

Kurz und knapp erklärt:

Datenschutz-Folgenabschätzung (DSFA)

[Anforderung] Was sagt das Gesetz?

Wann eine Datenschutz-Folgenabschätzung durchzuführen ist, verrät Art. 35 DSGVO:

Artikel 35:

„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.“ [Absatz 1; Sondertatbestände siehe Anlage]

[Maßnahmen] Was ist zu tun?

Verantwortliche müssen, um Ihren Pflichten nach Art. 35 nachzukommen:

- » Alle Verarbeitungen im Unternehmen einer Risikoeinschätzung unterziehen;
- » Die Verarbeitungen mit den speziellen Tatbeständen des Art. 35 Absatz 3 abgleichen;
- » Bei Ermittlung hoher Risiken ist eine Datenschutz-Folgenabschätzung durchzuführen;
- » Dokumentation der Datenschutz-Folgenabschätzung;
- » ggfs. Konsultation der Aufsichtsbehörde, wenn keine Risikoverminderung erreicht wird.

Dieser Prozess sollte von Datenschutz-Experten begleitet werden, um die gesetzlichen Bestandteile erfüllen zu können und durch Maßnahmen eine Risikoverminderung herbeizuführen.

Hinweis: Beachte auch One Pager „Risikobewertung“.

[Nutzen] Was bringt mir das?

Dieser gesetzliche Aufwand hat auch wesentliche Vorteile für das durchführende Unternehmen:

- » Erhöhung des Vertrauens seitens der Belegschaft
- » Erkennung von Schwachstellen und rechtlichen Risiken (frühzeitige Abhilfe)
- » Beitrag zum Business-Continuity-Management;
- » Erhöhung des Schutzes von Daten und IT-Systemen sowie der Informationssicherheit.

[UIMC] Wie hilft die UIMC?

Die UIMC hat ein pragmatisches Verfahren etabliert, eine Datenschutz-Folgenabschätzung effizient und lösungsorientiert durchzuführen. Hierbei kommen Datenschutz-Berater und -Auditoren mit langjähriger Erfahrung zum Einsatz. Insbesondere bei der Risikoverminderung können wir hilfreiche Maßnahmen und praxis-erprobte Handlungsempfehlungen aussprechen sowie bei der Umsetzung unterstützen.

[Anlage] Sondertatbestände für Datenschutz-Folgenabschätzungen und gesetzlicher Inhalt

Neben der allgemeinen risikoabhängigen Datenschutz-Folgenabschätzung nennt die DSGVO weitere Sachverhalte, bei deren Verwirklichung eine solche verpflichtend durchzuführen ist:

Art. 35 Absatz 3 DSGVO

„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;“

Zur Beurteilung insb. der Sondertatbestände sollte der Datenschutzbeauftragte involviert werden, denn auch das **Nicht-Zutreffen** bei grenzwertigen Verarbeitungsvorgängen **ist zu argumentieren** und zu dokumentieren.

Kommt man in der Beurteilung zu dem Schluss, dass eine Datenschutz-Folgenabschätzung durchzuführen ist, wird ebenso genau vorgeschrieben, welchen Inhalt diese haben muss:

Art.35 Absatz 7 DSGVO

„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.“

Die Erstellung erfolgt demnach nach einem bestimmten Muster, das vollständig vorliegen muss, um anerkannt zu werden und um der Rechenschaftspflicht zu genügen. Dabei treten oft Schwierigkeiten in der Erstellung auf, die durch die Unterstützung/Beratung von Experten aufgelöst werden können.

Hier empfiehlt es sich, mit unseren Datenschutz-Experten zusammenzuarbeiten, um alle Vorgaben vollumfänglich erfüllen zu können.