Automatisierte Entscheidungsfindung - altes Thema brandaktuell

Zur Erinnerung

Prinzipiell soll eine betroffene Person (also die Person, deren Daten verarbeitet werden) keiner aus einer automatisierten Datenverarbeitung resultieren Entscheidungsfindung unterworfen werden. Erwägungsgrund 71 der EU-DSGVO stellt hinsichtlich des Begriffs "Entscheidungsfindung" klar, dass dies alle Maßnahmen mit Wirkung auf die betroffene Person einschließen kann, auch das sogenannte Profiling. Ausnahmen sollten gesetzlich (also z. B. in der EU-DSGVO selbst oder im BDSG) geregelt werden. Kinder sollten von jeglicher automatisierten Entscheidungsfindung ausgenommen sein.

Umgesetzt wurde dieser Gedanke im Artikel 22 "Automatisierte Entscheidungen im Einzelfall einschließlich Profiling". Leider offenbart sich in diesem Artikel wieder einmal eine - ich nenne es - "handwerkliche Schwäche" im Verordnungstext, die eine Interpretation erschwert. Es heißt hierzu nämlich: "...die ihr [der betroffenen Person] gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt." Dass die Beeinträchtigung "erheblich" sein muss, um mit einem Verarbeitungsverbot belegt zu sein, erscheint noch relativ eindeutig, es ist also nicht jede automatisierte Entscheidungsfindung per se verboten. Schwieriger wird es mit dem Begriff der "rechtlichen Wirkung". Ist hiermit das Eingehen oder Ablehnen eines Vertragsverhältnisses gemeint, die Bewertung eines arbeitsrechtlichen Sachverhalts (z. B. Höhergruppierungen, Erlaubnis für mobiles Arbeiten, Gewährung der privaten Nutzung von Dienstfahrzeugen, Leistungsboni) oder fällt auch bereits die Gewährung von Rabatten an Kunden unter diese Kategorie, wenn diese auf eine automatisierte Auswertung des Kaufverhaltens beruht? Wir werden später auf diesen Punkt zurückkommen.

Aktualität des Themas

In der Vergangenheit war es meistens so, dass eine automatisierte Entscheidungsfindung auf Algorithmen beruhte, die vom Verantwortlichen selbst definiert und in der eigenen oder eigens für das Unternehmen programmierten Software festgeschrieben wurden. Sie waren nach außen nicht immer publiziert bzw. transparent, technisch aber zumindest durch den angewandten Programmcode festgeschrieben. So konnten wir bei der Ablehnung eines Smartphone-Vertrags oder eines Versicherungsverhältnisses vielleicht nur erahnen, warum eine Entscheidung für oder gegen uns getroffen wurde, an einer bestimmten Stelle war dies jedoch definiert und nachvollziehbar.

Mittlerweile aber wird zunehmend die sogenannte "künstliche Intelligenz" (KI) in Entscheidungsfindungen einbezogen. Hierbei handelt es sich nicht mehr um Algorithmen, welche durch den Verantwortlichen selbst festgelegt wurden, sondern um - ich nenne es vorsichtig - "Vorschläge" oder

Volker Baron (Dipl.-Geograph / IT-Systemelektroniker) – **Tel.:** +49 89 18923500 – **Fax:** +49 89 18923501
Büro: Haydnstraße 2, 80336 München – **E-Mail:** volker.baron@baron-consult.de – **Internet:** www.baron-consult.de
Finanzamt München I, USt-ID: DE 216791626
Bankverbindung: Münchner Bank eG, IBAN: DE84 7019 0000 0000 3389 15, BIC: GENODEF1M01

"Empfehlungen", die unter Einbeziehung externer Anbieter (ChatGPT der Firma OpenAI, Copilot von Microsoft etc.) und wechselnder, da sich eigenständig weiterentwickelnden Algorithmen beruhen. Eine nach Art. 22 Abs. 3 EU-DSGVO geforderte Möglichkeit, dass der Betroffene den eigenen Standpunkt gegen die automatisiert getroffene Entscheidung vorbringen kann, ist damit so gut wie ausgeschlossen.

Eindeutiges No-Go: Einbeziehung von besonderen Kategorien personenbezogener Daten

Zumindest in diesem Punkt besteht Klarheit: Besondere Kategorien personenbezogener Daten nach Art. 9 EU-DSGVO dürfen nicht in eine automatisierte Entscheidungsfindung einbezogen werden. Auch hier gibt es Ausnahmen, die sich jedoch in sehr engen Grenzen halten (erhebliches öffentliches Interesse) und damit in der Praxis keine Relevanz besitzen bzw. auf einer Einwilligung des Betroffenen beruhen, deren vollständige Freiwilligkeit nach umfassender Betroffeneninformation vom Verantwortlichen schwer nachweisbar sein dürfte. Die Freiwilligkeit der im Beschäftigungskontext erteilten Einwilligungen wird ohnehin regelmäßig angezweifelt.

Rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrischen Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person entfallen damit vollständig als Grundlage für derartige Verarbeitungsvorgänge.

Wann ist eine Datenschutz-Folgenabschätzung erforderlich?

Die Ausführungen zur Datenschutz-Folgenabschätzung (DSFA) in Art. 35 EU-DSGVO beziehen sich nicht ausschließlich auf die Fälle von automatisierten Entscheidungsfindungen, sollten aber auch hier gewissenhaft in die entsprechenden Prozesse einbezogen werden. Hier eine kleine Checkliste, wann eine DSFA gefordert sein kann:

1. "Verwendung neuer Technologien": Dieser Punkt ist beim Einsatz von Software mit KI eindeutig gegeben.
2. "Hohes Risiko für die Rechte und Freiheiten natürlicher Personen": Nicht jede Entscheidungsfindung stellt ein "hohes Risiko" dar, im Zweifelsfall empfehle ich aber, eine DSFA durchzuführen bzw. die Interessenabwägung zwischen Verantwortlichem und Betroffenen zu dokumentieren.
3. "Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen": Hier ist es nun eindeutig, das Wort "Rechtswirkung" steht ohne jegliches Adjektiv im Gesetzestext.

Das Bayerische Landesamt für Datenschutzaufsicht hat eine Positiv-Liste mit typischen Verarbeitungsvorgängen veröffentlicht, bei denen eine DSFA erforderlich ist:
https://www.lda.bayern.de/media/themen/dsfa_muss_liste_dsk_de.pdf

Die genannte Positiv-Liste kann auch zur Einschätzung herangezogen werden, welche automatisierten Verarbeitungsvorgänge mehr oder weniger kritisch betrachtet werden müssen. So sind beispielsweise Vorgänge der allgemeinen Betriebsorganisation (Urlaubsplanung, Diensteinsatzplanung, Tourenplanung etc.) hierin nicht zu finden, obwohl sie regelmäßig natürliche Personen betref-

fen. Gelistet sind jedoch Verarbeitungsvorgänge, die zu einer Leistungs- und Verhaltenskontrolle oder einer anderweitigen Überwachung natürlicher Personen verwendet werden können.

Grundsatz der Datensparsamkeit

Wie bei allen Verarbeitungsvorgängen personenbezogener Daten gilt auch beim Einsatz von Software der sogenannten KI der Grundsatz der Datensparsamkeit. Bitte bedenken Sie daher vor der Einführung eines solchen Verfahrens, welche Kategorien von personenbezogenen Daten für den gewünschten Verarbeitungszweck zwingend erforderlich sind. Bei meinen Bewertungen zur Rechtmäßigkeit der Verarbeitung unterscheide ich drei Möglichkeiten hinsichtlich des geplanten oder voraussichtlichen Nutzungsverhaltens:

1. Die Fragestellungen an die KI werden ohne die Übermittlung von personenbezogenen Daten durchgeführt, der Schutz personenbezogener Daten ist damit nicht relevant. Dies wäre z. B. der Fall, wenn über rechtliche oder technische Fragenstellungen recherchiert wird, ohne den Bezug zu einer natürlichen Person herzustellen. Eine automatisierte Entscheidungsfindung ist hieraus nicht ableitbar. Eine anderweitige Nutzung wird mittels organisatorischer Verfahren (z. B. Handlungsanweisungen) untersagt.
2. Die Abfragen an die Software zur KI werden über eine definierte Schnittstelle (API) geführt, z. B. aus einem System zur Auftrags- und Kundenverwaltung heraus. Die gewonnenen Erkenntnisse fließen in das Ursprungssystem oder eine andere Software zurück und werden dort zu einer automatisierten Entscheidungsfindung genutzt. Durch die technische Definition der Schnittstelle sind die übermittelten Daten festgeschrieben, die Bewertung, ob die Verarbeitung zulässig ist und ob eine DSFA durchgeführt werden muss kann zum Zeitpunkt der Definition der Schnittstelle getroffen werden. Änderungen an der Schnittstelle müssen allerdings zu einer erneuten Interessenabwägung oder DSFA führen.
3. Die Nutzung der Software zur KI obliegt dem jeweiligen Anwender. Es besteht die Möglichkeit, dass hierbei auch personenbezogene Daten übermittelt werden. Art und Umfang der Datenübermittlung ist jedoch situativ, so dass eine einzelfallbezogene Interessenabwägung nicht vorgenommen werden kann. Der Einsatz der Software ist damit nur im Umfeld von umfangreichen technisch-organisatorischen Maßnahmen möglich (siehe untenstehende Handlungsempfehlungen).

Handlungsempfehlungen

Die nachfolgenden Empfehlungen beziehen sich zum einen auf die Nutzung von Software zur KI allgemein, insbesondere aber auch zum Einsatz in Verbindung mit automatisierten Entscheidungsfindungen.

- Wählen Sie den Anbieter der Software für KI sorgfältig aus. In der Regel kommt man hierbei an US-amerikanischen Firmen nicht vorbei. Ist das Unternehmen nicht in der EU oder dem EWR ansässig und auch nicht in einem Land auf der Liste des Angemessenheitsbeschlusses der EU-Kommission für Länder mit gleichwertigem Datenschutzniveau prüfen Sie, ob anderweitige Garantien vorhanden sind. Dies können verbindliche interne Datenschutzvorschriften sein (Binding Corporate Rules BCR), wenn sie z. B. vollumfänglich den Mustervorgaben der Artikel-29-Datenschutzgruppe (Article 29 Data Protection Working Party) entsprechen. Bei US-amerikanischen Firmen sehen Sie nach, ob es sich auf der Liste

der zertifizierten Anbieter im Rahmen des EU-U.S.-Data Privacy Frameworks befindet: https://www.dataprivacyframework.gov/list. Große Unternehmen stehen mit ihren einzelnen Betriebsteilen und Untergliederungen ggf. mehrfach auf dieser Liste (Microsoft z. B. mit 14 weiteren „Entities“). Hier müssen Sie prüfen, ob der genaue Anbieter wirklich zu den zertifizierten Unternehmen gehört. Erstellen Sie sich auch eine Wiedervorlage, die Sie daran erinnert, dass die Überprüfung periodisch wiederholt werden sollte.

- Schließen Sie einen Vertrag zur Auftragsverarbeitung nach Art. 28 EU-DSGVO. Achten Sie darauf, dass der Anbieter eine Datenverarbeitung im Geltungsbereich der EU-DSGVO zusichert.
- Treffen Sie technische Maßnahmen, die eine unbefugte Nutzung verhindern. Welche dies sind lässt sich pauschal nicht festlegen. So gehört aber in jedem Fall dazu, dass nur befugte Anwender personenbezogene Daten aus bestehenden Systemen extrahieren bzw. einen Übermittlungsvorgang auslösen können. Stellen Sie andererseits sicher, dass Verarbeitungsergebnisse ebenfalls nur mit entsprechender Befugnis abgeholt bzw. in die vorhandenen IT-Systeme zurückgeführt werden können.
- Pflegen Sie das Verfahren möglichst genau in das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO und in das Löschkonzept ein.
- Sofern das gewählte System den Verarbeitungsverlauf einschließlich personenbezogener Daten speichert achten Sie darauf, dass die vorgesehenen Löschfristen eigehalten werden können.
- Schulen Sie die Anwender, die mit der entsprechenden Software arbeiten sollen. Betriebliche Anweisungen mit eindeutig definierten Rahmenbedingungen für die Nutzung sind unabdingbar, ersetzen wegen der Komplexität der Problematik eine Schulung in den meisten Fällen jedoch nicht. Nach Art. 4 EU-KI-Verordnung (AI Act) müssen Anbieter und Betreiber von KI-Systemen sicherstellen, dass Ihr Personal über ausreichende KI-Kompetenz verfügt.
- Letzter und nach meiner Bewertung mit der wichtigste Hinweis: Überprüfen Sie Erkenntnisse der sogenannten künstlichen Intelligenz mittels menschlicher Kompetenz, ehe die gewonnenen Verarbeitungsvorgänge rechtliche Wirkung auf eine natürliche Person entfalten oder Maßnahmen in Bezug zu dieser Person getroffen werden.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

München, 2025-12-01

Volker Baron