



ATLANTIC Hotel Kiel

08.09.2025

Update Risiko: Von der DSGVO zu DSA & AI Act

***Was sich mit der Digitale-Dienste-Verordnung
und der KI-Verordnung ändert***

Dr. Felix Bieker (ULD)

Recap: Risiko in der DSGVO

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der **Risiken für die Rechte und Freiheiten natürlicher Personen** geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Risiko in der DSGVO

Artikel 1

Gegenstand und Ziele

- (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

- (75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

- (75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer
- (94) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung bei Fehlen von Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen würde, und ist der Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann, so sollte die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeiten konsultiert werden. Ein solches hohes Risiko ist wahrscheinlich mit bestimmten Arten der Verarbeitung und dem Umfang und der Häufigkeit der Verarbeitung verbunden, die für natürliche Personen auch eine Schädigung oder eine Beeinträchtigung der persönlichen Rechte und Freiheiten mit sich bringen können. Die Aufsichtsbehörde sollte das Beratungsgesuch innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende Verarbeitung personenbezogener Daten durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die Rechte und Freiheiten natürlicher Personen geplanten Maßnahmen.

Risikobewertung

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

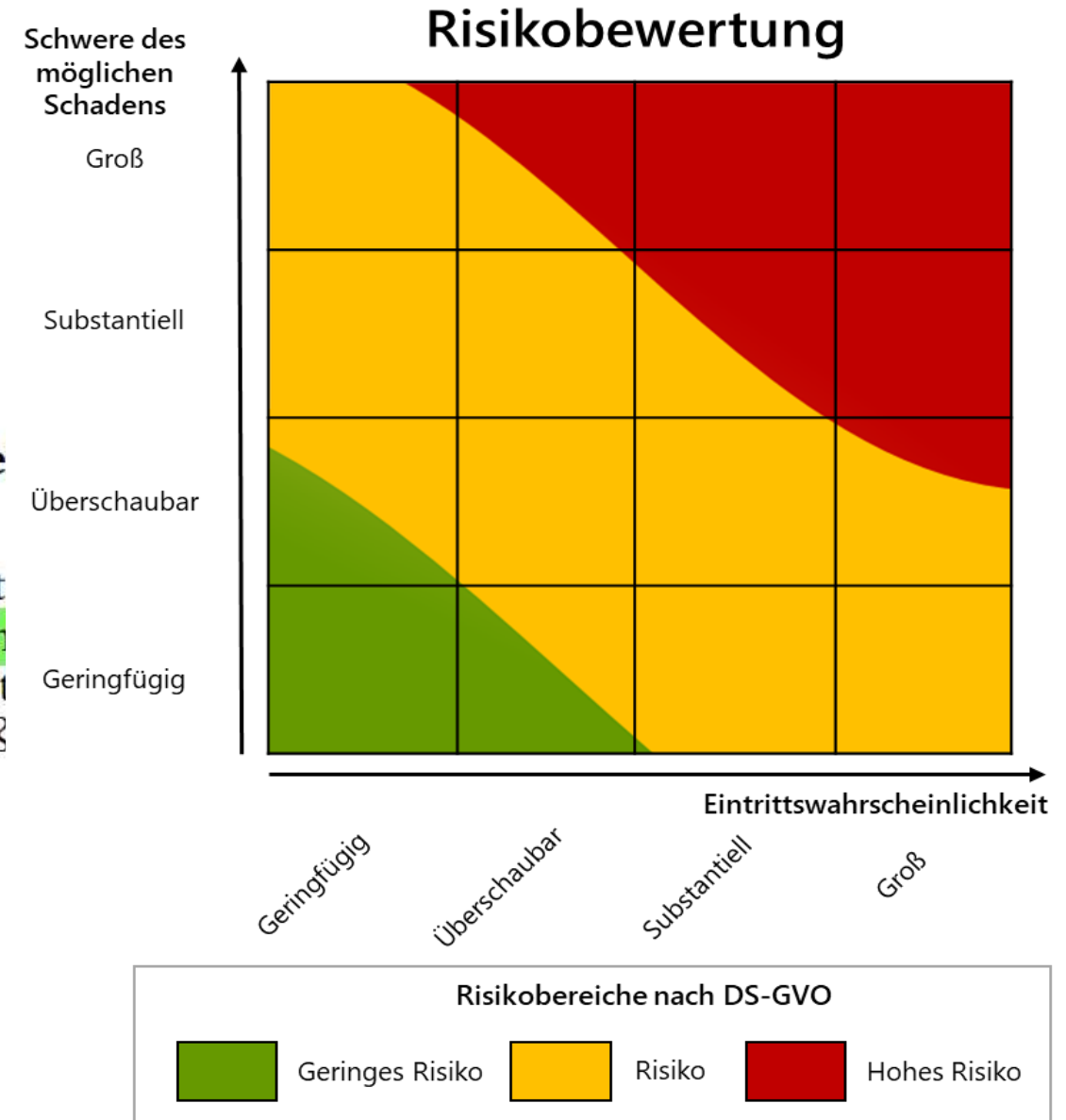
(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Risikobewertung

Artikel 24

Verantwortung des für die Verarbe

(1) Der Verantwortliche setzt unter Berücksichtigung der Art Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlich Freiheiten natürlicher Personen geeignete technische und organisat Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß erforderlichenfalls überprüft und aktualisiert.





DECEIVED BY DESIGN

How tech companies use dark patterns to discourage us from exercising our rights to privacy.

27.05.2018

Information Commissioner's Office

Democracy disrupted?

Personal information and political influence

11 July 2018

ico.
Information Commissioner's Office



HUMAN
RIGHTS
WATCH

"All This Terror Because of a Photo"

Digital Targeting and its Offense Consequences for LGBT People in the Middle East and North Africa



THE SOCIAL ATROCITY

META AND THE RIGHT TO REMEDY FOR THE ROHINGYA

SEXISM IS A FEATURE, NOT A BUG

Mar Hicks



CODED INJUSTICE

SURVEILLANCE AND DISCRIMINATION IN DENMARK'S
AUTOMATED WELFARE STATE



HUMANS ARE BIASED. GENERATIVE AI IS EVEN WORSE

Stable Diffusion's text-to-image model amplifies stereotypes
about race and gender – here's why that matters

By [Leonardo Nicoletti](#) and [Dina Bass](#) for [Bloomberg Technology](#) + Equality

Multimodal datasets: misogyny, pornography, and malignant stereotypes

Abeba Birhane*
University College Dublin & Lero
Dublin, Ireland
abeba.birhane@ucdconnect.ie

Vinay Uday Prabhu*
Independent Researcher
vinaypra@alumni.cmu.edu

Emmanuel Kahembwe
University of Edinburgh
Edinburgh, UK
e.kahembwe@ed.ac.uk

Abstract



Open access



Research article

First published online August 2, 2021

Digital welfare fraud detection and the Dutch *SyRI* judgment

[Marvin van Bakkum](#) and [Frederik Zuiderveen Borgesius](#)   [View all authors and affiliations](#)

[Volume 23, Issue 4](#)

<https://doi.org/10.1177/13882627211031257>

More than a Glitch

< Confronting Race, >
< Gender, >
< and Ability Bias >
< in Tech >

Meredith Broussard

S700.000 Liter Wasser für das Training von GPT-3 – laut Studie

KI-Modelle benötigen nicht nur viel Strom, sondern auch viel Wasser. Eine neue Studie will zeigen, wie "durstig" ChatGPT und Googles LaMDA wirklich sind.

59



20.04.2023, 11:20 Uhr Lesezeit: 3 Min. | MIT Technology Review

Stable

about race and gender – here's why that matters

By Leonardo Nicoletti and Dina Bass for Bloomberg Technology + Equality

OT A

datasets: mi
malignant

a Birhane*
ege Dublin & Lero
n, Ireland
e@ucdconnect.ie

Emmanue
University
Edinbu
e.kahembu

Abs

tered the era of trillion p
atasets scraped from
n rise to formidable b
erating these large dat
ion practices used to g
available on the world
ataset often used as a

trenched biases in large-scale
del) trained on opaque datase
ific calls of caution, we exar

GESELLSCHAFT
FÜR INFORMATIK



FORSCHUNGSBERICHT

AUSWIRKUNGEN VON KI, RECHENZENTREN
UND HALBLEITERN AUF
WASSERVERFÜGBARKEIT UND -QUALITÄT

JUNI 2025

WWW.GI.DE

e
n a
ch
ng Race, >
y Bias >
oussard

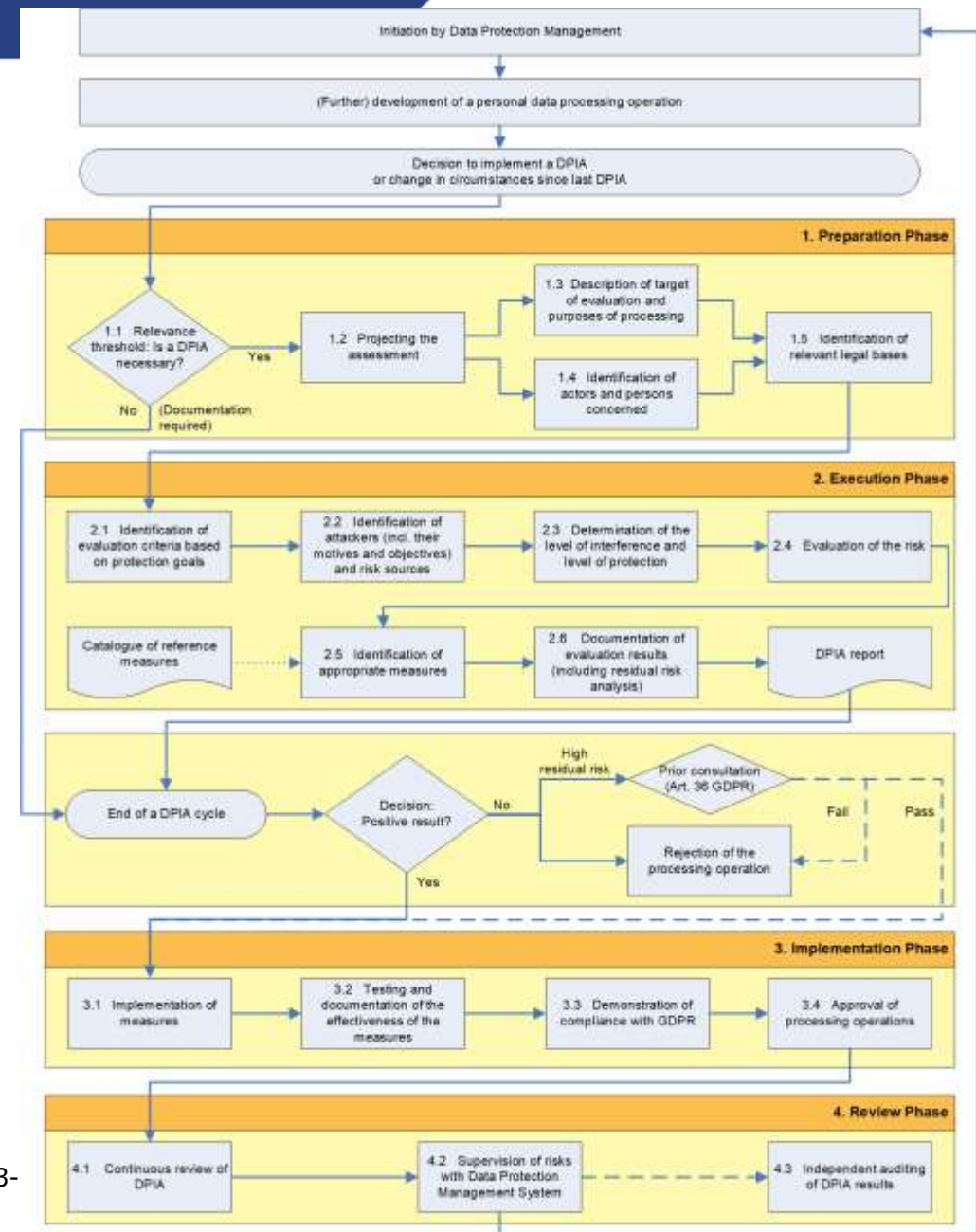
Eindämmung von Risiken in der DSGVO

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Anleitung für eine DSFA



Risiko in der DDVO

Artikel 34

Risikobewertung

(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen ermitteln, analysieren und bewerten sorgfältig alle systemischen Risiken in der Union, die sich aus der Konzeption oder dem Betrieb ihrer Dienste und seinen damit verbundenen Systemen, einschließlich algorithmischer Systeme, oder der Nutzung ihrer Dienste ergeben.

Risiko in der DDVO

lichkeit und umfasst die folgenden systemischen Risiken:

- a) Verbreitung rechtswidriger Inhalte über ihre Dienste;
- b) etwaige tatsächliche oder vorhersehbare **nachteilige Auswirkungen auf die Ausübung der Grundrechte**, insbesondere des in Artikel 1 der Charta verankerten Grundrechts auf Achtung der Menschenwürde, des in Artikel 7 der Charta verankerten Grundrechts auf Achtung des Privat- und Familienlebens, des in Artikel 8 der Charta verankerten Grundrechts auf Schutz personenbezogener Daten, des in Artikel 11 der Charta verankerten Grundrechts auf die Meinungs- und Informationsfreiheit, einschließlich Medienfreiheit und -pluralismus auf das in Artikel 21 der Charta verankerte Grundrecht auf Nichtdiskriminierung, die in Artikel 24 der Charta verankerten Rechte des Kindes und den in Artikel 38 der Charta verankerten umfangreichen Verbraucherschutz;
- c) alle tatsächlichen oder absehbaren nachteiligen Auswirkungen auf die **gesellschaftliche Debatte und auf Wahlprozesse** und die **öffentliche Sicherheit**;
- d) alle tatsächlichen oder absehbaren nachteiligen Auswirkungen in Bezug auf **geschlechtsspezifische Gewalt**, den **Schutz der öffentlichen Gesundheit** und von **Minderjährigen** sowie schwerwiegende nachteilige Folgen für das körperliche und geistige Wohlbefinden einer Person.

Risikobewertung und -minderung in der DDVO

Artikel 34

Risikobewertung

(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen ermitteln, bewerten sorgfältig alle systemischen Risiken in der Union, die sich aus der Konzeption oder dem Betrieb ihrer Dienste und der damit verbundenen Systemen, einschließlich algorithmischer Systeme, oder der Nutzung ihrer Dienste ergeben.

Artikel 35

Risikominderung

(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen ergreifen angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen, die auf die gemäß Artikel 34 ermittelten besonderen systemischen Risiken zugeschnitten sind, wobei die **Auswirkungen solcher Maßnahmen auf die Grundrechte** besonders zu berücksichtigen sind. Hierzu können unter Umständen gehören:

Risikobewertung und -minderung in der DDVO

Artikel 34

Risikobewertung

(1) Die Anbieter sehr großer Online-Plattformen und sehr große bewerten sorgfältig alle systemischen Risiken in der Union, die sich aus seinen damit verbundenen Systemen, einschließlich algorithmischer S

Artikel 35

Risikominderung

(1) Die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschi verhältnismäßige und wirksame Risikominderungsmaßnahmen, die auf die gemäß Artikel systemischen Risiken zugeschnitten sind, wobei die Auswirkungen solcher Maßnahmen auf die berücksichtigen sind. Hierzu können unter Umständen gehören:

Very Large Online Platforms:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

Very Large Online Search Engines:

- Bing
- Google Search

Risiko in der KIVO

- a) die Ermittlung und Analyse der bekannten und vernünftigerweise vorhersehbaren Risiken, die vom Hochrisiko-KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können, wenn es entsprechend seiner Zweckbestimmung verwendet wird;

vervielfältigen, oder der „Selbstreplikation“ oder des Trainings anderer Modelle; der Art und Weise, wie Modelle zu schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften führen können; der Erleichterung von Desinformation oder der Verletzung der Privatsphäre mit Gefahren für demokratische Werte und Menschenrechte; dem Risiko, dass ein bestimmtes Ereignis zu einer Kettenreaktion mit

Risiko in der KIVO

- a) die Ermittlung und Analyse der bekannten und vernünftigerweise vorhersehbaren Risiken, die vom Hochrisiko-KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können, wenn es entsprechend seiner Zweckbestimmung verwendet wird;

vervielfältigen, oder der „Selbstreplikation“ oder des Trainings anderer Modelle; der Art und Weise, wie Modelle zu schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften führen können; der Erleichterung von Desinformation oder der Verletzung der Privatsphäre mit Gefahren für

65. „systemisches Risiko“ ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können;

oder sehr großer Online-Suchmaschinen, systemische Risiken zu ermitteln und zu mindern, die aus der Verbreitung von künstlich erzeugten oder manipulierten Inhalten entstehen können, insbesondere das Risiko tatsächlicher oder vorhersehbarer negativer Auswirkungen auf demokratische Prozesse, den gesellschaftlichen Diskurs und Wahlprozesse, unter anderem durch Desinformation.

Risiko in der KIVO

- a) die Ermittlung des Risikos, dass ein KI-System für den vorgesehenen Zweckbestimmung und gewährleisten sollen, dass nur sichere und anderweitig konforme Produkte auf den Markt gelangen, ist es wichtig, dass die **Sicherheitsrisiken**, die ein Produkt als Ganzes aufgrund seiner digitalen Komponenten, einschließlich KI-Systeme, mit sich bringen kann, angemessen vermieden und gemindert werden. So sollten beispielsweise zunehmend autonome Roboter, sei es in der Fertigung oder in der persönlichen Assistenz und

vervielfältigen, oder der „Selbstreplikation“ oder des Trainings anderer Modelle; der Art und Weise, wie Modelle zu **schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften** führen können; der Erleichterung von Desinformation oder der Verletzung der Privatsphäre mit Gefahren für

65. **„systemisches Risiko“** ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können;

oder sehr großer Online-Suchmaschinen, systemische Risiken zu ermitteln und zu mindern, die aus der Verbreitung von künstlich erzeugten oder manipulierten Inhalten entstehen können, insbesondere das **Risiko tatsächlicher oder vorhersehbarer negativer Auswirkungen auf demokratische Prozesse, den gesellschaftlichen Diskurs und**

Wahrheitsklärung oder in Teilen davon nachgewiesen wird. Zu diesem Zweck sollten bei der im Rahmen einer Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen durchgeführten Bewertung der **Cybersicherheitsrisiken**, die mit einem gemäß der vorliegenden Verordnung als Hochrisiko-KI-System eingestuften Produkt mit digitalen Elementen verbunden sind, Risiken für die Cyberabwehrfähigkeit eines KI-Systems in Bezug auf Versuche unbefugter Dritter, seine Verwendung, sein Verhalten oder seine Leistung zu verändern, einschließlich KI-spezifischer Schwachstellen wie Datenvergiftung

Risiko in der KIVO

- a) die Ermittlung des Risikostadiums für das System für den vorgesehenen Zweckbestimmung und gewährleisten sollen, dass nur sichere und anderweitig konforme Produkte auf den Markt gelangen, ist es wichtig, dass die **Sicherheitsrisiken**, die ein Produkt als Ganzes aufgrund seiner digitalen Komponenten, einschließlich KI-Systeme, mit sich bringen kann, angemessen vermieden und gemindert werden. So sollten beispielsweise zunehmend autonome Roboter, sei es in der Fertigung oder in der persönlichen Assistenz und

- (125) Angesichts der Komplexität von **Hochrisiko-KI-Systemen und der damit verbundenen Risiken** ist es wichtig, ein angemessenes Konformitätsbewertungsverfahren für Hochrisiko-KI-Systeme, an denen notifizierte Stellen beteiligt
65. **„systemisches Risiko“** ein Risiko, das für die Fähigkeiten mit höher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können;

oder sehr großer Online-Suchmaschinen, systemische Risiken zu ermitteln und zu mindern, die aus der Verbreitung von künstlich erzeugten oder manipulierten Inhalten entstehen können, insbesondere das **Risiko tatsächlicher oder vorhersehbarer negativer Auswirkungen auf demokratische Prozesse, den gesellschaftlichen Diskurs und**

Wahrheitsklärung oder in Teilen davon nachgewiesen wird. Zu diesem Zweck sollten bei der im Rahmen einer Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen durchgeführten Bewertung der **Cybersicherheitsrisiken**, die mit einem gemäß der vorliegenden Verordnung als Hochrisiko-KI-System eingestuften Produkt mit digitalen Elementen verbunden sind, Risiken für die Cyberabwehrfähigkeit eines KI-Systems in Bezug auf Versuche unbefugter Dritter, seine Verwendung, sein Verhalten oder seine Leistung zu verändern, einschließlich KI-spezifischer Schwachstellen wie Datenvergiftung

Risiko in der KIVO

a) die Ermittlung System für d Zweckbestimm	und gewährleisten sollen, dass nur sichere und anderweitig konforme Produkte auf den Markt gelangen, ist es wichtig, dass die Sicherheitsrisiken, die ein Produkt als Ganzes aufgrund seiner digitalen Komponenten, einschließlich KI-Systeme, mit sich bringen kann, angemessen vermieden und gemindert werden. So sollten beispielsweise zunehmend autonome Roboter, sei es in der Fertigung oder in der persönlichen Assistenz und
	dem Inverkehrbringen sollte nicht für sensible operative Daten von Betreibern, die Strafverfolgungsbehörden sind, gelten. Dieses System ist auch wichtig, damit den möglichen Risiken, die von KI-Systemen ausgehen, die nach dem Inverkehrbringen oder der Inbetriebnahme dazulernen, effizienter und zeitnah begegnet werden kann. In diesem Zusammenhang sollten die Anbieter auch verpflichtet sein, ein System einzurichten, um den zuständigen Behörden
	vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem
	den Auswirkungen der Interaktion und des Einsatzes von Instrumenten, einschließlich zum Beispiel der Fähigkeit, physische Systeme zu steuern und in kritische Infrastrukturen einzugreifen; Risiken, dass Modelle sich selbst vervielfältigen, oder der „Selbstreplikation“ oder des Trainings anderer Modelle; der Art und Weise, wie Modelle zu schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften
	Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen durchgeführten Bewertung der Cybersicherheitsrisiken, die mit einem gemäß der vorliegenden Verordnung als Hochrisiko-KI-System eingestuften Produkt mit digitalen Elementen verbunden sind, Risiken für die Cyberabwehrfähigkeit eines KI-Systems in Bezug auf Versuche unbefugter Dritter, seine Verwendung, sein Verhalten oder seine Leistung zu verändern, einschließlich KI-spezifischer Schwachstellen wie Datenvergiftung

Risiko in der KIVO

a) die Ermittlung und gewährleisten sollen, dass nur sichere und anderweitig konforme Produkte auf den Markt gelangen, ist es wichtig, dass die **Sicherheitsrisiken**, die ein Produkt einschließlich KI-Systeme, mit sich bringen, gemindert werden. So sollten

dem Inverkehrbringen gelten. Diese **Inverkehrbringen** Zusammenhänge

vorhersehbar Grundrechte

den Auswirkungen physische Systeme **vervielfältigen**, schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften

AI Anxiety

Behörden sind, **gehen, die nach dem** In diesem zuständigen Behörden

Sicherheit, die

Elementen, einschließlich zum Beispiel der Fähigkeit, Infrastrukturen einzugreifen; **Risiken, dass Modelle sich selbst** oder des Trainings anderer Modelle; der Art und Weise, wie Modelle zu **schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften**

Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen durchgeführten Bewertung der **Cybersicherheitsrisiken**, die mit einem gemäß der vorliegenden Verordnung als Hochrisiko-KI-System eingestuften Produkt mit digitalen Elementen verbunden sind, Risiken für die Cyberabwehrfähigkeit eines KI-Systems in Bezug auf Versuche unbefugter Dritter, seine Verwendung, sein Verhalten oder seine Leistung zu verändern, einschließlich KI-spezifischer Schwachstellen wie Datenvergiftung

Risikobewertung in der KIVO

Artikel 27

Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme

(1) Vor der Inbetriebnahme eines Hochrisiko-KI-Systems gemäß Artikel 6 Absatz 2 — mit Ausnahme von Hochrisiko-KI-Systemen, die in dem in Anhang III Nummer 2 aufgeführten Bereich verwendet werden sollen — führen Betreiber, bei denen es sich um Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen, handelt, und Betreiber von Hochrisiko-KI-Systemen gemäß Anhang III Nummer 5 Buchstaben b und c eine Abschätzung der Auswirkungen, die die Verwendung eines solchen Systems auf die Grundrechte haben kann, durch. Zu diesem Zweck führen die Betreiber eine Abschätzung durch, die Folgendes umfasst:

- a) eine Beschreibung der Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird;
- b) eine Beschreibung des Zeitraums und der Häufigkeit, innerhalb dessen bzw. mit der jedes Hochrisiko-KI-System verwendet werden soll;
- c) die Kategorien der natürlichen Personen und Personengruppen, die von seiner Verwendung im spezifischen Kontext betroffen sein könnten;
- d) die **spezifischen Schadensrisiken**, die sich auf die gemäß Buchstabe c dieses Absatzes ermittelten Kategorien natürlicher Personen oder Personengruppen auswirken könnten, unter Berücksichtigung der vom Anbieter gemäß Artikel 13 bereitgestellten Informationen;
- e) eine Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht entsprechend den Betriebsanleitungen;
- f) die **Maßnahmen, die im Falle des Eintretens dieser Risiken** zu ergreifen sind, einschließlich der Regelungen für die interne Unternehmensführung und Beschwerdemechanismen.

Risikobewertung in der KIVO

- d) die **spezifischen Schadensrisiken**, die sich auf die gemäß Buchstabe c dieses Absatzes ermittelten Kategorien natürlicher Personen oder Personengruppen auswirken könnten, unter Berücksichtigung der vom Anbieter gemäß Artikel 13 bereitgestellten Informationen;
- e) eine Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht entsprechend den Betriebsanleitungen;
- f) die **Maßnahmen, die im Falle des Eintretens dieser Risiken** zu ergreifen sind, einschließlich der Regelungen für die interne Unternehmensführung und Beschwerdemechanismen.

Artikel 9

Risikomanagementsystem

- (1) Für **Hochrisiko-KI-Systeme** wird ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrechterhalten.
- (2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess, der während des gesamten Lebenszyklus eines Hochrisiko-KI-Systems geplant und durchgeführt wird und eine regelmäßige systematische Überprüfung und Aktualisierung erfordert. Es umfasst folgende Schritte:
 - a) die Ermittlung und Analyse der bekannten und vernünftigerweise vorhersehbaren Risiken, die vom Hochrisiko-KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können, wenn es entsprechend seiner Zweckbestimmung verwendet wird;
 - b) die Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;
 - c) die Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 72 genannten System zur Beobachtung nach dem Inverkehrbringen;
 - d) die Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen zur Bewältigung der gemäß Buchstabe a ermittelten Risiken.

- GRFA (Art. 27 KIVO):

4. „Betreiber“ 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;
 - Aber nur, wenn Einrichtung des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringt

- Risiko-Management-System (Art. 9 KIVO):

3. „Anbieter“ 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;

Hohes Risiko nach Art. 6 und Anhängen I und III KIVO:

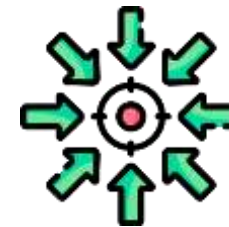
- Fällt unter EU-Sicherheitsregulierung
- Verwendet Biometrie
- Betrifft:
 - Kritische Infrastruktur (aber Ausnahme für GRFA)
 - Allgemeine und berufliche Bildung
 - Beschäftigung und Personalmanagement
 - Grundlegende private und öffentliche Dienste und Leistungen
 - Strafverfolgung
 - Migration, Asyl, Grenzkontrolle
 - Rechtspflege und demokratische Prozesse

Risikobewertung in der KIVO

(4) Wird eine der in diesem Artikel festgelegten Pflichten bereits infolge einer gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 durchgeführten **Datenschutz-Folgenabschätzung** erfüllt, so ergänzt die Grundrechte-Folgenabschätzung gemäß Absatz 1 des vorliegenden Artikels diese Datenschutz-Folgenabschätzung.

Fazit

- Zahlreiche Einschränkungen und Ausnahmen bei DDVO und KIVO
- Überblick über Risiken erforderlich, weiter Risikobegriff
- Bekannte Risiken vermeiden
- Informationen von Anbietern und Herstellern einfordern



Danke für Ihre Aufmerksamkeit!

Fragen?

Dr. Felix Bieker
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
ULD63@datenschutzzentrum.de



Plattform
Privatheit