

# FØYEN

## IKT-Norges risikovurdering av Facebook

Erfaringsseminar 21.6.2022 – Kjetil Wick Sætre

## Bakgrunn

Virksomheters bruk av sosiale medier til kommunikasjon med enkeltpersoner, vil nesten alltid innebære en form for *behandling av personopplysninger*, som virksomheten er ansvarlig for at skjer i samsvar med regelverket. Et av kravene i regelverket er at det skal gjøres en risikovurdering, i visse tilfeller i form av en *vurdering av personvernkonsekvenser* («data protection impact assessment, eller «DPIA»).

## Selskapet/virksomheten og den planlagte aktiviteten

IKT-Norge er en bransjeforening for virksomheter innenfor informasjons- og kommunikasjonsteknologi. IKT-Norge bruker Facebook-sider og tjenesten Sideinnsikt/Page Insights til kommunikasjon med medlemsbedrifter, med ansatte hos medlemsbedriftene og alle andre som har interesse av det arbeid som IKT-Norge bedriver.

## Vurdering av personvernkonsekvenser – bruk av Facebook som kommunikasjonskanal

- IKT-Norge tok utgangspunkt i Datatilsynets metodikk og fremgangsmåte.
- Vi gjorde en vurdering ut fra IKT-Norges behov for å bruke Facebook, men utformet som en mal som medlemmene kunne gjenbruke med tilpasninger.
- Vurderingene ble gjennomført i samarbeid mellom IKT-Norge og Føyen, uten involvering av Facebook.

## Innhold

- Systematisk beskrivelse av behandlingsaktivitetene
  - Formål
  - Innsamling og behandling
  - Tilgang
  - Teknologi
  - Omfang
  - Sammenheng
  - Sikkerhet
  - **Aktørene og ansvarsfordelingen**
- Håndtering av risiko for de registrerte – særlig om ansvarsfordelingen mellom IKT-Norge og Facebook
- Oppsummering – vurdering iht. GDPR art 35
- Vurdering av nødvendighet og rimelighet i forhold til formålet

## Felles behandlingsansvar

Utgangspunkter er at felles  
behandlingsansvar oppstår etter GDPR art  
26 når to eller flere behandlingsansvarlige «i  
fellesskap fastsetter formålene med og  
midlene for behandlingene».

## Artikkel 26.Felles behandlingsansvarlige

*1. Dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen, skal de være felles behandlingsansvarlige. De skal på en åpen måte fastsette sitt respektive ansvar for å overholde forpliktelsene i denne forordning, særlig med hensyn til utøvelse av den registrertes rettigheter og den plikt de har til å framlegge informasjonen nevnt i artikkel 13 og 14, ved hjelp av en ordning seg imellom, med mindre og i den grad de behandlingsansvarliges respektive ansvar er fastsatt i unionsretten eller medlemsstatenes nasjonale rett som de behandlingsansvarlige er underlagt. I ordningen kan det utpekes et kontaktpunkt for registrerte.*

*2. Ordningen nevnt i nr. 1 skal på behørig måte gjenspeile de felles behandlingsansvarliges respektive roller og forhold til de registrerte. Det vesentligste innholdet i ordningen skal gjøres tilgjengelig for den registrerte.*

*3. Uavhengig av vilkårene for ordningen nevnt i nr. 1 kan den registrerte utøve sine rettigheter i henhold til denne forordning med hensyn til og overfor hver av de behandlingsansvarlige.*

## Fordeling av det felles behandlingsansvar

GDPR art. 26 fastsetter videre i korte trekk at felles behandlingsansvarlige skal i en «ordning» seg imellom, fastsette sitt respektive ansvar for å oppfylle forordningen – i praksis i en avtale.

## Artikkel 26. Felles behandlingsansvarlige

*1. Dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen, skal de være felles behandlingsansvarlige. De skal på en åpen måte fastsette sitt respektive ansvar for å overholde forpliktelsene i denne forordning, særlig med hensyn til utøvelse av den registrertes rettigheter og den plikt de har til å framlegge informasjonen nevnt i artikkel 13 og 14, ved hjelp av en ordning seg imellom, med mindre og i den grad de behandlingsansvarliges respektive ansvar er fastsatt i unionsretten eller medlemsstatenes nasjonale rett som de behandlingsansvarlige er underlagt. I ordningen kan det utpekes et kontaktpunkt for registrerte.*

*2. Ordningen nevnt i nr. 1 skal på behørig måte gjenspeile de felles behandlingsansvarliges respektive roller og forhold til de registrerte. Det vesentligste innholdet i ordningen skal gjøres tilgjengelig for den registrerte.*

*3. Uavhengig av vilkårene for ordningen nevnt i nr. 1 kan den registrerte utøve sine rettigheter i henhold til denne forordning med hensyn til og overfor hver av de behandlingsansvarlige.*

## Hvilke aktiviteter har man felles behandlingsansvar for?

I Wirtschaftsakademie-avgjørelsen understrekes det at utgangspunktet for vurderingen er i hvilken grad partene deltar i å fastsette formål og midler («purposes and means») for behandlingen

*: «... it must be examined whether and to what extent the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, contributes in the context of that fan page to determining, jointly with Facebook Ireland and Facebook Inc., the purposes and means of processing the personal data of the visitors to the fan page and may therefore also be regarded as a ‘controller’ ...»*

# FØYEN

“In this context, according to the submissions made to the Court, the creation of a fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page. The administrator may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page.

In particular, the administrator of the fan page can ask for – and thereby request the processing of – demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers.” (vår utheving)



Hvilke aktiviteter har man felles behandlingsansvar for?

*«By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d).» - Fashion ID, avsnitt 76.*

Hvilke aktiviteter har man felles behandlingsansvar for?

*1. Innsamling og behandling før brukeren besøker Digdirs side*

***2. Innsamling av personopplysninger på Digdirs side***

***3. Overføring av personopplysninger til Facebook***

***4. Aggregering av personopplysninger til statistikkformål***

*5. Behandling etter at opplysningene er overført og aggregert*

*- Digdirs risikovurdering under «Avgrensninger».*

## KONSEKVENSEN AV FELLES BEHANDLINGSANSVAR

- Alle plikter i GDPR skal overholdes av partene i fellesskap.
- Oppgavefordelingen skal fastsettes i avtale.
- Partene står som utgangspunkt fritt til å fordele ansvar iht. GDPR art. 26. Forordningen er ikke til hinder for at for eksempel alt det interne ansvaret legges på en av partene.

## OPPSUMMERT

- Felles behandlingsansvar oppstår når to eller flere i fellesskap fastsetter «formål» og «midler».
- Felles ansvar betyr ikke «likt» ansvar – graden av ansvar varierer ut fra innflytelsen over behandlingen.
- Aktiviteter man ikke utøver innflytelse over, får man ikke ansvar for. Innflytelse på én aktivitet, medfører ikke ansvar for en annen, separat, aktivitet.