Kurzpapier Nr. 5
Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die Datenschutz-Grundverordnung (DS-GVO) unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) diese Risiken eingedämmt werden. Das Instrument einer Datenschutz-Folgenabschätzung (DSFA) kann hierfür systematisch eingesetzt werden.

Was ist eine Datenschutz-Folgenabschätzung nach DS-GVO?

Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Artikel 35 Absatz 1, 7 DS-GVO sowie Erwägungsgrund 84, 90). Zum Begriff des Risikos, der ein zentrales Konzept der DS-GVO ist, wird es ein eigenes Kurzpapier geben.

Verarbeitungsvorgang als Ankerpunkt

Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen.

Sofern mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden (Artikel 35 Absatz 1 DS-GVO). Ähnliche Risiken können beispielsweise dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten(-kategorien) zu gleichen Zwecken eingesetzt werden (vergleiche auch Erwägungsgrund 92 DS-GVO). Bei einer gemeinsamen Bewertung von ähnlichen Verarbeitungsvorgängen sind die im Folgenden dargestellten Vorgehensweisen gegebenfalls anzupassen.

Erforderlichkeit einer DSFA

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge ("Schwellwertanalyse"). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.

Artikel 35 Absatz 3 DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko im Sinne des Artikel 35 Absatz 1 DS-GVO führen. Aufbauend auf den Leitlinien der Artikel-29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen eine DSFA

durchzuführen ist, veröffentlichen. Auch zur Durchführung der Schwellwertanalyse werden künftig Hinweise zur Verfügung gestellt.

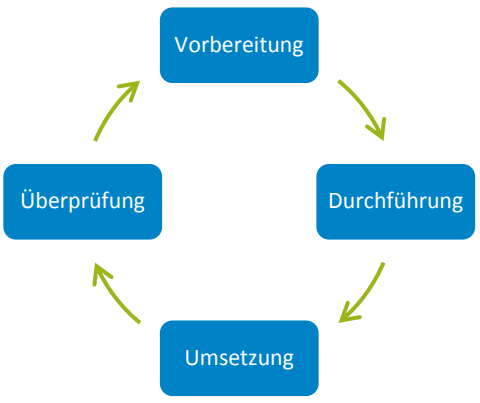
Zeitpunkt der Durchführung einer DSFA

Eine DSFA ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen. Da eine DSFA meist nicht ad hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig, beispielsweise unterstützt durch ein allgemeines Datenschutz-Managementsystem, auf den Weg gebracht werden.

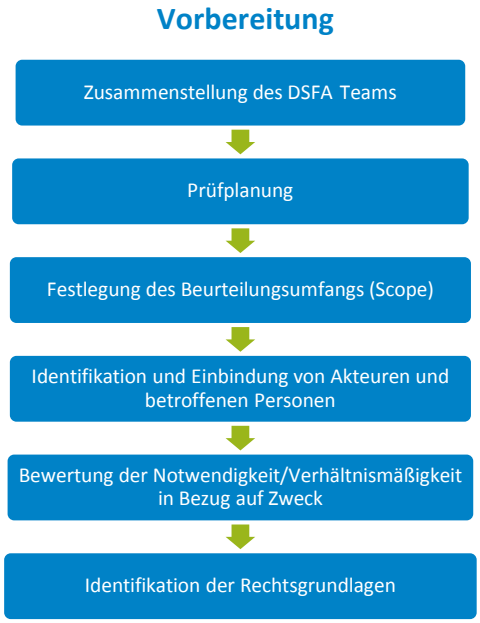
Wie kann eine DSFA durchgeführt werden?

Die formellen Anforderungen an die Durchführung einer DSFA ergeben sich aus der DS-GVO, speziell aus Artikel 35 sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Bei der verwendeten Methode wird dem Verantwortlichen mehr Spielraum gelassen. Werden bestehende Methoden oder Standards eingesetzt, ist zu beachten, dass die Anforderungen der DS-GVO immer vorrangig zu behandeln sind.

Eine DSFA ist kein einmaliger Vorgang. Sollten sich zum Beispiel neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren 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 Bestandteile der Hauptprozessschritte werden im Einzelnen nachfolgend dargestellt.



1. *Zusammenstellung des DSFA-Teams*
   Eine DSFA kann im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das Kompetenzen im Bereich Datenschutz, Risikoermittlung und Fachprozesse mitbringt. Der Datenschutzbeauftragte steht diesem während des gesamten Prozesses beratend zur Seite. Es kann sinnvoll oder notwendig sein, zum Beispiel 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 (zum Beispiel mit Methoden des Projektmanagements) empfehlenswert.

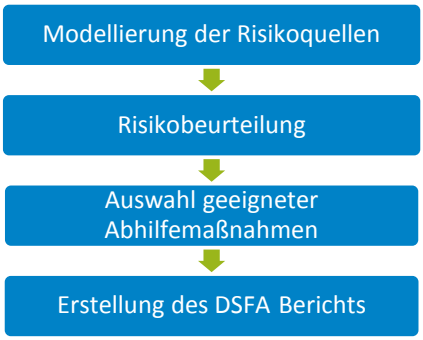
3. *Festlegung des Beurteilungsumfangs (Scope)*
   Die betrachteten Verarbeitungsvorgänge sind von anderen (Geschäfts-)Prozessen abzugrenzen und ausführlich und abschließend mit allen Datenflüssen zu beschreiben. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten.

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 (Artikel 35 Absatz 2 DS-GVO). Gegebenenfalls holt der Verantwortliche den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein (Artikel 35 Absatz 9 DS-GVO). Dies umfasst beispielsweise die Einbindung von Gremien der Mitbestimmung, zum Beispiel von Betriebsräten.

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. Gegebenenfalls nimmt der Verantwortliche eine Anpassung der Verarbeitungsvorgänge vor, zum Beispiel 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.

Durchführung



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 (Erwägungsgrund 75 folgende).

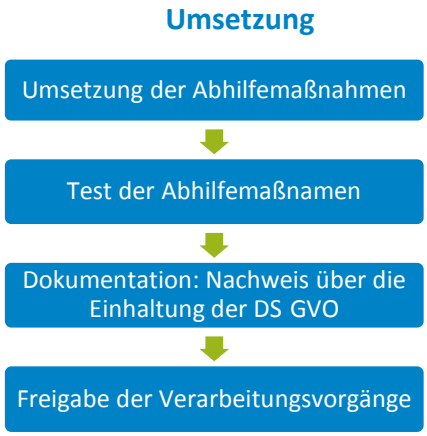
9. *Auswahl geeigneter Abhilfemaßnahmen*
   Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch TOMs) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und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

10. *Erstellung des DSFA-Berichts*

Der DSFA-Bericht enthält gemäß Artikel 35 Absatz 7 DS-GVO jedenfalls 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 Artikel 5 Absatz 2 DS-GVO normierten Rechenschaftspflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen.

Weitere Schritte nach Durchführung der DSFA

Die folgenden Schritte dienen der Implementierung der Abhilfemaßnahmen und sollten nicht lediglich linear durchlaufen werden, sondern eine Rückkoppelung der jeweiligen Ergebnisse im Sinne eines iterativen Vorgehens ermöglichen. Beispielsweise können durch eine Maßnahme weitere Verarbeitungsvorgänge nötig werden, für die wiederum etwaige Risiken zu betrachten sind.



11. *Umsetzung der Abhilfemaßnahmen*

Bevor die geplante Datenverarbeitung eingesetzt wird, müssen die für die Eindämmung des Risikos geeigneten Abhilfemaßnahmen (insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, sodass sie den Anforderungen der DS-GVO genügen.

12. *Test der Abhilfemaßnahmen*

Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

13. *Dokumentation: Nachweis über die Einhaltung der DS-GVO*

Gemäß Artikel 5 Absatz 2 DS-GVO hat der Verantwortliche eine umfassende Dokumentations- und Rechenschaftspflicht, durch die die Einhaltung der DS-GVO insgesamt nachgewiesen werden soll. Der DSFA-Bericht und eine Bestätigung der Wirksamkeit der umgesetzten Maßnahmen dienen als Bausteine zur Erfüllung dieser Pflicht.

14. *Freigabe der Verarbeitungsvorgänge*

Im Anschluss und mit Vorliegen der vollständigen Dokumentation können die Verarbeitungsvorgänge formal durch den Verantwortlichen freigegeben werden.

15. *Gegebenfalls Überprüfung und Audit der DSFA*

Um eine ordnungsgemäße Durchführung sicherzustellen, kann es sinnvoll sein, den DSFA-Bericht von einem unabhängigen Dritten überprüfen zu lassen. Auch könnte der Datenschutzbeauftragte, der gemäß Artikel 35 Absatz 2 DS-GVO sowieso einzubeziehen ist, die DSFA abschließend prüfen und das Ergebnis der Leitungsebene des Verantwortlichen mitteilen.

16. Fortschreibung

Die DSFA ist kein strikt linearer oder abgeschlossener Prozess. Vielmehr muss die Einhaltung der DS-GVO während der gesamten Dauer der Verarbeitungsvorgänge fortlaufend überwacht werden. Hierfür bietet sich ein Datenschutz-Managementsystem an. Spätestens wenn sich das mit der Verarbeitung verbundene Risiko ändert, muss erneut eine DSFA durchgeführt werden.

Umgang mit hohen Restrisiken

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 Artikel 36 DS-GVO 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 gegebenfalls welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Artikel 58 DS-GVO genannten Befugnisse ausüben und zum Beispiel eine Warnung, Anweisung oder Untersagung aussprechen.

Fazit

Die Datenschutz-Folgenabschätzung ist ein sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine der wichtigsten Neuerungen der DS-GVO gegenüber dem Bundesdatenschutzgesetz dar. Rechtzeitig auf den Weg gebracht hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der Grundverordnung umzusetzen.