Regulierung und Künstliche Intelligenz

Compliance-Risiken hinter der Anwendung von KI im Finanzbereich

Inhalt

Ausgangslage
Compliance-Risiken hinter der Anwendung von KI im Finanzbereich

Beispiele zur Regulierung von Künstlicher Intelligenz
Finanzdienstleistungen: Singapur und die Schweiz
Transparente KI im öffentlichen Sektor
GDPR-Vorschriften für die Anwendung von KI
Innovationsschutz für Algorithmen
Thema GDPR als Vorbote für eine Zertifizierung von KI?

Unser Angebot
Ein Halbtages-Workshop zum Thema KI-Compliance

Regulatoren, sowie grosse Unternehmen der Finanzbranche haben Risiken hinter KI erkannt

Bank of America:
“Automatische Bewertung von Individuen muss nachvollziehbar sein”

Algorithmen treffen potentiell regulatorisch oder ethisch nicht vertretbare Entscheidungen. Daher müssen Banken die Funktionsweise und das Zustandekommen einer Entscheidung durch KI nachvollziehen können.

Financial Stability Board:
“Deutliche Chancen durch AI, falls Risiken ausreichend beachtet werden”

Die noch fehlende Auditierbarkeit von KI kann ein systemisches Risiko bedeuten. Verbreitete Anwendung von “Black-box” Modellen kann unbeabsichtigte Folgen wie mangelnde Datensicherheit, Verhaltensrisiken und Cyber Security haben.

Allianz: “The rise of Artificial Intelligence”

Die Allianz identifiziert fünf Risikofaktoren leistungsfähiger KI: Ethik, Haftbarkeit, Verantwortlichkeit, Sicherheit und Zugang zu Software. Diese aufkommenden Risiken betreffen Geschäftsrisiken, Arbeitsunterbrechungen, Änderungen in Haftbarkeit, sowie Nicht-Konformität mit Regulierung

Finanzdienstleistungen: Singapur und die Schweiz

Die Monetary Authority of Singapore hat im November 2018 Prinzipien erlassen, um principles Fairness, Ethik, Verantwortlichkeit und Transparenz (FEAT) in der Anwendung von Künstlicher Intelligenz und Data Analytics im Finanzbereich zu fördern.

Darunter fallen unter anderem, dass KI-Modelle frei von nicht beabsichtigtem Bias sein sollen, und dass Firmen, welche KI-Modelle verwenden, verantwortlich sowohl für intern als auch extern entwickelte und eingekaufte Komponenten sein sollen.

Bereits im Rundschreiben 2013/8 stellte die Finma fest:

“Beaufsichtigte, die algorithmischen Handel betreiben (vgl. Rz 18), müssen durch wirksame Systeme und Risikokontrollen sicherstellen, dass dadurch keine falschen oder irreführen-den Signale für das Angebot, die Nachfrage oder den Kurs für Effekten erfolgen können.

Beaufsichtigte müssen die wesentlichen Merkmale ihrer algorithmischen Handels-strategien auf für Dritte nachvollziehbare Art und Weise dokumentieren.”

Transparente KI im öffentlichen Sektor

New York City verabschiedete im Dezember 2017 ein viel beachtetes Gesetz zu algorithmic accountability. Mit dieser Initiative möchte die Stadt eine Task Force ins Leben rufen, welche Fairness und Anwendbarkeit von Algorithmen, die von öffentlichen Einrichtungen angewendet werden, überwachen soll.

New York verwendet Algorithmen beispielsweise um zu bestimmen,

- ob bedürftige Angeklagte Anspruch auf ermässigte Kautionen bekommen sollen,
- wo in der Stadt optimal Feuerwehren eingerichtet werden sollen,
- um Schüler öffentlichen Schulen zuzuweisen,
- die Leistung von Lehrpersonen zu evaluieren,
- Betrug bei der Versicherung Medicad zu identifizieren,
- sowie Verbrechen vorherzusagen

GDPR-Vorschriften für die Anwendung von KI

Die GDPR hat unweigerlich Auswirkungen auf die Anwendbarkeit von Künstlicher Intelligenz. Als Hauptprobleme wurden identifiziert:

- Firmen unterschätzen die GDPR-Pflichten
- Firmen betrachten die Datenprozessierung als Geschäftsgeheimnis und möchten diese nicht öffentlich legen
- Die Erklärung einer Vorhersage eines ML-Algorithmus ist nicht immer einfach möglich.

Darüber hinaus stellen sich Fragen wie:

- Kann ein eindeutiger Zweck hinter der Prozessierung ermittelt werden?
- Wie lassen sich die sich stets veränderten Ergebnisse eines kontinuierlich lernenden Algorithmus argumentieren?
- Das Prinzip der Minimierung personenbezogener Daten (“adequate, relevant and limited”) scheint im Widerspruch mit den Anforderungen von Künstlicher Intelligenz zu sein.
- Wie ist das Recht der Person, “nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden” (Artikel 22 GDPR) mit dem expliziten Ziel der Automatisierung durch KI-Algorithmen überein zu bringen?

GDPR-Pflichten bei der Bearbeitung von Personendaten mit KI

- Grundsätze: Rechtmässigkeit, Verarbeitung von Treu und Glauben, **Transparenz**, Datenminimierung, **Richtigkeit**
- GDPR-Einhaltung muss vom Verantwortlichen nachgewiesen werden können (**Rechenschaftspflicht**)
- Betroffene Personen müssen informiert werden (**Informationspflicht**)
- Regeln für **automatisierte Entscheidungen** (Art. 22 GDPR) - ausdrückliche Einwilligung oder Recht “nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden”
- Bei Risiko für Rechte und Freiheiten der betroffenen Personen: Pflicht, eine **Datenschutz-Folgenabschätzung** durchzuführen (Art. 35 GDPR); hierzu gibt es black lists/white lists der Datenschutzbehörden
- **Procurement Assurance Compliance:** Pflichten beim “Einkauf” von KI-Dienstleistungen /Outsourcing (Art. 28 GDPR): Due Diligence; Auftragsverarbeitungsverträge
- GDPR fördert datenschutzspezifische Zertifizierungsverfahren und **Datenschutzsiegel** und -prüfzeichen, die dazu dienen, GDPR Compliance nachzuweisen

Innovationsschutz

- Wem “gehören” Algorithmen? Können diese als IP oder sonstwie geschützt werden?
- Wem “gehört” der Output? Kann der Output als IP oder sonstwie geschützt werden.

Thema GDPR als Vorbote für eine Zertifizierung von KI?

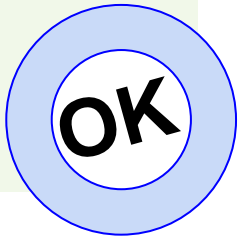
Für GDPR werden bereits Audits und Zertifizierungen angeboten. Wann wird die Zertifizierung von KI Einzug halten?

Heute:

Einkäufer digitaler Dienstleistungen muss durch Due Diligence sicherstellen, GDPR-compliant zu beschaffen.

→

Verkäufer muss GDPR-Compliance nachweisen können, allenfalls zertifiziert.



Künftig:

Einkäufer KI-unterstützter Produkte und Dienstleistungen muss durch Due Diligence sicherstellen, GDPR-compliant zu beschaffen.

→

Verkäufer muss GDPR-Compliance, sowie weitere Qualitätskriterien der KI nachweisen können, allenfalls zertifiziert.

Unser Angebot:
Ein Halbtages-Workshop zum Thema KI-Compliance

Rechtlicher Rahmen & Schutz

- Wie sieht das regulatorische Umfeld für KI-Projekte aus? Was sind die Pflichten?
- Was sind die rechtlichen Risiken? Wie können die Risiken minimiert werden?
- Wie können KI Algorithmen und der Output geschützt werden?
- Optik Anbieter/Einkäufer/Governance

Technische Massnahmen & KI-Einsatz

- Wie kann man Daten und Modelle auf unerwünschten Bias prüfen?
- Wie kann man Algorithmen für sich und für die Kunden interpretieren?
- Wie kann Drittanbieter-KI-Software einer Due Diligence unterzogen werden?
- Worauf sollte man beim Einkauf von KI-Software achten?

Preis: CHF 4‘850 exkl. MWSt.

Kontaktieren Sie uns!

Dr. Christian Spindler
+41 79 875 92 43
cspindler@dataaheadanalytics.ch

Dr. Martin Eckert
+41 44 254 99 66
martin.eckert@mme.ch

DATA AHEAD ANALYTICS
Technopark
8005 Zürich
Schweiz

+41 79 875 9243
info@dataaheadanalytics.ch

MME Legal | Tax | Compliance
Zollstrasse 62
8031 Zürich
Schweiz

+41 44 254 99 66
office@mme.ch