FØYEN

Dato: 25.1.2022

Vår ref.: 513786

VURDERING AV PERSONVERNKONSEKVENSER – BRUK AV FACEBOOK SOM KOMMUNIKASJONSKANAL

INNHOLD

Advokatfirmaet Føyen AS
foyen.no
Org nr.: NO 885 719 392 MVA

Dronning Eufemias gate 8
Postboks 7086 St. Olavs plass,
0130 Oslo

Tlf.: +47 21 93 10 00
Fax: +47 21 93 10 01
E-post: post@foyen.no

1. INNLEDNING

1.1. Bakgrunn

(I første kapittel beskrives bakgrunnen for vurderingen, herunder kort om IKT-Norge, aktivitetene de skal vurdere, og kort om de rettslige utgangspunktene. Bakgrunnsinformasjonen bør tilpasses den enkelte virksomhet som gjennomfører vurderingen, mens de rettslige utgangspunktene som beskrives vil være relevant for alle.)

Kort beskrivelse av 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.

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»).

En DPIA er en prosess ment for å beskrive aktiviteten som skal gjennomføres, vurdere om den er nødvendig og proporsjonal, og håndtere de risikoer som oppstår gjennom å vurdere dem og å finne tiltak for å adressere dem. Spørsmålene som derfor må besvares i en DPIA er:

- Hva består behandlingsaktivitetene egentlig i, og hva er formålet?
- Vil behandlingen medføre høy risiko for fysiske personers rettigheter og friheter?
- Er behandlingen nødvendig og står den i et rimelig forhold til formålet/formålene?
- Hva er risikoen for de man behandler opplysninger om?
- Hvordan håndteres risikoen?

Disse spørsmålene blir besvart av selskapet i dette dokumentet.

Inngangskriteriet for når man må gjennomføre en DPIA, er at behandlingsaktiviteten man planlegger kan medføre «høy risiko» for individers rettigheter og friheter. Det kan stilles spørsmål ved om det at et selskap ønsker å ha en side på Facebook, og benytte seg av tjenesten Sideinnsikt fra Facebook, er en type behandling som kan medføre høy risiko og som dermed utløser krav til DPIA. Teknologien er ikke ny, i den forstand at tjenesten har eksistert i flere år og er i bruk hos tusenvis av selskaper verden over. Selskapet har likevel valgt å gjennomføre en vurdering, da Datatilsynet har funnet det nødvendig for sin virksomhet å gjennomføre en slik vurdering.

Selve oppsummeringen og vurderingen av personvernkonsekvenser iht. GDPR art. 35 fremgår i kapittel 5.

Dette dokumentet skal gi ledelsen i selskapet et grunnlag til å gjøre en informert og forsvarlig beslutning om hvorvidt selskapet skal opprettholde og således fortsette å kommunisere gjennom en side på Facebook.

Kort beskrivelse av hvordan vurderingen er gjort:
Vurderingen er gjennomført av utvalgte ressurser hos IKT-Norge, i samarbeid med Advokatfirmaet Føyen AS. Føyen er selv medlemsbedrift i IKT-Norge. Facebook Norway AS er også medlemsbedrift i IKT-Norge. Verken det norske selskapet eller øvrige selskaper i konsernet har vært involvert i IKT-Norges vurdering.

Det faktiske grunnlaget for vurderingen er offentlig tilgjengelig informasjon direkte relevant for behandlingsaktivitetene, som Facebooks personvernerklæring og Facebooks «Sideinnsiktstillegg for behandlingsansvarlig». Det rettslige grunnlaget er personopplysningsloven og EUs personvernforordning («GDPR») med tilhørende rettspraksis.

Vurderingen er foretatt basert på tilgjengelige kilder og ressurser på tidspunktet for gjennomføring. Den vil kunne bli revidert ved eventuelle klargjøringer fra EU-domstolen eller andre autoritative kilder.

1.2. Nærmere om den rettslige vurderingen

GDPR art. 35 (1) fastslår at det skal gjennomføres en vurdering av personvernkonsekvenser («data protection impact assessment, eller «DPIA») dersom det er sannsynlig at «en type behandling» vil medføre høy risiko for fysiske personers rettigheter og friheter. Kravet gjelder særlig ved bruk av «ny teknologi», og det skal tas hensyn til «behandlingens art, omfang, formål og sammenhengen den utføres i».

Vurderingen skal iht. GDPR art. 35 (7) minst inneholde:

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige, (kapittel 2 under)

b) en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene (kapittel 3 under)

c) en vurdering av risikoene for de registrertes rettigheter og friheter (kapittel 4 under)

d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser (kapittel 5 under)

2. SYSTEMATISK BESKRIVELSE AV DE PLANLAGTE BEHANDLINGSAKTIVITETENE OG ORMÅLET MED BEHANDLINGEN, SAMT DEN BERETTIGEDE INTERESSEN SOM FORFØLGES AV SELSKAPET

2.1. Innledning

(Generell veiledning: For at det skal være mulig å gjennomføre en risikovurdering eller en DPIA, må man først kartlegge behandlingsaktivitetene, altså de prosessene man skal igangsette som medfører behandling av personopplysninger.)

I kapittel 2 gis en beskrivelse av behandlingsaktivitetene som selskapet har (felles) behandlingsansvar for, selskapet sitt formål og de berettigede interessene selskapet søker å oppnå ved aktivitetene.

I beskrivelsen av behandlingsaktivitetene, er det særlig relevant å beskrive følgende momenter:

- Hva er behandlingens art? (for eksempel, hvordan skal personopplysninger samles inn, lagres og brukes, hvem får tilgang, hvem behandles det personopplysninger om) (2.2 under)
- Hva er formålet? (2.2.2 under)
- Hva er behandlingens omfang? (hvilke type opplysninger behandles, mengden, antall personer som berøres, hvor ofte skal aktiviteten gjennomføres) (2.3 under)
- I hvilken sammenheng behandles opplysningene? (F.eks. hva slags relasjon har man til personene det gjelder, hva slags forventninger vil de ha) (2.4 under)
- Hvordan ivaretas informasjonssikkerheten til opplysningene? (2.5 under)
- Hvilke aktører er involvert? (kilder til opplysningene, mottagere, hvem er behandlingsansvarlig og ev. databehandler) (2.6 under)

2.2. Beskrivelse av behandlingsaktivitetene

2.2.1. Formål med behandlingen og eventuelt den berettigede interessen

Sett inn beskrivelse av formålet:
IKT-Norge sin interesse i behandlingen er å benytte dataene og statistikken til å nå ut så bredt som mulig til befolkningen og IKT-Norges medlemmer, og til å stimulere til debatt om temaer innen IKT-Norges virkeområde. IKT-Norge vil ikke benytte dataene til kontrollformål, til å treffe betydningsfulle avgjørelser om de registrerte, til profilering eller lignende. IKT-Norge har ikke en intensjon om å viderebehandle personopplysninger til andre formål enn det som her er nevnt.

Dersom det er relevant, beskriv den berettigede interessen som forfølges:
Den berettigede interessen er å drive kommunikasjon med norske borgere som benytter Facebook og IKT-Norge sine Facebook-sider.

2.2.2. Innsamling og behandling

Sett inn beskrivelse av hvordan personopplysningene skal samles inn og behandles:
Gjennom kommunikasjon på Facebook-sidene samles personopplysninger inn via det de registrerte skriver (herunder potensielt ytringer av politisk karakter, der IKT-Norge har oppfordret/tilrettelagt for debatt om aktuelle temaer), likes og data Facebook observerer om den registrertes bruk av sidene, som nærmere beskrevet i Facebooks retningslinjer for behandlingen av personopplysninger.[1] Denne innsamlingen danner så grunnlaget for Facebooks tjeneste Sideinnsikt. Tjenesten Sideinnsikt styres i sin helhet av Facebook, og resultatet presenteres for IKT-Norge som aggregert statistikk om de registrertes bruk av IKT-Norge sine Facebook-sider. Facebook sin beskrivelse av behandlingen inntas i sin helhet: *Sideinnsikt er aggregert statistikk som opprettes fra visse hendelser som logges av Facebook-serverne når folk samhandler med sider og innhold tilknyttet dem.* *Slike hendelser består av forskjellige datapunkter som disse, avhengig av den bestemte hendelsen:* *En handling. Dette inkluderer handlinger som disse (du kan se tilgjengelige handlinger for siden din i sideinnsikt-delen):* • *visning av en side, et innlegg, en video, en historie eller annet innhold tilknyttet en side* • *samhandling med en historie* • *følge eller slutte å følge en side* • *like eller slutte å like en side eller et innlegg* • *anbefale en side i et innlegg eller en kommentar* • *kommentere, dele eller reagere på et sideinnlegg (inkludert type reaksjon)* • *skjule et sideinnlegg eller rapportere det som spam* • *holde pekeren over en lenke til en side eller navnet eller profilbildet til en side for å se en forhåndsvisning av sidens innhold* • *klikke på knappene for nettsted, telefonnummer, Få veibeskrivelse eller en annen knapp på en side* • *visning av en sides arrangement på skjermen, svar på et arrangement, deriblant type reaksjon, klikk på en lenke for arrangementsbilletter*

[1] https://www.facebook.com/about/privacy/update

- *starte Messenger-kommunikasjon med siden*
- *se eller klikke på elementer i sidens butikk*

Informasjon som dette om handlingen, personen som utfører handlingen, og nettleseren/appen som brukes:

- *dato og tid for handlingen*
- *land/by (anslått fra IP-adresse eller importert fra brukerprofilen for innloggede brukere)*
- *språkkode (fra nettleserens http-topptekst og/eller språkinnstilling)*
- *alders-/kjønnsgruppe (fra brukerprofilen bare for innloggede brukere)*
- *tidligere besøkt nettsted (fra nettleserens http-topptekst)*
- *om handlingen ble utført fra en datamaskin eller mobilenhet (fra nettleserens brukeragent eller appegenskaper)*
- *FB-bruker-ID (bare for innloggede brukere)*

Vi avgjør om en person er en innlogget Facebook-bruker, via informasjonskapsler i samsvar med Retningslinjer for informasjonskapsler. Det er bare noen få hendelser som kan utløses av folk som ikke er logget inn på Facebook. Blant disse er besøk på side eller klikk på et bilde eller en video i et innlegg for å se det.
Sideadministratorer har ikke tilgang til personopplysningene som behandles som en del av hendelsene, men bare til den aggregerte sideinnsikten. Hendelser som brukes til å opprette sideinnsikt, lagrer ikke IP-adresser, nettkapsel-ID-er eller andre identifikatorer som er knyttet til personer eller enhetene deres, bortsett fra FB-bruker-ID-en til personer som er logget inn på Facebook.

Hendelsene som logges av Facebook for å opprette sideinnsikt, er helt og fullt definert av Facebook og kan ikke angis, endres eller på annen måte påvirkes av sideadministratorer. [2]

Oppsummert kan Sideinnsikt gi IKT-Norge informasjon om hvor mange som har sett innlegg, hvem som har likt, delt og kommentert, hvordan brukerne reagerer på innlegg, demografiske data, og hvor mange som ser sidene. [3]

IKT-Norge samler ikke inn ytterligere opplysninger via Facebook enn det som gjøres gjennom bruk av Sideinnsikt.

[2] https://www.facebook.com/legal/terms/page_controller_addendum
[3] En grafisk fremstilling av behandlingene finnes på denne siden: https://www.facebook.com/business/pages/manage#page_insights

2.2.3. *Tilgang til opplysninger*

Beskrivelse av hvem som vil ha tilgang til opplysningene:
I tillegg til Facebook og IKT-Norge, vil også andre besøkende på IKT-Norge sine Facebook-sider kunne se informasjon som deles av brukere som reagerer på eller kommenterer på sidene.

2.2.4. *Bruk av ny teknologi/ny bruk av eksisterende teknologi*

Beskriv dersom behandlingsaktivitetene medfører bruk av ny teknologi, eller ny bruk av eksisterende teknologi:
Facebook-sider og tilhørende bruk av Sideinnsikt er velkjente og svært utstrakt brukte tjenester, både i Norge og internasjonalt. Tjenestene er dynamisk i sin natur, og personvernkonsekvensene ved bruk kan derfor utvikle seg over tid. Dette har blant annet resultert i endring av tjenestevilkårene som følge av praksis fra EU-domstolen. [4] For norske virksomheter og borgere må imidlertid bruken av Facebook-sider og Sideinnsikt anses som velkjent og således ingen ny personvernrisiko. Det er også relevant at de registrerte selv har valgt å oppsøke Facebook, og i den anledning inngått brukeravtale med og avgitt samtykker til Facebook. Brukere av Facebook har tilgang til Facebooks personvernerklæringer og således anledning til å sette seg inn i hvordan Facebook behandler deres personopplysninger.

2.2.5. *Behandlingens omfang*

Beskriv behandlingens omfang (Omfanget har betydning for risikovurderingen i den forstand at jo større antall personer som berøres og jo større menger opplysninger, jo større kan personvernrisikoen være):
Behandlingen vil omfatte opplysninger som karakteriseres som alminnelige personopplysninger. IKT-Norge har ingen intensjon om å samle inn *særlige kategorier* av personopplysninger. Det vurderes som at det er liten risiko, gitt IKT-Norges virksomhet, at brukere selv vil publisere særlige kategorier opplysninger, eventuelt opplysninger om straffbare handlinger, på Facebook-sidene. Ytterligere tiltak for å unngå publisering av særlige kategorier opplysninger kan være å oppfordre i fritekst-feltet på siden om at slike opplysninger ikke skal deles, og at IKT-Norge kontrollerer jevnlig at det ikke gjøres. Antall registrerte som berøres av behandlingen, avhenger av hvor mange som besøker og ev. samhandler med IKT-Norges sider. Per i dag har IKT-Norge i underkant av 6000 som har trykket «like» på siden. Volumet av data kan avledes av antall følgere/besøkende, og datakategoriene beskrevet under pkt. 2.1. Behandlingen vil pågå kontinuerlig. Samlet vil behandlingen ha et relativt lavt omfang sammenlignet med andre Facebook-sider hvor antall følgere er langt høyere.

[4] https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=39049220

2.2.6. Behandlingens sammenheng

Beskriv i hvilken sammenheng behandlingsaktivitetene gjøres, og hvilken betydning dette har for personvernrisikoen:

Beskriv i hvilken sammenheng behandlingsaktivitetene gjøres, og hvilken betydning dette har for personvernrisikoen:
Kilden til dataene og informasjon som samles inn via Facebook-sidene og Sideinnsikt er brukerne selv og deres handlinger, samt de analyser som Facebook gjør og presenterer for IKT-Norge gjennom Sideinnsikt. IKT-Norges relasjon til brukerne er som uavhengig interesseorganisasjon. Den typiske bruker av IKT-Norges Facebook-sider vil være en ansatt i en av medlemsbedriftene, eventuelt andre med interesse for IKT-Norges meninger og bransjerelatert situasjon. I lys av IKT-Norges rolle, forventer trolig brukerne selv at de får informasjon og kan nå IKT-Norge via Facebook. Behandlingen av personopplysninger tilknyttet sidene, vil være så forutsigbar for brukeren som mulig, gitt kompleksiteten. Den jevne Facebook-bruker må antas å ha evne til å finne frem til de informasjonskilder Facebook har tilgjengeliggjort, som beskriver behandlingen. Når man oppretter en Facebook-bruker blir det innhentet samtykker, og brukeren har til enhver tid tilgang på Facebooks personvernerklæring og innstillinger. Det må også understrekes at brukerne benytter Facebook frivillig, og oppsøker IKT-Norges side frivillig. Den eventuelle negative personvernkonsekvensen av at IKT-Norge har egne Facebook-sider, i form av ytterligere behandling av brukernes personopplysninger, må sies å være marginal. Det må legges til bruk at ingen brukere er på Facebook utelukkende for å kommunisere med IKT-Norge. Å være på Facebook er heller ingen nødvendig betingelse for å kommunisere med IKT-Norge, da informasjon alltid vil være tilgjengelig via andre kanaler i tillegg.

2.2.7. Personopplysningssikkerhet

Beskriv hvordan personopplysningssikkerheten iht. GDPR art. 32 er ivaretatt:
Informasjonssikkerheten ved behandlingen ivaretas i all hovedsak av Facebook, noe som også fremgår av Sideinnsiktstillegg for behandlingsansvarlig, kulepunkt 4. Sideinnsiktstillegget inkluderer forpliktelser angående organisering, fysisk og miljømessig sikring, opplæring, screening og disiplinærtiltak overfor ansatte, testing, tilgangskontroll, kommunikasjonssikkerhet, sårbarhetshåndtering og håndtering av sikkerhetshendelser.

IKT-Norge ivaretar informasjonssikkerheten for sin egen behandling, særlig gjennom opplæring av ansatte med tjenstlig behov, samt tilgangsstyring når det gjelder muligheten for å administrere sidene

2.3. Aktørene involvert og ansvarsfordelingen – særlig forholdet til Facebook

I det følgende vurderes aktørene som er involvert i behandlingen og ansvarsfordelingen mellom dem. Målet med vurderingen er å avklare eventuelle uklare ansvarsforhold som kan utgjøre en personvernrisiko.

Et hovedspørsmål i denne sammenheng er hvorvidt og i hvilken utstrekning selskapet har felles behandlingsansvar med Facebook. Dette vurderes i det følgende.

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

EU-domstolen har i to saker vurdert hva som skal til for at felles behandlingsansvar oppstår, og konsekvensene av slikt ansvar. Disse avgjørelsene gjennomgås i den utstrekning det er relevant for vår vurdering i det følgende.

2.3.1. Wirtschaftsakademie-avgjørelsen

EU-domstolen kom i Wirtschaftsakademie-avgjørelsen til at administratorene (dvs. de som har inngått avtale med Facebook) av Facebook-sider er felles behandlingsansvarlig med Facebook, for behandling av personopplysninger som besøker Facebook-siden.[5] Saken gjaldt tolkningen av definisjonen av behandlingsansvarlig under personverndirektivet fra 1995, men må legges til grunn å ha betydning også under GDPR, hvor det altså stilles eksplisitte krav til hvordan felles behandlingsansvarlige skal oppfylle sine plikter etter forordningen.

Bakgrunnen for avgjørelsen var at slike administratorer kan få anonym, statistisk data om brukerne gjennom det som også den gang ble kalt Facebook Insights (Sideinnsikt). I spørsmålet om det forelå felles behandlingsansvar i Wirtschaftsakademie-avgjørelsen, la EU-domstolen vekt på at administratorer deltar i fastsettelsen av formål og midler for behandlingen, ved at de kan definere sitt målpublikum, og definerer selv formålet med siden sin. Domstolen vektla at sideadministratorer kan be om at visse typer data (f.eks. demografiske) skal inngå i analysen man får via Sideinnsikt, og dermed deltar i å definere behandlingsaktivitetene.[6]

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. For det første slås i det i premiss 31 fast at:

[5] Sak C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH.
[6] Avgjørelsens premiss 31 til 44.

> «*… 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' …*"

Videre går EU-domstolen i premiss 36 og 37 inn på de konkrete aktivitetene en sideadministrator for en Facebook-side gjør, som danner grunnlag for det felles behandlingsansvaret:

> *"36 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.*
>
> *37 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)

Den rettslige konsekvensen av disse aktivitetene som utføres av sideadministratoren, er at det oppstår felles behandlingsansvar, jf. premiss 39:

> *"In those circumstances, the administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised, in the present case, as a controller responsible for that processing within the European Union, jointly with Facebook Ireland, within the meaning of Article 2(d) of Directive 95/46."*

Felles behandlingsansvar innebærer ikke nødvendigvis lik fordeling av ansvar for hele behandlingen. Dette understrekes i premiss 43:

> «*However, it should be pointed out, as the Advocate General observes in points 75 and 76 of his Opinion, that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*."

Oppsummeringsvis er konsekvensen av avgjørelsen at sideadministratorer anses for å ha felles behandlingsansvar med Facebook. Dette innebærer imidlertid ikke at det skal være likt ansvar mellom sideadministratoren og Facebook. Med andre ord har ikke en sideadministrator ansvar for alt Facebook foretar seg med personopplysninger som samles inn via sideadministratorens Facebookside.

2.3.2. Fashion ID-avgjørelsen

EU-domstolen har også vurdert felles behandlingsansvar i den såkalte Fashion ID-avgjørelsen.[7] Avgjørelsen har betydning for å fastlegge i hvilken utstrekning man er ansvarlig for Facebooks etterfølgende behandling av personopplysninger, når man har felles behandlingsansvar for innsamlingen.

Fashion ID gjaldt en nettbutikk som brukte Facebooks «like»-knapp på sin nettside. Gjennom «like»-knappen ble informasjon om besøkende på nettsiden samlet inn og delt med Facebook. I avgjørelsen uttalte blant annet domstolen at Fashion ID ikke ville være felles behandlingsansvarlig for eventuell etterfølgende behandling Facebook måtte foreta:

> «*In view of that information, it should be pointed out that the operations involving the processing of personal data in respect of which Fashion ID is capable of determining, jointly with Facebook Ireland, the purposes and means are, for the purposes of the definition of the concept of 'processing of personal data' in Article 2(b) of Directive 95/46, the collection and disclosure by transmission of the personal data of visitors to its website.* ***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).*" [8] (vår utheving)

Oppsummeringsvis fremstår det klart at det kreves at begge parter gjør aktive valg mht. definering av formål og midler for behandlingen av personopplysninger, for at det skal oppstå et felles behandlingsansvar etter GDPR. Med andre ord vil en sideadministrator ikke være ansvarlig for Facebooks etterfølgende behandling av personopplysninger, dersom

[7] C-40/17 Fashion ID.
[8] Fashion ID premiss 76.

sideadministratoren ikke har deltatt i defineringen av formål og midler for den etterfølgende behandlingen.

2.3.3. Facebooks Sideinnsiktstillegg for behandlingsansvarlig

En konsekvens av EU-domstolens avgjørelser, er at Facebook har utarbeidet «Sideinnsikttillegg for behandlingsansvarlig», som er ment å oppfylle kravene i GDPR art. 26.

Sideinnsiktstillegget fastsetter eksplisitt i sitt andre kulepunkt hva partene (henholdsvis Facebook og den som har inngått avtale med Facebook om opprettelsen av en Facebook-side) har og ikke har felles behandlingsansvar for:

> «*Det felles behandlingsansvaret dekker opprettelsen av disse hendelsene og aggregeringen til sideinnsikten som leveres til sideadministratorene. Partene samtykker i at for all annen behandling av personopplysninger i tilknytning til en side og/eller innholdet forbundet med siden der det ikke er bestemt noen felles formål eller midler, forblir Facebook Ireland, eller hvis aktuelt, du, separate og uavhengige behandlingsansvarlige*.»

Med unntak av behandlingen som er omfattet av Sideinnsikt, har ikke Facebook og IKT-Norge noe kontraktsforhold eller annet samarbeid som medfører behandling av personopplysninger i fellesskap. De er derfor i utgangspunktet hver for seg behandlingsansvarlige for sine egne behandlinger av personopplysninger, med unntak for behandlingsaktiviteter som er omfattet av Sideinnsikt, i den utstrekning begge parter har bidratt til å definere formål og midler, jf. GDPR art. 4 (7) og art. 26.

3. VURDERING AV NØDVENDIGHET OG OM BEHANDLINGEN STÅR I ET RIMELIG FORHOLD TIL FORMÅLET

3.1. Innledning

I denne vurderingen er det relevant å ta hensyn til:

- Hva er det rettslige grunnlaget for behandlingen? (3.2 under)
- Er behandlingen nødvendig, altså begrenset til det som er nødvendig for å oppnå formålet? (3.3 under)
- Hva er konsekvensene av behandlingen for de registrerte? (3.4 under)

3.2. Rettslig grunnlag

Beskriv virksomhetens rettslige grunnlag for behandlingen av personopplysninger:
IKT-Norge sitt rettslige grunnlag for behandlingen vil være berettiget interesse iht. GDPR art. 6 (1) (f). Den berettigede interessen er å drive kommunikasjon med norske borgere som benytter Facebook og IKT-Norge sine Facebook-sider.

3.3. Nødvendighet av behandlingen og om den er rimelig i forhold til formålene

Beskriv hvorfor behandlingen av personopplysninger er nødvendig og står i et rimelig forhold til formålet:
IKT-Norge sitt formål med behandlingen er å benytte dataene og statistikken til å nå ut så bredt som mulig til befolkningen og IKT-Norges medlemmer. IKT-Norge vil ikke benytte dataene til kontrollformål eller til å treffe betydningsfulle avgjørelser om de registrerte. IKT-Norge har ikke en intensjon om å viderebehandle personopplysninger til andre formål enn det som her er nevnt. Fordelen for IKT-Norge ved å benytte Facebook-sider, er at en stor andel av det norske folk og dermed de IKT-Norge ønsker å nå, benytter plattformen i det daglige. Det gir dermed IKT-Norge mulighet til å nå ut til flest mulig på en effektiv måte med sin informasjon. Behandlingen anses av IKT-Norge for å være nødvendig og begrenset til det som er nødvendig for å oppnå formålet.

3.4. Konsekvensene for de registrertes rettigheter og friheter (personvernulempene)

Beskriv hvilke konsekvenser behandlingen har for de registrertes rettigheter og friheter:
Vi kan ikke se at IKT-Norge sin bruk av Facebook-sider *i seg selv* utsetter de registrerte for noen særskilt personvernulempe. At en bruker kommenterer, liker, eller beveger seg rundt på IKT-Norges side, gir etter vår vurdering IKT-Norge relativt harmløs informasjon om brukeren (jf. oversikten i pkt. 2 over). Gitt at IKT-Norge sin virksomhet primært er å styrke de overordnede rammebetingelsene for det digitale næringslivet, ser vi ikke noen særskilt personvernrisiko som oppstår ved at IKT-Norge har sider på Facebook. Dette gjelder særlig sett hen til at det må legges til grunn at brukerne selv frivillig velger å bruke Facebook, og oppsøke IKT-Norges sider. Riktignok må det understrekes at brukernes politiske ståsted og meninger til en viss grad kan avledes av aktiviteten deres på IKT-Norges nettsider. For eksempel vil kommentarer, delinger, og likes fort gi en indikasjon på brukerens syn på lovforslag, politiske vedtak, og dagsaktuelle hendelser. Likevel er ikke dette annen informasjon enn det som ellers vil fremkomme av de flestes øvrige aktiviteter på Facebook. Personvernulempen ved å benytte Facebook generelt, består i at Facebook vil samle inn og benytte personopplysninger fra besøkende på IKT-Norge sine sider, til Facebooks egne formål. Dette gjør imidlertid Facebook som egen og selvstendig behandlingsansvarlig. IKT-Norge vil ikke kunne ha full innsikt og forståelse for hvordan Facebook benytter data som selvstendig behandlingsansvarlig, tross all informasjon Facebook har tilgjengeliggjort i sine personvernerklæringer og avtalevilkår. Så lenge Facebook driver sin selvstendige virksomhet og tilsynsmyndighetene ikke griper inn, kan vi ikke se at IKT-Norge verken kan eller bør gjøre en nærmere vurdering av hvorvidt Facebooks egne behandlinger er i samsvar med GDPR. Det må være forsvarlig av IKT-Norge å legge til grunn at Facebook gjennomfører denne

behandlingen i samsvar med GDPR. Dette er også i samsvar med Fashion ID-avgjørelsen, hvor det ble lagt til grunn at Fashion ID ikke hadde felles behandlingsansvar for Facebooks behandling etter at personopplysningene hadde blitt overført til Facebook.

IKT-Norge anser på denne bakgrunn sin behandling av personopplysninger ved bruk av Facebook-sider som proporsjonal. I denne vurderingen legges det særlig vekt på at IKT-Norge ikke samler inn andre data enn det alle andre Facebook-sider gjør, og at delingen er frivillig fra de registrertes side og at de selv har et avtaleforhold med Facebook og gitt samtykker som danner grunnlag for behandlingen. Facebook har tilgjengeliggjort informasjon om behandlingen for de registrerte, og den registrerte kan selv påvirke hvilke data som deles med Facebook og IKT-Norge. IKT-Norge lagrer ikke selv noen andre data enn den aggregerte statistikken som Sideinnsikt-tjenesten gir.

4. HÅNDTERING AV RISIKO FOR DE REGISTRERTES RETTIGHETER OG FRIHETER - ANSVARSFORDELING MELLOM SELSKAPET OG FACEBOOK

Beskriv hvordan de registrertes rettigheter etter GDPR ivaretas (*Spørsmålet som vurderes er om det foreligger tiltak for å håndtere risikoen ved behandlingen, jf. GDPR art. 35 (7) (d)*)

Facebook og IKT-Norge har felles behandlingsansvar iht. GDPR art. 26, for behandling av personopplysninger som skjer når de registrerte samhandler med IKT-Norge sine Facebooksider. Ansvarsfordelingen mellom Facebook og IKT-Norge følger av vilkårsettet/avtalen «Sideinnsikttillegg for behandlingsansvarlig».

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. [9]

I henhold til Sideinnsiktstillegget påtar Facebook seg ansvaret for ivaretagelse av gjeldende forpliktelser under GDPR, inkludert, men ikke begrenset til, artiklene 12 og 13 GDPR, artiklene 15 til 21 GDPR, artiklene 33 og 34 GDPR. Facebook gir informasjon til de registrerte gjennom policyen «Informasjon om sideinnsiktsdata». [10]

Avtalen fastslår at IKT-Norge selv må ha et rettslig grunnlag for sin behandling, og inkludere kontaktinformasjon iht. GDPR art. 13(1) (a–d). Dette vil IKT-Norge påse at gjøres. IKT-Norge vil gjennom sin egen personvernpolicy redegjøre for den behandlingen som IKT-Norge gjør.

De registrerte har iht. GDPR art. 26 (3) rett til å håndheve sine rettigheter både overfor Facebook og overfor IKT-Norge. IKT-Norge vil imidlertid ikke være i stand til å alene oppfylle alle rettigheter, eksempelvis rett til innsyn og dataportabilitet. Dersom IKT-Norge mottar slike forespørsler, fastslår avtalen med Facebook at IKT-Norge skal videreformidle forespørselen

[9] Jf. kommentar til art. 26 i kommentarutgaven til personvernforordningen, ved Åste Marie Bergseng Skullerud, Cecilie RønnevikJ, ørgen Skorstad og Marius Engh Pellerud.
[10] https://www.facebook.com/legal/terms/information_about_page_insights_data

gjennom et eget skjema, jf. Sideinnsiktstillegget kulepunkt 9. [11] Facebook påtar seg gjennom Sideinnsiktstillegget å svare på slike forespørsler i henhold til forpliktelsene deres som felles behandlingsansvarlig iht. Sideinnsiktstillegget.

Det bemerkes at avtalen som IKT-Norge har med Facebook inneholder Facebooks forpliktelser til å ivareta informasjonssikkerheten iht. GDPR art. 32. Dette inkluderer forpliktelser angående organisering, fysisk og miljømessig sikring, opplæring, screening og disiplinærtiltak overfor ansatte, testing, tilgangskontroll, kommunikasjonssikkerhet, sårbarhetshåndtering og håndtering av sikkerhetshendelser. IKT-Norge kan ivareta informasjonssikkerheten for sin egen behandling, særlig gjennom opplæring av ansatte med tjenstlig behov, samt tilgangsstyring.

Under henvisning til at Facebook har gjort tilgjengelig informasjon om hvilke valg en administrator har, med tilhørende avtalevilkår for dette, fremstår dermed Sideinnsiktstillegget som en oppfyllelse av kravet til at felles behandlingsansvarlige skal i en «ordning» seg imellom, fastsette sitt respektive ansvar for å oppfylle forordningen.

Det konkluderes på bakgrunn av ovenstående at det foreligger tiltak som håndterer risikoen ved behandlingen, jf. GDPR art. 35 (7) (d).

[11] https://www.facebook.com/help/contact/308592359910928

5. OPPSUMMERING - VURDERING AV PERSONVERNKONSEKVENSER IHT. GDPR ART. 35

Beskriv om behandlingen vil medføre en høy risiko for fysiske personers rettigheter og friheter, basert på faktorene beskrevet over;
Etter vår vurdering vil svaret for IKT-Norges del være nei. Dette fordi: • Behandlingsaktivitetene, formålene og kategoriene av opplysninger som behandles tilsier i seg selv ikke at det er høy risiko ved behandlingen • IKT-Norges behandlingsaktitiveter anses å være nødvendige og stå i et rimelig forhold til formålene som søkes oppnådd • De registrertes rettigheter og friheter tilknyttet behandlingsaktivitetene vil kunne ivaretas • De planlagte tiltakene for å håndtere risikoen anses tilfredsstillende, hensyntatt de registrertes og andre berørte personers rettigheter og berettigede interesser.