ChatGPT og personvern – hvorfor "mission impossible"?

Førsteamanuensis Malgorzata Cyndecka, PhD

Lærernes dag 2025

En utopi eller dystopi?

ernes
dag 2025

Hvorfor er personvern viktig?

- **«Right to be left alone»**

- **Den enkelte**
  - Menneskerettighet, selvbestemmelse, autonomi, tillit, misbruk, svindel, diskriminering,
- **Samfunnet**
  - Demokrati, ytringsfrihet, rettferdighet, bias, masseovervåkning.

Lærernes dag 2025

KI og personvern/GDPR

- KI v. personvernprinsippene:

- Big Data v. dataminimering
- «Black box» v. åpenhet (transparency)
- Bias i data og diskriminering v. riktighet
- Ny teknologi og nye formål med bruken av data v. formålsbegrensningsprinsippet

Lærernes dag 2025

ChatGPT/OpenAI og personvern

1. Har ChatGPT/OpenAI lov til å bruke våre personopplysninger?

2. Hva med våre rettigheter i møte med ChatGPT/OpenAI?

3. Hva gjør myndighetene (i EU/EØS og i Norge)?

4. Hva kan/bør JEG gjøre?

Lærernes dag 2025

1. Har ChatGPT/OpenAI lov til å bruke våre personopplysninger?

Hva er en personopplysning?

- Alle typer opplysninger
- Om en fysisk person
- Personen er indentifisert eller mulig å identifisere, enten direkte eller indirekte

Opplysning – kobling (direkte eller indirekte) – fysisk person

- **Objektive og subjektive**
- **Sanne og usanne – hallusinasjoner og deep fakes!**
- **Et svært vidt begrep!**

- **Anonyme personopplysninger v. KIs potensiale.**

Lærernes dag 2025

1. Har ChatGPT (OpenAI) lov til å bruke våre personopplysninger?

- Hvilke personopplysninger bruker den og når?

- Loggdata, bruksdata og stedsdata som IP-adresse, nettlesertype og -innstillinger, dato og klokkeslett for instruksen, tjenester, instrukser, informasjonskapsler og lignende teknologier for å bl.a. «forbedre opplevelsen din»

- Trening av algoritmer (inkludert pre-training)
- Interaksjon med bruker – prompts/instruks
- Videreutvikling av algoritmer
- Utlevering til tredjeparter, leverandører, myndigheter …

- Spør ChatGPT selv om den bruker personopplysninger!

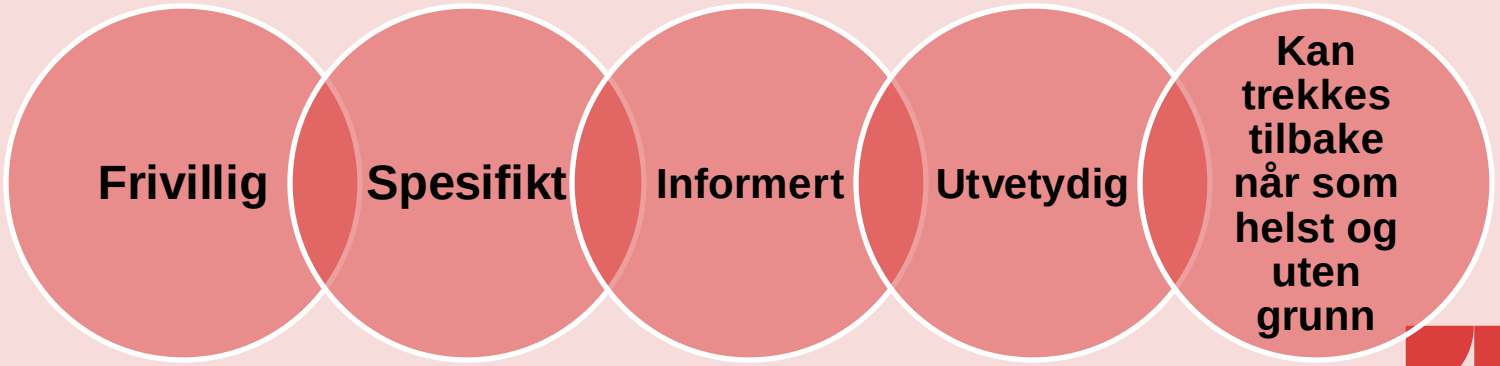
Lærernes dag 2025

1. Har ChatGPT/OpenAI lov til å bruke våre personopplysninger?

- Når er det lov å bruke personopplysninger etter GDPR?
- Behandlingsgrunnlag for alminnelige personopplysninger):
- Den registrerte samtykket til behandling av sine personopplysninger...
- Behandling er nødvendig for...
  - Avtale
  - Verne vitale interesser
  - Rettslig plikt
  - Oppgave i offentlig interesse, offentlig myndighet
  - Berettiget interesse.

Lærernes dag 2025

Hva kreves av LOVLIG samtykke?



Lærernes dag 2025

Berettiget interesse

*Behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den **behandlingsansvarlige** eller en **tredjepart,** med mindre **den registrertes** interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.*

- **Berettiget interesse (hva og hvem sin?)**
- De registrertes interesser og rettigheter
- **Balansetest som må dokumenteres!!**

Hva med sensitive personopplysninger?

- **I utgangspunktet FORBUDT å bruke informasjon om:** rase, etnisitet, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, biometri, helseopplysninger, genetiske opplysninger, seksuelle forhold og orientering
- **OpenAI nevner dem ikke i sin personvernerklæring!**
- Potensielle **unntak fra forbudet** om å behandle slike personopplysninger:
  - Eksplisitt samtykke
  - Personopplysninger vi åpenbart offentliggjorde selv
  - Viktige allmenne interesser.

Lærernes dag 2025

2. Hva med våre rettigheter?

Noen av rettigheter GDPR gir oss, dvs. de registrerte:

Rett til informasjon

Rett til innsyn

Rett til retting

Rett til sletting…

Lærernes dag 2025

3. Hva gjør myndighetene?

- Det italienske datatilsynet **Garante og OpenAI**
- Mars 2023 – **et midlertidig forbud**, snart opphevet
- **Dataskraping, mangel på behandlingsgrunnlag og åpenhet, aldersverifisering**
- Desember 2024 – **bot på €15 millioner**.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Lærernes dag 2025

3. Hva gjør myndighetene?

- **Datatilsynet**
- **Dataskraping:** et felles internasjonalt initiativ av datatilsyn https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2024/ny-global-uttalelse-om-ulovlig-dataskraping – Joint Statement av oktober 2024:
  - «Gode intensjoner» er **ikke nok**
  - Krav om å ha hjemmel til å bruke personopplysninger
  - Plikt til å **beskytte** mor dataskraping.

3. Hva gjør myndighetene?

- **Datatilsynet og NTNU**
- **Microsoft Copilot**
  https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2024/lansering-rapport-om-copilot/
- Svært krevende å kunne bruke den på lovlig vis
- Mulig i det hele tatt?
- Flere liknende vurderinger, f.eks. i Nederland.

3. Hva gjør myndighetene?

- **European Data Protection Board** – Personvernrådet
- Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models av 18. desember 2024: **3 spørsmål fra det irske datatilsynet**
- **1. Kan KI-modeler være anonyme?**
- **2. Hvordan lovlig bruke "berettiget interesse" for å utvikle KI-modeler?**
- **3. Hva hvis KI-modellen ble utviklet ved ulovlig bruk av personopplysninger?**

4. Hva kan/bør jeg gjøre?

- OpenAI lever av dataskraping – **ikke gi OpenAI og andre informasjon om deg selv og andre** (særlig barn!)
- Les personvernerklæringen (i hvert fall prøv…)
- Les hva du eventuelt samtykker til
- Må du opprette en bruker?
- Ikke oppgi sensitive opplysninger i instrukser!
- Ikke la deg spore av OpenAI og co – sjekk instillingene
- **Tenk på hva du bruker den til! F.eks. på jobb v. hjemme.**

Lærernes dag 2025

Lærernes dag 2025