Tech-juss oppdatering

august 2024

DFØ-rapport 2024:8 Både vaktbikkje og førerhund?

Direktoratet for forvaltning og økonomistyring (DFØ) har på oppdrag for Digitaliserings- og forvaltningsdepartementet evaluert Datatilsynet.

68 medarbeidere i N, 138 i S, 78 i DK Befolkning: N: 5,4 S: 10,4 DK: 5,9

	2015	2016	2017	2018	2019	2020	2021	2022	2023
Høringssvar	39	47	53	36	33	50	61	46	52
Tilsyn*								28	119
Saker**	1374	1745	1807	2654	3118	3271	3474	3519	4204
Meldte avvik	84	206	349	1275	1916	2008	2255	2250	2822

Tabell 2: Gjennomsnittlig saksbehandlingstid på klagesaker (kilde: årsrapporter)

	Norge	Sverige	Danmark
Saksbehandlingstid 2023 - dager	Ca. 365	101	85

Medarbeiderne i Datatilsynet er stolte av hva som er oppnådd i det internasjonale arbeidet. Det stilles i liten grad spørsmål ved ressursbruken, og inntrykket gjennom våre samtaler er at det er bred forståelse for at Datatilsynet prioriterer disse oppgavene.

Datatilsynets internasjonale engasjement har også blitt lagt merke til av våre eksterne informanter. Det blir stort sett oppfattet positivt og til dels imponerende. «Å bokse over egen vektklasse» er et uttrykk som går igjen, og som særlig knyttes til Datatilsynets håndtering av Meta-saken. Samtidig reiser noen spørsmål ved hva denne innsatsen går på bekostning av. En virksomhet som har mye kontakt med Datatilsynet, ordlegger seg på denne måten: *«De har jobbet veldig godt og metodisk med internasjonale saker. Disse sakene er veldig viktig internasjonalt, og har gjort at personvern har kommet på dagsorden. Spørsmålet er jo om de norske selskapenes behov har blitt liggende, og bør prioriteres opp»*.

- Datatilsynet som vaktbikkje og veileder: Datatilsynet bør fungere både som en kontrollerende vaktbikkje og en veiledende førerhund, og tilby mer **konkret og løsningsorientert veiledning**.

- **Ombudsrollen bør fjernes fra instruksen for Datatilsynet** og det bør heller legges vekt på den faglige rollen som premissgiver overfor departementene og faglig rådgiver til forvaltningen og allmennheten.

- Dialogbasert arbeidsform: Det anbefales at Datatilsynet tar i bruk en mer dialogbasert arbeidsform i tilsyn og veiledning, noe som krever **økt kapasitet og kompetanse.**

- Samarbeid for samfunnsutfordringer: Datatilsynet bør øke samarbeidet med andre myndigheter for å bidra til løsninger på store samfunnsutfordringer, som økonomisk kriminalitet og beskyttelse av sårbare grupper.

I en artikkel i Juridika uttaler førsteamanuensis Malgorzata Agnieszka Cyndecka ved Universitetet i Bergen følgende som illustrerer dette:

> «Vern av fysiske personer i forbindelse med behandling av personopplysninger er en grunnleggende rettighet, men det er på ingen måte en absolutt rettighet. Den må ses i lys av andre rettigheter og den må jo hele tiden balanseres mot andre rettigheter, verdier og interesser.»[3]

Noen av våre eksterne informanter mener at Datatilsynet gjør for lite for å finne løsninger på viktige samfunnsproblemer der hensynet til personvern hindrer deling av data. Eksempelvis etterlyser informanter fra *finanssektoren* større mulighet for deling av data mellom banker for å avdekke økonomisk svindel. De er bekymret for en sterk økning i digital økonomisk kriminalitet. Her er det i dag et tett samarbeid mellom politiet og finansnæringen, men de gir uttrykk for at de er avhengige av et samarbeid med Datatilsynet for å komme videre.

Flere av våre eksterne informanter er opptatt av digitalisering og deling av data. Her er det et ønske både om konkret veiledning og nødvendige avklaringer fra Datatilsynet. For å få på plass gode digitale tjenester på ulike samfunnsområder krever det også at Datatilsynet i større grad går inn i diskusjoner om hvordan personvernhensyn kan avveies andre samfunnshensyn.

- Tydeligere faglig rolle: Datatilsynet bør **styrke sin faglige rolle og bruke sin ekspertise til å påvirke både departementer og ulike sektorer**.

- **Ressursstyrking**: Det er behov for å styrke Datatilsynet ressursmessig for å håndtere økt oppgavemengde og forbedre veiledning og tilsyn.

- Effektivisering og styring: Samtidig som ressursene styrkes, må det stilles **krav til effektivisering** av arbeidet gjennom bedre styring og ledelse.

- For få tilsyn etter at GDPR kom?

Direktoratet for forvaltning og økonomistyring (DFØ) anbefaler å legge den nasjonale markedsovervåknings-/tilsynsfunksjonen og kontaktpunktrollen opp mot EU til Nasjonal kommunikasjonsmyndighet (Nkom).

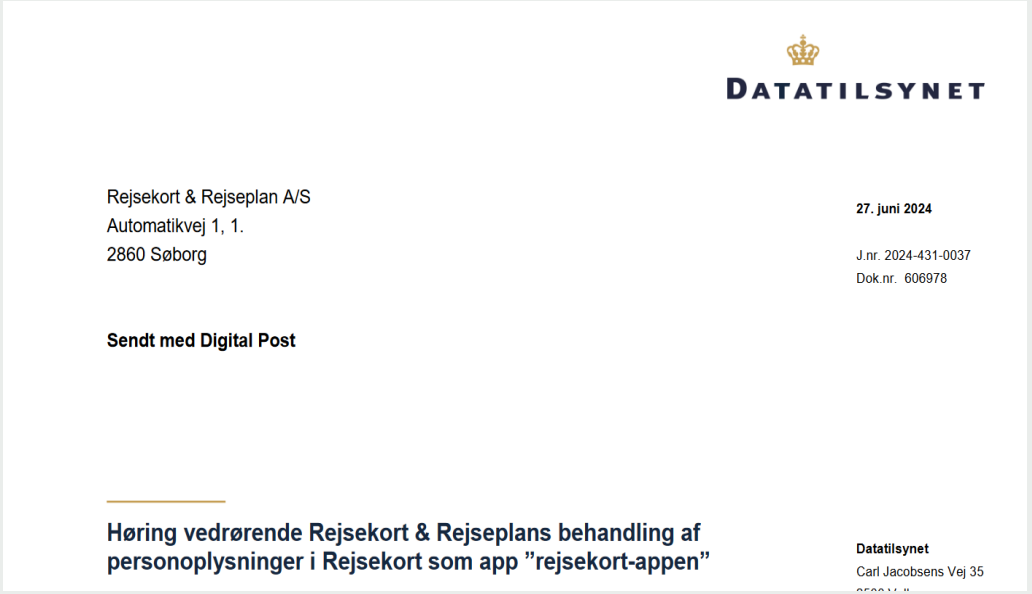
Dansk fokus på lokasjonsdata

Gransking pågår

Pay-as-you-go – løsning

- DPIA/personvernerklæring: skrev anonymisering av lokasjonsdata
- Viser seg å være pseudonymisering
- Lokasjonsdata anses sensitive – kan utlede «hverdag og vaner»
- Potensielt særlige kategorier – utlede «seksuell orientering eller religiøs overbevisning»

OK dataminimering?
OK lagringstid



DATATILSYNET

Rejsekort & Rejseplan A/S
Automatikvej 1, 1.
2860 Søborg

27. juni 2024

J.nr. 2024-431-0037
Dok.nr. 606978

Sendt med Digital Post

Høring vedrørende Rejsekort & Rejseplans behandling af personoplysninger i Rejsekort som app "rejsekort-appen"

Datatilsynet
Carl Jacobsens Vej 35

Ansiktsgjenkjenning

Amazon-KI-kameraer brukes til å overvåke og analysere passasjerers følelser

- Testet på åtte togstasjoner i England
- Registrerer alder, kjønn og **følelser**
- Kan forhindre konflikter eller nødsituasjoner

Maskinlæring brukes til å **oppdage farlige situasjoner og antisosial atferd**

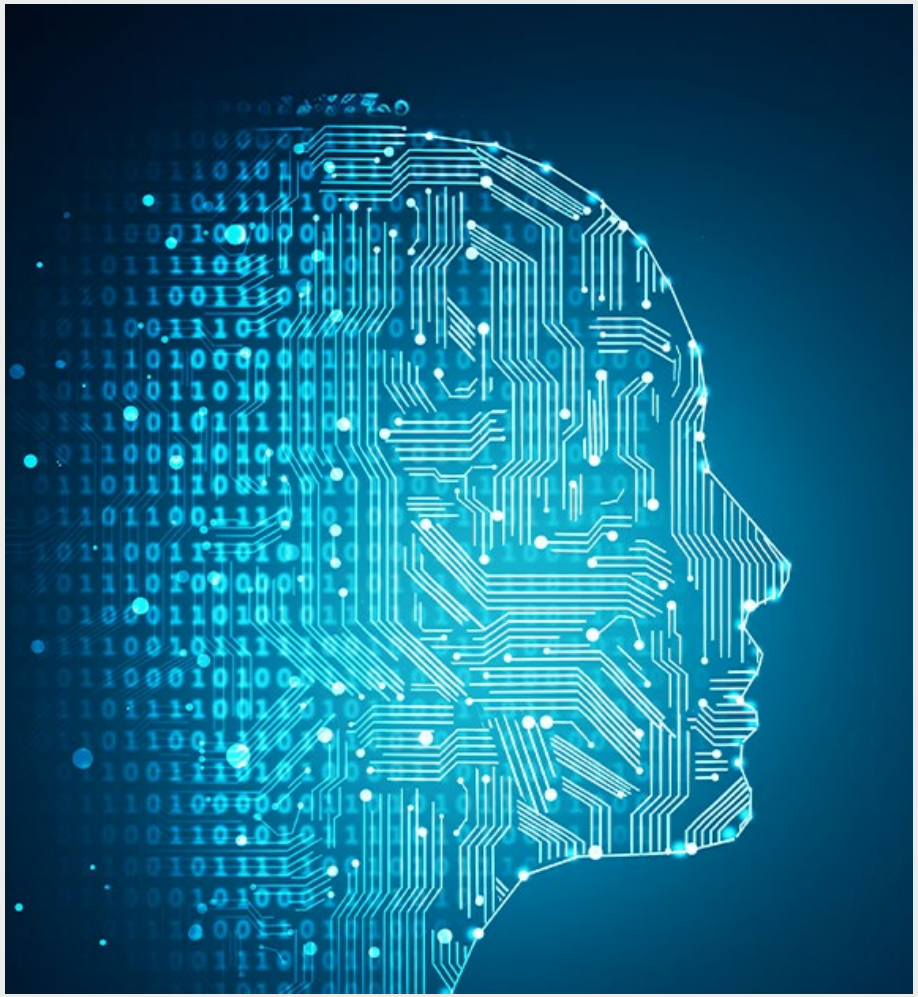
London Underground finner fordeler:

- Kan generere **sanntidsvarsler for billettfusk og andre regelbrudd**
- Ansiktsgjenkjenning kan **avsløre gjengangere**

Skeptisk om tillatt innenfor EØS

Nevrodata og “Brain Fingerprinting” – reproduksjon av tanker

- Veileder EDPS om nevroteknologier
  - Produkter som samler inn og behandler nevrale data
  - Velværeprodukter, underholdning, oppmerksomhetstrening og maskinstyring, medisin, markedsføring, sikkerhet, overvåkning av ansatte
- Hjernen: aktiv 24/7
- EDPS og Datatilsynet i Spania: Reproduksjon av tanker/hjerneaktivitet – helse - svært restriktive



Hjemmel for utvikling av KI

- Debatt om utviklingen av LLM-modeller
  - Samtykke vs berettiget interesse
  - Italienske datatilsynet og OpenAI's ChatGPT
  - EDPB Taskforce rapport
- Taskforcen:
  - **Mye om webscraping - tredjeparts data**
  - **Forskjell på førsteparter og tredjeparter**
- Norske datatilsynet og Meta – samtykke kreves
- Meta/Apple pauser utrulling av AI i Europa

Meta i Afrika

Nigerianske konkurranse- og forbrukervernmyndigheten gransket Facebook og Whatsapp

- Mange nigerianske brukere
- Personvernlov med **krav til personvernorganisasjon og rapportering**
- Bot på 220 000 000 amerikanske dollar

2 klager fra NOYB på Microsoft – juni 2024 – på vegne av 2 skolebarn i Østerrike

Far ville ha innsyn i hvordan barnets PO ble behandlet

- MS svarte at det var **skolen som var behandlingsansvarlig**
  - ikke helt usannsynlig - eleven har ikke direkte forbindelse med MS og det er skolen som har kjøpt inn programvaren
- Skolen: vi er **kun ansvarlig for elevens epostadresse**

- Uklar situasjon - NOYB skriver at brukervilkår og personvernerklæringer er en "labyrint«

- MS skal ha installert **informasjonskapsler som analyserer brukeratferd**, samler inn nettleserdata og brukes til reklame
- NOYB**: ulovlig profilering** - sannsynlig at selskapet sporer alle mindreårige som bruker deres utdanningsprodukter uten gyldig behandlingsgrunnlag

Ref Chromesaken i Danmark – Google endret vilkår

Innsynsbegjæringer i sikkerhetslogger

- Innsyn avskjæres ofte pga sikkerhet
- Innsynsbegjæring om hvem som hadde slått opp i folkeregieteret
- CJEU sak C-579/21: logg viser informasjon som den registrerte har krav på, så skal vedkommende få dette.
- Det betyr at man må se på hva loggen faktisk viser
- Aktuelt hvis den registrerte mistenker at vedkommendes opplysninger har vært gjenstand for et uautorisert søk

Tøffere tider for adtech – NOYB klager til Garante

Xandr - stort adtech selskap eid av Microsoft
- Real Time Bidding (RTB) plattform
- Beriker Xandr informasjonen? Kjøper de informasjon fra tredjeparter?

NOYB mener Xandr samler inn og deler store mengder personlige data
- Kan lage profiler, målrettet reklame
- Segmenter som tilbys: 'pregnant', 'lgbt', 'gender_equality', 'jewishfrench'

Xandr offentliggjør intern statistikk over hvordan de behandling av innsynsopplysninger
- **Oppgir at de aldri gir innsyn eller respekterer sletteanmodninger (!)**
- **Vet ikke hvem dataene gjelder**

NOYB har klaget Xandr inn for det italienske datatilsynet, Garante
- Kan resultere i en omfattende kartlegging av RTB'ene og Xandr

APRA - American Privacy Rights Act

Association of National Advertisers og American Association of Advertising Agencies:

- brev til representantenes hus og senatet – vil ha oppmyking
- raserer den moderne reklameindustrien
- ødelegger små og mellomstore bedrifter som er avhengige av reklame for å nå kundene
- fratar enkeltpersoner tilgang til produktene, tjenestene, informasjonen og ressursene de nyter og er avhengige av

Heritage Foundation's Tech Policy Center:

- roser APRA-utkastet for å «redusere insentiver for å misbruke amerikanske forbrukere»

Krav til consent bannere varierer – **oversikt fra NOYB**

DPA/Cookie Banner Question	EDPB Report	Austria	Belgium	Czech Republic	Denmark	Finland	France	German DSK (DPAs)	Greece	Ireland	Italy	Luxem-bourg	Nether-lands	Spain
Requires cookie reject option on first layer	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	✓	✓
Considers pre-ticked boxes illegal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Considers a link option to be misleading	✓	✓	?	✓	✓	?	✗	✗	✓	✓	✗	✓	?	✓
Agrees that no nudging through different button colours should occur	✓	✓	?	✗	✓	?	✗	✗	✓	✓	✗	✓	?	✓
Agrees that no nudging through button con-trast (compared to back-ground) should occur	✓	✓	?	✗	✓	?	✗	✗	✓	✓	✗	✓	?	✓
Relying on legitimate in-terest for installing non-essential cookies is illegal	✓	?	✓	✓	?	✓	?	✓	?	?	✓	?	?	✓
Wrong classification of cookies and therefore installing them without consent is an issue	✓	✓	✓	✓	?	✓	?	✓	?	✓	?	✓	✓	✓
Withdrawal is only per-missible through a per-manently visible floating icon	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

..Oversikten kan endres raskt

Tekster om personvern må være konsekvente

AQUAPHOTO: fototjenester med ansiktskjenning i lekepark

Nettsiden: besøkende vil bli fotografert ved å oppsøke fotografene – besøkende med barn kan bli fotografert med mindre de har et særlig tegn som viser at de ikke vil bli fotografert

Vilkårene fra AQUAPHOTO: ikke-fotografer tegn deles ut av parken eller fotografene. Informasjonsskilt ved kassen: "Ikke vær redd for AQUAPHOTO-fotografen. Du vil ikke bli fotografert i rødt. Grønne armbånd gir mange flotte bilder".

Selskapet mente de hadde innhentet samtykke – grønt armbånd for å bli fotografert, rødt armbånd for å unngå fotografering.

Datatilsynet: AQAPHOTOs fulgte ikke egne regler, ikke god nok informasjon, **det ble det tatt bilder i situasjoner der armbåndene ikke var synlig**, f eks i attraksjonen "Unique Tornado".

Datatilsynet: bot €1000

EU utsetter omstridt forslag om bakdører i chat-kommunikasjon

Forslaget begrunnes med å skulle hindre seksuelle overgrep mot barn (CSAM) ved å overvåke chatkommunikasjon

- Mye kritikk

Forslaget medfører at f eks WhatsApp og Signal må bygge inn en bakdør for tilgang

- Myndigheter kan skanne meldinger for materiale relatert til seksuelle overgrep mot barn
- **Men om et slikt skanningssystem bygges inn i en applikasjon, kan det brukes til andre formål også**
- **Nedkjølingseffekt**

EU kommisjonene skulle ha stemt over forslaget den 19. juni, men dette ble utsatt fordi det er så omstridt

- Det betyr ikke at forslaget ikke kommer opp igjen

KI på mobiltelefoner gir en rekke utfordringer – kommersielt stor betydning

Apple og OpenAI vil integrere ChatGPT i iphone, Ipad, mac

- Konkurranserettslige problemer, dominans for store teknologiselskaper (DMA)
- Bekymringer for tilgang til tredjepartsapper og personvern

«Siri» vil få tilgang til ChatGPT og brukernes meldinger og e-poster

Notes og Pages vil også få tilgang til ChatGPT 4

OpenAI skal ikke lagre data, IP-adresser skal være skjult

- **Diskusjon om dette er teknisk riktig**
- **Baseres på samtykke – men hvordan? – ved hver bruk av KI?**

- Utsetter innføring av tjenester i EU
- Kina tillater ikke Chatgpt

2 nye saker om erstatning for tort og svie

- Mange CJEU-saker viser at nasjonale domstoler synes området er komplisert

- Norske domstoler har vært tilbakeholdne med å be om avklaring fra EFTA-domstolen, sannsynlig endring nå etter rapport om EØS-medlemsskap

Sak 1 Applikasjon fra Scalable Capital hacket, brukeres personopplysninger ble tatt

CJEU:

- Formålet med artikkel 82 er kompenserende og ikke straffende
- Kriteriene for å vurdere erstatningen fastsettes av rettssystemet i hver medlemsstat
- Skade forårsaket av brudd på personopplysninger ikke er mindre betydningsfull enn fysisk skade
- Domstol kan gi en mindre erstatning hvis skaden ikke er alvorlig

- CJEU om begrepet "identitetstyveri", (fortalens punkt 75 og 85)
- Selve *tyveriet* av personopplysninger er ikke identitetstyveri
- Erstatning ikke bare der datatyveriet fører til identitetstyveri. Datatyveri i seg selv kan være tilstrekkelig.

https://curia.europa.eu/juris/document/document.jsf?text=&docid=287303&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9875513

Sak 2: Skattemelding med info om funksjonshemninger og religiøs tilhørighet ble sendt til feil adresse

Uklart om mottaker leste opplysningene

Registrerte ba om erstatning på 15 000 euro

CJEU:

Frykten en registrert opplever for mulig misbruk av personopplysningene, kan utgjøre "ikke-materiell skade« - viste til tidligere avgjørelser

"a person’s fear that his or her personal data have, as a result of an infringement of that regulation, **been disclosed to third parties, without it being possible to establish that that was in fact the case,** is sufficient to give rise to a right to compensation, provided that that fear, with its negative consequences, is duly proven.", se dommens punkt 36.

Kommentar om erstatning – gruppesøksmål

https://www.austenhays.com/claims/grindr-breach-of-privacy-investigation/

Grindr breach of privacy claim

Austen Hays is bringing a claim on behalf of thousands of Grindr users against Grindr for breaching data protection laws.
The claimants claim that Grindr shared users' personal and sensitive data for profit with third party advertising companies without their consent.

You car
details

Find out if you are eligible:

JOIN THE CLAIM

What are the steps involved in joining the claim?

› **Step 1:** Complete the questionnaire to see if you are eligible

If you used the free version of the app between 2018 and 2021 you may be entitled to up to £10,000 of compensation.

Ny svensk gjennomgang av personvernombudets rolle

Ombud med andre roller i virksomheten i tillegg til å være ombud - tilstrekkelig uavhengige?

Flere av virksomhetene unngikk kritikk eller bot selv om ombudet også hadde et visst ansvar for compliance, risiko/sikkerhet og jurist.

Västerbotten: **kritikk for å tillate at ombudet også er jurist sitter i ledelsen**

Örebro: **kritikk for å ikke gi ombudet tilstrekkelige ressurser (det var ikke ressurser nok til å kunne rapportere) og for ikke å ha rutiner som sikrer rapportering til øverste hold**

IMY er også opptatt av Meta – 15 mill i bot

Avanza Bank brukte Facebook pixel

Juni 2021: avviksmelding til IMY om feilaktig dataoverføring til FB i perioden fra 15. november 2019 til 2. juni 2021

To funksjoner i analyseverktøyet ble utilsiktet aktivert av banken

Overførte personnummer og økonomisk informasjon om lån og kontonummer– noen ganger i klartekst, **noen ganger i hashet format**

> **”Genom att funktionen AAM oavsiktligt aktiverats av banken kunde Meta-pixeln matcha de hashade uppgifterna med besökarnas beteende på webbplatsen för profilering. Detta gjorde det möjligt att få en mer detaljerad bild av besökarna.”**

IMY:

Ikke tilstrekkelige tekniske og organisatoriske tiltak

Tap av kontroll over denne type bankinformasjon er en høy risiko for de registrertes friheter og rettigheter.