How-to: Datenschutzkonforme Durchführung von KI-Projekten

Projekte im Zusammenhang mit künstlicher Intelligenz («KI») haben sich unterdessen zu einer vielversprechenden Möglichkeit für nach Innovation und Effizienz strebende Unternehmen entwickelt. In KI-Projekten werden Algorithmen des maschinellen Lernens eingesetzt, um umfangreiche Datensätze zu analysieren und komplexe Aufgaben zu automatisieren. Die Vorteile von KI-Initiativen liegen auf der Hand. Doch stellt der Umstand, dass zur Nutzung von KI auch umfangreiche Datensätze verwendet werden, Unternehmen vor datenschutzrechtliche Fragestellungen.

Von Dirk Spacek und Julia Nitschke

Wie KI funktioniert und wofür sie verwendet wird

KI lässt sich grob formuliert beschreiben als die Fähigkeit eines Programms, Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern oder besser gesagt eine Art «erhöhte Intelligenz» eines Computerprogramms. Dazu gehören z. B. die Problemlösung, Spracherkennung, Lernen, Planung, Wahrnehmung und Entscheidungsfindung. Ein wichtiges Teilgebiet der KI stellt das sog. maschinelle Lernen dar, im Rahmen dessen Computersysteme aus zahlreichen historischen Daten lernen und ihre Leistung in Bezug auf eine bestimmte Aufgabe verbessern können, ohne explizit dafür programmiert zu werden.

Heutzutage kommen zahlreiche Unternehmen nicht umhin, sich mit der Nutzung von KI auseinanderzusetzen und durch deren Vorteile (insbesondere Effizienzsteigerung, Präzision der Aufgabenausführung und Kostenersparnis) mit Konkurrenzunternehmen Schritt zu halten. Die Nutzung von KI erfordert jedoch den Einsatz umfangreicher Daten, mit denen die KI sozusagen «gefüttert» werden muss, um ihre Lernfähigkeit zu entfalten. Dies bringt auch Herausforderungen und ethische Fragestellungen mit sich, die nicht zuletzt datenschutzrechtliche und IT-sicherheitstechnische Rahmenbedingungen betreffen.

Wie KI-Innovation und Datenschutz Hand in Hand gehen

Wenn ein KI-System mit personenbezogenen Daten gespeist werden soll, müssen Unternehmen ethischen und rechtlichen Überlegungen zum Schutz der Privatsphäre des Einzelnen Rechnung tragen.

a) Klärung der Zulässigkeit von Datennutzungen und der Rahmenbedingungen für die Nutzung des KI-Tools

In einem ersten Schritt ist es für ein Unternehmen unerlässlich, zu prüfen, woher es personenbezogene Daten überhaupt erhält und ob es befugt ist, diese im Rahmen eines KI-Tools überhaupt einzusetzen. Denn nicht zuletzt werden solche Daten dadurch mit dem Anbieter dieser KI-Tools unter Umständen ausgetauscht und Bearbeitungen zugänglich gemacht, die den betroffenen Datensubjekten möglicherweise nicht transparent klar sind. Letzteres ist aber ein Grunderfordernis des schweizerischen Datenschutzgesetzes (siehe Art. 19 DSG zur allgemeinen Informationspflicht gegenüber Betroffenen). In einem zweiten Schritt sollten die vertraglichen Rahmenbedingungen der Nutzung eines KI-Tools geprüft werden (insbesondere Terms of Use, Usage Policies). Im Hinblick auf die datenschutzrechtliche Verantwortlichkeit sind Szenarien der getrennten oder gemeinsamen Verantwortlichkeit sowie der Auftragsdatenbearbeitung mit dem KI-Tool-Anbieter vorstellbar. Im letztgenannten Szenario wäre die Notwendigkeit des Abschlusses eines Auftragsverarbeitungsvertrags mit dem Anbieter des KI-Tools zu prüfen (ggf. unter Einschluss von Standardvertragsklauseln für die Übermittlung

von Personendaten an unsichere Drittländer).

Ebenso sollte ein Unternehmen die Funktionsweise des KI-Tools zumindest im Wesentlichen nachvollziehen können, um nicht zuletzt die Datensubjekte transparent über die Datenbearbeitung informieren zu können. Dieser Schritt gestaltet sich in der Praxis häufig als schwierig, denn die konkreten Verarbeitungsschritte eines KI-Tools sind komplex und für IT-Laien von aussen oft kaum fassbar. Oftmals bedingen sich Anbieter von KI-Tools das Recht aus, einmal gelieferte Daten für maschinelles Lernen und neu daraus gewonnene Erkenntnisse (Output) nach freiem Ermessen für beliebige Zwecke weiter nutzen zu können. Dies wäre z. B. mit dem Zweckbindungsgrundsatz aus Sicht des Unternehmens nicht ohne Weiteres vereinbar.

b) Einhaltung der Datenschutzgrundsätze

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte («EDÖB») hat öffentlich mitgeteilt, dass das am 1. September 2023 in Kraft getretene revidierte Bundesgesetz über den Datenschutz («DSG») auf KI-gestützte Datenbearbeitungen direkt anwendbar sei. Die Datenbearbeitungen müssen daher insbesondere den Grundsätzen in Art. 6 DSG der Verhältnismässigkeit, der Zweckbindung und Datenrichtigkeit entsprechen. Unternehmen seien nach Auffassung des EDÖB gehalten, eine ausdrückliche Einwilligung des Datensubjekts einzuholen, sofern besonders schützenswerte Personendaten (z. B. genetische oder biometrische Daten) bearbeitet werden und ein Profiling mit einem hohen Risiko für die Betroffenen durchgeführt wird (z. B. bei KI-gestützter personalisierter Online-Werbung oder auch Arbeitsplatzüberwachung). Ferner sollte die Gewährleistung von Transparenz gegenüber den Datensubjekten mit Priorität behandelt werden. Eine transparente Kommunikation – beispielsweise im Wege der Datenschutzerklärung – über die Verwendung der Daten, den Zweck der Datenbearbeitung und deren mögliche Auswirkungen ist angezeigt. Grundlage dafür bildet das bereits erwähnte Verständnis Betroffener für die Einzelheiten der KI-basierten Bearbeitung ihrer personenbezogenen Daten. Schliesslich sollten Unternehmen nur Daten erheben und bearbeiten, die für die Ziele des KI-Projekts unbedingt erforderlich sind (Grundsatz der Datensparsamkeit). Ausserdem sollten die Daten nicht für Zwecke verwendet werden, die über das hinausgehen, worüber die Betroffenen bei der Einholung der Zustimmung ursprünglich informiert wurden (Grundsatz der Zweckbindung).

c) Datenschutz-Folgenabschätzung

Bringt die KI-basierte Datenbearbeitung ein hohes Risiko für die Persönlichkeit der Datensubjekte mit sich (was tendenziell bei umfangreicher Bearbeitung besonders schützenswerter Personendaten der Fall sein kann), hat der Verantwortliche vor der Datenbearbeitung eine Datenschutz-Folgenabschätzung durchzuführen und unter Umständen die eigene/den eigenen Datenschutzberater*in oder den EDÖB zu konsultieren. Als sog. besonders schützenswerte Personendaten gelten neben Gesundheitsdaten auch genetische und biometrische Daten.

d) Technische und organisatorische Massnahmen

Geeignete technische und organisatorische Massnahmen (sog. TOMs) sind für den Schutz personenbezogener Daten in KI-Projekten unerlässlich. Verschlüsselung, Zugriffskontrollen und sichere Speicherung sind unerlässlich, um unbefugten Zugriff und potenzielle Datenverletzungen zu verhindern. Die Prozesse beim Einsatz eines KI-Tools sollten derart ausgestaltet sein, dass Betroffene ihre Datenschutzrechte auch z. B. gegenüber dem KI-Anbieter durchsetzen könnten. In diesem Zusammenhang sollten Mechanismen erwogen werden, die einen einfachen Zugang der Datensubjekte zu ihren persönlichen Daten gewährleisten.

e) Automatisierte Entscheidungen

Gemäss dem revidierten Schweizer DSG sind automatisierte Entscheidungen, d. h. Entscheidungen, die ausschliesslich auf einer automatisierten Datenbearbeitung basieren und mit

einer Rechtsfolge für die Betroffenen verbunden sind, transparent offenzulegen. Ferner haben die Betroffenen ein Interventionsrecht und können die Vornahme einer menschlichen Entscheidung einfordern. Sollte somit ein KI-Tool eingesetzt werden, um automatisierte Entscheidungen mit Rechtsfolgen für Individuen zu treffen, dann müsste dies im Rahmen der Datenschutzerklärung des jeweiligen Unternehmens offengelegt werden.

Ein Blick über die Schweizer Landesgrenzen: EU-Künstliche-Intelligenz-Verordnung («KI-Verordnung»)

Obwohl die genannte Gesetzgebung für die Schweiz als Nicht-EU-Mitglied nicht verbindlich ist, ist darauf hinzuweisen, dass die Europäische Union mit der (noch nicht definitiv verabschiedeten) KI-Verordnung beabsichtigt, den Umgang künstlicher Intelligenz weitgehender zu regulieren – d. h. auch über den datenschutzrechtlichen Rahmen hinausgehend. Eine Vertiefung dieses Aspekts muss hier aus Platzgründen unterbleiben, doch sollte bei grösseren KI-Projekten mit Auslandsbezug in die EU (z. B. wenn die Auswertungsergebnisse in der EU verwertet werden sollen) eine Prüfung dieser zusätzlichen Normen nicht unterlassen bleiben.

Fazit: Datenschutz wahren, Vertrauen gewinnen

Ethisch vertretbare und rechtlich zulässige KI-Projekte können zu Sprungbrettern für zukunftsgerichtete Unternehmen werden. Zwangsläufig haben sich Unternehmen jedoch mit den datenschutzrechtlichen Rahmenbedingungen auseinanderzusetzen, um das Vertrauen der Datensubjekte zu gewinnen. Dieses Vertrauen der Datensubjekte, das Fundament des unternehmerischen Geschäfts, wird bedauerlicherweise immer häufiger durch Online-Angriffe und Datenlecks erschüttert. Es liegt an den Unternehmen, dieses Vertrauen durch regelmässige Audits zu schützen. Schliesslich drohen bei Verletzungen datenschutzrechtlicher Sorgfaltspflichten neben Imageschäden nach dem neuen DSG in gewissen Konstellationen gegebenenfalls persönliche Bussen bis zu CHF 250 000.–.

CHECKLISTE

- Evaluierung der Basis, aufgrund derer personenbezogene Daten für den Einsatz in KI-Tools überhaupt verwendet werden dürfen (insbesondere transparente Information Betroffener im Vorfeld und Umschreibung der in Aussicht stehenden Bearbeitungsprozesse)
- Prüfung der Vertragsbedingungen des Anbieters des KI-Tools, allenfalls Abschluss eines Auftragsverarbeitungsvertrags (ggf. einschliesslich Datentransfer-Standardvertragsklauseln je nach Standort des Anbieters)
- Schulung des Projektteams über Funktionen des KI-Tools und Datenschutzimplikationen, ggf. arbeitsvertragliche Anpassungen
- vorgängige Durchführung einer Datenschutz-Folgenabschätzung (sofern erforderlich)
- Evaluierung der in Aussicht stehenden Datenbearbeitung: Werden die Daten entsprechend ihrem Erhebungszweck bearbeitet (Zweckbindung)? Werden nur zwingend notwendige Daten bearbeitet resp. nicht benötigte Daten regelmässig gelöscht oder anonymisiert (Datensparsamkeit)?
- transparente Aufklärung der Datensubjekte über die Verwendung der Daten: Welche Daten werden zu welchem Zweck bearbeitet? Wie funktionieren die KI-Algorithmen, und wie können diese die Daten beeinflussen? Ist die Datenschutzerklärung hinreichend transparent formuliert? Werden automatisierte Entscheidungen mit Rechtsfolgen für Betroffene mit dem KI-Tool getroffen?
- allfällige Einholung einer Einwilligung der Datensubjekte (sofern erforderlich)
- Sicherstellung der Einhaltung von TOMs (Verschlüsselungstechnologien, Zugriffskontrollen etc.)
- Implementierung von Mechanismen, die einen einfachen Zugang der Datensubjekte zu ihren persönlichen Daten gewährleisten
- Durchführung von Datenschutzaudits zur Sicherstellung der datenschutzrechtlichen Rahmenbedingungen

AUTOREN

Dirk Spacek ist Partner und Co-Verantwortlicher der Praxisgruppen TMC und IP. Er befasst sich vornehmlich mit neuen Geschäftsmodellen im Medien-, Internet- und Technologiesektor, der Datenvermarktung und dem Immaterialgüterrecht.

Julia Nitschke ist Rechtsanwältin und gehört den Praxisgruppen TMC und IP an. Sie berät Klienten vornehmlich aus der Medien-, Software-, Life-Sciences- und Finanzdienstleistungsbranche in technologiebezogenen Fragen, insbesondere in den Bereichen Datenschutz, IT-Vertragsrecht, Outsourcing sowie Cybersecurity.

IMPRESSUM

Verlag: WEKA Business Media AG, Hermetschloostrasse 77, CH-8048 Zürich, www.weka.ch
Herausgeber: Stephan Bernhard
Redaktion: Marco S. Meier
Korrektorat: Margit Bachfischer M.A., Bobingen
Layout/Satz: Tonio Schelker
Publikation: 10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten. Als digitale Publikation erhältlich unter: www.weka-library.ch
Bildrechte: www.istockphoto.com
Bestell-Nr.: 9231

Scannen und bestellen:
Dieser Newsletter ist in gedruckter Form und digital in unserem Online-Shop erhältlich.

Ihre Vorteile
- Fundiertes Praxiswissen der Datenschutzanforderungen
- Lösungen für Datenschutzthemen

www.weka.ch/shop

© WEKA Business Media AG, Zürich, 2024

Urheber- und Verlagsrechte: Alle Rechte vorbehalten, Nachdruck sowie Wiedergaben, auch auszugsweise, sind nicht gestattet. Die Definitionen, Empfehlungen und rechtlichen Informationen sind von den Autoren und vom Verlag auf ihre Korrektheit in jeder Beziehung sorgfältig recherchiert und geprüft geworden. Trotz aller Sorgfalt kann eine Garantie für die Richtigkeit der Informationen nicht übernommen werden. Eine Haftung der Autoren bzw. des Verlags ist daher ausgeschlossen. Wenn möglich verwenden wir immer geschlechtsneutrale Bezeichnungen. Aus Platzgründen oder aufgrund einer besseren Lesbarkeit verwenden wir bei Texten nur eine Schreibweise.