CAMPUS
TAGE

www.campustage.org

2024
CAMPUS
TAGE

KI trifft auf Datenschutz Digitalstrategien

DSN Aka demie

KI-Software als digitale Endzeit?

Stefan R. Seiter | Senior Berater Datenschutz

www.dsn-group.de

Agenda

DSN Aka demie

1. Derzeitige Einsatzmöglichkeiten
2. Was Bären mit Datenschutz zu tun haben
3. Aktuelle und zukünftige Anforderungen
4. Richtigkeit von Daten und deren technische Umsetzung

1. Derzeitige Einsatzmöglichkeiten

Bilder, Texte & Videos

Beispiel: Bild

Beispiel: Video

→ SORA (von Anbieter OpenAI)

Beispiel: Musik

2. Datenschutz mit Bären

Für (kleine und große) Tierfreunde

Was ist echt und was nicht?

Sprichwort & Herleitung

Woher kommt´s ?

„Jemandem einen Bären aufbinden."

3. Aktuelle & zukünftige Anforderungen

Es grüßen DSGVO + KI-Verordnung

Art. 5 Abs. 1 lit. f DSGVO

Grundsätze der Verarbeitung

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder **unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität** und Vertraulichkeit").

Art. 5 Abs. 1 lit. f DSGVO

Grundsätze der Verarbeitung

Checkliste zur „Good Practice bei technischen und organisatorischen Maßnahmen nach Artikel 32 DSGVO"

Bayerische Landesamt für Datenschutzaufsicht (BayLDA), 2020

Auszug: Checkliste BayLDA

15 Kryptographie

Mittels kryptographischen Verfahren nach Stand der Technik kann die Vertraulichkeit, Integrität und Authentizität von Daten, Systemen und Entitäten sichergestellt werden.

- ☐ Regeln für die effektive Nutzung der Kryptographie, einschließlich der Schlüsselverwaltung, sollten definiert werden
- ☐ Mit Hash-Verfahren kann die Integrität von Daten, Software und IT-Systemen erreicht werden – Stand der Technik sind u. a SHA-256, SHA-512, SHA-3, bcrypt, Blowfish

Art. 50 Abs. 2 S. 1 KI-VO

Kennzeichnungspflicht

Anbieter von KI-Systemen, einschließlich KI-Systemen mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, stellen sicher, dass die Ergebnisse des KI-Systems **in einem maschinenlesbaren Format gekennzeichnet** und als künstlich erzeugt oder manipuliert erkennbar sind.

4.

Richtigkeit von Daten

… und deren technische Umsetzung

Maßnahmen bei Videos

Wie Sie Deepfakes erkennen

DAS **RÄT** DAS BUNDESAMT FÜR VERFASSUNGSSCHUTZ

Quelle: https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/deepfakes-2246064

Sorgen Sie für gute (Bild-)Qualität

Achten Sie auf die Mimik der Person

Prüfen Sie die Quelle

Ratschläge (I)

- **Sorgen Sie für gute (Bild-)Qualität**
  Je höher die Auflösung beziehungsweise die Bildgröße, desto leichter lassen sich Ungereimtheiten im Bild erkennen. Videos sollten daher nicht auf dem Handy, sondern auf einem größeren Monitor geschaut werden. Gute Farbeinstellungen zeigen ebenfalls Unstimmigkeiten, zum Beispiel im Hautbild.

Ratschläge (II)

- **Achten Sie auf die Mimik der Person**
  Natürliche Reaktionen, wie Blinzeln, Stirnrunzeln oder die berühmte „Zornesader" können von einer KI ebenfalls noch nicht gut dargestellt werden. Ein genauer Blick auf die Augen und Stirn kann einen Fälschung schnell enttarnen. Schauen Sie dafür das Bild verlangsamt, um eventuelle Verzerrungen zu erkennen.

Ratschläge (III)

- **Prüfen Sie die Quelle**
  Letztlich hilft natürlich auch immer eine Quellenprüfung oder bei Unsicherheit in Videoschalten die Bitte um Rückruf, um zumindest die Gelegenheit zu bekommen, den Videoanruf oder das Video zu verifizieren.

Maßnahmen bei Videos

Erläuterungen des BSI

„Mittels Methoden aus der *Medienforensik* ist es möglich, Artefakte zu detektieren, welche bei der Verwendung von Manipulations-methoden auftreten. Hiermit ist es *für Expertinnen und Experten* möglich, Fälschungen nachvollziehbar zu erkennen."

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

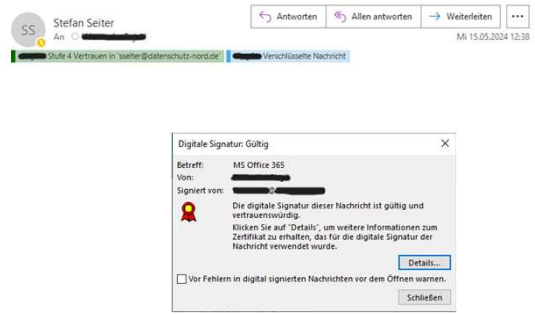
Beispiel: E-Mail

Mail-Server prüfen automatisch **Echtheit der Nachricht.**

Verwendung entweder „nur" als Signatur oder auch zur Inhalts-Verschlüsselung (S/MIME, PGP).

Keinerlei Interaktion der Benutzer*innen erforderlich.

Beispiel: E-Mail




Vielen Dank
für Ihre
Aufmerksamkeit!
Konsul-Smidt-Straße 88 • 28217 Bremen
T +49 (0) 421 69 66 32-298
Mail: akademie@dsn-group.de
https://www.dsn-group.de/dsn-akademie