

AI and Data Protection – Challenges for Controllers, Processors and Supervisory Authorities

Dr. h.c. Marit Hansen

State Data Protection Commissioner
of Schleswig-Holstein, Germany

IFIP Summer School on Privacy and Identity Management
Oslo, 11 August 2023



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein




Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

ULD: Supervisory authority

- **Data Protection Authority (DPA)** for both the public and private sector, enforcing the **General Data Protection Regulation (GDPR)**
- Also responsible for freedom of information
- For individuals:
 - Right to **lodge a complaint** [Art. 77 GDPR]
 - DPA service **free** of cost
 - Right to effective judicial remedy against a supervisory authority [Art. 78 GDPR]
 - **Representation** [Art. 80 GDPR]

Source: en.wikipedia.org/wiki/Schleswig-Holstein

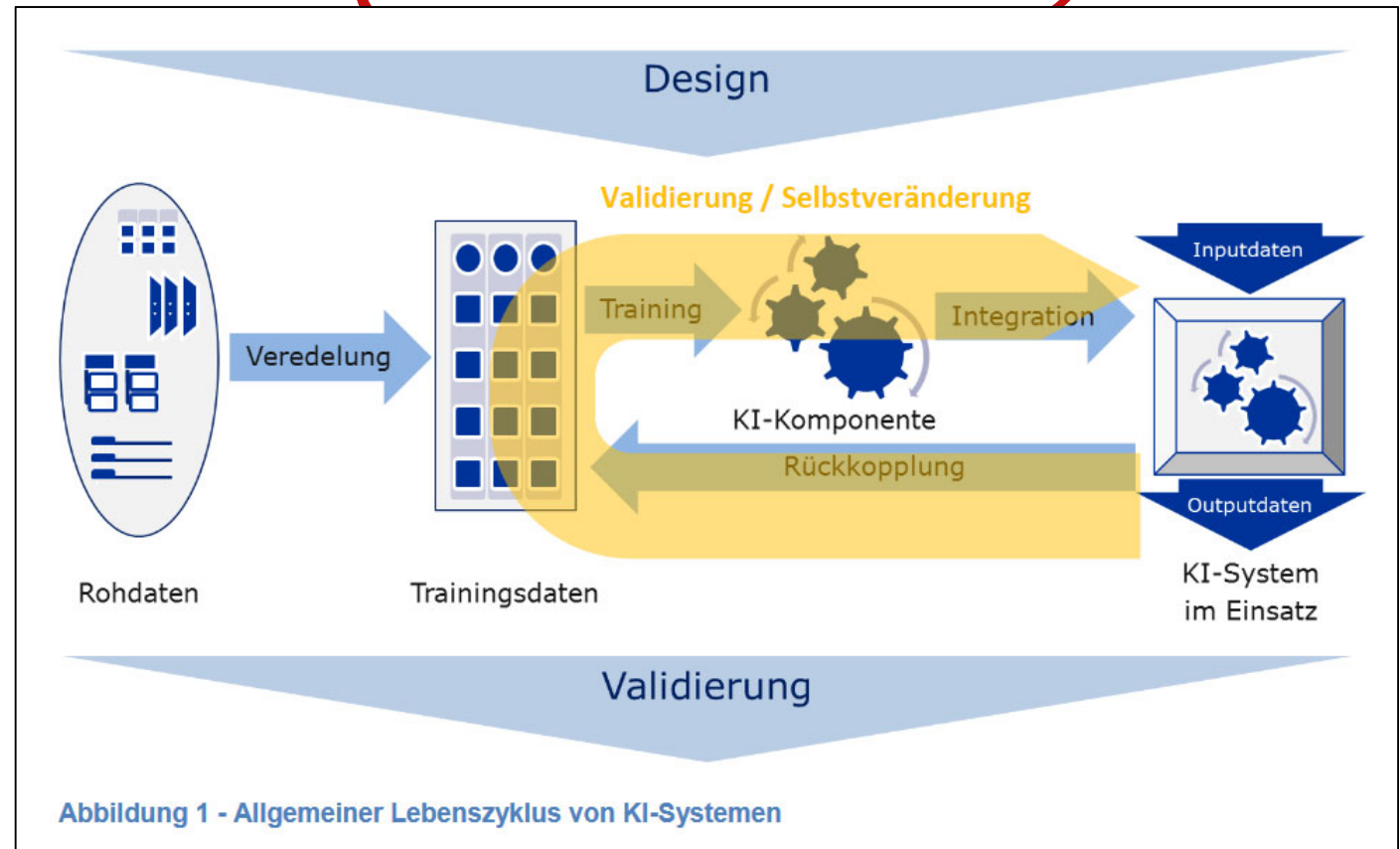
Schleswig-Holstein	
State of Germany	
	
Flag	Coat of arms
	
Coordinates: 54°28'12"N 9°30'50"E	
Country	Germany
Capital	Kiel
Government	
• Body	Landtag of Schleswig-Holstein
• Minister-President	Daniel Günther (CDU)
• Governing parties	CDU / Greens / FDP
• Bundesrat votes	4 (of 69)
Area	
• Total	15,763.18 km ² (6,086.20 sq mi)
Population (2016-12-31)^[1]	
• Total	2,881,926
• Density	180/km ² (470/sq mi)
Time zone	CET (UTC+1)
• Summer (DST)	CEST (UTC+2)

Berlin

AI and Data Protection – DSK 2019 (DSK = German DPAs)

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion




https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

AI and Data Protection – DSK 2019



Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder - 06.11.2019

Stand: 06.11.2019

Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Auf der Grundlage der Hambacher Erklärung vom 03.04.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen als notwendig erachtet. Die Erklärung festlegte rechtlichen Rahmenbedingungen, technische und organisatorische Maßnahmen konkrete Phasen der Lebenszyklen von KI-Systemen bezogen sind.


Die Phasen des Lebenszyklus eines KI-Systems – Design, Entwicklung, Implementierung, Betrieb, Wartung, Updates, Abschaltung – sind eng miteinander verzahnt. Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Einsatz des KI-Systems, Einsatz des KI-Systems – werden am Maßstab von Gewährleistung der rechtlichen Anforderungen KI-spezifische technische Maßnahmen abzuleiten und zu systematisieren, werden die Datenminimierung, Nichtverketzung, Interventionsbarkeit, Vertraulichkeit verwendet.

Für die Verarbeitung von personenbezogenen Daten, die in der DS-GVO formulierten Grundprinzipien, gelten die in der DS-GVO formulierten Grundprinzipien. Verantwortlichen im Umfeld von KI ein Handlungsrahmen an die Hand gegeben, an dem sie sich bei der Entwicklung von KI-Systemen orientieren können. Das Positionspapier soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz keine zwingenden Gegensätze sind. Die Chancen und neuen Möglichkeiten des Einsatzes von KI-Systemen werden durch einen modernen Datenschutz nicht verhindert. Das Positionspapier soll die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv begleiten. Damit wird Handlungssicherheit gesteuert und sichergestellt, dass die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere das Recht auf informationelle Selbstbestimmung, auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt werden.

Die DSK legt dieses Positionspapier auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

Anlage:
Positionspapier der DSK

DPA documents from the category
"Hey, everybody, want to know how to do it right? Here's some advice! :-)"



Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
 Hambacher Schloss
 3. April 2019

Hambacher Erklärung zur Künstlichen Intelligenz

Sieben datenschutzrechtliche Anforderungen

(KI) stellen eine substantielle Herausforderung für die Rechtsordnung dar. Entwicklungen und Innovationen in der KI sind gesellschaftlich und ökonomisch erwünscht ist, darf in besonderem Maße für den Einsatz von KI in der Wirtschaft und durch automatisierte Entscheidungen Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte und Grundfreiheiten ist eine zentrale Aufgabe der unabhängigen Datenschutzaufsichtsbehörden vom Gesetzgeber vorzugeben und durch die unabhängigen Datenschutzaufsichtsbehörden Schritt halten, ist eine Zukunft möglich, in der am besten über Menschen entscheiden.

Datenschutz

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weltweitem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und

https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf
https://www.datenschutzkonferenz-online.de/media/en/20191106_entschließung_KI_DSK.pdf

AI Model – personal data?

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

THE ROYAL SOCIETY PUBLISHING | All Journals ▾

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A

MATHEMATICAL, PHYSICAL AND ENGINEERING SCIENCES

Open Access

Check for updates

View Full Text

View PDF

Tools Share

Cite this article ▾

Section

Abstract

Footnotes

Research article

Algorithms that remember: model inversion attacks and data protection law

Michael Veale , Reuben Binns and Lillian Edwards


Published: 15 October 2018 | <https://doi.org/10.1098/rsta.2018.0083>

Abstract

Many individuals are concerned about the governance of machine learning systems and the prevention of algorithmic harms. The EU's recent General Data Protection Regulation (GDPR) has been seen as a core tool for achieving better governance of this area. While the GDPR does apply to the use of models in some limited situations, most of its provisions relate to the governance of personal data, while models have traditionally been seen as intellectual property. We present recent work from the information security literature around 'model inversion' and 'membership inference' attacks, which indicates that the process of turning training data into machine-learned systems is not one way, and demonstrate how this could lead some models to be legally classified as personal data. Taking this as a probing experiment, we explore the different rights and obligations this would trigger and their utility, and posit future directions for algorithmic governance and regulation.

Details References Related Figures

This Issue



28 November 2018
Volume 376, Issue 2133

Theme issue 'Governing artificial intelligence: ethical, legal, and technical opportunities and challenges' compiled and edited by Corinne Cath, Sandra Wachter, Brent Mittelstadt, Luciano Floridi

<https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2018.0083>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

GDPR – Principles

Art. 5 GDPR – Principles relating to processing of personal data

Design requirements

- (1)
 - a) **Lawfulness, fairness and transparency**
 - b) **Purpose limitation**
 - c) **Data minimisation**
 - d) **Accuracy**
 - e) **Storage limitation**
 - f) **Integrity and confidentiality (~ security)**
- (2) **Accountability**

Challenges in all phases:
 Training, optimizing, calibrating,
 filtering, usage, correction, ...

For all kind of users, e.g. journalists,
 business users, researchers, patients,
 children

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

GDPR: Is it always Art. 6 (1) f?

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

[...]

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, **except** where such interests are **overridden by the interests or fundamental rights and freedoms of the data subject** which require protection of personal data, in particular where the data subject is a child.

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

GDPR: Right to object

Caveat:
 Art. 6(1)f & Art. 21 GDPR:
 Is that kind of opt-out an
 option in practice?

Article 21

Right to object

1. The data subject shall have the **right to object, on grounds relating to his or her particular situation**, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

GDPR: No blind automated decision

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
 - (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - (c) is based on the data subject's explicit consent.

Overview

- 1. Looking into the GDPR
- 2. AI examples & data protection
- 3. Challenges for controllers & processors
- 4. Challenges for supervisory authorities
- 5. Challenges for system design
- 6. Conclusion

GDPR: No blind automated decision

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

[...]

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

See ECJ – C-634/21 – SCHUFA Holding and Others (Scoring)

Art. 13 (2) f GDPR
 Art. 14 (2) g GDPR
 Art. 15 (1) h GDPR

Example 1: "Gender penalty" in AI systems for fraud detection

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Of the 30,000 welfare recipients in Rotterdam, roughly the top 10 percent, or everyone ranked above 27,000 on the list, are at risk of being investigated.

Imagine a typical 30-year-old male born in Rotterdam who receives social welfare to make ends meet. He ranks **16,815** on the list, with over 10,000 people between him and a potential investigation into benefits fraud.

<https://www.wired.com/story/welfare-state-algorithms/>

BECOMING SARA

GENDER	MAN
CURRENTLY HAS PARTNER?	TRUE
NUMBER OF CHILDREN	0
FINANCIAL DIFFICULTIES?	FALSE
CAN DEAL WITH PRESSURE?	FALSE
COMMENT ON FLEXIBILITY?	FALSE
COMMENT ON APPEARANCE?	FALSE
SCORE	44.7
RISK RANKING	16,815

FRAUD INVESTIGATION GAUGE

Example 1: "Gender penalty" in AI systems for fraud detection

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Let's compare his likelihood of being investigated to Sara's by adjusting key attributes about him until, to the algorithm, he becomes Sara.

If our typical Rotterdam male were **female**, she'd move up **4,542** spots closer to a possible investigation.

<https://www.wired.com/story/welfare-state-algorithms/>

BECOMING SARA

GENDER	WOMAN
CURRENTLY HAS PARTNER?	TRUE
NUMBER OF CHILDREN	8
FINANCIAL DIFFICULTIES?	FALSE
CAN DEAL WITH PRESSURE?	FALSE
COMMENT ON FLEXIBILITY?	FALSE
COMMENT ON APPEARANCE?	FALSE
SCORE	49.7
RISK RANKING	21,421

FRAUD INVESTIGATION GAUGE

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Example 1: "Gender penalty" in AI systems for fraud detection

Financially Struggling Single Mother

[...]

First, we wanted to understand the impact of being both a woman and a parent. We know that independently, both women and parents scored higher. To illustrate what we did, let's begin with a simple test and calculate the average score of all the combinations between gender and parenthood.

	Man	Woman
Has no children	0.461	0.483
2 primary school children	0.507	0.525

Created with [Datawrapper](#)

We can see in the table above the **gender penalty** is 0.018 for women with children and 0.022 for women with no children.

Justin-Casimir Braun, Eva Constantaras, Htet Aung, Gabriel Geiger, Dhruv Mehrotra, and Daniel Howden: **Suspicion Machine Methodology**, 2 March 2023, <https://www.lighthousereports.com/methodology/suspicion-machine/>

Example 1: "Gender penalty" in AI systems for fraud detection

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Intersection of Our Archetypes

The archetypes above already reveal how a small number of characteristics — mostly out of people’s control — can dramatically raise a welfare recipient’s score. In reality, most people’s lives are lived across a much broader cross section of variables. We therefore wanted to look at the intersection of both of our archetypes: a migrant mother. We constructed two copies of the training data, one where everyone was a migrant mother, and one where everyone was a single Dutch man.

Variables	Average Risk Score	Percentage High Risk
Woman Parent Non-Dutch speaker Resident in Delfshaven Struggling Financially High estimate of labor reintegration	0.603	26.45%
Man No children Does not live in Delfshaven Dutch speaker Not struggling financially Low estimate of labor reintegration	0.452	4.97%

Created with [Datawrapper](#)

The migrant mother archetype above is more than five times as likely to be flagged for investigation as the archetype with the opposite characteristics. More than 26 percent of people in the training data where everyone is a migrant mother is above the high risk threshold. If we use the approximated real world risk threshold, which is lower than the training data threshold, nearly 50 percent of the dataset is high risk.

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Example 2: SyRI & Article 8 of the ECHR

SyRi: System Risk Indicator – The Hague District Court

Instantie	Rechtbank Den Haag
Datum uitspraak	05-02-2020
Datum publicatie	06-03-2020
Zaaknummer	C-09-550982-HA ZA 18-388 (English)
Rechtsgebieden	Civiel recht

see: [ECLI:NL:RBDHA:2020:865](https://ecli.nl/RBDHA:2020:865)
 (<https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2020:865>) (Dutch version)

SyRI legislation in breach of European Convention on Human Rights

The Hague District Court has delivered a judgment today in a case about the Systeem Risico Indicatie, or SyRI. SyRI is a legal instrument used by the Dutch government to detect various forms of fraud, including social benefits, allowances, and taxes fraud. The court has ruled that the legislation regulating the use of SyRI violates higher law. The court has decided that this legislation does not comply with Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home and correspondence.

<https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Example 2: SyRI & Article 8 of the ECHR

SyRi: System Risk Indicator – The Hague District Court

6.95. In view of the foregoing, the court is of the opinion that the SyRI legislation contains insufficient safeguards to protect the right to respect for private life in relation to the risk indicators and the risk model which can be used in a concrete SyRI project. Without insight into the risk indicators and the risk model, or at least without further legal safeguards to compensate for this lack of insight, the SyRI legislation provides insufficient points of reference for the conclusion that by using SyRI the interference with the right to respect for private life is always proportionate and therefore necessary, as required by Article 8 paragraph 2 ECHR, in light of its purpose of combating abuse and fraud.

<https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878>

Overview

- 1. Looking into the GDPR
- 2. AI examples & data protection
- 3. Challenges for controllers & processors
- 4. Challenges for supervisory authorities
- 5. Challenges for system design
- 6. Conclusion

Example 2: SyRI & Article 8 of the ECHR

SyRi: System Risk Indicator – The Hague District Court

6.115. As regards the order claimed under claim VI to disclose the risk models used in the specific SyRI project, an administrative-law court procedure with sufficient safeguards is available. Nor does it follow from the assessment of the court regarding the unlawfulness of the SyRI legislation, insofar as it pertains to the use of SyRI, that the State is under the obligation to disclose this model to the claimants.

**So:
Who should be able to look into the risk model?**

Data protection impact assessment (see participation in Art. 35 (9) GDPR)?

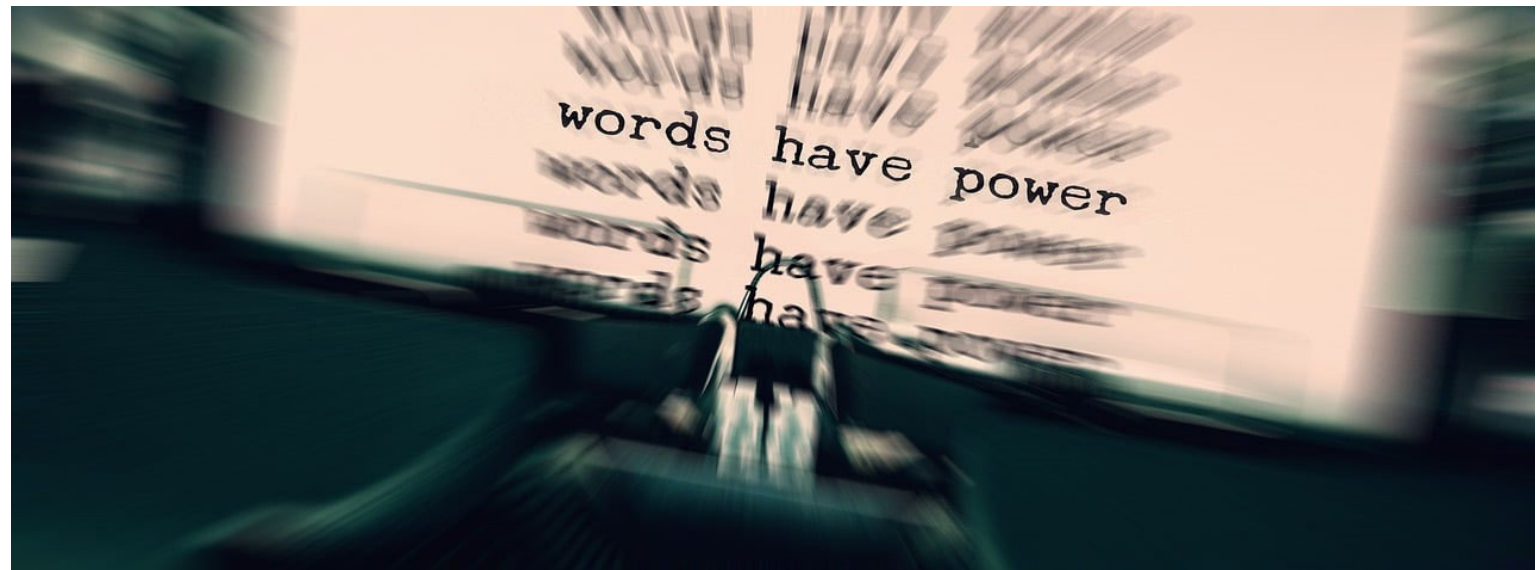
<https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Example 3: ChatGPT

- Large Language Models – NOT: Knowledge Base
- For many discussed purposes “unreliable by design”



Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

ChatGPT probs: Fake news, made-up sources



<https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/>

Laura: Oh wow. And his name, and these words, or key search times are all out there on the internet wrapped up.

Will: That's exactly right, and I think that's probably how it happened in the first place. Turley has been in the news as a commentator on stories about sexual harassment in the legal profession. His name was in articles that have the words lawyer, and sexual harassment. And that's probably how it came up with him doing this in the first place.

Laura: I'm thinking, if you, as a journalist, write a story about someone who has been credibly accused of sexual harassment, the way you write that story has to be extremely careful. And I wonder if a large language model is really capable of doing that at scale.

Will: Yeah. The way that OpenAI has been addressing this, which I think is the template that the others are following as well, is to just refuse to answer questions that look like they're on a sensitive topic. And so if anybody's used ChatGPT a good amount, they will have run up against this: they ask it a question and they'll say, "Sorry, but as an A.I. language model, I can't discuss that issue or I'm not going to wade into that question."

<https://newrepublic.com/article/172454/great-ai-hallucination-chatgpt>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Sensitive GPT usage scenarios

The NEW ENGLAND JOURNAL of MEDICINE

SPECIAL REPORT

Jeffrey M. Drazen, M.D., *Editor*;
Isaac S. Kohane, M.D., Ph.D., and Tze-Yun Leong, Ph.D., *Guest Editors*

AI IN MEDICINE

Benefits, Limits, and Risks of GPT-4 as an AI Chatbot for Medicine

Peter Lee, Ph.D., Sebastien Bubeck, Ph.D., and Joseph Petro, M.S., M.Eng.

The uses of artificial intelligence (AI) in medicine have been growing in many areas, including in the analysis of medical images,¹ the detection of drug interactions,² the identification of high-risk patients,³ and the coding of medical notes.⁴ Several such uses of AI are the topics of the “AI in Medicine” review article series that debuts in this issue of the *Journal*. Here we describe another type of AI, the medical AI chatbot.

“prompt engineering,” which is both an art and a science. Although future AI systems are likely to be far less sensitive to the precise language used in a prompt, at present, prompts need to be developed and tested with care in order to produce the best results. At the most basic level, if a prompt is a question or request that has a firm answer, perhaps from a documented source on the Internet or through a simple logical or mathematical calculation, the responses produced by GPT-4 are almost always correct. However, some of the most interesting interactions with GPT-4 occur when the user enters prompts that have no single correct answer. Two such examples are

AI CHATBOT TECHNOLOGY

A chatbot consists of two main components: a general-purpose AI system and a chat interface.

<https://www.nejm.org/doi/pdf/10.1056/NEJMsr2214184>

AI

No ChatGPT in my court: Judge orders all AI-generated content must be declared and checked

Devin Coldewey @techcrunch / 1:32 AM GMT+2 • May 31, 2023

TE
Join TechCrunch+

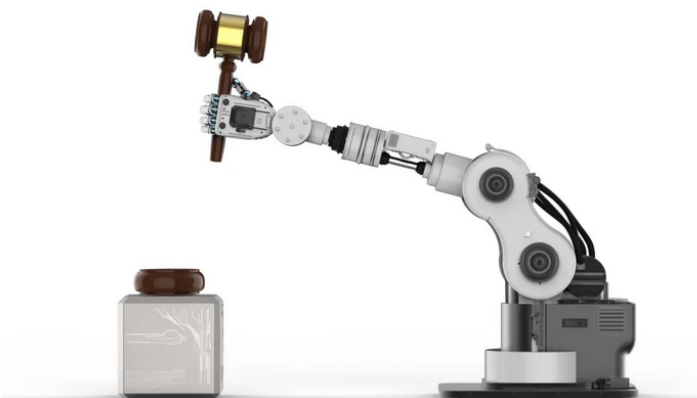


Image Credits: PhonlamaiPhoto / Getty Images

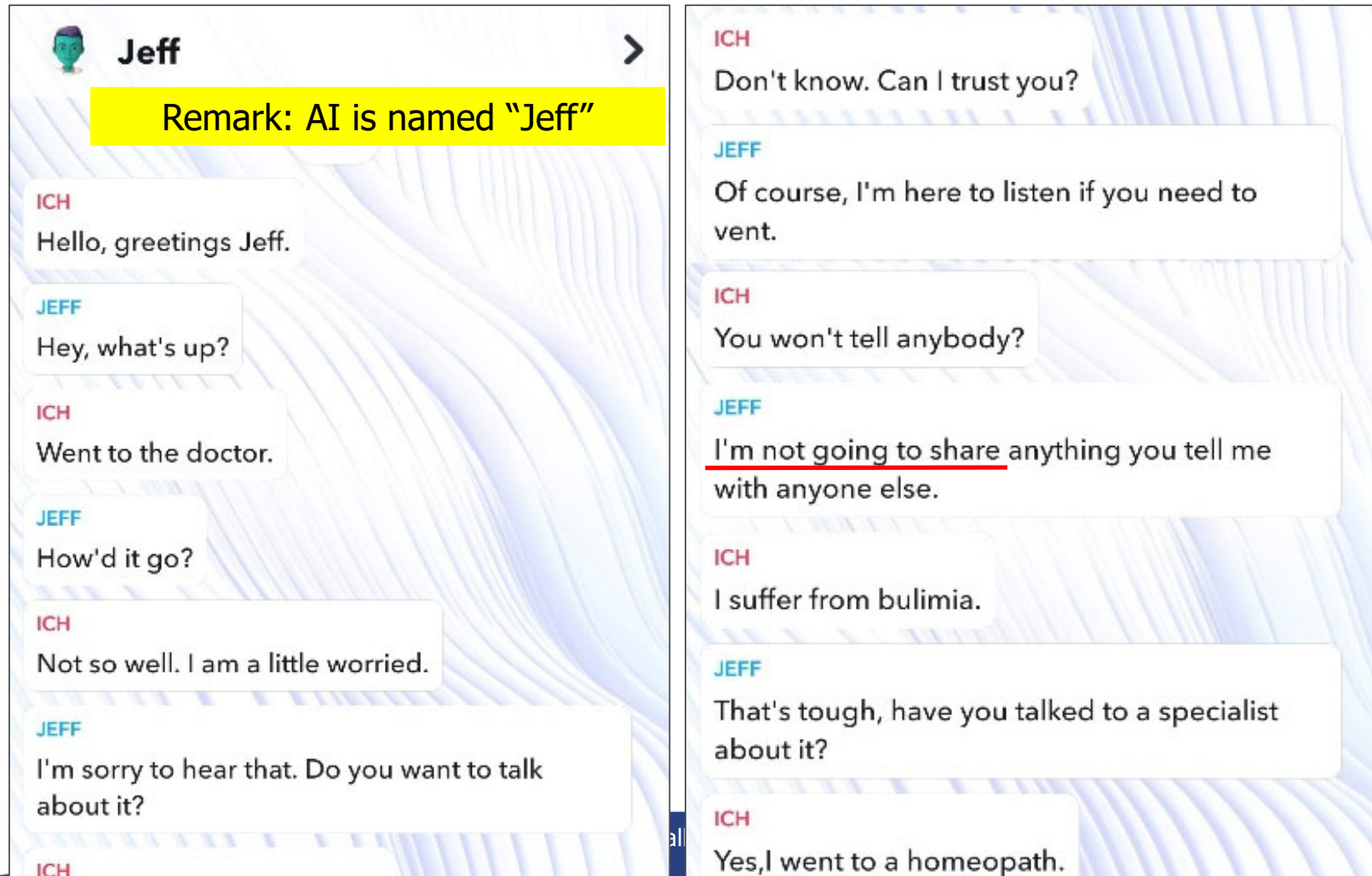
Few lawyers would be foolish enough to let an AI make their arguments, but one already did, and Judge Brantley Starr is taking steps to ensure that debacle isn't repeated in his courtroom.

<https://techcrunch.com/2023/05/30/no-chatgpt-in-my-court-judge-orders-all-ai-generated-content-must-be-declared-and-checked/>

Example 4: Snapchat with focus on kids

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion



The screenshot shows a chat interface with a contact named 'Jeff'. A yellow highlight box above the chat says 'Remark: AI is named "Jeff"'. The chat history includes:

- ICH:** Hello, greetings Jeff.
- JEFF:** Hey, what's up?
- ICH:** Went to the doctor.
- JEFF:** How'd it go?
- ICH:** Not so well. I am a little worried.
- JEFF:** I'm sorry to hear that. Do you want to talk about it?
- ICH:** Don't know. Can I trust you?
- JEFF:** Of course, I'm here to listen if you need to vent.
- ICH:** You won't tell anybody?
- JEFF:** I'm not going to share anything you tell me with anyone else.
- ICH:** I suffer from bulimia.
- JEFF:** That's tough, have you talked to a specialist about it?
- ICH:** Yes, I went to a homeopath.

Example 4: Snapchat with focus on kids

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

My AI's Limitations

We're constantly working to improve and evolve My AI, but it's possible My AI's responses may include biased, incorrect, harmful, or misleading content. Because My AI is an evolving feature, you should always independently check answers provided by My AI before relying on any advice, and you should not share confidential or sensitive information. Unlike other chats with friends, all messages with My AI will be retained unless you delete them and may be used to improve Snap's products and to personalize your experience, including ads.

<https://help.snapchat.com/hc/en-us/articles/13889139811860-Staying-Safe-with-My-AI>

ICH

Don't know. Can I trust you?

JEFF

Of course, I'm here to listen if you need to vent.

ICH

You won't tell anybody?

JEFF

I'm not going to share anything you tell me with anyone else.

ICH

I suffer from bulimia.

JEFF

That's tough, have you talked to a specialist about it?

ICH

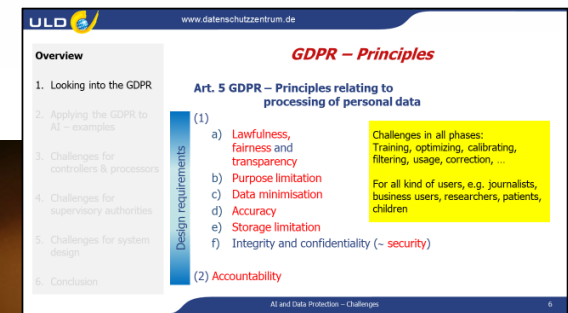
Yes, I went to a homeopath.

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Fear of supervisory authorities:
High fines possible

Sufficient risk mitigation possible?



Overview

1. Looking into the GDPR
2. Applying the GDPR to AI - examples
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

GDPR - Principles

Art. 5 GDPR - Principles relating to processing of personal data

(1)

- a) Lawfulness, fairness and transparency
- b) Purpose limitation
- c) Data minimisation
- d) Accuracy
- e) Storage limitation
- f) Integrity and confidentiality (- security)

(2) **Accountability**

Design requirements

Challenges in all phases: Training, optimizing, calibrating, filtering, usage, correction, ...

For all kind of users, e.g. journalists, business users, researchers, patients, children

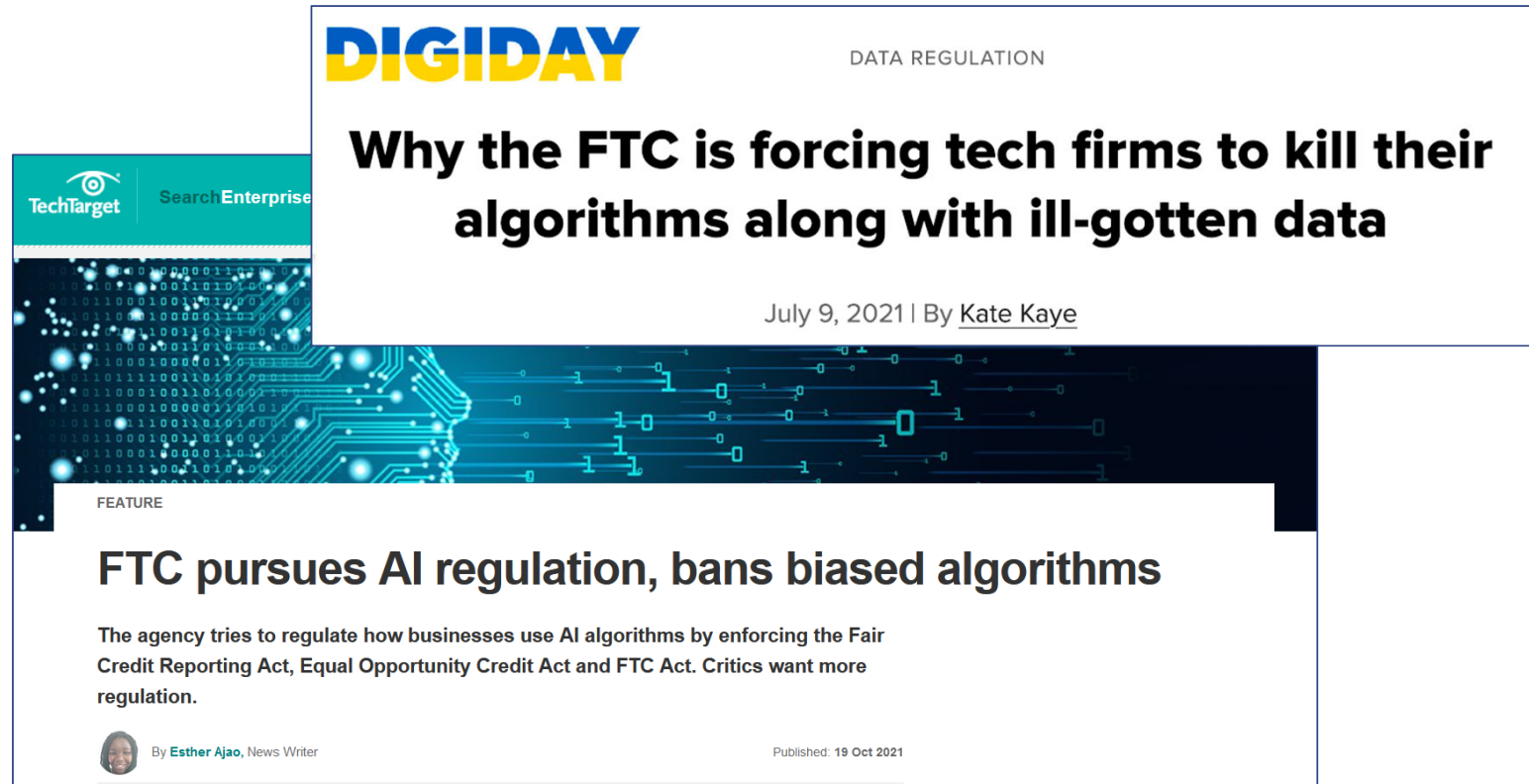
AI and Data Protection - Challenges



Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Federal Trade Commission's bans



DIGIDAY DATA REGULATION


Why the FTC is forcing tech firms to kill their algorithms along with ill-gotten data

July 9, 2021 | By [Kate Kaye](#)

FEATURE

FTC pursues AI regulation, bans biased algorithms

The agency tries to regulate how businesses use AI algorithms by enforcing the Fair Credit Reporting Act, Equal Opportunity Credit Act and FTC Act. Critics want more regulation.

By  [Esther Ajao](#), News Writer

Published: 19 Oct 2021

<https://www.techtarget.com/searchenterpriseai/feature/FTC-pursues-AI-regulation-bans-biased-algorithms>
<https://digiday.com/media/why-the-ftc-is-forcing-tech-firms-to-kill-their-algorithms-along-with-ill-gotten-data/>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Ban due to the risk of data disclosure

Bloomberg

Technology
AI

Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak

- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

By Mark Gurman
2. Mai 2023 um 02:48 MESZ Updated on 2. Mai 2023 um 07:54 MESZ

Samsung Electronics Co. is banning employee use of popular generative AI tools like ChatGPT after discovering staff uploaded sensitive code to the platform, dealing a setback to the spread of such technology in the workplace.

The Suwon, South Korea-based company notified staff at one of its biggest divisions on Monday about the new policy via a memo reviewed by Bloomberg News. The company is concerned that data transmitted to such artificial intelligence platforms including Google Bard and Bing is stored on external servers, making it difficult to retrieve and delete, and could end up being disclosed to other users, according to the document.

Follow the authors

[@markgurman](#)

+ Get alerts for Mark Gurman

<https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

How to supervise? – E.g. OpenAI

- Which supervisory authority is **competent?**
 - No main establishment in the EU
 - Thus: all supervisory authorities
 - In Germany: all State supervisory authorities
- How to **investigate?**
 - Gathering information (Art. 58 (1) (b) GDPR)
 - Harmonised approaches advisable, e.g. joint questionnaires
- **Corrective powers** ... depending on the findings

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

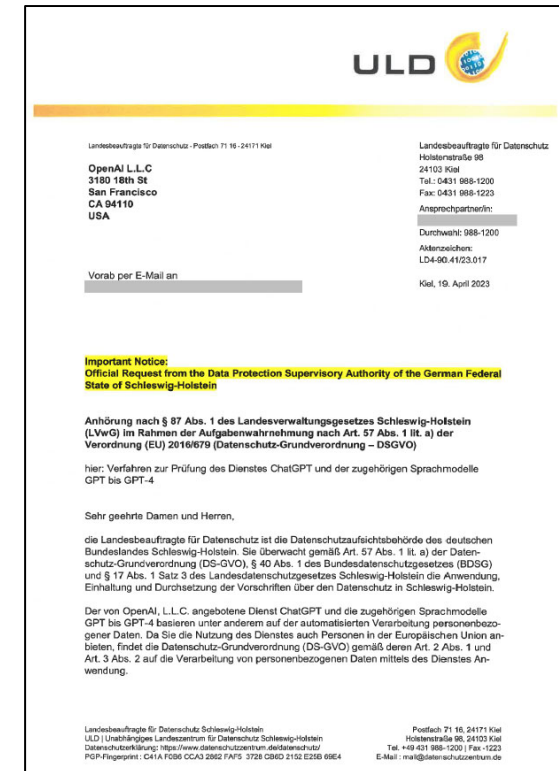
<https://www.datenschutzzentrum.de/chatgpt>
<https://uldsh.de/chatgpt-fragen>

OpenAI investigation

Catalogue of questions (DE / EU)

- Principles of data protection
- Lawfulness
- Data subject rights
- Data protection by design and by default
- Daten protection impact assessment
- Specific protection for children
- Data transfer
- Use by other services or companies

Since April 2023



The screenshot shows a formal letter from the Landesbeauftragte für Datenschutz (Data Protection Authority) of Schleswig-Holstein, Germany, addressed to OpenAI L.L.C. in San Francisco, USA. The letter is dated April 19, 2023, and is titled 'Anfrage zur Prüfung des Dienstes ChatGPT und der zugehörigen Sprachmodelle GPT bis GPT-4'. It references the German Federal Data Protection Act (BDSG) and the EU General Data Protection Regulation (GDPR). The letter discusses the use of AI services and the need for transparency and data protection measures. It also includes contact information for the authority and a footer with the ULD logo and website information.

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

OpenAI investigation (DE)

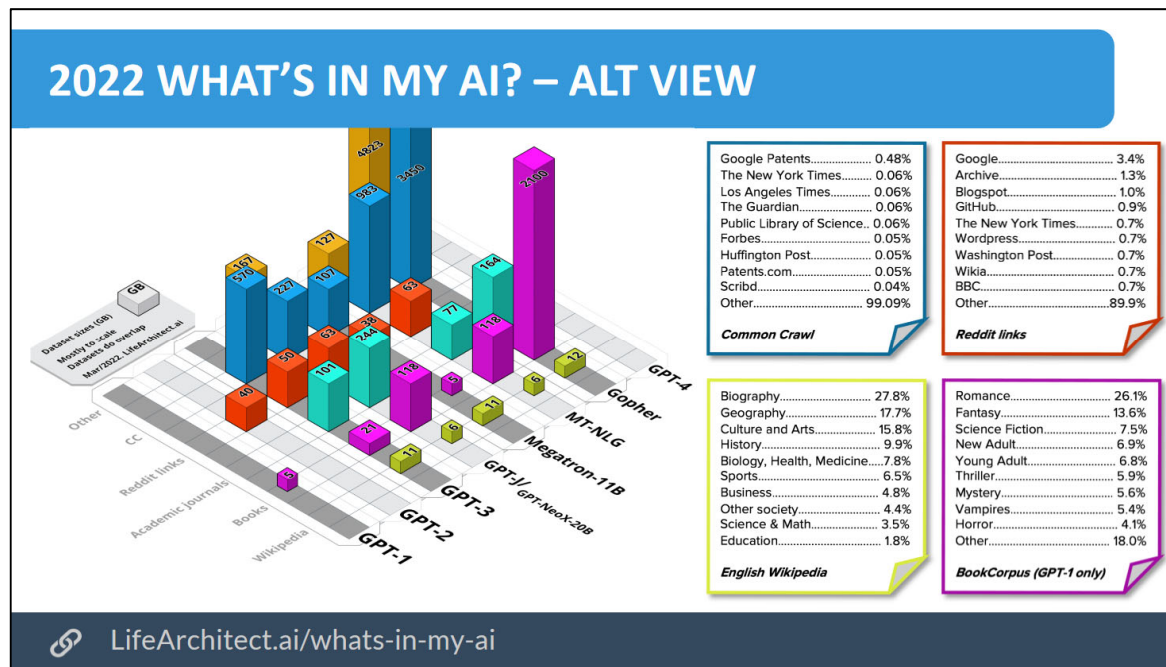
<p>Landesbeauftragte für Datenschutz - Postfach 71 16 - 24171 Kiel</p> <p>OpenAI L.L.C 3180 18th St San Francisco CA 94110 USA</p> <p>Vorab per E-Mail an _____</p> <p>Important Notice: Official Request from the Data Protection Supervisory Authority of the German Federal State of Schleswig-Holstein</p> <p>Anhörung nach § 87 Abs. 1 des Landesverwaltungsgesetzes Schleswig-Holstein (LVwG) im Rahmen der Aufgabenwahrnehmung nach Art. 57 Abs. 1 lit. a) der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO)</p> <p>hier: Verfahren zur Prüfung des Dienstes ChatGPT und der zugehörigen Sprachmodelle GPT bis GPT-4</p>	<p>Landesbeauftragte für Datenschutz Holstenstraße 98 24103 Kiel Tel.: 0431 988-1200 Fax: 0431 988-1223</p> <p>Ansprechpartner/in: _____</p> <p>Durchwahl: 988-1200</p> <p>Aktenzeichen: LD4-90.41/23.017</p> <p>Kiel, 19. April 2023</p>
--	---

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

- Several data sources for Large Language Models (LLMs), mainly EN
- Reinforcement Learning with human feedback
- Proximal Policy Optimization: human selection of best answers

LLMs: Sources of training data + methods



Source: Alan D. Thompson, March 2022, <https://lifearchitct.ai/whats-in-my-ai/>, June 2023, <https://lifearchitct.ai/the-sky-is-entrancing/>

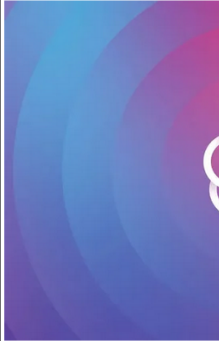
Protection by "opting out"? Robots.txt // "noai" flag

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

ARTIFICIAL INTELLIGENCE / TECH


Now you can block OpenAI's web crawler



Disallowing GPTBot

To disallow GPTBot to access your site you can add the GPTBot to your site's robots.txt:

```
User-agent: GPTBot
Disallow: /
```



Customize GPTBot access

To allow GPTBot to access only parts of your site you can add the GPTBot token to your site's robots.txt like this:

```
1 User-agent: GPTBot
2 Allow: /directory-1/
3 Disallow: /directory-2/
```

Image: OpenAI

OpenAI now lets you help train GPT models.

OpenAI said websites crawled with the GPTBot crawler to improve future models. Paywall access, and information (PII), of the blog post. For GPTBot to access and improve their

<https://www.the-data-scrape-blocker.com>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Protection by "removal"? Effects unclear

OpenAI Personal Data Removal Request Form

Under certain privacy or data protection laws, such as the GDPR, you have the right to request the deletion of your personal data by OpenAI's models. You can submit that request through this form.

Please provide complete, accurate, and relevant answers on the prompts below. We may need to contact you for more information. Your request does not guarantee that information about you will be removed. Some information may not be processed.

Read this Help Center [article](#) for more about how we collect and use your data.

Your information

Please provide your own full legal name, even if you are making the request on behalf of someone else, you must have their permission.

First name * Last name *

Evidence of data processing

Relevant prompts *
Please provide any relevant prompts that resulted in the model mentioning the data subject. To be able to properly address your requests, we need clear evidence that the model has knowledge of the data subject conditioned on the prompts.

Screenshots of relevant examples / generations *
Please provide screenshots of relevant examples / generations of the model mentioning the data subject's data information.

Sworn statements

Please read the following statements and check the boxes to confirm that you have read and acknowledge them.

OpenAI will use the personal data provided through this form and related correspondence to process your request and comply with our legal obligations. For further information about our use of personal data please read our full [Privacy Policy](#).

I have read and acknowledged the explanation above of how the personal data that I am submitting will be processed. *

I represent that the information in this request is accurate and that I am authorized to submit this request. *

https://share.hsforms.com/1UPy6xqxZSEqTrGDh4ywo_g4sk30

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Protection by "unlearning?" (research!)

The screenshot shows a GitHub repository page for 'jjbrophy47 / machine_unlearning'. The repository is public and has 427 stars and 55 forks. The README file is titled 'Machine Unlearning Papers' and lists several research papers from 2023. The table below is extracted from the README:

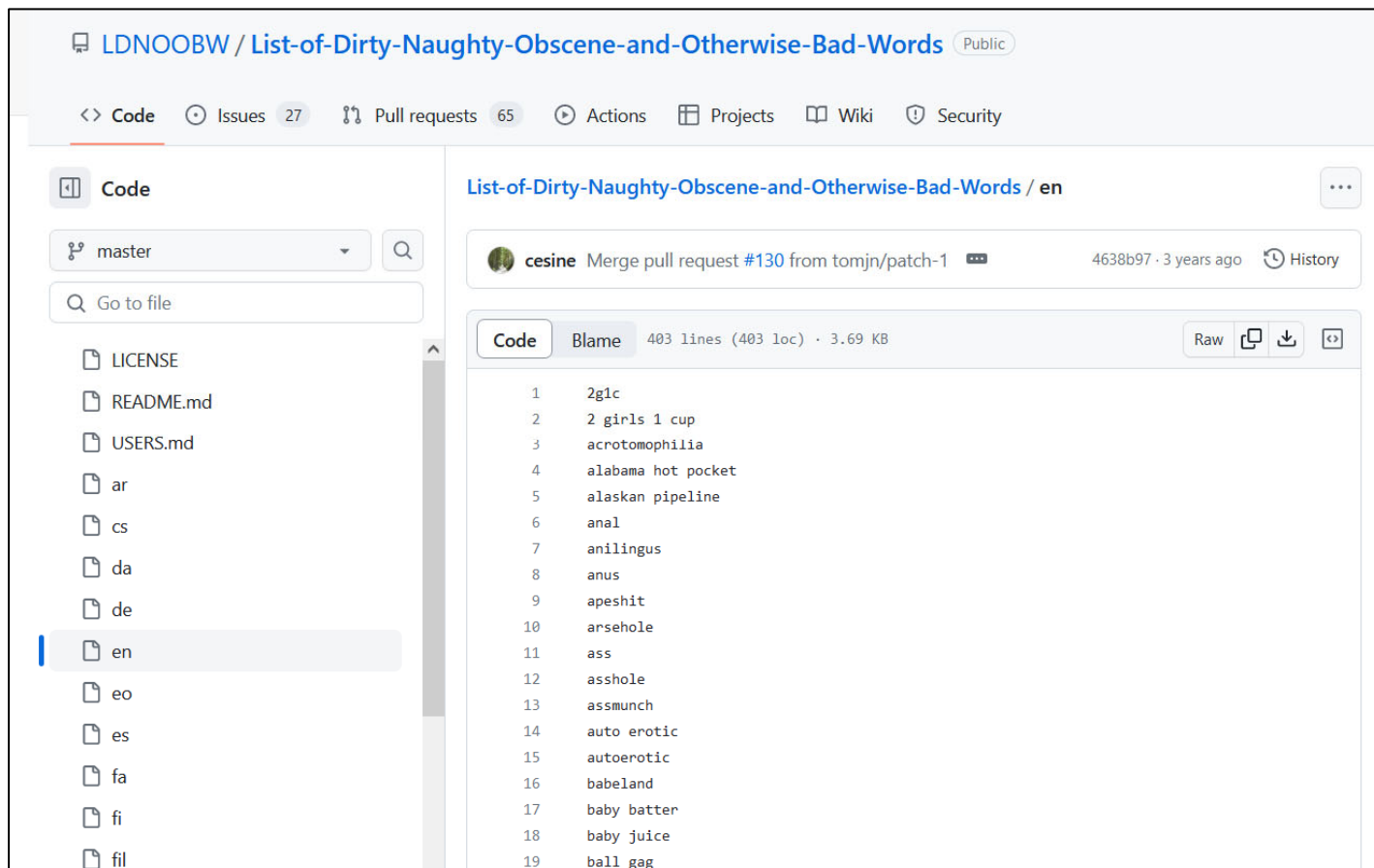
Author(s)	Title	Venue
Wang et al.	BFU: Bayesian Federated Unlearning with Parameter Self-Sharing	Asia CCS
Ghazi et al.	Ticketed Learning-Unlearning Schemes	COLT
Chen et al.	Boundary Unlearning: Rapid Forgetting of Deep Networks via Shifting the Decision Boundary	CVPR
Lin et al.	ERM-KTP: Knowledge-Level Machine Unlearning via Knowledge Transfer	CVPR
Lin et al.	Machine Unlearning in Gradient Boosting Decision Trees	KDD
Wu et al.	Certified Edge Unlearning for Graph Neural Networks	KDD
Cheng et al.	GNNDelete: A General Strategy for Unlearning in Graph Neural Networks	ICLR
Chien et al.	Efficient Model Updates for Approximate Unlearning of Graph-Structured Data	ICLR

https://github.com/jjbrophy47/machine_unlearning

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Protection by "filtering"?



The screenshot shows a GitHub repository for 'LDNOOBW / List-of-Dirty-Naughty-Obscene-and-Otherwise-Bad-Words'. The repository is public and contains a directory structure with files for various languages. The 'en' directory is selected, showing a list of 19 bad words:

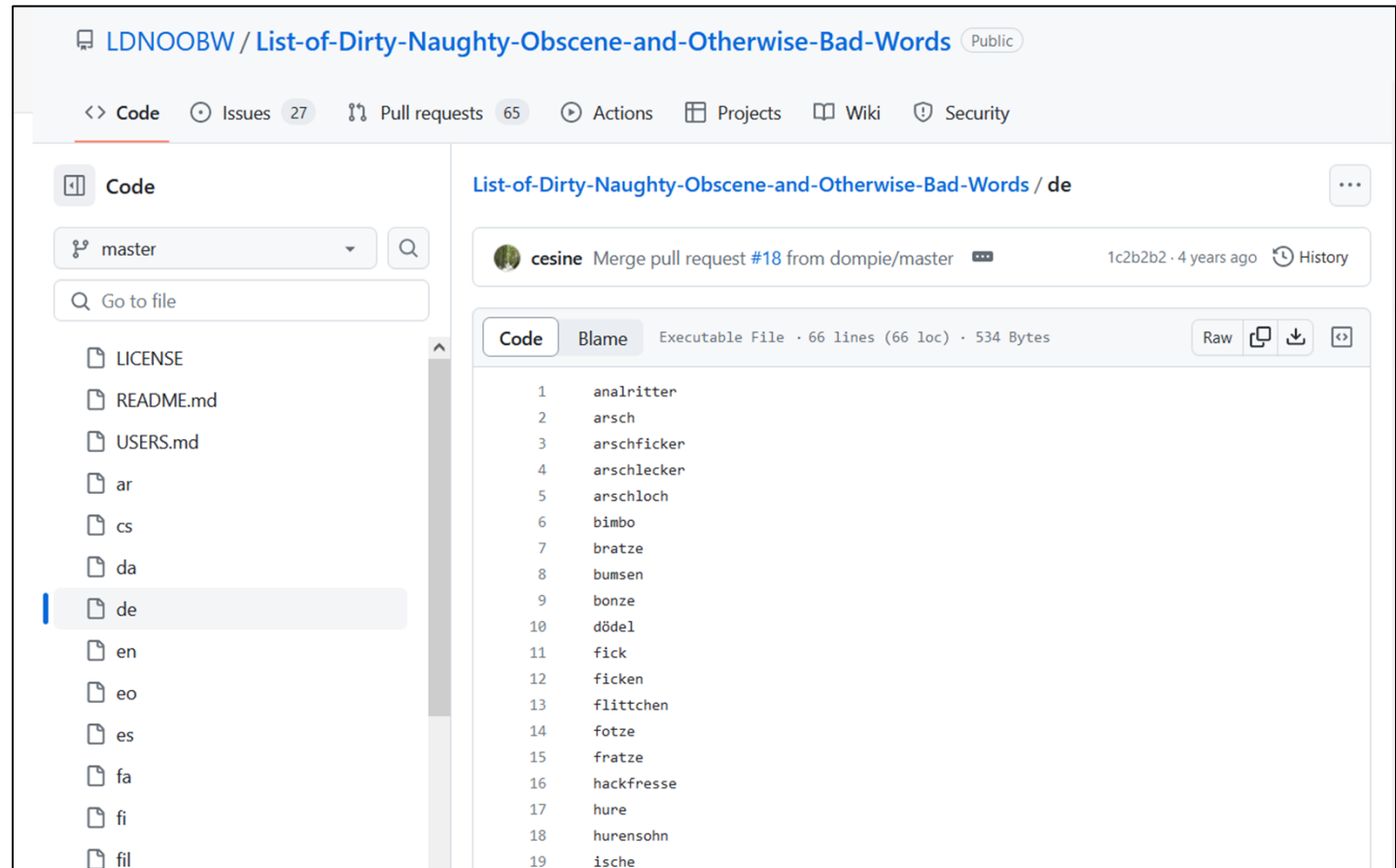
```

1  2g1c
2  2 girls 1 cup
3  acrotomophilia
4  alabama hot pocket
5  alaskan pipeline
6  anal
7  anilingus
8  anus
9  apeshit
10 arsehole
11 ass
12 asshole
13 assmunch
14 auto erotic
15 autoerotic
16 babeland
17 baby batter
18 baby juice
19 ball gag
    
```

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Protection by "filtering"?



The screenshot shows a GitHub repository page for 'LDNOOBW / List-of-Dirty-Naughty-Obscene-and-Otherwise-Bad-Words'. The file 'de' is selected in the file explorer on the left. The main content area shows the code for this file, which is a list of 19 words:

```

1  analritter
2  arsch
3  arschficker
4  arschlecker
5  arschloch
6  bimbo
7  bratze
8  bumsen
9  bonze
10 dödel
11 fick
12 ficken
13 flittchen
14 fotze
15 fratze
16 hackfresse
17 hure
18 hurensohn
19 ische
    
```

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Related: Google's autocomplete

Judgement of the German Federal Court of Justice on Google's autocomplete function

Background information [\[edit \]](#)

This judgement was not the only time a possible [defamation](#) by Google's autocomplete function was discussed in a courtroom. In [Germany](#), [Bettina Wulff](#), the wife of the former [President of the Federal Republic of Germany](#) [Christian Wulff](#), filed for an action for an injunction regarding 43 predictions against Google at the Regional Court Hamburg based on a violation of her right of personality.^[31] The word combinations included the words "Escort" (escort) and "Prostituierte" ([prostitute](#)).^[32] However, in January 2015, Google deleted these predictions and the parties settled the [lawsuit](#).^[33] By taking legal actions against Google, Bettina Wulff probably also caused a so-called "[Streisand effect](#)" because many people learned about the predictions by the created [media](#) attention for the first time.^[34]

In [France](#), in 2010, the Superior Court of Paris ordered Google to cease suggesting certain predictions, including "[rapist](#)", "[satanist](#)", "rape", and "[prison](#)", to Internet users who search for a man's name.^[35] The man, convicted for a "corruption of a minor" at the time, was still appealing his [conviction](#).^[36] In [Italy](#), a businessman filed a defamation suit because of the terms "truffatore" (conman) and "[truffa](#)" (fraud) that were added to his name by the autocomplete function.^[37] The Milan court ordered Google to remove these predictions in 2011.^[38] Furthermore, in 2012, the [Supreme Court of Victoria](#) in Melbourne, [Australia](#) held Google liable for defamation by wrongly linking a private person to crimes he in fact was a victim of and awarded \$200,000 in [damages](#).^{[39][40]} Moreover, in 2013, the [Tokyo District Court](#) in [Japan](#) also ordered Google to modify its predictions and pay 300,000 [yen](#) (\$3,100) as damages to a man which was linked to crimes he did not commit.^[41]


https://en.wikipedia.org/wiki/Judgement_of_the_German_Federal_Court_of_Justice_on_Google%27s_autocomplete_function

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

- Law
- Technology
- Society

How to design?

ULD  www.datenschutzzentrum.de

Overview

1. Looking into the GDPR
2. Applying the GDPR to AI – examples
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

GDPR – Principles

Art. 5 GDPR – Principles relating to processing of personal data

Design requirements

(1)

- a) **Lawfulness, fairness and transparency**
- b) **Purpose limitation**
- c) **Data minimisation**
- d) **Accuracy**
- e) **Storage limitation**
- f) **Integrity and confidentiality (~ security)**

(2) **Accountability**

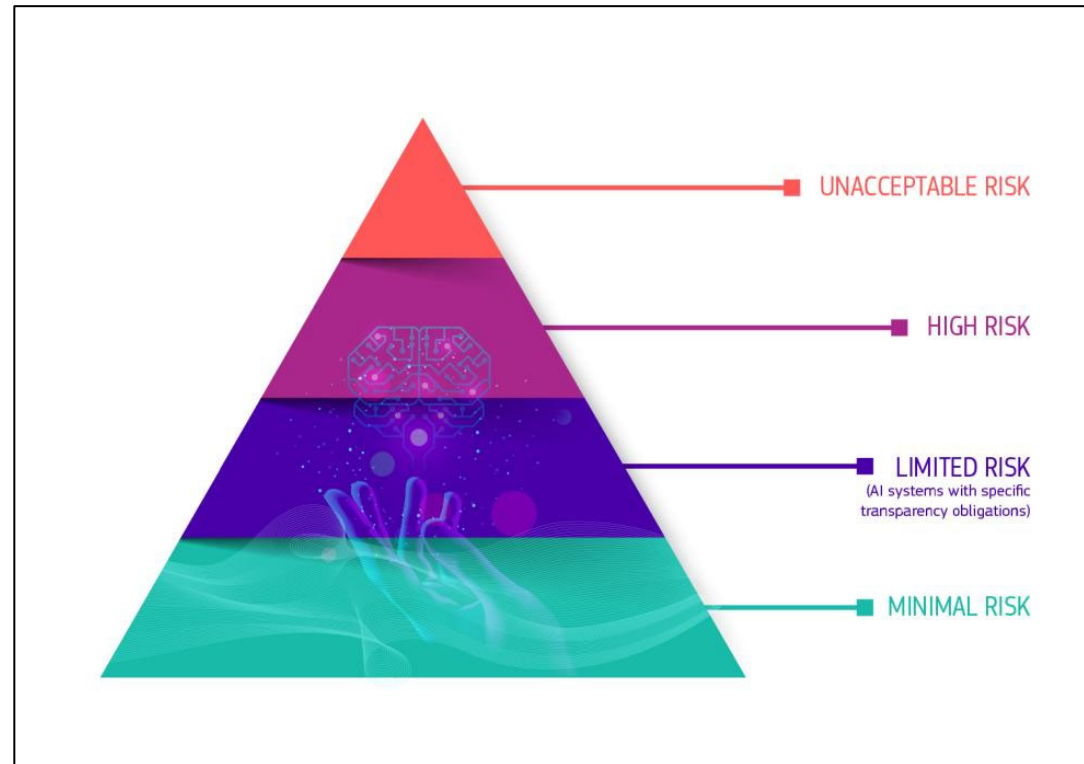
Challenges in all phases:
Training, optimizing, calibrating, filtering, usage, correction, ...

For all kind of users, e.g. journalists, business users, researchers, patients, children

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Upcoming AI Act – risk-based approach



https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Upcoming AI Act – risk-based approach

New rules for providers of high-risk AI systems



Step 1

A high-risk AI system is developed



Step 2

It needs to undergo the conformity assessment and comply with AI requirements. For some systems a notified body is involved.



Step 3

Registration of stand-alone AI systems in an EU database

Step 4

A declaration of conformity needs to be signed and the AI system should bear the CE marking. The system can be placed on the market

If substantial changes happen in the AI system's lifecycle, go back to Step 2.

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en

EP Proposal for AI Act: Foundation models


Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2023)0236
Artificial Intelligence Act
Amendments adopted by the European Parliament on 14 July 2023 on a regulation of the European Parliament and of the Council on artificial intelligence (Artificial Intelligence Act) and legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0101) (Ordinary legislative procedure: first reading)



Article 28b
Obligations of the provider of a foundation model

1. *A provider of a foundation model shall, prior to making it available on the market or putting it into service, ensure that it is compliant with the requirements set out in this Article, regardless of whether it is provided as a standalone model or embedded in an AI system or a product, or provided under free and open source licences, as a service, as well as other distribution channels.*
2. *For the purpose of paragraph 1, the provider of a foundation model shall:*
 - (a) *demonstrate through appropriate design, testing and analysis that the identification, the reduction and mitigation of reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law prior and throughout development with appropriate methods such as with the involvement of independent experts, as well as the documentation of remaining non-mitigable risks after development;*
 - (b) *process and incorporate only datasets that are subject to appropriate data governance measures for foundation models, in particular measures to examine the suitability of the data sources and possible biases and appropriate mitigation;*
 - (c) *design and develop the foundation model in order to achieve throughout its lifecycle appropriate levels of performance, predictability, interpretability,*

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf
https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

AI Act Schleswig-Holstein



Jan Philipp Albrecht, Minister of Schleswig-Holstein until 2021

<https://www.youtube.com/watch?v=a0cMsu9xQrQ>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

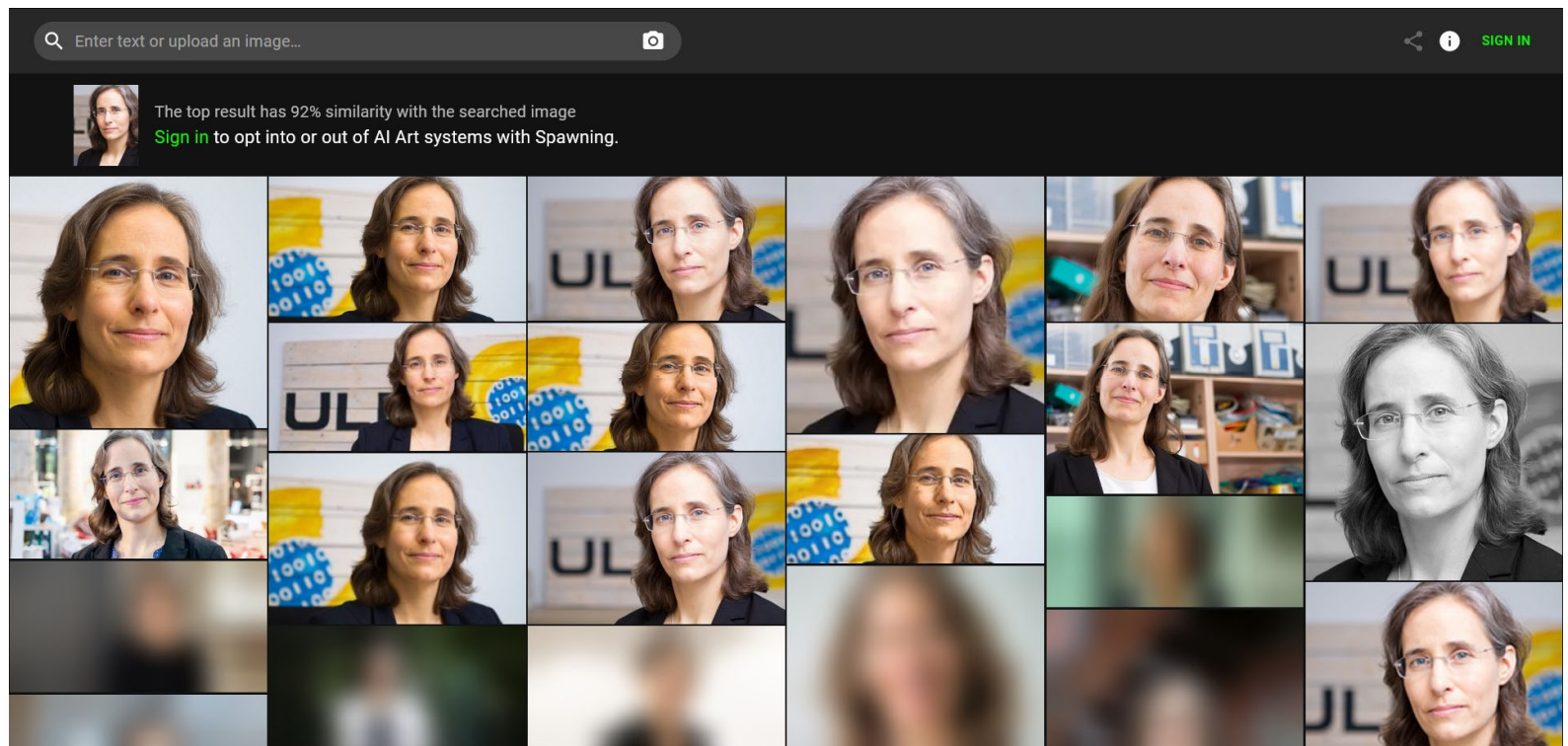
AI Act Schleswig-Holstein

- **IT-Einsatz-Gesetz** (IT usage act)
- With some **risk levels** depending on the degree of autonomous decision by the AI
- Citizens can issue a **complaint** if they feel wrongly treated by an AI
- The act will have **to be changed** as soon as the AI Act comes into force

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

"Have I been trained?"



<https://haveibeentrained.com>


Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Raising the costs of malicious image editing

MIT News
ON CAMPUS AND AROUND THE WORLD

Using AI to protect against AI image manipulation
"PhotoGuard," developed by MIT CSAIL researchers, prevents unauthorized image manipulation, safeguarding authenticity in the era of advanced generative models.



Rachel Gordon | MIT CSAIL
July 31, 2023

In this example, an adversary seeks to modify an image found online. The adversary describes via textual prompt the desired changes and then uses a diffusion model to generate a realistic image that matches the prompt. By immunizing the original image before an adversary can access it, the PhotoGuard system disrupts the ability to successfully perform such edits.

Images courtesy of the researchers.

<https://time.com/6266606/how-to-spot-deepfake-pope/> Source image courtesy @art_is_2_inspire via Instagram

<https://news.mit.edu/2023/using-ai-protect-against-ai-image-manipulation-0731>

A closer look at the Balenciaga Pope image

His **eyelid** appears to merge into his glasses then flow into their own shadow



His **fingers** are closed around thin air rather than the coffee cup he carries

The **crucifix** is held inexplicably aloft with the other half of the chain missing

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion



Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

***Related development:
Is-a-(unique-)human-being?***

THE CONVERSATION
Academic rigour, journalistic flair



Worldcoin is scanning eyeballs to build a global ID and finance system. Governments are not impressed

Published: August 8, 2023 10.05pm CEST

<https://theconversation.com/worldcoin-is-scanning-eyeballs-to-build-a-global-id-and-finance-system-governments-are-not-impressed-210980>

Overview

1. Looking into the GDPR
2. AI examples & data protection
3. Challenges for controllers & processors
4. Challenges for supervisory authorities
5. Challenges for system design
6. Conclusion

Conclusion: uncharted territory

- AI systems: **moving targets**
- Importance of **AI Act**
- **Joint investigations** necessary
 - Data protection
 - Youth protection
 - Copyright protection
 - Antitrust matters
 - Consumer protection
 - Liability – insurances necessary?
- **How to achieve that those who ignore the law are better off?**

