KI – Impuls Privacy und Datenschutz

Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

Workshop der Plattform Lernende Systeme
27.09.2018 in Berlin

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. **Begriffswelten Privacy & Datenschutz**
2. **Das Risiko nach der DSGVO**
3. **Schutzziele**
4. **Für KI?**

Beim Datenschutz geht es um ~~Daten~~

Menschen mit ihren Rechten

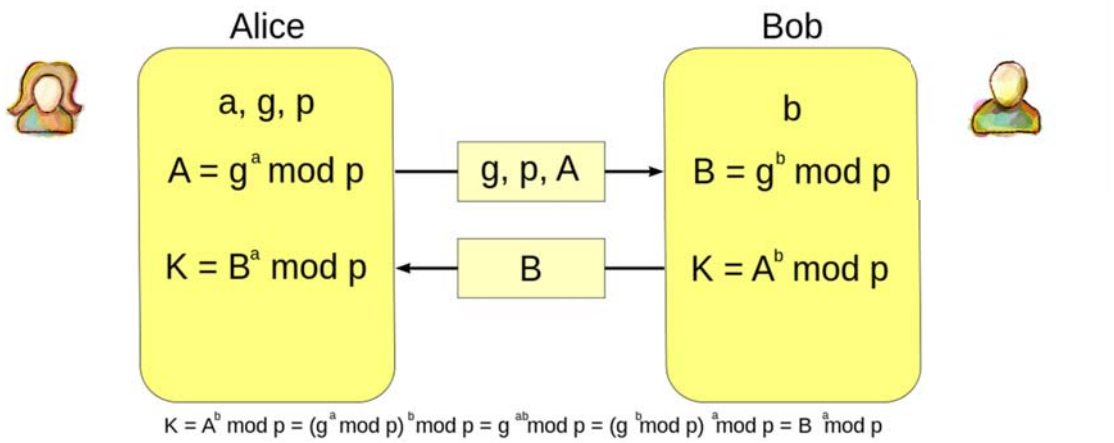
Fragen:

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?

Datenschutz nötig:

Machtgefälle zwischen Individuen und Organisationen

Datenschutz: weiter als IT-Sicherheit



IT-Sicherheit: Die Angreiferin ist Eve (oder Mallory).

Datenschutz: Der Angreifer ist Bob!
(Zumindest auch.)

Datenschutz: Schutz von Individuen

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.

Art. 8 GRCh: Grundrecht auf Datenschutz

- Datenschutz ist auf Verfassungsebene verankert
- Nicht nur Privatsphäre
- Schützt alle personenbezogenen Daten
- Verarbeitung von Daten ist Eingriff
  - Muss gerechtfertigt sein
  - Eingriff so mild wie möglich

Weitere relevante Grundrechte

- Artikel 7: Recht auf Schutz des Privatlebens (privacy)
- Artikel 11: Meinungsfreiheit
- Artikel 12: Versammlungsfreiheit
- Artikel 21: Nichtdiskriminierung
- Und weitere, je nach Kontext

Nicht nur individuell, auch im Kollektiv

Überblick

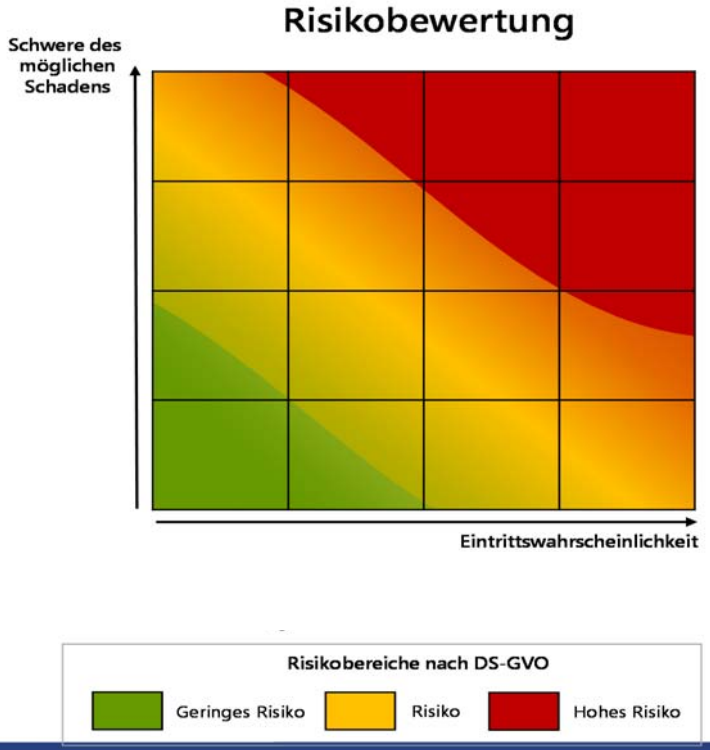
1. **Begriffswelten Privacy & Datenschutz**
2. **Das Risiko nach der DSGVO**
3. **Schutzziele**
4. **Für KI?**

Risikobegriff der DSGVO

- Risiko = Schwere möglicher Schäden x Eintrittswahrscheinlichkeit
- Lässt sich aber nicht quantifizieren
- Soll aber „objektiv bestimmt“ werden

- Risiken für Rechte müssen mit technischen und organisatorischen Maßnahmen eingedämmt werden

→ Artt. 24, 25, 32, 35 DSGVO sowie insb. ErwGr. 75



Risiko „fehlende Beherrschbarkeit“

Bild: sarangib via Pixabay

Brücken-stabilität

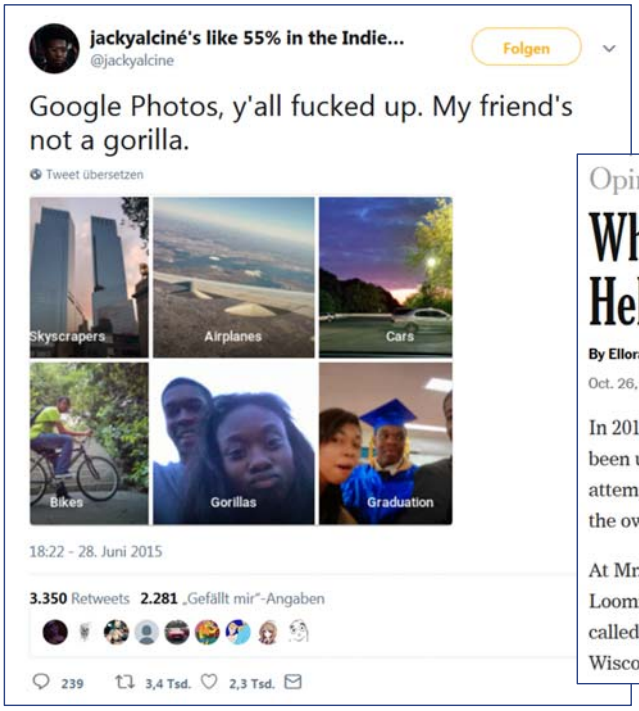
Bild: 3839153 via Pixabay

Predictive Policing

Risiko „Diskriminierung“

https://twitter.com/jackyalcine/status/615329515909156865

Risiko „Diskriminierung“



jackyalciné's like 55% in the Indie...
@jackyalcine

Folgen

Google Photos, y'all fucked up. My friend's not a gorilla.

Tweet übersetzen

Skyscrapers | Airplanes | Cars | Bikes | Gorillas | Graduation

18:22 - 28. Juni 2015

3.350 Retweets 2.281 „Gefällt mir“-Angaben

239 3,4 Tsd. 2,3 Tsd.

https://twitter.com/jackyalcine/status/615329515909156865

https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html

Opinion

The New York Times

When an Algorithm Helps Send You to Prison

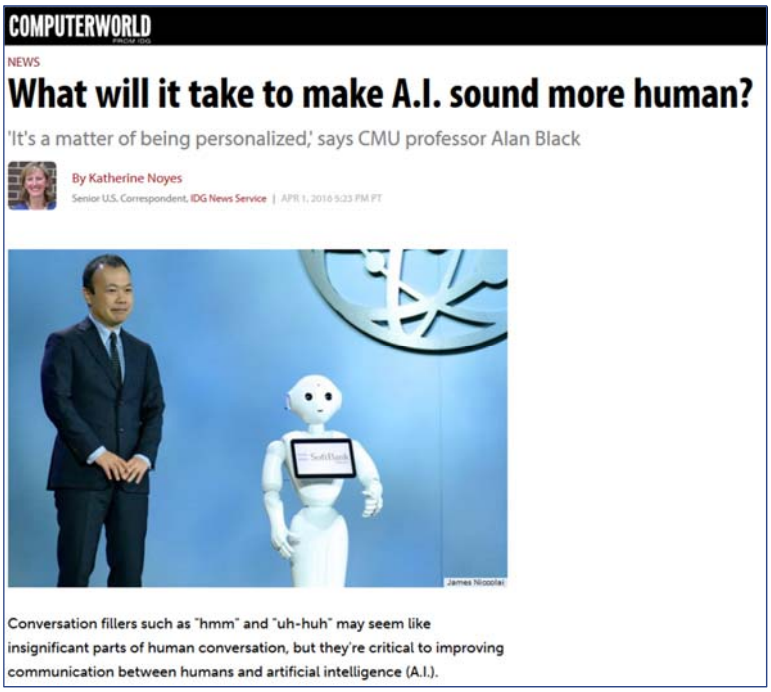
By Ellora Thadaney Israni

Oct. 26, 2017

In 2013, police officers in Wisconsin arrested a man driving a car that had been used in a recent shooting. The man, Eric Loomis, pleaded guilty to attempting to flee an officer, and no contest to operating a vehicle without the owner's consent. Neither of his crimes mandates prison time.

At Mr. Loomis's sentencing, the judge cited, among other factors, Mr. Loomis's high risk of recidivism as predicted by a computer program called COMPAS, a risk assessment algorithm used by the state of Wisconsin. The judge denied probation and prescribed an 11-year

Risiko „Verschwimmen von Grenzen“



COMPUTERWORLD

NEWS

What will it take to make A.I. sound more human?

'It's a matter of being personalized,' says CMU professor Alan Black

By Katherine Noyes

Senior U.S. Correspondent, IDG News Service | APR 1, 2016 5:23 PM PT

Conversation fillers such as "hmm" and "uh-huh" may seem like insignificant parts of human conversation, but they're critical to improving communication between humans and artificial intelligence (A.I.).

https://www.computerworld.com/article/3051174/big-data/what-will-it-take-to-make-ai-sound-more-human.html

Risiko „Verschwimmen von Grenzen“

COMPUTERWORLD

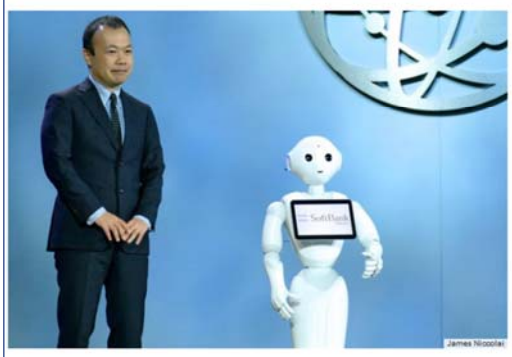
NEWS

What will it take to make A.I. sound more human?

'It's a matter of being personalized,' says CMU professor Alan Black

By Katherine Noyes

Senior U.S. Correspondent, IDG News Service | APR 1, 2016 5:23 PM PT



Conversation fillers such as "hmm" and "uh-huh" may seem like insignificant parts of human conversation, but they're critical to improving communication between humans and artificial intelligence (A.I.).

https://www.computerworld.com/article/3051174/big-data/what-will-it-take-to-make-ai-sound-more-human.html

Travis Korte @traviskorte — Folgen

We should make AI sound different from humans for the same reason we put a smelly additive in normally odorless natural gas.

Bridget Carey @BridgetCarey

I am genuinely bothered and disturbed at how morally wrong it is for the Google Assistant voice to act like a human and deceive other humans on the other line of a phone call, using upspeek and other quirks of language. "Hi um, do you have anything available on uh May 3?" #io18

Diesen Thread anzeigen

13:44 - 8. Mai 2018

769 Retweets **1.725** „Gefällt mir"-Angaben

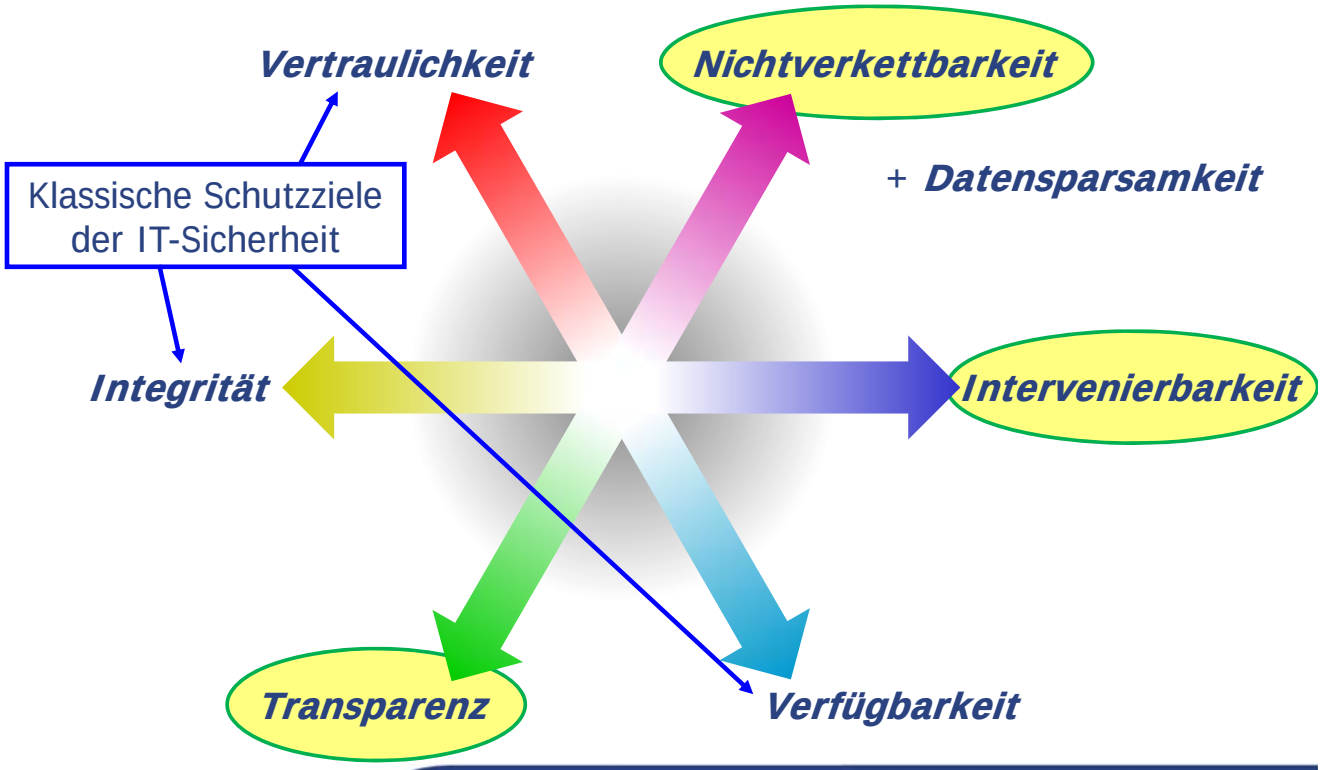
48 769 1,7 Tsd.

https://twitter.com/traviskorte/status/993954759932612608

Überblick

1. Begriffswelten Privacy & Datenschutz
2. Das Risiko nach der DSGVO
3. Schutzziele
4. Für KI?

Schutzziele im Standard-Datenschutzmodell



Überblick

1. Begriffswelten Privacy & Datenschutz
2. Das Risiko nach der DSGVO
3. Schutzziele
4. Für KI?

Wie? Datenschutz-Schutzziele implementieren

Nichtverkettbarkeit

Trennung von Domänen, Gewaltenteilung, Zweckbindung

Bild: ivanacoi via Pixabay

Transparenz

Ziel: Nachvollziehbarkeit & Überprüfbarkeit

Bild: geralt via Pixabay

z.B. (situationsgerecht): Widerspruch, Rechtsschutz, Rückabwicklung von Entscheidungen ...

Bild: geralt via Pixabay

Ziel: Risikobeherrschung –
Risiko für die Rechte und Freiheiten natürlicher Personen

Intervenierbarkeit

Vergleich mit Datenschutzgrundsätzen gem. Art. 5 DSGVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  (→ Rechtsgrundlagen, Nachvollziehbarkeit)
- Zweckbindung (→ festgelegte, eindeutige und legitime Zwecke)
- Datenminimierung (→ Begrenzung durch Zwecksetzung)
- Richtigkeit (→ Berichtigung/Löschung personenbezogener Daten)
- Speicherbegrenzung (→ Erforderlichkeit)
- Integrität und Vertraulichkeit (→ technisch-organisatorische Maßnahmen)

- Rechenschaftspflicht
  (→ Dokumentationspflicht)

- \+ Betroffenenrechte gem. Artt. 12-22

Artikel 22
Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Absatz 1 gilt nicht, wenn die Entscheidung
a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Transparenzanforderungen – wie weit?

In Artt. 13-15 DSGVO:

„das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.“

Bild: geralt via Pixabay

Datenschutz-Grundverordnung

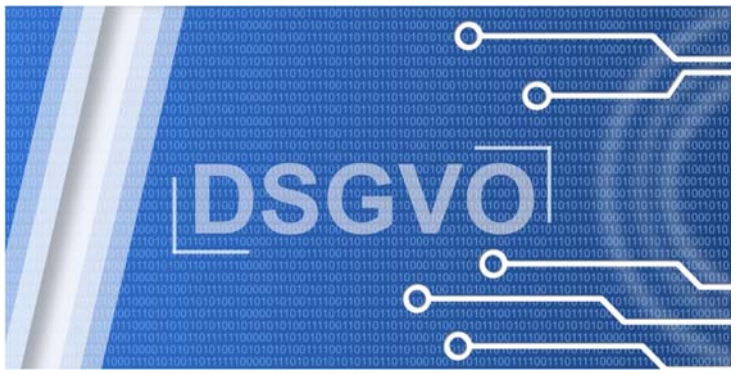
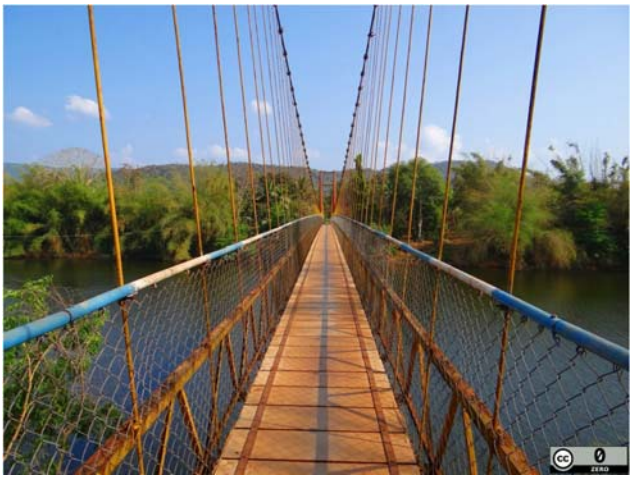


Bild: skylarvision via Pixabay

- Der Verantwortliche ist verantwortlich, Hersteller indirekt: Fehlentwicklungen vermeiden
- Ziel: Risikobeherrschung + Nachweis der Datenschutzkonformität
- Neue Anforderung: Datenschutz „by design“ & „by default“

Fazit: verantwortungsvolle Gestaltung



- Startpunkt „Datenschutz“
- Folgenabschätzung
- Risiken im Griff