Noen viktige tema og saker siste måneder

Eva Jarbekk

Om forsikring

- Ikke mulig å forsikre seg mot cyberangrep?

Sjefen for forsikringsgiganten Zurich Insurance Group sier at det kan bli umulig å forsikre seg mot cyberangrep – kosten blir for stor

Britiske Lloyds: cyberforsikringer må ha unntaksbestemmelser for statlig støttede cyberangrep

Hydro tapte 1 milliard kr. på hackerangrepet i 2019 – utbetalt 800 millioner?

- Ikke mulig å forsikre seg mot cyberangrep?

Men hjelper cyberforsikring? For alle?

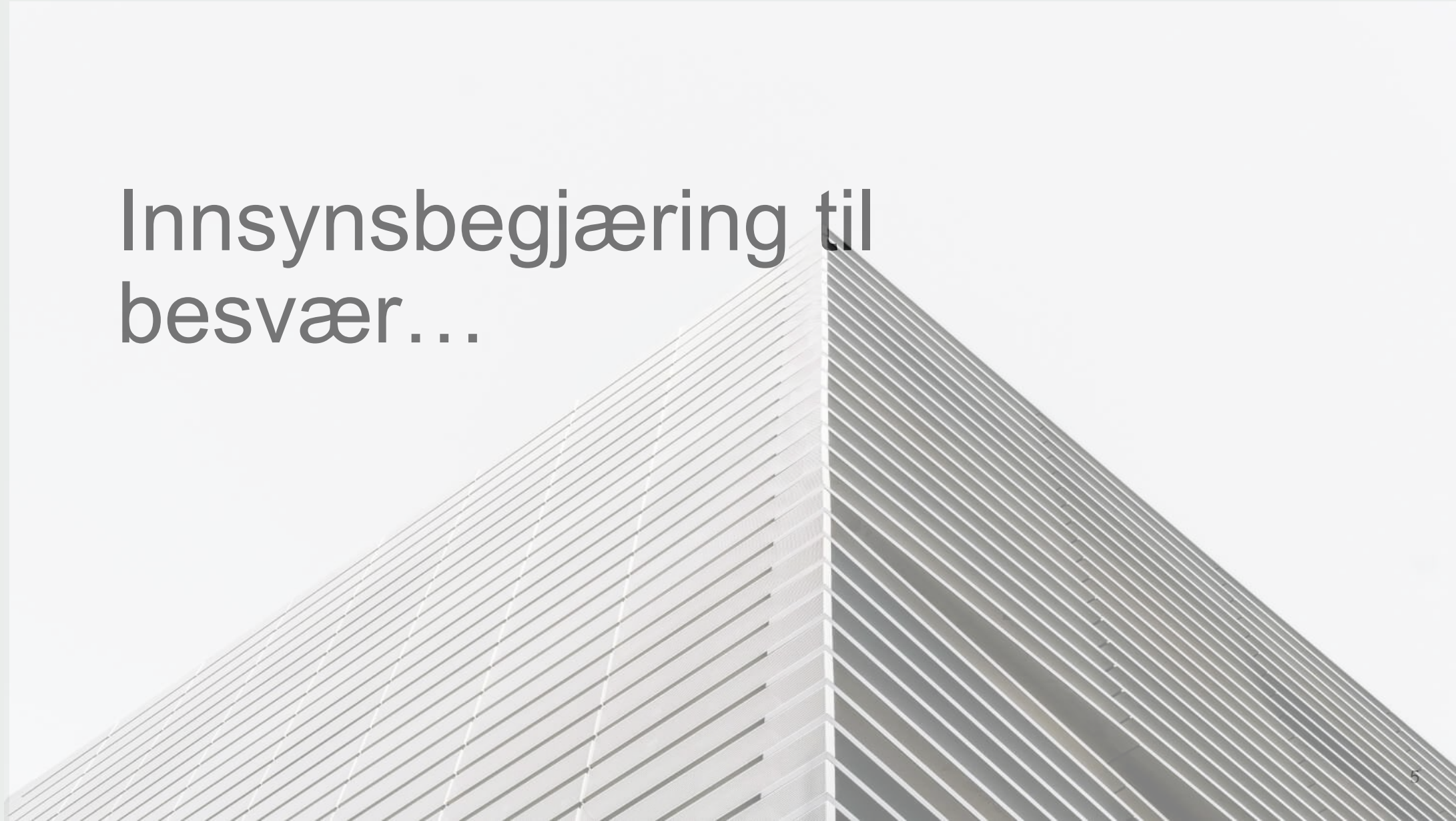
Krav til eksisterende beskyttelsestiltak før forsikring?

Kan ofte utvides til å dekke krav fra tredjepart etter GDPR pga. lekkasje

Kan (antakelig) ikke dekke overtredelsesgebyr – det er formelt sett «straff» som man ikke kan forsikre mot

Fungerer dårlig som «tiltak» mot non-compliance i due diligence/verdisetting

Innsynsbegjæring til besvær…



Hva sier loven – GDPR artikkel 15:

1. Den registrerte skal ha rett til å få den behandlingsansvarliges bekreftelse på om personopplysninger om vedkommende behandles, og, dersom dette er tilfellet, innsyn i personopplysningene og følgende informasjon:

a. formålene med behandlingen,

b. de berørte kategoriene av personopplysninger,

c. mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig mottakere i tredjestater eller internasjonale organisasjoner,

d. dersom det er mulig, hvor lenge det forventes at personopplysningene vil bli lagret, eller, dersom dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden,

e. retten til å anmode den behandlingsansvarlige om retting eller sletting av personopplysninger eller begrensning av behandlingen av personopplysninger som gjelder den registrerte, eller til å protestere mot nevnte behandling,

f. retten til å klage til en tilsynsmyndighet,

g. dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra,

h. forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.

2. Dersom personopplysningene overføres til en tredjestat eller til en internasjonal organisasjon, skal den registrerte ha rett til å bli underrettet om de nødvendige garantiene i henhold til artikkel 46 i forbindelse med overføringen.

3. Den behandlingsansvarlige skal gjøre tilgjengelig en kopi av personopplysningene som behandles. Dersom den registrerte anmoder om flere kopier, kan den behandlingsansvarlige kreve et rimelig gebyr basert på administrasjonskostnadene. Dersom den registrerte inngir anmodningen elektronisk, og med mindre den registrerte anmoder om noe annet, skal informasjonen gis i en vanlig elektronisk form.

4. Retten til å motta en kopi nevnt i nr. 3 skal ikke ha negativ innvirkning på andres rettigheter og friheter.

Sak fra Italia

Innsynsbegjæring – artikkel 15(1)(a) og (h)
- formål og automatiserte behandlinger

PO fantes ikke lenger, kun informasjon om hvordan PO var blitt behandlet (hvem de var delt med, etc.)
- rett til innsyn i dette?

Vid forståelse av personvernbegrepet

“The Court recalled that the **GDPR**, although known as the Privacy Regulation, **actually has a far wider scope of application that extends beyond and individual's right to privacy**, which is historically linked to their most private sphere. While the liberal concept of privacy requires essentially refraining from something for its protection, **the current conception of privacy has an interactive and dynamic nature. It particularly concerns personal data and their circulation.** The right to data protection is the cornerstone of **the (positive) freedom to fully control the flow of an individual's own data. It is distinct from the (negative) freedom not to be interfered with in an individual's own private sphere.** This is also, and above all, in the logic of market regulation covered by the GDPR.

Og antakelig riktig forståelse..

Konsekvens

Fortell «alt» om hvordan var PO blitt behandlet
Hvem var de delt med
- F.eks. undertegnet dokumentasjon/samtykker delt videre

Ny sak fra ECJ – Østerrike ba om avklaring

Innsynsbegjæring mot postvesen

Betyr GDPR art 15(1)(c) at man «kun» må fortelle om kategorier av mottakere eller må man være konkret og fortelle om HVEM?

Den registrerte skal ha rett til å få [..] følgende informasjon:
c. mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig mottakere i tredjestater eller internasjonale organisasjoner,

Domstolen legger avgjørende vekt på at ordlyden må tolkes i lys av hensynene bak GDPR, de lister opp rettigheter individet har

Hvis man ikke får vite hvem som har ens personopplysninger, så kan man ikke håndheve sine rettigheter

Etter min mening legger de selve ordlyden på strekk, men hensynene bak ivaretas og det blir bra personvern

Konsekvens

Må redegjøre for hvem man har delt opplysninger med

Det vil favne vidt - «mottaker» dekker både databehandlere og andre selvstendig behandlingsansvarlige, noen eksempler:

- hvem sender cookies opplysninger til,
- hvilke it-leverandører brukes og
- hvilke samarbeidspartnere i og utenfor konsern som har mottatt opplysninger

Dommen er ganske kort og er lesverdig

Norsk avgjørelse - Zalaris

X-ansatt begjærte innsyn hos Zalaris (jobbet i tysk datterselskap)

- Først med epost til CEO
- Så til epostkassen for innsyn

Zalaris svarte først ikke, men svarte etter gjentatt begjæring via epost og purring fra Datatilsynet

Zalaris ga ut kopi av PO og personvernerklæring

Norsk avgjørelse - Zalaris

DT:

- OK at første begjæring ble oversett fordi den be sendt til CEO og **ikke gjennom anbefalt innsynskanal** (uventet!)
- Annen begjæring ble fanget i spam og derfor ikke besvart – det skulle systemet unngått – mindre brudd pga kun 1 individ påvirket og CAPTCHA løsning innført for å detektere spam

Brudd:

- Å ikke informere om formål som ikke lå i personvernerklæringen
- Informasjonen var ikke tilpasset behandlingene vedkommende var utsatt for
- Intet overtredelsesgebyr

Irland og tech-gigantene

META – Scraping-saken

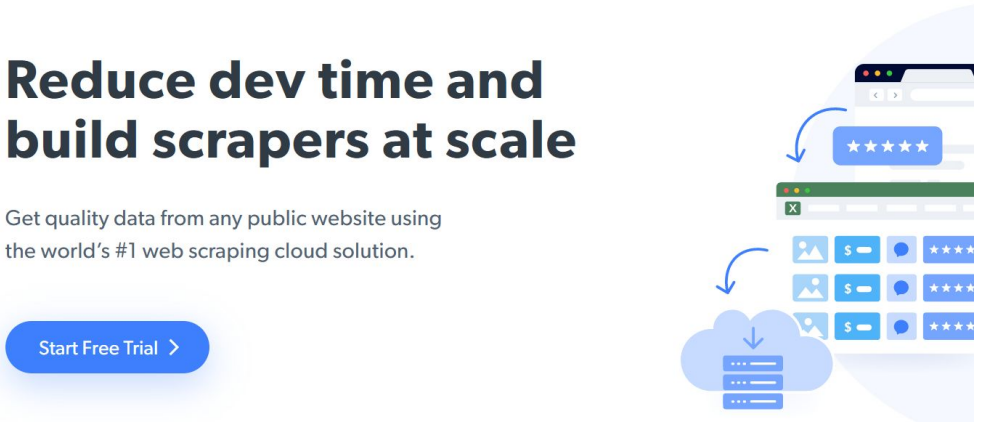
Personopplysningene (telefonnummer, Facebook ID, navn og fødselsdato) til 530 millioner brukere kunne skrapes av tredje parter fra Facebook i tidsrommet 25. mai 2018 til september 2019

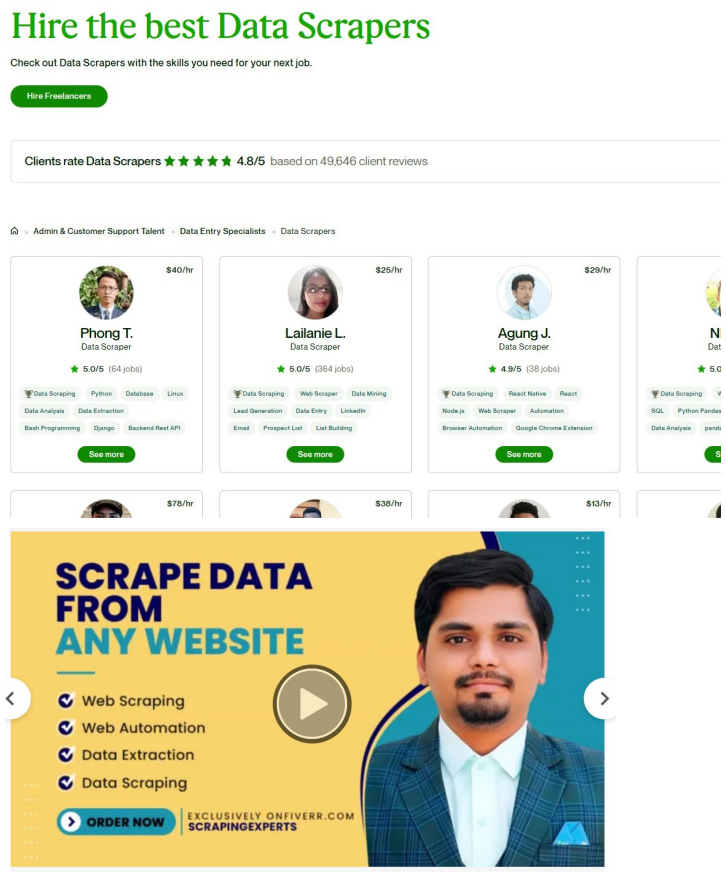
Bot: 256 millioner euro – over 2,5 milliard kroner

Endrede systemer ble ikke vektlagt (uklart hva som ble endret)

Meta: *"made changes to our systems during the time in question, including removing the ability to scrape our features in this way using phone numbers. Unauthorized data scraping is unacceptable and against our rules"*

Husk – amerikansk opphavsrett kan tillate scraping fra åpne kilder – er ikke OK i Europa (Og ikke ifht GDPR heller..)





META – Scraping

META har nå saksøkt flere selskaper som scraper fra FB – baserer det på brudd på avtalevilkår/bruksvilkår

> In July, Meta filed separate actions in federal court against a US subsidiary of a Chinese national high-tech enterprise Octopus and Ekrem Ateş for scraping data from Facebook and Instagram.
>
> The company accused Octopus, a US subsidiary of a Chinese national high-tech enterprise, of building a cloud-based platform to provide paying customers access to on-demand scraping software and services. A Turkey-based defendant Ekrem Ateş is being sued for allegedly using automated Instagram accounts to scrape data from the profiles of over 350,000 Instagram users.

https://cybernews.com/editorial/meta-data-scraping/

Scraping

Er det tilstrekkelig med en policy om at scraping ikke er tillatt?

- (Det bør antakelig mange ha for å verne seg mot scraping fra land utenfor EØS)

Men kan scraping forhindres?
Visstnok særlig vanskelig på app-er
En «request» mot et system/informasjonsbit må bestemmes om kommer fra en person eller en bot, krever ofte mer enn en enkelt handling

> Bots are, in fact, quite hard to stop since requests are not usually coming from the same IP or the same session ID.
>
> "Scrapers now have the ability to break up the scraping work into chunks and send them to different bots. I don't mean 1 or 2, more like thousands to 10s of thousands of bots. That activity is harder to spot. I know this is accurate because security researchers use the same techniques to scrape threat actor forums and channels," David Maynor, Head of Cybrary Threat Intelligence Group (CTIG), told Cybernews.

https://cybernews.com/editorial/meta-data-scraping/

Mer om Facebook – historien om de største milliardbøtene

EDPB i desember - spørsmål:
Kan en behandling av personopplysninger i FB, Instagram og Whatsapp baseres på behandlingsgrunnlaget «avtale» når formålet er

1) adferdsbasert markedsføring (FB og Instagram)
2) forbedring av selskapets tjenester (WhatsApp-saken)
3) sikkerhet (WhatsApp-saken)

Grunnen til at EDPB ble involvert: Uenighet irsk datatilsyn og mange andre om juss og størrelse på bot, deriblant det norske tilsynet

VIKTIG for utforming av kundevilkår/lojalitetsprogrammer

Ørliten ansvarsfraskrivelse

Sakene er omfattende og dette er en innledende vurdering, ikke en dyptpløyende analyse

Det står mye villedende på nett om avgjørelsene – f eks at opt-in alltid kreves

En god podcast om dette fra 2. februar der NOYB også deltar er her:

https://privacypod.libsyn.com/website/31-unwrapping-the-irish-dpas-meta-rulings-with-a-noyb-insider

Elementer i klagen fra NOYB

1 Personifisert reklame er ikke en nødvendig del av kontrakten

- FB er en sosial møteplass, ikke en adtech-generator
- Datatilsyn *kan* mene noe om kontraktstolkning, det er ikke utenfor deres kompetanse (slik FB hevdet) – hvis ikke blir artikkel 6 «meningsløs» og folks rettigheter
- En avtale plikter ikke å hensynta individets interesser – slik en vurdering av berettiget interesse gjør
- En avtale plikter ikke å hensynta hva individet forventer – slik en vurdering av berettiget interesse gjør
- En avtale kan individet ikke protestere mot
- Ellers kan man komme i en situasjon der «*en baker kan kreve å få vite din inntekt for å finne passende brød»*

Elementer i klagen fra NOYB

2 Kontraktsgrunnlag kan aldri hjemle behandling av særlige kategorier personopplysninger (som man finner i FB)

3 Det er uklart hvordan FB vil bruke opplysningene

…..disse elementene er utelatt/ikke drøftet i DPC's avgjørelse

EDPBs gamle veileder for retargeting i sosiale media

Gjelder fremdeles – åpner for samtykke eller berettiget interesse
AVHENGIG AV KONTEKST

Kort om EDBPs beslutning til DPC

Understreker at kun ett behandlingsgrunnlag skal brukes

Årsaken er bla at rettighetene til ulike behandlingsgrunnlag er ulike

Og det skal ikke byttes ut underveis
- FB skiftet fra opprinnelig samtykke (før GDPR)
  til avtale (etter GDPR)

Resultat januar 2023

FB og Instagram

- Bot øket fra 28 000 000 Euro til 390 000 000 Euro
- **Disse aktørene må ha opt-in samtykke for ads**
    - **OBS: det betyr ikke at alle andre må det, det spørs på hva man gjør**

Avgjørelsene om FB og Instagram

Opprinnelig klage handlet om «personalised advertising»

Endelig (?) avgjørelse fra DPC handler om «retargeting i social media»

..som er noe mindre enn det klagen omhandlet

Resultat januar 2023

WhatsApp

- Bot 5 500 000 Euro
- **Kan ikke bruke avtale som grunnlag for «product improvement»**
- **Kan ikke bruke avtale for «security»**
    - men antakelig berettiget interesse

- Ads ikke omtalt – de deler data med Meta (hvem snakker med hvem, hvor ofte, kobles via tel nr)

NOYB om saken

Next steps: DPC sues EDPB, Meta likely to appeal. Meta is expected to appeal the decision in the Irish Courts, but the chances to win such an appeal are minimal after a binding EDPB decision. There are also two similar cases before the Court of Justice of the EU (CJEU) on Meta's consent bypass, that may settle the issue and all appeals for good. In a side-story the DPC also announced that it may sue the EDPB on a related issue, as the EDPB required the DPC to take further investigative steps on Meta, beyond the decided complaints by *noyb*. The DPC takes the view that the EDPB does not have these powers and will try to get this decision annulled. Users may also take action over the illegal use of their data for the past 4.5 years.

Et mulig søksmål fra DPC gjelder EDPBs pålegg om å undersøke ad-bundling for Whatsapp og deling av data i konsernet og om det er sensitive data (avtale kan ikke brukes på sensitive data)

Og – klager NOYB pga elementer utelatt fra opprinnelig klage?

CNIL og tech-gigantene

CNIL og tech-gigantene

Microsoft bøtelegges 60 millioner euro for feil bruk av cookies

- Den største boten CNIL har gitt i 2022
- Søkemotoren Bing tillot ikke brukere å avslå cookies like enkelt som de kunne aksepteres

- Uklar rettstilstand i Norge pt. – NKOM/Datatilsynet
- Ny ekomlov i Norge vil antakelig gjøre rettstilstanden i Norge lik som i EU – kommer antakelig første halvår – trolig effekt 1. januar 2024

Lojalitetsprogrammer

Douglas parfymerikjede - lojalitetsprogram

Italiensk datatilsyn bøtela Douglas ca 14 000 000 NOK for manglende overholdelse av individets rettigheter, manglende hjemmel, transparens, for lang lagring

- Trigget av art 15-22 begjæring fra kunde, intet svar

- Klaget til DPA, som kontrollerte Douglas
- App'en bundlet vilkår, personvernerklæring, cookieerklæring i en «agree-knapp»

Douglas parfymerikjede - lojalitetsprogram

Douglas ble i 2019 fusjonert – fra 3 andre selskap

- Kunne ikke vise markedsføringssamtykker fra tidligere selskaper
- Over 3'' kunder fra de «gamle» selskapene var fremdeles lagret selv om de ikke hadde videreført lojalitetsprogrammet
- Ingen informasjon til kundene om hvordan informasjon ble håndtert etter fusjon
- De som samtykket til SMS fikk også telefonhenvendelser – og omvendt
- Blog manglet personvernerklæring og informerte ikke om formål og lagringstid for informasjon

Og en snodig sak vi har diskutert tidligere

Kan markedsføring være en tvungen del av avtalen – eller kan man kreve «goodies» uten å få reklame?

Magasins kundeklubb

- ”Datatilsynet vurderede, at fordelene ved medlemskab af Magasins kundeklub Goodie mod til gengæld at give samtykke til markedsføring, lå inden for rammerne af et incitament, som en dataansvarlig kan give med henblik på at opnå samtykke, uden at et sådant samtykke kan anses for at være i strid med betingelsen om frivillighed.

- Datatilsynet lagde i den forbindelse vægt på, at man som medlem af kundeklubben kan opnå visse fordele, men at man uanset disse fordele, må anses for at have et reelt og frit valg i forhold til køb af Magasins produkter på almindelige vilkår.”

Samtykketeksten

- [ ] Jeg samtykker til at modtage målrettede henvendelser via e-mail, push-beskeder i tilknyttede apps, og sms fra Magasin du Nord (”Magasin”) med nyheder, tilbud, kampagner og konkurrencer, der vedrører de produkter og services, som Magasin udbyder.
- For at kunne målrette henvendelserne til mig, vil Magasin benytte oplysninger (navn, kontaktdetaljer, køn, fødselsdato, interesser, købshistorik, brug af fordele og søgeadfærd) tilknyttet mit Goodie medlemskab eller indsamlet via cookies på magasin.dk via særskilt cookiesamtykke.
- Jeg kan i Magasins persondatapolitik læse nærmere om, hvordan Magasin som dataansvarlig behandler mine personoplysninger i forbindelse med mit Goodie medlemskab.
- Jeg kan altid trække mit samtykke tilbage via fx magasin.dk eller Goodie appen. Hvis jeg trækker mit samtykke tilbage, så ophører mit medlemskab af Goodie.

Hva med GDPR art 21 nr 2?

Ikke nevnt i saken:

- «Dersom personopplysninger behandles med henblikk på direkte markedsføring, skal den registrerte til enhver tid ha rett til å protestere mot behandling av personopplysninger som angår vedkommende, til slik markedsføring, herunder profilering i den grad dette er knyttet til direkte markedsføring.»

- Og: samtykke/protestrett etter markedsføringsloven er ikke drøftet i saken – antakelig fordi utenfor Datatilsynets virkeområde

Schjødt

Eva Jarbekk
Partner/lawyer,
Head of privacy & information security
m: +47 900 51 011
d: +47 23 01 18 29
eva.jarbekk@schjodt.com