Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

# Datenschutzfolgenabschätzung und künstliche Intelligenz

MICHAEL RÄTZE


Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Für besondere Formen der Verarbeitung personenbezogener Daten, sieht Art. 35 Datenschutzgrundverordnung (DSGVO) eine sog. Datenschutzfolgenabschätzung vor. Diese ist durch den Verantwortlichen der Verarbeitung durchzuführen. Er schätzt dabei die Risiken für die Betroffenenrechte ein, die von der Verarbeitung ausgehen. Wie dies grundsätzlich unter dem Einsatz von künstlicher Intelligenz (KI) zu erfolgen hat, erläutern wir in diesem *Nachgelesen*.

Die Inhalte:




## Impressum

**HERAUSGEBER**
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

**REDAKTION** Diana Falke

**GESTALTUNG**
PUNKT191 – Marketing und Design
www.punkt191.de

**BILDNACHWEIS TITEL**
jofreepik auf Freepik.com

**VERÖFFENTLICHUNG** Januar 2023


## Die Datenschutzfolgenabschätzung im Überblick

Gem. Art. 35 DSGVO hat der Verantwortliche vor der Verarbeitung von personenbezogenen Daten eine Datenschutzfolgenabschätzung (DSFA) durchzuführen, sofern mit der Verarbeitung ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der Betroffenen einhergeht. Ziel ist die Bewertung des Risikos als Grundlage für die Vereinbarkeit mit der DSGVO. Für diese Risikobewertung ist nicht allein die Informationssicherheit ausschlaggebend, auch wirtschaftliche oder gesellschaftliche Nachteile sind zusammen mit ihrer Eintrittswahrscheinlichkeit zu betrachten. Der Verantwortliche prüft seine Verarbeitungsvorgänge auf eventuelle Risiken hin.

Art. 35 Abs. 1 und 3 DSGVO enthalten Kriterien, wann eine DSFA notwendig wird. Diese werden durch Listen der Aufsichtsbehörden gem. Art. 35 Abs. 4 und 5 DSGVO ergänzt. Den erforderlichen Inhalt einer DSFA liefert Art. 35 Abs. 7 DSGVO.

## Kriterien der Datenschutzfolgenabschätzung

Art. 35 Abs. 3 DSGVO konkretisiert den Abs. 1, der recht abstrakt von hohen Risiken spricht, indem er drei Fallgruppen benennt, in denen eine DSFA erforderlich ist. Diese Aufzählung ist nicht abschließend, sondern benennt Beispiele für solche Situationen.

Die erste Fallgruppe erfasst die „systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen“ durch eine automatisierte Verarbeitung (Art. 35 Abs.3 lit a.). Beispiele hierfür sind das Scoring oder automatisierte Einzelfallentscheidungen.

Die zweite Fallgruppe erfasst die „umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten“ (Art. 35 Abs. 3 lit. b.). Dazu gehören vor allem die besonderen Daten aus Art. 9 DSGVO, die teilweise als „sensible Daten“ bezeichnet werden. Dazu zählen u. a. Informationen zur rassischen oder ethnischen Herkunft, Religionszugehörigkeit, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten.

Die dritte Fallgruppe erfasst die „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c.). Dazu zählen beispielsweise Video-, Ton- oder Sensorüberwachungen im öffentlichen Raum.

## Mögliche Risiken beim Einsatz von KI

Werden KI-Systeme in Bereichen eingesetzt, in denen personenbezogene Daten verarbeitet werden, entstehen eine Reihe von grundsätzlichen Risiken. Solche Risiken bestehen bei der Verarbeitung reiner Sach- und Maschinendaten nicht. Das Profiling birgt die Gefahr der Preismanipulation. Auch das KI-gestützte Tracking oder die Identitäts-Identifikation, etwa durch Gesichtserkennung, sind nicht frei von Risiken, da sie einen Verlust der Anonymität bedeuten können. Wird KI zur Verhaltensanalyse eingesetzt, kann ggf. das Kaufverhalten manipuliert werden und das Risiko eines Kontrollverlusts über die eigene Entscheidung entstehen. Ebenso ist das Risiko der Diskriminierung aufgrund von Gruppenbildung in einem Bewerbungsverfahren denkbar. Auf diese und andere Risiken hin sind KI-Systeme zu untersuchen. Helfen können hier die von der Datenschutzkonferenz herausgearbeiteten Prinzipien bzw. datenschutzrechtlichen Anforderungen, welche an KI-Systeme zu stellen sind.

**DATENSCHUTZRECHTLICHE ANFORDERUNGEN AN KI-SYSTEME:**

1. KI darf Menschen nicht zum Objekt machen
2. KI darf nur für verfassungsrechtlich legimitierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben
3. KI muss transparent, nachvollziehbar und erklärbar sein
4. KI muss Diskriminierungen meiden
5. Für KI gilt der Grundsatz der Datenminimierung
6. KI braucht Verantwortlichkeit
7. KI benötigt technische und organisatorische Standards

## Durchführung einer Datenschutzfolgenabschätzung

Eine DSFA muss gem. Art. 35 Abs. 7 DSGVO mindestens Folgendes enthalten

- **eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen:** In KI-Systemen übernimmt üblicherweise der Algorithmus die Verarbeitungsvorgänge, welcher die entsprechenden Datensätze analysiert. Hier stößt man ein Stück weit auf die Blackbox-Problematik, also die Schwierigkeit von außen zu erkennen, auf welcher Grundlage die KI eine Entscheidung getroffen oder einen Schluss gezogen hat. Die Norm geht jedoch von einer Beschreibung der geplanten Verarbeitungsvorgänge aus. Es genügen daher Beschreibungen, soweit sie prinzipiell möglich sind.

- **eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck:** Für die Risikobewertung werden die Verarbeitungsvorgänge mit den rechtlichen Anforderungen abgeglichen. So normiert Art. 5 Abs. 1 lit. c.) DSGVO den Datenminimierungsgrundsatz. Das heißt, es dürfen nur Daten verarbeitet werden, die erheblich, erforderlich und angemessen für den Zweck sind. Das widerspricht natürlich ein Stück weit den großen Datenmengen, welche KI in der Regel braucht, um verwertbare Ergebnisse generieren zu können. Daher empfiehlt es sich, soweit möglich, mit synthetischen, künstlichen oder anonymisierten Daten zu arbeiten.

- **eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person:** Die Risikobewertung kann anhand des Standard-Datenschutzmodells und seinen sieben Gewährleistungszielen erfolgen. Diese lauten Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit. Die einzelne Risikobewertung ist das Verhältnis aus Eintrittswahrscheinlichkeit und Schadenshöhe.

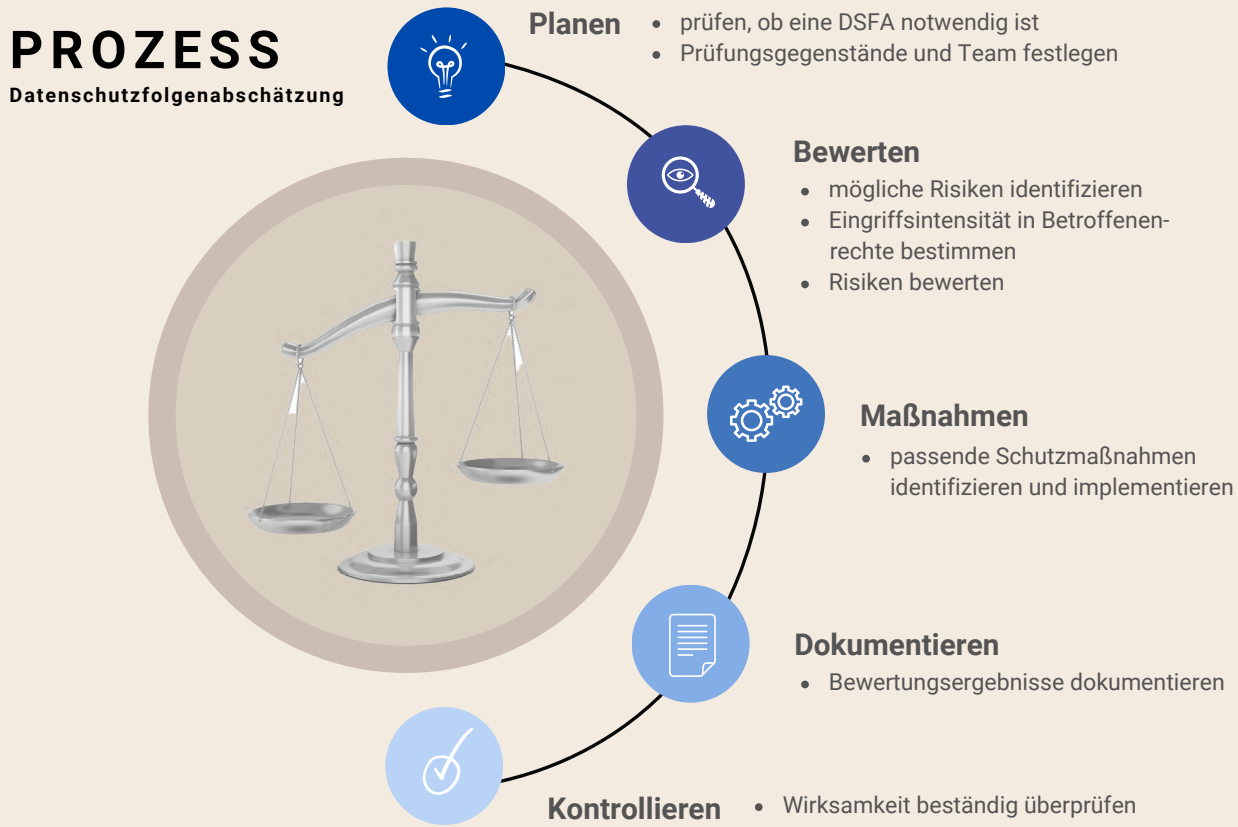


Abbildung 1: Prozess Datenschutzfolgenabschätzung

- **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 Risiken können durch technische und organisatorische Maßnahmen minimiert werden. Solche sind zum Beispiel Transport- und Inhaltsverschlüsselung von Daten, Schulungen für Mitarbeiter, Zugriffs-, Berechtigungs- und Löschkonzepte. Für KI-Systeme empfiehlt es sich, einen Mitarbeiter mit der Kontrolle dieser Systeme zu beauftragen.

## Zusammenfassung

Aufgrund der KI-Systemen grundsätzlich innewohnenden Risiken und der Einstufung als neue Technologie im Sinne des Art. 35 Abs. 1 DSGVO ist eine Datenschutzfolgenabschätzung stets notwendig. Allerdings verlangt das Gesetz nichts Unmögliches und durch die Orientierung, welche das Standard-Datenschutzmodell gibt, ist die effiziente Durchführung einer Datenschutzfolgenabschätzung möglich.

# Autor

**MICHAEL RÄTZE** ist wissenschaftlicher Mitarbeiter an der Professur für Privatrecht und Recht des geistigen Eigentums von Prof. Dr. Dagmar Gesmann-Nuissl an der Technischen Universität Chemnitz. Im Mittelstand-Digital Zentrum Chemnitz ist er als Fachkoordinator Recht tätig und beschäftigt sich mit Schnittstellen-Themen wie dem Datenschutzrecht, dem Arbeitsrecht oder dem Wettbewerbsrecht.
michael.raetze@digitalzentrum-chemnitz.de

# Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

**WAS IST MITTELSTAND-DIGITAL?**

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages