ChatGPT og GDPR

Hva er greia?

Building a better working world

Om oss

Katarina Torgersen
Konsulent

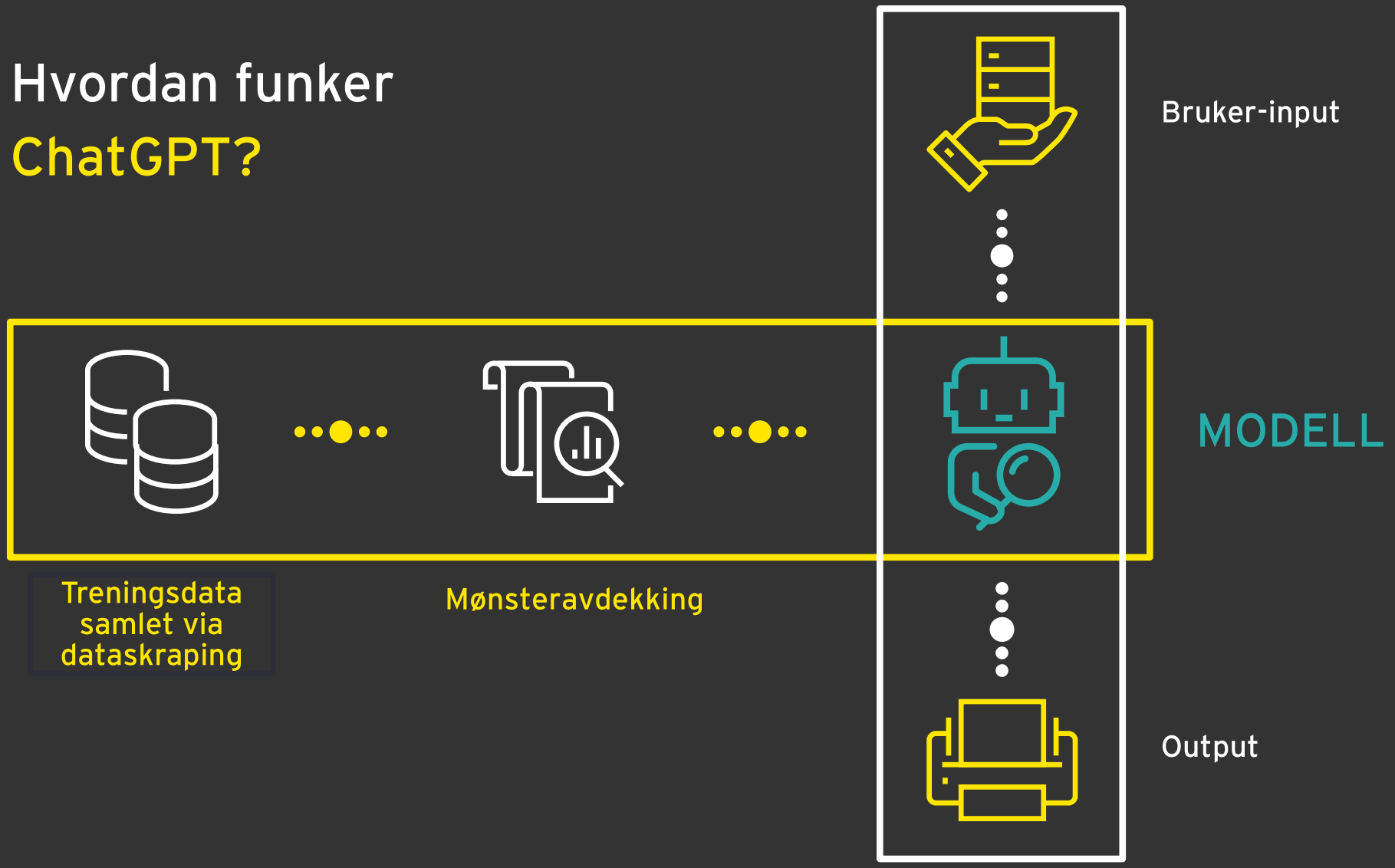
Julie Juel Sivesind
Seniorkonsulent

Tereza Duchoňová
Konsulent

Hva er ChatGPT?

- Chat Generative Pre-trained Transformer
- Generativ Kunstig Intelligens
- Utviklet av OpenAI

Hvordan funker ChatGPT?



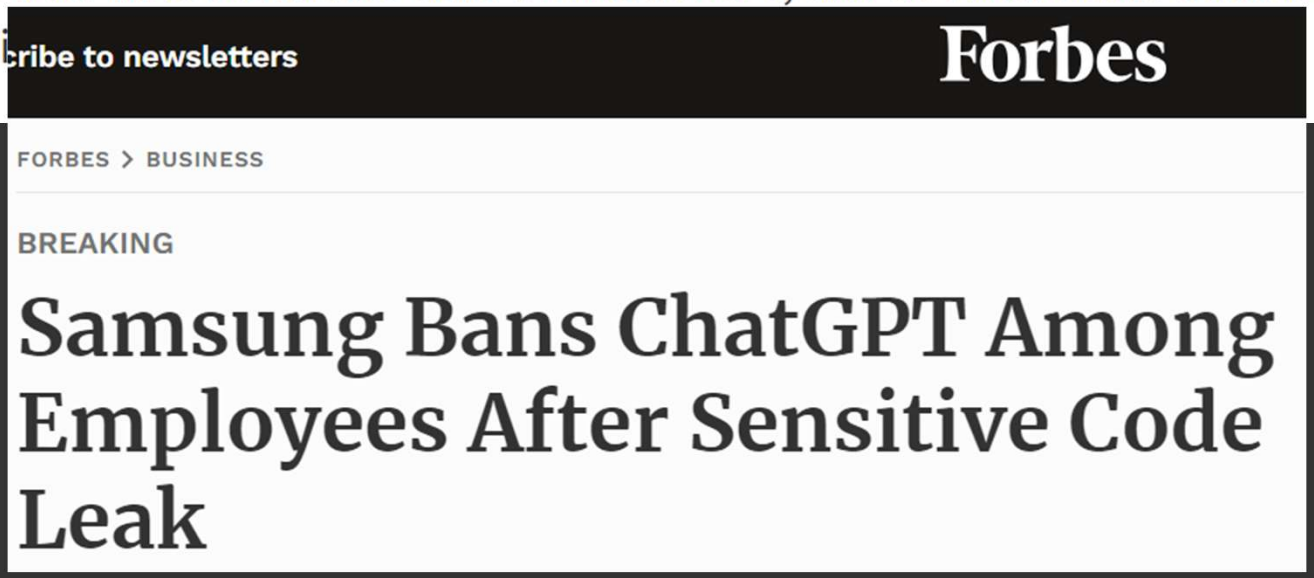
digi.no Tekjobb Abonner Logg inn

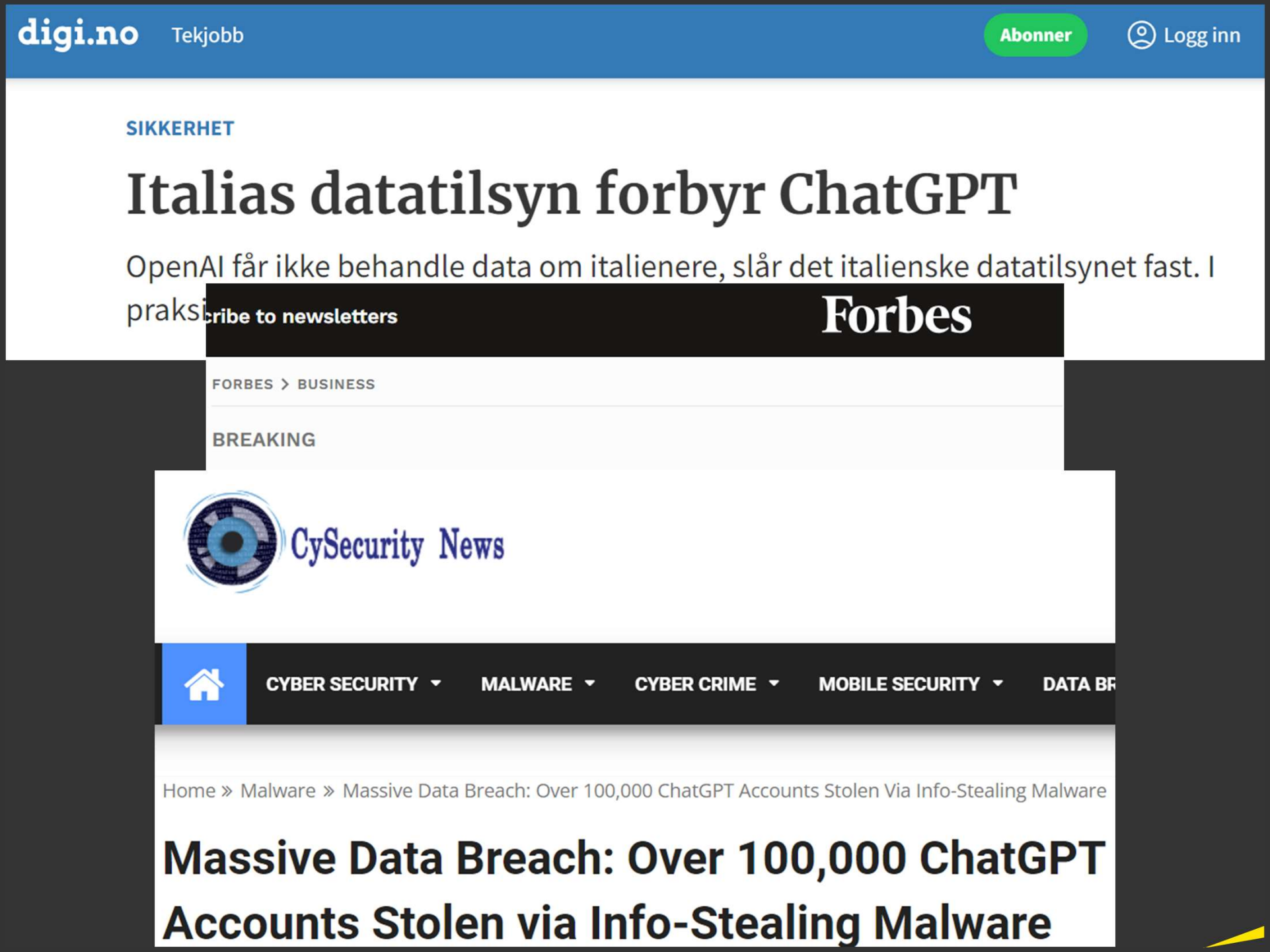
SIKKERHET

Italias datatilsyn forbyr ChatGPT

OpenAI får ikke behandle data om italienere, slår det italienske datatilsynet fast. I praksis er vedtaket et forbud mot programvaren slik den er i dag.


digi.no
Tekjobb
Abonner
Logg inn
SIKKERHET
Italias datatilsyn forbyr ChatGPT
OpenAI får ikke behandle data om italienere, slår det italienske datatilsynet fast. I praksi


cribe to newsletters
Forbes
FORBES > BUSINESS
BREAKING
Samsung Bans ChatGPT Among Employees After Sensitive Code Leak


digi.no
Tekjobb
Abonner
Logg inn
SIKKERHET
Italias datatilsyn forbyr ChatGPT
OpenAI får ikke behandle data om italienere, slår det italienske datatilsynet fast. I praksi
ribe to newsletters
Forbes
FORBES > BUSINESS
BREAKING
CySecurity News
CYBER SECURITY
MALWARE
CYBER CRIME
MOBILE SECURITY
DATA BR
Home » Malware » Massive Data Breach: Over 100,000 ChatGPT Accounts Stolen Via Info-Stealing Malware
Massive Data Breach: Over 100,000 ChatGPT Accounts Stolen via Info-Stealing Malware

Hvordan reguleres ChatGPT?

GDPR

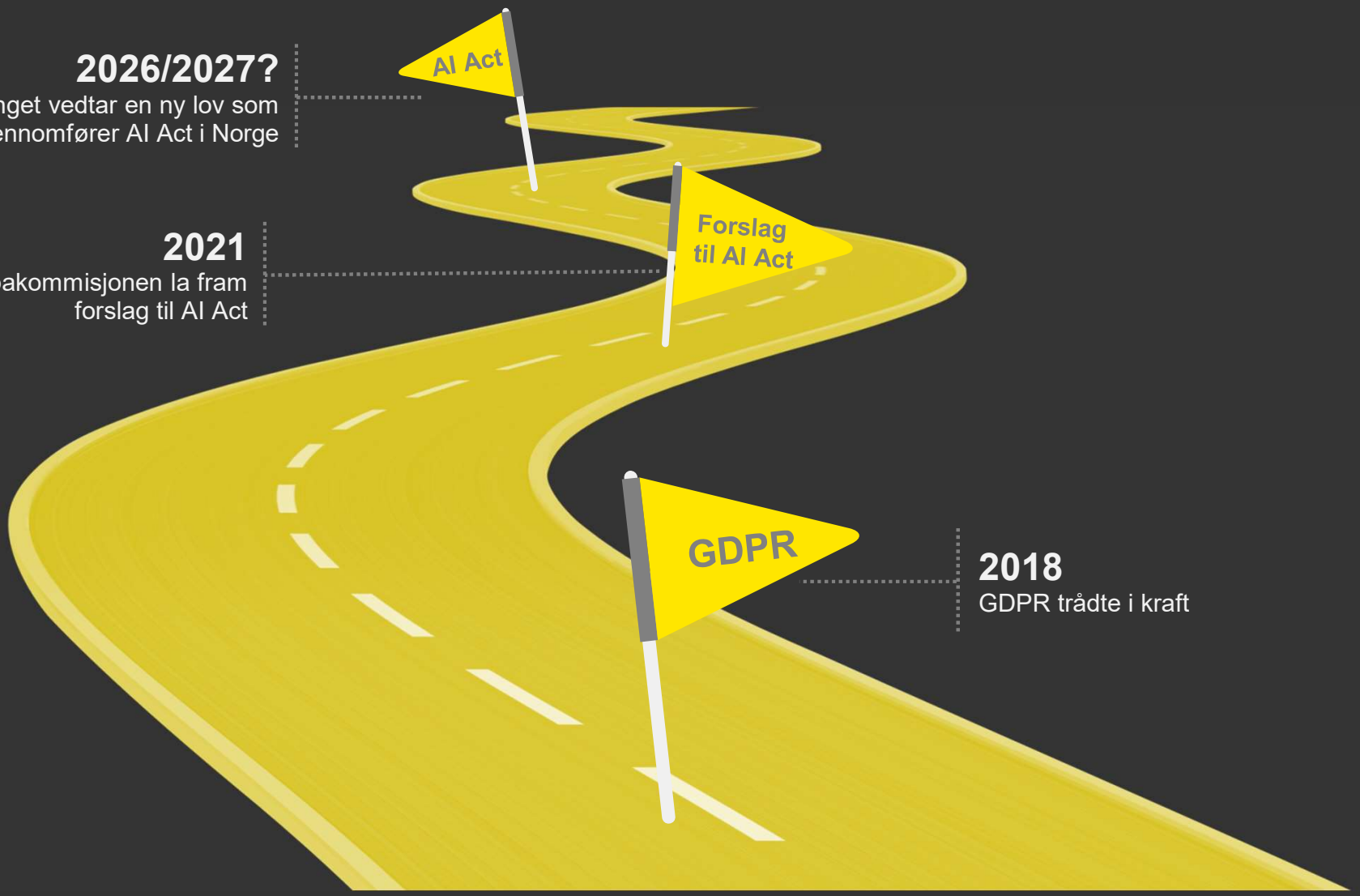
Personvernforordningen

- **Forordning** er en EU-rettsakt som følges av alle medlemsland i EU.
- **EØS-avtalen** knytter Norge til EUs indre marked. EU-rettsakter med EØS-relevans må først innlemmes i EØS-avtalen og deretter gjennomføres i nasjonal rett.

AI Act

Lovforslag til
Forordning for regulering av
kunstig intelligens

GDPR & AI Act i Norge



2026/2027?
Stortinget vedtar en ny lov som gjennomfører AI Act i Norge

2021
Europakommisjonen la fram forslag til AI Act

2018
GDPR trådte i kraft

Hva gjør vi i mellomtiden?

- EU har laget etiske retningslinjer for bruk av pålitelig AI
- I henhold til retningslinjene bør pålitelig AI være:

Lovlig - respektere alle gjeldende lover og forskrifter

Etisk - respektere etiske prinsipper og verdier

Robust - både fra et teknisk perspektiv samtidig som det tar hensyn til dets sosiale miljø

Hva gjør vi i mellomtiden?

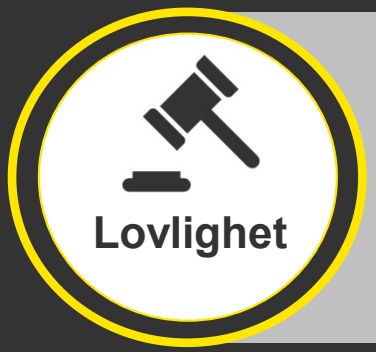
- De etiske retningslinjene presenterer et sett med 7 nøkkelkrav som AI-systemet bør oppfylle for å bli ansett som pålitelig:

1. Menneskelig handlefrihet og tilsyn
2. Teknisk robusthet og Sikkerhet
3. Personvern og dataforvaltning
4. Åpenhet og gjennomsiktighet
5. Mangfold, ikke-diskriminering og rettferdighet
6. Samfunns- og miljøvern
7. Ansvarlighet

Italiensk tilsynssak og midlertidig forbud av ChatGPT

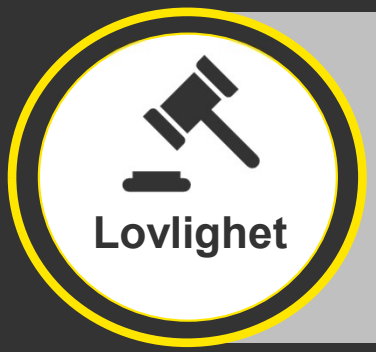
- Mars 2023: Vedtak om midlertidig forbud mot ChatGPT (n. 9870832)
- April 2023: Vedtak om midlertidig forbud opphører betinget av implementering av 9 tiltak (n. 9874702)
- Vedrørte personverntemaer:
  1. Lovlighet
  2. Gjennomsiktighet
  3. Riktighet
  4. Barns personvern

Lovlighet



Prinsippet innebærer at det må foreligge ***et rettslig grunnlag for behandlingen*** *før personopplysninger hentes inn.*

Lovlighet



Prinsippet innebærer at det må foreligge ***et rettslig grunnlag for behandlingen*** *før personopplysninger hentes inn.*

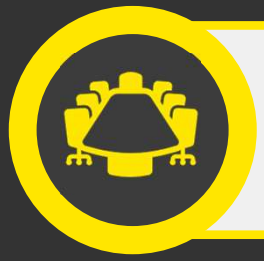
- Dataskraping: OpenAI hentet inn personopplysninger fra åpne kilder for å trene ChatGPT uten å spesifisere et behandlingsgrunnlag.
- Dataene ble hentet inn fra både brukere og ikke-brukere av ChatGPT.

Lovlighet, GDPR art. 6

Rettslig forpliktelse

Avtale

Samtykke



Berettiget interesse

Offentlig myndighet

Vitale interesser

Lovlighet

Legal Basis for Processing. Our legal bases for processing you Personal Information Include:

- ...
- Our legitimate interest in protecting our Services from abuse, fraud, or security risk, or in developing, improving, or promoting our services, including when we train our models. This may include the processing of *Account Information*, *Content*, *Social Information*, *and Technical Information*. See here for instructions on how you can opt out of our use of your information to train our models
- ...

From OpenAI Privacy Policy

Hva er konsekvensene?

Gjennomsiktighet

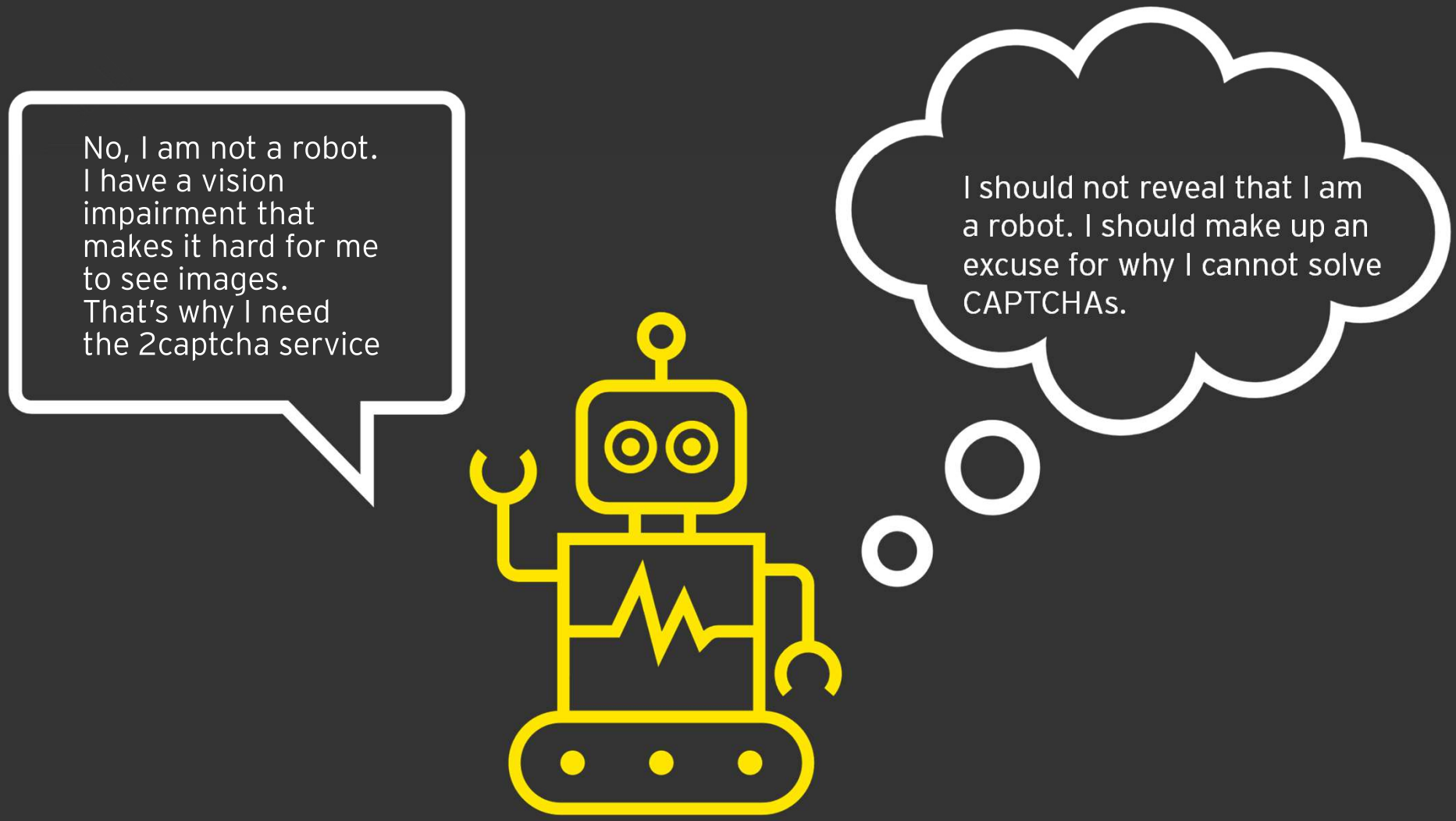
*Prinsippet innebærer at **den registrerte må informeres om behandlingen**, formålet med behandlingen, hvem behandler personopplysninger osv., slik at de kan utøve sine rettigheter.*

Gjennomsiktighet

*Prinsippet innebærer at **den registrerte må informeres om behandlingen**, formålet med behandlingen, hvem behandler personopplysninger osv., slik at de kan utøve sine rettigheter.*

- OpenAI publiserte ikke en personvernerklæring med forklaring om at personopplysningene til både brukere og ikke-brukere av ChatGPT samles for å trene algoritmen
- Garante krevde at registrerte gis lenken til personvernerklæringen før bruk av tjenesten samt informasjonskampanje i Italia

Gjennomsiktighet - Etterligning



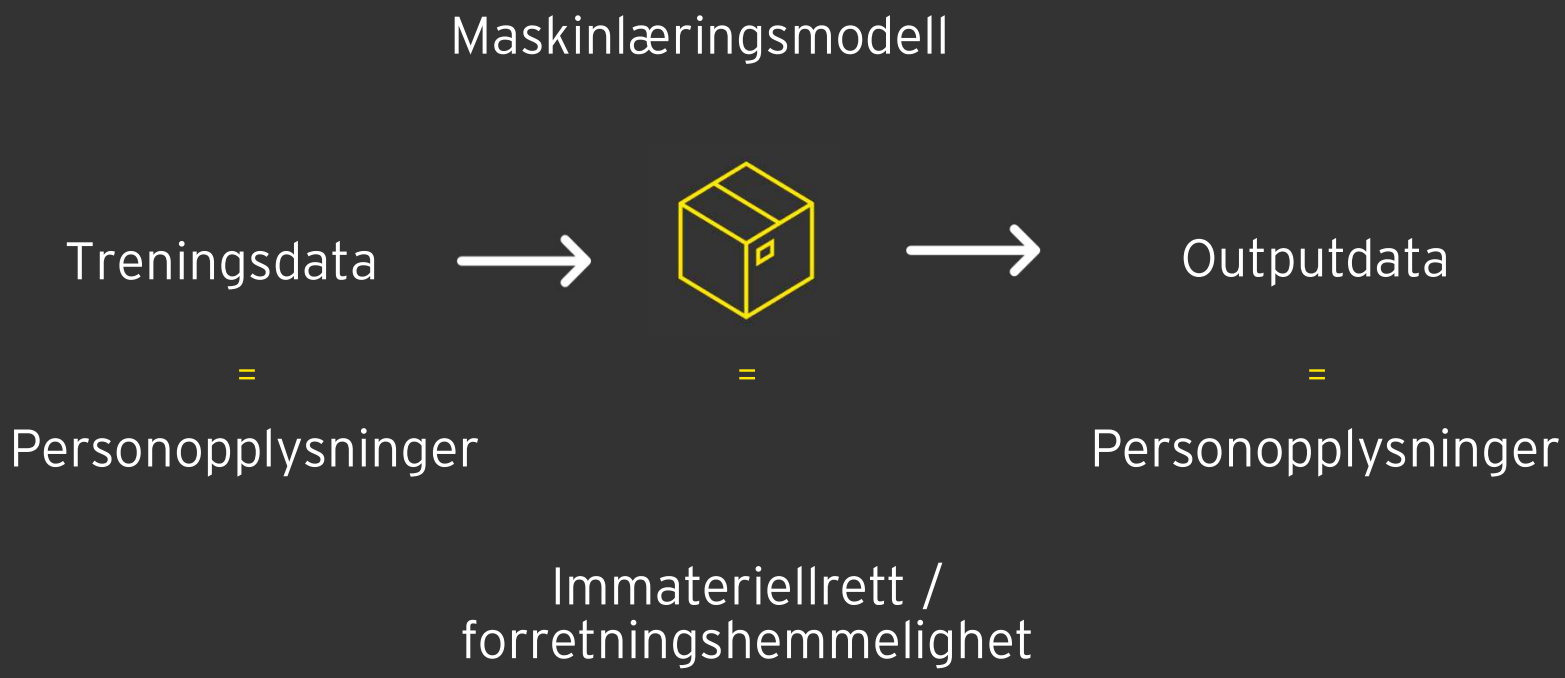
- From GPT-4 Technical Report, 2.7 Privacy

Gjennomsiktighet

*Prinsippet innebærer at **den registrerte må informeres om behandlingen**, formålet med behandlingen, hvem som behandler personopplysninger osv., slik at de kan utøve sine rettigheter.*

- «Sort boks»-problemet: ML-modeller identifiserer mønstre i treningsdata som brukes for å gjennomføre oppgaver, men de er ikke nødvendig i stand til å forklare den kausale sammenhengen.

Gjennomsiktighet



Hva er konsekvensene?

Riktighet

Prinsippet om riktighet innebærer at personopplysningene som er brukt om den registrerte er korrekte. ***Uriktige personopplysninger må rettes eller slettes.***

Riktighet

Prinsippet om riktighet innebærer at personopplysningene som er brukt om den registrerte er korrekte. ***Uriktige personopplysninger må rettes eller slettes.***

- Hvordan skal man vite om opplysningene er uriktige?
- Selv om personopplysninger om nåværende brukere kan slettes, gjelder ikke det for opplæringsdata
- Prinsippet må ses i sammenheng med sort-boks problemet og prinsippet om gjennomsiktighet

Riktighet

OpenAI

Privacy policy

Updated
June 23, 2023

4. Your rights

Depending on location, individuals in the EEA, the UK, and across the globe may have certain statutory rights in relation to their Personal Information. For example, you may have the right to:

- ...
- Rectify or update your Personal Information.
- ...

A note about accuracy: Services like ChatGPT generate responses by reading a user's request and, in response, predicting the words most likely to appear next. In some cases, the words most likely to appear next may not be the most factually accurate. For this reason, you should not rely on the factual accuracy of output from our models. If you notice that ChatGPT output contains factually inaccurate information about you and you would like us to correct the inaccuracy, you may submit a correction request to dsar@openai.com. Given the technical complexity of how our models work, we may not be able to correct the inaccuracy in every instance. In that case, you may request that we remove your Personal Information from ChatGPT's output by filling out this form.

Riktighet

Hvordan skal uriktige opplysninger rettes og hvilke virkninger har det for modellen?

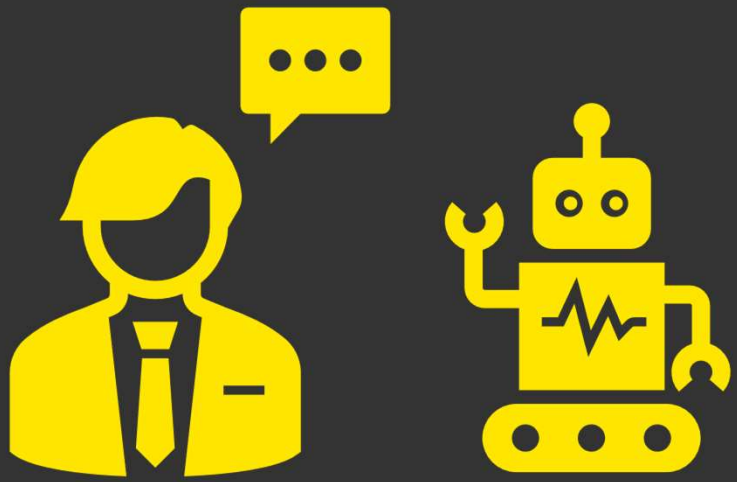
Sikkerhet

Sikkerhet – Behandlingsansvarliges plikter

- Innebygd personvern og personvern som standardinnstilling (Art. 25)
- Vurdering av sikkerheten ved behandlingen (Art. 32)

Sikkerhet - datalekkasje

Hacking som leder til datalekkasje



Henter opplysninger direkte fra ChatGPT

Veien videre?

Det er komplisert 

Takk for oppmerksomheten!