Alert

Breaking News
von Blum & Grob

Zürich, Juli 2024

Der EU AI Act und seine Auswirkungen auf Unternehmen in der Schweiz

Die europäische Verordnung zur Regulierung von künstlicher Intelligenz (häufig AI Act genannt) ist am 12. Juli 2024 im Amtsblatt der Europäischen Union veröffentlicht worden. Damit stellen sich Fragen, ob, wann und inwiefern Unternehmen in der Schweiz vom AI Act betroffen sein könnten.

Anwendungsbereich: Der AI Act regelt den Umgang mit künstlicher Intelligenz («KI» oder auf Englisch mit «AI» für Artificial Intelligence abgekürzt). Der AI Act wird auch ausserhalb der EU Wirkung entfalten, also auch auf Schweizer Unternehmen anwendbar sein, die nicht in der EU ansässig oder niedergelassen sind, wenn sie eine der vorliegenden Voraussetzungen erfüllen:

- Anbieter, die in der Union KI in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;
- Anbieter und Betreiber von KI, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn die von der KI hervorgebrachte Ausgabe in der Union verwendet wird oder sofern sich betroffene Personen in der EU befinden;
- Produkthersteller, der KI zusammen mit seinem Produkt und unter seiner eigenen Handelsmarke in der EU in Verkehr bringt oder in Betrieb nimmt;
- Einführer oder Händler, der KI auf dem Unionsmarkt bereitstellt;
- Bevollmächtigte von Anbietern, die nicht in der Union niedergelassen sind.

Was versteht die Verordnung unter KI? Im AI Act wird zwischen KI-Systemen und KI-Modellen unterschieden: Ein KI-System ist ein computergestütztes System, das eigenständig funktionieren kann und sich an neue Situationen anpassen kann. Es kann aus den Informationen, die es bekommt, lernen und dann Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen treffen, die entweder in der realen oder in der virtuellen Welt Wirkung zeigen können. Die EU-Kommission hat eine breite Definition gewählt, um sicherzustellen, dass sie auch für zukünftige technologische Entwicklungen passt. Beispiele für solche KI-Systeme sind ChatGPT, Gemini oder Mistral. KI-Modelle sind das Herzstück von KI-Systemen und somit deren Bestandteil. Damit ein KI-Modell zum KI-System wird, müssen weitere Komponenten, wie z.B. Nutzerschnittstellen hinzugefügt werden, sie müssen also in ein KI-System integriert werden. Der AI Act sieht für KI-Systeme und KI-Modelle mit allgemeinem Verwendungszweck (General Purpose Modelle), die systemische Risiken bergen, spezifische Regelungen vor. Derartige KI-Systeme und Modelle sind bereits weitläufig im Einsatz, vielleicht auch in Ihrem Unternehmen.

Wie funktioniert der AI Act: Der AI Act folgt einem risikobasierten Ansatz. Dabei unterscheidet die Verordnung KI-Systeme je nach Höhe des Risikos für Betroffene oder die Gesellschaft. Unterschieden wird in KI-Systeme, die verboten sind, Hochrisiko-KI-Systeme, KI-Systeme mit limitiertem Risiko und KI-Systeme mit minimalem Risiko.

Verbotene KI-Systeme: Solche KI-Systeme sind generell verboten. Dazu gehören z.B. KI-Systeme, welche die Entscheidungen von Menschen manipulieren oder ihre Schwachstellen ausnutzen, die zu Social Scoring verwendet werden oder das Risiko einer Person, eine Straftat zu begehen (Predictive Policing), vorhersagen. Auch verboten sind KI-Systeme, die eigenständig Gesichtsbilder aus dem Internet oder aus Videoüberwachungsanlagen auslesen, Emotionen am Arbeitsplatz oder in Bildungseinrichtungen erkennen und Menschen auf der Grundlage ihrer biometrischen Daten kategorisieren (jedoch mit Ausnahmen für Strafverfolgungszwecke).

Hochrisiko-KI-Systeme: Hochrisiko-KI-Systeme sind solche Technologien, die ein hohes Risiko für die Gesellschaft oder Einzelpersonen darstellen können. Dazu zählen KI-Systeme, die biometrische Daten verwenden oder als wichtige Sicherheitskomponente in kritischen Infrastrukturen eingesetzt werden. Ebenso fallen unter diese Kategorie Systeme, die automatisch Bewerber auswählen oder Entscheidungen treffen, die das Arbeitsverhältnis beeinflussen können. Für diese Hochrisiko-KI-Systeme gibt es strenge Regelungen. Sie müssen zum Beispiel sicherstellen, dass die Entscheidungswege nachvollziehbar sind und Risiken bewertet sowie minimiert werden.

KI-Systeme mit limitiertem Risiko: Darunter fallen z.B. KI-Systeme, wie Textgeneratoren (z.B. ChatGPT) und solche, die Deep Fakes generieren. Hier müssen natürliche Personen, die mit diesen KI-Systemen interagieren, informiert werden, dass sie es mit einem KI-System zu tun haben, sofern dies nicht offensichtlich ist.

KI-Systeme mit minimalem Risiko: Dies betrifft beispielsweise Spamfilter oder Videospiele mit KI-Unterstützung. Hier werden lediglich freiwillige Verhaltenskodizes vom AI Act vorgegeben.

Umsetzungsfristen: Der AI Act wurde am 12. Juli 2024 im Amtsblatt der EU veröffentlicht und tritt 20 Tage später In Kraft, wobei es ab Inkrafttreten verschiedene Umsetzungsfristen für bestimmte Vorschriften geben wird:

- 6 Monate für verbotene KI-Systeme
- 12 Monate für KI-Modelle mit allgemeinem Verwendungszweck (General Purpose Modelle)
- 24 Monate für Hochrisiko-KI-Systeme nach einem separaten Anhang III und die restlichen Bestimmungen
- 36 Monate für Hochrisiko-KI-Systeme nach einem separaten Anhang I

Situation in der Schweiz: Bereits mit Veröffentlichung im Amtsblatt kann der AI Act Schweizer Unternehmen betreffen. Aber selbst wenn Unternehmen noch nicht in den Anwendungsbereich der Verordnung fallen, so ist es bereits jetzt sinnvoll sich vorzubereiten! Denn auch hierzulande lässt der Bundesrat momentan prüfen, welche Regulierungsansätze in der Schweiz möglich wären. Somit ist zu erwarten, dass auch in der Schweiz eine Regulierung zum Einsatz von künstlicher Intelligenz bevorsteht. Ein frühzeitiges Bewusstsein über die eigenen Systeme und Anforderungen hilft der späteren Regulierung Herr zu werden. Dabei darf nicht vergessen werden, dass schon heute diverse Regelungen beim Einsatz von künstlicher Intelligenz zu beachten sind (z.B. Datenschutzrecht, Urheberrecht).

Gerne unterstützen wir Sie bei der gesetzeskonformen Implementierung von KI in Ihr Unternehmen. Informieren Sie sich rechtzeitig, ob Ihr Unternehmen vom AI Act betroffen ist und welche Vorschriften eingehalten werden müssen. Wir freuen uns darauf, Sie auf diesem Weg zu begleiten. Bei Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit besten Grüssen,

Ihr Blum&Grob-Team

David Schwaninger
d.schwaninger@blumgrob.ch

Simon Fritsch
s.fritsch@blumgrob.ch

Elisabeth Niederstetter
e.niederstetter@blumgrob.ch