LEITFADEN

ZUR DATENSCHUTZKONFORMEN GESTALTUNG VON KI-GESTÜTZTEN GESCHÄFTSMODELLEN, DIENSTEN UND PRODUKTEN BEI DER DEUTSCHEN TELEKOM

Group Headquaters, Group Privacy

Version 1.0
Stand 07.12.2018
Status *final*

INHALTSVERZEICHNIS

1 VORBEMERKUNGEN

Um einen Aufsetzpunkt für die Entwicklung von praktikablen Datenschutzvorgaben für KI-Systeme bei der Deutschen Telekom zu erhalten, wurde die breite öffentliche Diskussion zu künstlicher Intelligenz auf die aktuellen, datenschutzrechtlichen Erfordernisse der Deutschen Telekom fokussiert.
Dieser Leitfaden richtet sich an Produkt- u. Geschäftsmodellverantwortliche, Entwickler, PSA Anforderer von Systemen und Projekten mit KI-Anteil und an Datenschutzberater.
Nach der Datenschutz-Grundverordnung kann zwischen KI-Systemen, die als Assistenzsysteme den Menschen bei ihren Entscheidungen unterstützen und solchen Systemen, die eigenständig Entscheidungen treffen (automatisierte Einzelentscheidungen) unterschieden werden. Für KI-gestützte Assistenzsysteme gelten die allgemeinen datenschutzrechtlichen Regelungen der DSGVO. Für die sogenannten ADM Systeme (Algorithmic Decision Making) enthält Artikel 22 DSGVO spezielle Regelungen.
Unabhängig von dieser rechtlichen Differenzierung verschiedener KI-Lösungen, soll in der Deutschen Telekom eine einheitliche Governance für KI-Projekte gelten, die sowohl KI-Assistenzsysteme, als auch die sogenannten ADM-Systeme abdeckt.
Der vorliegende Leitfaden soll in der Phase zwischen Geschäfts- bzw. Produktidee und dem PSA Verfahren bei den operativ verantwortlichen Stellen für die erforderliche Orientierung und Handlungssicherheit sorgen.

2 ALLGEMEINE FRAGESTELLUNGEN

2.1 Was ist „Künstliche Intelligenz“?

Aktuelle KI-Systeme stellen eine Kombination aus Analysesystemen auf Basis formalisierten Expertenwissens (Data Warehouse, Business Intelligence) und maschinellem Lernen sowie der gezielten Anwendung des Erlernten dar. Bei dem einer KI regelmäßig zu Grunde liegenden Verfahren einer algorithmischen Entscheidungsfindung erfolgt auf Grundlage von Informationen eine Bewertung, die zu einer Entscheidung, Prognose oder Handlungsempfehlung führt. Damit birgt nicht lediglich die Datenverarbeitung selbst, sondern insbesondere die Entscheidung als Konsequenz der Verarbeitung ein potenzielles Risiko für den Betroffenen.

Die klassische IT mit ihren Elementen „Eingabe“ – „Verarbeitung“ – „Ausgabe“ wird um die Fähigkeiten „Wahrnehmen“ – „Verstehen“ – „Handeln“ – „Lernen“ erweitert1. Diese bisher eigentlich nur dem Menschen zugeordneten Eigenschaften können in zunehmend stärkeren Umfang auch durch Maschinen erledigt werden. Der Begriff „Verstehen“ ist im Zusammenhang mit Computern Neuland und muss im Hinblick auf die Nachvollziehbarkeit und Einhaltung ethischer Werte kritisch begleitet werden.

Maschinelles Lernen bezeichnet eine Reihe von Optimierungsmethoden u.a. in künstlichen neuronalen Netzwerken. Zwischen Ein- und Ausgabeschicht können KI-Systeme dabei sehr komplexe Strukturen aufweisen. Durch die Abbildung mehrerer hierarchischer Verarbeitungsschichten, kann das maschinelle Lernen erheblich effizienter werden (Deep Learning). Damit einher geht jedoch zwangsläufig ein Verlust an Nachvollziehbarkeit bei KI-Entscheidungen. Die tieferen Verarbeitungsschichten (Hidden Layer) entziehen sich wegen der Komplexität der Algorithmen und der Vielzahl der durch die Maschine vorgenommenen Rechenoperationen der Transparenz bei den Entscheidungskriterien und deren Gewichtung. Zwar ist die Offenlegung der der KI zu Grunde liegenden Algorithmen eine Kernforderung in der aktuellen Debatte um mehr Transparenz bei KI-Systemen; die konkrete Überprüfung der Entscheidungslogik hochkomplexer KI-Systeme anhand offengelegter Algorithmen dürfte in der Praxis jedoch schwierig sein. „Erklärbare KI-Systeme“ (Explainable AI) ist ein Ansatz, an dem derzeit intensiv geforscht wird. Wünschenswert wäre, dass KI-Systeme zukünftig die Entscheidungskriterien und deren Gewichtung bei Entscheidungen mitliefern.

[1] Vgl. Positionspapier Bitkom: https://www.bitkom.org/Bitkom/Publikationen/Kuenstliche-Intelligenz-Wirtschaftliche-Bedeutung-gesellschaftliche-Herausforderungen-menschliche-Verantwortung.html

Praktikabler ist zum gegenwärtigen Zeitpunkt eine Überwachung der Entscheidungsprozesse von KI-Systemen von „außen", bei der die durch die KI getroffenen Entscheidungen gegen eine zuvor festgelegte Zweckbestimmung des Systems und die „Ethik-Governance" geprüft werden.

KI-Entscheidungen, die außerhalb der erwarteten Bandbreite liegen, können identifiziert und es kann eingegriffen werden. Tools, die speziell zur Analyse von KI-Entscheidungen entwickelt werden, können dabei helfen. Es gilt aber der Grundsatz, dass eine Überwachung von Maschinen ausschließlich durch Maschinen paradox ist. Menschliche Beurteilungen müssen bei KI-Überwachungsprozessen immer dominieren.
Neben der Effizienz der Lernmechanismen, hängt erfolgreiches maschinelles Lernen nicht zuletzt von Menge und Qualität der verfügbaren Daten ab. Der „Big Data" Trend in der IT und die massenhafte Verfügbarkeit von Daten beschleunigen die Entwicklung von KI-Systemen derzeit maßgeblich.

Transparenz über verwendete Datenquellen und die Rechtmäßigkeit ihrer Verarbeitung in KI-Systemen sind daher zentrale Datenschutzanforderungen.

Die sehr komplexen psychischen und emotionalen Prozesse menschlicher Erkenntnisse und Entscheidungen, dürften den Maschinen noch geraume Zeit verborgen bleiben. Bei der datenschutzrechtlichen Bewertung und Abwägung ist deshalb zu berücksichtigen, dass maschinelle Entscheidungen auf anderen Grundlagen und Mechanismen beruhen, als dies bei Entscheidungen durch Menschen der Fall ist.
Um die erforderliche Handlungssicherheit im Umgang mit KI-Systemen zu erzielen, ist eine umfassende ethische und rechtliche Governance für KI-Entscheidungen wirksam zu implementieren.
Alle im Konzern vereinbarten ethischen Verhaltensregeln und alle Compliancevorgaben die für Organisationseinheiten und jeden Mitarbeiter verbindlich sind, sind auch zur Grundlage für Entscheidungen von KI-Systemen zu machen.

2.2 Welche spezifischen datenschutzrechtlichen Fragen sind bei KI-Projekten zu klären?

Im Konzern gestalten wir täglich datenschutzkonforme Big Data, BI, Data Warehouse und Data Analytics Systeme und verfügen über hinreichende Erfahrung und Vorgaben im Umgang mit den datenschutzrechtlichen Fragen rund um diese IT-Prozesse. Bei KI-Systemen und KI-gestützten Geschäftsmodellen sind natürlich alle diese bestehenden datenschutzrechtlichen Anforderungen anzuwenden und einzuhalten. Das gilt insbesondere für die Frage der Zulässigkeit der Verarbeitung personenbezogener Daten.

Darüber hinaus ergeben sich bei der datenschutzrechtlichen Bewertung von KI-Systemen im Wesentlichen folgende spezifische Fragestellungen:

1. Wie werden Transparenz und Einwirkungsrechte der Nutzer / Betroffenen gewährleistet?

Verträge und Kundenprozesse müssen derart gestaltet sein, dass Art und Umfang des Anteils an KI-gestützten Entscheidungen transparent ist. Es muss also klar sein, ob ein KI-System eingesetzt wird, und welchen Anteil an getroffenen Entscheidungen, die KI tatsächlich hat. Die gesetzlich geforderten Einspruchs- und Beschwerdemöglichkeiten müssen im Geschäftsmodell prozessual hinterlegt sein und auf einfache Weise genutzt werden können.

2. Wie wird die (innere) Transparenz bezüglich der KI-Entscheidungen gewährleistet und wie kontrollieren und überwachen wir KI-Systeme?

Im Rahmen eines Abwägungsprozesses muss für die Entscheidungen eines KI-Systems eine angemessene Kontrollmethode und eine Überwachungsintensität festgelegt werden. Dabei muss geprüft werden, ob durch das KI-System getroffene / empfohlene Entscheidungen im Einklang stehen mit der zuvor festgelegten Zweckbestimmung des KI-Systems, den Bedürfnissen des Betroffenen und den ethischen Grundsätzen unseres Unternehmens. Ethische Grundsätze sind alle Verhaltensregeln, die wir in unserem Unternehmen für den Umgang miteinander und mit unseren Kunden festgelegt haben. Dazu zählt insbesondere ein achtsamer Umgang mit den Persönlichkeitsrechten, Fairness, Nichtdiskriminierung, soziale Teilhabe und Pluralismus.

Datenschutzkonform sind KI-Systeme nach unserer Auffassung dann, wenn

- die Rechtmäßigkeit der Verarbeitung aller Daten(quellen) gewährleistet ist,
- der Einsatz von künstlicher Intelligenz allen Beteiligten hinreichend transparent ist,
- Regelungsmöglichkeiten bei vermeintlich bestehenden Fehlentscheidungen bestehen,
- die Entscheidungsprozesse von KI-Systemen regemäßig überwacht werden und
- sichergestellt werden kann, dass jede von der KI getroffene Entscheidung stets mit den Leitsätzen des Konzerns zur digitalen Ethik im Einklang steht.

Zur Erfüllung der Transparenzanforderungen der DSGVO bei KI-Systemen muss der Nutzer sich darauf verlassen können, dass die ethischen Grundsätze bei KI-Entscheidungen transparent sind, eingehalten und wirksam überwacht werden. Die fachseitige Projektverantwortung umfasst auch die Abbildung und Umsetzung der hierfür erforderlichen Transparenz- und Kontrollprozesse.

3 KONKRETE DATENSCHUTZANFORDERUNGEN DES KONZERNS BEI DER GESTALTUNG VON KI PROJEKTEN

Die Deutsche Telekom hat sich unter dem Aspekt „Digitale Verantwortung“ in neun Leitlinien zu einem transparenten und menschenzentrierten Umgang mit KI-Systemen bekannt.

https://www.telekom.com/de/konzern/digitale-verantwortung

Nachfolgend konkretisiert Group Privacy die datenschutzrechtlichen Anforderungen die jeweils auf die einzelnen Leitlinien einzahlen:

Wir übernehmen Verantwortung.

- Der Zweck des eingesetzten KI-Systems ist abschließend zu bestimmen und zu dokumentieren.
- Die Verantwortlichkeiten für das Geschäftsmodell / Produkt sind klar definiert. Ebenso ist die Verantwortlichkeit für den Einkauf, die Entwicklung sowie für den ordnungsgemäßen Betrieb der KI Elemente eindeutig zugeordnet.
- Die Rechtmäßigkeit der Nutzung aller verwendeten Datenquellen sowie der Daten ist nachgewiesen und dokumentiert.

Wir gehen sorgsam mit Künstlicher Intelligenz um.

- Zur Kontrolle der Entscheidungen des KI-Systems ist durch die verantwortliche Fachseite ein angemessener und wirksamer Überwachungsprozess zu implementieren. Der Überwachungsprozess muss mindestens die nachfolgenden Anforderungen erfüllen:
  - Von der KI-Entscheidung Betroffene, können eine Beschwerde adressieren. Die für die Beschwerde ursächliche Entscheidung der KI muss auf Einhaltung des vereinbarten Geschäftszwecks und auf Einhaltung der Konzern-Governance überprüft werden. Die Entscheidung ist dem Beschwerdeführer nachvollziehbar zu machen und ist im Zweifelsfall zu korrigieren.
  - Alle mit dem Betrieb des KI-Systems betrauten Mitarbeiter sind im Hinblick auf die Bandbreite der zu erwartenden Entscheidungen des KI-Systems im Rahmen der Zweckbestimmung und den relevanten Governancevorgaben in besonderer Weise sensibilisiert. Falls die Mitarbeiter Anhaltspunkte für eine Abweichung der KI-Entscheidungen von der vorgegebenen Entscheidungsbandbreite haben, muss ein sofortiges Eingreifen möglich sein („Not-Aus Taste“). Die Ursachen für die festgestellten Abweichungen sind zu identifizieren und zu dokumentieren. Ggf. erforderliche Korrekturmaßnahmen sind vor Wiederaufnahme des KI-Systems umzusetzen.

- Je nach Kritikalität der verarbeiteten Daten, bzw. der Tragweite der durch das KI-System getroffenen Entscheidungen, wird durch die verantwortliche Fachseite in regelmäßigen zeitlichen Abständen eine Überprüfung des KI-Systems durchgeführt. Hierbei werden die Entscheidungen des KI-Systems auf Einhaltung der Governancevorgaben überprüft. Das Ergebnis ist zu dokumentieren. Art und Umfang der durchzuführenden Überprüfungen werden im Rahmen des PSA-Prozesses zwischen der Fachseite und GPR vereinbart und im Regelbetrieb prozessual abgebildet.
- Für jedes KI-Projekt ist im Rahmen des PSA Verfahrens eine Datenschutz-Folgenabschätzung durchzuführen. Risiken sind zu analysieren und Maßnahmen zur Risikominderung sind zu definieren und im Projekt umzusetzen.

Wir stellen unsere Kunden in den Mittelpunkt.

- Oberster Maßstab für die Gestaltung KI-basierter Geschäftsmodelle ist die Integrität der Persönlichkeitsrechte der betroffenen Kunden bzw. Mitarbeiter. Werden Persönlichkeitsrechte beeinträchtigt, geht Vertrauen verloren. Ohne Vertrauen, gibt es keinen Geschäftserfolg und die Reputation des Konzerns wird beschädigt. KI-Lösungen werden daher vom Kunden/Mitarbeiter her gedacht und entwickelt.

Wir stehen für Transparenz.

- Kunden und Mitarbeitern muss zu jedem Zeitpunkt transparent sein, ob sie mit einem KI-System kommunizieren und welchen Anteil das KI-System bei getroffenen Entscheidungen hat.
- Kunden und Mitarbeitern muss transparent sein, welche ihrer Daten in einem KI-System verarbeitet werden und zu welchem Zweck.
- KI-Entscheidungen müssen vom Betroffenen hinterfragt, und die Entscheidung muss nachvollziehbar erläutert werden können.

Wir bieten Sicherheit.

- Über die hier im Speziellen genannten Anforderungen hinaus, gelten bei der Gestaltung KI-gestützter Geschäftsmodelle und Produkte natürlich sämtliche im Konzern etablierten Datenschutz- und Datensicherheitsvorgaben.
- Für alle KI-Basierten Geschäftsmodelle und Produkte ist das Privacy & Scurity Assessment Verfahren (PSA) zwingend durchzuführen.

Wir legen das Fundament.

- Die Entwicklung eigener KI-Systeme muss die ethischen und rechtlichen Vorgaben für unseren Konzern bereits bei der Entwicklung berücksichtigen (Privacy by Design, Ethic by Design, Transparency by Design).
- Eingekaufte KI-Systeme müssen im praktischen Betrieb die Einhaltung unserer ethischen und rechtlichen Anforderungen einhalten können. Ist dies nicht garantiert, kann das Produkt nicht eingesetzt werden. Vor Nutzung externer KI-Systeme muss dies evaluiert und dokumentiert werden.

Wir behalten den Überblick.

- Unabhängig von den oben genannten Überwachungsprozessen, müssen KI-Systeme und deren Betriebsprozesse derart gestaltet sein, dass ein sofortiger Eingriff zur Vermeidung bzw. Reduzierung von Schäden gewährleistet ist

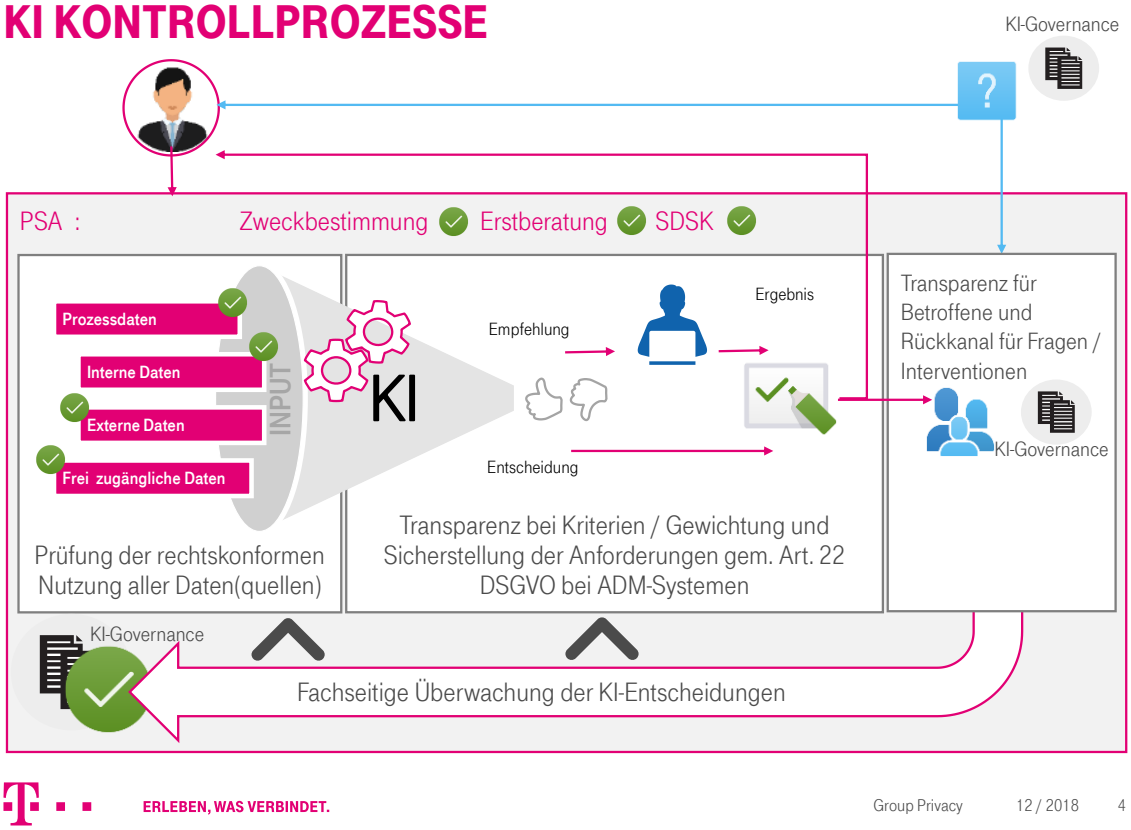
Wir leben das Kooperationsmodell.

- Den Menschen und seine Persönlichkeitsrechte als Maßstab für die Gestaltung von KI-Systemen zu betrachten, schließt eine weitreichende Kooperation zwischen Menschen und Maschinen nicht aus. Durch innovative Ideen und der Berücksichtigung der menschlichen Interessen bereits bei der Planung und Entwicklung von KI-Geschäftsmodellen und Produkten, können wir Standards etablieren, die das Vertrauen in die Produkte der Deutschen Telekom nachhaltig sichert und eine fruchtbare Kooperation von Mensch und Maschine ermöglicht.

Wir teilen und erklären.

- Unsere Ideen für eine datenschutzkonforme Gestaltung von KI-Geschäftsmodellen und Produkten teilen wir mit Anderen und werben so für unsere hohen Standards.

4 DIE KONTROLLPROZESSE



Durch die operativ verantwortlichen Stellen sind prozessual nachfolgende Anforderungen abzubilden:

- Transparenz über den KI-Anteil im Geschäftsmodell und die etablierten Kontrollprozesse gegenüber dem Betroffenen sicherstellen und überwachen.
- Einwirkungs- und Beschwerdeprozesse für alle an der Datenverarbeitung beteiligten sicherstellen und überwachen.
- Überwachung der KI-Entscheidungen auf Einhaltung der definierten Zweckbestimmung des Systems und der KI-Governance.

5 DATENSCHUTZRECHTLICHE BEWERTUNG KI

Der datenschutzrechtliche Rahmen ist – aufgrund des eingeschränkten Geltungsbereichs datenschutzrechtlicher Normen - immer nur ein Teilbereich der im Rahmen einer KI und der zu Grunde liegenden Prozesse betrachtet werden muss und der diesbezügliche Anforderungen normiert. Verfahren, die von vornherein oder aufgrund von entsprechenden Maßnahmen (Anonymisierung) auf Informationen aufbauen, die keinen Personenbezug haben, fallen aus dem Anwendungsbereich datenschutzrechtlicher Vorschriften (z.B. DSGVO) heraus. Datenschutzrechtliche Normen zielen zudem primär auf den Schutz von individuellen Rechten des Einzelnen ab – gruppen- oder gesellschaftsbezogene Ziele, wie z.B. Nichtdiskriminierung und Teilhabe, werden regelmäßig nicht abgesichert.

In dem Bereich jedoch, auf den die Vorschriften der DSGVO anwendbar sind, bestehen bereits ausreichende Regelungen und Anforderungen, die KI bzw. die zu Grunde liegenden Verfahren algorithmischer

Entscheidungsfindung betreffen. Dabei handelt es sich sowohl um spezifische Normen, die sich mit diesen Verfahren beschäftigen, als auch um allgemeine Grundsätze und Anforderungen des Datenschutzes, die aufgrund der Verarbeitung personenbezogener Daten im Rahmen von KI zu beachten sind.
Es lassen sich grob zwei Typen von algorithmischen Systemen unterscheiden. Die datenschutzrechtlichen Vorschriften sehen in Art. 22 DSGVO spezifische Regelungen zu Systemen vor, die Menschen bewerten und algorithmenbasiert Entscheidungen treffen (Algorithmic Decision Making Systems, kurz: ADM-Systeme).

Davon zu unterscheiden sind Decision-Support-Systeme, die den Entscheider bei der menschlichen Entscheidung „lediglich" unterstützen und nur dazu dienen, menschliche Entscheidungen vorzubereiten (DS-Systeme). Letztere können beliebig weitreichend im Rahmen der allgemeinen Anforderungen der DSGVO eingesetzt werden.

Aus datenschutzrechtlicher Sicht ist daher zunächst entscheidend, ob der Geltungsbereich datenschutzrechtlicher Normen eröffnet ist.

Definition: Personenbezug bzw. Personenbeziehbarkeit
Dann sind – wie bei jeder Datenverarbeitung – die allgemeinen Anforderungen der DSGVO zu beachten. Hier kann auf bereits bestehende Leitlinien, z.B. zu Big Data verwiesen werden.

Nur für den Fall, dass im Rahmen der KI auch ein ADM-System eingesetzt wird, d.h. algorithmenbasiert Entscheidungen automatisiert getroffen und nicht lediglich vorbereitet werden, finden darüber hinaus die spezifischen Anforderungen des Art. 22 DSGVO zu automatisierten Entscheidungen (einschließlich Profiling) Anwendung.

5.1 Verbot einer automatisierten Einzelfallentscheidung

Gemäß Art. 22 DSGVO hat der Einzelne das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihm gegenüber rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt.
Profiling wird in Art. 4 Nr. 4 DSGVO definiert und bildet einen Unterfall der automatisierten Einzelfallentscheidung.

5.1.1 Ausschließliche automatisierte Verarbeitung

Art. 22 DSGVO umfasst daher nur Systeme, bei denen die Entscheidung „ausschließlich auf einer automatisierten Verarbeitung" ohne jegliche menschliche Einflussnahme beruht. Die Möglichkeit zur Einflussnahme bzw. die Beteiligung des Menschen darf dabei jedoch nicht lediglich ein formaler Akt sein, sondern muss den Raum für eine inhaltliche Mitverantwortung bieten, d.h. der Mensch muss sich ohne Nachteile befürchten zu müssen auch gegen die Empfehlung entscheiden können.

5.1.2 Rechtliche Wirkung oder erhebliche Beeinträchtigung

Weiterhin muss die Entscheidung gegenüber der betroffenen Person eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. Von einer „rechtlichen Wirkung" kann immer dann die Rede sein, wenn sich durch die Entscheidung die Rechtsposition des Betroffenen ändert. Eine „erhebliche Beeinträchtigung" ist immer dann anzunehmen, wenn der Betroffene in seiner wirtschaftlichen oder persönlichen Entfaltung erheblich gestört wird.

5.1.3 Ausnahmen

Nach Art 22. Abs. 2 DSGVO sind Systeme automatisierter Entscheidungen „ausnahmsweise" dann zulässig, wenn (a) die Entscheidung für den Vertragsschluss oder die Vertragserfüllung zwischen Betroffenem und Verantwortlichem erforderlich ist, (b) die ADM-Entscheidung durch eine gesetzliche Vorschrift im Land des Betroffenen für zulässig erklärt wurde oder wenn (c) die Entscheidung mit ausdrücklicher Einwilligung des Betroffenen erfolgt.

5.1.4 Besondere Kategorien personenbezogener Daten

Eine Grenze besonderer Art für die Zulässigkeit von ADM-Systemen sieht Art. 22 Abs. 4 DSGVO vor: Die Verwendung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO dürfen nicht zur automatisierten Entscheidungsfindung genutzt werden – außer wenn die betroffene Person eingewilligt hat oder eine EU- oder mitgliedstaatliche Rechtsvorschrift aus Gründen eines erheblichen öffentlichen Interesses dies erlaubt.

5.1.5 Angemessene Schutzmaßnahmen

Ist eine automatisierte Einzelentscheidung schließlich nach Art. 22 Abs. 2 oder Abs. 4 DSGVO ausnahmsweise zulässig, stellt Art. 22 Abs. 3 DSGVO spezifische Anforderungen hinsichtlich flankierender angemessener Maßnahmen auf, „um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren“ (Art.22 Abs. 2 b), Abs. 3 und Abs. 4 DSGVO).

Anhaltspunkte zu diesen Maßnahmen gibt Art. 22 Abs.3 und Erwägungsgrund 71 DSGVO. Dabei handelt es sich um Verfahrensmaßnahmen und technische Maßnahmen.

Prozessuale Maßnahmen:

- Recht, das Eingreifen einer Person zu verlangen
- Recht, den eigenen Standpunkt darzulegen
- Recht auf Anfechtung einer Entscheidung

Entgegen dem Wortlaut wird wohl davon auszugehen sein, dass diese Rechte nicht vorbehaltlos, sondern aus berechtigten Gründen im Einzelfall eingeräumt werden müssen.

Beispiele für technische Maßnahmen:

- Geeignete mathematische oder statistische Verfahren
- Technische und organisatorische Maßnahmen zur Vermeidung unrichtiger personenbezogener Daten
- Regelmäßige Überprüfung der Datensätze und des Verfahrens (ggf. Audit-Algorithmen)
- Prüfroutinen bei Entwicklung und Betrieb

Konkretisierungen lassen sich auch aus der Stellungnahme der Artikel-29-Datenschutzgruppe (Oktober 2017) ableiten[2].

5.2 Grundsätze der Verarbeitung

Sowohl in Bezug auf die Verarbeitung von personenbezogenen Daten im Rahmen von ADM-Systemen, als auch bei Systemen, wie z.B. DS-Systemen, die nicht unter die speziellen Anforderungen des Art. 22 DSGVO fallen, müssen die Grundsätze der Verarbeitung personenbezogener Daten im Sinne von Art. 5 DSGVO beachtet werden. Diese Grundsätze werden wiederum durch eine Reihe von Einzelregelungen in der DSGVO konkretisiert.

Dazu zählen Rechtmäßigkeit, Transparenz, Zweckbindung, Richtigkeit, Integrität und Vertraulichkeit der Verarbeitung sowie die Rechenschaftspflicht.

[2] „Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679“, WP251 rev01 - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

5.3 Transparenz

Zu den Transparenzpflichten zählt die Verpflichtung, den Betroffenen über die Datenverarbeitung zu informieren (Art. 13 und 14 DSGVO). Die Informationspflichten sollen sicherstellen, dass der Betroffene von der Datenverarbeitung und deren Reichweite erfährt, damit er seine Rechte effektiv wahrnehmen kann.

Im Falle einer automatisierten Entscheidungsfindung gem. Art. 22 Abs.1 und 4 DSGVO muss der Betroffene darüber informiert werden, dass ein ADM-Systems zum Einsatz kommt. Zudem sind „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" gefordert (Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2 lit. g DSGVO).

Da hierbei regelmäßig das Recht des Betroffenen auf aussagekräftige Informationen dem berechtigten Interesse des Verantwortlichen auf den Schutz seiner Geschäftsgeheimnisse (auch Erwägungsgrund 63 DSGVO) gegenübersteht, bedeutet dies nicht automatisch, dass der Algorithmus des Verfahrens mitgeteilt werden muss. Es sollte aber der Zweck und die Kriterien offengelegt werden, die bei der Entscheidungsfindung berücksichtigt werden (so auch Artikel-29-Datenschutzgruppe). Auch wird hier der Verhältnismäßigkeitsgrundsatz anzuwenden sein.

Zu den Transparenzpflichten zählt auch der Auskunftsanspruch gem. Art 15 DSGVO, wonach der Betroffene das Recht hat, von dem Verantwortlichen Auskunft über den Zweck und die Reichweite der Datenverarbeitung zu verlangen. Der Auskunftsanspruch soll es dem Betroffenen insbesondere ermöglichen zu überprüfen, ob die Daten rechtmäßig verarbeitet werden. Im Falle einer automatisierten Entscheidungsfindung gem. Art. 22 Abs. 1 und 4 DSGVO muss die Auskunft auch „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" enthalten (Art. 15 Abs. 1 lit. h DSGVO).

Festzuhalten ist, dass der gesetzliche Wortlaut erheblichen Auslegungsspielraum zulässt, sodass auch hier eine lediglich abstrakte Information über die Systemfunktionalität und nicht die Offenlegung des Algorithmus angenommen werden kann.

Wird ein lediglich entscheidungsunterstützendes oder empfehlendes Decision Support System (DS-System) genutzt, sind die speziellen Transparenzpflichten des Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2 lit. g DSGVO hingegen nicht anwendbar.
Ein spezieller Rechtsrahmen gilt für automatisierte Entscheidungen im Bereich der öffentlichen Verwaltung, wo bereits gesetzliche Vorgaben hinsichtlich der Nachvollziehbarkeit einer Entscheidung aus rechtsstaatlichen Gründen eine Begründungspflicht vorsehen.

5.4 Datenschutz-Folgenabschätzung

Begründet die Datenverarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten der Betroffenen, so hat der Verantwortliche vorab eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 Abs. 1 DSGVO). Die Datenschutz-Folgenabschätzung ist damit ein wichtiges Instrument, um der Verpflichtung aus Art. 5 Abs. 2 DSGVO nachzukommen, die Einhaltung der DSGVO nachzuweisen („Rechenschaftspflicht"). Zusätzlich hat die Datenschutz-Folgenabschätzung die Funktion eines Frühwarnsystems und der Risikoanalyse, durch die eine potentielle Verletzung von Persönlichkeitsrechten verhindert werden kann. In diesem Rahmen wird – schon um eine hinreichende Risikobewertung vornehmen zu können – ein gewisses Maß an Dokumentation der zu Grunde liegenden Algorithmen zu fordern sein.

Bei einer automatisierten Entscheidungsfindung (ADM-System) ist aufgrund von Art. 35 Abs. 3 lit. a DSGVO die Datenschutz-Folgenabschätzung in der Regel verpflichtend - doch werden nach Auffassung der Artikel-29-Datenschutzgruppe auch solche Konstellationen erfasst, in denen der Algorithmus nur vorbereitend zur Entscheidungsunterstützung eingesetzt wird (DS-Systeme). Die Datenschutzkonferenz (Gremium der deutschen Datenschutzaufsichtsbehörden) hat in Konkretisierung der Vorgaben der Artikel 29-Datenschutzgruppe eine Liste von Verarbeitungsvorgängen veröffentlicht, bei denen immer einer Datenschutzfolgenabschätzung durchzuführen ist.

Geht aus der Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, besteht gem. Art. 36 Abs. 1 DSGVO schließlich eine Pflicht zur Konsultation der Aufsichtsbehörde.

Die erforderliche Datenschutz-Folgenabschätzung ist Bestandteil des PSA Verfahrens.

6 BEREITS BESTEHENDE VORGABEN DIE BEI DER BEWERTUNG VON KI PROJEKTEN ZU BEACHTEN SIND

6.1 Allgemeine Vorgaben

Für alle IT/NT Systeme des Konzerns, sowie für alle Produkte der Telekom ist das Privacy and Security Assessment (PSA) zu durchlaufen.

6.2 BigData

Whitepaper Group Privacy zur datenschutzkonformen Gestaltung datengetriebener Geschäftsmodelle.

OnePager zur datenschutzkonformen Gestaltung datengetriebener Geschäftsmodelle.

Leitsätze der Deutschen Telekom zu BigData

7 ÜBERSICHT ALLER DATENSCHUTZRECHTLICHEN ANFORDERUNGEN

Alle spezifischen Anforderungen aus diesem Leitfaden in der Übersicht:

7.1 Vor Durchführung des PSA Verfahrens

- Der Zweck des KI-Systems ist abschließend bestimmt.
- Die Verantwortlichkeiten für das Geschäftsmodell / Produkt / IV-Prozesse sind klar definiert.
- Der geplante Einsatz der KI-Lösung wird vom Kunden/Mitarbeiter hergedacht und entwickelt.
- Eingekaufte KI-Systeme müssen im praktischen Betrieb die Einhaltung unserer ethischen und rechtlichen Anforderungen einhalten können. Ist dies nicht garantiert, kann das Produkt nicht eingesetzt werden. Vor Nutzung externer KI-Systeme muss dies evaluiert und dokumentiert werden.

7.2 Während des PSA Verfahrens

- Die Rechtmäßigkeit der Nutzung aller verwendeten Daten(quellen) ist sichergestellt.
- Zur Kontrolle der Entscheidungen des KI-Systems ist ein angemessener und wirksamer Überwachungsprozess implementiert.
- Für das Projekt wurde eine Datenschutz-Folgenabschätzung durchgeführt.
- Die Entwicklung eigener KI-Systeme muss die ethischen und rechtlichen Vorgaben unseres Konzerns bereits bei der Entwicklung berücksichtigen (Privacy by Design, Ethic by Design, Transparency by Design).
- KI-Systeme und deren Betriebsprozesse müssen derart gestaltet sein, dass ein sofortiger Eingriff zur Vermeidung bzw. Reduzierung von Schäden gewährleistet ist.

7.3 Nach Abschluss des PSA Verfahrens

- Kunden und Mitarbeitern muss zu jedem Zeitpunkt transparent sein, ob sie mit einem KI-System kommunizieren und welchen Anteil das KI-System bei getroffenen Entscheidungen hat.
- Kunden und Mitarbeitern muss transparent sein, welche ihrer Daten in einem KI-System verarbeitet werden und zu welchem Zweck.
- KI-Entscheidungen müssen vom Betroffenen hinterfragt, und die Entscheidung muss nachvollziehbar erläutert werden können.
- Kontinuierliche Überwachung der KI-Entscheidungen auf Einhaltung der definierten Zweckbestimmung des Systems und der KI-Governance.