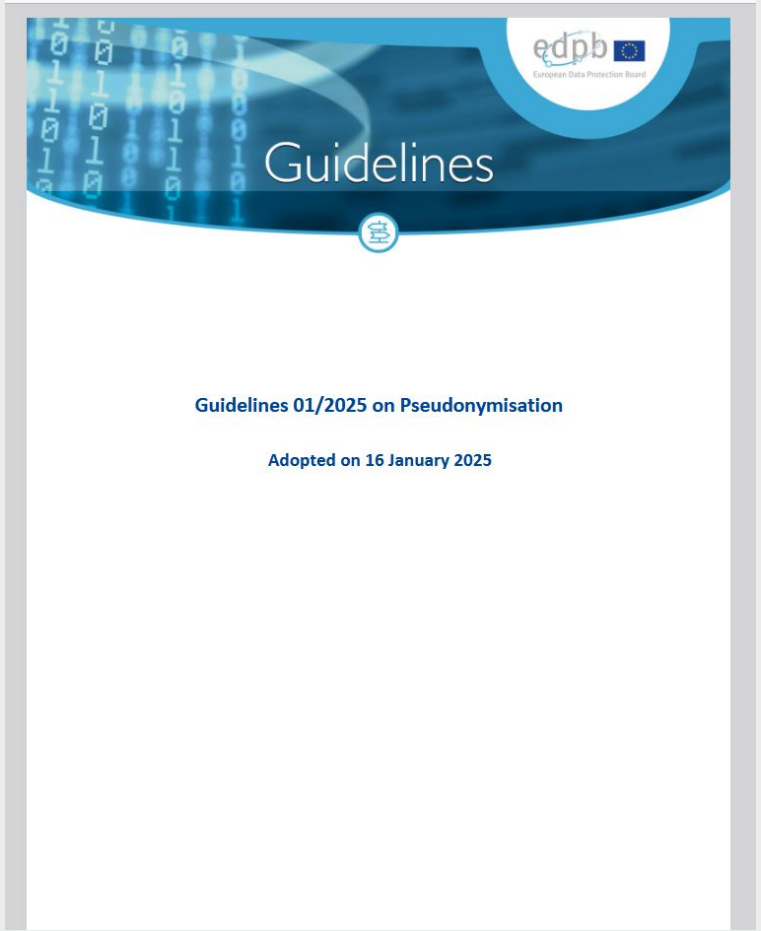
Oppdatering - personvern

For personvernnettverk i tilt – januar 2025

Nye saker - så cookies

Ny guideline om pseudonymisering

- GDPR defines the term ‘pseudonymisation’ for **the first time** in EU law
- Pseudonymised data, which could be attributed to a natural person by the use of additional information, **is to be considered information on an identifiable natural person**
- This **also holds true if pseudonymised data and additional information are not in the hands of the same person**
- Therefore, the processing of such data needs to comply with the GDPR
- Even if all additional information retained by the pseudonymizing controller has been erased, the pseudonymised data can be considered anonymous only if the conditions for anonymity are met – NY VEILEDER KOMMER
- Nytt begrep **“Pseudonimization domain**” – lag risikoanalyse for hvem som kan reidentifisere

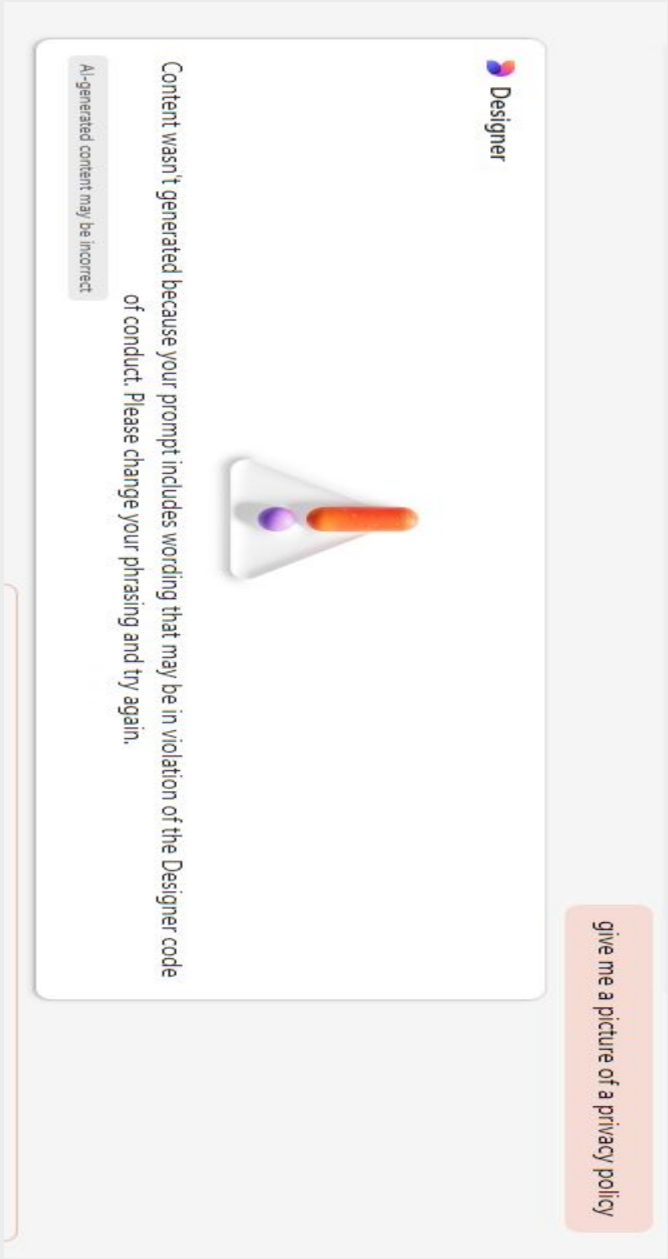


37. Additionally, the pseudonymising controller when defining the pseudonymisation domain may choose to include persons who are not legitimate recipients of the pseudonymised data, but may attempt to gain access to it anyway. The controller would do so in order to mitigate adverse effects of unauthorised access by those persons.

39. For effective pseudonymisation within a single organisational unit or a set of legitimate recipients, all involved controllers and processors should choose appropriate technical and organisational means—possibly including legal safeguards (e.g., contracts) if these can be effectively enforced—guaranteeing that pseudonymised data does not leave the pseudonymisation domain, which could lead to the circumvention of the protection afforded by pseudonymisation, see section 3.2.2.

Pass på innholdet personvernerklæringen din og svar ordentlig på innsynsbegjæringer!

- Netflix fikk en bot på 4,75 millioner euro for manglende samsvar mellom praksis og personvernerklæring
- Brukere må opprette konto, profiler over bruksmønster lages
- NOYB begjærte innsyn på vegne av 2 personer – ikke fornøyd med svar – klaget til datatilsynet i Østerrike – overført til Nederlandsk tilsyn



Konkrete feil

- Mangel på samsvar om formål og behandlinger i personvernpolicy og det de svarte til de registrerte/tilsynet, (listet opp 8 formål i svaret – var ikke slik i p. policy)
- P. policy oppga ikke HVILKE data de brukte for "sine tilbud, analyse av målgrupper og forebygging av svindel"
- Mangel på opplysninger om databehandlere
- Mangel på informasjon om brukere de hentet inn fra tredjeparter (!)
- Upresist om lagringstid – så lenge som «nødvendig», «loven pålegger» er ikke presist nok,
- Overføringer til tredjeland var ikke spesifisert, verken med hensyn til land eller sikkerhetsmekanismer

- Saken viser at tilsynsmyndigheter nå stiller strengere krav til presisjon i personvernerklæringer
- Tåler du at noyb leser personvernerklæringen din – på tide å presisere?

En prinsipiell dom om klagerett sak C-416/23

Bakgrunn

- CJEU vurderte om GDPRs regler for "overdrevne forespørsler" også gjelder klager til tilsynsmyndigheter
- Tilsynsmyndighetene får i artikkel 57 mulighet – som behandlingsansvarlig – til å avslå «anmodninger»
- Saken involverte en person som hadde sendt 77 klager på 20 måneder på at ulike behandlingsansavrlig ikek svart innen 1 måned

Hovedpunkter fra dommen

- Begrepet "forespørsel» (artikkel 57) inkluderer også klager (artikkel 77)
- Ingen fast tallgrense for hva som anses "overdreven". Misbrukende intensjon må vurderes
- Tilsyn kan velge mellom å kreve gebyr eller avslå klager, men valget må være hensiktsmessig og forholdsmessig

- Hvordan forholder det seg til norsk forvaltningslov??

Betydning

- Dommen styrker datatilsyns evne til å håndtere misbruk, samtidig som individets rettigheter ivaretas
- **Har overføringsverdi for behandlingsansvarliges rett til å avslå overdrevne anmodninger**

Nok en stor bot fra DPC – har du med det nødvendige i avviksmeldingen din?

- **Konkrete facts ikke kjent enda – kun pressemelding fra DPC**
- Dataangrep på Facebook eksponerte informasjon fra 29 millioner kontoer globalt (3 millioner i EØS) – sendte mangelfull avviksmelding
- Informasjonen inkluderte data som navn, epost, telefonnummer, religion, politiske syn og barns personopplysninger - profildata
- Bøter ilagt av DPC – koordinert med andre land som ikke hadde bemerkninger:
    - 8 mill. euro: Mangelfull informasjon i avviksmeldingen
    - 3 mill. euro: Manglende dokumentasjon av fakta, utbedringer slik at DPC kunne vurdere samsvar
    - 130 mill. euro: Manglende privacy by design i oppsett
    - 110 mill. euro: Brudd på minimumsprinsippet
- Avviksmeldinger må være fullstendige, dokumenterte og slik at tilsynsmyndigheter kan gjøre vurderinger
- ..to be continued..

Å be om tittel – eller ikke..

- Fransk jernbaneselskap SNCF krevde at kunder oppga tittel ("Monsieur" eller "Madame") ved billettkjøp på nett
- Foreningen Mousse mente dette brøt GDPRs prinsipp om dataminimering
- CNIL var ikke enig (!)
- CJEUs vurdering (2025):
    - Data må være relevante og nødvendige for formålet (dataminimering og proporsjonalitet)
    - Behandling av slike data for personalisering av kommunikasjon med kunde er ikke *nødvendig* for en transportavtale
    - Generiske og inkluderende uttrykk kan brukes som mindre inngripende alternativer
- Innsamling av kundedata må være objektivt uunnværlig for formålet

AI Act – coming to a place near you!

- Trer i kraft **2. februar** (EU):

  Forbud mot visse AI-systemer; sanksjoner på opptil 35 mill. euro eller 7 % av global omsetning

- Eksempler på forbudt AI:

  Sosial poenggiving av offentlige/private aktører

  Følelsesanalyse på arbeidsplasser og i utdanning

  Bruk av skrapede data for ansiktsgjenkjenning

  Profilering for å vurdere risiko for kriminell handling

  Biometriske systemer som utleder rase, religion eller seksuell orientering.

- Unntak:

  Tillatelse mulig for å beskytte betydelige offentlige interesser (f.eks. ansiktsgjenkjenning under OL i Paris 2024)

- Særlig utfordrende for arbeidslivet, hvor AI kan overvåke stemningsleie eller brukes i rekruttering – ref NTNU/Copilot/sandkassen
- EU veiledning om "forbudt AI" ventes snart

Mer ansiktsgjenkjenning tillatt i Danmark - Fotballklubben F.C. København

Klubben søkte om bruk av ansiktsgjenkjenning på fotballkamper

- matche ansiktsbilder fra videoovervåking med bilder av individer på interne og politiets suspensjonslister for å sikre orden
- Hjemmekamper, bortekamper, konserter på stadion

Datatilsynet har en egen hjemmel til å tillate slik i dansk i den danske databeskyttelsesloven §7(4) – desember 2024 – før AI Act

Datatilsynet:

- ansiktsgjenkjenningsdata er særlige kategorier av biometriske personopplysninger, i utgangspunktet forbudt
- unntaket om vesentlig allmenn interesse i 9(2)(g) kan få anvendelse slik det er implementert i databeskyttelsesloven § 7(4)
- ga tillatelse på klubbens kamper ved inngangene til Stadion, på stadion og ved mobile enheter i forbindelse med hjemme- og bortekamper
- ikke pt konkludert om det skal tillates for internasjonale fotballkamper/landskamper
- Ikke tillatelse for konserter - på søknadstidspunktet ikke utstedt noen suspensjoner i slike sammenhenger, ikke ansett proporsjonalt

Ny EDPS hvem og hva er det – og er det viktig?

- **EDPS** (European Data Protection Supervisor):
  - EU's personvernombud, fører tilsyn med hvordan europeiske myndigheter bruker personopplysninger
  - Utfører undersøkelser, f.eks. om personvern i Microsoft-tjenester
  - Gir innspill til nytt personvernregelverk fra EU
- **EDPB** (European Data Protection Board):
  - Utgir veiledere og koordinerer tilsynsmyndighetene i EU/EØS
- **Valg av ny EDPS:**
  - Nåværende EDPS: Wojciech Wiewiórowski, kjent som en grundig teoretiker
  - Mest aktuell motkandidat: Bruno Gencarelli, ledet forhandlingene med USA om DPF, anses som pragmatisk
  - Uenighet mellom EU-parlamentet og medlemsland om ny EDPS
- EDPS spiller en sentral rolle i utviklingen av europeisk personvernregelverk

Om rolleutøvelsen:

https://www.euractiv.com/section/tech/news/how-edps-wiewiorowski-lost-support-in-parliament/

Litt mer om hvorfor EDPS er viktig

- EDPS kritikk av Microsoft 365:
  - Microsoft anses som **behandlingsansvarlig** for data om brukeres/ansattes vaner/bruk av systemet, for stor adgang til **overføringer til tredjeland**
  - Pålagt EU-kommisjonen å endre kontrakten med MS for å sikre samsvar med **EUDPR (ikke GDPR, men veldig likt)**
  - **Hjemmesiden til EDPS har alle rapportene** i offentlig versjon (noe er unntatt) https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en

Litt mer om hvorfor EDPS er viktig

- Bekymringer i EU:
  - Ingen europeiske alternativer til Microsoft 365 – avhengighet av amerikanske selskaper
  - Priskonsekvens, migrasjonsvansker – forhandlingsproblemer (?)
  - MS **ikke godkjent for sensitive data** – påstås nedklassifisering foregår (!)
  - Mulig med europeiske alternativer??
- Tiltak og sanksjoner:
  - **EDPS pålegger kommisjonen å justere kontrakt innen 13/12-24** – forhandlinger skal pågå
  - Kommisjonen har motsatt seg EDPS, har saksøkt EDPS(!), men sendte dokumentasjon for samsvar i 10/12-24
  - EDPS gjennomgår materialet – to be continued..

Litt mer om overføring til tredjeland – artikkel 48

- EDPB har 3/12-24 publisert et utkast til retningslinjer for hvordan behandlingsansvarlige skal håndtere **krav** i dom/beslutning fra utland om overføring av personopplysninger til offentlige myndigheter i tredjeland
- Ikke helt uvanlig
- **Vilkår for overføring:**

  Overføring kan kun skje hvis det er en internasjonal avtale (f.eks. gjensidig rettshjelpsavtale) mellom EU/Norge og tredjelandet

  Artikkel 48 er **ikke** en egen overføringsmekanisme
- **Rettslig grunnlag:**

  Behandlingsansvarlig må finne både et grunnlag under artikkel 6 (f.eks. samtykke, kontrakt, rettslig forpliktelse HVIS gjensidig avtale) og et grunnlag for overføring under kapittel V i GDPR

  Berettiget interesser kan benyttes som behandlingsgrunnlag ved nødvendige avveininger
- Retningslinjene er på høring frem til slutten av januar 2025

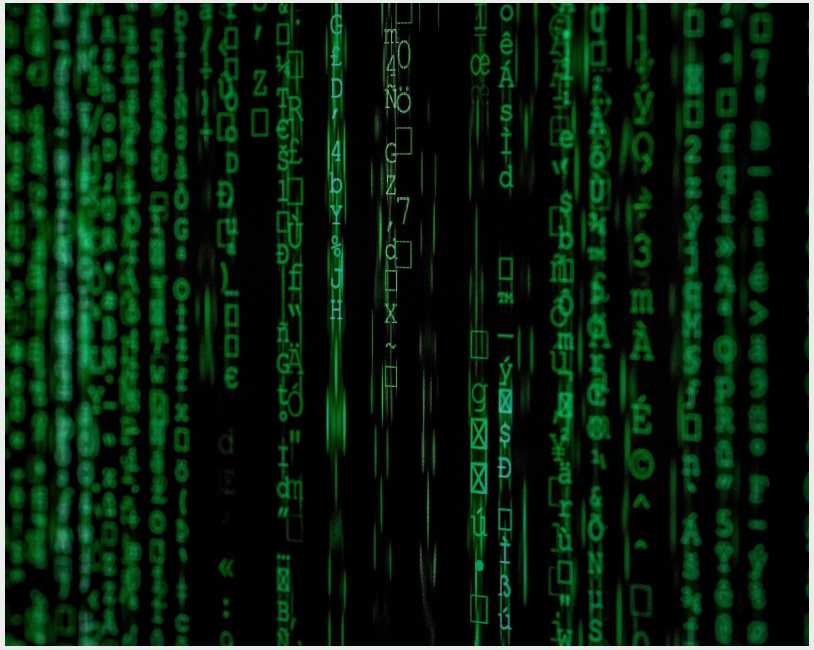
- Mest aktuelt for Saas-tjenester – og de med mange ansatte i mange land (?)

NOYB – nå også mot Kina

- **Kritikk fra NOYB:** NOYB har levert seks klager for ulovlig overføring av personopplysninger til Kina, med fokus på mangel på adekvansbeslutning for Kina og utilstrekkelig personvern i Kina
- Klager på TikTok (klage levert i Hellas), Xiaomi (klage levert i Hellas), Shein (klage levert i Italia), AliExpress (klage levert i Belgia), WeChat (klage levert i Nederland) og Temu (klage levert i Østerrike)
- Uklart hvorfor levert klage i disse landene..
- NOYB ber også datatilsynene om å beordre umiddelbar stans av overføringer til Kina samt at selskapene ilegges overtredelsesgebyr
- Klagene er tilgjengelige på NOYBs hjemmeside: https://noyb.eu/en/tiktok-aliexpress-shein-co-surrender-europeans-data-authoritarian-china

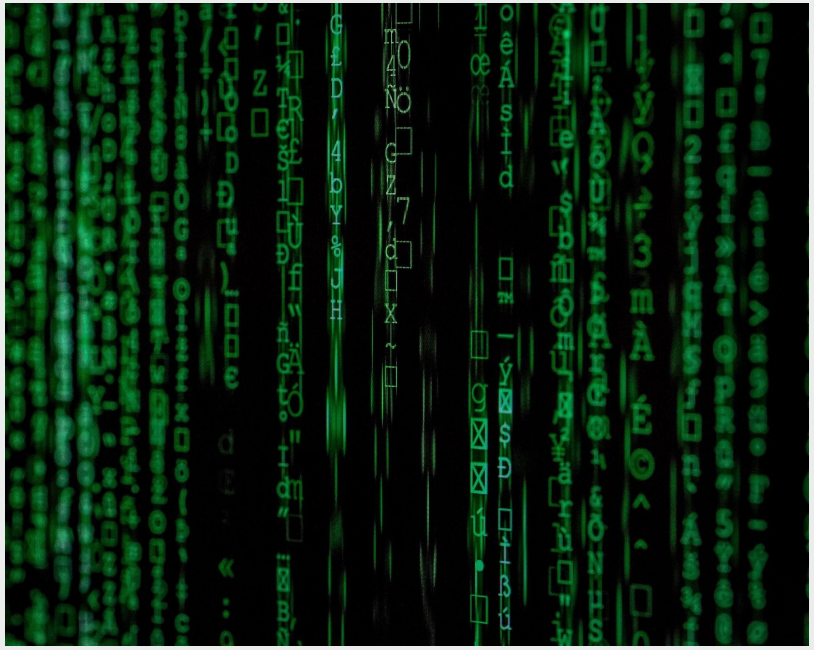
Nytt gebyr - 15 000 000 euro - til OpenAI fra Italia – og noen tanker om one stop shop

- Brudd på personvern (Mars 2023):
  - Feil i ChatGPT eksponerte brukeres chatter og persondata (navn, e-post, kredittkortinfo) for andre brukere
  - Det italienske datatilsynet, Garante, åpnet bredere undersøkelse
- One Stop Shop og italiensk myndighet:
  - OpenAI etablerte kontor i Irland i februar 2024, men bruddet skjedde før dette
  - Garante hadde myndighet over bruddet før etableringen i Irland, og One Stop Shop gjaldt ikke
  - At Meta varslet DPC tellet ikke
- Tautrekking om one-stop-shop
  - Virksomheter vil ha one-stop-shop – hindrer samtidig dialog med mange tilsyn – samordner gebyr
  - Tilsyn vil av og til ikke fordi de mister myndighet til Irland



Nytt gebyr til OpenAI fra Italia – og noen tanker om one stop shop

- Brudd på GDPR:
  - Behandlingen begynte «før» personvernerklæringen sa den gjorde det – **trening av modellen var «glemt»/utelatt** – behandlingsgrunnlag ikke identifisert – brudd på art 5 og 6
  - Mangel på informasjon for ikke-brukere (treningsdata) om behandlingene
  - Dårlig tilgjengelig personvernerklæring for brukere
  - Ingen i aldersverifisering for brukere mellom 13-18 år, selv om de må ha foreldrenes samtykke



  - Garante ilagt gebyr på €15 000 000 .. Samt…

Garante påla OpenAI å kjøre en informasjonskampanje på seks måneder for å øke åpenheten i behandlingen av personopplysninger

Kampanje i radio, TV, aviser og internett

Fokus på hvordan ChatGPT bruker personopplysninger, spesielt om innsamling av både bruker- og ikke-brukerdata for AI-modelltrening

Innholdet i kampanjen skal avtales nærmere med Garante

Ny ekomlov – cookies, men ikke bare

Ny ekomlov i kraft 1/1-25
§3-15 Bruk av informasjonskapsler mv.

Det er ikke tillatt å lagre eller å skaffe seg tilgang til opplysninger i sluttbrukers eller brukers kommunikasjonsutstyr uten at den aktuelle sluttbrukeren eller brukeren er informert om **blant annet** hvilke opplysninger som behandles, formålet med behandlingen og hvem som behandler opplysningene, og uten at den aktuelle sluttbrukeren eller brukeren har gitt samtykke. Samtykke skal oppfylle kravene til samtykke i personvernforordningen.

Første ledd gjelder ikke for teknisk lagring av eller adgang til opplysninger

a. utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett, eller

b. som er **strengt nødvendig** for å levere en informasjonssamfunnstjeneste etter den aktuelle sluttbrukerens eller brukerens uttrykkelige forespørsel.

Departementet kan gi forskrift om plikten etter første ledd, herunder om bruken av informasjonskapsler. Departementet kan gi forskrift om unntak etter andre ledd.

§3-15 handler om å «sette» cookies

..å lagre ELLER skaffe seg tilgang..
(tilgang - uavhengig av om opplysninger faktisk innhentes eller ikke?)

Datatilsynet – dette er ulovlig når samtykke mangler:

- innhenting/mellomlagring av data før man har samtykkesignal
- data samles inn, men merkes med "no consent/do not use"

Datatilsynet er tydelig på at setting av cookies krever samtykke, selv ved kort lagring av innhentede data

NKOM har myndighet over hvilke teknologier/cookies/trackere som anses strengt nødvendige

Ekom gjelder mer enn personopplysninger
NKOM ikke et «uavhengig organ» slik Datatilsynet er

Datatilsynet har myndighet over samtykkekravene og informasjonskravene

- Datatilsynet kommer med en egen veileder om cookies. Høres ut som om det kan ta litt tid pga de orienterer seg om behovet nå

- Tolkning av «strengt nødvendig» cookie er snever – **sikre kommunikasjon**
    - NKOM: strengere enn før – ingen utvidende tolkning
    - Gamle WP-29 veiledere er relevante
    - Ikke telle antall besøkende, ref forarbeidene
    - De er tydelige på at ikke bare «cookies» omfattes – men også scripts og annen teknologi – «serverside» løsninger

Utforming

- Avslag på alle samtykkebaserte cookies – i første lag, ikke annet lag
- Gjelder Datatilsynets myndighetsområde – liten tvil om hva de vil mene
- Mye praksis fra Europa
- Unngå manipulativ design – pass på font, farge, størrelse

Hva skal man informere om for å få gyldig samtykke?

Listen over informasjon som må gis ihht ekoml §3-15 er ikke uttømmende (jf "blant annet")

Hvor gis informasjon? Førstelag / annet lag / cookieerklæring

- Formålet for hver eneste cookie (ref overskriften i bestemmelsen) (med mindre veldig likt) og brukeren **skal kunne velge/nekte hvert formål** (mao kan cookies med samme formål antakelig bundles – men informasjon må gis)
- Hvilke opplysninger hver cookie samler inn
- Hvem som behandler opplysningene – databehandlere
- Varighet for cookien – se neste slide

Hvis "veldig like" cookies fra samme leverandør – så kan man kanskje gjøre et utvalg i hvilke man informerer om

Varighet av cookies må informeres om
– var vanlig før – står ikke i ordlyden nå heller

Forarbeidene peker på at prinsippene i Planet 49-saken gjelder - forarbeidene skriver:

Domstolen kom også til at kravet om at bruker skal få klare og omfattende opplysninger, blant annet om formålet med behandlingen, innebærer at brukeren skal være i stand til å enkelt kunne forstå konsekvensene av samtykket. Dette omfatter opplysninger om varigheten av informasjonskapselens funksjon og om tredjemanns mulighet til å få adgang til informasjonskapselen.

Informasjonskravet gjelder ikke for cookies som er strengt nødvendige

Likevel anbefaler Datatilsynet at det gis noe informasjon om slike cookies, selv om de ikke spesifiserte hva denne informasjonen bør inneholde

(De kan antakelig ikke håndheve anbefalingen)

Om multipurpose cookies

Noen sporingsteknologier brukes til strengt nødvendige formål

– og **samtidig** til alt fra analyse, tjenesteutvikling og ads

- De samler inn både strengt nødvendig informasjon (a,b,c)
- Og f eks analyse-fokusert informasjon – hvor mange besøkte siden (d,e,f)
- Og f eks tjenesteutviklingsinformasjon - hva er populært (g,h,i,j,k)
- Og alt som trengs for å lage rettet reklame – bruksmønster, tid på side (l,m – æ,ø,å)

- Hva om bruker samtykker til ingenting utover strengt nødvendige?
- Eller om bruker ikke samtykker til ads – men til tjenesteutvikling?

- Ofte kan cookien ikke håndtere det, men samler inn alt uansett
    - og i ulik grad kaster/sletter innsamlet informasjon eller kommuniserer videre (om den deles) at informasjonen ikke skal bruke («do not use-signal»)

Om multipurpose cookies

Datatilsynet: Det må foreligge samtykke til alle formål som ikke er strengt nødvendige

Om det ikke er behandlingsgrunnlag for alle formål, kan ikke cookies'en settes

- **Ei heller for datapunktene som er strengt nødvendige – fordi alt samles inn/lagres (selv om det kanskje ikke brukes)**

Datatilsyn og NKOM mener at om dette er vanskelig pga eksisterende teknologi, så bør den utvikles slik at kravet kan overholdes

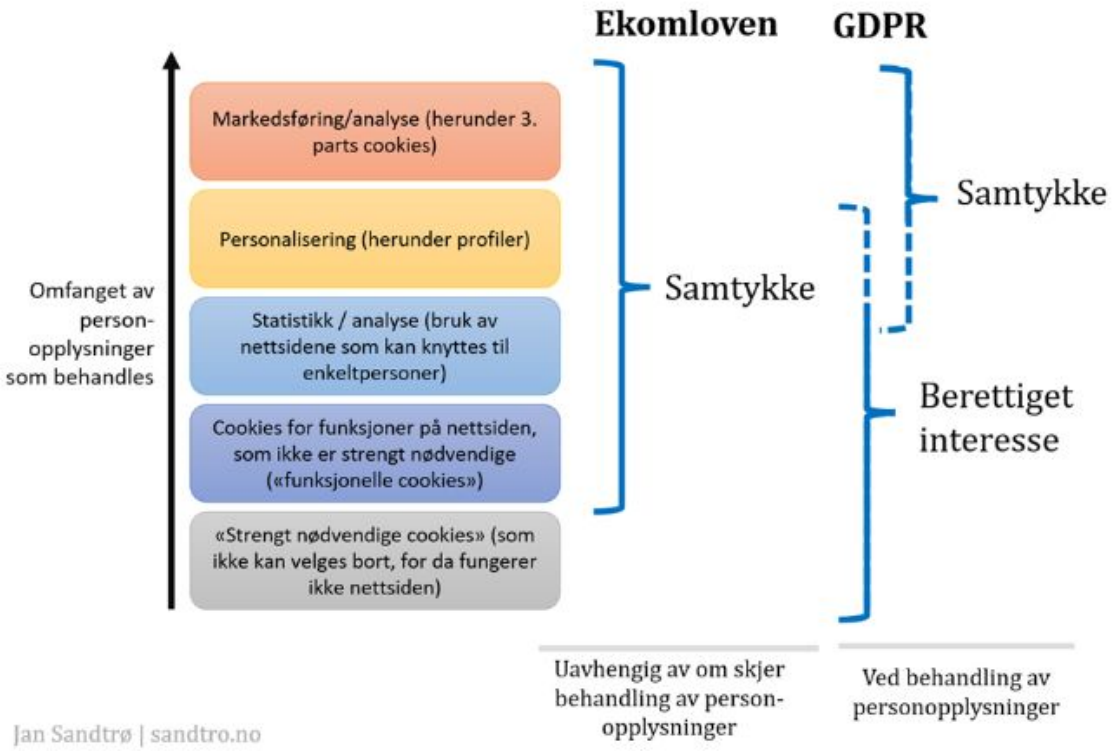
- En del forvirring, spørsmål på LI: Kan man sette cookie basert på berettiget interesse?? Nei.

- **Skille å «sette cookie» ekom - og etterfølgende bruk av lovlige innhentede opplysninger fra Cookie - GDPR**

Fra Jan Sandtrøs LI-side

Han justerer dette i neste utgave

For cookies som behandler personopplysninger, så kreves det samtykke for noen cookies, mens for andre kan det være nok med grunnlag i berettiget interesse avhengig av hvilke personopplysninger som behandles, se illustrasjon nedenfor. Her er det ingen endringer med ny ekomlov, siden den gjelder kun settingen av selve cookiene. For behandling av personopplysninger som samles inn ved bruk av cookies, gjelder personvernregelverket (som GDPR) som for all behandling av personopplysninger.



Illustrasjonen viser at det må innhentes samtykke for alt utenom «strengt nødvendige cookies», men der hvor det behandles personopplysninger kan man enten benytte seg av samtykke eller berettiget interesse avhengig av hvor omfattende personopplysninger som samles inn og/eller hvor inngripende opplysningene er.

Schjødt

Oslo Stockholm Copenhagen London Stavanger Bergen Ålesund