www.jusletter-it.eu

Christine Möhrke-Sobolewski

KI: Privacy Impact Assessment als Mittel zur Risikominimierung?

Artificial intelligence (AI) requires data protection – a plea for the efficient use of data protection impact assessments in the development of artificial intelligence. The following article deals with different aspects of artificial intelligence: After an introduction to criticism, myths and public opinion on AI projects (I), some serious data-based risks for companies and other affected individuals are explained (II). Finally, it is discussed how data protection as best practice ultimately serves to minimise risks and what prospects the European legislation offers for companies and affected individuals (III). (kg)

Category: Articles
Region: EU
Field of law: Artificial Intelligence & Law; Big Data, Open Data & Open Government; Data Protection

Citation: Christine Möhrke-Sobolewski, KI: Privacy Impact Assessment als Mittel zur Risikominimierung? , in: Jusletter IT 4 December 2018

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

I. Öffentliche Kritik, Mythen und Meinungsmache zu Big-Data-Analysen?

[Rz 1] Der österreichische Arbeitsmarktservice (AMS) will künftig die Chancen Arbeitsloser auf dem Arbeitsmarkt algorithmisch bewerten lassen. Big-Data-Analysen sollen die Entscheidungsgrundlage bieten, wer von der Behörde welche Maßnahmen zur Aufnahme einer neuen Arbeitsstelle vorgeschlagen bekommen soll.[1] Auf der Grundlage insbesondere von Alter, Geschlecht, Staatsangehörigkeit und Qualifikation soll dann mittels KI ein «Integrations-Chancenwert» berechnet werden, anhand dessen die Arbeitssuchenden in drei Gruppen («Hoch» = chancenreich, «Mittel» und «Niedrig» = chancenarm) eingeteilt werden. Ein ähnliches Beispiel auf unternehmerischer Ebene ist das Bewerbertool von Amazon,[2] das unter Bewerbern automatisch die besten herausfinden sollte.

[Rz 2] Die Ankündigung dieser Projekte hat in sozialen Medien und der Datenschutzöffentlichkeit hohe Wellen geschlagen. Big-data-basierte KI-Ansätze dieser Art sollen daher im Folgenden herangezogen werden, den risikobasierten Ansatz der (DSGVO) näher zu beleuchten.

[Rz 3] KI-Projekte, insbesondere die algorithmenbasierte Kategorisierung von Personen beispielsweise in arbeitsfähig/arbeitswillig und nicht arbeitsfähig/arbeitswillig stehen oft in öffentlicher Kritik. Gleichzeitig ist großes politisches Interesse zu verzeichnen, das Wachstumspotential von Big Data und KI zu fördern.

[Rz 4] «Ich bin der Überzeugung, dass wir die herausragenden Möglichkeiten der digitalen und keine Grenzen kennenden Technologien viel besser nutzen müssen. Hierfür brauchen wird allerdings den Mut, die bestehenden nationalen Silostrukturen in den Telekommunikationsvorschriften, im Urheberrechts- und Datenschutzrecht (..) und in der Anwendung des Wettbewerbsrechts aufzubrechen». [3]

---

1 Süddeutsche Zeitung, Arbeit aus den Automaten, https://www.sueddeutsche.de/digital/digitalisierung-arbeitslosigkeit-jobcenter-1.4178635, alle Websites zuletzt abgerufen am 23. Oktober 2018.

2 Jeffrey Dastin, Amazon scraps secret AI recruiting tool that showed bias against women, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

3 Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192&from=BG.

[Rz 5] Jean-Claude Juncker hob in seiner Agenda «Strategie für einen vernetzten digitalen Binnenmarkt» für die Kommission bereits 2014 die Bedeutung von Big Data und KI für den europäischen Markt und die Herausforderungen für die anwendenden Unternehmen hervor. Als Beispiele für die Art der Herausforderungen, vor denen sich die Unternehmen stehen sehen werden, nannte er: Urheberrecht, Datennutzungsrechte, offene und interoperable Systeme und Dienste, mangelnde Übertragbarkeit von Daten.

[Rz 6] Die EU-Kommission war sich des Potentials und der Relevanz insbesondere von KI-Projekten durchaus bewusst. Dennoch ist klar, dass neben Potentialen auch Risiken aus Big-Data-Analysen, die Grundlage für künstliche Intelligenz sind, erwachsen können. Davon betroffen sind zunächst einmal die Personen, auf die sich die analysierten Daten beziehen, und des Weiteren auch das Unternehmen, das sich auch bei gravierenden Entscheidungen auf die Ergebnisse von KI stützt.

II. Muss eine neue Risikobewertung bei KI vorgenommen werden?

[Rz 7] Viele Menschen fürchten um negative Entscheidungen durch KI.[4] Hintergrund ist: Viele von KI üblicherweise verwendeten Daten (Big Data) repräsentieren einen Teil von Persönlichkeit und Identität von Betroffenen und lassen möglicherweise unerwünschte Rückschlüsse auf sie zu.

[Rz 8] Erst Anfang 2017 hat daher das EP eine Entschließung zu Big Data auf den Weg gebracht.[5] Kernaussage: Diskriminierende Auswertungspraktiken müssen verhindert und die Betroffenenrechte gestärkt werden.

[Rz 9] Ein maßgeblicher Aspekt für diese Entschließung des EP war, dass Daten fragwürdiger Qualität sein können und damit eben nicht neutral sind. Mit Big Data können beispiellose Erkenntnisse über das menschliche Verhalten, ihr Privatleben und Gesellschaften gewonnen werden. Darauf beruhende KI verspricht einfache Entscheidungen. Ohne Zweifel kann daraus ein Mehrwert für die Vermittlung Arbeitssuchender, für die Gesundheitsfürsorge, den Klimawandel, den Energieverbrauch, die Verkehrssicherheit, die Effizienz/Optimierung von Unternehmen etc. gezogen werden.

[Rz 10] Big-Data-basierte Entscheidungen schmerzen nicht, solange der einzelne Betroffene nicht nachteilige Folgen spürt. Hat Big Data den Charakter von anonymisierten Statistiken, haben daher auch Datenschützer wenig Bedenken.

[Rz 11] Allerdings ist klar, dass gerade der Charme von KI in der Verknüpfung dieser vielen Daten liegt. Geht es um die Frage, ob eine Person diese oder jene Eigenschaft hat, wird sich mit einer Anonymisierung nicht viel gewinnen lassen. Es hilft nicht, zu wissen, dass eine Menge X wahrscheinlich weniger arbeitsfähig ist als eine Menge Y.

[Rz 12] Dazu kommt auch die Kraft des Faktischen: Je größer die Datenmenge, desto größer ist die Möglichkeit, dass sich eindeutige identifier in der Datenmenge befinden, die eine Identifizierung des Betroffenen erleichtern.

---

4 Vodafone Institut für Gesellschaft und Kommunikation, Wann Menschen bereit sind, ihre Daten zu teilen, https://www.vodafone-institut.de/de/studien/wann-menschen-bereit-sind-ihre-daten-zu-teilen/.

5 Entwurf einer Entschliessung des europäischen Parlaments http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0044&format=XML&language=DE.

III. Typische Big-Data-Risiken

[Rz 13] Die bereits erwähnten Aspekte von Big-Data-Anwendungen ziehen teils gravierende Risiken nach sich. Der Beitrag beschränkt sich im Folgenden auf vier der wesentlichsten Risiken, die im Rahmen der Zulässigkeitsbewertung von Big-Data-Anwendungen im Blick behalten werden müssen.

1. Risiko: Aufhebung der Pseudonymisierung oder gar der Anonymisierung

[Rz 14] Jede Anonymisierungstechnik ist nur so gut, wie die Unkenntnis über ihre De-Anonymisierung. Wird etwas Salz in die Daten gestreut und ein Hash, beispielsweise SHA 256 darüber gelegt, ist das heute noch als Anonymisierungstechnik in Ordnung. Aber wie sieht es aus, wenn diese sorgsam versalzenen und verschlüsselten Datenbestände mit anderen nicht ganz so gut anonymisierten Datenbeständen verknüpft werden? Oder wenn sich jemand Zugang zum Salz/zum Schlüssel verschafft? Kann man heute wirklich davon ausgehen, dass Verschlüsselung und die Anwendung altbekannter Anonymisierungstechniken auch künftig bestandskräftig sind? Im Gegenteil muss befürchtet werden, dass selbst heute verhältnismäßig starke Maßnahmen wie das u.a. von Apple genutzte differential privacy[6] – die verschränkte und differenzierte Anwendung verschiedener Anonymisierungstechniken auf Kopien des Originaldatensatzes unter gleichzeitiger kontinuierlicher Überwachung der einzelnen Abfragen – spätestens mit einem Populäraufkommen rechenstarker Quantenmechanik geschwächt werden.

[Rz 15] Nicht umsonst arbeitet der europäische Gesetzgeber stets mit der Floskel «state of the art»/«Stand der Technik» bei Normen wie Art. 25 DSGVO und dem dazugehörigen Erwägungsgrund (EG) 78 im Zusammenhang mit Verschlüsselungstechniken. Daher muss der einzelne Big-Data-Anwender im regelmäßigen Turnus seine Verschlüsselungs- und sonstigen Anonymisierungstechniken überprüfen.

[Rz 16] Darüber hinaus aber steigt das Risiko der Identifizierung der ursprünglich anonymen Daten mit dem Grad der Datenmenge. Wird ein Big-Data-Datenschatz, veröffentlicht und mit einem eingekauften Datenschatz verknüpft, der auch nur wenige personenbezogene Daten enthält, so kann es durchaus sein, dass sich darunter identifier finden, die den gesamten, also auch den zuvor anonymisierten Datenschatz wieder unter die strengen Normen des Datenschutzes fallen lassen, weil der einzelne Betroffene re-identifiziert werden kann. Das Risiko der De-Anonymisierung ist also durch den Einkauf fremder Daten immens gestiegen.

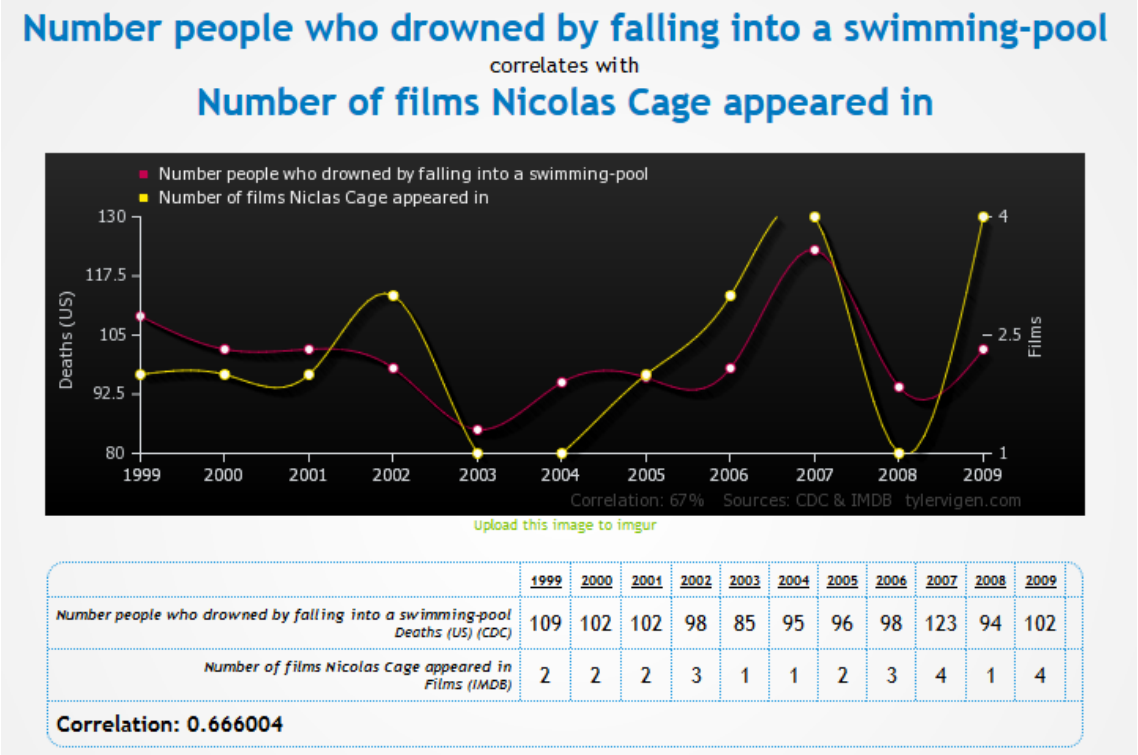
2. Risiko: nicht gesicherte Entscheidungsgrundlage

[Rz 17] Big Data ist nach wie vor nur statistische Wahrscheinlichkeit. Es geht um Korrelationen, nicht um Kausalitäten.

[Rz 18] So ist zum Beispiel die Grafik bekannt, wonach eine Korrelation zwischen der Anzahl der Personen, die in einen Pool gefallen sind und der Anzahl an Filmen, in denen Nicolas Cage mitspielt, vorhanden ist. Kann die Korrelation valide auf folgende Kausalität schließen lassen: Je

6 Art. 29-Gruppe, WP 216, S. 17ff.

weniger Filme in dem jeweiligen Jahr erscheinen, desto weniger Menschen fallen in einen Pool und ertrinken?



	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Number people who drowned by falling into a swimming-pool Deaths (US) (CDC)	109	102	102	98	85	95	96	98	123	94	102
Number of films Nicolas Cage appeared in Films (IMDB)	2	2	2	3	1	1	2	3	4	1	4

Correlation: 0.666004

CC-BY 4.0 tylervigen.com

[Rz 19] Sollte nun folgende Konsequenz gezogen werden: «Werden dieses Jahr viele Filme mit Nicholas Cage veröffentlicht, sollten die Pools besser überwacht werden?»

[Rz 20] Selbst bei noch so vielen Daten wird aller Voraussicht nach eine Kausalität zwischen dem Tod durch Ertrinken und der Veröffentlichung von Filmen mit Nicholas Cage beim besten Willen nicht begründet werden können. Dieses Beispiel zeigt, dass die Datenverarbeitung großer Datenmengen, und sei es auch in Echtzeit, nur so gut ist, wie die Fragestellung und die Schlussfolgerung.

[Rz 21] Dies stellt ein Risiko für beide Seiten dar: Unternehmen entbehren einer validen Basis für Entscheidungen, beispielsweise für die Einladung eines Bewerbers bei entsprechender Empfehlung eines solchen KI-Tools. Betroffene können die Grundlage einer KI-basierten Entscheidung nicht nachvollziehen und fürchten nachteilige Folgen für sich, wenn beispielsweise eine Korrelation aus Hobby und Vermittelbarkeit auf dem Arbeitsmarkt gezogen würde: «Wessen Hobby Eiskunstlauf ist, lässt sich schwerer vermitteln?»

[Rz 22] Reine Korrelationen bergen die Gefahr falscher Schlussfolgerungen. Die öffentliche Kritik beruht also im Wesentlichen auf bereits zwei undefinierten Ängsten: Sind die Daten wirklich anonymisiert und können valide Schlussfolgerungen daraus gezogen werden?

3. Risiko: Vertrauensverlust

[Rz 23] Ein dritter für Unternehmen nicht unwesentlicher Aspekt von Big-Data-Analysen ist die Fragilität von Vertrauen. Unternehmen, deren Philosophie in der Customercentricity liegt, nehmen diese Ängste und etwaiges Misstrauen der Kunden sehr ernst.

[Rz 24] Ängste und Vertrauensverlust entstehen dort, wo nicht nachvollziehbar ist, wie Entscheidungen zustande gekommen sind.

[Rz 25] Variable Preisbildung ist ein klassisches Beispiel: Uber nutzt dynamic pricing gerade in Stoßzeiten.[7] Ein Preisanstieg von USD 37 auf USD 135 in der Neujahrsnacht ist für Kunden zwar ärgerlich, aber angesichts der hohen Nachfrage durchaus nachvollziehbar.

[Rz 26] Uber wird aber auch mittels KI die Grenzen der Zahlungsbereitschaft herausfinden können. Dies kann routenabhängig ermittelt und Grundlage für entsprechende Schlussfolgerungen bei der weiteren (differenzierten) Preisbildung sein. Ein Ergebnis könnte sein, dass Bezirk A weniger zahlungsbereite Kundschaft aufweist als Bezirk B. Nachvollziehbar wäre also die Unternehmensentscheidung, bei hohem Verkehrsaufkommen und/oder schlechten Wetterbedingungen die Kundschaft für Bezirk B vorzuziehen und Kundschaft für Bezirk A im Regen auf andere Verkehrsmittel warten zu lassen. Führt dies in letzter Konsequenz dazu, dass an diesem oder jenem Platz künftig kaum noch Uber-Fahrzeuge auffindbar sein werden, weil die Kundschaft dort üblicherweise nicht so viel zahlt?

[Rz 27] Fakt ist: Uber nutzt alle verfügbaren Daten über Kundenverhalten entlang spezieller Routen, um kundenspezifische Preise zu verlangen. Die Unsicherheit darüber, warum der Preis wie zustande kommt, kann bei Kunden Angst vor Diskriminierung auslösen und Misstrauen schüren. Vertrauen aber ist eine der wesentlichsten Grundlagen für die Freigabe der Daten durch die Kunden.[8] Bei unternehmerischen Entscheidungen für oder gegen den Einsatz von KI spielen die genannten Aspekte eine wesentliche Rolle.

[Rz 28] Was bedeutet das jetzt aber für die Risikobewertung? Sie muss den Vertrauensverlust als eigene Risikokategorie einbeziehen.

4. Risiko: fehlende Datenqualität

[Rz 29] Bei der Erläuterung wesentlicher Risiken im Einsatz von Big-Data- oder KI-Tools darf auch ein technisches Risiko nicht unerwähnt bleiben: Das der Datenqualität. Bei den gigantischen Datenmengen, die von Big-Data-Anwendungen genutzt werden, entsteht eine ganz eigene weitere Risikostruktur: Stimmen die Daten nicht mit der Realität überein – finden sich also beispielsweise im Cluster «1. Klasse- Fahrer, Pendler» Daten, die diese Kriterien gar nicht abbilden – etwa Familien, die üblicherweise 2. Klasse fahren und den Regionalzug in den Ferien nutzen – so verfälscht dies die Aussage und damit die darauf beruhende unternehmerische Entscheidung etwa der Preisbildung. Drastischer ist folgendes Beispiel: Im Cluster «Chancenarm» fänden sich Daten zu Akademikern, weiblich mit Familie. Welche junge Nachwuchswissenschaftlerin mit Familie wird dann noch erfolgreich vermittelt werden?

---

7 Uber, Dynamic Pricing, https://www.uber.com/en-ZA/drive/resources/dynamic-pricing/.

8 Stefanie King, «Big Data: Potential und Barrieren der Nutzung im Unternehmenskontext», S. 162ff.

[Rz 30] Die Validität der Daten kann über Schicksale entscheiden, wenn KI die Grundlage aller Entscheidungen wird.

[Rz 31] Nur vollständige und richtige Daten gewährleisten valide KI-Ergebnisse. Bei der eigentlichen Risikoanalyse müssen daher auch die Daten selbst ins Visier kommen.

[Rz 32] Die Qualität der Daten muss dementsprechend als Risikoquelle erfasst werden.[9] Nicht alle Daten sind geeignet, die Realität in dem Maße abzubilden, wie dies die Fragestellung erfordert. Gute Entscheidungen und richtige Vorhersagen gelingen nur, wenn die Daten vollständig sind und ihre Qualität gesichert ist. Die Faktoren, die zu einer mangelnden Datenqualität führen, können vielfältig sein. Dazu zählen, um nur einige zu nennen, beispielsweise:

- Fehlerhafte Datensätze
- Fehler in der Interpretation
- Ungenaue oder fehlleitende Fragestellungen

Diese Faktoren bergen das Risiko, dass aus den Daten ein Modell gebildet wird, das die Wirklichkeit nicht oder nur unzureichend beschreibt. Damit steigt das Risiko unzulässiger Datenverarbeitung.

[Rz 33] So komplex und vielfältig die Risiken von KI-Projekten sind, so ehrgeizig und passgenau müssen die risikominimierenden Lösungen ausfallen. Um KI erfolgreich in ein Unternehmen zu integrieren, ist das Zusammenspiel vieler Abteilungen bzw. Kompetenzen nötig. Gerade weil KI-Strategien deshalb ressourcenintensiv sein können, lohnt es sich, die Risiken genau im Blick zu behalten.

IV. Datenschutz als Mittel der Risikominimierung

[Rz 34] Damit das Potential von KI gehoben werden kann und die Menschen weiterhin vertrauensvoll ihre Daten zur Verfügung stellen, bieten die europäischen Regelungen etwa der Datenschutzgrundverordnung unterstützende Rahmenbedingungen. Diese stellen bestimmte Aspekte in den Vordergrund, deren Bewältigung KI-Projekte zulässig und für die Öffentlichkeit akzeptabel machen.

[Rz 35] Datenschutz bezweckt den Schutz des Menschen vor Eingriffen in sein Recht auf informationelle Selbstbestimmung. Der Ursprungskonzeption nach ging es um den Bürger, der gegenüber dem Staat selbst über den Umgang mit seinen Daten entscheiden können sollte.

[Rz 36] Im Zusammenhang mit KI-Projekten eröffnet sich auch noch eine völlig neue Dimension der Datenschutzvorgaben: Der Datenschutz mit seinem umfangreichen Anforderungskatalog zum Schutz der Betroffenen, hilft KI-Projekten, auch die oben genannten Risiken in Schach zu halten. Anforderungen wie Folgenabschätzungen, Risikomanagement und Dokumentationen der vorab vorgenommenen Bewertungen, helfen, Risiken angemessen einzuschätzen, rechtzeitig Sicherheitsmaßnahmen zu treffen und somit eine KI-Anwendung sorgfältig im Betrieb zu implementieren. Datenschutz hilft also, die Risiken gigantischer Datenpools neu zu bewerten und in letzter Konsequenz zu minimieren.

9 Thomas Hoeren, MMR 2016, S. 8ff.

1. Privacy Impact Assessment, Art. 35 DSGVO

[Rz 37] Eines dieser Datenschutzinstrumente zur Risikominimierung dürfte hier das Data Privacy Impact Assessment nach Art. 35 DSGVO sein.

[Rz 38] Ziel einer jeden Risikoanalyse ist die Abschätzung des Risikos und Prüfung alternativer Verfahren. Fehlentwicklungen sollen innerhalb des Datenverarbeitungsprojekts vermieden werden, Bedrohungen vorab eingeschätzt und darauf beruhende Risiken bewertet werden. Wie hoch wird der mögliche Schaden sein? Welchen Nutzen haben Angreifer aus dem Angriff? Wie hoch ist der Aufwand eines Angriffs?

[Rz 39] Nach Art. 35 DSGVO besteht für besonders risikobehaftete Verarbeitungsvorgänge eine Pflicht zur vorherigen Analyse der Folgen der Datenverarbeitung. Wir haben es also mit einem Instrument zur Risikoerkennung und -bewertung zu tun.

[Rz 40] Mit Risiko ist hier die Prognose gemeint, dass ein Schaden eintritt.[10] Der Kontext der DSGVO bezieht sich dabei ausdrücklich auf Gefährdungen der Persönlichkeit Betroffener. Als typische Risiken heben EG 75 und 85 S. 1 DSGVO die Diskriminierung von Personen, Identitätsdiebstahl oder auch die unbefugte Aufhebung der Pseudonymisierung hervor. Ein Vertrauensverlust der oben beschriebenen Art erhält damit im Vergleich zu einem reinen finanziellen Schaden ein ungleich höheres Gewicht.

[Rz 41] Als wichtige Indizien für eine mögliche Schädigung oder Beeinträchtigung der persönlichen Rechte Betroffener versteht die DSGVO gerade Art, Umfang und die Häufigkeit der Verarbeitung. Softwaretools zur Aufbereitung von Big Data sind klassische Beispiele, in denen eine Pflicht zur Datenschutzfolgenabschätzung besteht.[11] Bei gigantischen Datenmengen potenzieren sich allein aufgrund der schieren Menge, der Geschwindigkeit und Vielfalt der Daten Art, Umfang und Häufigkeit der Verarbeitung.

[Rz 42] Je größer der Datenpool, desto folgenreicher kann mangelnde Qualität von Daten oder gar ein Missbrauch der Daten sein. Diese Risiken großer Datenpools vor dem Hintergrund sich immer weiter verbessernder Analysemöglichkeiten neu zu bewerten, gehört also zu jeder seriösen Beratung von KI-Projekten.

[Rz 43] Hier setzt die DSGVO an, die KI-Anwendungen bewusst nicht verbietet. Die DSGVO intensiviert vielmehr die Pflichten der verantwortlichen Stellen. Schon heute sollte zwar vor dem Hintergrund der IT-Sicherheit vor jeder Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens eine Risikobewertung vorgenommen werden. Auch heute schon sollte geprüft werden, ob und in welchem Umfang Gefahren für die Rechte der Betroffenen verbunden sind. Eine Bewertung und Ableitung von Maßnahmen anhand von Risiken ist in vielen Unternehmen keine neue Methode. Jedoch unterscheidet sich der Ansatz in der DSGVO von der reinen Betrachtung aus der Perspektive der Informationssicherheit.

[Rz 44] Die DSGVO hat beispielsweise das Privacy Impact Assessment/Datenschutzfolgenabschätzung mit umfangreichen Dokumentationspflichten versehen und der Risikobewertung teilweise auch eine zulässigkeitsbegründende (Bsp: Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9 Abs. 2 i.V.m. Art. 35 Abs. 3 lit. b) DSGVO) oder zumindest pflichtenerleichternde Rolle (Bsp: Entfall der generellen Meldepflicht, EG 89) gegeben.

---

10 Mario Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 35, Rn. 15a.

11 Mario Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 35, Rn. 18.

[Rz 45] Nach der DSGVO müssen die für die Verarbeitung Verantwortlichen geeignete Maßnahmen ergreifen, um sicherzustellen und den Nachweis dafür zu erbringen, dass die Verarbeitung gemäß der DSGVO erfolgt, wobei sie unter anderem die «unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen» (Art. 24 Abs. 1 DSGVO) berücksichtigen müssen.

[Rz 46] Zwar besteht nicht für alle Verarbeitungsvorgänge gleichermaßen eine Pflicht zur Durchführung einer Datenschutzfolgeabschätzung. Die Durchführung einer Datenschutzfolgeabschätzung ist nur dann obligatorisch, wenn die Verarbeitung «wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt», Art. 35 Abs. 1 DSGVO. Dies gilt insbesondere bei der Einführung neuer Datenverarbeitungstechnologien (EG 89) (z.B. Big-Data-Analysen, KI-Tools). Auch der Fall der systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (z.B. Videoüberwachung) nach Art. 35 Abs. 3 lit. c DSGVO macht beispielsweise eine Datenschutzfolgeabschätzung erforderlich.[12] Beide Fälle können klassische Anwendungsgebiete von Big-Data-Analysen oder KI-Anwendungen sein.

[Rz 47] Die datenschutzrechtlich vorgegebene Risikobewertung ist daher für KI zu einem besonders starken Gatekeeper geworden. Datenschutz entwickelt sich damit zu einem Frühwarnsystem, um geeignete Maßnahmen zur Risikominimierung zu planen und umzusetzen.

2. Leitlinien Privacy Impact Assessment der Art. 29-Gruppe

[Rz 48] Die Leitlinien der Art. 29-Gruppe zum Privacy Impact Assessment stellt Vorschläge zur Diskussion, wie Risikobewertungen künftig erfolgen sollten und welche Maßnahmen zur Abwehr persönlichkeitsrechtlicher Eingriffe getroffen werden sollten.

[Rz 49] Kriterien für ein akzeptables Privacy Impact Assessment sind demnach

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke der Verarbeitung
- Bestimmung der betroffenen Datenkategorien, Zugriffsberechtigungen, Fristen, etc. wie aus den Verfahrensmeldungen bekannt
- Bewertung von Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

a. Vorbereitungsphase

[Rz 50] Erste Prüfschritte zur Risikobewertung im Rahmen der Vorbereitungsphase sollten sein:

- Mögliche Risikoquellen identifizieren
- Bedrohungen identifizieren, die zu unerwünschten Datenverarbeitungen führen können
- Den potentiellen Einfluss des Risikos auf Rechte und Freiheiten der Betroffenen abschätzen
- Und die Wahrscheinlichkeit und Schweregrad des Eingriffs in die Persönlichkeitssphäre des Betroffenen abschätzen

[Rz 51] Für jedes Risiko empfiehlt es sich künftig dessen Ursprung, Natur und Schwere des Eingriffs zu prüfen.

12 Art. 29-Gruppe, WP 248 Rev. 01, S. 11.

b. Bewertungsphase

[Rz 52] Hieran schließt sich nahtlos die Bewertungsphase nach Art. 35 Abs. 7 lit. b) und c): Es muss bewertet werden, ob zwischen den legitimen Verarbeitungszielen und den dadurch ausgelösten Beeinträchtigungen ein angemessener Ausgleich erzielt werden kann. In dieser Phase müssen die Gefahrenlagen sowie die Gewährleistungsziele als Prüfungsmaßstab identifiziert werden und daraus erwachsende Konsequenzen auf die konkreten Verarbeitungsvorgänge herauskristallisiert werden.[13] Ziel der Bewertung muss sein,[14] einen Abgleich zwischen legitimen Verarbeitungszielen und den dadurch ausgelösten Beeinträchtigungen der Rechte und Freiheiten Betroffener vorzunehmen und auf dieser Grundlage zu einem angemessenen Ausgleich der kollidierenden Interessen zu gelangen.

[Rz 53] Gerade KI-Projekte haben schon mit der Beschreibung des konkreten Zwecks der Verarbeitung und der geplanten Verarbeitungsvorgänge zu kämpfen: Erst wenn die Korrelationen bekannt sind, kann beispielsweise bei der Personalfrühfluktuationsanalyse oder bei dem erwähnten AMS-Modell zur Kategorisierung Arbeitssuchender geprüft werden, zu welchem Zweck beispielsweise Alter, Geschlecht und frühere Arbeitgeber wie häufig verarbeitet werden müssen.

c. Umsetzungsphase

[Rz 54] Datenschutz bedeutet in diesem Zusammenhang auch, dass konkrete Maßnahmen getroffen werden, mit denen eine Bewältigung der Risiken erreicht werden kann. Diese müssen dokumentiert werden, um nachzuweisen, dass die Vorgaben der DSGVO eingehalten werden, vgl. Art. 35 Abs. 7, EG 84, 90. In dieser sog. Umsetzungsphase werden Abhilfemaßnahmen eingeleitet und dokumentiert. Die zuvor skizzierten gestiegenen Risiken wie Re-Identifizierbarkeit, Diskriminierung, Fälschungen sind im Blick. Hier bietet die datenschutzrechtlich nun erfolgende Maßnahmenphase, Raum, konkrete Instrumente zur Risikominimierung umzusetzen.

[Rz 55] Meist handelt es sich in diesem Zusammenhang um Maßnahmen technisch-organisatorischer Art: So gehören beispielsweise Anonymisierungsmaßnahmen zu den wichtigsten im Zusammenhang mit KI- oder Big-Data-Projekten. Wirksame Anonymisierung kann die Risikoabwägung zu Gunsten einer Big-Data-Anwendung ausfallen lassen. Jede Maßnahme zur Sicherung des Stands der Technik («state of the art») kann beispielsweise De-Anonymisierungsrisiken minimieren. Dazu gehören etwa regelmäßige Monitoring-Maßnahmen, mittels derer geprüft werden kann, welchem Stand der Technik die derzeitige Anonymisierungstechnik entspricht.

[Rz 56] Auch Penetrationtests, kurz Pentests – also Prüfung der Sicherheit von Netzwerkanwendungen oder Systembestandteilen mit Mitteln und Methoden, die ein Angreifer verwenden würde – regelmäßig prozessual eingebaut, unterstützen ebenfalls dabei den Stand der Technik zu halten. Auch Fortbildungsmaßnahmen des eingesetzten Personals, Aktualisierungen von Software etc. sind denkbare Maßnahmen zur Unterstützung einer sicheren Anonymisierung.

[Rz 57] Daneben sind auch juristische Maßnahmen wie der Abschluss eines Vertrages,[15] die Vereinbarung einer wirksamen Vertragsstrafe denkbar, um identifizierte Risiken einer KI-Anwendung zu minimieren.

---

13 Martin Rost/Kirsten Bock, DuD 2011, 30 (32f).

14 Marit Hansen in: Beck-OK|Datenschutzrecht, Wolff/Brink, DSGVO, Art. 35, Rn. 43ff.

15 Marit Hansen in: Beck-OK|Datenschutzrecht, Wolff/Brink, DSGVO, Art. 35, Rn. 48.

[Rz 58] Die Einhaltung der Prüfschritte der Datenschutzfolgenabschätzung stellt sich also als ein durchaus geeignetes und effizientes Instrument dar, diese Risiken nachhaltig zu verringern.

[Rz 59] Hier nimmt der Datenschutz damit eine Enabler-Rolle ein. Ein kooperatives Zusammenspiel zwischen Datenschutzaufsichtsbehörde und KI-Anwender nach den Regelungen der DSGVO, so umfangreich oder auch auslegungsbedürftig sie ohne Frage sein mögen, können helfen, KI-Projekte zulässig umzusetzen. Die Vorgaben bieten ein straffes Gerüst der Risikoprüfung, an dem sich auch die Entscheidungsfindung im Rahmen der Projektarbeit orientieren kann. So gelingt es, ohne unzulässige Eingriffe in die Persönlichkeitsrechte der Betroffenen und unter Wahrung der eigenen unternehmerischen Interessen das KI-Projekt umzusetzen.

V. Fazit

[Rz 60] Die datenschutzrechtlichen Vorgaben der DSGVO, die sich am Schutz des Betroffenen orientieren, können hilfreiche Anhaltspunkte bieten, auch unternehmerische Risiken zu minimieren. Schützte Datenschutz zunächst in erster Linie den Bürger – nämlich den Bürger einer offenen, auf freie Entfaltung bedachten Gesellschaft – gegenüber staatlicher Datenverarbeitung, so unterstützen datenschutzrechtliche Instrumente heute in einer Daten- und Informationsgesellschaft auch die datenverarbeitenden Stellen vor typischen datenbezogenen Risiken: Die Pflicht zur intensiven Prüfung der Risiken und die Schaffung etwaiger Abhilfemaßnahmen minimieren beispielsweise solche datenbasierte Risiken, deren Schaden sich mit der wachsenden Menge an Daten potenzieren kann.

[Rz 61] Unter Geltung der DSGVO, nach Durchführung und Einhaltung der dort implizierten strikten Pflichten und Risikominimierungsmaßnahmen wird der Erfolg eines Kategorisierungstools wie die algorithmenbasierte Entscheidung, ob ein Arbeitssuchender/Bewerber als chancenreich oder chancenarm eingeordnet wird, von der Risikoabwägung für die Interessen der Betroffenen abhängen. Das Wissen um Einhaltung und Kontrolle der datenschutzrechtlichen Regelungen aus der DSGVO könnte dann das Vertrauen in die Rechtmäßigkeit von KI-Anwendungen auch in der Öffentlichkeit wieder herstellen.

Christine Möhrke-Sobolewski, Rechtsanwältin/Syndikusanwältin bei der Deutschen Bahn AG, Doktorandin an der Universität Basel

Der Beitrag wurde mit Unterstützung des Schweizerischen Nationalfonds im Rahmen des SNF-Projekts NFP 75 «Big Data» erstellt.