Solving GDPR – Lösungsansätze für KI – Compliance

Künstliche Intelligenz und Compliance

Philipp Kaufold, Jurist; Consultant, ISiCO Datenschutz GmbH
Simone Rosenthal, Rechtsanwältin; Partnerin, Schürmann Rosenthal Dreyer

31. Oktober 2018

LR 2018, Seiten 189 bis 193 (insgesamt 5 Seiten)

Neben großen Konzernen hat auch der deutsche Mittelstand das Potenzial automatischer Entscheidungsfindung unter Verwendung von Machine-Learning Algorithmen erkannt und Projekte im Bereich Data Science und Künstliche Intelligenz angestoßen, um technisch nicht ins Hintertreffen zu geraten.[1] Angesichts der dazu erforderlichen umfangreichen Nutzung von größtenteils personenbezogenen Daten und erheblichen Regulierungsanstrengungen des europäischen Gesetzgebers, wird die effektive Umsetzung von Compliance-Anforderungen und Data Governance zum Wettbewerbsvorteil, indem Entwicklern die rechtlich zulässige Nutzung qualitativ hochwertiger Daten ermöglicht wird, ohne den Entwicklungsprozess durch Compliance-Anforderungen auszubremsen. 1

Gerade bei neuen KI-Projekten kann durch die Berücksichtigung rechtlicher und struktureller Anforderungen in der Planungsphase die Arbeit der Entwickler nachhaltig unterstützt werden – der Beitrag zeigt dazu anhand eines Machine-Learning-Modells Best-Practices und Privacy-by-Design Grundsätze auf.

I. Effektives Verarbeitungsmodell für Machine-Learning

Ein herkömmlicher Machine-Learning Algorithmus kann im einfachsten Sinne als Funktion verstanden werden, die einer bestimmten Eingabe auf Grundlage eines Regelwerks ein deterministisches Ergebnis zuordnet. Davon unterscheidet sich ein Machine-Learning-Algorithmus dahingehend, dass dieser das Regelwerk als Ergebnis eines Lernprozesses selbst bestimmt.[2] Dies stellt Unternehmen vor Herausforderungen bei der Erfüllung regulatorischer Transparenz- und Accountability-Pflichten, da in beiden Fällen ein detailliertes Verständnis des dynamischen Regelwerks erforderlich ist. 2

[1] Unterwegs zu digitalen Welten – Trendstudie von TCS und Bitkom Research (https://downloads.studie-digitalisierung.de/2018/de/Trendstudie_TCS_2018_Bericht_DE.pdf)
[2] Venkat, Suresh, 01.10.2015, When an algorithm isn't… (https://medium.com/@geomblog/when-an-algorithm-isn-t-2b9fe01b9bb5)

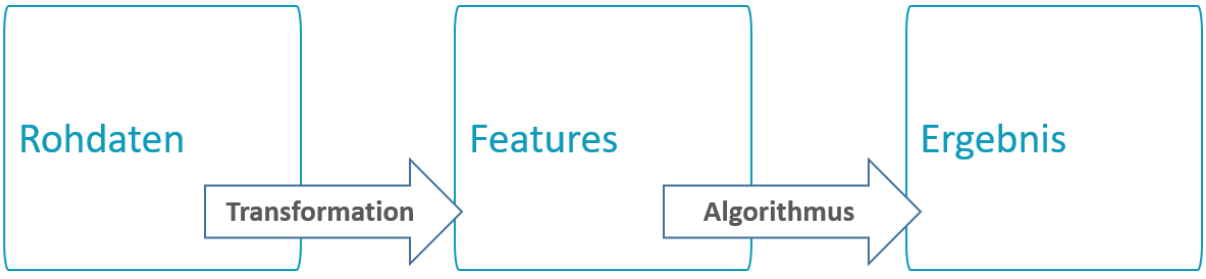
Unabhängig vom konkreten Umfang dieser Pflichten müssen Unternehmen daher grundsätzlich in der Lage sein, Algorithmus-basierte Entscheidungsprozesse sowie die zugrundeliegenden Datenverarbeitungen nachzuvollziehen und zu überwachen.[3] Eingriffsbefugnisse der Behörden, Dokumentationspflichten und Rechte betroffener Personen sorgen zusätzlich für Aufwand bei der Handhabung personenbezogener Daten.

Ein **effektives Verarbeitungsmodell schafft Lösungen für Transparenz & Accountability, und minimiert den Compliance-Aufwand** bei der erforderlichen Datenverarbeitung. Darüber hinaus muss das Modell als Grundlage für zukünftige Machine-Learning-Projekte dienen, deren Zwecke und Voraussetzungen – insbesondere hinsichtlich der erforderlichen Rohdaten – aufgrund der technischen Entwicklung noch nicht absehbar sind. 3

II. Betroffenenrechte der DSGVO – Compliance-Aufwand vermeiden

Der Compliance-Aufwand unter der DSGVO wächst grundsätzlich mit dem Risiko, das für betroffene Personen von einer Datenverarbeitung ausgeht. Umgekehrt belohnt die DSGVO risikominimierende Maßnahmen mit Ausnahmetatbeständen. 4

Insbesondere individuelle Betroffenenanfragen zu personenbezogenen Daten bremsen Entwicklungsprozesse, etwa, wenn Trainingsdaten hinsichtlich einzelner Personen durchsucht, kopiert oder gelöscht werden müssen. Eine erhebliche Erleichterung ermöglichen hier die rechtzeitige Pseudonymisierung oder Anonymisierung der Daten, die dem Machine-Learning-Modell zugrunde liegen. Je nach konkreter Gestaltung des Datensatzes können dadurch der Befreiungstatbestand des Art. 11 Abs. 2 DSGVO genutzt oder gar der Anwendungsbereich der DSGVO verlassen werden. Um dabei den statistischen Aussagegehalt eines Datensatzes und damit die Performance eines Machine-Learning-Algorithmus nicht zu beeinträchtigen, empfiehlt es sich, die erforderlichen Transformationen gemeinsam mit der Auswahl der dem Algorithmus zugrundeliegenden Features zu definieren und vorzunehmen. 5



[3] Vergleiche zu den Konflikten von Transparenz, Accountability und Machine-Learning-Algorithmen Kontext, m.w.N. Rosenthal, Simone: 16.10.2018: DSGVO vs. Künstliche Intelligenz, LR 2018, 173

Die zunächst i.d.R. personenbezogenen Rohdaten werden im Rahmen der Modellierung und Transformation für den Algorithmus aufbereitet, indem gewisse Interpretationen vorgenommen werden. Der daraus resultierende Datensatz enthält dann nur noch beschreibende Merkmale bezüglich der Rohdaten. So kann beispielsweise der *Name* darauf reduziert werden, dass die Groß- und Kleinschreibung nicht beachtet oder eine zufällige Buchstabenfolge verwendet wurde, woraus sich etwa auf betrügerisches Verhalten bei einem Bestellvorgang schließen ließe. Abhängig vom Use-Case kann dabei eine **vollständige Anonymisierung des Feature-Sets** erreicht werden, zumindest jedoch durch die effektive Pseudonymisierung[4] die Arbeit des Teams erheblich erleichtert werden. 6

Um Machine-Learning-Projekte nicht durch datenschutzrechtliche Anforderungen zu verkomplizieren, sollte daher der Transformationsprozess bereits in der Speicherumgebung der Rohdaten erfolgen, um die Machine-Learning-Umgebung nicht mit personenbezogenen Daten zu „kontaminieren". 7

III. Transparency und Accountability durch technisches und operatives Monitoring

Transparenz und Accountability erfordern gleichermaßen ein Verständnis des vom Algorithmus angewendeten Regelwerks. Unabhängig vom Trainingsmodell müssen daher zumindest initial die Gewichtungen der Kriterien und die Auswirkungen verschiedener Korrelationen auf die Ergebnisse dokumentiert werden. Verändern sich die Gewichtungen während der Verwendung des Algorithmus, lernt also das Programm im Live-Betrieb, muss zusätzlich gewährleistet sein, dass Veränderungen der Gewichtungen erkannt werden können. Diese Art des **Algorithmus-Monitorings** ist nicht zuletzt auch im Interesse des Unternehmens, da i.d.R Entscheidungen von operativer Bedeutung getroffen werden, von deren Qualität der Unternehmenserfolg zumindest teilweise abhängt. 8

Während zumindest bei den häufig verwendeten Random-Forest Algorithmen die Gewichtung einzelner Kriterien einfach möglich ist,[5] ist diese Bewertung bei komplexen neuronalen Netzen, die insofern häufig als „Black-Box" bezeichnet werden, ungleich schwerer.[6] Zudem kommt das Erfordernis, die Informationen zu interpretieren und Betroffenen sowie Behörden in einem verständlichen Format zu präsentieren. 9

Einen operativen Ansatz für das (regelmäßige) Monitoring der Entscheidungsprozesse bietet **Blackbox-Tinkering**. Dabei werden testweise in jeweils einem Kriterium veränderte Feature- oder Rohdatensätze vom Algorithmus verarbeitet. Die Ergebnisse 10

[4] Dazu ist entscheidend, dass keine direkten Identifier mehr enthalten sind, Art. 89 Abs. 1 S. 4 DSGVO, und eine Identifizierung der betroffenen Person allenfalls noch durch statistische Überlagerung o.ä. Techniken ermöglicht wird.

[5] Donges, Niklas: The Random Forest Algorithm, 22.02.2018https://towardsdatascience.com/the-random-forest-algorithm-d457d499ffcd

[6] Vgl. zu den Möglichkeiten: Sarle, Warren S, 23.06.2000.: How to measure importance of inputs?

dieser Verarbeitung lassen im Vergleich zu den Ergebnissen der originalen Datensätze Rückschlüsse darauf zu, wie sich bestimmte Kriterien oder Kombinationen von Kriterien auf das Ergebnis auswirken.[7] Hinsichtlich der Interpretation und Offenlegung der Informationen bietet dies den Vorteil, dass nicht zwangsläufig die Features des Algorithmus und damit eine unternehmerisch schützenswerte Information offengelegt werden müssen[8] und die Erkenntnisse auf Rohdatenebene bereits in interpretierbarer Form vorliegen.

IV. Verwendung von Bestandsdaten

Neben den akuten regulatorischen Anforderungen muss bei der Planung von Machine-Learning-Projekten berücksichtigt werden, dass sich Anforderungen an den Rohdatenbestand aufgrund technischer Entwicklungen und Erkenntnisse ändern können. Daten, die bei Beginn eines Projekts möglicherweise aus qualitativen Gründen ungeeignet sind, können durch neu gewonnene Erkenntnisse oder neue Zielsetzungen in einem späteren Stadium des Projekts an Relevanz gewinnen. Unternehmen sollten daher möglichst früh ihre Ziele und Erwartungen derart konkretisieren, um datenschutzrechtliche Grundsätze, insbesondere den der Datenminimierung, bei der Konzeptionierung zu berücksichtigen. 11

Hinsichtlich bereits vorhandener Daten kann unter Umständen eine zulässige Zweckänderung Machine-Learning Projekte ohne gesonderten Rechtfertigungstatbestand ermöglichen, soweit es sich um statistische Datenverarbeitungen handelt.[9] Vorausgesetzt, die Daten werden entsprechend der obigen Darstellung derart transformiert, dass eine Re-Identifizierung einzelner Personen ausgeschlossen ist, profitieren die anschließenden Verarbeitungsschritte von der Privilegierung statistischer Methoden, die auch KI-Anwendungen erfasst. Die DSGVO-Compliance für die nachfolgende Verarbeitung wird dadurch im Wesentlichen auf die Informationspflichten beschränkt – vor diesem Hintergrund empfiehlt es sich, Machine-Learning-Projekte bereits in der Planungsphase in der Datenschutzerklärung transparent zu berücksichtigen. 12

V. Fazit

Neben der richtigen technischen Gestaltung sollten Machine-Learning-Projekte von rechtlichen Erwägungen flankiert werden. Zusammengefasst können sich Unternehmen an folgenden Handlungsempfehlungen orientieren: 13

[7] Perel, Maayan; Elkin-Koren, Niva, 18.10.2018: Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement
[8] Vgl. zum Sonderproblem der Offenlegung des Algorithmus Rosenthal, Simone: a.a.O.
[9] BeckOK DatenschutzR/Schantz DS-GVO Art. 5 Rn. 22

1. Berücksichtigung von rechtlichen Aspekten bei der Feature-Auswahl
2. Machine-Learning-Entwicklungsumgebung ohne personenbezogene Daten
3. Regelmäßiges Monitoring und Evaluation der Entscheidungen
4. Nachhaltiges Datennutzungs- und Datenschutzkonzept

So lassen sich Risiken auch in einem anspruchsvollen regulatorischen Umfeld vermeiden, ohne den Anschluss an die technische Entwicklung zu verlieren. 14