Praxishandbuch für Betreiber: Nutzung bestehender DSGVO-Instrumente zur KI-Verordnung-Compliance

Juni 2024

Dieses Praxishandbuch dient als Leitfaden zur Anpassung von Instrumenten, die gemäß der DSGVO entwickelt wurden, um die Anforderungen der KI-Verordnung (KI-VO) zu erfüllen. Der Fokus liegt darauf, Synergien zwischen Datenschutz- und KI-Compliance herzustellen und praxisnahe Schritte zur Umsetzung zu bieten.

Executive Summary

Die wichtigsten Aspekte, die sich für einen Betreiber eines KI-Systems ergeben:

1. Identifikation von KI-Systemen
Wird oder soll ein KI-System genutzt werden?

2. Rollenverteilung
Welche Rolle kommt mir nach der KI-Verordnung zu? Bin ich Anbieter, Bereitsteller, Händler etc.?

3. Aufgaben
Je nach Risikokategorie des KI-Systems kommen Aufgaben auf mich zu, insbesondere:

- Regelmäßige Risikoeinschätzungen
- Informations- und Transparenzpflichten
- Regelmäßige Prüfungen der Ergebnisse
- Einrichtung menschlicher Kontrollmechanismen

4. Synergien finden
Synergien im Unternehmen finden: (DORA, NIS II, Datenschutzmanagementsystem, ISO 27001) und andere Rechtsgebiete beachten (DSGVO, Urheberrecht, Data Act etc.).

5. Sanktionen

- Durchführung von verbotenen AI-Praktiken: Geldbuße bis zu EUR 35 Mio, bei Unternehmen bis zu 7 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist.
- Nichteinhaltung von Pflichten im Zusammenhang mit Hochrisiko-KI-Systemen und Nichteinhaltung von Transparenzpflichten: Geldbuße bis zu EUR 15 Mio, bei Unternehmen bis zu 3 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist.

Einleitung

Mit der KI-VO will die EU bessere Bedingungen für die Entwicklung und Nutzung von innovativen Technologien schaffen und die Sicherheit, Transparenz, Nachvollziehbarkeit und Umweltfreundlichkeit von KI-Systemen gewährleisten.

Um dieses Ziel zu erreichen, legt die KI-VO den jeweiligen Akteuren risikobasierte Verpflichtungen auf. Die Risikobewertung von KI-Systemen steht daher als Anknüpfungspunkt der zu treffenden Maßnahmen im Mittelpunkt. Nicht nur die Entwicklung von KI-Systemen oder deren Bereitstellung auf dem Markt, sondern auch die Nutzung von KI-Systemen setzt verschiedene Umsetzungsmaßnahmen voraus.

Um nicht gänzlich neue Strukturen zu schaffen, sollte bei der Umsetzung der Pflichten in der KI-VO auf bestehende Prozesse und Systeme im Unternehmen zurückgegriffen werden. Synergien ergeben sich bei gesetzlichen Bestimmungen oder selbst auferlegten Verhaltensweisen, die bereits Prozesse und Dokumentation im Unternehmen vorsehen. Aus den Dokumentationspflichten von NIS II, DORA, der DSGVO oder zB den in der ISO 27001 vorgesehenen Maßnahmen ergeben sich Synergien, die genutzt werden sollten, um dort mit den Pflichten aus der KI-VO anzuschließen.

Unternehmen sollten sich zur Herstellung der KI-Compliance insbesondere die nachstehenden Fragen stellen:

1 Ist in meinem Unternehmen ein KI-System vorhanden?

Zunächst ist festzustellen, ob im Unternehmen bereits KI-Systeme verwendet werden oder ob sie in Zukunft eingesetzt werden sollen.

Die KI-VO definiert ein KI-System als "*ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können*."

To the point:

KI-Systeme sind Computersysteme, die menschliche Intelligenz simulieren und daher komplexe Aufgaben bewältigen können. Sie können Probleme lösen, lernen, Entscheidungen treffen und mit ihrer Umgebung interagieren. Generative KI erzeugt durch vom Nutzer bereitgestellte Prompts neue Inhalte wie Text, Audio, Bilder oder Videos.
Zunächst ist daher zu prüfen, ob die hergestellte, verkaufte bzw genutzte Software diese Definition erfüllt.

Achtung:

"Herkömmliche Software", also ein System, das auf Regeln basiert, die ausschließlich von natürlichen Personen festgelegt werden, um automatische Vorgänge auszuführen, fällt nicht in den Anwendungsbereich der KI-Verordnung.

2 In welche Risikokategorie fällt mein KI-System?

2.1 Datenschutz-Folgenabschätzung (DSFA) zur Risikobeurteilung des KI-Systems

Nicht nur die DSGVO, sondern auch die KI-Verordnung verfolgt einen risikobasierten Ansatz. Die KI-Verordnung unterscheidet vier Risikokategorien: unannehmbares Risiko (Art 5 KI-VO); hohes Risiko (Art 6 ff KI-VO); geringes Risiko und minimales Risiko.

Ein KI-System gilt als Hochrisiko-KI-System, wenn es in Anhang III genannt ist, es sei denn, es stellt kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte natürlicher Personen dar und beeinflusst ua nicht wesentlich die Entscheidungsfindung. Werden mit dem KI-System personenbezogene Daten verarbeitet, kann für die Risikoabwägung die datenschutzrechtliche DSFA herangezogen werden. Eine DSFA ist gemäß Art 35 DSGVO insbesondere in folgenden Fällen erforderlich:

- systematische und umfassende Bewertung persönlicher Aspekte, die auf einer automatisierten Verarbeitung gründet und natürliche Personen erheblich beeinträchtigt
- umfangreiche Verarbeitung besonders schützenswerter Daten
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Diese Datenverarbeitungen können mit der Einordnung als Hochrisiko-KI-System korrelieren, zB biometrische Identifizierung und Kategorisierung natürlicher Personen, Strafverfolgung, etc.

Aufgrund der Bewertung von persönlichen Aspekten natürlicher Personen erfüllen die in der KI-VO genannten Hochrisiko-KI-Systeme regelmäßig auch die Definition des "Profiling" des Art 4 Z 4 DSGVO.

Praxistipp:
Bereits im Unternehmen durchgeführte DSFA können einen Hinweis darauf geben, ob es sich dem genutzten oder zu nutzenden System um ein Hochrisiko-KI-System handelt.

3 Welche Rolle kommt mir nach der KI-Verordnung zu?

Ähnlich der datenschutzrechtlichen Rollenverteilung ist zunächst zu klären, welche Rolle man gemäß der KI-Verordnung einnimmt.

- **Anbieter:** Anbieter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich.

- **Betreiber:** Betreiber ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet.

- **Bevollmächtigter:** Bevollmächtigter ist eine in der EU ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in der KI-VO festgelegten Pflichten zu erfüllen bzw Verfahren durchzuführen.

- **Einführer:** Einführer ist eine in der EU ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt.

- **Händler:** Händler ist eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers.

4 Welche Pflichten treffen mich als Betreiber laut der KI-Verordnung?

Im Nachfolgenden wird im Sinne der DSGVO-Synergien überblicksmäßig auf die Pflichten von Betreibern eingegangen. Da für die Nichteinhaltung der Pflichten der Betreiber mit einer Geldbuße von bis zu 15.000.000 EUR oder im Falle von Unternehmen von bis zu 3% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden können, sollten Betreiber nach der Ermittlung, in welche Risikoklasse ihre derzeit verwendeten bzw für den Einsatz geplanten KI-Systeme fallen, die Erfordernisse für die ordnungsgemäße KI-Nutzung ableiten.

4.1 Informationspflichten von Betreibern

Klare Informationsprozesse sind sowohl für die Einhaltung der DSGVO als auch für die Einhaltung der KI-VO notwendig. Betreiber haben sicherzustellen, dass sie Betroffene und Mitarbeiter darüber informieren, welche ihrer Daten in einem KI-System verarbeitet werden und zu welchem Zweck.

Achtung:
Werden personenbezogene Daten im KI-System verarbeitet, muss der für die Datenverarbeitung verantwortliche Betreiber gemäß Art 12 DSGVO Maßnahmen treffen, um die betroffenen Personen über diese Datenverarbeitung zu informieren.

4.1.1 Informationspflichten gegenüber Arbeitnehmervertretern und betroffenen Arbeitnehmern

Betreiber von Hochrisiko-KI-Systemen müssen Arbeitnehmervertreter und betroffene Arbeitnehmer informieren, dass sie der Verwendung eines Hochrisiko-KI-Systems unterliegen (werden).

Praxistipp:
Überprüfen, ob auch eine Verpflichtung besteht, eine Betriebsvereinbarung abzuschließen.

4.1.2 Informationspflichten gegenüber natürlichen Personen

Betreiber von Hochrisiko-KI-Systemen müssen betroffene natürliche Personen informieren, dass sie der Verwendung eines Hochrisiko-KI-Systems unterliegen. Art 86 KI-VO sieht vor, dass betroffene Personen, die von einer Entscheidung betroffen sind, die der Betreiber aufgrund der Ausgaben eines Hochrisiko-KI-Systems getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Art erheblich beeinträchtigt und die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte beeinträchtigt, das Recht haben, eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten.

Praxistipp:
Prüfen, ob Auskünfte über aussagekräftige Informationen über diebezüglich der involvierten Logik sowie derie Tragweite und derie angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person iSd Art 15 Abs 1 lit h DSGVO im Falle einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art 22 DSGVO genutzt werden können.

4.2 Transparenzpflichten von Betreibern

Der Grundsatz der Transparenz findet sich nicht nur in Art 5 Abs 1 lit a DSGVO, sondern liegt auch der KI-VO zugrunde. Während Verantwortliche sicherstellen müssen, dass Informationen über die Datenverarbeitung klar, verständlich und leicht zugänglich sind, sieht die KI-VO vor, dass die Funktionsweise von KI-Systemen und ihre Entscheidungsfindung transparent sein muss.

4.2.1 Emotionserkennungssysteme oder Systeme zur biometrischen Kategorisierung

Betreiber eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung müssen betroffene natürliche Personen über den Betrieb des Systems informieren.

4.2.2 Deepfakes

Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden.

Praxistipp:
Mit (digitalen) Hinweisen, zB Disclaimern, kann den Transparenzpflichten nachgekommen werden.

4.3 Sonstige Betreiberpflichten mit DSGVO-Bezug

4.3.1 Einrichtung von TOMs, um den Einklang mit der Gebrauchsanweisung sicherzustellen

Betreiber von Hochrisiko-KI-Systemen müssen geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass das KI-System ordnungsgemäß und gemäß der Betriebsanleitung verwendet wird.

Praxistipp:
Gebrauchsanleitung genau lesen und entsprechende TOMs setzen, zB Prüfprotokolle über für die mit KI-Systemen durchgeführten Vorgänge, begrenzte Zugriffsberechtigungen und strenge Zugangskontroll-/Authentifizierungsprotokolle, Mitarbeiterschulungen, KI-Guidelines, etc.

4.3.2 Überprüfung der Eingabedaten mit der Zweckbestimmung des Hochrisiko-KI-Systems

Gebrauchsanweisungen enthalten die Zweckbestimmung des Hochrisiko-KI-Systems. Betreiber haben sicherzustellen, dass die Daten, die in das Hochrisiko-KI-System eingegeben werden, für den vorgesehenen Zweck des Systems ausreichend repräsentativ, dh so weit wie möglich fehlerfrei und vollständig, sind.

Praxistipp:
Hierbei sind auch die Grundsätze der Datenverarbeitung, insbesondere der Grundsatz der Datenminimierung, zu beachten. Aus datenschutzrechtlichen Aufzeichnungen (zB Verarbeitungsverzeichnis) kann abgeleitet werden, ob die Eingabedaten für die vorgesehenen Zwecke des KI-Systems geeignet sind.

4.3.3 Aufbewahrungspflicht für automatisch erzeugte Protokolldaten

Betreiber eines Hochrisiko-KI-Systems haben Protokolle aufzubewahren, wenn diese ihrer Kontrolle unterliegen. Falls aus den Daten der Protokolle Rückschlüsse auf natürliche Personen möglich sind, handelt es sich um eine Datenverarbeitung und muss diese im Verarbeitungsverzeichnis erfasst werden. Zudem müssen diese Daten auch bei unternehmensweiten Löschroutinen berücksichtigt werden.

4.3.4 Durchführung einer DSFA

Bei der Durchführung der DSFA haben Betreiber von Hochrisiko-KI-Systemen auf die Informationen, die ihnen von dem Anbieter des KI-Systems zur Verfügung gestellt werden, zurückzugreifen. Dies setzt voraus, dass die Informationen über das KI-System hinreichend transparent und verständlich sind.

Praxistipp:
Falls es sich bei dem Anbieter des KI-Systems um einen Auftragsverarbeiter handelt, sollten die Unterstützungspflichten in der DSGVO eingefordert werden.

Kontakt

Günther Leissler
Partner
T: +43 664 80060 3276
E: g.leissler@schoenherr.eu

János Böszörményi
Rechtsanwalt
T: +43 1 534 37 50211
E: j.boeszoermenyi@schoenherr.eu

Denise Stahleder
Rechtsanwaltsanwärterin
T: +43 1 534 37 50912
E: de.stahleder@schoenherr.eu

Christian Kracher
Rechtsanwaltsanwärter
T: +43 1 534 37 50053
E: ch.kracher@schoenherr.eu

Florian Terharen
Rechtsanwaltsanwärter
T: +43 1 534 37 50625
E: fl.terharen@schoenherr.eu

Abonnieren Sie den Schönherr Datenschutzmonitor und bleiben Sie auf dem Laufenden: Unser Newsletter kommt wöchentlich in Ihr E-Mail-Postfach und informiert über aktuelle Datenschutz-Rechtsprechung!

schoenherr.eu/datenschutzmonitor