Handreichung für die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 EU-DSGVO

Eine DSFA ist kein einmaliger Vorgang. Sollten sich z .B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren (Neue Software, neue Verarbeitungsprozesse usw.) ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung empfohlen.

Die einzelnen Schritte zur Durchführung der DSFA werden nachfolgend dargestellt:

1. Zusammenstellung des DSFA-Teams
Eine DSFA kann im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das über Kompetenzen im Bereich Datenschutz, Risikoermittlung und Fachprozesse verfügt. Der Datenschutzbeauftragte steht diesem Team während des gesamten Prozesses beratend zur Seite. Es kann sinnvoll oder notwendig sein, z. B. Auftragsverarbeiter oder Hersteller von IT-Systemen ebenfalls mit einzubeziehen.

2. Prüfplanung
Da eine DSFA meist ein komplexer Prozess ist, der viele Mitwirkende einbindet, ist eine Prüfplanung (z. B. mit Methoden des Projektmanagements) empfehlenswert.

3. Festlegung des Beurteilungsumfangs
Die betrachteten Verarbeitungsvorgänge sind von anderen (Geschäfts-)Prozessen abzugrenzen und ausführlich und abschließend mit allen Datenflüssen zu beschreiben. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten.

4. Identifikation und Einbindung von Akteuren und betroffenen Personen
Die Akteure und betroffenen Personen sind zu identifizieren. Bei der Durchführung der DSFA zieht der Verantwortliche den Datenschutzbeauftragten zurate (Art. 35 Abs. 2 EU-DSGVO). Ggf. holt der Verantwortliche den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein (Art. 35 Abs. 9 EU-DSGVO). Dies umfasst beispielsweise die Einbindung von Gremien der Mitbestimmung, z. B. von Personalräten.

5. Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf ihren Zweck
Die im vorigen Schritt beschriebenen Verarbeitungsvorgänge werden ausgehend von den mit ihnen verfolgten Zwecken daraufhin bewertet, ob der durch sie bewirkte Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zu dem angestrebten Zweck steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Rechte und Freiheiten

der Betroffenen weniger stark eingreifen. Ggf. nimmt der Verantwortliche eine Anpassung der Verarbeitungsvorgänge vor, z. B. durch Beschränkung der zu verarbeitenden Daten oder durch Änderung der beteiligten Akteure oder eingesetzten Technologien.

6. Identifikation der Rechtsgrundlagen
Aufbauend auf dem vorigen Schritt können sodann die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert werden.

7. Modellierung der Risikoquellen
Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre Beweggründe und möglichen Ziele sein können. Anhand dessen können die damit zusammenhängenden Eintrittswahrscheinlichkeiten ermittelt werden.

8. Risikobeurteilung
Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Ihre Schwere sowie die jeweilige Eintrittswahrscheinlichkeit sind dabei zu berücksichtigen.

9. Auswahl geeigneter Abhilfemaßnahmen
Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Datenschutzmaßnahmen) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen. Verbleibende Restrisiken werden ermittelt und dokumentiert.

10. Erstellung des DSFA-Berichts
Der DSFA-Bericht enthält nach Art. 35 Abs. 7 EU-DSGVO die systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Beurteilung der Risiken sowie der Abhilfemaßnahmen zur Risikoeindämmung. Der Bericht ist um eine Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen zu ergänzen. Er kann sich dabei an den hier dargestellten Phasen orientieren. Der DSFA-Bericht dient ferner als Baustein einer umfassenden Dokumentation zur Umsetzung der in Art. 5 Abs. 2 EU-DSGVO normierten Rechenschafts-pflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen.
Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher

Personen besteht (Restrisiko), muss nach Art. 36 EU-DSGVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Er trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DS-GVO genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung aussprechen.

Die Datenschutz-Folgenabschätzung unterstützt bei der systematischen Risikoeindämmung. Rechtzeitig durchgeführt hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der Grundverordnung umzusetzen.