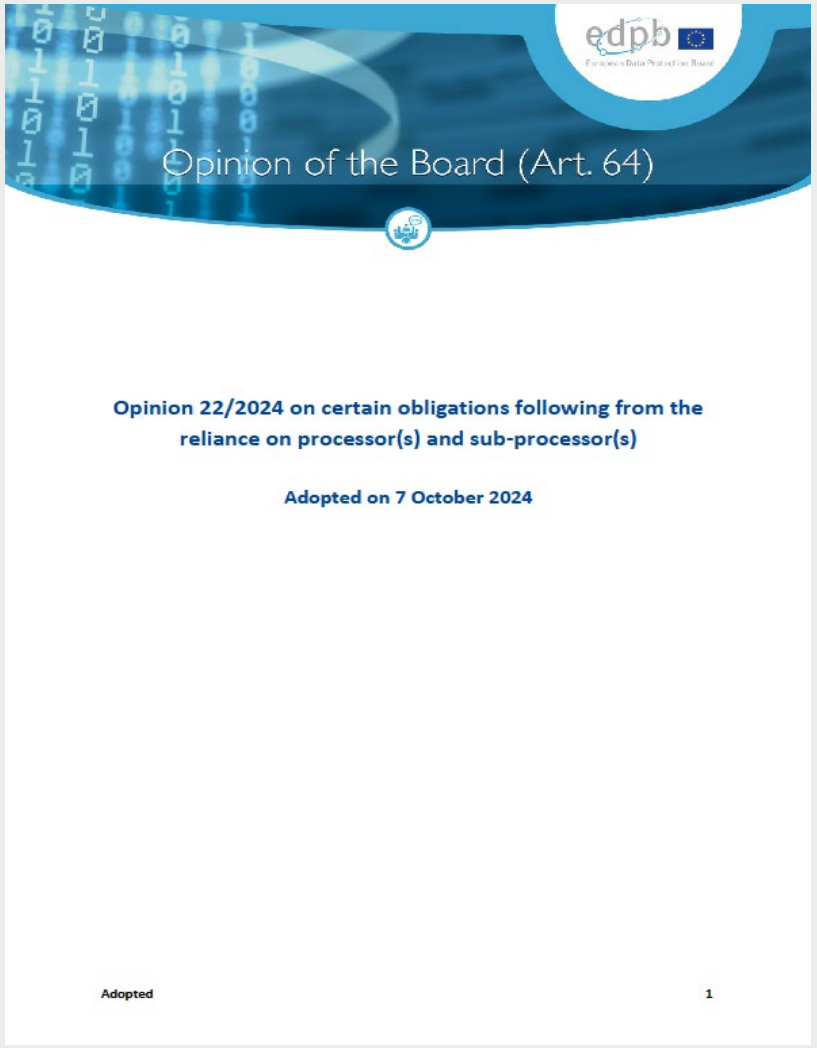
Oppdatering - personvern

For personvernnettverk i tilt - desember 2024

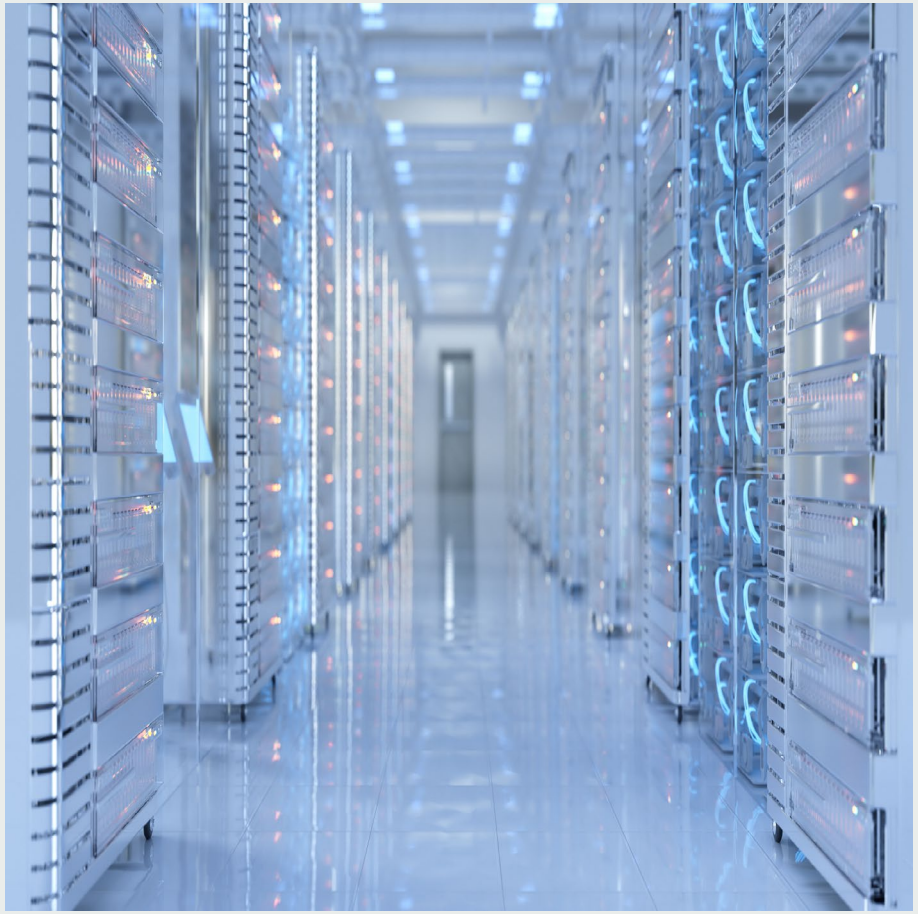
De store tingene først

Guidelines og sentrale opinions – samt ny norsk lov og en sandkasse


edpb
Opinion of the Board (Art. 64)
Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)
Adopted on 7 October 2024
Adopted
1

EDPBs opinion om databehandlere – art 64(2) kvasi-bindende

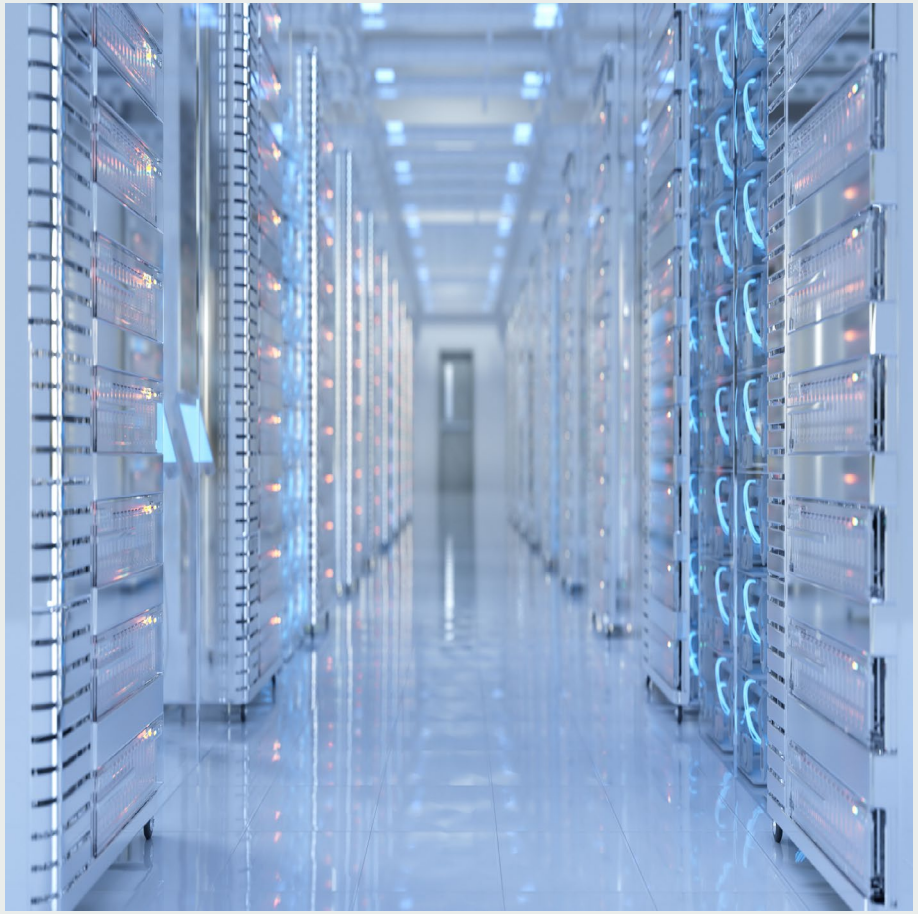
- **Bakgrunn:** Komplekse databehandler-strukturer for skytjenester. Anmodning fra dansk DT
- Ha detaljert oversikt over alle databehandlere og underdatabehandlere «**regardless of risk**»
  - Navn, adresse, kontaktperson
- Databehandlere må sørge for å tilgjengeliggjøre dette «at all times»
  - Oppdateringsregime trengs – sjekk DBA

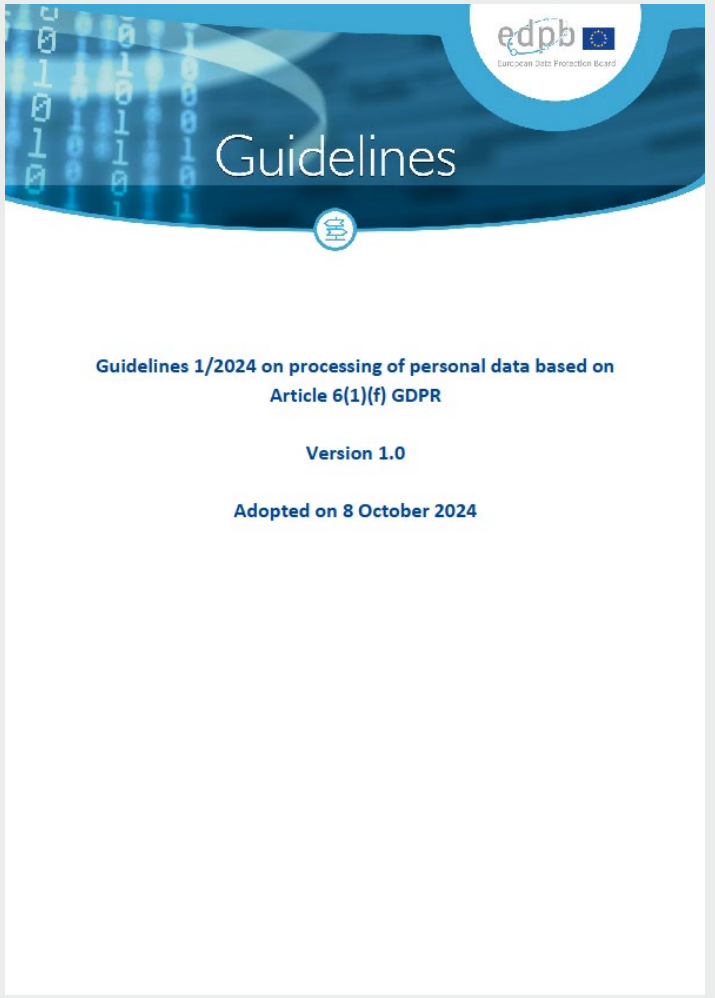


EDPBs opinion om databehandlere – art 64(2) kvasi-bindende

- **Leverandørkontroll:** Behandlingsansvarlig er ansvarlig for å kontrollere databehandlere - still spørsmål og utfør undersøkelser
  - **Graden av undersøkelser kan være risikobasert**
  - Databehandler undersøker under-databehandlere og behandlingsansvarlig kan stole på informasjon fra databehandler, men **må «verify» informasjon fra databehandler ved høy risiko, evt ved å be om kopi av kontrakter** for å kunne «demonstrate compliance»

- (Overraskende) Mye oppmerksomhet på tredjelandsoverføringer: Vurder risiko og sikre tilstrekkelige garantier




edpb
European Data Protection Board
Guidelines
Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR
Version 1.0
Adopted on 8 October 2024

EDPBs veileder om berettiget interesse

- Ikke veldig kontroversiell – AI ikke med (pga egen opinion på vei)
- Tre kumulative vilkår – som før
  - Må foreligge en berettiget interesse
  - Behandlingen må være nødvendig
  - Avveining mot individets interesse

EDPBs veileder om berettiget interesse

- **Nytt:**

- Kommersielle interesser kan vektlegges (Case C-621/22, KNLTB)
- Strenge krav til dokumentasjon
- Streng nødvendighetstolkning
- Høyere krav til balanseøvelse
- Mange nye eksempler
- OBS - fokus: personvernerklæring skal informere om formål som vektlegges, jf art 13

EDPBs veileder om berettiget interesse

- Interesser kan omfatte mye
  - Må være **lovlig**
  - Må være **klart formulert**
  - Må **ikke være hypotetisk**, må være tilstede

  - Ikke OK å sende DM om å fylle på innhold i elektroniske sigaretter pga tobakksreklame er ulovlig
  - Ikke OK å installere overvåkingskamera «for the greater good» - for vagt
  - Ikke OK å lagre adresser til de som har sagt opp et abonnement med tanke på å lansere nytt magasin og få nye abonnenter – for hypotetisk
  - Dele passasjerinfo om passasjer som har forvoldt skade på tredjemann – tredjeparts interesse - er OK
  - Statistikk i konsern – kan være OK
  - Informasjonssikkerhet kan være OK – gitt balansert

OBS: Neste uke kommer EDPB med 2 nye dokumenter

Opinion om hjemmel for AI-trening – berettiget interesse eller samtykke

Opinion om «Pay or OK»

Ny ekomlov – i kraft for cookies 1. januar 2025?

Samtykke – GDPR-compliant – kreves for å «sette» cookie ELLER annen sporingsteknologi

- Avslag i første eller annet lag?
- Tolkning av «nødvendig» cookie er streng og snever – sikre kommunikasjon

- En del forvirring, spørsmål på LI: Sette cookie basert på berettiget interesse??

- Hva med «multi-purpose trackere» (sikkerhet, analyse, bruksmønster, ads) – ofte samles alt inn, men bare noe brukes - om noe krever samtykke, farger det på alt

- Aktualiserer revisjon av hvordan mottakere bruker info fra cookies

On November 14, 2024, the French Data Protection Authority (CNIL) fined the French telecommunications operator ORANGE 50 million euros, notably for displaying advertisements between the e-mails of users of its email service without their consent.

Failure to comply with Article 82 of the French Data Protection Act: cookies read in spite of user consent withdrawal

The CNIL noticed that when a user of the orange.fr website accepted the deposit and reading of cookies on their device, and then withdrew their consent, the cookies previously deposited continued to be read by ORANGE and its partners.

The CNIL pointed out that **such a reading operation**, which consists in accessing data stored in the user's terminal, is explicitly **prohibited** by Article 82 of the French Data Protection Act, **even if this data is not subsequently used.**

Norsk Datatilsyn og NTNU om Copilot – lansert 26/11 – omfattende! (1/4)

NTNU, sluttrapport: Copilot med personvernbriller på

Generativ kunstig intelligens (KI) er ikke lenger bare et artig verktøy på si, men er nå i ferd med å bli integrert i de digitale løsningene vi allerede bruker. Microsoft lanserte sin Copilot for Office-pakken i november 2023, med potensial for å forenkle arbeidshverdagen betraktelig. Noen har tatt det i bruk, helt eller delvis. Mange sitter på gjerdet. For hva skjer egentlig når du slår på Microsoft 365 Copilot?

M365 Copilot rapport – high level take aways (2/4)

- DPIA trengs - DT ønsker mer spesifikk DPIA enn NTNU har gjort
- DPIA må ta utgangpunkt i konkrete behandlinger (mange hundre?)
  - Finn hvilke behandlinger dere gjør (art 30-protokoll)
  - Vanskelig når prompt bestemmer

- Copilot utfordrer formålsbegrensning og dataminimalisering
- Om PO brukes til nye formål (vanlig med KI) – vurder forenlighet

- Tilgangsstyring essentielt – svakheter forsterkes
  - Ved avvik kan vanskelig tilgjengelighet gjøre en feil mindre alvorlig - ikke slik når Copilot brukes – høyere risiko

- Når bruker har dårlig tid til QA – lite lurt å bruke KI – f eks HR
- Særlige kategorier bør vurderes nøye/unngås – minimum klassifisert på dokumentnivå

- Copilot logger alt – kanskje OK ifht epostforskriften/overvåking – sett grenser for bruk

M365 Copilot rapport – high level take aways (3/4)

3 typetilfeller – særlig om referatfunksjon:

Copilot bruker transkripsjon og «nærliggende dokumenter» -

> Ved bruk av M365 Copilot vil nye behandlingsoperasjoner oppstå i form av opptak og transkripsjon av møtet som vil innebære behandling av flere personopplysninger enn før, slik som stemme, stemmeleie, uttrykksform, kjønn (antakelse fra stemmeleie), samt (person)opplysninger som M365 Copilot finner når den leter etter «nærliggende dokumenter». I tillegg kan de valgfrie innstillingene påvirke hvilke andre behandlingsoperasjoner som skjer (f.eks. oversikt over hvem snakker, når og hvor lenge).

M365 Copilot rapport – high level take aways (4/4)
- Noen av NTNUs 41 risikoreduserende tiltak

Gjennomgå rutiner for ansvar for personvern
Lage egne rutiner for **administrasjon av Copilot**
Lage egne rutiner for **bruk** av Copilot
Lage egne rutiner for **fagspesifikke oppgaver**
Rutiner **for tilgang og sletting**
Berettiget interesse – sannsynlig hjemmel – revidere balansevurdering jevnlig
Sikre åpenhet, informasjon til brukere
Vurdere om MS er felles behandlingsansvarlig
Sikre «human in the loop»
Exit-strategi
Skru av tilgang til «uformelle» og «private» områder

Enkeltavgjørelser

Opp som en løve og ned som en fell?

2. Mai 2021: Varsel om **25 000 000** i bot til Disqus for manglende samtykke på deling av info til morselskap basert på daværende cookieregel (fra DT, ikke NKOM..) – innsigelser innlevert

2022 – ingen tilbakemelding
2023 – ingen tilbakemelding

28. Oktober 2024: **Bot frafalles i sin helhet**, men irettesettelse gis

Tilgangsstyring

- Overtredelsesgebyr til Universitetet i Agder (UiA): dokumenter med personopplysninger åpent **tilgjengelig i flere Teams-kanaler for ansatte uten tjenstlig behov**
    - PO: navn, fødselsnummer, opplysninger om tilrettelagt eksamen, eksamensforsøk og eventuelle særordninger
    - Ca 16 000 registrerte er berørt

- Datatilsynet: brudd på konfidensialitet og internkontroll og personopplysningssikkerhet

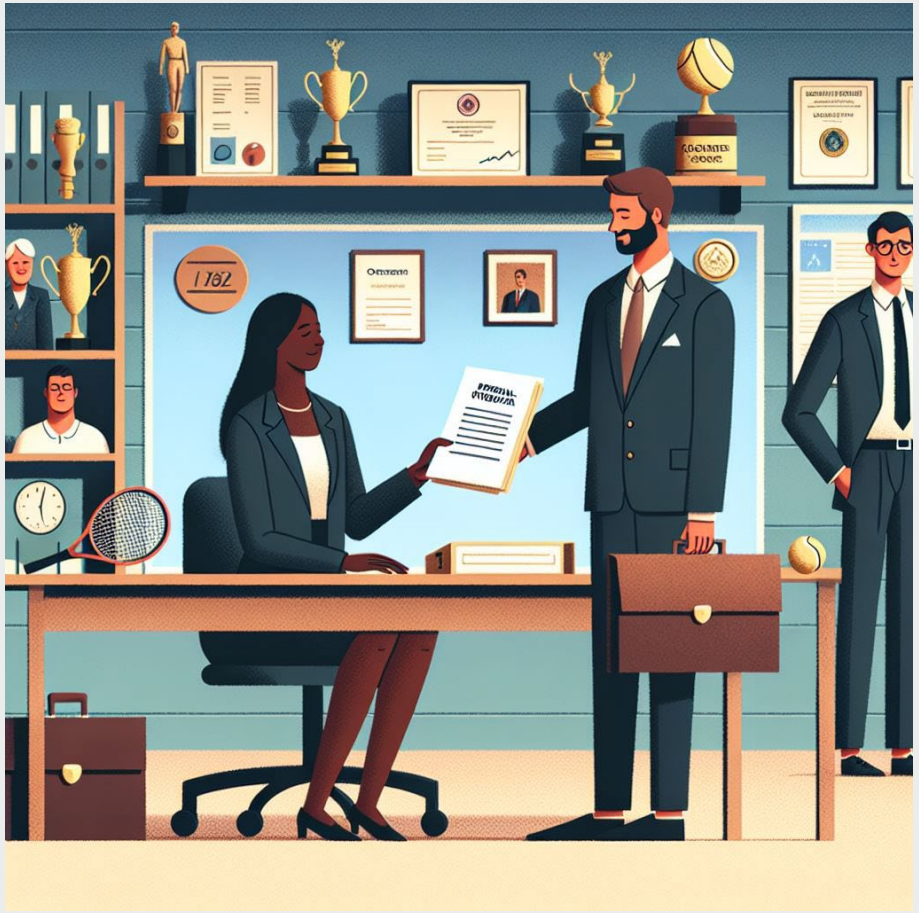
Grunn til å minne om at det er nyttig å ha logger. Det er kun de som eventuelt kan vise at opplysninger faktisk ikke har blitt aksessert og misbrukt.

.. lurt å se over hvordan tilgangsstyring er satt opp...

KNLTB (C-621/22) art 6(f) - Kommersielle interesser kan være en berettiget interesse

- Nederlandsk tennisforbund delte medlemsdata med eksterne aktører uten samtykke

- **Tre kumulative vilkår:**
  - **Vilkår 1:** Berettiget interesse som ikke strider mot annen lovgivning.
  - **Vilkår 2:** Behandlingen må være nødvendig og ikke kunne oppnås (enkelt) med andre tiltak**.** **Forventninger teller tungt. Informasjon om deling er viktig (personvernerklæring)**
  - **Vilkår 3:** Interesseavveining mot de registrertes grunnleggende rettigheter og friheter. Konsekvenser.



Belgisk tilsyn: samtykke til biometri vanskelig i ansettelsesforhold

Tidsregistreringssystem basert på fingeravtrykk, levert av et datterselskap til et japansk konsern
En ansatt klaget til datatilsynet

Datatilsynet: Krever behandlingsgrunnlag etter artikkel 6 og artikkel 9, samtykke ikke gyldig innhentet

- **Ikke informert (nok):** Informasjon om tidsregistreringssystemet kun gitt i velkomstbrosjyre og arbeidsreglementet
- Selv om ansatte signerte arbeidsreglementet og velkomstbrosjyren, **ikke klart nok** (noen kan nok være uenige her..)
- Det fantes **alternativer** til biometrisk registrering som kunne oppnå ønskede formål med mindre omfattende inngrep
- Samtykke ikke ansett som frivillig fordi det var **negative konsekvenser** ved ikke å samtykke
- **Formalistisk kritikk**: formålene med tidsregistreringssystemet ikke angitt i dokumentasjonen i arbeidernes personvern

Lindenapotheke (C-21/23)

- Tysk apotekkjede solgte reseptfrie medisiner på nett via Amazon
- **Sentralt spørsmål:** Vil personopplysninger som samles inn i nettapotek regnes som helseopplysninger under GDPR? (For paracet?)
- **Utvidet tolkning:** Vid tolkning av sensitive personopplysninger under GDPR
- **Praktiske konsekvenser:** Økning i rettslige utfordringer og strengere krav til samtykke. Revurdere hva som betraktes som sensitive personopplysninger?

Belgisk datatilsyn om felles behandlingsansvar (1/2)

Freedelity: elektroniske eID tibys bl.a. butikkjeder for å samle info ett sted

Bruker er dels butikk, dels forbruker, dels Freedelity

Hvem er behandlingsansvarlig?

Freedelity ville ha mye ansvar selv – ble ikke slik

Kan sammenlignes med et visst felles behandlingsansvar for f eks Meta og virksomheter for facebooksider for virksomheter - og for reklame på andres nettsider

Generelt: bruken av ulike web-løsninger, typisk innloggingsløsninger, ofte gir et felles behandlingsansvar – ikke vanskelig, men det krever en del nøyaktighet

Belgisk datatilsyn om felles behandlingsansvar (2/2)

Tilsynet:

Freedelity behandlingsansvarlig **for sin egen "Freedelity-fil"** som opprettes av forbruker og "Min Side"

Felles behandlingsansvar for personopplysningene fra butikkjedene som ble delt med Freedelity-plattformen for å kunne identifisere forbrukere - felles interesser i å få tilgang til, og bruke, kundedata samlet inn via eID

En rekke pålegg om endringer:

Samtykkeløsning endres slik at man **ikke må akseptere Freedelitys alminnelige vilkår for å kunne ta del i lojalitetsprogram** (utfordrende!)

Krav til **informasjon om formålene** med hver enkelt behandling (omstendelig – men i tråd med art 13)

(kan ha stor betydning for mange nettsider!) **Tilbaketrekking av samtykke skjedde via "Min side" på nettsiden, men det var ikke enkelt nok**

Schrems v Meta Platforms Ireland Ltd (C-446/21)

- **Bakgrunn:** Schrem fikk rettet reklame tilpasset hans seksuelle legning - anklaget Meta for ulovlig behandling av personopplysninger

- **Metas metode:** Informasjon om seksuell legning samlet fra eksterne nettsteder (tredjeparts data – antakelig basert på cookie-samtykke) via bla cookies

- **Domstolens avgjørelse**
  - Målrettet annonsering er lovlig, men underlagt begrensninger, bl.a. dataminimeringsprinsippet.
  - Bruk av **sensitive data krever uttrykkelig samtykke** og nødvendige begrensninger knyttet til bl.a. behandlingens varighet.
  - Og videre: **offentliggjøring av sensitive opplysninger av brukeren selv**, ikke automatisk gir plattformer som Facebook rett til å bruke denne informasjonen til andre formål, som for eksempel tilpasset markedsføring

Kan en unnskyldning være tilstrekkelig kompensasjon? (C-507/23)

- **Bakgrunn:** Klage fra journalist etter at det latviske forbrukertilsynet la ut en video som inneholdt en parodi av journalisten.
- **EU-domstolens vurdering:** Brudd på GDPR gir ikke automatisk rett til erstatning.
- **Erstatningskriterier:** Krav om GDPR-brudd, påvisbar skade og adekvat årsakssammenheng.
- **Unnskyldning som kompensasjon?** Ja, kan være passende for ikke-materiell skade.
- **Vil graden av skyld ha betydning?** Intensjon eller motivasjon hos behandlingsansvarlig er ikke relevant for erstatningens størrelse.

Anerkjennelse av transpersoners rettigheter (C-4/23)

- **Bakgrunn:** Britisk-rumensk statsborger endret juridisk kjønn og fornavn i Storbritannia. Romania nektet å registrere endringene på fødselsattesten. Mente han måtte gjennomgå nasjonal prosedyre for kjønnsendring.
- **EU-domstolens konklusjon:** Avslaget krenket rettigheter under EU-lovgivningen, inkludert retten til fri bevegelse.
- **Betydning for transpersoner:** Dommen sikrer anerkjennelse av identitetsendringer på tvers av EU-land. Kritikk fra land som Ungarn og Slovakia, som hevder dette utgjør overkjøring av nasjonale prinsipper.
- **Prinsipiell sak:** Selv om saken ikke er direkte relevant for Norge, har saken stor prinsipiell betydning.

Politiets tilgang til mobiltelefon ved mistanke om kriminalitet (C-548/21)

- **Bakgrunn:** Østerriksk borger fikk beslaglagt sin mobil etter funn av 85 gr cannabis. Østerriksk lovgivning tillater at politiet får tilgang til mobiltelefon i slike tilfeller.
- **EU-domstolen**: Mobiltelefoninngrep er et alvorlig inngrep i personvernet. Vurdering av forbrytelsens alvorlighet er nødvendig for å rettferdiggjøre inngrepet.
- **Juridiske krav**: Nasjonale lover må definere klare kriterier og kreve forhåndsgodkjenning fra domstol eller uavhengig myndighet. **I denne saken: kun ett års strafferamme, men CJEU stilte ikke krav til at det kun gjelder alvorlig kriminalitet. Dog plikt til å informere så langt det ikke setter etterforskning i fare**

Land Hessen (C-768/21)

- **Bakgrunn:** Bankansatt skaffet seg urettmessig tilgang til kundes personopplysninger
- **Arbeidsgiver:** Avviksmelding til datatilsynet, disiplinære skritt, og skriftlig forsikring fra ansatt om at PO ikke var misbrukt
- **Tilsynets avgjørelse:** Ingen tiltak mot arbeidsgiver, selskapet hadde utført risikovurdering
- **Juridisk spørsmål:** Om tilsynsmyndigheter må ilegge sanksjoner ved alle GDPR-brudd
- **Konklusjon: Tilsynsmyndigheter er ikke forpliktet til å ilegge sanksjoner; har skjønn til å velge passende tiltak**

Schjødt

Oslo Stockholm Copenhagen London Stavanger Bergen Ålesund