

# Kostenlose Vorlage:

# Richtlinie zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA) gemäß DSGVO

Bei diesem Dokument handelt es sich um eine kostenlose Vorlage bzw. Checkliste der activeMind AG zu den Themenbereichen Datenschutz und Datensicherheit. Die aktuellste Version finden Sie stets auf [im Downloadbereich unserer Website](https://www.activemind.de/datenschutz/dokumente/).

Sie können dieses Dokument an die Bedürfnisse in Ihrem Unternehmen anpassen, speichern und ausdrucken. Bitte haben Sie Verständnis dafür, dass die activeMind AG keinerlei Haftung für etwaige Fehler übernimmt.

Bei Fragen oder Problemen helfen wir Ihnen gerne weiter!

Ihr Team der activeMind AG

Telefon: +49 (0)89 / 91 92 94 – 900  
E-Mail: [anfrage@activemind.de](mailto:anfrage@activemind.de)  
Web: <https://www.activemind.de>

Richtlinie: Risikoanalyse und Durchführung von Datenschutz-Folgenabschätzungen

Jedes Unternehmen hat die gesetzliche Pflicht, personenbezogene Daten risikoangemessen zu schützen. Die Risikobestimmung erfolgt dabei individuell für jede Verarbeitung und ist bei veränderten Umständen (z.B. Einsatz neuer Technologien oder neuer Auftragsverarbeiter) zu wiederholen. Entscheidend ist dabei das Risiko aus Sicht des Betroffenen. Wurde im Rahmen der Risikoanalyse ein hohes Risiko für die betroffenen Personen, deren Daten verarbeitet werden sollen, festgestellt, muss vom Unternehmen eine Datenschutz-Folgenabschätzung durchgeführt (DSFA) werden.

Ziel einer DSFA ist es die Risiken für die betroffenen Personen zu analysieren, indem die potentiellen Schäden für die betroffenen Personen sowie die möglichen Ursachen dafür identifiziert werden und geeignete und wirksame (technische und organisatorische) Maßnahmen ausgewählt werden, um diese Risiken zu reduzieren.

Diese Richtlinie stellt Regeln zur Durchführung einer Datenschutz-Folgenabschätzung auf, um dem potentiellen hohen Risiko für die betroffenen Personen bereits im Vorfeld zu begegnen.

Verstöße gegen die Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen, können Schadensersatzansprüche nach sich ziehen und nach EU-Datenschutz-Grundverordnung (DSGVO) mit sehr hohen Bußgeldern geahndet werden. Neben den direkten Schäden kann auch das Ansehen des Unternehmens dauerhaft beeinträchtigt werden und dies zu einem Vertrauensverlust seitens der betroffenen Personen führen.

Werden hohe Risiken nicht eingedämmt, sind Datenschutzverletzungen sehr wahrscheinlich. Diese können für das Unternehmen, Partner und Kunden sowie vor allem für die betroffene Person schwerwiegende Folgen haben.

Diese Richtlinie soll deshalb eine konkrete Hilfestellung zur Bestimmung des relevanten Risikos und der korrekten Durchführung von Datenschutz-Folgenabschätzungen geben.

# Präambel

Fügen Sie hier eine Kurzbeschreibung Ihres Unternehmens und die Motivation zur Einhaltung des Datenschutzes in Ihrem Unternehmen ein. Sollen mit dieser Richtlinie besondere Ziele erreicht werden, gehören diese Informationen auch hierher.

# Geltungsbereich

* Unternehmen
* Ggf. externe Personen / Auftragsverarbeiter (z.B. im Rahmen einer Unterstützungspflicht)

# Gesetzliche Grundlagen

Folgende Regelungen sind im Zusammenhang mit einer Datenschutz-Folgenabschätzungen besonders relevant (die Liste ist nicht abschließend):

* Art. 35 DSGVO
* Art. 36 DSGVO
* Erwägungsgründe 75, 84, 89, 90 – 96

# Rollen

Festlegung der Rollen und Verantwortlichkeiten, z. B.:

* Gesamtverantwortlichkeit (Geschäftsführung)
* Durchführungsverantwortung (intern und ggf. extern)
* Datenschutzbeauftragter (Beteiligungspflicht, Art. 35 Abs. 2 DSGVO)
* Ggf. Hersteller / Lieferanten von IT-Systemen und Anwendungen
* Ggf. Vertreter der von der Verarbeitung betroffenen Personen / Kreise

# Risikoanalyse

* Vereinfachte Methode zur Bestimmung des Risikos z.B. durch die sog. Schwellwertanalyse unter Berücksichtigung der Empfehlungen der [Art. 29 Gruppe, WP248](https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf)
* Ermittlung des Risikos in anderen Fällen:
  + Begriffsklärung „Risiko“, z.B. anhand der Erwägungsgründe 75 und 92
  + Darstellung der Vorgehensweise zur Risikoidentifikation mit
    - Auflistung möglicher Schäden für betroffene Personen hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität (z.B. Finanzielle Verluste, Diskriminierung, Identitätsdiebstahl)
    - Beispielhafte Nennung von Ereignissen, die zu den o.g. Schäden führen können (z.B. Verlust von IT-Geräten, Versehentliche Löschung oder Vernichtung von Daten)
    - Darstellung der wesentlichen Quellen möglicher Schäden (z.B. Cyberkriminelle)
  + Festlegung von Stufen (z.B. von gering bis groß) der Eintrittswahrscheinlichkeit und der Schwere möglicher Schäden
  + Erläuterung der grundsätzlichen Bewertung der festgestellten Risiken nach Schwere des Schadens und Höhe der Eintrittswahrscheinlichkeit (z.B. anhand einer Skala, siehe auch [DSK-Kurzpapier Nr. 18](https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf))
  + Darstellung der grundsätzlichen Behandlung der Risiken auf den verschiedenen Risiko-Levels („gering“, „normal“, „hoch“).

# Durchführung der Datenschutz-Folgenabschätzung

* Auflistung, wann zwingend eine Datenschutz-Folgenabschätzungen durchzuführen ist, insbesondere bei Treffern auf der [Positivliste](https://www.datenschutzkonferenz-online.de/anwendungshinweise.html) oder in den gesetzlich genannten Fällen des Art. 35 Abs. 3 a bis c DSGVO
* Pflichtinhalte einer DSFA, Art. 35 Abs. 7 DSGVO, insbesondere:
  + detaillierte Beschreibung des Verarbeitungsvorgangs und welche Angaben für die detaillierte Beschreibung notwendig sind (z.B. Art, Umfang, Umstände, Zwecke der Verarbeitung, Empfänger, Speicherfrist usw.).
  + Bewertung der Verhältnismäßigkeit (insbes. Rechtmäßigkeit, Zweckbindung, Datenminimierung, Speicherbegrenzung, Rechte der Betroffenen, Auftragsverarbeitung, Garantien in Bezug auf Drittstaaten).
  + Detaillierte Bestimmung und Bewertung der festgestellten Risiken für die Rechte und Freiheiten der betroffenen Personen, ggf. Identifizieren weiterer Risiken.
  + Beschreibung der Pflicht zur Reduzierung der Risiken und wie mit Restrisiken umgegangen wird.

# Aufgaben des Durchführungsverantwortlichen

Beschreibung der Aufgaben (Zusammenstellung des DSFA-Teams, Prüfung der DSFA, Risikoanalyse, Veranlassung von Maßnahmen zur Risikoreduzierung, Dokumentation der DSFA, Beteiligung des DSB etc.).

Wichtig ist, dass alle relevanten Fachkreise an der DSFA beteiligt werden, um eine möglichst vollständige Beurteilung der Risiken und Abhilfemaßnahmen gewährleisten zu können.

# Dokumentation und Nachbereitung

Die Datenschutz-Folgenabschätzung ist vollständig und aussagekräftig zu dokumentieren. Der in der Richtlinie beschriebene Prozess ist zu bewerten und zu dokumentieren.