Intern risikovurdering: skal Datatilsynet ha egen side på Facebook?

Sluttrapport 2021

Datatilsynet

Innhold

Forord

Denne rapporten er basert på en intern risikovurdering av hvorvidt Datatilsynet skal ha en side på Facebook eller ikke. Dokumentets opprinnelige og primære hensikt var å gjøre organisasjonens ledelse i stand til å fatte en ansvarlig beslutning om organisasjonen skal ha en Facebook-side.

Vi mener vurderingen også vil ha interesse for offentligheten. Rapporten oppsummerer våre analyser, vurderinger og konklusjoner av risiko, risikohåndtering og plikter etter personvernregelverket idet Datatilsynet som en offentlig myndighet oppretter og kommuniserer gjennom en side på Facebook.

I denne vurderingen opptrer Datatilsynet verken som tilsynsorgan eller ombud, men som behandlingsansvarlig med plikter etter personvernforordningen. I rapporten uttaler vi oss dermed ikke generelt om lovlighet eller ansvarlighet ved å ha en Facebook-side.

Rapporten ble lagt frem for Datatilsynets ledelse i mars 2020. Den offentlige rapporten er supplert med noen avklaringer med tanke på viktige utviklinger på personvernfeltet.

Sammendrag

Datatilsynet har et mål om å øke bevisstheten om og interessen for personvern i Norge. For å oppnå dette målet, vurderer vi tilstedeværelse på kommunikasjonsplattformer som gjør at vi kan kommunisere effektivt med viktige målgrupper. Vi anser Facebook som godt egnet til å dekke flere av virksomhetens kommunikasjonsbehov- og ambisjoner.

Innføringen av personvernforordningen (General Data Protection Regulation, GDPR) i 2018 har gitt innbyggere nye rettigheter og virksomheter flere plikter. Som følge av det nye regelverket har både private selskap og offentlige myndigheter vært nødt til å gjennomgå rutiner, praksis og anskaffelser som involverer behandling av personopplysninger for å tilfredsstille kravene i den nye loven. Regelverkets plikter gjør seg også gjeldende når en virksomhet tar i bruk sosiale medier, for eksempel en side på Facebook.

Et viktig verktøy for å sikre at personvernet til de som er registrert i en løsning ivaretas, er å gjennomføre risikovurderinger og vurdering av personvernkonsekvenser (Data Protection Impact Assessment, DPIA). Rapporten inneholder en systematisk beskrivelse av løsningen, som inkluderer en juridisk vurdering av ansvarsforhold, en vurdering av behandlingens nødvendighet og proporsjonalitet, og vurderer tiltak for å redusere personvernrisiko for de registrerte i løsningen. Det er også lagt vekt på mer etiske spørsmål med utgangspunkt i Datatilsynets verdier[1] og posisjon som rollemodell med hensyn til personvern.

Konklusjon

Datatilsynets ledergruppe besluttet at Datatilsynet *ikke* skal opprette og kommunisere gjennom en side på Facebook. Konklusjonen er basert på en helhetsvurdering, men spesielt forankret i punktene under:

- Arbeidsgruppen mener at Datatilsynets behandling av personopplysninger gjennom en side på Facebook medfører en for høy risiko for de registrertes rettigheter og friheter.
- Arbeidsgruppen mener at Datatilsynet ikke vil være i stand til å iverksette tiltak som reduserer risikoen i tilstrekkelig grad.
- Vår vurdering er at Datatilsynet i liten grad vil være i samsvar med personvernforordningen artikkel 26 om felles behandlingsansvar.
- Arbeidsgruppen men er at det ikke er tilstrekkelig for Datatilsynet å inngå Facebooks standardavtale om felles behandlingsansvar. Datatilsynet vil ikke ha mulighet til å inngå egne avtaler med Facebook.
- Arbeidsgruppens vurdering er at det sannsynligvis ikke vil være mulig for Datatilsynet å tilfredsstille kravene i artikkel 25 i personvernforordningen om innebygget personvern og personvern som standardinnstilling dersom vi tar i bruk Facebook.
- Datatilsynets personvernombud tilråder at Datatilsynet ikke tar i bruk Facebook som kommunikasjonsplattform.
- Arbeidsgruppen mener at Datatilsynet også bør tillegge hensynet til sin posisjon som rollemodell for personvern og samsvar med gjeldende personvernregelverk stor vekt.

Arbeidsgruppens analyser, vurderinger og anbefalinger dokumenteres i denne rapporten.

Rapporten er basert på en intern risikovurdering av hvorvidt Datatilsynet skal ha en side på Facebook eller ikke. I denne vurderingen opptrer Datatilsynet verken som tilsynsorgan eller ombud, men som behandlingsansvarlig med plikter etter personvernforordningen (se forord).

[1] https://www.datatilsynet.no/om-datatilsynet/planer/datatilsynets-strategi/

Innledning

Vårt arbeid startet med en anerkjennelse: At store deler av den offentlige samtalen er flyttet inn på det digitale rom, og i økende grad inn på plattformer som eies av store, private teknologiselskaper. Direkte adgang til målgrupper, mulighet til å snakke med mennesker der de er og bruker sin tid, og muligheten til å snakke til dem på en måte de liker og er vant til, gjør plattformene attraktive for mange virksomheter.

Inngangsbilletten for å delta på disse plattformene er brukervennlig og tilsynelatende gratis. Men fra et personvernståsted er ikke det helt tilfellet. Opplysninger om hva vi gjør på plattformene blir samlet inn i stor skala for å forstå oss og våre vaner, og gir oss tilpasset reklame og innhold. Dersom en person oppretter en profil, eller en virksomhet oppretter en side på en slik plattform, vil det som regel medføre en ganske omfattende behandling av personopplysninger.

At en datatilsynsmyndighet oppretter en side på en slik plattform kan derfor fremstå som en selvmotsigelse. Det er likevel kommunikasjonsavdelingens oppfatning at virksomheten bør vurdere å satse på nye type kanaler og nye typer innhold som passer disse kanalene for å delta og ta større plass i den offentlige samtalen. Tanken er at slike kanaler kan bidra med effektiv spredning og hosting av ulike typer innhold, føre til økt trafikk til nettsiden og åpne nye arenaer for debatt og veiledning. Denne konseptsammensetningen er blant grunnene til at vi vurderer Facebook som kommunikasjonsplattform.

Datatilsynet har stor interesse av økt synlighet for vår virksomhet og våre interesseområder utenfor eget domene (www.datatilsynet.no), og å drive trafikk til nettsiden. I dag produserer vi mye eget innhold, og stadig mer audiovisuelt innhold, og har ansatte med kanalkompetanse og erfaring med sosiale medier. I tillegg er det investert i utstyr og kompetanse for nye typer innholdsproduksjon. Vi tror dessuten at mer kanalspesifikk kommunikasjon, slik som kommentarfelt, nettverking og relasjonsbygging, vil kunne ha verdi for utstrekningen av vår ombudsrolle.

Samtidig må vi være klar over at tilstedeværelse på Facebook innebærer flere forpliktelser. Deriblant må vi sette av tilstrekkelige ressurser, arbeide for å engasjere målgruppene med godt og relevant innhold som er tilpasset kanalens egenart, og vurdere kanalens effekt, nytteverdi og vilkår med jevne mellomrom.

Formål

På bakgrunn av dette formulerte vi to formål ved å opprette og kommunisere via en side på Facebook:

- *Formål 1:* Opplyse og engasjere norske Facebook-brukere om personvernregelverket, personverntematikk og tilgrensende emner, og informere om Datatilsynets kjernevirksomhet.
- *Formål 2:* Stimulere til debatt om personvernregelverket og personverntematikk, og invitere norske borgere til dialog om og utvikling av personvernområdet og Datatilsynets rolle i samfunnsutviklingen.

En sideeffekt ved å bruke side på Facebook er at Datatilsynet vil få innsikt om kommunikasjon på siden, eksempelvis statistikk om demografi og interaksjoner. Aggregert innsiktsdata er standard for eiere av side på Facebook og kan ikke velges bort. Vi valgte imidlertid ikke å formulere dette som et eget formål.

Vi ønsker ikke å benytte plattformens annonsetjeneste eller integrere Facebook widgets, plugins eller lignende på egen nettside. Analyser og vurderinger av dette er derfor ikke vurdert i rapporten.

Risikovurdering

Vurderingen skal gi ledelsen et grunnlag til å gjøre en informert og forsvarlig beslutning om hvorvidt Datatilsynet som behandlingsansvarlig skal opprette og kommunisere gjennom en side på Facebook.

Organisering og bakgrunnsarbeid

Bruk av Facebook som kommunikasjonsplattform har tidligere vært oppe til diskusjon internt i Datatilsynet, men det er ikke blitt gjort en reell vurdering av bruk av en side på plattformen opp mot samsvar med gjeldende personvernregelverk.

Vi nedsatte en tverrfaglig gruppe bestående av jurister, teknologer og en medieviter for å gjennomføre vurderingen.

Kartleggingen og analysen er primært basert på Facebooks personvernerklæring[2] og annet offentlig tilgjengelig materiale fra Facebook. Dette analysematerialet er fortrinnsvis hentet inn i perioden juli 2019 til og med februar 2020. I tillegg har vi hentet dokumentasjon fra andre kilder som vi har ansett som egnet til å belyse behandlingen og risikoene ved bruk av plattformen. Dommer, vedtak, veiledere og annen rettspraksis er benyttet for å belyse og vurdere Datatilsynets felles behandlingsansvar med Facebook.

Aktører og roller

Denne vurderingen tar sikte på å klargjøre roller og ansvar. Ved bruk av Facebook vil flere aktører involveres: tilbyderen (Facebook), eier av side (Datatilsynet), brukere (den registrerte) og andre aktører (for eksempel annonsører, underleverandører og partnere av Facebook). I denne vurderingen mener vi at det er spesielt viktig å identifisere, og så langt det lar seg gjøre, klargjøre rollene og ansvaret til henholdsvis Datatilsynet og Facebook i behandlingen.

Rollene og ansvaret i sosiale medier har blitt fremhevet gjennom rettspraksis fra EU-domstolen med dommene i Wirtschaftsakademie (C-210/16)[3] og Fashion ID (C-40/17)[4]. Begge sakene viser at samspill mellom sosiale medier og andre aktører kan føre til felles ansvar under personvernforordningen artikkel 26. Der det er felles behandlingsansvar, vil denne rapporten forsøke å avklare hvordan ansvarsfordelingen kan se ut mellom Facebook og Datatilsynet. Dommene er prosessert under det gamle lovverket, men overføringsverdien til nytt lovverk er høy, og muligens også skjerpende[5].

Gjennomføring

I denne vurderingen har vi tatt utgangspunkt i Datatilsynets egne maler for risikovurdering og vurdering av personvernkonsekvenser. Malene utgjør en bred ramme for å utforme og gjennomføre analysen og vurderingene.

Forordningens kapittel IV gir føringer og setter krav som den behandlingsansvarlige plikter å etterleve. Vi har strukturert analysen, vurderingene – og rapporten etter en fremgangsmåte det norske Datatilsynet selv har utarbeidet[6]. Fremgangsmåten er illustrert nederst i dette avsnittet. Den tar både for seg plikter den behandlingsansvarlige alltid må ivareta, og plikter som tilkommer dersom behandlingen antas å ha høy risiko for den registrertes rettigheter og friheter.

Vi starter med å gjøre en *systematisk beskrivelse av behandlingen* som skjer ved å ha en side på Facebook. Målet er at vi som behandlingsansvarlige skal få en fullstendig oversikt over behandlingen, og sørge for at beskrivelsene er komplette og tydelige. Beskrivelsene sees opp imot artiklene 24, 30, 32 i personvern-forordningen. Beskrivelsene omfatter behandlingens art, omfang, formål og sammenheng, kilder, mottakere og ansvarsforhold, samt informasjonssikkerhet, som inkluderer identifisering av informasjonssikkerhetsrisiko. Dessuten vurderer vi vårt

---

[2] https://www.facebook.com/policy.php

[3] C-210/16 *Wirtschaftsakademie*. Pressemelding: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081en.pdf

[4] C-40/17 *Fashion ID*. Pressemelding: https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf

[5] Se for eksempel: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/ny-dom-fra-eu-domstolen-om-fellex|s-behandlingsansvar/

[6] https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf

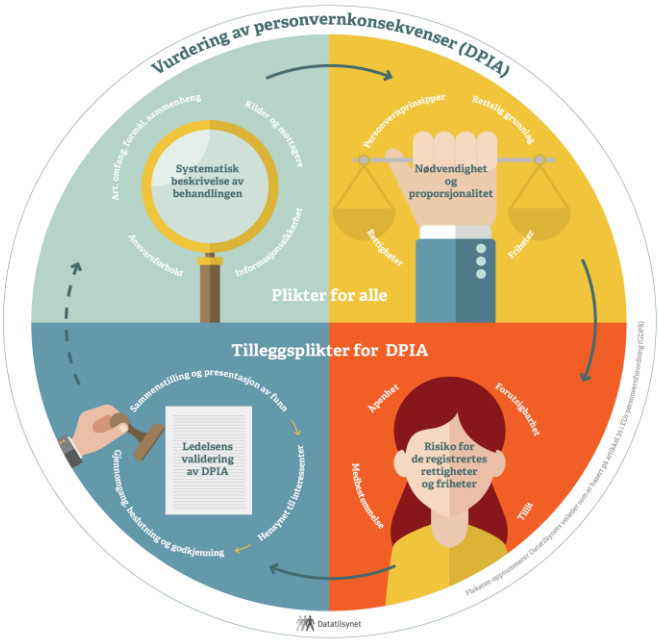
samsvar med bestemmelsene om felles behandlingsansvar med Facebook etter artikkel 26 i personvernforordningen.

Videre vurderer vi behandlingens nødvendighet og proporsjonalitet. Målet her å sikre at valgene vi som behandlingsansvarlig gjør, er legitime og utført slik at behandlingen står i rimelig forhold til formålene. Vi vurderer hvorvidt personvernprinsippene (artikkel 5, 6 og 9), de registrertes rettigheter (artikkel 12-22) og de registrertes friheter (fortalepunkt 4 og EMK artikkel 8) er ivaretatt. Her gjør vi også kort rede for vår vurdering av om bruk av side på Facebook er i samsvar med reglene om innebygget personvern og personvern som standardinnstilling etter artikkel 25.

Basert på kartlegging av art, omfang, formål og sammenheng gjort i den systematiske beskrivelsen, fant vi at det var høy risiko for den registrertes rettigheter og friheter. I vår vurdering av nødvendighet og proporsjonalitet fant vi at det var vanskelig å sette inn tiltak som reduserer risikoen i tilstrekkelig grad. Derfor gjennomførte vi også en vurdering av personvernkonsekvenser (DPIA, artikkel 35) for å se om vi likevel kan gjennomføre behandlingen. En DPIA innebærer å snu perspektivet, fra å fokusere på Datatilsilsynets egne plikter, til å se behandlingen fra den registrerte sin synsvinkel.

Arbeidsgruppen har rådført seg med Datatilsynets personvernombud (PVO) etter artikkel 35(2). PVO sine synspunkter er adressert i rapporten.

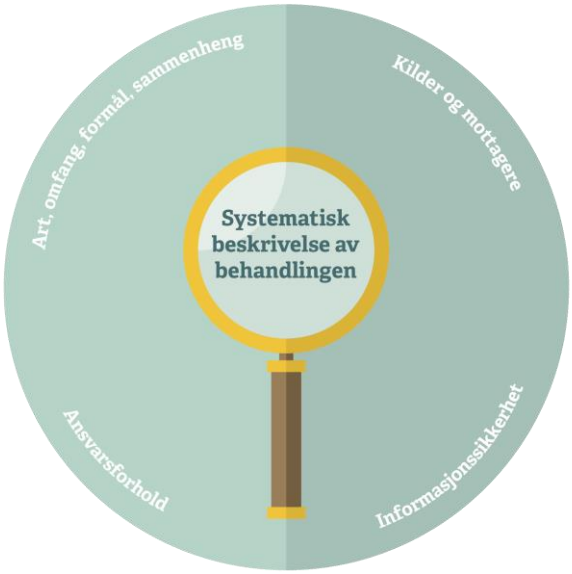
Arbeidet fører til en konklusjon og en anbefaling til ledergruppen.



«DPIA-hjulet»: Figuren oppsummerer og illustrerer den alminnelige prosessen ved gjennomføring av en vurdering av personvernkonsekvenser (DPIA).

Systematisk beskrivelse av behandlingen

I det følgende gjør vi en systematisk beskrivelse av behandlingen ved å gå gjennom behandlingens art, omfang, formål, sammenheng, kilder, mottakere, ansvarsforhold og informasjonssikkerhet jfr. figuren under. Målet er å få en så fullstendig oversikt som mulig over behandlingen og identifisere risiko ved bruk av en side på Facebook. Vi forsøker gjennomgående å skille Datatilsynets og Facebook sine behandlingsaktiviteter.



Art, omfang, formål og sammenheng

Behandlingens art
Beskrivelsen av behandlingens art omhandler behandlingens iboende karakteristikk:

Innsamling: Personopplysninger vil samles inn fra innhold som den registrerte selv skaper[7], altså ytringer og engasjement, enten dette fremkommer i relasjon til Datatilsynets egne publiseringer eller i toveiskommunikasjonen med brukere. I tillegg vil Faceboook samle inn observert data[8], og utlede ny data om brukere[9] som interagerer med Datatilsynets side.

Lagring: Datatilsynet er prisgitt hvordan Facebook velger å lagre og mellomlagre personopplysningene, samt hvordan Facebook velger å dele personopplysningene med søsterselskaper og andre eksterne samarbeidspartnere. Personopplysninger deles globalt[10][11].

Bruk: Datatilsynet vil bruke personopplysninger til å drive opplysning, debatt og innhente aggregert statistikk. Facebook kan blant annet sammenstille personopplysninger som genereres gjennom Datatilsynets side på tvers av sine produkter for å tilby og støtte produktene og tjenestene, samt tilby tilpasset innhold til brukerne. Facebook vil også utføre analyse av personopplysninger, for å profilere og tilpasse informasjon og annonser[12].

Tilgang til opplysningene: Publikum vil ha tilgang til alt materiale som deles på siden. Datatilsynets redaktør/moderator vil ha tilgang til direktemeldinger og upubliserte innlegg. Facebook vil i teorien ha tilgang all kommunikasjon på siden og vil også kunne gi tilgang til en rekke tredjeparter[13].

Hvem det skal samles inn opplysninger om:
Datatilsynet vil samle inn personopplysninger fra ansatte, artikkelforfattere og øvrige samarbeidspartnere, samt enhver som velger å interagere med Datatilsynets side.

Hvordan de registrerte kan utøve sine rettigheter:
Datatilsynet kan bistå den registrerte i noen grad, men er begrenset til å kunne gi informasjon om selve behandlingen og veilede brukerne i å utøve sine rettigheter på plattformen. Datatilsynets moderator kan rette og slette informasjon på vår side ved konkrete henvendelser, men denne informasjonen vil likevel være tilgjengelig for Facebook. Brukere vil kunne utøve en rekke rettigheter etter personvernforordningen på

---

[7] https://www.facebook.com/policy.php («Hvilke typer informasjon samler vi inn?»)

[8] Inkluderer også datapunkter til bruk for innsikt for eiere av side: https://www.facebook.com/legal/terms/page_controller_addendum

[9] https://www.facebook.com/about/privacy/update («Hvordan bruker vi denne informasjonen?»)

[10] Ibid. («Hvordan administrerer og overfører vi data som en del av våre internasjonale tjenester?»)

[11] https://www.facebook.com/legal/terms/ («Tjenestene vi leverer»)

[12] https://www.facebook.com/about/privacy/update («Hvordan bruker vi denne informasjonen?»)

[13] Ibid.

dedikerte sider i plattformen eller i brukergrensesnittet[14][15][16].

Hvorvidt det vil være en systematisk behandling av personopplysninger: Datatilsynets bruk av siden vil være målrettet og strategisk i henhold til visse redaksjonelle mål og kommunikasjonsplan, men det vil ikke være snakk om en systematisk behandling av personopplysninger. Facebook vil kontinuerlig utføre systematiske behandlinger av alle personopplysninger som genereres på Datatilsynets side[17].

Bruk av ny teknologi/ny bruk av eksisterende teknologi: For Datatilsynet vil opprettelse og bruk av en side på Facebook kunne betraktes som å ta i bruk ny teknologi. Oss bekjent er vi den første virksomheten i Norge som gjør en større analyse og vurdering av om bruk av en side på Facebook er i samsvar med personvernforordningen. Facebook benytter seg av stadig ny og innovativ teknologi som medfører nye typer behandlinger[18]. En teknologi som i sin natur er innovativ og i utvikling, og som har dynamiske avtalevilkår[19], vil kunne få praktiske og uforutsigbare konsekvenser for vår internkontroll og våre vurderinger i den systematiske beskrivelsen av Facebook, det juridiske ansvaret for oss som (felles) behandlingsansvarlig og for selve kommunikasjonen gjennom siden på plattformen.

Behandlingens omfang
Beskrivelsen av behandlingens omfang omhandler:

Kategorier personopplysninger: Av innhold Datatilsynet selv ønsker å dele på Facebook-siden, mener vi at det først og fremst vil fremkomme alminnelige personopplysninger som ikke faller inn under artikkel 9 i personvernforordningen, altså særlige kategorier personopplysninger. Vi må likevel ta noen forbehold når det gjelder personopplysninger som kommer frem gjennom visuelt og audiovisuelt innhold. Vi har også en del erfaringer fra vår veiledningstjeneste og vet at mange sårbare personer tar kontakt med Datatilsynet og ønsker å dele svært private og inngående personopplysninger som vil falle inn under artikkel 9. Vi kan ikke utelukke at samme type henvendelser vil forekomme ved Datatilsynets tilstedeværelse på Facebook, og at brukere vil kunne dele mange typer personopplysninger. Videre vil Facebook samle inn informasjon og innhold som brukere gir, informasjon om sider en bruker er i kontakt med samt enhetsinformasjon/metadata og observert data[20], og av dette kunne utlede nye kategorier personopplysninger og profilere personer[21].

Antall registrerte: Antall registrerte er vanskelig å anslå. Vi kan likevel estimere at Datatilsynets maksimale rekkevidde på brukere vil nå ca. 100 000 brukere i en femårsperiode. Det er omkring 3,5 millioner norske Facebook-brukere. På verdensbasis er det omkring 2,5 milliarder brukere på Facebook[22].

Volumet av data: Alle frivillig avgitte personopplysninger, kombinert med observert data og metadata vil kunne multipliseres med ca. 100 000 brukere[23]. Antall variabler og detaljeringsgrad vil derfor være stort og uklart for oss. For Facebook kommer profilering, sammenstilling og utledet data om disse 100 000 personene og all annen adferd og bruk på plattformen i tillegg. Facebook henter også personopplysninger utenfor plattformen og gjennom partnere[24], og kan potensielt sammenstille disse med personopplysninger som genereres gjennom Datatilsynets side. Facebook er et av selskapene i verden som behandler mest personopplysninger.

Frekvens: Datatilsynets moderator vil daglig og regelmessig følge med på og moderere siden, men i praksis vil det være en kontinuerlig behandling av personopplysninger med hensyn til egne formål. Facebook vil kontinuerlig, systematisk og automatisk

---

[14] Ibid.

[15] Se også: https://www.facebook.com/settings

[16] Se også: https://www.facebook.com/help/contact/367438723733209

[17] https://www.facebook.com/about/privacy/update («Hvilke typer informasjon samler vi inn?»)

[18] Ibid. For eksempel produktutvikling, forskning og innovasjon («Hvordan bruker vi denne informasjonen?»)

[19] https://www.facebook.com/legal/terms/update («Tilleggsbestemmelser»)

[20] https://www.facebook.com/about/privacy/update («Hvilke typer informasjon samler vi inn?»)

[21] Ibid. («Hvordan bruker vi denne informasjonen?»)

[22] For eksempel Statista: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[23] Et hypotetisk tilfelle.

[24] https://www.facebook.com/about/privacy/update («Hvilke typer informasjon samler vi inn?»)

behandle personopplysninger[25], inkludert personopplysninger fra Datatilsynets Facebook-side.

Lagringstid: Datatilsynet vil vurdere relevans og aktualitet for informasjon på siden minst én gang i året. Udatert informasjon slettes. Vi anser at maksimum slettefrist på informasjon på siden vår vil være fem år. Hvor lenge personopplysninger lagres i Facebook-systemet bestemmes ifølge selskapet fra sak til sak, og avhenger blant annet av arten av data, hvorfor den er hentet inn og behandlet, samt relevante juridiske eller driftsmessige bevaringsbehov. Facebook oppgir også at de sletter informasjon i den forstand at dataene skjules for brukerne. Samtidig sier Facebook at de sletter data når de ikke lenger er nødvendig[26].

Geografisk omfang: Datatilsynets innhold er ment for et norsk publikum, og vi har mulighet til å avgrense siden og innleggenes synlighet og tilgjengelighet basert på land. Facebook samler inn, lagrer og distribuerer personopplysninger i en egen infrastruktur med datasentre og systemer over hele verden[27]. Selskapet anvender også standard kontraktklausuler godkjent av EU-kommisjonen som overføringsgrunnlag[28][29]. Vurderingen vår fant sted før EU-domstolens avgjørelse i Schrems II-saken (C-311/18)[30] forelå, og derfor har vi ikke undersøkt hvilke ytterligere tiltak Facebook eventuelt har iverksatt som følge av denne dommen. Personopplysninger som genereres gjennom Datatilsynets side på Facebook vil være underlagt samme struktur, og vi må forvente at dataene lagres og behandles fra hvor som helst i verden.

Behandlingens formål

Beskrivelsen av behandlingens formål søker å vektlegge hva personopplysningene etter planen skal brukes til:

Formål: Datatilsynets formål med behandlingen er folkeopplysning og debatt. I den grad Facebook har et overordnet formål, er følgende formulering å finne på Facebooks forside: "Give people the power to build community and bring the world closer together." Facebook behandler imidlertid personopplysninger til en rekke formål: 1) Tilby tilpassede tjenester, samt forbedre dem, 2) utføre målinger og analyse for å støtte sine samarbeidspartnere, slik som annonsører, 3) fremme sikkerhet for å detektere uønsket materiale og for å opprettholde produktenes integritet, 4) kommunisere med sine brukere og bistå og 5) støtte forskning og innovasjon[31].

Kontrollformål[32]: Datatilsynet benytter ikke personopplysningene til kontrollformål. Vår vurdering er at Facebook neppe behandler personopplysninger til kontrollformål.

Treffe avgjørelser om den registrerte basert på systematisk/omfattende analyse: Datatilsynet benytter ikke personopplysningene til treffe avgjørelser om den registrerte basert på systematisk/omfattende analyse. Vi mener at Facebook bruker personopplysninger til å treffe avgjørelser om den registrerte basert på systematisk/omfattende analyse[33].

Betydningsfulle beslutninger for den registrerte: Datatilsynet benytter ikke personopplysningene til å treffe betydningsfulle beslutninger for den registrerte. Vår vurdering er at beslutningene som Facebook treffer om den registrerte er *betydningsfulle,* ettersom de bestemmer hvem som ser hva, som igjen kan påvirke den registrertes valg og beslutninger. Det kan imidlertid diskuteres om hvorvidt beslutningene som Facebook treffer om den registrerte faller inn under artikkel 22 i personvernforordningen. Vår vurdering er uansett at opplysninger generert gjennom vår side i liten grad medvirker i det totale beslutningsgrunnlaget.

Profilere: Datatilsynet benytter ikke personopplysningene til å profilere brukerne. Vi mener det er rimelig å anta at Facebook benytter personopplysninger til å profilere sine brukere, inkludert opplysninger som genereres gjennom vår side.

---

[25] Ibid.

[26] Ibid. («Datalagring, deaktivering og sletting av en konto»)

[27] Ibid. («Hvordan administrerer og overfører vi data som en del av våre internasjonale tjenester?»)

[28] https://www.facebook.com/help/566994660333381?

[29] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[30] C-311/18 *Schrems II*. Pressemelding: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[31] https://www.facebook.com/about/privacy/update («Hvordan bruker vi denne informasjonen?»)

[32] Jfr. punkt 3 «Behandlingens formål» i veilederen: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10362

[33] Flere eksempler listet under «Hvordan bruker vi denne informasjonen?» https://www.facebook.com/about/privacy/update

Avdekke ukjente sider/gjenkjenne mønstre: Datatilsynet benytter ikke personopplysningene til å avdekke ukjente sider eller gjenkjenne mønstre hos brukeren. Vi mener det er rimelig å anta at Facebook også benytter personopplysninger som genereres gjennom vår side til å avdekke ukjente sider eller gjenkjenne mønstre hos brukeren.

Viderebehandling av personopplysninger til nye formål: Datatilsynet benytter ikke personopplysningene som samles inn gjennom Facebook-siden til å viderebehandle personopplysninger til nye formål. Facebook har etter vår vurdering så vide og vagt formulerte formål[34] at det er vanskelig å si hva som behandles for opprinnelige formål og hva som behandles for såkalte *nye* formål.

Behandlingens sammenheng
Beskrivelsen av behandlingens kontekst ser på sammenhengen behandlingen utføres i:

Kilder: Datatilsynet vil hente personopplysninger direkte fra brukerens ytringer og innebygde muligheter for interaksjoner i plattformen. Vi kan også velge å kuratere eller dele innhold fra andre aktører på eller utenfor Facebook. Aggregert statistikk om interaksjon på egen side kommer fra Facebook. Facebook får tilgang til all informasjon som genereres gjennom Datatilsynets side på plattformen. Utover selve plattformen og domenet, samler Facebook inn personopplysninger fra blant annet nettsideintegrasjoner og plugins (for eksempel like-button), cookies[35], datterselskaper, partnere, reklamebyråer, og fra brukernes ulike enheter[36].

Relasjon: Datatilsynet er både ombud og tilsyn. Med andre ord er vi en offentlig myndighet, og brukere kan oppleve oss som en myndighet som kan treffe beslutninger og som potensielt har stor påvirkningskraft og faglig autoritet. For mange brukere kan vi oppleves som tillitsfull aktør og en «redning» og/eller garantist i personvernspørsmål. Det kan diskuteres om brukerne opplever interaksjonene med oss på Facebook som kommunikasjon med en myndighet eller som en hvilken som helst annen Facebook-side. Etter hvert som kommunikasjon med offentlige og private aktører på Facebook er blitt normalisert, er det grunn til å forvente at den registrerte vil kunne forholde seg annerledes til en tilsynsmyndighet på Facebook enn den samme tilsynsmyndigheten gjennom andre kanaler og andre kontekster. Kunnskap om mennesker er makt og Facebook vil sitte på mye og betydningsfulle personopplysninger om brukerne. Vår vurdering er at Facebook også vil sitte på informasjon som brukeren mest sannsynlig ikke selv er kjent med.

Den registrertes kontroll over sine personopplysninger: Brukeren kan slette og redigere egne innlegg og engasjement fra Datatilsynet side. Datatilsynet kan også bistå i sletting av informasjon fra siden. Innlegg som andre brukere allerede har delt, kan ikke slettes av brukeren selv, og heller ikke av Datatilsynet (så sant det ikke skjer på vår side). Facebook er i stand til å slette informasjon, men vår erfaring er at det er vanskelig å få kontakt med Facebook som eier av side eller som bruker. Vi mener at det kan være vanskelig for brukeren å holde oversikt over egen samhandling med Datatilsynet side *over tid*. Vi er også av den oppfatning at det kan være vanskelig å ha kontroll og oversikt over bruk, rekkevidde og konsekvenser av Facebooks videre behandling av personopplysninger som genereres gjennom siden.

Behandlingens forutsigbarhet for brukeren: Vi vil jobbe for at Datatilsynets behandling etter egne formål – vår kommunikasjonsvirksomhet - vil oppfattes som begrenset i omfang, ryddig og profesjonell. De fleste brukere av Facebook vil være kjent med å kommunisere med sider, og slik sett vil behandlingen kunne oppleves som forutsigbar. Likevel er det trolig flere aspekter ved behandlingen som kan oppleves som uforutsigbare. Mange vil ikke være innforstått med rekkevidden, synligheten og offentligheten av deres ytringer og interaksjoner på plattformen, inkludert samhandling med sider. Brukeren forstår kanskje ikke informasjonens *virale* kraft, som her betyr at den har potensiale til å spres videre utenfor siden gjennom deling, tagging og nyhetsstrøm. Det kan være at den registrerte oppgir for mye personlig informasjon, inkludert særskilte kategorier data, i en slags misforstått fortrolig dialog med Datatilsynet, enten offentlig eller i direktemelding. Den enkelte kan misforstå Datatilsynets tilstedeværelse som en garanti for at plattformen er mer personvernvennlig enn den faktisk er. Mange er nok ikke klar over at all interaksjon bruker har med Datatilsynets side vil samles inn og sammenstilles med øvrig informasjon som Facebook sitter på om dem. Mange vil være uvitende om at informasjonen som

[34] Ibid. («Hvordan bruker vi denne informasjonen?»)

[35] Spesifikt om cookies: https://www.facebook.com/policies/cookies/

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

genereres om dem gjennom Datatilsynets side kan lagres globalt og kan deles med en rekke søsterselskaper, partnere og tredjeparter. Mange vil nok også være ukjent med omfanget av opplysninger som genereres om dem over tid og «minnet» Facebook har om dem.

Særskilt forventning om konfidensialitet: Vi tror at de fleste brukerne ikke har en *særskilt* forventning konfidensialitet. Samtidig er det rimelig å anta at mange ikke vet hva de kan eller bør forvente med tanke på konfidensialitet, eksempelvis barn eller lite erfarne og kompetente brukere. Enkelte vil trolig ha forventning om konfidensialitet i sidens direktemeldingsfunksjon[37]. Endelig er det vår vurdering at det vil foregå en rekke behandlinger som brukeren ikke er kjent med og dermed heller ikke kan ha noen forventning til.

Særskilt forventning om nødvendig og korrekte opplysninger: Brukere oppgir i stor grad sine egne personopplysninger, inkludert meningsytringer og engasjement. Facebook vil utlede ny informasjon om brukeren som genereres på Datatilsynets side. Den registrerte vil vite lite om hvorvidt de utledete dataene, eller profileringen, blir korrekt - eller om hvor viktig "korrekthet" er for avgjørelsene som Facebook treffer om brukerne.

Særskilt forventning om privatliv: Mange har en idé om hvordan Facebook opererer, og vil ikke ha en slik forventning. Men det vil være rimelig å anta at mange ikke vet hva de kan eller bør forvente med tanke på privatliv i sosiale medier, eksempelvis barn eller lite erfarne eller lite kompetente brukere. Det vil også trolig overraske mange hvor detaljert, nært og "intimt" Facebook kan gå for å samle inn og behandle enkelte typer personopplysninger, ikke minst med tanke på kombinasjonen av flere data. Flere kan misforstå direktemeldingsfunksjonen som en reell privat eller mer fortrolig kanal (på lik linje med lukkede grupper på Facebook).

Personopplysninger om barn, pasienter eller andre sårbare kategorier personer: Datatilsynet vil ikke publisere personopplysninger om identifiserbare, sårbare kategorier personer på siden. Vi må samtidig ta høyde for at sårbare kategorier personer kan velge å interagere med siden og oppgi opplysninger om seg selv, og at andre brukere kan oppgi personopplysninger om slike personer. Facebook vil behandle sårbare kategorier personer dersom slike personopplysninger genereres gjennom siden. Det er satt en aldersgrense på bruk av Facebook til 13 år. Vi vet likevel at Facebook benyttes av barn som er yngre enn 13[38].

Tidligere erfaring med tilsvarende type behandling: Oss bekjent er det ikke foretatt en analyse og risikovurdering etter personvernforordningen av en behandlingsansvarlig som ønsker å bruke side på Facebook. Det finnes lignende typer kommunikasjonsplattformer som *kan* ha tilsvarende type behandlinger, eksempelvis Instagram, Twitter, LinkedIn.

*Eventuelle relevante fremskritt innen teknologi eller sikkerhet***:** Selskapet publiserer jevnlig nyheter om tiltak de gjør for å fremme personvern i produktene sine[39]. De skriver på bloggen sin at det nye designet skal sette Facebook-grupper og arrangementer i sentrum, som etter Facebooks mening gjør plattformen mer privat og personvernvennlig[40]. Vi er også kjent med at Facebook har uttalte visjoner om å innføre kryptering på enkelte typer informasjon som gjør at Facebook selv ikke kan aksessere informasjonen. Et annet forslag fra selskapet er å sette tidsfrister og levetid slik at enkelte typer informasjon blir fjernet automatisk som standardinnstilling[41].

Allmenn bekymring omkring den beskrevne måten å behandle personopplysninger på: Facebook har i senere år vært under konstant mediedekning og press fra myndigheter og organisasjoner vedrørende overholdelse av personvernlovgivning og respekt for enkeltmenneskers privatliv og personvern[42]. I januar 2020 valgte et av de tyske datatilsyns-myndighetene, *Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg* (LFDI), å

---

[37] F.eks: https://www.an.no/nyheter/norsk-advokat-ble-overvaket-av-usa-pa-facebook/s/1-33-6704657

[38] Se f.eks. https://medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/200211-barn-og-medier-2020-delrapport-1_-februar.pdf

[39] https://about.fb.com/news/tag/privacy-matters/

[40] https://www.dn.no/medier/mark-zuckerberg/messenger/whatsapp/mark-zuckerberg-endevender-facebook-designet/2-1-595876

[41] https://about.fb.com/news/2019/03/vision-for-social-networking/

[42] Kanskje best eksemplifisert av Cambidge Analytica-saken: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

avslutte konto på Twitter[43][44] grunnet dommene relatert til artikkel 26 om felles behandlingsansvar med utgangspunkt i manglende samsvar med personvernforordningen.

Behandling av personopplysninger fra ulike datasett, for ulike formål, fra ulike behandlingsansvarlige, samt kobling fra ulike registre for å gi ny type informasjon om den registrerte: Datatilsynet vil ikke behandle personopplysninger fra ulike datasett eller koble ulike registre for å få nye typer informasjon om de registrerte. Facebook, og forskjellige underselskaper og tredjeparter, vil potensielt kunne bruke data og datasett med personopplysninger som genereres fra Datatilsynets side. Vår vurdering er at personopplysninger som blir importert fra andre samarbeidspartnere kobles opp mot eksisterende brukere[45].

Ansvarsforhold, kilder og mottakere

Beskrivelsen av kilder og mottakere skal gi en oversikt over mottakere, dataflyt og lagring:

Identifisering av behandlingsansvarlig, felles behandlingsansvarlig og databehandlere: Datatilsynet og Facebook vil på enkelte områder være behandlingsansvarlig hver for seg. Datatilsynet og Facebook vil imidlertid være felles behandlingsansvarlig for noen aktiviteter. Vår vurdering er at det vil foreligge et felles behandlingsansvar mellom Facebook og oss som eier av side. Vi har ikke funnet en oversikt over øvrige databehandlere og underleverandører som er tilgjengelig for offentligheten. Vi har videre funnet Facebook sin avtale med eiere av side om felles behandlingsansvar, "Facebook page insights"[46]. Denne kan ikke reforhandles, og omfatter kun noen av behandlingsaktivitetene som vi mener vi er felles behandlingsansvarlige for med Facebook. Vi redegjør for felles behandlingsansvar i rapportens Vedlegg 1.

Identifisering av mottaker av personopplysninger: All informasjon og engasjement på offentlige innlegg på vår side på Facebook, vil i praksis være tilgjengelig for alle. Datatilsynets redaktør og moderator vil i tillegg ha tilgang til sidens direktemeldinger og aggregert statistikk. Facebook overfører data innenfor Facebook-konsernet[47], til tjenesteleverandører og til tredjeparter, og andre partnere[48]. Facebook overfører personopplysninger til land utenfor EU/EØS-området.

Identifisering av dataflyt, lagring og mellomlagring: Facebook overfører personopplysningene globalt, både internt i Facebook-selskapene og eksternt med sine partnere samt brukere[49]. Vi har ikke klart å finne noe flytskjema for hvor og hvor lenge personopplysninger lagres ulike steder. Se også «Lagring» på side 9.

Personopplysningssikkerhet

I denne beskrivelsen vurderer vi om behandlingens personopplysningssikkerhet er tilstrekkelig ivaretatt i henhold til artikkel 32.

Risiko knyttet til personopplysningssikkerhet er sammenhengen mellom verdier, trusler/trusselaktører og sårbarheter. Vår konkrete vurdering av disse, samt tiltak for å redusere risiko knyttet til personopplysningssikkerheten, kommer frem i rapportens vedlegg 2.

Facebook beskriver intern organisering av informasjonssikkerhet[50][51]. Vi må være klar over at dersom vi tar i bruk Facebook, må vi akseptere de premisser for sikkerhet som Facebook til enhver tid setter overfor eiere av side. Vi mener imidlertid at Facebook ønsker og har iverksatt tiltak med henblikk på å ivareta sin interne informasjonssikkerhet. Facebook sier[52] at de årlig har en tredjepart SOC 2 type II-revisjon relatert til databehandlingstjenestene, og annen revisjon etter bransjestandard som anses passende av Facebook som del av Facebooks revisjonsprogrammer. SOC2 tar for seg internkontroller knyttet til informasjonssikkerhet

---

[43] https://www.baden-wuerttemberg.datenschutz.de/bye-bye-twitter/

[44] LfDI tydeliggjør viktige krav for myndigheters bruk av sosiale medier i en pressemelding: https://www.baden-wuerttemberg.datenschutz.de/lfdi-stellt-wesentliche-anforderungen-an-die-behoerdliche-nutzung-sozialer-netzwerke-klar/

[45] https://www.facebook.com/about/privacy/update (flere oppføringer)

[46] https://www.facebook.com/legal/terms/page_controller_addendum

[47] https://www.facebook.com/help/111814505650678

[48] https://www.facebook.com/about/privacyshield

[49] https://www.facebook.com/privacy/explanation

[50] https://www.facebook.com/legal/terms/dataprocessing

[51] https://www.facebook.com/legal/terms/page_controller_addendum

[52] https://www.facebook.com/legal/terms/dataprocessing

generelt. Vi er usikker på hvilke bransjestandarder som Facebook anser som passende å revidere etter i tillegg.

Oppsummering og vurdering: systematisk beskrivelse av behandlingen

I dette kapittelet har vi fremlagt en beskrivelse av behandlingen av personopplysninger som skjer ved å opprette og kommunisere gjennom en side på Facebook. Gjennom beskrivelsen av art, omfang, formål og sammenheng kan vi utlede en første identifisering av risiko for den registrertes personvern og rettigheter og friheter. Vi oppsummerer risikoene og arbeidsgruppens vurderinger av dem under:

Risiko knyttet til behandlingens art:

- Arbeidsgruppen mener det er vanskelig for Datatilsynet å hjelpe den registrerte å utøve sine rettigheter etter personvernforodningen overfor Facebook
- Arbeidsgruppen mener at behandlingen av personopplysninger er preget av uforutsigbarhet
- Arbeidsgruppen mener at behandlingen av personopplysninger er preget av mangel på åpenhet overfor den registrerte
- Arbeidsgruppen er mener det er usikkerheter rundt ivaretakelsen av flere personvernprinsipper
- Arbeidsgruppen mener at vår kommunikasjon på en side medfører systematisk behandling i form av innsamling, profilering og automatiserte avgjørelser
- Arbeidsgruppen mener at spørmål om maktforhold i relasjonen mellom selskap og enkeltbruker kan problematiseres
- Arbeidsgruppen mener at det er snakk om innovativ teknologi som er i stadig endring

Risiko knyttet til behandlingens omfang:

- Arbeidsgruppen mener at behandlingen vil innebære en rekke kategorier personopplysninger, herunder potensielt særskilte kategorier data.
- Arbeidsgruppen mener at behandlingen potensielt vil innebære behandling av personopplysninger om sårbare personer
- Arbeidsgruppen mener at behandlingen vil innebære et høyt antall registrerte.
- Arbeidsgruppen mener at volumet av personopplysninger om den registrerte er stort og detaljert
- Arbeidsgruppen mener at det er visse usikkerheter rundt lagringstid, som potensielt er permanent.
- Arbeidsgruppen mener at det geografiske omfanget på lagring er globalt, det vil si også utenfor EU/EØS.

Risiko knyttet til behandlingens formål:

- Arbeidsgruppen mener at Facebook sine formål er vage, uklare og omfattende. Vi mener de i stor grad divergerer fra de formål arbeidsgruppen selv har definert for behandling.
- Arbeidsgruppen er usikre på om personopplysningene vil brukes til nye eller andre formål.
- Arbeidsgruppen mener at beslutningene som tas om den registrerte kan få betydelig betydning for den registrerte
- Arbeidsgruppen mener at det treffes beslutninger om den registrerte basert på systematisk og omfattende analyse av personopplysninger

Risiko knyttet til behandlingens sammenheng:

- Arbeidsgruppen mener det er flere usikkerheter rundt kilder, datasett og sammenstilling av forskjellige datasett på og utenfor plattformen
- Arbeidsgruppen mener den registrerte vil kunne ha en forventning om konfidensialitet og privatliv i visse typer kommunikasjon med en side på plattformen.
- Arbeidsgruppen mener det er vanskelig for den registrerte å ha oversikt og kontroll over egne opplysninger.
- Arbeidsgruppen mener at dataflyten og kjeden av behandlinger er uklar, inkludert hvem som er mottakere av personopplysninger

I vår vurdering av felles behandlingsansvar (Vedlegg 1) forsøker vi å kartlegge roller og ansvar mellom Datatilsynet og Facebook i behandlingen. Arbeidsgruppen har kommet frem til følgende:

- Datatilsynet har felles behandlingsansvar med Facebook, ref. dommene Fashion ID og Wirtschaftsakademie, ved opprettelse av en side på Facebook.

Datatilsynet og Facebook vil etter vår vurdering i hvert fall være felles behandlingsansvarlig for følgende:

- Datatilsynet og Facebook vil være felles behandlingsansvarlig for innsamling av personopplysninger om personer som besøker og interagerer med Datatilsynets Facebook-side.

- Datatilsynet og Facebook vil være felles behandlingsansvarlig for resultatet av analysen av personopplysninger om personer som besøker og interagerer med Datatilsynets Facebook-side («Page Insights»).
- Arbeidsgruppen er usikre om Datatilsynet vil ha et visst felles behandlingsansvar for at Facebook bruker personopplysninger om brukere som besøker Datatilsynets Facebook-side til å berike personprofiler med formål å levere persontilpasset innhold og markedsføring.

Som konsekvens av å konstatere et felles behandlingsansvar, mener vi i tillegg at:

- Datatilsynet og Facebook har et felles ansvar for å informere på en åpen, tilgjengelig og forståelig måte om hva brukernes personopplysninger vil brukes til.
- Facebok og Datatilsynet er felles ansvarlige for at de registrertes rettigheter og friheter ivaretas.

Vi vurderer at Datatilsynets samsvar med personvernforordningen artikkel 26 er som følger:

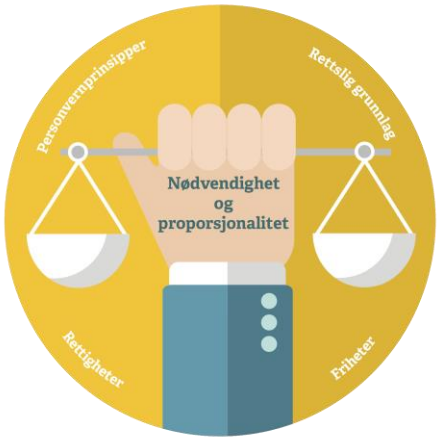
- Datatilsynet vil *kun delvis* oppfylle artikkel 26(1) i personvernforordningen.
- Datatilsynet vil *kun delvis* oppfylle artikkel 26(2) i personvernforordningen.
- Datatilsynet vil *ikke* oppfylle artikkel 26(3) i personvernforordningen.

Videre oppsummerer vi vår vurdering av hvorvidt behandlingens personopplysningssikkerhet (Vedlegg 2) er ivaretatt:

- I verdivurderingen kom vi frem til at vårt krav til integritet for verdien *Offentlig kommunikasjon* (informasjon som Datatilsynet selv velger å publisere på plattformen, jfr. formål 1) på siden er «høy». Vi kom også frem til at våre krav til konfidensialitet og integritet er henholdsvis «svært høy» og «høy» for verdien *Kommunikasjon med brukere* (kommentarer, direktemeldinger, engasjement og andre interaksjoner mellom Datatilsynet og brukere, jfr. formål 2*)*.
- I trusselvurderingen har vi identifisert og beskrevet et utvalg av det vi anser som de mest aktuelle truslene/ trusselaktørene. Dette inkluderer vanlige brukere, barn, mentalt ustabile personer, nettaktivister, nettroll og ansatte i Datatilsynet.
- I sårbarhetsvurderingen har vi beskrevet våre antatte sårbarheter i denne behandlingen, som inkluderer f.eks. publiseringer uten avklaring, mangel på kontroll over sidens kommentarfelt og informasjonsflyt, eller svak tilgangskontroll.
- Vi mener at enkelte risikoer knyttet til personopplysningssikkerheten i behandlingen kan reduseres ved å sette inn tiltak, f.eks. ved å fastsette rutiner og ansvar for moderering, aktivere to-faktor-autentisering, og definere roller og ansvar.
- Vår vurdering er at vi må kunne stole på at Facebook er i stand til og sørger for å ivareta sin interne informasjonssikkerhet.

Nødvendighet og proporsjonalitet ved behandlingen - interesseavveining

I dette kapittelet vurderer og kvalitetssikrer vi at behandlingen, slik den er beskrevet i den systematiske beskrivelsen i forrige kapittel, er nødvendig og proposjonal. Dette innebærer vurdering av det rettslige grunnlaget for behandlingen, ivaretakelse av personvernprinsippene, og brukerenes rettigheter og friheter, jfr. figuren under.



Rettslig grunnlag

Datatilsynets rettslige grunnlag for å ta i bruk en side på Facebook vil være personvernforordningens artikkel 6(1)(f) interesseavveiing. Dette rettslige grunnlaget gir oss som virksomhet anledning til å behandle personopplysninger dersom det er nødvendig for å ivareta en berettiget interesse som veier tyngre enn hensynet til den enkeltes personvern.

Facebook benytter flere behandlingsgrunnlag overfor den enkelte bruker avhengig av type behandling, for eksempel kontrakt, samtykke, legitime interesser, i allmennhetens interesse og rettslige forpliktelser[53].

Datatilsynets interesser:
Datatilsynets interesser legitimeres i formål 1 og 2, som er definert i rapportens innledning.

Hvilke fordeler oppnår virksomheten med behandlingen og hvor viktige er disse fordelene for virksomheten?

Mange av fordelene ved å opprette og kommunisere gjennom en side på Facebook, er nevnt i rapportens innledende kapittel. Kommunikasjonsavdelingen ser på mange måter på tilstedeværelse gjennom en side på Facebook som en «luksuskanal». I dette legger vi at kanalen hverken erstatter eller innoverer virksomhetens kommunikasjon som sådan. Men heller vil kommunikasjon i denne kanalen supplere annen kommunikasjon. Den vil kunne gjøre oss *mer* tilgjengelige for viktige målgrupper, *øke* synlighet av og kjennskap til budskapene og virksomheten i befolkningen, og oppnå *større* effekt av allerede produsert innhold og igangsatte tiltak. I tillegg er kanalen egnet til å kommunisere multimedialt innhold, som virksomhetens satsing på innhold som video og livestrømming vil kunne nyte godt av. Kanalen vil også kunne gjøre det lettere å være en *mer* aktiv og tydelig stemme i personverndebatten, og samtidig *øke* demokratisk deltakelse.

Har behandlingen offentlig interesse eller varetar den ideelle interesser som kommer flere til gode?

Vi mener at tilstedeværelse på Facebook nettopp vil ha som hovedmål å være i offentlighetens interesse. Vi argumenterer for at vår tilstedeværelse i kanalen vil gjøre oss mer åpen og tilgjengelig, og tilrettelegger for mer medvirkning fra norske innbyggere. Tilstedeværelse i kanalen vil gi Facebook-brukerne, altså innbyggerne, mulighet til å få klar, korrekt og oppdatert informasjon om sine personvernrettigheter og -plikter i henhold til regelverket, få tilgang til nyheter og informasjon om Datatilsynets virksomhet og interesseområder, samt inviteres til å delta i debatter på personvernfeltet med Datatilsynet som moderator. Interessen bør spesielt begrunnes i at mange benytter kanalen som sin primære informasjons- og nyhetskanal, der brukerne selv abonnerer på personer, virksomheter og merkevarer de er interessert i. Det betyr at vi også i større grad kan nå innbyggere med nyheter og annen informasjon som de «ikke visste at de trengte» i sin daglige informasjonsflyt, fremfor at de kun får informasjon fra oss når de aktivt søker etter det.

Hensynet til personvernet:
Ved å ha en side på Facebook vil vi generere en rekke

[53] Se fullstendig oversikt: https://www.facebook.com/privacy/explanation

personopplysninger og muliggjøre flere typer behandlinger for både Datatilsynet og Facebook. I den systematiske beskrivelsen oppsummeres en rekke vurderinger av risiko og hensynet til personvernet. I tillegg ønsker vi her å trekke frem noen vurderinger av hensynet til personvernet av mer etisk karakter, eksempelvis:

- Datatilsynet som troverdig samfunnsaktør og som rollemodell for personvern og foregangseksempel for samsvar med personvernforordningen
- Datatilsynets eget omdømme og etiske standard
- Datatilsynets tilstedeværelse på Facebook kan oppfattes som en garanti for plattformens hensyn til personvernet
- Vi tror *ikke* behandlingen vil ha en nedkjølende effekt på befolkningen
- Vi vet ikke hva potensielle registrerte eller øvrige interessenter utenfor virksomheten vil mene om denne behandlingen av personopplysninger.
- Vi har grunn til å tro at det vil være flere ulike og motstridende synspunkter på behandlingen innad i Datatilsynet.

Tiltak for å minimere personvern-konsekvensene:
Datatilsynet vil være prisgitt Facebook og deres betingelser ved å ta i bruk en side på plattformen. Det betyr at vi har ingen mulighet til å inngå egne avtaler med eller på annen måte påvirke Facebooks behandling av personopplysninger. Samtidig må vi være klar over at betingelsene når som helst kan endres av Facebook. Likevel kan vi fremsette noen viktige poenger og iverksette noen tiltak for å bedre personvernvilkårene:

- Vi vil kunne gå lengre enn de fleste virksomheter i å være åpen rundt vårt valg av kommunikasjons-plattform og være transparent om våre vurderinger rundt behandlingen av personopplysninger og demonstrere eget ansvar som følger av å kommunisere gjennom en side på Facebook. Den aller viktigste informasjonen vil være på plass ved opprettelse av side, og kan for eksempel gjøres tilgjengelig i beskrivelsen av siden («About»), ha en festet post øverst på siden, samt ha en dedikert og mer detaljert erklæring på Datatilsynets hjemmeside. Det er imidlertid mye vi ikke vet om behandlingen.
- Vi bør også være åpen om vårt kanalkonsept og utøvelse av intern policy og moderering i kanalen, slik at denne er forutsigbar for brukere. Denne må også være kjent internt.
- Fange opp endringer i Facebooks avtale/vilkår med eiere av side, samt definere og fange opp eventuelle avvik. I tillegg bør vi fange opp negative medieoppslag og annen type negativ publisitet som angår vår tilstedeværelse på plattformen.
- Vi vil kunne iverksette tiltak som beskrevet i underkapittel om informasjonssikkerhet i den systematiske beskrivelsen av behandlingen, eksempelvis god passordhygiene og tofaktorautentisering.
- Ikke benytte Facebook-plugins eller liknende på egen hjemmeside. Dette for å minimere mengden data som samles inn utenfor Facebook.

Det er vanskelig å rettferdiggjøre våre egeninteresser av å bruke Facebook-side når vi ser den omfattende behandlingen av personopplysninger det innebærer, samt de begrensede mulighetene Datatilsynet for å sette inn personvernfremmende tiltak.

Personvernprinsippene

Rettferdighet
Datatilsynet vil at behandling av personopplysninger på en side på Facebook skal være rettferdig og at behandlingen av personopplysninger skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Dessuten vil vi at behandlingen skal være gjennomsiktig og forståelig for de registrerte, og ikke foregå på fordekte eller manipulerende måter. Tiltak som åpenhet om intern policy om moderering og en tilgjengelig kontaktperson vil bidra til dette. Selv om Datatilsynet vil at behandlingen skal være rettferdig, er vi likevel i stor grad prisgitt Facebook.

Arbeidsgruppen er usikre på om og eventuelt til hvilken grad Facebook behandler personopplysningene i respekt for de registrertes interesser, for eksempel når brukeren får innhold og reklame relatert til den digitale profilen Facebook har gitt brukeren. Ut ifra vår vurdering kan behandlingen av brukerens personopplysninger overgå den registrertes forventninger, både for konkrete typer kommunikasjon på en side og på plattformen generelt. Personopplysningene som Facebook samler inn brukes for å treffe beslutninger om og påvirke brukere. Facebooks analyser, profileringer og beslutninger kan være lite transparente, og vi er bekymret for at profileringen kan være diskriminerende og manipulerende. Det er imidlertid usikkert hvor mye Datatilsynets side på plattformen vil bidra til dette.

Åpenhet
Datatilsynet vil gi informasjon til den registrerte. Vi er imidlertid bekymret for at behandlingen av personopplysninger og tydeliggjøring av ansvar kan være preget av mangel på åpenhet overfor eiere av side

og den registrerte. Videre er det rimelig å stille spørsmålstegn ved den offentlige dokumentasjonen til Facebook sin tilgjengelighet og fullstendighet. Dokumentasjonen fremstår kompleks og preget av vanskelig språk og struktur. Etter å ha lest dokumentasjonen, og forsøkt å gjøre en komplett systematisk beskrivelse av behandlingen på plattformen, er det fremdeles mye vi ikke vet om behandlingen. Det er problematisk i et personvernperspektiv.

Formålsbegrensing
Vi mener at Datatilsynets egenformulerte formål er klart spesifisert og samsvarer med forventingene til brukerne i kontekst av å følge og interagere med en side på Facebook.

For Facebook mener vi at formålene kan være vide, vage og altomfattende. Derfor tror vi at det er vanskelig for brukerne å vite hva deres personopplysningene faktisk brukes til.

Dataminimering
Vi mener at formålet med behandlingen kan oppnås ved å begrense innsamling av personopplysninger, ved å bruke mindre detaljerte personopplysninger og uten bruk av fortrolig eller særlige kategorier personopplysninger. For Datatilsynets del, bør data slettes etter formålet er oppnådd, for eksempel etter seks måneder. Vi mener også at behandlingen kan oppnås ved større grad av pseudonyme og/eller aggregerte personopplysninger.

Datatilsynet kan imidlertid ikke hindre brukere i å ytre og dele hva de vil på siden, og det er heller ikke målet. Vi kan heller ikke påvirke hva Facebook samler inn av brukerens delte data, metadata, observert data og utledete data når de interagerer med siden vår. Vi mener at vi heller ikke har en oversikt over omfanget av Facebook sin videredeling av innsamlet informasjon til andre aktører.

Vi mener det er vanskelig å opptre i henhold til kravet om dataminimering i kontekst av en side på Facebook. Vi mener dette må sees i sammenheng med selskapets forretningsmodell, som er å samle inn store og detaljerte mengder informasjon om Facebook-brukere, som de igjen kan benytte til egne formål.

Riktighet
Når Datatilsynet publiserer informasjon på siden kvalitetssjekker vi riktighet i det vi legger ut. De registrerte vil selv kunne redigere, oppdatere og slette egne innlegg og engasjement. Datatilsynet vil aldri kunne garantere riktighet av det brukerne legger ut. Moderator vil også vurdere brukernes innlegg opp mot vår egen policy, og teoretisk sett slette innlegg som av forskjellige grunner vurderes som «uriktige». Brukerne kan melde fra om innlegg som de mener er uriktige og bør slettes, enten til Facebook eller til eier av siden.

Facebook gir til en viss grad brukeren kontroll over informasjon de selv velger å dele, de kan rapportere informasjon som andre legger ut og de kan protestere på utvalgte behandlinger. Vi vil påstå at en del av kommunikasjonen på siden vil være synspunkter, tolkninger og lignende. Derfor mener vi at det kan argumenteres for at prinsippet om riktighet er mindre relevant i kontekst av å kommunisere gjennom en side på Facebook. siden det er uklart hvilke type behandlinger Facebook utfører, vil det i praksis være vanskelig for brukeren å ettergå om personopplysninger er korrekte[54].

Lagringsbegrensning
Moderator vil fortløpende slette innformasjon som ikke er relevant, som kan oppfattes støtende eller som inneholder særlige kategorier personopplysninger. Moderator vil vurdere alle innlegg årlig og som utgangspunkt slette alle innlegg på siden som er over 5 år gamle. Dynamisk innhold på siden vil etter vårt syn ikke være arkivverdig og vil derfor ikke arkiveres utenfor plattformen.

Vår vurdering er at det er uklart i hvilken grad Facebook sletter informasjon på eget initiativ. Facebook skriver at brukeres opplysninger slettes straks de ikke lenger er nødvendige for å tilby tjenester til en bruker, eller når en brukerkonto slettes[55].

Integritet og konfidensialitet
I den *systematiske beskrivelsen av behandlingen* utredet vi vår vurdering av behandlingens personopplysningssikkerhet. Vi mener at Facebook ønsker og har iverksatt tiltak med henblikk på å ivareta sin interne informasjonssikkerhet. Vi mener at enkelte risikoer knyttet til personopplysningssikkerheten ved

[54] Se f.eks diskusjon i https://agendamagasin.no/kommentarer/tror-diskret-pa-nettet-tro-igjen/

[55] https://www.facebook.com/privacy/explanation

behandling av opplysninger på siden kan reduseres til et akseptabelt nivå ved å sette inn sikkerhetstiltak.

De registretes rettigheter og friheter

Vår mulighet til å legge til rette for og forbedre de registrertes rettigheter og friheter er minimale, og er i stor grad prisgitt Facebook. Datatilsynet behandling av personopplysninger vil etter vår vurdering, isolert sett, ikke være til hinder for retten til ikke bli diskriminert, tanke-, tro- eller religionsfrihet, eller ytrings- og informsjonsfrihet. Uavhengig av Datatilsynets rutiner og innsats, vil vi ikke kunne påvirke Facebooks etterfølgende behandling av personopplysninger og dermed ikke de prosessene som i siste instans kan lede til for eksempel manipulasjon eller diskriminering.

Vi mener at Facebooks informasjon kan være utfordrende å forstå og at de fleste brukerne kanskje ikke vil skjønne omfang og rekkvidde av behandlingen. Mer spesifikt mener vi at informasjonen tidvis kan være preget av teknisk og juridisk sjargong samt uklare og vage formuleringer, og det er vanskelig å finne frem i store mengder informasjon. Dette gjelder også rettighetene, som vi stiller spørsmålstegn ved om er relle og fullstendige. Vi mener at det er et stort forbedringspotensiale i måten de registrertes rettigheter og friheter kan ivaretas av Facebook. Facebooks analyser, profileringer og beslutninger kan være lite transparente og vi er bekymret for at profileringen både vil kunne virke diskriminerende og være manipulerende. Det er imidlertid usikkert hvor mye Datatilsynets side på plattformen vil bidra til dette, og hvor mye ansvar vi har, jfr vurdering av felles behandlingsansvar.

Artikkel 25 Krav om innebygget personvern og personvern som standardinnstilling

Den behandlingsansvarlige plikter å anskaffe, ta i bruk og vedlikeholde løsninger, programmer og verktøy som behandler personopplysninger etter kravene i personvernforordningens artikkel 25 om innebygget personvern og personvern som standard innstilling.

Hovedbudskapet ved innebygget personvern og personvern som standardinnstilling er at tiltakene skal bidra til å effektivt implementere og vedlikeholde personvernprinsippene, samt de registrertes rettigheter og friheter i behandlingen ved løsningen som benyttes.

Gjennomgående i vår vurdering av nødvendighet og proporsjonalitet ved bruk av side på Facebook, avdekker vi at på tross av at Datatilsynet selv har en intensjon om å ivareta personvernprinsippene og de registretes rettigheter og friheter, er vi likevel prisgitt Facebook og deres betingelser ved å ta i bruk en side på plattformen.

Uten at vi går dypere inn i en vurdering av kravene i artikkel 25, stiller vi spørsmål ved om

§ Artikkel 25: Innebygd personvern som standardinnstilling

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

2. Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.

3. En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.

personopplysningene som samles inn ved side på Facebook vil behandles i henhold til krav om innebygd personvern og personvern som standardinnstilling.

Oppsummering og vurdering: nødvendighet og proporsjonalitet

Oppgaven i dette kapittelet var å vurdere om våre behandlingsaktiviteter er nødvendige og om de er rimelige i forhold til formålene.

- Datatilsynets rettslige grunnlag for å ta i bruk en side på Facebook er personvernforordningen artikkel 6(1)(f) interesseavveiing. Arbeidsgruppen mener at vi har en rekke interesser av å være tilstede på plattformen, og at behandlingen vil ha flere positive konsekvenser for den registrerte. Arbeidsgruppen mener likevel at det er vanskelig å rettferdiggjøre Datatilsynets interesser av å bruke Facebook-side når disse interessene veies mot behandlingen av personopplysninger i Facebook.
- Arbeidsgruppen mener at Datatilsynets egne formål er klart spesifisert og samsvarer med forventingene til brukerne i kontekst av å abonnere på og/eller interagere med en side på Facebook.
- Arbeidsgruppen har identifisert tiltak for dataminimering med tanke på Datatilsynets formål isolert sett, men plattformen gir ikke mulighet for å implementere disse.
- Arbeidsgruppen mener at prinsippet om riktighet er mindre relevant i vår kontekst av å behandle personopplysninger gjennom bruk av en side på Facebook.
- Datatilsynet kan redigere og slette innhold etter eget forgodtbefinnende. Men det er uklart om opplysningene også slettes fra Facebooks underliggende systemer, eller om de blir værende her også etter at Datatilsynet har slettet dem og de ikke lenger er synlige for brukeren.

På tross av at Datatilsynet selv vil ha intensjon om å ivareta rettslig grunnlag, personvernprinsippene og de registretes rettigheter og friheter, er vi prisgitt Facebook og deres betingelser ved å ta i bruk en side på plattformen. Dette har følgende implikasjoner:

- Arbeidsgruppen mener at Facebooks formål kan fremstå vide, vage og altomfattende. Vi tror at det er vanskelig for brukerne å vite hva de kan forvente av behandlingen.
- Arbeidsgruppen er av den oppfating at vi ikke kan påvirke hva Facebook samler inn av metadata, observert data og utledet data når brukere interagerer med siden vår.
- Det vil være vanskelig for brukere å ettergå om personopplysninger korrekte.
- Arbeidsgruppen mener det er usikkerhet knyttet til faktisk lagringstid i Facebook.
- Arbeidsgruppen mener at det er flere usikkerheter knyttet til måten de registrertes rettigheter og friheter ivaretas av Facebook. Datatilsynet vil ikke kunne påvirke Facebooks behandling av personopplysninger og dermed ikke de prosessene som måtte true den registrertes rettigheter og friheter.

Vurdering av risiko for de registrertes rettigheter og friheter

Hittil i rapporten har vi vurdert tilstedeværelse gjennom en side på Facebook med utgangspunkt i at Datatilsynet er en behandlingsansvarlig med en rekke plikter etter personvernforordningen. I dette kapittelet snur vi perspektivet og ser behandlingen fra den registrerte sin synsvinkel.

Må vi utføre en DPIA?

Personvernforordningen artikkel 35 slår fast at en vurdering av personvernkonsekvenser (DPIA) skal gjennomføres når det er sannsynlig at en viss type behandling av personopplysninger medfører høy risiko for at de registrertes rettigheter og friheter etter forordningen ikke ivaretas.

Basert på risikoene vi identifiserte i den systematiske beskrivelsen med hensyn til art, omfang, formål og sammenheng, og konklusjonen vi kom frem til i vår vurdering av nødvendighet og proporsjonalitet, har vi kommet frem til at det å ta i bruk Facebook som kommunikasjonsplattform, sannsynligvis medfører en høy risiko for de registrertes rettigheter og friheter.

Vi mener dessuten behandlingen kan sees opp mot flere av kriteriene i Artikkel 29-gruppens kriterier for å vurdere behov for DPIA[56] og Datatilsynets liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA[57].

Vurdering av manglende reell medbestemmelse, åpenhet og forutsigbarhet

I vår DPIA tar vi utgangspunkt i kriteriene overfor og vurderer *reell medbestemmelse, reell åpenhet, reell forutsigbarhet* ved behandlingen for å kontrollere om behandlingen kan gjennomføres på en måte som er akseptabel og tillitsskapende overfor den registrerte.

Reell medbestemmelse
Vi knytter først og fremst grad av medbestemmelse til den registrertes rettigheter etter personvernforordningen.

Det er opp til den enkelte å benytte Facebook som informasjons- og kommunikasjonsplattform. Den registrerte velger selv å opprette profil og forelegges tjenestens avtalevilkår ved opprettelse av profil på plattformen.

Det er også valgfritt å abonnere på og interagere med Datatilsynets side. Det aller meste av informasjonen som Datatilsynet selv er avsender av, vil allerede være offentlig tilgjengelig og dermed ikke tilbys eksklusivt på Facebook. Debatten som kommer frem i kommunikasjon med brukere vil imidlertid være kanalspesifikk.

Datatilsynet med personvernombud (PVO) kan hjelpe den registrerte med informasjon og veiledning i utøvelse av rettigheter i Facebook-systemet så langt vi kan. Datatilsynet kan imidlertid i liten grad aktivt hjelpe den registrerte med å utøve øvrige rettigheter.

Arbeidsgruppen har utarbeidet en guide som den registrerte kan bruke for å gå frem for å utøve sine rettigheter overfor Facebook.

---

[56] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/?id=10362

[57] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/

I Facebook har den registrerte rett og mulighet til, utover å bli informert, å få tilgang til (innsyn), korrigere (retting), overføre (dataportabilitet) og slette egne data. Etter loven har også den registrerte rett til å motsette seg (protestere) og begrense bestemte behandlinger av personopplysninger. Dette inkluderer blant annet retten til å motsette seg behandling av sine data for direkte markedsføring, retten til å motsette seg behandling av egne data hvor Facebook mener at de utfører en oppgave i offentlighetens interesse eller der Facebook forfølger egne eller en tredjeparts legitime interesser. En bruker kan trekke tilbake samtykket sitt i forbindelse med bestemte typer behandling på Facebook, eksempelvis behandling av spesialkategorier av personopplysninger, bruk av lokasjonsdata eller bruk av ansiktsgjenkjenning. En bruker kan velge å slette sin konto på Facebook når som helst.

Den registrerte kan kontakte Facebook via et kontaktskjema, via post eller gjennom dedikert datatilsynsansvarlig hos Facebook Ireland Ltd. Den registrerte har også rett til å fremme en klage til Facebook Irelands ledende tilsynsmyndighet, Irish Data Protection Commission, eller via den norske tilsynsmyndigheten.

Det er allerede påpekt at det etter arbeidsgruppems vurderinger er flere usikkerheter rundt den reelle utøvelsen av rettighetene, f.eks. knyttet til fullstendigheten i innsynet av egne data eller om permanent sletting av personopplysninger. Av plattformens natur følger det at en registrert i liten grad vil kunne benytte rettigheter opp imot en spesifikk side på plattformen.

Den registrerte vil videre ha en viss valgfrihet gjennom plattformens funksjoner, eksempelvis redigere og slette noe de selv aktivt har delt på en Facebook-side. Arbeidsgruppen er likevel av den oppfatning av at den registrerte kan ha lite valgfrihet, mulighet til reservasjon og lite reell medbestemmelse over en rekke behandlinger, inkludert behandlinger knyttet til en spesifikk Facebok-side, slik som:

- Hvilke personopplysninger som samles inn, samt bruk av ulike kilder.
- Volumet av personopplysninger
- Hva som er grunnlag for vurdering eller bedømmelse av den registrerte
- Lagringstid
- Geografisk omfang av lagring
- Beslutninger om den registrerte basert på systematisk og omfattende analyse av personopplysninger
- Bruk av personopplysningene til nye eller andre formål.
- Lite kontroll over dataflyt, kjeden av behandlinger og utlevering til tredjeparter.

Vi mener at muligheten til å utøve sine rettigheter etter personvernforordningen styrker den registrertes valg og medbestemmelse. Datatilsynet er imidlertid prisgitt hvordan Facebook lar brukeren ha innflytelse og kontroll over behandlingen av sine personopplysninger og i hvor stor grad de kan utøve sine rettigheter og friheter.

Reell åpenhet
Facebook beskriver behandlingen av personopplysninger i sin personvernerklæring og en lang rekke andre offentlige dokumenter som man finner på plattformen. Vi stiller likevel spørsmål om hvorvidt Facebook er tilstrekkelig åpen om:

- Ivaretakelse av personvernprinsippene
- Kompleksiteten i behandlingene
- Den regelmessige og systematiske behandlingen
- Til hvem opplysningene blir utlevert, og generell dataflyt, programvare og algoritmer som benyttes, samt grunnlag for beslutninger
- Kjeden av behandlingsaktiviteter
- Hvor mye informasjon Facebook faktisk sitter på og hvordan denne informasjon kan benyttes for å påvirke brukeren
- Grunnlag for vurdering eller bedømmelse av den registrerte
- Behandlingens størrelse og rekkevidde
- Matching eller kobling av datasett fra ulike kilder

Vi stiller også spørsmål ved om Facebook er tilstrekkelig åpen om ordningen om felles behandlingsansvar med eiere av side. Det bidrar til å svekke muligheten til å tydeliggjøre ansvar overfor eiere av side og den enkelte bruker.

Trusselen ved eventuell manglende reell åpenhet er at Facebook potensielt kan skjule illegitim behandling bak uklar, uforståelig og mangelfull informasjon. Det kan medføre at den registrerte ikke får godt nok informasjonsgrunnlag til å ta gode valg i sin tilstedeværelse på plattformen, eller de kan være uvitende om hvorfor gitte beslutninger blir tatt om dem. Lite tilgjengelig informasjon kan potensielt medføre at den registrerte heller ikke får utøvd sine rettigheter etter personvernforordningen. I en situasjon der den ene parten vet mye mer om den andre vil det også være snakk om et skjevt maktforhold.

Vi mener at Datatilsynets tilstedeværelse på Facebook, gjennom en side, isolert sett ikke vil forverre eller på annen måte prege graden av åpenhet overfor den registrerte i plattformen. Som behandlingsansvarlig er vi imidlertid også her prisgitt i hvor stor grad Facebook velger å være åpen rundt sine behandlingsaktiviteter og hva de velger å gi den registrerte informasjon om og innsyn i.

Reell forutsigbarhet
Facebook vil behandle de personopplysningene som genereres på Datatilsynets side på Facebook til egne formål, som trolig vil være uforutsigbart for den registrerte. Vi mener at Facebooks behandling av personopplysninger kan være uforutsigbar på flere punkter, blant annet:

- Profilering, automatiserte avgjørelser og beslutninger basert på systematisk og omfattende analyse
- Grunnlag for vurdering eller bedømmelse av den registrerte
- Den registrertes forventning om konfidensialitet og privatliv i visse typer kommunikasjon på plattformen.
- Lagringstid og hvorvidt sletting av personopplysninger er permanent
- Volumet av personopplysninger knyttet til enkeltindivider og hva dette kan innebære
- Eventuell bruk av særlige kategorier personopplysninger
- Matching eller kobling av datasett fra ulike kilder
- Facebook benytter seg av stadig ny og innovativ teknologi som medfører nye typer behandlinger
- Facebook kan når som helst velge å endre sine vilkår. Ved betydelige endringer vil imidlertid den registrerte og/eller eiere av sider varsles.

Kompleksiteten i behandlingene i Facebook vil etter vår vurdering være så omfattende at den registrerte i mange tilfeller ikke vet hva de kan forvente. Behandlingene kan slå ut på uforutsigbare måter og lede til uforutsigbare beslutninger i brukeropplevelsen.

Arbeidsgruppen er av den oppfatning av at Datatilsynets side på Facebook, isolert sett, i liten grad vil stride mot den registrertes rimelige forventninger. Arbeidsgruppen tror at Datatilsynets behandling etter egne definerte formål vil kunne oppleves som begrenset i omfang, ryddig, forutsigbar og profesjonell. De fleste brukere av Facebook vil være kjent med å kommunisere med sider, og slik sett vil disse behandlingene kunne oppleves som forutsigbar for den registrerte. Vi er likevel prisgitt hvordan Facebook velger å behandle personopplysninger etter sine formål og i hvilken grad de velger å være åpne om behandlingene for at de registrerte skal oppleve dem som forutsigbare.

Hva kan vi gjøre for å opparbeide tillit?
For å oppnå en større grad av tillit hos de registrerte, lister arbeidsgruppen opp følgende forslag til tiltak:

- Vurdere tilgjengeliggjøring av risikovurdering av Facebook ved forespørsel eller vurdere å proaktivt kommunisere dette arbeidet jf. bruk av ombudsrollen.
- Vise til undersøkelser, rapporter, forskning etc. om Facebook og sosiale medier
- Følge med på eventuelle endringer i Facebooks policy/vilkår og vurdere risiko fortløpende
- Medieovervåking av personvernrelatert omtale av Facebook i mediene
- Følge med på andre europeiske datatilsynsmyndigheter og hvordan de posisjonerer seg i henhold til bruk av Facebook og andre sosiale medier.
- Innhente de registrertes/representanter for de registrerte sitt syn på behandlingen

PS! Selv om dette allerede er forpliktelser etter personvernforordningen, kan også konsultering med PVO og validering av DPIA i ledelsen betraktes som tillitsskapende tiltak.

Notat fra PVO

Vårt personvernombud gav sine vurderinger og betraktninger basert på en tidligere versjon av rapporten som ble lagt frem for ledelsen. Ombudets betraktninger er adressert i denne versjonen.

Oppsummering og vurdering: vurdering av risiko for den registrertes rettigheter og friheter

Vi mener at vi måtte utføre en DPIA basert på følgende:

- Behandlingen treffer flere av Artikkel 29-gruppens kriterier.
- Behandlingen treffer flere av kriteriene på Datatilsynets egen DPIA-liste.

Det medfører at vi skal vurdere reell medbestemmelse, reell åpenhet og reell forutsigbarhet ved behandlingen. Her kom vi frem til følgende:

- Den registrerte vil ha *lite valg og lite reell medbestemmelse* over en rekke behandlinger, f.eks.

hvilke personopplysninger som samles inn, hvordan de brukes, lagringstid eller det geografiske omfanget på lagringen. Det kan innebære flere trusler for den registrertes rettigheter og friheter. Mangelen på reell medbestemmelse inkluderer også behandlinger knyttet til en spesifikk Facebok-side.

- Vi stiller spørsmål ved om Facebook *er tilstrekkelig åpen* om f.eks. algoritmene og kompleksiteten i behandlingene, utlevering av personopplysninger, eller matching av datasett. Det kan innebære flere trusler og ha flere implikasjoner for den registrertes rettigheter og friheter, eksempelvis at de ikke utøver sine rettigheter etter personvernforordningen. Vi stiller også spørsmål ved om Facebook i tilstrekkelig grad tydeliggjør ansvarsordningen overfor brukere eller eiere av side.
- Vi mener *at Facebooks behandlinger kan være uforutsigbare* på flere punkter, f.eks. profilering og automatiserte avgjørelser, forventning om konfidensialitet, matching av datasett eller bruk av ny og innovativ teknologi. Facebook kan når som helst velge å endre sine vilkår. Behandlingene kan slå ut på uforutsigbare måter for den registrerte. Vi tror interaksjon med sider på Facebook, isolert sett, vil fremstå forutsigbart.
- Vi kan sette inn noen øvrige tillitsskapende tiltak, utover de som er skissert i vurderingen av nødvendighet og proporsjonalitet.

Vi er generelt prisgitt hvordan Facebook velger å behandle personopplysninger etter sine formål. Vi er også prisgitt i hvilken grad Facebook velger å gi brukere av plattformen reelle valg, og hvor forutsigbare og åpne om behandlingene de ønsker å være overfor de registrerte.

Vi mener at det fremdeles er en høy risiko for de registrertes rettigheter og friheter etter foreslåtte tiltak.

Validering hos ledelsen

Vi mener at vi med denne rapporten har gitt ledelsen tilstrekkelig informasjon til å danne et beslutningsgrunnlag. Spesielt med hensyn til DPIA og hensynet til relevante interessenter bes ledelsen om å beslutte enten:

1. Om vi skal ta i bruk side på Facebook som kommunikasjonsplattform. Det innebærer at ledelsen ikke anser at behandlingen av personopplysninger medfører høy risiko for de registrertes rettigheter og friheter.
2. Betinget forbedringer i vurderingen. Ledelsen gir forklaring på hvilken måte, og arbeidsgruppen kommer tilbake med en revidert DPIA som legges frem for ledelsen.
3. Avvist: Ledelsen beslutter å ikke gjennomføre behandling av personopplysninger på side på Facebook.
4. Dersom ledelsen ønsker å gå videre og rapporten er behandlet i ledelsen mer enn én gang, men risiko fremdeles er høy for den registrertes rettigheter og friheter (og vi ikke greier ta denne ned) ber ledelsen (Datatilsynet) om en forhåndsdrøftelse med et settedatatilsyn

Konklusjon og anbefaling fra arbeidsgruppen

I en vurdering av en offentlig aktør som Datatilsynet sin tilstedeværelse og rolle på et sosialt medium, kan ikke et demokratisk perspektiv undervurderes. Det er ingen tvil om Facebook sitt potensial som informasjons- og kommunikasjonskanal for viktige målgrupper og det brede lag av befolkningen.

Men fordelene ved sosiale medier må vurderes opp imot ulempene. Tross i de kommunikative formålene med tilstedeværelse på en plattform der mange potensielle brukere og publikum er, anbefaler vi at Datatilsynet ikke tar i bruk Facebook.

Etter å ha foretatt en strukturert vurdering, er vår konklusjon ganske klar. For det første mener vi at behandlingen av personopplysninger medfører høy risiko for de registrertes rettigheter og friheter (pkt 1). Vi kan vanskelig se at en revidert DPIA vil endre på dette (pkt 2). Vi anbefaler ledelsen å ikke gjennomføre behandling av personopplysninger på side på Facebook (pkt. 3). En forhåndsdrøftelse med et settedatatilsyn bør være irrelevant dersom anbefalingene i punktene ovenfor følges (pkt. 4).

I tillegg mener vi at tilstedeværelse på Facebook og selskapets etterfølgende behandling av personopplysninger vil ha stor betydning for Datatilsynets omdømme og etiske standard. Vi mener at Datatilsynets beslutning om å ta i bruk Facebook eller ikke vil bli lagt merke til og få betydning for andre aktørers bruk av plattformen. Dermed vil kretsen av registrerte som påvirkes av Datatilsynets beslutning være flere enn bare de som ville benyttet seg av Datatilsynet sin side. Vi mener at Datatilsynet i sin natur bør tillegge hensynet til sin posisjon som rollemodell i personvernsaker stor vekt. Hvis Datatilsynet entrer Facebook, kan det være med på å legitimere at virksomheter tar i bruk en plattform som kan utgjøre en høy risiko for de registrertes rettigheter og friheter.

Det er likevel arbeidsgruppens anbefaling å vurdere andre sosiale medieplattformer for å hegne om en profesjonell og aktiv kommunikasjonsvirksomhet, få best mulig effekt av virkemidlene våre og møte publikum på en måte de er vant til og på en måte de liker.

Beslutning fra ledergruppen

I ledermøte 03.03.2020 besluttet ledelsen å stille seg bak anbefalingen fra arbeidsgruppen, med små endringer. Disse endringene er tatt med i denne versjonen av rapporten.

Vedlegg 1 – vurdering av felles behandlingsansvar

I denne vurderingen er det spesielt viktig å identifisere og klargjøre rollene og ansvaret til henholdsvis Datatilsynet og Facebook i behandlingen.

Hva er felles behandlingsansvar?
Personvernforordningen slår fast at to eller flere behandlingsansvarlige kan ha et felles behandlingsansvar.

Et felles behandlingsansvar oppstår når to eller flere separate behandlingsansvarlige i felleskap beslutter formål og de avgjørende midlene i behandlingen, eller når beslutningene deres om formål og avgjørende midler konvergerer. Det oppstår derimot ikke et felles behandlingsansvar når flere behandlingsansvarlige hver for seg tar beslutninger knyttet til formål og midler, selv om virksomhetene behandler de samme personopplysningene.

Hver enkelt behandlingsansvarlig må ha et behandlingsgrunnlag for å kunne behandle personopplysningene. De behandlingsansvarlige må sørge for en ordning som på en åpen måte fastsetter deres respektive ansvar for å overholde reglene i forordningen, samt de behandlingsansvarliges rolle og forhold til de registrerte. Personvernrådet (EDPB) har gitt ut retningslinjer om behandlingsansvarlige og databehandlere[58]. Der presiseres det at begge de behandlingsansvarlige har et overordnet ansvar for behandlingen i helhet, selv om de har fordelt ansvar seg imellom i en ordning.

EU-domstolen har uttalt at felles behandlingsansvar mellom to aktører ikke fører til at den ene aktøren også blir ansvarlig for forutgående eller etterfølgende behandling som den andre aktøren er ansvarlig for alene.[59] I praksis kan det være vanskelig å trekke grensene mellom behandlingsaktiviteter og avgjøre hvor det felles behandlingsansvaret «begynner» og «slutter».

EU-domstolens avgjørelse i C-210/16 Wirtschaftsakademie
EU-domstolen kom i sin avgjørelse kalt Wirtschaftsakademie[60] til at en administrator av en side

§ Artikkel 26: Felles behandlingsansvarlig

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.

[58] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[59] C-40/17 *Fashion ID* para. 74.

[60] C-210/16 *Wirtschaftsakademie*.

(«fan page») på Facebook kan anses som en behandlingsansvarlig etter det daværende personverndirektivet[61], for innsamling

av personopplysninger om personer som besøker siden. Avgjørelsen er relevant også etter dagens personvernforordning. Det er verdt å merke seg at Facebook og Wirtschaftsakademie hadde delvis ulike formål med innsamlingen. Domstolen sier at Facebook og administratoren ikke nødvendigvis har likt ansvar, selv om de har et felles ansvar, og at ansvaret avhenger av i hvilken grad de to aktørene er involvert i behandlingen.[62]

EU-domstolens avgjørelse C-40/17 Fashion ID

EU-domstolen har i sin avgjørelse kalt Fashion ID[63] uttalt seg om felles behandlingsansvar. Avgjørelsen gjaldt fortolkningen av reglene i det daværende personverndirektivet, men vil i likhet med Wirtschaftsakademie-dommen være relevant i fortolkningen av dagens personvernforordning.

Fashion ID handler om en nettbutikk som hadde gjort Facebooks «like»-knapp til en del av sin nettside. Gjennom «like»-knappen ble informasjon om besøkende på nettsiden samlet inn og delt med Facebook, også uten at de besøkende trykket på eller på annen måte interagerte med «like»-knappen.

EU-domstolen uttalte i Fashion ID-avgjørelsen at nettbutikken og Facebook hadde felles behandlingsansvar for den behandlingsaktiviteten som besto i innsamling og utlevering til Facebook av opplysninger om besøkende på nettsiden («*collection and disclosure by transmission*»).[64] Begrunnelsen for dette er det er at det er denne behandlingsaktiviteten som nettbutikken og Facebook i fellesskap beslutter formål og midler for. Facebook og Fashion ID hadde ulike formål med behandlingsaktiviteten, men den fant sted i deres felles økonomiske interesse.

Domstolen fremhever videre at Facebook ikke ville fått tilgang til personopplysninger om de besøkende på nettsiden uten at nettbutikken hadde gjort «like»-knappen til en del av nettsiden. Nettbutikken utøver derved avgjørende innflytelse over innsamlingen av personopplysninger («*exerts a decisive influence*»).[65]

Domstolen uttaler også at de to aktørene har felles behandlingsansvar, også selv om nettbutikken ikke har tilgang til personopplysningene som samles inn.[66]

Beskrivelse av behandlingsaktiviteten(e) som Datatilsynet og Facebook får felles behandlingsansvar for

Det er vanskelig å beskrive grensene for behandlingen som Facebook og Datatilsynet vil få felles behandlingsansvar for. Basert på kartleggingen som er gjort, behandler Facebook personopplysninger for en rekke formål som går lenger enn de formål som Datatilsynet vil behandle personopplysninger for. Etter vår oppfatning kan flere av formålene til Facebook fremstå som vagt definert og uklare. Spørsmålet er om Datatilsynet vil kunne anses som felles behandlingsansvarlig med Facebook også for behandling som Facebook i hovedsak er involvert i, og som gjøres for å oppnå formål definert av Facebook.

Det fremgår av Fashion ID-avgjørelsen at det foreligger felles behandlingsansvar for innsamling fra nettsiden til Fashion ID og utlevering av personopplysninger fra Fashion ID til Facebook, selv om aktørene har ulike formål med behandlingen. Samtidig fremgår det også at nettbutikken ikke har felles behandlingsansvar med Facebook for den etterfølgende behandlingen som Facebook eventuelt måtte foreta, selv om aktørene har felles behandlingsansvar for selve innsamlingen av personopplysninger.

Med andre ord: Datatilsynet kan være felles behandlingsansvarlig for behandlingsaktiviteter vi bidrar til og muliggjør, selv om Facebooks formål med aktiviteten er forskjellige fra våre. Det betyr ikke at vi har likt ansvar; det kan foreligge ulike nivåer av ansvar. Vi er imidlertid ikke ansvarlige for Facebooks etterfølgende behandlingsaktiviteter som vi ikke bidrar til.

Basert på dette vil det være en ytre grense for hvilken behandlingsaktivitet som Datatilsynet og Facebook har felles behandlingsansvar for. Dersom man følger resonnementet i Fashion ID, får Datatilsynet med andre

---

[61] Det vil si gjeldende personvernregelverk før mai 2018, Europaparlamentet og Rådets direktiv 95/46/EF av 24. oktober 1995

[62] C-210/16 *Wirtschaftsakademie* para. 43.

[63] C-40/17 *Fashion ID.*

[64] *Ibid.* para. 76.

[65] *Ibid.* para. 78.

[66] *Ibid.* para 82.

ord ikke et felles behandlingsansvar med Facebook som dekker all Facebooks etterfølgende behandling. Vil det i teorien kunne være mulig å oppstille en grense for hvor Datatilsynet og Facebook ikke lenger i fellesskap bestemmer formål og middel for behandlingen av personopplysninger? Vi mener at det er vanskelig å fastsette hvor en slik grense går.
Av hensyn til prinsippene om ansvarlighet, gjennomsiktighet og forutsigbarhet, kan det argumenteres for at Datatilsynet fra et etisk perspektiv kan være ansvarlig for Facebooks etterfølgende behandling. Dette fordi Datatilsynet ved sin side bidrar til innsamling av personopplysninger som deretter benyttes av Facebook til noen behandlinger som vi mener kan utgjøre en risiko for den registrertes rettigheter og friheter.

Hensynet til at de registrerte har kontroll over sine personopplysninger peker også i denne retningen. Dette er personopplysninger som Facebook ikke ville hatt tilgang til uten Datatilsynets handlinger, jf. også resonnementet i Fashion ID para. 78. Uavhengig av spørsmålet om (felles) behandlingsansvar, er vår vurdering at denne etterfølgende behandlingen av Facebook er av betydning for hvilken informasjonsplikt Datatilsynet har etter artikkel 5, 12, 13 og 14.

Selv om grensene er uklare, mener vi i alle fall at følgende behandlingsaktiviteter *kan* inngå i et felles behandlingsansvar med Facebook:

- Datatilsynet og Facebook vil være felles behandlingsansvarlig for innsamling av personopplysninger om personer som besøker og interagerer med Datatilsynets Facebook-side.
- Datatilsynet og Facebook vil være felles behandlingsansvarlig for resultatet av analysen av personopplysninger om personer som besøker og interagerer med Datatilsynets Facebook-side («Page Insights»).
- Vi er usikre på om Datatilsynet vil ha et visst felles behandlingsansvar for at Facebook bruker personopplysninger om brukere som besøker Datatilsynets Facebook-side til å berike personprofiler med formål å levere persontilpasset markedsføring.

I tillegg mener vi at:

- Datatilsynet og Facebook har et felles ansvar for å informere på en åpen, tilgjengelig og forståelig måte om hva brukernes personopplysninger vil brukes til.
- Facebok og Datatilsynet er felles ansvarlige for at de registrertes rettigheter og friheter ivaretas.

Facebooks avtale om felles behandlingsansvar er problematisk

Facebook har laget en avtale om felles behandlingsansvar («*joint controllership arrangement*»), kalt *Page Insights Addendum*[67], som en del av Facebooks vilkår.

Datatilsynet vil ikke kunne forhandle en egen avtale eller ordning med Facebook om felles behandlingsansvar. Datatilsynet må følgelig vurdere om vilkårene som presenteres av Facebook er akseptable. Om avtalen er akseptabel avhenger både av om Datatilsynet anser (1) at avtalen dekker all behandlingen som partene har felles behandlingsansvar for, (2) at Datatilsynet gjennom inngåelse av avtalen vil oppfyller kravene i personvernforordningen art. 26, og (3) at de konkrete vilkårene i avtalen er akseptable for Datatilsynet.

Ifølge avtalen gjelder den det felles behandlingsansvaret som aktørene har for aggregert statistikk som er laget fra hendelser som registreres i Facebooks servere når folk interagerer med en side og innholdet som er knyttet til siden. Avtalen fastslår at det kun er Facebook som har tilgang til de underliggende personopplysningene og hendelsene som er grunnlaget for innsikten. En side-administrator som Datatilsynet vil bare få tilgang til resultatet av analysen som Facebook leverer («*Page Insights*»).

Avtalen sier at hendelser som danner grunnlaget for innsikt også kan knytte seg til personer som ikke er logget inn som Facebook-brukere. Dette skjer dersom personene besøker en side eller klikker på et bilde eller en video i et innlegg for å se på det.

Avtalen *Page Insights Addendum* er den eneste avtalen Facebook har laget om felles behandlingsansvar. Etter vår vurdering er det usikkert om avtalen dekker behandlingsaktivitetene som vi anser Facebook og Datatilsynet for å ha felles behandlingsansvar for. Forholdet kompliseres ytterligere ved at det også er

[67] https://www.facebook.com/legal/terms/page_controller_addendum

vanskelig å fastsette grensene for det felles behandlingsansvaret.

Når det gjelder de konkrete vilkårene i avtalen, vil vi trekke frem noen hovedpunkter: Avtalen er dynamisk, Facebook vil kunne endre avtalen som de ønsker, og det er usikkert om Facebook vil varsle om endringer i avtalen. Datatilsynets eneste handlingsmulighet dersom man anser at eventuelle endringer ikke er akseptable, vil være å avslutte bruken av siden. Slik vi forstår det, gir ikke avtalen oss rett til å kreve at allerede innsamlede personopplysninger slettes. Ved å inngå avtalen godtar Datatilsynet at eventuelle tvister mellom Datatilsynet og Facebook avgjøres av irske domstoler etter irsk rett – Datatilsynets rettsstilling ved en eventuell tvist er derfor uklar for oss.

Gjennomgang av artikkel 26 nr. 1, 2 og 3

Formål og interesser
Datatilsynets formål avviker i stor grad fra Facebook sine formål. Facebooks sitt hovedformål er "Give people the power to build community and bring the world closer together" og en rekke formal listet i Facebooks Retningslinjer for data[68]. Datatilsynets formål er folkeopplysning og debatt om personvern. Facebook sitt formål er såpass bredt at det nødvendigvis vil omfatte Datatilsynet sine formål. Vår felles interesse er å nå ut bredt med budskap og engasjere Facebook-brukere, samt måling og analyse av trafikk/innhold på siden.

Midler
For at Datatilsynet skal oppnå gitte formål, ønsker Datatilsynet å bruke en side på Facebook som middel, dvs. som kommunikasjonsplattform.
Behandlingsansvarlig plikter etter artikkel 25 å benytte løsninger som har innebygget personvern og personvern som standardinnstilling. Vi stiller spørsmål ved om personopplysningene som samles inn ved side på Facebook vil behandles i henhold til dette kravet, ref. i kapittelet om Nødvendighet og proporsjonalitet. Dermed er det usikkert om vi vil opptre i tråd med denne plikten, basert på ansvaret vi kan ha i denne relasjonen.

Ansvar, forpliktelser, informasjon og kontaktpunkt (jf. art 26 nr. 1)
Artikkel 26 sier at ansvarsforhold skal fastsettes/avklares. Vår vurdering er at det er uklart hvor grensene går for de behandlingsaktivitetene Datatilsynet og Facebook har felles behandlingsansvar for og hvilke aktiviteter Datatilsynet og Facebook har ansvar for hver for seg.

Videre er det også uklart hvilke behandlinger Facebook gjør basert på personopplysninger som genereres fra Datatilsynet sin side. Gjennom Facebook-siden bidrar Datatilsynet til innsamling av personopplysninger. Disse personopplysningene brukes videre i andre behandlingsaktiviteter hos Facebook. Ettersom Facebooks etterfølgende behandlingsaktiviteter er ukjente og uklare for oss, er det vanskelig for Datatilsynet å opptre i samsvar med sitt ansvar. Igjen: Det er vanskelig å fastslå hvor Datatilsynets ansvar «begynner» og «slutter». Det er derfor vanskelig å oppfylle kravet om å fastsette sitt *respektive ansvar* i henhold til artikkel 26.

Det er uklart i hvor stor grad Datatilsynet er i stand til å overholde sine *forpliktelser* etter personvernforordningen, særlig om den registrertes reelle mulighet til å utøve sine rettigheter. Den registrerte vil i stor grad være avhengig av å henvende seg til Facebook for å få gjennomført en rettighet. Dersom Facebook ikke svarer eller ikke etterkommer den registrertes ønske, vil Datatilsynet ha begrenset mulighet til å hjelpe den registrerte. Plikten til å *fremlegge informasjon* etter artikkel 13 og 14 mener vi kan ivaretas av både Facebook og av Datatilsynet.

Kontaktpunkt for de registrerte er opprettet på Facebook og vil etableres hos Datatilsynet, i henhold til artikkel 26(1).

Vår vurdering at Datatilsynet bare delvis oppfyller artikkel 26(1) i personvernforordningen.

Ordning (jf. art 26 nr. 2)
Ordningen om felles behandlingsansvar er uklar og kan endres på Facebooks initiativ.

Ordningen som er etablert om felles behandlingsansvar er utarbeidet av Facebook og gjelder kun måling og analyse («Insights»). Vi er av den oppfatning av at det felles ansvaret er bredere enn denne ordningen. Dermed mangler vi ordninger for de øvrige behandlinger som utføres. Rollene og ansvaret for aktivitetene som ikke inngår i avtalen er derfor ikke definert.

---

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

Den ene ordningen for Insights er publisert på Facebook sine nettsider og er tilgjengelig for de registrerte. Vi mener at det vil være usannsynlig at vi får på plass en ordning for øvrige behandlingsaktiviteter. En mulig etablering vil kompliseres ytterligere ved at det er vanskelig å fastsette grenser for felles behandlingsansvar.

Vår vurdering er at Datatilsynet kun delvis oppfyller artikkel 26(2) i personvernforordningen.

Utøvelse av rettigheter hos den enkelte behandlingsansvarlige Ordning (jf. art 26 nr. 3)
Den registrerte kan i liten grad utøve sine rettigheter hos Datatilsynet. Utøvelse av øvrige rettigheter må skje hos Facebook.

Vår vurdering er at Datatilsynet derfor ikke kan oppfylle artikkel 26(3) i personvernforordningen.

Vedlegg 2 – vurdering av personopplysningssikkerhet

I denne beskrivelsen vurderer vi om behandlingens personopplysningssikkerhet/informasjonssikkerhet er tilstrekkelig ivaretatt i henhold til artikkel 32.

Informasjonssikkerhetsrisiko er sammenhengen mellom følgende tre faktorer.

1. **Verdivurdering**, dvs. klassifisering av informasjon/personopplysninger (verdi)
2. **Trusselvurdering** – trusler og trusselaktører som kan true våre verdier
3. **Sårbarhetsvurdering** – hvor sårbare er vi, og hvor er våre sårbarheter, gitt våre verdier og trusler mot våre verdier

Verdivurdering: Personvernregelverket definerer personopplysninger som en verdi. Ved å kommunisere gjennom en side på Facebook vil Datatilsynet generere en rekke personopplysninger. Vi har valgt å dele opp og definere verdiene (personopplysningene) som behandles i Facebook i to: Vi skiller mellom «*Offentlig informasjon*» etter formål 1 og «*Kommunikasjon med brukere*» etter formål 2.

Verdien *Offentlig informasjon* er den informasjonen Datatilsynet selv velger å publisere på Facebook-siden. Det omfatter blant annet informasjon fra våre nettsider, nyheter, veiledninger, blogginnlegg, deling av andre siders/firmaers innhold (kuratert innhold), videoer, livesendinger, bilder, grafikk og lenker. Basert på disse opplysningene har vi vurdert våre krav til konfidensialitet, integritet og tilgjengelighet, som følgende:

Sum konfidensialitet	Lav
Sum integritet	Høy
Sum Tilgjengelighet	Lav

Vår vurdering er at det ikke er noe fare i at informasjonen vi legger ut spres (informasjonens konfidensialitet), fordi det nettopp er hensikten ved å benytte en Facebook-side. Tilgjengelighetsegenskapen er også vurdert til lav, som betyr at hvis informasjon som vi publiserer på Facebook-siden forsvinner eller blir borte, har det mindre betydning for Datatilsynet. Vår hovedkanal vil være www.datatilsynet.no, og vi forvalter flere andre kanaler (personvernblogg, nyhetsbrev, Twitter). Den viktigste sikkerhetsegenskapen til *offentlig informasjon* er etter vår vurdering integritet. Vi har stor interesse av at det vi publiserer skal være korrekt og ikke endres på av uvedkommende.

Verdien Kommunikasjon med brukere er all informasjon som utgjør dialogen mellom brukere og Datatilsynet på vår side på Facebook, og inkluderer kommentarer, direktemeldinger, brukers delinger og engasjement. Det vil følge av Facebook-plattformen sin natur, som et profilbasert medium, og direkte i ytringer og engasjement, at det genereres en rekke personopplysninger gjennom brukeres interaksjon med Datatilsynets side på Facebook. Vi har vurdert våre krav til konfidensialitet, integritet og tilgjengelighet som følgende:

Sum konfidensialitet	Svært høy
Sum integritet	Høy
Sum Tilgjengelighet	Lav

Basert på den kunnskapen vi har fra veiledning og øvrig dialog med publikum, tror vi at det også kan komme frem særlige kategorier personopplysninger på Datatilsynet side på Facebook, eksempelvis fra sårbare brukere eller brukere som ikke forstår i hvilket omfang de deler informasjon om seg selv eller andre. For verdivurderingen av kommunikasjon med brukere er derfor personopplysningenes konfidensialitet satt til svært høy. Det vil også si at vi må klare å slette uønsket informasjon, slik som upassende, diskriminerende eller sjikanerende kommentarer og særlige kategorier personopplysninger lagt ut av brukere, om seg selv eller andre. Videre er vår vurdering at kravet til integritet bør være høy. Det indikerer at vi antar at brukere synes det er viktig at ingen endrer eller manipulerer deres ytringer, kommentarer eller øvrig engasjement i kommunikasjonen med vår side. Når det gjelder opplysningenes tilgjengelighet er vår vurdering at det ikke er vesentlig dersom dialogen med brukerne skulle forsvinne. Det kan muligens oppleves som irriterende for enkelte brukere, men vi vurderer den likevel til lav.

Trusselvurdering: I trusselvurderingen ser vi på hvilke trusler og trusselaktører som potensielt, bevisst eller ubevisst, kan skade våre verdier, det vil si personopplysningene identifisert i verdivurderingen over, og som Datatilsynet vil forvalte gjennom en side på Facebook. I det følgende beskriver vi noen sentrale

trusselaktører, samt deres antatte intensjon og angrepsvektor:

Trussel-aktør	Intensjon	Angrepsvektor/ trussel
Vanlige brukere/ barn/ inkompetente brukere	Ingen ondsinnede intensjoner, men kan interagere med siden uten å forstå konsekvens.	Via kommentarfelt, DM mm. som tilgjengeliggjør egne og andres (særskilte kategorier) personopplysninger
Mentalt ustabile personer	Hevn, frustrasjon, desperasjon, markering	Via kommentarfelt, DM mm. som tilgjengeliggjør egne og andres (særskilte kategorier) personopplysninger
Aktivister/ nettaktivister	Intensjon om å undergrave DTs myndighet, omdømme eller enkeltpersoner i DT eller øvrig publikum	Kompromittering: tilgang til brukerkontoer med Datatilsynet sine administrative rettigheter Endring av informasjon eller publisering på DTs konto
Nettroll	Intensjon om provosere, distrahere, skape splid og undergrave	Publisering av mye kritisk og spam/irrelevant innhold på DTs side.
Interne/ ansatte i DT	Kan publisere personopplysninger uten at det er avklart med den registrerte. Ingen ondsinnede intensjoner, men kan handle uten å forstå konsekvens.	Via publisering Har administrative tilganger for å utføre operasjoner eller innstillinger på siden.

Sårbarhetsvurdering: En sårbarhetsvurdering er nødvendig for å identifisere hva slags risikoreduserende tiltak som er nødvendig. Gitt våre verdier og de identifiserte truslene/trusselaktørene: hvor sårbare er Datatilsynet, og hvor er våre sårbarheter, overfor disse angrepsvektorene?

Når man ser etter sårbarheter, tar man utgangspunkt i kontroller i ulike sikkerhetsstandarder. Disse kontrollene bidrar til å avdekke om vi er sårbare overfor gitte trusler og setter en minimumsstandard for sårbarhetsreduserende tiltak.

Sårbarhetene i tabellen under vil stort sett reflektere over de sårbarhetene som Datatilsynet vil ha mulighet til å gjøre noe med.

Datatilsynet opererer med følgende fire risikonivåer: LAV, MODERAT, HØY og SVÆRT HØY.

Nr.	Sårbarhet	Risiko-nivå
1	Vi er prisgitt databehandlingsbetingelsene til Facebook og som behandlingsansvarlig kan vi ikke stille krav til informasjonssikkerhet til vår databehandler og/eller felles behandlingsansvarlig.	HØY
2	Datatilsynet publiserer personopplysninger uten god nok avklaring eller lovgrunnlag	LAV
3	Fritekst i innlegg og kommentarer	HØY
4	Brukere kan spre personinformasjon andre steder enn på siden, på eller utenfor plattformen	HØY
5	Mangel på kontroll på sidens informasjons- og kommunikasjonsflyt og informasjonens levetid	MODERAT
6	Manglende rutiner og policy i Datatilsynet for moderering av siden	LAV
7	Uklar ansvarsfordeling internt i Datatilsynet for siden på Facebook	LAV
8	Mangel/svak tilgangskontroll og autentisering	MODERAT

9	Tilgangsstyring og sletting internt i Facebook	HØY
10	Mangel på kontroll på IKT-enheter som moderatorer/ administratorer benytter	LAV

Risiko for personopplysningssikkerheten, sårbarhetsreduserende tiltak og restrisiko

Sårbarhetene nummerert i første kolonne korresponderer med sårbarhetene i tabellen i forrige avsnitt. Videre viser tabellen risiko før og etter implementering av sårbarhetsreduserende tiltak.

Nr.	Risiko-nivå	Sårbarhets-reduserende tiltak	Rest-risiko
1	HØY	Ingen tiltak	HØY
2	LAV	Datatilsynet må fastsette rutiner og roller for publisering.	LAV
3	HØY	Kun etterfølgende kontroll: Moderere, dvs. slette/skjule innlegg. Aktivere "profanity filter".	HØY
4	HØY	Slette innlegg ASAP fra siden (moderering og etterkontroll). Brukerne vil likevel ha et vindu til å spre innlegget videre.	HØY
5	MODERAT	Fastsette ansvar og rutiner for moderering	LAV
6	LAV	Definere og dokumentere bruk av Facebook gjennom org. tiltak: policy, opplæring mm. Vårt styringssystem inkluderer føringer for bruk av siden.	LAV
7	LAV	Vårt styringssystem inkluderer føringer for bruk av side på Facebook. Fastsette ansvar og rutiner for moderering. Definere og dokumentere bruk av plattformen. Fastsette og kontrollere roller, inkludert ressursbruk.	LAV
8	MODERAT	Dedikert bruker utelukkende for å moderere og administrere siden. Passordhygiene. Aktivere to-faktor-autentisering. Definere roller og brukertyper. Gjennomføre regelmessig revisjon av tilganger	
9	HØY	Vi har ingen adgang til å instruere Facebook angående tilgang til og sletting av «våre» personopplysninger	HØY
10	LAV	Mobile Device Management. Passordhygiene	LAV

Besøksadresse:
Trelastgata 3, 0191 Oslo

Postadresse:
Postboks 458 Sentrum
0105 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no
twitter.com/datatilsynet