

KI und Datenschutz

Anne Riechert

KI und Datenschutz

Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen:

https://www.datenschutzkonferenz-online.de/media/en/20191106_entschlie%C3%9Fung_KI_DSK.pdf

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder - Stand: 06.11.2019

KI und Datenschutz

Positionspapier der Datenschutzkonferenz zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen:

https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf - Stand: 06.11.2019

Datenethikkommission

Verständnis der Datenethikkommission zu KI :

Datenethikkommission

Sammelbegriff für Technologien/Anwendungen:

- die ein Ergebnis ermitteln
- das ggf. automatisiert zur Anwendung gebracht wird

und zwar

- durch digitale Methoden
- auf der Grundlage sehr großer und heterogener Datensätze
- in einem komplexen und die menschliche Intelligenz gleichsam nachahmenden maschinellen Verarbeitungsprozess

Datenethikkommission

- „KI ist eine besondere Ausprägung von algorithmischen Systemen “
- Bandbreite der KI nutzenden Anwendungen:
 - ⇒(Einfache) Errechnung von Wegerouten
 - ⇒Bild- und Spracherkennung/-erzeugung
 - ⇒komplexe Entscheidungs-, Vorhersage- und Beeinflussungsumgebungen

Datenethikkommission

Hinweis auf Unterscheidung „maschinelles Lernen“ und „Künstliche Intelligenz“:

⇒ Im aktuellen Sprachgebrauch wird Maschinelles Lernen als Künstliche Intelligenz (KI) bezeichnet

⇒ Maschinelles Lernen: „schwache KI“ (bzw. Verfahren innerhalb der „schwachen KI“), die „wohlspezifizierte“ Aufgaben löst

⇒ „Starke KI“: soll ein breites Spektrum von Aufgaben (teilweise) ohne Eingriffe eines Menschen bewältigen

Datenethikkommission

Rechtliche und ethische Fragestellungen?

⇒ z.B. Möglichkeit der Diskriminierung

Anforderungen aus der DSGVO

Datenverarbeitung

Anforderungen aus der DSGVO

z.B.:

- **Verzeichnis von Verarbeitungstätigkeiten**
- **Datenschutz-Folgenabschätzung**
- **Informations- und Auskunftspflichten**

Anforderungen aus der DSGVO

- **Verzeichnis von Verarbeitungstätigkeiten**

⇒ Dokumentation der Datenverarbeitung

⇒ Etwa Zweck der Verarbeitung : Was ist Beweggrund und Ziel der Verarbeitung?
(z.B. Datenerhebung für eine Entscheidung im Bewerbungsverfahren)

Anforderungen aus der DSGVO

Verzeichnis von Verarbeitungstätigkeiten

⇒ https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf (Hinweise)

⇒ https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Muster_Verzeichnis_Verantwortlicher.pdf;jsessionid=36FEF53D39A5A60B3783F371F20226DD.1_cid343?blob=publicationFile&v=2
(Muster zum Verarbeitungsverzeichnis Verantwortlicher)

Anforderungen aus der DSGVO

- **Datenschutzfolgenabschätzung**

⇒ Prüfung der Risiken einer Datenverarbeitung für die persönlichen **Rechte und Freiheiten** von Betroffenen

⇒ Dokumentationspflichten

⇒ Abhilfemaßnahmen

⇒ Interner Prozess

Anforderungen aus der DSGVO

*Unter welchen Voraussetzungen sind die **Rechte und Freiheiten** natürlicher Personen betroffen?*

⇒ zentraler Begriff in DSGVO

⇒ Risikobasierter Ansatz

⇒ Aber: keine Definition

Anforderungen aus der DSGVO

Liste der Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung durchgeführt werden muss:

Datenschutzkonferenz https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf

- ⇒ z.B. Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen in großem Umfang unter Anwendung von Algorithmen, die für die betroffenen Personen nicht nachvollziehbar sind und die dazu genutzt werden können, Entscheidungen zu treffen
- ⇒ Anwendungsbeispiel: Eine Auskunftfei führt ein Scoring im Hinblick auf die Vertrauenswürdigkeit von Personen durch

Anforderungen aus der DSGVO

Beispielhafter Kriterienkatalog der „Artikel-29-Datenschutzgruppe“:

⇒ **Datenschutz-Folgenabschätzung (-)**:

Werbung, die auf einer E-Commerce-Website und auf Grundlage von „begrenztem“ Profiling früherer Käufe und Verhalten angezeigt wird

⇒ Bewerten und Einstufen, aber nicht in großem Umfang

⇒ Insgesamt: sogenannte Schwellenwertanalyse

Anforderungen aus der DSGVO

„Schwellenwertanalyse“, ob hohes Risiko vorliegt:

- Bewerten oder Einstufen
- **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung**
- Systematische Überwachung
- Vertrauliche Daten oder höchst persönliche Daten
- **Datenverarbeitung in großem Umfang**
- **Abgleichen oder Zusammenführen von Datensätzen**
- Daten zu schutzbedürftigen Betroffenen
- **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**
- Fälle, in denen die Verarbeitung an sich die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert

Anforderungen aus der DSGVO

Datenschutzaufsichtsbehörden:

„Erfüllt ein Verarbeitungsvorgang zwei dieser Kriterien, muss der für die Datenverarbeitung Verantwortliche **in den meisten Fällen** zu dem Schluss kommen, dass eine Datenschutz-Folgenabschätzung obligatorisch ist.“

Anforderungen aus der DSGVO

Zu beachten ist:

- ⇒ Profiling als solches ist nicht verboten
- ⇒ Profiling als solches löst noch nicht die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung aus
- ⇒ Eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung besteht aber, wenn auf dieser Basis **eine Entscheidung** mit rechtlicher Wirkung oder mit erheblicher Beeinträchtigung getroffen wird

Anforderungen aus der DSGVO

Artikel-29-Datenschutzgruppe, Workingpaper WP 248 der (<https://www.datenschutz-bayern.de/technik/orient/wp248.pdf>)

Siehe auch: **Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz**,

<https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/datenschutz-folgenabschaetzung/>

Anforderungen aus der DSGVO

Kurzpapiere der Datenschutzkonferenz:

https://www.lida.bayern.de/media/dsk_kpnr_18_risiko.pdf (Risiko für die Rechte und Freiheiten natürlicher Personen)

https://www.lida.bayern.de/media/dsk_kpnr_5_dsfa.pdf (Hinweise
Datenschutzfolgenabschätzung)

Anforderungen aus der DSGVO

- **Informations- und Auskunftspflichten bei einer automatisierten Entscheidungsfindung**

⇒ Logik und Tragweite und angestrebte Auswirkungen

⇒ z.B. Änderung der Bezahlungsmöglichkeiten in Abhängigkeit der ermittelten Bonität

⇒ Keine Offenlegung des Algorithmus des Verfahrens beim Scoring wegen Verletzung von Geschäfts- und Betriebsgeheimnissen (siehe bereits BGH Rechtsprechung)

Anforderungen aus der DSGVO

**Verbot von automatisiert generierten
Einzelfallentscheidungen ohne das
Dazwischentreten eines Menschen**

Anforderungen aus der DSGVO

z.B. automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne menschliche Entscheidung (vgl. Erwägungsgrund 71 DSGVO)

Anforderungen aus der DSGVO

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Anforderungen aus der DSGVO

- Ausschließliche Entscheidung?
- Erhebliche Beeinträchtigung?
- Außerdem: Ausnahmen!

Anforderungen aus der DSGVO

Unter welchen Voraussetzungen
werden Entscheidungen gefällt?

„Ethische und rechtliche“ Anforderungen

Unterteilung der Datenethikkommission:

- Algorithmenbasierte Entscheidung („Empfehlung“)
- Algorithmengetriebene Entscheidung („Ranking“)
- Algorithmen determinierte Entscheidung („Systemauswahl“)

„Ethische und rechtliche“ Anforderungen

Datenethikkommission:

- Nachteile bereits bei Profilbildung als solcher, nicht erst bei einer Entscheidung
- Gesetzliche Verbote bestimmter kritischer Einsatzzwecke (z.B. Verwendung von Profilen, die aus Daten aus dem Privatleben gewonnen wurden, bei Bewerberauswahl)
- Digitaler Neuanfang

Ethics by Design

Was sind ethische Maßstäbe?

**(Wie) können ethische Maßstäbe
berücksichtigt werden?**

Ethics by Design

Datenethikkommission:

Maßstab für einen **verantwortungsvollen Umgang** mit KI: **Verfassung**, insbesondere die **Grundrechte** und die Prinzipien der **Rechts- und Sozialstaatlichkeit** sowie das **Demokratieprinzip**.

⇒ Schutz der individuellen Selbstbestimmung
Transparenz

⇒ Respektierung individueller Nutzerentscheidungen

⇒ Schutz vor ungerechtfertigter Diskriminierung

⇒ Überprüfung von maschinellen Entscheidungen

Ethics by Design

Datenethikkommission:

⇒ **Ethische Klassifikation von
Algorithmen**

Ethics by Design

Entwicklung einer fünfstufigen „Kritikalitätspyramide“:

Stufe 1:

Anwendungen ohne oder mit nur sehr geringem
Schädigungspotenzial

⇒ **keine Notwendigkeit** einer besonderen Kontrolle

Stufe 5:

Anwendungen mit unvertretbarem Schädigungspotenzial

⇒ **Vollständiges oder teilweises Verbot**

Ethics by Design

Stufen 2-4:

Anwendungen mit mäßigem **bis erheblichem**
Schädigungspotenzial

⇒ Zulassungsverfahren, Live-Schnittstelle zum System, ex-post-Kontrollen, Erstellen und Veröffentlichen einer angemessenen Risikofolgenabschätzung

Ethics by Design

Konkret:

- Aufsicht durch die bestehenden Behörden, z.B. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Datenschutzaufsichtsbehörden
- Regulierung algorithmischer Systeme im Recht der Europäischen Union (Verordnung für Algorithmische Systeme, EUVAS)

Ethics by Design

Warum?

Ethics by Design

Kritik (Bitkom):

- Generalverdacht für nahezu alle Algorithmen
- Im Regelfall kein Risiko von Diskriminierung oder Gefahr für Leib und Leben
- Risikobewertung ist für jeden einzelnen Algorithmus weder notwendig noch in der Praxis durchführbar

Ethics by Design

Warum zusätzliche Regulierung?

Datenethikkommission:

- ⇒ Risiken können sich auch dann für den Einzelnen und für Gruppen ergeben, wenn keine personenbezogenen Daten verarbeitet werden
- ⇒ Risiken stellen nicht unbedingt solche des Datenschutzes dar (z.B. Vermögen, Eigentum, körperliche Integrität oder Diskriminierung)
- ⇒ Zulassungsverfahren, Kennzeichnungspflicht zur Abwendung von Schäden für Betroffene, Bevölkerungsgruppen oder die Gesellschaft

Ethics by Design

Außerdem:

„Privacy by Design“ ?

⇒ Hersteller der Produkte, Dienste und Anwendungen sollten **ermutigt** werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen.....

⇒ Verantwortung?

Ethics by Design

Was ist zu tun?

Ethics by Design

Breite Diskussionen in der Öffentlichkeit:

- Neue Foren für Debatten
- Welche Rahmenbedingungen werden benötigt, damit Bürgerinnen und Bürger kompetent mit Anwendungen umgehen können und diese kritisch hinterfragen können?
- Außerdem: Fähigkeiten und Kompetenzen können verloren gehen – welche Auswirkungen hat dies auf die nächste Generation? Hat menschliches Handeln einen ethisch relevanten Wert?

(Siehe hierzu die Datenethikkommission!)

Ethics by Design

- Förderung und Entwicklung praktikabler und verständlicher und datenschutzfreundlicher Anwendungen
- Implementierung von „ethischen Grundsätzen“ bereits in der Analysephase der Softwareentwicklung

Ethics by Design

- Förderung der Datenportabilität, der Interoperabilität und damit auch der Datensouveränität: Wie können Verbraucher in ihren Alltagsentscheidungen unterstützt werden?
- Wann handelt ein Nutzer souverän? Unter welchen Voraussetzungen ist er in der Lage, einer Maschine überlegene Entscheidungen zu treffen?
-

Ethics by Design

Insgesamt: dynamische Entwicklung

Daher:

dynamischer und anpassungsfähiger
Prozess

Ethics by Design

- **Datenethikkommission:**

Gutachten:

https://www.bmjb.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html;jsessionid=48F70E8D3CD669ABCA7B375FF1CBF502.1_cid289?nn=11678504

Kurzfassung:

https://www.bmjb.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_Kurzfassung.html;jsessionid=48F70E8D3CD669ABCA7B375FF1CBF502.1_cid289?nn=11678504

Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung:

https://www.bmjb.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Empfehlungen.html;jsessionid=48F70E8D3CD669ABCA7B375FF1CBF502.1_cid289?nn=11678504

Ethics by Design

- Die **Europäische Kommission** hat im Juni 2018 eine Expertengruppe eingesetzt, die ethische Leitlinien für eine vertrauenswürdige Künstliche Intelligenz (KI) erarbeitet hat (<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>). Diese soll als Hilfestellung für die mögliche Umsetzung ethischer Grundsätze bei der Entwicklung und Anwendung von KI dienen. Im Februar 2020 hat die Kommission ein Weißbuch vorgestellt, in welchem auf die Leitlinien verwiesen wird (siehe Kapitel „Ökosystem des Vertrauens“). Weißbuch vom 19.02.2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf
 - <https://orbilu.uni.lu/bitstream/10993/38926/1/p60-dignum.pdf>
- ⇒ Ethics by Design: Necessity or Curse?