum die Verwendung der Daten **angemessen, erheblich und auf das notwendige Maß beschränkt ist** (Art 5 Abs 1 lit c DSGVO) und ausführen, warum welche **Speicherfrist** gewählt wurde (Art 5 Abs 1 lit e DSGVO).

12.78 Als nächster Schritt erfolgt in Art 35 Abs 7 lit c) DSGVO nun die eigentliche Folgenabschätzung:[1212]

> c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

Der Verantwortliche muss nun die **Risiken**[1213] **für die Rechte und Freiheiten der Betroffenen abschätzen.** Es ist eine **Risikobewertung** für die Verarbeitungsvorgänge mit hohem Risiko gem Art 35 Abs 1 DSGVO durchzuführen und zu dokumentieren. Es soll dabei die konkrete Bewertung der Risiken anhand **Eintrittswahrscheinlichkeit** und **Schwere** der Auswirkungen, wie nach Abs 1 vorgesehen, dargelegt werden.

Diese Bewertung ist der zentrale Bestandteil der Dokumentation der Datenschutz-Folgenabschätzung, der auf die in Abs 7 lit a) und b) DSGVO geforderte Beschreibung und Verhältnismäßigkeitsprüfung aufbaut. Die Risikobewertung hat daher entsprechend detailliert zu erfolgen.[1214]

Beispiel für Bewertung jeweils der Risiken und auch der Auswirkungen:

- Stufe 1 = vernachlässigbar, dh Risikoeintritt: sehr unwahrscheinlich; Risikoauswirkungen: sehr gering.
- Stufe 2 = limitiert, dh Risikoeintritt: mit höherer Wahrscheinlichkeit anzunehmen; Risikoauswirkungen: limitiert;
- Stufe 3 = signifikant, dh Risikoeintritt: durchaus wahrscheinlich; Risikoauswirkungen: nicht vernachlässigbar;
- Stufe 4 = maximal, dh Risikoeintritt: höchstwahrscheinlich; Risikoauswirkungen: nicht abschätzbar bzw existenzgefährdend.

Daraus lässt sich dann für die einzelnen identifizierten Risiken eine Risikomatrix wie folgt erzeugen:[1215]

1211 *Baumgartner* in *Ehmann/Selmayr*, DS-GVO[2] Art 35 Rz 52.
1212 Siehe auch Praxisbeispiel von *Oman/Gruber*, DSFA (Teil 3), Dako 2019, 52.
1213 *Jandt* in *Kühling/Buchner*, DS-GVO/BDSG[2] Art 35 Rz 42 ff will diese Risiken mE unzutreffend ausschließlich auf die technischen Risiken einschränken. Siehe aber die Auflistung von Risiken bei *Oman/Gruber*, DSFA (Teil 1), Dako 2019, 28 (30).
1214 *Baumgartner* in *Ehmann/Selmayr*, DS-GVO[2] (2017) Art 35 Rz 53.
1215 Siehe https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf (abgefragt am 9. 3. 2020). Siehe auch *Oman/Gruber*, DSFA (Teil 1), Dako 2019, 28 (31).

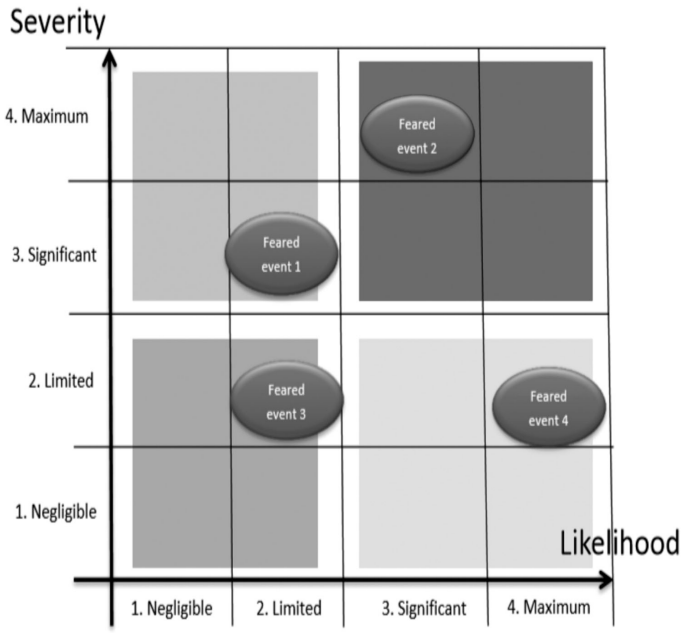


Abbildung 26: Risikomatrix

Zur genauen Abgrenzung der Komponenten eines Risikomanagements verweist die Art-29-Datenschutzgruppe auf zB ISO 31000.[1216]

Die Art-29-Datenschutzgruppe hat in ihren Leitlinien zur Datenschutz-Folgenabschätzung in Anhang 1 **Beispiele zu Methodiken** für die Datenschutz-Folgenabschätzung aufgenommen, Anhang 2 enthält allgemeine **Kriterien**, anhand derer sich nachweisen lässt, dass eine bestimmte Methodik die Standards laut DSGVO-Anforderungen erfüllt. Zwar ist die Wahl einer Methodik laut Leitlinien Sache des für die Verarbeitung Verantwortlichen, dieser muss jedoch beachten, dass die Kriterien gemäß Anhang *2* erfüllt sind.[1217]

Als letzter Schritt erfolgt in Art 35 Abs 7 lit d) DSGVO nun die Bewältigung der Risiken: **12.79**

> 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.

Der finale Schritt der Datenschutz-Folgenabschätzung ist nun, auf Grundlage der Bewertungsergebnisse **Abhilfemaßnahmen zu den Risiken zu planen**.

1216 *Art-29-Datenschutzgruppe,* Leitlinien zur Datenschutz-Folgenabschätzung, WP 248 rev.01, 21. Zum sog Standard-Datenschtuzmodell, das in Deutschland zur Folgenabschätzung entwickelt wurde siehe *Martini* in *Paal/Pauly,* DS-GVO/BDSG[2] Art 35 Rz 49 ff.

1217 *Art-29-Datenschutzgruppe,* Leitlinien zur Datenschutz-Folgenabschätzung, WP 248 rev.01, 23 sowie Anänge 1 und 2.

Bei den Abhilfemaßnahmen kann es sich um **technische Maßnahmen** (zB wirksame Festplattenverschlüsselung, geeignete Zugangskontrolle, zuverlässige Datensicherung, Pseudonymisierung) oder **organisatorische Maßnahmen** (zB Vier-Augen-Prinzip, Schaffen von Policies, Leitlinien um bestimmte Risiken zu reduzieren) handeln. Auch bei lediglich geringen Risiken gilt, dass die Schutzmaßnahmen so zu wählen sind, dass die Realisierung des Risikos so weit wie möglich ausgeschlossen wird.[1218]

Für die Planung dieser Abhilfemaßnahmen gehört nach Ansicht der Art-29-Datenschutzgruppe ua auch die Berücksichtigung vorhandener **Leitlinien des Europäischen Datenschutzausschusses** und der Aufsichtsbehörden sowie des **Stands der Technik** (s dazu Rz 10.4) und der Implementierungskosten gem Art 35 Abs 1 DSGVO.[1219]

Praxistipp

In der Datenschutz-Folgenabschätzung sollte zu jedem identifizierten Risiko eine **übersichtliche Darstellung** enthalten sein, die das identifizierte Risiko inkl Schwere und Eintrittswahrscheinlichkeit aufzeigt, die zu treffenden Abhilfemaßnahmen beschreibt und schließlich eine (Neu-)Bewertung des Risikos unter Berücksichtigung der zu treffenden Abhilfemaßnahmen. Sinnvoll ist es überdies festzulegen, wer für die Umsetzung der Abhilfemaßnahmen verantwortlich ist, bis wann die Umsetzung erfolgt und welche Mittel hierfür zur Verfügung gestellt werden.

Wenn die Risiken durch die zu treffenden Abhilfemaßnahmen **ausreichend gemindert** werden können, dann kann die **Verarbeitung ohne Konsultation** der Aufsichtsbehörde stattfinden. Falls das Ergebnis der Datenschutz-Folgenabschätzung ist, dass trotz der geplanten Abhilfemaßnahmen das **Risiko der Verarbeitung weiterhin hoch** wäre, dann muss der Verantwortliche nach Art 36 DSGVO **vor Beginn der Verarbeitung die Datenschutzbehörde konsultieren**. Siehe dazu weiter unten.

3. Dokumentation und regelmäßige Überprüfung

12.80 Art 35 Abs 11 DSGVO verpflichtet den Verantwortlichen, „erforderlichenfalls" eine **Überprüfung der Datenschutz-Folgenabschätzung durchzuführen**, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird.[1220] Laut Abs 11 soll dies zumindest geschehen, wenn hinsichtlich des mit der Verarbeitung verbundenen Risikos Änderungen eingetreten sind.

Praxistipp

Da gerade in größeren Unternehmen der laufende Überblick über die Datenverarbeitungen nicht „automatisch" gewährleistet ist, sollte ein Prozess implementiert werden, der regelmäßig überprüft, ob die Datenverarbeitung weiterhin in dem Rahmen, der in der Datenschutz-Folgenabschätzung dokumentiert wurde, stattfindet.

1218 *Nolte/Werkmeister* in *Gola,* DS-GVO[2] Art 35 Rz 54.
1219 *Art-29-Datenschutzgruppe,* Leitlinien zur Datenschutz-Folgenabschätzung, WP 248 rev.01, 23.
1220 Laut *Martini* in *Paal/Pauly,* DS-GVO/BDSG[2] Art 35 Rz 73 ist eine Überprüfung jedenfalls dann erforderlich, wenn das tatsächliche von dem kalkuliertenVerarbeitungsrisiko abweicht.

II. Vorherige Konsultation der Datenschutzbehörde

A. Auslöser der Konsultationsverpflichtung

12.81 Wenn die Datenschutz-Folgenabschätzung wie im vorigen Unterkapitel beschrieben abgearbeitet wurde und deren Ergebnis ist, dass **trotz der geplanten Abhilfemaßnahmen die Verarbeitung zu einem hohen Risiko führen würde, ist laut Art 36 Abs 1 DSGVO ein Konsultationsverfahren durchzuführen**:

> Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

12.82 Es muss also dann, wenn der Verantwortliche entweder **keine Abhilfemaßnahmen treffen will** (etwa weil ihm der finanzielle Aufwand dafür unverhältnismäßig erscheint) oder die in der Datenschutz-Folgenabschätzung **geplanten Abhilfemaßnahmen nicht zu einer ausreichenden Risikoreduktion führen** und dadurch **ein hohes Restrisiko der Verarbeitung bleibt**, die **Datenschutzbehörde konsultiert werden**.[1221] Ein solches hohes Restrisiko wäre beispielsweise eine Situation, in der die Betroffenen erheblichen oder gar unumkehrbaren und nicht zu bewältigenden Folgen ausgesetzt sind (zB unrechtmäßiger Datenzugriff, der eine Gefahr für ihre finanzielle Situation darstellt) und/oder in der das Eintreten eines Risikos unausweichlich scheint (zB 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). Pseudonymisierung und Verschlüsselung personenbezogener Daten sind dabei nicht zwingend geeignete Maßnahmen, um ein hohes Restrisiko zu verhindern, denn deren Wirkung hängt von den Umständen und Risiken im jeweiligen Einzelfall ab.[1222]

12.83 Der Konsultationsmechanismus nach Art 36 DSGVO ist für den einzelnen Verantwortlichen nach der DSGVO die einzige Möglichkeit, von der Behörde vorab eine beabsichtigte Datenverarbeitung, zumindest faktisch, genehmigen zu lassen. Grundsätzlich empfiehlt sich daher, zur Gewinnung einer Rechtssicherheit über die Konformität der beabsichtigten Datenverarbeitung ein Konsultationsverfahren nach Art 36 DSGVO durchzuführen.

12.84 Wenn der Verantwortliche in der Datenschutz-Folgenabschätzung zum Ergebnis kommt, dass ein hohes Restrisiko bleibt, und er eine **vorige Konsultation durchführen müsste, diese aber unterlässt**, so droht ihm nach Art 83 Abs 4 lit a DSGVO eine **Geldbuße von bis zu EUR 10 Mio oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes**. Es empfiehlt sich daher, bei Zweifeln über die verpflichtende Notwendigkeit einer vorigen Konsultation diese durchzuführen, da im Falle, dass die Datenschutzbehörde diese für nicht erforderlich erachtet, eine Zurückweisung durch die Behörde erfolgt, dann aber jedenfalls keine Strafe wegen Nichtdurchführung mehr drohen kann.

Laut Art 36 Abs 5 DSGVO können unabhängig von der Grundregel des Abs 1 Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung

1221 So auch *von dem Bussche* in *Plath*, DSGVO[3] Art 36 Rz 7.
1222 *Art-29-Datenschutzgruppe,* Leitlinien zur Datenschutz-Folgenabschätzung, WP 248 rev.01, 23.

zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen. Bis zur Drucklegung dieses Buches waren keine solchen Verpflichtungen im österreichischen Recht implementiert.

B. Konsultationsantrag

12.85 Ist ein Konsultationsverfahren durchzuführen, dann muss der Verantwortliche der Aufsichtsbehörde nach Art 36 Abs 3 DSGVO folgende Informationen zur Verfügung stellen:

a) gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;

b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;

c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;

d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

e) die Datenschutz-Folgenabschätzung gemäß Artikel 35 und

f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen

12.86 Diese Aufzählung ist in sich nicht sehr logisch, denn die in Punkt e) geforderte Datenschutz-Folgenabschätzung sollte ohnehin die Punkte a) bis c) enthalten. Jedenfalls die Beschreibung der Zwecke und der geplanten Verarbeitungsvorgänge der lit b) ist laut Art 35 Abs 7 lit b) DSGVO Pflichtinhalt einer Datenschutz-Folgenabschätzung, ebenso die Abhilfemaßnahmen und Garantien der lit c) laut Art 35 Abs 7 lit d) DSGVO.

Praxishinweis

Das Konsultationsverfahren wird **durch einen formellen Antrag bei der Datenschutzbehörde eingeleitet**, mit dem die oben genannten Informationen – also vor allem die bereits durchgeführte Datenschutz-Folgenabschätzung eingereicht werden und die Durchführung des Konsultationsverfahrens begehrt wird. Wichtig ist, dass aus der Datenschutz-Folgenabschätzung deutlich hervorgeht, warum trotz Abhilfemaßnahmen ein hohes Risiko bei Durchführung der Datenverarbeitung bleibt, denn Aufgabe der Datenschutzbehörde ist, zu beurteilen, ob die Datenverarbeitung trotz dieses hohen Risikos durchgeführt werden darf.

Weiters kann im Antrag die Durchführung einer mündlichen Verhandlung beantragt werden, wobei die Datenschutzbehörde diesem Antrag nicht nachkommen muss.

Nach lit f) kann die Datenschutzbehörde im Konsultationsverfahren noch weitere Informationen einholen. Die Nichtlieferung solcher Informationen führt zu einer Fristaussetzung für die Datenschutzbehörde, siehe dazu im folgenden Punkt. In der Praxis fordert die Datenschutzbehörde, wenn sie Fragen hat, den Antragsteller zur Stellungnahme auf.

C. Konsultationsverfahren

12.87 Der Ablauf des Konsultationsverfahrens und dessen Beendigung sind in Art 36 Abs 2 DSGVO sehr knapp geregelt.