



Update KI-Verordnung und Data Act – Was die aktuellen Anforderungen für ChatGPT und KI-Anwendungen bedeuten

Dr. Christiane Bierekoven, Rechtsanwältin, Fachanwältin für IT-Recht, GfA Davit

11.10.2023, Knowledge Forum A, Nürnberg



AGENDA

1. Rechtsrahmen - Update KI-VO-E
2. Rechtsrahmen - Update Data Act
3. Bedeutung für ChatGPT und KI-Anwendungen - Fazit

1. Rechtsrahmen - Update KI-VO-E



AGENDA

1. Rechtsrahmen – Update KI-VO-E

Aktueller Stand der Gesetzgebung

- Initiative EU-Kommission: Entwurf KOM (2021) 206 final vom 21.04.2021 („KI-VO-E“)
- **Aktuell:** Trilog-Verhandlungen mit Position des Rates der EU v. 06.12.2022 und den **771 Änderungsanschlügen** des EU-Parlamentes vom 14.06.2023

Wesentliche Änderungen des EU-Parlamentes:

- Ausweitung des Anwendungsbereiches
- Ausweitung der Verbote
- Änderungen bei Hochrisiko-Systemen
- Neu-Regelung zu Basismodellen/Generativer KI

1. Rechtsrahmen – Update KI-VO-E

Änderung 1 - Ausweitung des Anwendungsbereichs

durch

Erweiterung des Begriffs „KI-System“, Art. 3 Nr. 1 KI-VO-E

Danach ist **ein KI-System**

- ein maschinenbasiertes System, das so konzipiert ist,
- das es mit *unterschiedlichem Grad an Autonomie* operieren kann und
- das für explizite oder implizite Ziele
- *Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann,*
- *die das physische oder virtuelle Umfeld beeinflussen.*

Entspricht Definition des OECD.

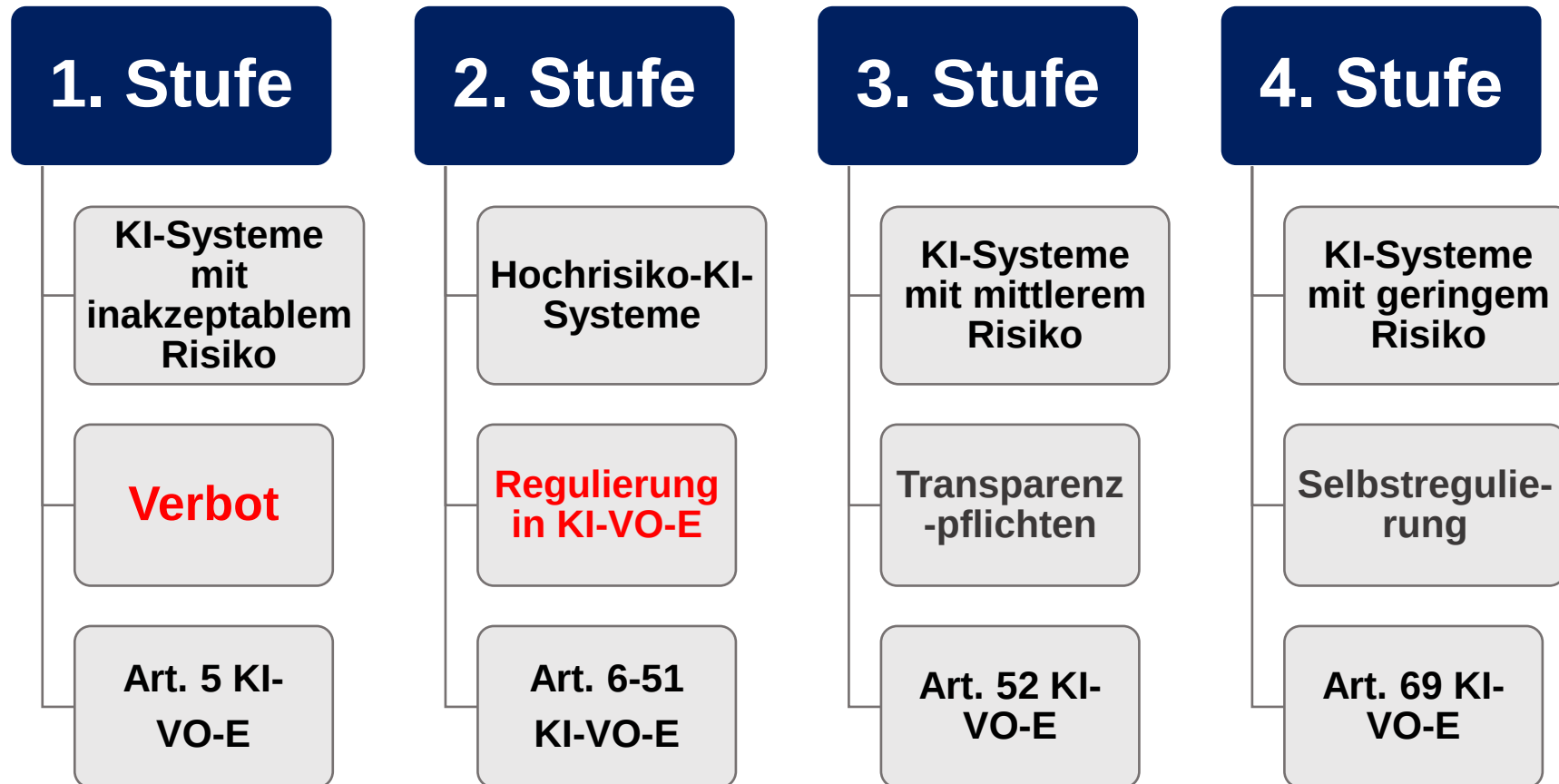
1. Rechtsrahmen – Update KI-VO-E

Änderung 1 - Ausweitung Anwendungsbereich

- **Kritik und Risiko für die Praxis:**
 - zu weit gefasst
- **Folge:**
 - erfasst sind auch technisch einfache Geräte – wie
 - normale Software
 - Smart-Home-Geräte (dazu unten Folie 19)

1. Rechtsrahmen - Update KI-VO-E

Änderung 2 – Ausweitung der Verbote – Anwendungsbereich aktuell



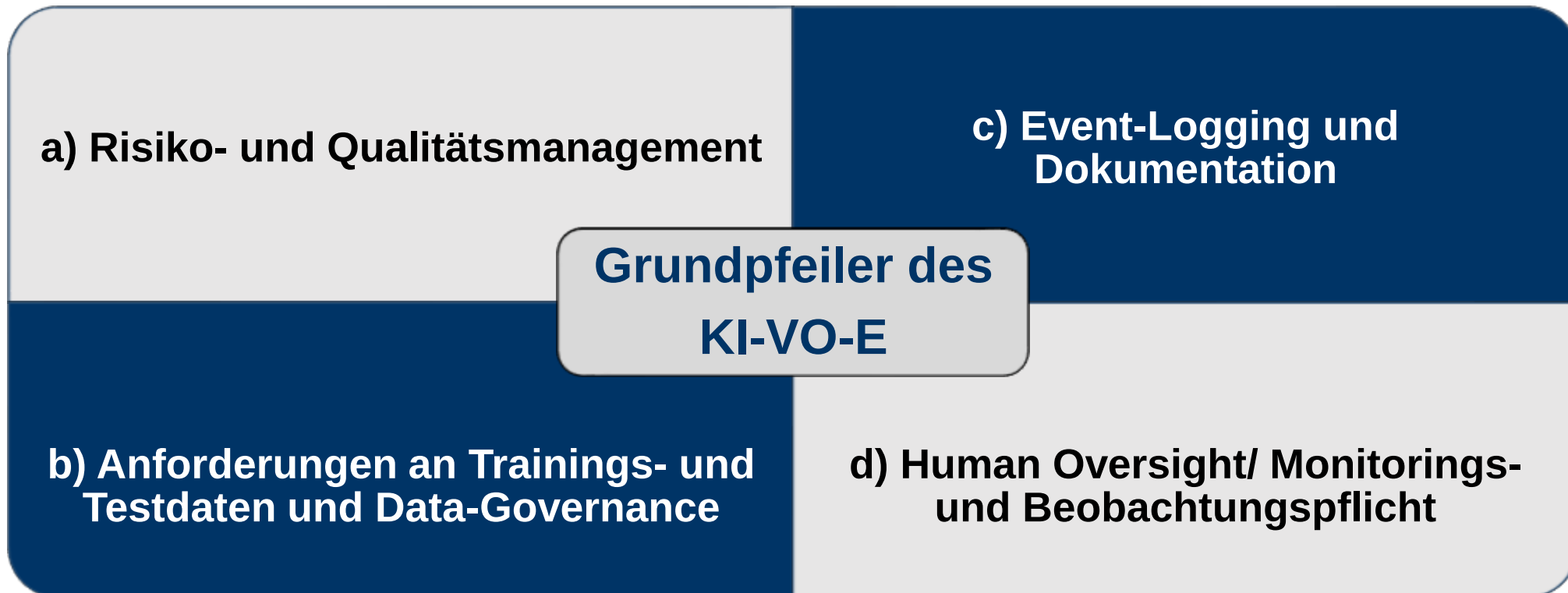
1. Rechtsrahmen – Update KI-VO-E

Änderung 2 – Ausweitung der Verbote – Parlamentsentwurf - Beispiele

Stufe	KI-System	Beispiel
1	Inakzeptables Risiko Verbot, Art. 5 KI-VO-E	• Predictive Policing • Risk Assessment Tools • Biometrische Kategorisierungssysteme • Gesichtserkennungsdatenbanken durch Scraping von Social Media/ Überwachungskameras (im öffentlichen Raum) • Emotionserkennungssysteme bei Strafverfolgung, Grenzmanagement, am Arbeitsplatz, in Bildungseinrichtungen • Biometrische Identifizierungssysteme
2	Hochrisiko-Systeme	• Empfehlungssysteme sehr großer Online-Plattformen (VLOPs) • KI-Systeme zur Beeinflussung von Wahlen/Wählerverhalten

1. Rechtsrahmen - Update KI-VO-E

Anforderungen Hochrisiko-Systeme



1. Rechtsrahmen – Update KI-VO-E

Änderung 3 – Änderungen bei Hochrisiko-Systemen, Art. 6 KI-VO-E

Einführung einer 2. Stufe der Risikobewertung:

- **Art. 6 Abs. 1 lit. b): für Produkte gemäß Anhang II**

Konformitätsbewertung durch Dritte *in Bezug auf die Risiken für Gesundheit und Sicherheit* im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieser Produkte;

- **Art. 6 Abs. 2: für Produkte gemäß Anhang III -**

Einstufung als hochriskant, (...) *wenn sie ein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte von natürlichen Personen darstellen.*

- **Art. 6 Abs. 2: für Produkte gemäß Anhang III Nr. 2 – Verwaltung / „kritische (digitale) Infrastrukturen“**

Einstufung als hochriskant, *wenn es ein erhebliches Risiko für die Umwelt bergen.*

- **Dazu 6 Monate vor Inkrafttreten der KI-VO Leitlinien der EU-Kommission zur Bestimmung dieser Risiken**

- **Art. 6 Abs. 2a) 2b): Pflicht der Anbieter zur Risiko-Einstufung ihrer KI-Systeme**

Anbieter, die ihr KI-System *fälschlicherweise als nicht den Anforderungen von Titel III Kapitel 2* dieser Verordnung *unterliegend einstufen* und es *vor Ablauf der Einspruchsfrist* der *nationalen Aufsichtsbehörden auf den Markt bringen*, werden gemäß Artikel 71 mit *Geldbußen* belegt.

1. Rechtsrahmen – Update KI-VO-E

Änderung 4 – Regelung von Basismodellen – Generative KI – lex ChatGPT & Co., Art. 28b KI-VO-E

Definition Basismodell, Art. 3 Abs. 1 Nr. 1lit. C) KI-VO-E

Ein Basismodell ist,

- ein *KI-Systemmodell*,
- das *auf* einer *breiten Datenbasis trainiert* wurde,
- *auf* eine *allgemeine Ausgabe ausgelegt* ist,
- *anpassbar an* eine *breite Palette unterschiedlicher Aufgaben*.

Bedeutung nach EG 60e:

- Wiederverwendung eines jeden Basismodells
- in unzähligen nachgelagerten KI-Systemen/ KI-Systemen mit allgemeinem Verwendungszweck

Folge:

- Wachsende Bedeutung für viele nachgelagerte Anwendungen und Systeme

1. Rechtsrahmen – Update KI-VO-E

Änderung 4 – Regelung von Basismodellen – Generative KI – lex ChatGPT & Co., Art. 28b KIVO-E

- **Besondere Pflichten für Anbieter eines Grundlagenmodells, Art. 28b Abs. 2 KI-VO-E**
- Einrichtung eines *Risikomanagementsystems*
 - zur Identifizierung/Verringerung/Abschwächung von vernünftigerweise vorhersehbaren Risiken für
 - Gesundheit/Sicherheit/Grundrechte/Umwelt/Demokratie/Rechtsstaatlichkeit
- Verwendung *geeigneter Datensätze*
- Etablierung von *Data-Governance-Maßnahmen* zur Prüfung von Verzerrungen (Bias)
- Sicherstellung eines *angemessenen Niveaus* an
 - *Leistung/Vorhersagbarkeit/Interpretierbarkeit/Korrigierbarkeit/Sicherheit und Cybersicherheit*
 - durch Modellevaluierung
- Vergleichbar den 4 Grundpfeilern für Hochrisiko-Systeme (Folie 9)

1. Rechtsrahmen – Update KI-VO-E

Änderung 4 – Regelung von Basismodellen – Generative KI – lex ChatGPT & Co., Art. 28b KIVO-E

- **Besondere Pflichten für Anbieter „generativer KI“, Art. 28b Abs. 4 KI-VO-E,**
 - KI-Systeme zur Generierung von komplexen Texten/Bildern/Audio- oder Videodateien („ChatGPT“)
 - sowie zur Integration von Basismodellen in ein generatives KI-System
- sind
- *Transparenzpflichten* nach Art. 52 Abs. 1 KI-VO-E
 - Etablierung *angemessener Schutzmaßnahmen* nach allgemein anerkanntem Stand der Technik *gegen*
 - Erzeugung von *Inhalten, die*
 - *gegen EU-Recht verstoßen,*
 - jedoch *ohne Beeinträchtigung von Grundrechten* wie der Meinungsfreiheit
 - Öffentlich zugängliche zusammenfassende *Dokumentation* der Verwendung von *urheberrechtlich geschützten Trainingsdaten*

2. Rechtsrahmen – Update Data Act



AGENDA

2. Rechtsrahmen – Update Data Act

Norm:

- Entwurf KOM(2022) 68 final vom 23.02.2022 für eine Verordnung über harmonisierte Vorschriften für ein Datengesetz

Aktueller Stand:

- Kompromiss zwischen Rat der EU und Parlament vom 07.07.2023
- Konsolidierung des Gesetzestextes

Anwendungspflicht:

- Nach 20 (statt bisher 12) Monaten ab Inkrafttreten

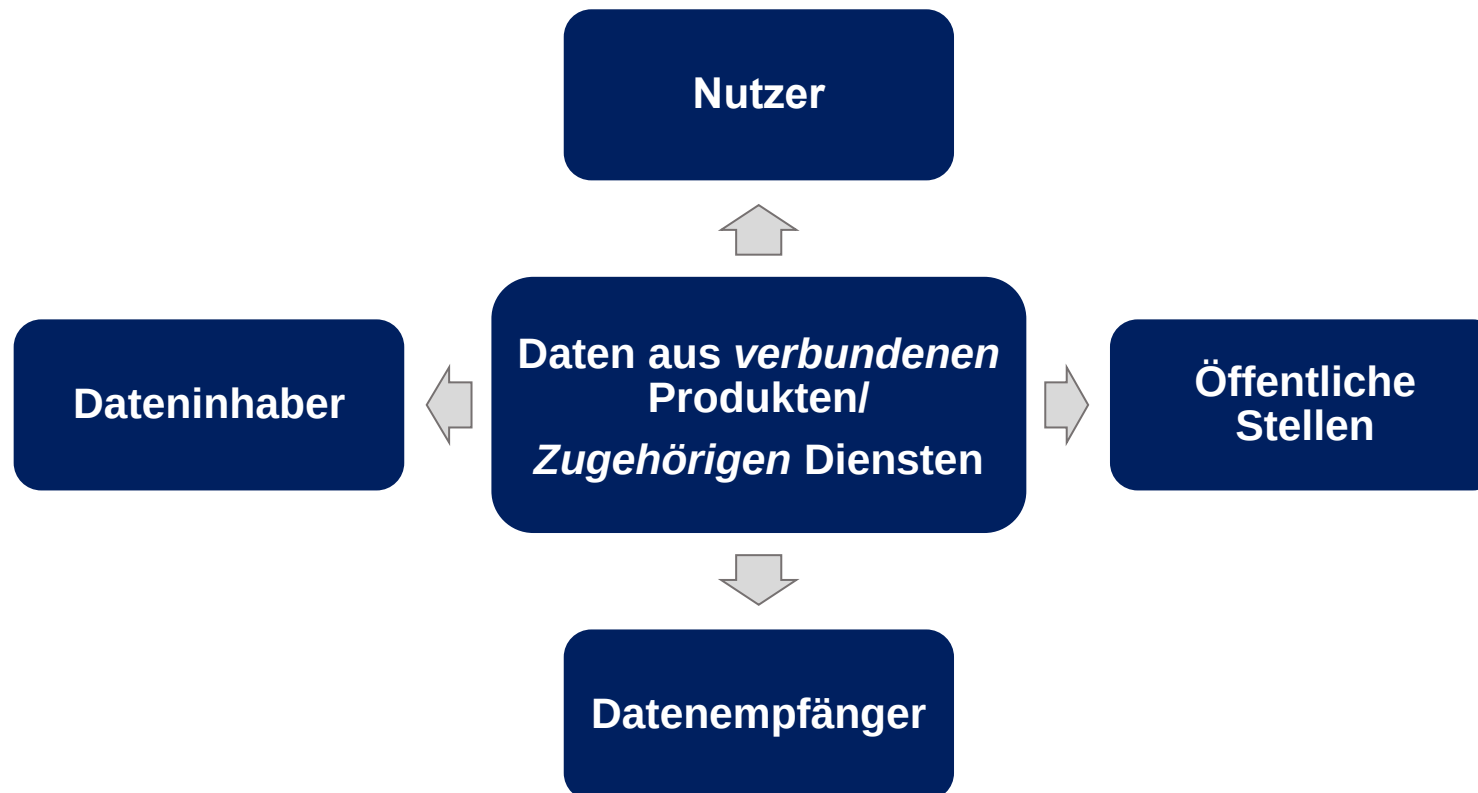
2. Rechtsrahmen – Update Data Act

Wesentliche Änderungen:

- Schärfung der Definitionen der relevanten Daten und Beteiligten/Adressaten
- Unterscheidung zwischen „Produktdaten“ und „Daten der verbundenen Services“
- Stärkung des Schutzes der Geschäftsgeheimnisse
- Beschränkung des Teilens von Daten mit öffentlicher Hand auf Notfälle
- Einführung einer vertraglichen Beschränkung des Zugangs, der Verwendung oder des weiteren Teilens von Daten bei möglichen ernststen nachteiligen Auswirkungen
- Schärfung der Regelungen zur Datenportabilität und Verbot der Implementierung von Hindernissen zur Entflechtung der Daten

2. Rechtsrahmen – Update Data Act

Gegenstand, Art. 1 Abs. 1 Data Act – zentraler Begriff:



2. Rechtsrahmen – Update Data

Gegenstand, Art. 1 Abs. 1 Data Act – Definitionen

Verbundene Produkte, Art. 2 Abs. 2 Data Act

- Gegenstand,
- der Daten über seine Nutzung/ Umgebung
- erhält, erzeugt oder sammelt und
- *Produktdaten über einen elektronischen Kommunikationsdienst/ physische Verbindung oder einen geräteinternen Zugang übermitteln kann*

Zugehörige Dienste, Art. 2 Nr. 2 Data Act

- Anderer digitaler Dienst als elektronische Kommunikationsdienste, einschließlich Software,
- der zum Zeitpunkt des Kaufs so mit Produkt verbunden ist, dass
- dieses ohne diesen Dienst eine/mehrerer seiner Funktionen nicht ausführen könnte
- *oder der später vom Hersteller/ einem Dritten mit dem Produkt verbunden wird, um die Funktionen des Produkts zu ergänzen, zu aktualisieren oder anzupassen.*

2. Rechtsrahmen – Update Data Act

Gegenstand, Art. 1 Data Act – Beispiele für Produkte/verbundene Dienste

Verbundene Produkte

- Alle **smarten Geräte**, die Sensoren und Chips enthalten – **IoT-Devices**:
- Waschmaschinen, Autos, Kleidungsstücke
- Aufzüge
- Mähdrescher
- Roboter
- Fertigungsanlagen

Zugehörige Dienste

- **Virtuelle Assistenten**, die smarte Produkte steuern, Art. 7 Abs. 2 Data Act (**IoT-Devices**), wie
- Smart-Home-Geräte
- Smart Cars

2. Rechtsrahmen – Update Data Act

Kernregelungen des Data Act:

- Zugang zu Daten/**Metadaten** für Nutzer durch **Access-by-Design**, Art. 3 Data Act
- **Hilfsweise Anspruch des Nutzers auf Zugang zu Daten/**Metadaten** auf Verlangen** durch technische Bereitstellung, Art. 4 Abs. 1 Data Act
- **Wichtig: Die Anforderungen der DSGVO gelten daneben, Art. 4 Abs. 5 Data Act**
- **Zugang zu Daten für Dateninhaber:**
Datenlizenzvertrag Dateninhaber/Nutzer zur Nutzung und damit wirtschaftlichen Verwertung durch den Dateninhaber selbst

2. Rechtsrahmen – Update Data Act

Kernregelungen des Data Act:

- **Datenzugang für Dritte** auf *Verlangen des Nutzers*, Art. 5 Abs. 1 Data Act,
- Grundlage: **Datenlizenzvertrag Nutzer/Dritter**, Art. 6 Abs. 1 Data Act
- **Einschränkungen der Nutzung durch Dritten:**
 - **Kein Profiling**, Art. 6 Abs. 2 lit. b) Data Act
 - **Ausweitung des Schutzes von Geschäftsgeheimnissen** des Dateninhabers, **Art. 5 Abs. 8-8c)** Data Act
 - strenge **Zweckbindung** durch Datenlizenzvertrag, Art. 6 Abs. 1 Data Act
 - **Beschränkungen** der **Weitergabe** an andere, Art. 6 Abs. 2 lit. c) Data Act
 - **Keine Weitergabe an Gatekeeper**, Art. 6 Abs. 2 lit. d) Data Act
 - **Keine** Entwicklung eines **Wettbewerbsproduktes**, Art. 6 Abs. 2 lit. e) Data Act
- **Wichtig:** DSGVO gilt daneben, Art. 5 Abs. 7 Data Act

3. Bedeutung für ChatGPT und KI-Anwendungen - Fazit



AGENDA

3. Bedeutung für ChatGPT und KI-Anwendungen - Fazit

1. Der Anwendungsbereich des KI-VO-E ist durch die Erweiterung des Begriffs „KI-System“ in Art. 3 Nr. 1 KI-VO-E nochmals ausgeweitet worden. Deshalb ist in der Praxis noch genauer zu prüfen, ob eine Anwendung in den Bereich der KI-VO-E fällt. Dies gilt namentlich bei Software- und smarten Anwendungen.
2. Bei der Prüfung, ob ein KI-System ein Hochrisiko-System darstellt, ist zusätzlich auf einer weiteren Stufe je nach Einsatzzweck und Anwendungsbereich zu prüfen, ob besondere Risiken für die Gesundheit, die Sicherheit, die Grundrechte oder die Umwelt bestehen und sind diese Risiko-Einschätzungen von Betreibern kritischer Infrastrukturen an die zuständigen Aufsichtsbehörden zu melden.
3. Für die Praxis besonders relevant ist die neu eingeführte Regelung für Basismodelle und Generative KI, wie ChatGPT. Diese werden zwar nicht als Hochrisiko-System eingestuft, dennoch haben deren Anbieter Pflichten, die denjenigen eines Hochrisiko-Systems vergleichbar sind.

3. Bedeutung für ChatGPT und KI-Anwendungen - Fazit

4. Hohe Anforderungen werden zudem an generative KI, wie ChatGPT gestellt, da diese Systeme sicherstellen müssen, dass rechtswidrige Inhalte vermieden werden, ohne gleichzeitig die Meinungsfreiheit zu beeinträchtigen, ein schwieriger Spagat, der im Ergebnis die Implementierung einer Grundrechtsabwägung in der Entwicklung und der Nutzung von generativer KI bedeutet.
5. Zu begrüßen ist die Kennzeichnungspflicht nach Art. 52 Abs. 1 KI-VO-E, um Täuschungen über den Urheber von Texten, Bildern, Audio- oder Videodateien zu verhindern, wenngleich die Grenzen, ab wann diese Transparenzpflicht greift, in der Praxis noch zu bestimmen sein wird.

3. Bedeutung für ChatGPT und KI-Anwendungen - Fazit

6. Die Anforderungen des Data Act wurden in wesentlichen Bereichen in den Definitionen und im Schutz von Geschäftsgeheimnissen geschärft.
7. Vom Grundsatz verbleibt es dabei, dass die Nutzung dieser Daten durch Dateninhaber, Hersteller, Nutzer, oder (dritte) Datenempfänger auf einer Kombination von technischen Anforderungen an die Produkte – Access-by-Design – und vertraglichen Regelungen – Datenlizenzverträgen – zwischen den Beteiligten basiert.
8. Durch die Ausweitung des Anwendungsbereiches der KI-VO-E könnten künftig jedoch verstärkt und einfacher smarte und IoT-Anwendungen sowohl in den Anwendungsbereich des Data Act als auch der KI-VO-E fallen, sodass sowohl der Anwendungsbereich des Data Act als auch der KI-VO-E zu beachten ist und diejenigen der DSGVO.

3. Bedeutung für ChatGPT und KI-Anwendungen - Fazit

9. Dementsprechend ist in der Praxis zur Bestimmung des Rechtsrahmen zu prüfen,
- ob es sich um ein KI-System im Sinne des KI-VO-E handelt,
 - ob es sich bei der smarten Anwendung um ein KI-System im Sinne von Art. 3 Nr. 1 KI-VO-E handelt,
 - wenn dem so ist, unter welche Kategorie sie einzuordnen ist,
 - welche Anforderungen der KI-VO-E greifen,
 - Insbesondere ob es sich um ein Basismodell handelt,
 - ob Daten verwendet werden sollen, die mit verbundenen Produkten oder zugehörigen Diensten erzeugt wurden,
 - um die Nutzung der Anwendung selbst und der mit ihr erzeugten Daten rechtssicher zu gestalten.

Ihre Ansprechpartnerin



Dr. Christiane Bierekoven

Rechtsanwältin / Fachanwältin für IT-Recht

Dr. Ganteführer, Marquardt & Partner

Poststraße 1-3

40213 Düsseldorf

Bierekoven@gamapa.de

0211 / 8989-270