

KRISTIANSAND KOMMUNE
Postboks 4
4685 NODELAND

Sendt per e-post til post@kristiansand.kommune.no

Deres referanse

Vår referanse
24/01055-10

Dato
10.06.2025

Vedtak om overtredelsesgebyr - Tilsyn med sporingsverktøy - Alarmtelefonen for barn og unge (116111.no)

1. Innledning

Vi viser til vårt varsel om vedtak 26. mars 2025 til Kristiansand kommune ved Alarmtelefonen for barn og unge («Alarmtelefonen»). Datatilsynet varslet om at det vurderte å legge et overtredelsesgebyr for å brudd på personvernforordningen i forbindelse med Alarmtelefonens nettsted 116111.no («Nettstedet»). Vi viser også til tidligere korrespondanse i forbindelse med tilsynet.

2. Vedtak om overtredelsesgebyr

Datatilsynet fatter følgende vedtak:

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i og artikkel 83, jf. personopplysningsloven § 26 andre avsnitt, pålegges Kristiansand kommune å

- *betale et overtredelsesgebyr på 250 000 NOK – to hundre og femti tusen norske kroner – til statskassen for behandling av personopplysninger om barn i strid med personvernforordningen artikkel 6 nr. 1, ved bruk av sporingsverktøyene Meta Pixel og Snap Pixel på nettstedet 116111.no, og for brudd på informasjonsplikten etter personvernforordningen artikkel 12 nr. 1 og 13.*

3. Sakens faktiske bakgrunn

3.1. Om Alarmtelefonen

Saken gjelder bruken av sporingsverktøy på nettsidene til tjenesten Alarmtelefonen for barn og unge som drives av Kristiansand kommune.

Alarmtelefonen er en gratis hjelpetjeneste for dem opp til 18 år som er utsatt for vold, overgrep eller annen omsorgssvikt. Tjenesten ble opprettet i 2009 for å innføre det felleseuropeiske hjelpetelefonnummeret 116 111. Tjenesten er døgnåpen og tilgjengelig for barn i hele landet. De kan henvende seg til Alarmtelefonen på telefon, chat, SMS og e-post, og henvendelsene kan videreformidles til riktig instans i den aktuelle kommunen for oppfølging. Nettstedet inneholder informasjon om hvordan man kan kontakte tjenesten, samt videoer og artikler med råd til barn og unge i vanskelige situasjoner.

Tjenesten drives av barnevernvakten i Kristiansand kommune, men den finansieres gjennom øremerkede tilskudd fra Barne-, ungdoms og familiedirektoratet (Bufdir). I brev 30. april 2025 opplyste kommunen at tjenesten begynte som en ren telefontjeneste. Nettstedet ble opprettet i forbindelse med et nytt oppdrag fra Bufdir i 2020 om at kommunen også skulle tilby en chat-tjeneste på internett. I tildelingsbrevet fra Bufdir 1. april 2020 sto det at Alarmtelefonen skulle nå ut til barn og unge med informasjon om tjenesten på sosiale medieplattformer.

Tilsynet er rettet mot Kristiansand kommune. Det er kommunen som driver tjenesten og som er operatøren av Nettstedet. Kommunen har derfor ansvaret for behandlingen av personopplysninger på Nettstedet. Vi har ikke gjennomført tilsyn av kommunens øvrige nettsider.

3.2. Om tilsynet: saksgang og omfang

3.2.1. Tilsynets bakgrunn

Vedtaket gjelder behandling av personopplysninger i tilknytning til Alarmtelefonens bruk av sporingsverktøy på Nettstedet. Med sporingsverktøy mener vi teknologi, herunder informasjonskapsler og piksler, som integreres på nettsider for å monitorere besøkendes adferd på siden. Sporingsverktøy kan brukes til å samle inn opplysninger som IP-adresse, annonse-ID, geografisk lokasjon og teknisk informasjon, for eksempel skjermstørrelse og -oppløsning. Disse opplysningene kan sammenstilles av nettsideoperatør eller annonseselskaper og dermed identifisere en enkeltperson via brukerens kommunikasjonsenhet.

Datatilsynets oppgave er å føre tilsyn med etterlevelsen av personvernforordningen, jf. personvernforordningen artikkel 57 nr. 1 bokstav a og personopplysningsloven § 20.

Datatilsynet har gjennomført et digitalt tilsyn mot seks nettsider for å se nærmere på deres bruk av sporingsverktøy. Nettstedet 116111.no er ett av nettstedene som er valgt ut i tilsynet.

Bakgrunnen for tilsynet er medieoppslag om nettsteder som deler personopplysninger med tredjeparter ved bruk av sporingsverktøy.¹ I flere av tilfellene omtalt i media kan informasjonen som er samlet inn og delt med tredjeparter utgjøre personopplysninger av

¹ Se for eksempel [Nettapotek delte med Facebook at du så på klamydiatester – NRK Kultur og underholdning](#), publisert 4. desember 2023.

sensitiv art eller særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1. Det siste året har Datatilsynet oppfordret virksomheter til å gjennomgå nettsidene sine for å vurdere hvilke sporingsverktøy de bruker, og i desember 2023 varslet vi at vi vil gjennomføre tilsyn med norske nettsiders bruk av sporingsverktøy.²

Vi valgte ut ulike kategorier av nettsider som behandler beskyttelsesverdig informasjon om de som besøker sidene og plukket ut seks aktører fra de ulike kategoriene som vi førte tilsyn med. Formålet med å gjennomføre disse tilsynene er å kunne belyse ulike problemstillinger i forbindelse med bruk av sporingsverktøy. Videre har vi hatt som et viktig mål at vurderingene våre skal kunne gi veiledning til aktører utover de som er omfattet av dette tilsynet.

I tilsynene har vi gjennomgått og kontrollert om nettstedenes bruk av sporingsverktøy er i samsvar med de relevante kravene i personvernforordningen, herunder rettslig grunnlag, jf. personvernforordningen artikkel 6 nr. 1.

3.2.2. Innledende saksbehandling

Vi gjennomførte et digitalt tilsyn på Nettstedet 14. mars 2024. Vi besøkte nettsidene og dokumenterte innholdet på den, herunder personvernerklæringen. Vi gjennomførte også en teknisk undersøkelse som viste hvilke sporingsverktøy som var integrert i Nettstedet.

Vi sendte et brev 19. mars 2024 med dokumentasjon på våre faktiske funn på Nettstedet. Brevet inneholdt skjermdumper av Nettstedet samt en teknisk rapport utarbeidet av Datatilsynet som registrerte hvilke sporingsverktøy som var aktive på Nettstedet. Vi oppfordret kommunen til å sende oss kommentarer på funnene, dersom de hadde noen.

I brev 30. april 2025 skrev kommunen at den fant det «underlig» at tilsynet ikke ble «forhåndsvarslet ved en formell henvendelse», og at det var «beklagelig at det ikke er kommunisert initielle vurderinger av funnene som ble gjort på (Nettstedet)».

Brevet 19. mars 2024 var ikke ment å være et varsel om tilsyn eller en oppfordring om å gjøre endringer på Nettstedet. Datatilsynet ønsket å få en omforent forståelse av de faktiske forholdene i saken før vi gikk nærmere inn i de rettslige vurderingene. Brevets formål var å få eventuelle kommentarer på dokumentasjonen vi hadde samlet inn. I brevet presiserte Datatilsynet at vi ikke hadde gjort noen rettslige vurderinger av funnene på det tidspunktet.

23. april 2024 snakket vår saksbehandler på telefon med nettsideutvikleren til Alarmtelefonen, Tress Design AS. I samtalen presiserte vi hva som var formålet med tilsynet, at vi ikke hadde gjort noen rettslige vurderinger enda og at vi sendte brevet i tilfelle kommunen ønsket å kommentere de faktiske funnene våre. Nettsideutvikleren sa deretter at Alarmtelefonen ikke delte personopplysninger med tredjeparter og at sporingsverktøyene på Nettstedet var standard å bruke. Vi tok dette til etterretning.

² Se [Datatilsynet varsler granskning etter NRK-avsløringer – NRK Norge – Oversikt over nyheter fra ulike deler av landet](#), publisert 21. desember 2023.

Alarmtelefonens leder, Margrethe Østerhus, bekreftet deretter at kommunen ikke hadde noen ytterligere merknader til de faktiske funnene i e-post 24. april 2024.

Datatilsynet ba Alarmtelefonen 13. juni 2024 om å legge frem opplysninger om hvor mange besøkende de har på sine nettsider. Alarmtelefonen la frem utdrag fra sine årsrapporter 2021-2023 med denne informasjonen 19. juni 2024.

Datatilsynet sendte varsel om vedtak til kommunen 26. mars 2025. I varslet skrev Datatilsynet at vi vurderte å ilegge et overtredelsesgebyr på 300 000 kroner, samt å gi et pålegg om å fjerne sporingsverktøyene Snap Pixel og Meta Pixel fra Nettstedet.

3.2.3. Kommunens brev med kommentarer på varselet om vedtak og avviksmeldingen fra kommunen

Vi mottok kommunens kommentarer til varselet 30. april 2025. Kommunen hadde ikke innvendinger mot de sentrale konklusjonene i varselet, men ba Datatilsynet om å vurdere nivået på overtredelsesgebyret på nytt i lys av kommunens tiltak for å stanse behandlingen. Vi fikk også opplyst at kommunen hadde fjernet alle sporingsteknologier på Nettstedet som ikke var nødvendige for at Nettstedet skulle fungere.

Datatilsynet mottok også en melding om avvik fra kommunen 1. april 2025. Kommunen skrev at Nettstedet brukte flere sporingsteknologier, som Google Analytics, som muligens tilgjengeliggjorde personopplysninger for tredjeparter. I tillegg skrev kommunen at den hadde oppdaget flere mulige brudd på personvernforordningen, herunder pliktene til den behandlingsansvarlige etter artikkel 24 og manglende protokoll over behandlingsaktiviteter etter artikkel 30.³

Avviksmeldinger til Datatilsynet brukes til å rapportere om brudd på personopplysningssikkerheten, jf. artikkel 33 i personvernforordningen. Datatilsynet avsluttet avvikssaken siden den ikke gjaldt et slikt sikkerhetsbrudd, men vi tar hensyn til opplysningene vi mottok i denne saken.

3.2.4. Avgrensning av tilsynet

I forbindelse med tilsynet besøkte vi Nettstedet flere ganger etter den opprinnelige undersøkelsen 14. mars 2024. Det siste besøket skjedde 25. mars 2025.

Dette tilsynet gjelder kun enkelte utvalgte aspekter ved bruk av tredjeparts sporingsverktøy på nettsider. Vi har ikke tatt stilling til andre personvernrettslige problemstillinger i dette tilsynet. Fravær av kommentarer på andre personvernspørsmål betyr derfor ikke at dette er godkjent av oss.

³ Kommunen skrev også opprinnelig at det hadde funnet sted overføring av personopplysninger til tredjeland uten tilstrekkelig overføringsgrunnlag, i strid med artikkel 45. I e-postdialog med kommunen 15. mai fikk vi avklart at meldingen om manglende overføringsgrunnlag skyldtes en misforståelse. Datatilsynet har ikke tatt stilling om kommunen hadde overføringsgrunnlag etter Artikkel 44 i forordningen.

Datatilsynet har valgt å avgrense vår vurdering til Alarmtelefonens behandling av personopplysninger for markedsføringsformål gjennom bruk av sporingsverktøyene Meta Pixel og Snap Pixel i lys av personvernforordningens regler. Vurderingene våre er likevel være relevante for bruk av andre informasjonskapsler, piksler og sporingsverktøy for øvrig. I den sammenhengen noterer vi oss at kommunen fjernet andre sporingsverktøy som faller utenfor avgrensningene til dette tilsynet etter at den mottok varselet 26. mars 2025.

Tilsynet er også avgrenset til etterlevelsen av reglene i personvernforordningen. Vi tar ikke stilling til etterlevelsen av ekomloven.⁴

3.3. Beskrivelse av de faktiske funnene i tilsynet

Under det digitale tilsynet 14. mars 2024, registrerte Datatilsynet at besøkende til forsiden på Nettstedet fikk plassert 17 informasjonskapsler («cookies») i sin nettleser. En informasjonskapsel er en tekstfil som plasseres i brukerens nettleser eller enhet når vedkommende besøker en nettside. Informasjonskapslene kan blant annet brukes til å følge med på hva den besøkende foretar seg på nettsiden. Disse opplysningene sendes til domenet som er knyttet til informasjonskapselen og blir dermed tilgjengeliggjort for nettsideoperatøren.

Flere av informasjonskapslene var førstepartsinformasjonskapsler. Det vil si at de var eid at nettsiden selv. Vi fant også informasjonskapsler som tilhørte Google, Meta og Snap. Selv om disse tilbys av tredjeparter, så er det nettsideoperatøren, i dette tilfellet kommunen, som bestemmer hvilke informasjonskapsler som plasseres i nettleseren når noen besøker Nettstedet.

Nettstedet brukte også sporingspikslene Snap Pixel og Meta Pixel på forsiden og på undersidene. Disse tilhørte henholdsvis Snap Inc., som driver tjenesten Snapchat, og Meta Platforms Ireland Limited, som driver blant annet tjenestene Facebook og Instagram i EU/EØS-landene.

Sporingspiksler er bygget inn i selve nettsiden av operatøren, og de lagres ikke i enheten til brukeren slik som informasjonskapsler. Når en nettside har en sporingspiksel, sendes informasjon til tilbyderen av pikselen om hvilke handlinger brukeren foretar seg på nettsiden.

Meta Pixel registrerer besøkendes handlinger på nettsider og sender informasjon til «connect.facebook.net/en_US/fbevents.js». Dermed tilgjengeliggjøres informasjonen også for Meta Platforms Ireland Limited, som blant annet driver tjenestene Facebook og Instagram i EU/EØS-landene.

Pikselen lastes inn i nettsidens HTML-kode når noen besøker nettsiden. Det fører til at det lagres en _fbp-informasjonskapsel automatisk i nettleseren til den besøkende, med mindre

⁴ Se ellers del 5 i varselet.

informasjonskapselen allerede finnes der. Den lagrer en unik nettidentifikator i _fbp-informasjonskapselen.

Pikselen kan konfigureres til å spore ulike handlinger som brukerne foretar seg på nettsiden pikselen er plassert på. I tilsynet har vi registrert at Meta Pixel sporer hvilke nettsider en bruker laster inn på enheten sin, såkalte «page load events».

Datatilsynet ser at når pikselen lastes inn, så aktiveres også et sporingsscript (/tr-script) som håndterer innsamlingen og tilgjengeliggjøring av data til Meta, herunder informasjon om variabelen «c-user». Våre undersøkelser viser at dersom en bruker er logget inn på Facebook i den samme nettleseren som man laster inn Nettstedet på, så vil denne variabelen vise den unike ID-en tilknyttet personens Facebook-profil. Dermed mottar Meta direkte identifiserende informasjon når noen som er innlogget på Facebook laster inn Nettstedet.

Dersom brukeren ikke er logget inn på Facebook, så vil Nettstedet fremdeles sende informasjon om «page load events» til Meta, sammen med en unik bruker-ID, IP-adresse og digitalt fotspor med informasjon om nettleser, operativsystem, skjermstørrelse mv. Dette er informasjon som gjør det mulig å identifisere de ulike brukerne. Snap Pixel (_scid, __scid_r) fungerer på tilsvarende måte.

Da vi gjennomførte tilsynet 14. mars 2024, gikk det frem av personvernerklæringen til Alarmtelefonen at de bruker informasjonskapsler for å «analysere det generelle bruksmønsteret». Det ble videre opplyst om at opplysningene er «helt anonymisert og blir brukt for statistikk og analyse, samt annonsering». Det ble også opplyst om at informasjonskapslene «registrerer IP-adresse og hvor lenge besøkende er på siden, hva de klikker på og hvilken enhet de bruker, samt gir oss en oversikt over hvor mange besøkende siden har.» Det ble ikke gitt noe informasjon om sporingspikslene, og heller ikke om delingen med Snap eller Meta.

Personvernerklæringen inneholdt ingen informasjon om behandlingsgrunnlaget for behandlingen.

Etter at de faktiske funnene ble lagt frem fra Datatilsynet 19. mars 2024, har Alarmtelefonen gjort endringer i personvernerklæringen slik at den nevnte bruken av pikslene. Det er redegjort for endringene i del 6.4 i vedtaket.

Kommunen fjernet Meta Pixel og Snap Pixel fra Nettstedet etter at den mottok varselet om vedtak. I brevet 30. april 2025 opplyste kommunen også at det fjernet øvrige sporingsverktøy fra Google, herunder tilknyttet Google Analytics og YouTube. Våre undersøkelser bekrefter at disse er fjernet fra Nettstedet. Nettstedet bruker nå bare informasjonskapsler som er nødvendige for at nettsidene skal fungere. Kommunen har også oppdatert personvernerklæringen på Nettstedet.

4. Rettslig bakgrunn

«Personopplysninger» er i personvernforordningen artikkel 4 nr. 1 definert som:

enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

Nettidentifikatorer er uttrykkelig nevnt i personvernforordningen artikkel 4 nr. 1 som et eksempel på en personopplysning. I fortalepunkt 30 begrunnes hvorfor slike opplysninger regnes som personopplysninger:

«Fysiske personer kan knyttes til nettidentifikatorer via utstyr, programmer, verktøy og protokoller, f.eks. IP-adresser, informasjonskapsler eller andre identifikatorer, f.eks. radiofrekvensidentifikasjonsmerker. Dette kan etterlate spor som særlig i kombinasjon med entydige identifikatorer og andre opplysninger som serverne mottar, kan brukes til å opprette profiler for fysiske personer og identifisere dem.»

I fortalepunktet fremheves muligheten til å identifisere personer ved å sammenstille andre opplysninger som mottakeren rimeligvis har tilgang på.⁵

Hva som utgjør behandling av personopplysninger er definert i artikkel 4 nr. 2:

Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

I henhold til personvernforordningen artikkel 4 nr. 7 er en «behandlingsansvarlig»:

en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes (...).

Personopplysninger skal behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte, se personvernforordningen artikkel 5 nr. 1 bokstav a).

Personopplysninger skal videre samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene, se personvernforordningen artikkel 5 nr. 1 bokstav b).

⁵ Se også fortalepunkt 26 til personvernforordningen.

Det er den behandlingsansvarliges ansvar å kunne påvise at behandlingen av personopplysninger skjer i tråd med prinsippene oppstilt i artikkel 5 nr. 1. Dette ansvarlighetsprinsippet er nedfelt i artikkel 5 nr. 2.

All behandling av personopplysninger må ha et rettslig grunnlag i artikkel 6 nr. 1 for å være lovlig. Bestemmelsen lister opp ulike rettslige grunnlag, herunder:

Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

- (a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål, (...)*
- (e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt, (...)*
- (f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.*

Artikkel 6 nr. 3 slår fast at behandling med grunnlag i bokstav e) må skje med grunnlag i lov. Det er med andre ord ikke tilstrekkelig at behandlingen skjer for å utføre en oppgave i allmennhetens interesse eller for å utøve offentlig myndighet. Formålet som gjør behandlingen nødvendig må være angitt i norsk lov.

Med samtykke menes en «frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende», se personvernforordningen artikkel 4 nr. 11 og fortalen punkt 32.

Etter fortelepunkt 42 skal et samtykke «ikke anses som frivillig dersom den registrerte ikke har en reell valgfrihet, eller ikke er i stand til å nekte å gi eller trekke tilbake et samtykke uten at det er til skade for vedkommende».

Når samtykke anvendes som rettslig grunnlag, skal den registrerte ha fått informasjon om hva vedkommende samtykker til, inkludert hvilke personopplysninger som skal behandles og hva som er formålet med behandlingen. Den registrerte skal kunne forutse konsekvensene av å gi samtykke basert på informasjonen som den behandlingsansvarlige gir.⁶ Dette innebærer at den behandlingsansvarlige ikke skal tilsløre realitetene, men forklare tydelig og rett frem hvilke opplysninger som skal samles inn og hva de skal brukes til.⁷ Dersom samtykket ikke er informert, vil den registrerte sin kontroll over egne personopplysninger bli illusorisk, og samtykket vil ikke være et gyldig rettslig grunnlag etter artikkel 6 nr. 1.⁸

⁶ Se "Personvernforordningen Lovkommentar" om artikkel 6, av Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud, konsultert 19. juni 2024 på juridika.no.

⁷ Se "Personvernforordningen Lovkommentar" om artikkel 7(2), av Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud, konsultert 19. juni 2024 på juridika.no.

⁸ Se EDPB Guidelines 05/2020 on consent under Regulation 2016/679, avs. 62-63.

Det europeiske personvernrådet (EDPB) har i sine retningslinjer om samtykke uttalt at den behandlingsansvarlige må vurdere hva slags gruppe personer virksomheten behandler personopplysninger om. For eksempel, dersom en tjeneste er rettet mot en gruppe personer som inkluderer mindreårige, så skal den behandlingsansvarlige sørge for at det gis informasjon som er forståelig for mindreårige.⁹ For å kunne samle inn et informert samtykke fra et barn, så må altså den behandlingsansvarlige forklare hvordan personopplysningene vil behandles på en måte som er klar og enkel for barn å forstå.¹⁰

Samtykket skal gis for et spesifikt formål. Det innebærer at formålet må være tilstrekkelig konkret til å muliggjøre en vurdering av hvorvidt det er nødvendig å behandle de aktuelle personopplysningene og hvorvidt en behandling er i tråd med personvernforordningen.¹¹ Kravet om at samtykke skal være spesifikt skal sikre brukerkontroll og åpenhet for de registrerte, og det er tett knyttet til kravene om at samtykket skal være informert og frivillig. For å oppfylle kravet må den behandlingsansvarlige sørge at formålet er spesifikt på en slik måte at formålsutglidning unngås.¹² ¹³ En behandlingsansvarlig som ber om samtykke for flere ulike formål bør tilrettelegge for en opt in-løsning for hvert enkelt formål. Den behandlingsansvarlige bør gi spesifikk informasjon knyttet til hver enkelt samtykkeforespørsel, slik at den registrerte er kjent med virkningen av de ulike valgene.¹⁴

Et samtykke antas å ikke være gitt frivillig dersom det ikke er mulig å gi separat samtykke for forskjellige behandlingsaktiviteter, se punkt 43 i fortalen til personvernforordningen.¹⁵ Personvernrådet har uttalt at en tjeneste kan inkludere flere behandlingsaktiviteter for flere enn ett formål. I slike saker skal de registrerte kunne velge hvilket formål de aksepterer, og ikke måtte samtykke til flere behandlingsformål under ett (såkalt «bundling»)¹⁶ Slik granularitet er nødvendig for at et samtykke skal være gyldig.

Personvernrådet har gitt råd og anbefalinger til hvordan man skal utforme brukergrensesnitt uten å bruke manipulativt design som bryter med personvernforordningen.¹⁷ Manipulerende design kan påvirke brukeres oppførsel ved å utnytte menneskers biologiske tendenser til å

⁹ Se EDPB Guidelines 05/2020 on consent under Regulation 2016/679, avs. 70.

¹⁰ Se EDPB Guidelines 05/2020 on consent under Regulation 2016/679, avs. 126.

¹¹ Se “Personvernforordningen Lovkommentar” av Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud, konsultert 19. juni 2024 på juridika.no. Se også EDPBs retningslinjer om samtykke hvor det refereres til A29 WP Opinion 3/2013 on determination of purposes, i fotnote 28 på s. 13 og fotnote 30 på s. 14. Se Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, s. 15-16.

¹² Se EDPB Guidelines 05/2020 on consent under Regulation 2016/679, s. 14.

¹³ Personvernrådets forgjenger, Artikkel 29-gruppen, har uttalt at et formål som er vagt eller generelt, slik som for eksempel «markedsføring» («marketing purposes»), vil, uten flere detaljer, vanligvis ikke oppfylle kravet til å være spesifikt. Hvor detaljert et formål må være beskrevet for å være tilstrekkelig spesifikt avhenger av konteksten opplysningene er samlet inn i og hvilke personopplysninger som er omfattet. Se Article 29 Data Protection Working Party Opinion 03/2013 on purpose limitation, s. 15-16.

¹⁴ Se EDPB Guidelines 05/2020 on consent under Regulation 2016/679, s. 14-15.

¹⁵ Se også EDPB Guidelines 05/2020 on consent under Regulation 2016/679, s. 12.

¹⁶ Se EDPB Guidelines 05/2020 on consent under Regulation 2016/679, s. 12.

¹⁷ Se EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them.

gjøre feilslutninger, såkalte kognitive bias. Det kan eksempelvis føre til at den registrerte ikke gjør egne bevisste valg og heller velger det enkleste alternativet, uten tanke på eventuelle virkninger av valget¹⁸ Dette kan for eksempel gjøres med fargevalg i brukergrensesnittet ved at ulike valg har ulike farger, og hvor et alternativ er mer iøynefallende enn det mest personvernvennlige alternativet.

Det franske datatilsynet, CNIL, fattet et vedtak i desember 2023 hvor de kom til at «nudging» i form av farge, design og valg av tekst på knappene for samtykke medførte at kravet til frivillighet ikke var oppfylt.¹⁹

At samtykket skal være utvetydig innebærer at det skal gis ved en aktiv handling eller erklæring fra den registrerte. Det skal være klart at den registrerte har samtykket til den aktuelle behandlingen.²⁰

I punkt 38 i fortalen til personvernforordningen står det at:

«Barns personopplysninger fortjener et særlig vern, ettersom barn kan være mindre bevisste på aktuelle risikoer, konsekvenser og garantier samt på de rettigheter de har når det gjelder behandling av personopplysninger. Et slikt særlig vern bør især få anvendelse på bruk av barns personopplysninger for markedsføringsformål eller for å opprette personlighets- eller brukerprofiler samt på innsamling av personopplysninger om barn når de bruker tjenester som tilbys direkte til barn. Samtykke fra den som har foreldreansvaret, bør ikke være nødvendig i forbindelse med forebyggings- eller rådgivningstjenester som tilbys direkte til barn.»

Ettersom barn fortjener et særlig vern, bør all informasjon og kommunikasjon, dersom behandlingen gjelder barn, være formulert på et klart og enkelt språk som barnet lett kan forstå, se punkt 58 i fortalen til personvernforordningen.

I forlengelsen av prinsippet om åpenhet gjelder flere regler om åpenhet og informasjon om behandlingen i kapittel III i forordningen. Artikkel 13 stiller krav til hvilke opplysninger de registrerte skal få av behandlingsansvarlig når det samles inn personopplysninger om den, herunder hvilket grunnlag behandlingen bygger på og hvem dataene deles med. Den behandlingsansvarlige skal gi den registrerte informasjon om behandlingen på tidspunktet for innsamlingen av personopplysningene.

Artikkel 12 nr. 1 slår fast at informasjonen som gis til de registrerte skal være «kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk, især når det gjelder informasjon som spesifikt er rettet mot et barn». Informasjonen må med andre ord tilpasses den aktuelle gruppen registrerte.

¹⁸ Se EDPB Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them, i avsnitt 3. Se også Forbrukerrådets rapport «Deceived by design», [Manipulerende design – Forbrukerrådet](#).

¹⁹ SAN-2023-025 [Data brokers: TAGADAMEDIA fined €75,000 | CNIL](#)

²⁰ Se EDPB Guidelines 05/2020 on consent under Regulation 2016/679, s. 18.

Artikkel 24 nr. 1 pålegger den behandlingsansvarlige å gjennomføre egnede tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen.

5. Tilsynets avgrensning mot ekomloven

Datatilsynet skal håndheve regelverket i personopplysningsloven, herunder personvernforordningen. Regelverket gjelder for all behandling av personopplysninger når ikke annet er bestemt i eller med hjemmel i lov, jf. personopplysningsloven § 2 første ledd.

Bruk av informasjonskapsler var på tilsynstidspunktet særregulert i ekomloven 2003 § 2-7 b, som gjennomfører artikkel 5 nr. 3 i EUs kommunikasjonsverndirektiv.²¹

I dag er ekomloven 2003 § 2-7 b erstattet av ekomloven 2024 § 3-15. Den største forskjellen mellom gammel og ny bestemmelse er at ny bestemmelse spesifiserer at samtykket skal oppfylle kravene etter personvernforordningen.

Av ekomloven 2003 § 2-7 b første ledd følger det at:

«Lagring av opplysninger i brukers kommunikasjonsutstyr, eller å skaffe seg adgang til slike, er ikke tillatt uten at brukeren er informert om hvilke opplysninger som behandles, formålet med behandlingen, hvem som behandler opplysningene, og har samtykket til dette.»

Ifølge ordlyden omfatter bestemmelsen for det første lagring av opplysninger på den registrertes enhet (mobiltelefon, datamaskin, nettbrett mv.). Bestemmelsen omfatter også det å få tilgang til opplysningene som er lagret på enheten. I forarbeidene til bestemmelsen presiseres det at regelen regulerer selve handlingen – det å lagre eller å hente ut informasjonen.²² Bestemmelsen har som formål å verne brukerens kommunikasjonsutstyr ettersom dette er en del av privatlivet, uavhengig av om det skjer en behandling av personopplysninger, jf. kommunikasjonsverndirektivet fortalepunkt 24.

I majoriteten av tilsynstidsperioden var Nasjonal kommunikasjonsmyndighet (Nkom) fagmyndighet for denne bestemmelsen i Norge. Ekomlovens særkrav ble derfor ikke vurdert i tilsynet.

Behandlingen av personopplysninger utover det å lagre opplysninger i enheten, eller å skaffe seg tilgang til disse, faller utenfor virkeområdet til bestemmelsen i ekomloven. Som tilsynsmyndighet for personopplysningsloven har Datatilsynet alltid kompetanse til å vurdere denne behandlingen.

Personopplysningsloven gjelder også for behandling som faller innenfor ekomloven 2003 § 2-7 b og ekomloven 2024 § 3-15 så langt det er snakk om personvernaspekter som ikke er

²¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [ePrivacy Directive].

²² Prop. 69 L (2012-2013), s. 102.

regulert av bestemmelsen. Det vil si at for eksempel prinsippene for behandling av personopplysninger i personvernforordningen artikkel 5 og kravene til informasjonssikkerhet i artikkel 32 også gjelder når man lagrer eller får tilgang til personopplysninger i den registrertes enhet. Dette er i tråd med kommunikasjonsverndirektivet fortalepunkt 10 og personvernforordningen fortalepunkt 173, som sier at personvernforordningen gjelder for alle sidene ved vern av grunnleggende rettigheter og friheter som ikke er særregulert i kommunikasjonsverndirektivet, inkludert den registrertes rettigheter og de behandlingsansvarliges plikter.

Tilsynet er avgrenset til bruken av sporingsverktøy på Nettstedet som faller inn under Datatilsynets kompetanse etter personopplysningsloven og personvernforordningen.

Datatilsynet er fra og med 2025 tilsynsmyndighet også for selve lagringen i kommunikasjonsutstyr og adgang til de lagrede opplysningene etter ekomloven 2024 § 3-15, sammen med Nkom.²³ Vi understreker derfor viktigheten av at nettsideoperatøren sørger for å overholde kravene til samtykke i ny ekomlov ettersom dette kan bli gjenstand for senere tilsyn.

6. Datatilsynets vurdering

6.1. Behandling av personopplysninger

Når en besøkende laster inn en nettside på Nettstedet, aktiveres de innebygde pikslene. Da sender pikslene informasjon om den spesifikke nettsiden som er lastet inn sammen med identifikatorer om den besøkende. Opplysningene som deles inkluderer dermed unike identifikatorer som utpeker den enkelte personen og skiller dem fra andre besøkende på Nettstedet.

I dette tilfellet ble personopplysningene tilgjengeliggjort for Snap og Meta, som er operatører av store plattformer for sosiale medier. Plattformene deres, som for eksempel Snapchat og Instagram, har mange brukere, herunder barn og unge. Brukerprofilene inneholder som regel direkte identifiserende informasjon som kan knyttes til personopplysningene som samles inn gjennom pikslene.

Formålet med pikslene er knyttet til selskapenes forretningsmodell, som går ut på å samle inn data om sine brukere for å selge persontilpasset reklame. Dette fremgår av deres personvernerklæringer. Vi legger derfor til grunn at det også har skjedd her.

Meta skriver i sin personvernerklæring:

«Vi samler inn og mottar informasjon fra partnere, målingsleverandører, markedsføringsleverandører og andre tredjeparter om diverse informasjon om deg og aktivitetene dine på og utenfor produktene våre. Her er noen eksempler på informasjon vi mottar om deg: (...) Nettsteder du besøker og data fra informasjonskapsler, f.eks.

²³ Forskrift 2024-12-20-3413 om delegering av myndighet etter lov om elektronisk kommunikasjon pkt. 12.

gjennom sosiale programtillegg eller Meta-pikselen (...) Vi bruker informasjonen vi samler inn, for å gi deg en personlig opplevelse, inkludert annonser (hvis vi viser deg annonser i Meta-produkter), sammen med de andre formålene vi forklarer i mer detalj nedenfor.»²⁴

I sin personvernerklæring skriver Snap:

«For eksempel behandler vi informasjonen din for å gi deg en mer personlig opplevelse, inkludert for å vise deg innhold og informasjon som er mest relevant for opplevelsen din, samt mer relevante annonser. Ved å forstå interessene og preferansene dine kan vi gi deg en bedre produktopplevelse. (...)

Den siste kategorien med data vi samler inn er informasjon om deg som vi kan motta fra andre, som for eksempel andre brukere, våre tilknyttede selskaper, og tredjeparter. Dette inkluderer koblete tredjepartstjenestedata (informasjon vi får når du kobler Snapchat-kontoen din til en annen tjeneste), data fra annonsører (informasjon fra annonsører, apputviklere, utgivere og andre tredjeparter for å hjelpe til med å målrette eller måle ytelsen til annonser) (...).»²⁵

Snap Pixels rolle i innsamlingen av personopplysninger beskrives i Snaps retningslinjer for annonsesalg:

«Annonsørene og samarbeidspartnerne våre gir oss data fra sine egne apper, nettsteder og plattformer, som vi bruker til å tilpasse annonsene vi viser. (...) Vi henter inn denne informasjonen på noen forskjellige måter, inkludert gjennom Snap Pixel og Snap sin konverterings-API. I begge tilfeller er det innebygd en liten kode i tredjepartsplattformer (som nettsteder og apper) som samler inn informasjon om begrensede aktiviteter på disse plattformene. Vi bruker også denne informasjonen til å gi annonsører rapporter om hvor effektive annonsene deres er.»²⁶

I begge erklæringene fremgår det klart at personopplysninger ble samlet inn av selskapene og kombinert med annen informasjon for å «personalisere» brukerens opplevelse på deres plattform.

Det er uklart i hvilken grad selskapene bruker personopplysninger innhentet om barn til å tilpasse annonser, men i mange tilfeller vil de ikke vite om en bruker er mindreårig (for eksempel der noen har oppgitt feil fødselsdato). Det er uansett på det rene at Nettstedet delte og tilgjengeliggjorde dataene for selskapene i perioden 14. mars 2024 til 25. mars 2025.

²⁴ Metas personvernerklæring, [Metas retningslinjer for personvern – Slik samler Meta inn og bruker brukerdata | Personvernssenter | Administrer personvernet ditt på Facebook, Instagram og Messenger | Facebook Personvern](#), sist besøkt 25. november 2024.

²⁵ Snaps personvernerklæring, values.snap.com/privacy/privacy-policy?lang=nb-NO, sist besøkt 28. januar 2025.

²⁶ Snaps retningslinjer for personvern og annonsesalg, [Åpenhet om annonser på Snapchat | Personvern på Snapchat](#), sist besøkt 28. januar 2025.

Sammenkoblingen av informasjon gjorde det mulig for Snap eller Meta å kunne knytte informasjon om at noen hadde besøkt Alarmtelefonens nettsider med deres profil på plattformene deres. Dataene som ble tilgjengeliggjort gjennom pikslene var derfor personopplysninger etter personvernforordningen artikkel 4 nr. 1.

Det er dessuten klart at det skjer videre behandling av personopplysninger ut over å lagre eller lese av informasjon i brukerens utstyr, for eksempel gjennom behandling av personopplysninger innhentet ved hjelp av sporingspiksel og etterfølgende behandling, jf. personvernforordningen artikkel 4 nr. 2. Dette faller klart innenfor personvernforordningen.

6.2. Behandlingsansvar

Behandlingsansvarlig er et rettslig pliktsubjekt med ansvar for å behandle personopplysningene i tråd med reglene i personvernforordningen. Som nevnt i punkt **Feil! Fant ikke referanse-kilden.** defineres «behandlingsansvarlig» som den som alene eller sammen med andre fastsetter formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. artikkel 4 nr. 7.

EU-domstolen har også fastslått at fysiske eller juridiske personer som utøver innflytelse over behandlingen av personopplysninger til eget formål, og som deltar – som et resultat – i fastsettelsen av formål og midler for denne behandlingen, kan anses som en behandlingsansvarlig.²⁷ Når det er felles behandlingsansvar blant flere aktører for en behandling, kreves det ikke at hver aktør har tilgang til de aktuelle personopplysningene. Felles ansvar betyr likevel ikke at forskjellige aktører har samme ansvar for en behandling av personopplysninger. De forskjellige aktørene kan være ansvarlige for behandlingen av personopplysninger på forskjellige faser og i varierende grader, som betyr at hver aktørs ansvar må vurderes i lys av alle relevante sider av saken.²⁸

I Fashion ID-dommen²⁹ tok EU-domstolen stilling til ansvarsfordelingen mellom en nettstedsoperatør og tilbyderer av et sporingsverktøy. Spørsmålet var om nettstedsoperatøren var behandlingsansvarlig ved å implementere en programkode på nettsiden som overførte personopplysninger til en tredjepart, til tross for at nettstedsoperatøren ikke selv kunne påvirke hva som skjedde med opplysningene etter at de ble hentet av tredjeparten. EU-domstolen konkluderte med at nettstedsoperatøren hadde gjort det mulig for tredjeparter, i dette tilfellet Facebook, å få tilgang til personopplysninger om brukeren. Videre kom EU-domstolen frem til at nettstedsoperatøren, sammen med tredjeparten, bestemte formål og virkemidler ved innsamling og deling av personopplysninger fra nettstedet. Nettstedsoperatøren var derfor behandlingsansvarlig for opplysningene som endte hos tredjepart til tross for at de ikke hadde tilgang til opplysningene selv. EU-domstolen understreket at nettstedsoperatøren hadde godtatt innsamlingen og den videre utleveringen til tredjeparter ved å implementere sporingsverktøy på nettsiden for å få kommersielle fordeler i form av markedsføring.

²⁷ C-25/17, *Jehovan todistajat*, avsnitt 68.

²⁸ C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, avsnitt 38 og C-25/17, *Jehovan todistajat*, avsnitt 69.

²⁹ C-40/17, *Fashion ID GmbH & Co. KG*.

Ut ifra personvernerklæringen på Nettstedet, slik den så ut pr. 13. mai 2024, virker det som om formålet med å bruke pikslene var å måle effekten av annonsekampanjer på sosiale medier.³⁰ Kommunen bekreftet at dette var formålet i brevet 30. april 2025.

Kommunen er den som har besluttet å integrere pikslene på Nettstedet. Piksler kan også konfigureres til å spore spesifikke typer «hendelser» på nettsidene. På den måten bestemmer nettstedsoperatøren hvilke personopplysninger som tilgjengeliggjøres for pikseltilbyderen.

Kommunen har innlemmet pikslene på Nettstedet og dermed tilrettelagt for at tredjepart får tilgang til personopplysninger om de som besøker Nettstedet. Dette innebærer også at kommunen har muliggjort de etterfølgende aktivitetene for markedsføringsformål. Den etterfølgende behandlingen i markedsføringsøyemed skjer også i kommunens interesse. Kommunen har derfor utøvd bestemmende innflytelse over formål og midler og har derfor behandlingsansvar for behandlingen av personopplysninger som skjer ved bruken av sporingsverktøy på Nettstedet, jf. personvernforordningen artikkel 4 nr. 7.

6.3. Rettslig grunnlag

Behandling av personopplysninger ha et rettslig grunnlag i en av alternativene i artikkel 6 nr. 1. Det er særlig samtykke etter bokstav a) og en interesseavveining etter bokstav f) som kan utgjøre behandlingsgrunnlag for behandling av personopplysninger for markedsføringsaktiviteter.

Vi bemerker at det fra 1. januar 2025 gjelder krav om gyldig samtykke for plassering av informasjonskapsler, men dette kravet gjaldt ikke på tilsynstidspunktet.

Kommunen har ikke angitt hvilket behandlingsgrunnlag de bruker for å dele personopplysninger med Snap og Meta.

Datatilsynet kan ikke se at kommunen kan basere seg på behandlingsgrunnlaget i artikkel 6 nr. 1 bokstav e) siden det ikke er noen relevant lovgivning som gjør denne behandlingen nødvendig for kommunen å utføre.

Siden det er en kommune som er behandlingsansvarlig, så skal som hovedregel ikke interesseavveining brukes som et behandlingsgrunnlag, jf. artikkel 6 nr. 1 siste setning.

Datatilsynet legger til grunn at kommunens interesse i behandlingen er å måle effekten av sine markedsføringskampanjer. Uavhengig av om behandlingen er nødvendig for å oppnå det formålet, så er Datatilsynets vurdering at en interesseavveining ikke rettferdiggjør tilgjengeliggjøringen i dette tilfellet.

³⁰ Datatilsynet legger til grunn at det også var formålet da vi gjennomførte tilsynet 14. mars 2024, før endringen i personvernerklæringen.

Nettstedet retter seg mot barn, og det er først og fremst personopplysninger om barn som behandles for markedsføringsformål. Fortalepunkt 38 i personvernforordningen sier at barn har rett på et særlig vern i slike sammenhenger.

Datatilsynet vurderer også at kan det si mye om en person at vedkommende har vært inne på Nettstedet, særlig når det skjer gjentatte ganger og over tid. Selv om Nettstedet retter seg mot mange ulike typer problematikk og de ulike undersidene ikke er rettet mot f.eks. diagnoser, kan man indirekte utlede at vedkommende person har det vanskelig, som i seg selv er veldig privat. Dersom vedkommende i tillegg har vært inne på en av veiledningsartiklene, kan man utlede informasjon om at vedkommende for eksempel har kjærlighetssorg, negative tanker eller søvnproblemer. Dette er problematikk som befinner seg tett opp til definisjonen av særlige kategorier av personopplysninger i personvernforordningen artikkel 9, uten at Datatilsynet har konkludert på dette punktet.

Tilgjengeliggjøringen av disse opplysningen har klare personvernkonsekvenser for de registrerte. Behandlingen gjelder opplysninger av en veldig privat art, og de settes i sammenheng med annen informasjon som kan brukes av tredjepartsaktører til kommersielle formål. Det er ellers uklart hvordan personopplysningene behandles videre av Snap og Meta. Mange av de berørte er barn, og det er personer som ikke nødvendigvis forstår at deres aktiviteter på en internettside spores eller som er i stand til å ivareta sine rettigheter. Vi kan ikke se at interessen i behandlingen lar seg rettferdiggjøre, holdt opp mot behandlingens virkning på de registrertes personvern og rettigheter. Den aktuelle behandlingen kan ikke la seg basere på en interesseavveining etter artikkel 6 nr. 1 bokstav f).

Datatilsynet kan ikke se at delingen er nødvendig for å oppfylle en avtale eller en rettslig forpliktelse for kommunen, og heller ikke for å verne om enkeltpersoners vitale interesser.

Samtykke etter artikkel 6 nr. 1 bokstav a) står derfor igjen som det eneste mulige rettslige grunnlaget.

Nettstedet har ikke etablert løsninger for å innhente samtykke til behandlingen av personopplysninger fra de som besøker siden.

Vår konklusjon er derfor at behandlingen ikke oppfyller krav til rettslig grunnlag, og følgelig er i strid med personvernforordningen artikkel 6 nr. 1.

6.4. Informasjon om behandlingen

Nettstedet opplyste om at henvendelser til Alarmtelefonen var anonyme gjennom hele tilsynsperioden. Dette sto gikk frem av forsiden på Nettstedet og i pop-up knappen som sender brukene til Alarmtelefonens chat-tjeneste. Denne knappen er synlig på alle sidene på Nettstedet. Disse løftene om anonymitet må antas å gjelde direkte henvendelser på telefon eller på chat-tjenesten, men de skaper også en forventning om fortrolighet mellom Alarmtelefonen og brukeren av tilbudet. Siden Nettstedet er en måte for å gi informasjon om Alarmtelefonens tilbud og veiledning, så vil forventningen om fortrolighet naturligvis også gjelde behandlingen av personopplysninger i forbindelse med besøk på Nettstedet.

I brevet 30. april skrev kommunen:

«Kommunen kjenner seg ikke igjen i at det skapes en forventning om fortrolighet som strekker seg ut over de direkte henvendelsene, da det skrives eksplisitt at det handler om henvendelser. Men vi tar Datatilsynets forståelse til etterretning og vil etterleve den i det videre.

Forståelsen om fortrolighet som er lagt til grunn fra Alarmtelefonen sin side, er hentet fra en barnevernfaglig forståelsesramme, hvor teksten fra nettsiden «Du velger selv hva du vil fortelle, og om du vil fortelle hvem du er eller ikke.» ligger til grunn. I denne forståelsen er det forholdet mellom «klient» og «terapeut» som er anonymt, og «klienten» behøver ikke å identifisere seg.

Vi ser at dette ikke er tilstrekkelig i kontekst av dette tilsynet, og at det er særlig problematisk da identifiserende opplysninger er overlatt til tredjepart.»

Datatilsynet oppfatter ikke at kommunen er direkte uenig i vår vurdering om at brukere av Nettstedet har en berettiget forventning om fortrolighet. Datatilsynet presiserer likevel at løftene om anonymitet i forbindelse med henvendelsene bare er en del av konteksten rundt Nettstedet som skaper en forventning om fortrolighet. De som ønsker å bruke chat-tjenesten må besøke Nettstedet for å få tilgang til den, og det er rimelig å forvente at besøk på Nettstedet ikke deles med tredjeparter for kommersielle formål. I tillegg er innholdet på Nettstedet rettet mot barn og unge som trolig ikke ønsker å snakke med foresatte, venner eller andre tillitspersoner. De forventer ikke at deres besøk på Nettstedet deles med sosiale medieplattformer som Snapchat eller Instagram.

Personvernerklæringen slo også fast at behandlingen av personopplysninger på Nettstedet var anonym. Den 14. mars 2024 omtalte personvernerklæringen bruken av informasjonskapsler på generelt nivå:

«For at vår nettside skal fungere optimalt, bruker vi cookies for å analysere det generelle brukermønsteret. Disse opplysningene er helt anonymisert og blir brukt for statistikk og analyse av nettsiden, samt annonsering.

Informasjonskapsler (på engelsk "Cookies") er små tekstfiler som blir lagret på enheten din når du besøker nettsiden vår. Disse registrerer IP-adresse og hvor lenge besøkende er på siden, hva de klikker på og hvilken enhet de bruker, samt gir oss en oversikt over hvor mange besøkende siden har.»

Det ble opplyst at dataene var anonyme. Samtidig sto det at opplysninger som IP-adresse og hvilken enhet den registrerte bruker for å få tilgang til siden, ble registrert. Dette er unike identifikatorer som altså ble tilgjengeliggjort med tredjeparter. Det stemte med andre ord ikke at opplysningene var anonyme.

Informasjonen på nettstedet var derfor både mangelfull, uriktig og misvisende.

Personvernerklæringen omtalte ikke bruken av pikslene, og heller ikke at personopplysningene ble tilgjengeliggjort for Snap eller Meta. Det ble heller ikke redegjort for hvilket behandlingsgrunnlag Alarmtelefonen la til grunn for behandlingen.

Informasjonen var heller ikke tilpasset målgruppen for Alarmtelefonens nettsider, barn mellom 7 og 18 år. Informasjonen var teknisk og ga et villedende inntrykk av hva behandlingen gikk ut på. Vi legger til grunn at barn, spesielt unge barn, i mange tilfeller ikke hadde forutsetninger for å forstå den.

Etter at varslet om tilsyn ble sendt 19. mars 2024, gjorde kommunen endringer i personvernerklæringen. Endringen gikk hovedsakelig ut på at listen over informasjonskapsler og sporingspiksler ble gjort mer fullstendig. 13. mai 2024 opplyste personvernerklæringen om bruken av henholdsvis Snap Pixel og Meta Pixel:

«_scid

Informasjonskapsel assosiert med Snapchat. Angir en unik ID for den besøkende, som gjør det mulig for tredjepartsannonsører å målrette den besøkende med relevant reklame. Denne sammenkoblingstjenesten leveres av tredjeparts annonsehuber, noe som letter sanntidsbudgivning for annonsører. Fjernes etter 1 år og 1 måned.

_scid_r

Angir en unik ID for den besøkende, som lar tredjepartsannonsører målrette den besøkende med relevant reklame. Denne sammenkoblingstjenesten leveres av tredjeparts annonsehuber, som letter budgivning i sanntid for annonsører. Fjernes etter 1 år og 1 måned. (...)

_fbp

_fbp-cookien, eller Facebook Pixel, brukes til å spore og måle Facebook-annonsekampanjer. Den samler inn brukerinteraksjonsdata, og hjelper annonsører med å optimalisere annonser og målgrupper. Denne førstepartsinformasjonskapselen inneholder ikke personlig identifiserbar informasjon, men fungerer sammen med andre Facebook-informasjonskapsler for å lage unike brukeridentifikatorer. Fjernes etter 3 måneder.»³¹

Disse endringene er utilstrekkelige for å bøte på informasjonsmanglene vi avdekket da vi gjennomførte tilsyn i mars. Den uriktige påstanden om anonymitet sto fortsatt i personvernerklæringen, og angivelsen av behandlingsgrunnlaget manglet fortsatt. Informasjonen om pikslene er meget teknisk og er ikke egnet til å gi barn noen reell forståelse av hvem deres personopplysninger ble tilgjengeliggjort for eller hva de ble brukt til.

³¹ Personvernerklæringen hadde samme ordlyd da Datatilsynet undersøkte den for siste gang 25. mars 2025.

På tilsynstidspunktet oppga kommunen at den ikke behandlet personopplysninger i kontekst av sporingsverktøyene, hvilket er feil, og de besøkende fikk derfor ikke informasjonen de har krav på etter artikkel 13 i relasjon til disse behandlingene. Kommunen har derfor brutt artikkel 13 i personvernforordningen.

I den grad det er gitt informasjon om sporingsverktøyene, var informasjonen vanskelig å forstå og uklar, og den var i alle fall ikke tilpasset barn. Dette utgjør et brudd på artikkel 12 nr. 1.

Kommunen opplyste i brevet 30. april 2025 at de har endret personvernerklæringen siden de mottok varselet, og at den jobber med å gjøre personvernerklæringen bedre tilpasset Nettstedets målgruppe. Datatilsynet har ikke gjort noen vurderinger av disse endringene, men bemerker at det er positivt at kommunen har iverksatt dette arbeidet.

7. Valg av reaksjon

7.1. Pålegg om stans

Datatilsynet varslet et pålegg om stans i bruken av Meta Pixel og Snap Pixel 26. mars 2025. Siden kommunen har fjernet sporingsverktøyene fra Nettstedet, har behovet for et pålegg falt bort.

Datatilsynet ilegger ikke pålegg om stans.

7.2. Ileggelse av overtredelsesgebyr

7.2.1. Om vilkårene for ileggelse av overtredelsesgebyr

Overtredelsesgebyr er et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsregelverket.

I samsvar med Høyesteretts praksis, jf. Rt-2012-1556, legger vi til grunn at overtredelsesgebyr er å anse som straff etter Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for overtredelse for å kunne ilegge gebyr.

Forvaltningsloven § 46 første avsnitt presiserer at det er gjelder et skyldkrav for å ilegge administrative sanksjoner. Med mindre noe annet er bestemt er skyldkravet uaktsomhet.

Personvernforordningen artikkel 83 inneholder vilkårene for ileggelse av overtredelsesgebyr. Ordlyden i bestemmelsen stiller ikke opp et uttrykkelig skyldkrav, men EU-domstolen har slått fast at virksomheten må ha utvist uaktsomhet med hensyn til overtredelsene for å kunne ilegges overtredelsesgebyr.³² Det er derimot ikke nødvendig at en identifisert enkeltperson i

³² C-807/21 (Deutsche Wohnen), domsslutningen punkt 2.

virksomheten har handlet uaktsomt.³³ Det er tilstrekkelig at virksomheten som helhet burde ha klart å unngå overtredelsen. Det betyr at såkalte anonyme eller kumulative feil kan føre til at skyldkravet er oppfylt.

7.2.2. Datatilsynets kompetanse til å ilegge overtredelsesgebyr

Etter personopplysningsloven § 26 andre avsnitt kan Datatilsynet ilegge overtredelsesgebyr mot offentlige myndigheter og organer for brudd på personvernforordningen, i tråd med personvernforordningen artikkel 83.

Overtredelsesgebyr skal være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Artikkel 83 nr. 2 lister opp en rekke momenter som skal vektlegges ved illeggelse av overtredelsesgebyr:

- a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,*
- b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,*
- c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd,*
- d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32,*
- e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren,*
- f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den,*
- g) kategoriene av personopplysninger som er berørt av overtredelsen,*
- h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen,*
- i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes,*
- j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42 og*

³³ C-807/21 (Deutsche Wohnen), domsslutningen punkt 1.

k) enhver annen skjerpene eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen

I denne saken er den maksimale gebyrsatsen 20 000 000 euro, jf. artikkel 83 nr. 3 og 5

7.2.3. Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet har konkludert med at Kristiansand kommune brøt artikkel 6, 12 og 13 i personvernforordningen ved bruken av Snap Pixel og Meta Pixel på Nettstedet.

Nedenfor gjennomgår vi de momentene som vi anser som relevante for vurderingen av om overtredelsesgebyr skal ilegges:

- a) *karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd*

Når det gjelder karakteren av overtredelsen, er det snakk om manglende lovlighet og åpenhet, altså helt grunnleggende personvernnormer. De øvrige reglene om behandling av personopplysninger forutsetter at den behandlingsansvarlige har et lovlig behandlingsgrunnlag. Uten åpenhet kan ikke den registrerte ivareta rettighetene sine.

Når det gjelder alvorlighetsgraden, ser Datatilsynet alvorlig på disse overtredelsene. Nettstedet har lagt til rette for at det har blitt samlet inn private og følsomme personopplysninger om barn, og behandlingen av dem gir betydelige personvernkonsekvenser. Opplysningene har blitt tilgjengeliggjort for kommersielle aktører som er lite åpne om hva de vil bruke personopplysningene til eller hvor lenge de vil behandle dem. Den konkrete personvernkonsekvensen for de registrerte er et tap av kontroll over personopplysninger som man med rette kan forvente skal holdes privat. I tillegg er det vanskelig for Datatilsynet å kartlegge den eventuelle risikoen for øvrige brudd grunnet de kommersielle aktørenes manglende åpenhet. Dette er meget skjerpene.

Barn og unge har i tillegg krav på et særlig vern om deres personopplysninger siden de er særlig sårbare og mindre i stand til å gjøre vurderinger av mulige konsekvenser av andres behandling av deres personopplysninger.³⁴ Dette særlige vernet gjelder spesielt i situasjoner der deres personopplysninger samles inn i forbindelse med tjenester som er rettet mot barn.

Alarmtelefonens nettsider er direkte rettet mot barn, og det er grunn til å tro at de fleste som besøker siden er barn. I dette tilfellet har personopplysninger om at de har besøkt nettsidene blitt tilgjengeliggjort for Snap og Meta. Disse selskapene kunne sammenstille dataene med deres profiler på selskapenes plattformer, uten barnas kunnskap eller noen mulighet for dem

³⁴ Se personvernforordningens fortale, avsnitt 38.

til å hindre delingen. Det er ikke klart hva Snap eller Meta brukte personopplysningene til, og personvernerklæringene deres ga ikke klare rammer for hvordan de kunne brukes.

Overtredelsene har medført en betydelig risiko for at barn og unge i potensielt svært sårbare situasjoner blir identifisert av kommersielle aktører. Dette var direkte i strid med påstandene om anonymitet på Nettstedet.

Når det gjelder arten, omfanget og formålet med behandlingen, er det verdt å notere at det er snakk om behandling av personopplysninger for markedsføringsformål ved hjelp av kommersielle verktøy. Når denne typen sporingsverktøy tas i bruk, mister man i realiteten kontrollen på opplysningene så snart de overføres til tredjeparter som Snap og Meta. De kan sammenstille dem med andre personopplysninger og bruke dem til sine egne formål. Derfor må behandlingsansvarlige som tar i bruk kommersielle sporingsverktøy kartlegge og forstå hvordan verktøyet vil behandle personopplysninger, samt hvilke konsekvenser behandlingen kan få for de registrerte. I denne saken virker det som om kommunens tilgjengeliggjøring av personopplysningene er en utilsiktet konsekvens av bruken av pikslene på Nettstedet. Det er oppsiktsvekkende og skjerpene at et offentlig organ tar i bruk slike verktøy slik Alarmtelefonen har gjort her – uten å ha undersøkt og vurdert hvilke konsekvenser det har for brukernes personvern. Dette er et skjerpene moment.

Datatilsynet viser til at nettsidene hadde rundt 73 800 besøk i 2023, og at det var til sammen rundt 11 000 visninger av sidene «Barn 7-12 år» og «Ungdom 13-18 år». Dette står i Alarmtelefonens årsrapport for 2023. Rapporten viser også at de besøkende befinner seg rundt om i hele Norge. Det er skjerpene at det er et høyt antall registrerte som er berørt av behandlingen.

Datatilsynet har ikke informasjon om konkrete skade lidd av de registrerte. Dette kan ha sammenheng med at kommunen har delt barnas personopplysninger med lite transparente kommersielle aktører.

Vi finner momentene under artikkel 83 nr. 2 bokstav a) som skjerpene.

b) Hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Uaktsomhet er definert slik i straffeloven § 23:

«Den som handler i strid med kravet til forsvarlig opptreden på et område, og som ut fra sine personlige forutsetninger kan bebreides, er uaktsom. Uaktsomheten er grov dersom handlingen er svært klanderverdig og det er grunnlag for sterk bebreidelse.»

I henhold til kravet om forsvarlig opptreden må virksomheter og ansvarlige personer som opptrer på deres vegne, undersøke rettskravene som gjelder for deres felt og gjennomføre disse. Ellers kan virksomheten anses å ha handlet uaktsomt når det gjelder denne feilen.

I brevet 30. april 2025 erkjente kommunen at den ikke har gjort vurderinger om bruken av sporingsverktøyene:

«Sporingsverktøyene har ikke vært i bruk hos kommunen, det vil si at det ikke har vært bygget en målgruppe som får tilpasset reklame etter bruk av disse verktøyene. Vi har like fullt blitt klar over at disse har levert informasjon til Meta og Snap.

Kommunen har ikke i tilstrekkelig grad hatt forståelse for konsekvensene av sporingsverktøyene som var aktive på denne nettsiden. Kommunen har heller ikke tatt aktivt stilling til at disse verktøyene skulle brukes, eller til hvilket formål. Men har hatt tillitt til leverandørens forsikringer om at nettsidens brukere er anonyme. Kommunen har aldri hatt til hensikt at personopplysninger skulle deles med tredjeparter.»

Datatilsynet forstår at kommunen ikke hadde som hensikt å dele personopplysninger om besøkende til Nettstedet med tredjeparter eller å spore aktivitetene til enkeltpersoner som besøkte Nettstedet.

Den behandlingsansvarlige har et ansvar for å sørge for at man forstår konsekvensene av behandlingen. Som vi var inne på ovenfor, har barn krav på et særlig vern om deres personopplysninger. Derfor gjelder det et strengt krav til aktsomhet rundt lovligheten av behandlingen.

Både Snap og Meta er selskaper som har vært i medienes søkelys over flere år på grunn av hvordan de behandler personopplysninger. Sporing på nett og risikoene det medfører har også vært hyppig diskutert. At disse selskapene tilbød sporingsverktøy som kunne integreres på Nettstedet vederlagsfritt burde ha gitt særskilt grunn undersøke ekstra nøye hvordan de fungerte. Det fremgikk av både Snap og Metas personvernerklæringer at pikslene deres ble brukt til å samle inn personopplysninger fra nettsidene som de var integrert i.

Selv om kommunens leverandør forsikret om at sporingsverktøyene var anonyme, så var formålet med å bruke dem å spore trafikk fra sosiale medier til Nettstedet. Det er vanskelig å gjøre dersom opplysningene var anonyme, og dette var en påstand som burde blitt undersøkt nærmere.

Sett i lys av at Nettstedet er drevet av det offentlige for å hjelpe barn under en forutsetning av anonymitet, hadde kommunen en klar oppfordring til å sette seg inn i hvordan disse verktøyene fungerer og bare implementere verktøy som det var forsvarlig å bruke på denne typen nettsted. Her er det klart at kommunen burde gjort mer.

Datatilsynet mener at kommunen har handlet uaktsomt.

- c) *eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd*

Dette momentet kommer ikke til anvendelse i denne saken.

- d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32*

Dette momentet kommer ikke til anvendelse i denne saken.

- e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren*

Dette momentet kommer ikke til anvendelse i denne saken.

- f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den*

Kommunen har samarbeidet med Datatilsynet ved å gi oss svar på spørsmålene, men ikke ut over det som var påkrevd av dem.

Alarmtelefonen gjorde endringer i personvernerklæringen etter at Datatilsynet varslet at det gjennomførte tilsyn mot bruken av sporingsverktøy på Nettstedet 19. mars 2024. Personvernerklæringen ble endret til å inkludere informasjon om bruken av pikslene til Snap og Meta, men Alarmtelefonen stanset ikke bruken av dem. Etter Datatilsynets syn var ikke endringene tilstrekkelige til å oppfylle kravene som følger av personvernforordningen artikkel 12 og 13, og de stanset heller ikke den ulovlige behandlingen. Dette tillegges derfor ikke vekt i formildende retning.

Derimot er det grunn til å fremheve kommunens positive og tillitsvekkende opptreden etter at vedtak ble varslet.

Det er et tegn på godt samarbeid at kommunen på eget initiativ meldte inn brudd på personvernforordningen gjennom avviksmeldingen av 1. april 2025.

Videre fremgår det klart av kommunens brev 30. april 2025 at den tar saken på største alvor. I brevet forklarer kommunen at den stanset bruken av alle sporingsverktøy på Nettstedet som ikke er nødvendige for at nettsidene skal fungere. Dette gjelder også andre sporingsverktøy enn Meta Pixel og Snap Pixel. Kommunen har altså gått lenger enn det varslede pålegget om stans krevde.

Kommunen la også ut informasjon om hva som hadde skjedd på Nettstedet og på kommunens nettsider. Kommunen jobber videre med å lage en ny personvernerklæring på Nettstedet som tilpasser informasjonen til den aktuelle målgruppen.

I brevet står det også at ansvaret for å drive Nettstedet har blitt flyttet internt i kommunen:

«Etter varsel om vedtak, har kommunen endret forståelsen av rollen som behandlingsansvarlig for nettstedet. Nettstedet inngår nå i porteføljen til teamet som jobber med blant annet fagsystemer og personvern, i stedet for at dette administreres

lokalt hos Alarmtelefonen. Dette gjøres for å sikre at personell med personvernkompetanse gjør vurderingene som omhandler personvern i samarbeid med personell fra Alarmtelefonen, som på sin side står for det faglige innholdet.»

Datatilsynet vurderer dette som en positiv utvikling som kan bidra til å hindre lignende overtredelser i fremtiden.

Vi finner disse omstendighetene formildende.

g) kategoriene av personopplysninger som er berørt av overtredelsen

Personopplysningene som er samlet inn og delt er av en privat og beskyttelsesverdig karakter. De avslører barn som kontakter en tjeneste som er ment for personer som har det vanskelig, og som har veiledning knyttet til forskjellige sårbare livssituasjoner.

Vi finner dette momentet som skjerpende.

h) hvilken måte tilsynsmyndigheten fikk kunnskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen

Datatisynet oppdaget forholdet da vi gjennomførte tilsyn av eget tiltak.

Vi finner dette momentet som hverken skjerpende eller formildende.

i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes

Dette momentet kommer ikke til anvendelse i denne saken.

j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42

Dette momentet kommer ikke til anvendelse i denne saken.

k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen

Det fremgår av brevet 30. april 2025 at kommunen brukte sporingsverktøyene for å måle effekten av tiltak for å nå ut til Nettstedets målgruppe på sosiale medier. Dette gjorde den for å rapportere om effekten til Bufdir. Datatilsynet har ikke konstatert at Alarmtelefonen har hatt økonomiske fordeler, eller unngått direkte eller indirekte tap, som et resultat av overtredelsene. Dette momentet finner Datatilsynet verken skjerpende eller formildende.

Samlet vurdering

Alarmtelefonen for barn og unge er en offentlig tjeneste som henvender seg direkte til mindreårige i sårbare situasjoner. Sett i lys av tjenestens art, målgruppen til Nettstedet og innholdet i de personopplysningene som deles, anser vi overtredelsen som meget alvorlig. De som besøker Nettstedet har en berettiget forventning om vern om deres personopplysninger, særlig når Nettstedet sier at henvendelser til Alarmtelefonen er anonyme.

Det er positivt at kommunen tok saken på alvor ved sette i gang flere tiltak for å stanse overtredelsen etter at den mottok varselet om vedtak. Etter en samlet vurdering har Datatilsynet likevel kommet til at Kristiansand kommune, som behandlingsansvarlig for tjenesten Alarmtelefonen, må ilegges et overtredelsesgebyr.

7.2.4. Gebyrets størrelse

I forarbeidene til ny personopplysninglov (Prop. 56 LS (2017-2018 s. 141) uttaler departementet at:

«som utgangspunkt [skal] de samme reglene for overtredelsesgebyr gjelde for offentlige organer som for private, da dette er ordningen etter gjeldende personopplysningslov.»

De nevnte momentene i artikkel 83 er styrende for utmålingen av overtredelsesgebyret. Departementet legger til grunn at Datatilsynet kan utøve et betydelig skjønn med hensyn til størrelsen på gebyret. Det uttaler også at «[b]eløpsgrensene i forordningen artikkel 83 angir maksimalgrenser for utmåling av administrative gebyrer, mens det ikke er fastsatt noen minimumsgrenser.» Gebyret bør likevel settes så høyt at det får virkning også utover den konkrete enkeltsaken.

Datatilsynet har fastslått at delingen av personopplysninger i denne saken utgjør brudd på artiklene 6, 12 og 13 i personvernforordningen. Overtredelsene er alvorlige og berører mange personer.

Det legges betydelig vekt på at de berørte i denne saken i stor grad er barn og at personopplysningene er svært sensitive. Når opplysninger om besøk på Nettstedet har blitt tilgjengeliggjort for Snap og Meta, har de berørte mistet kontroll over opplysningene sine. Vi vet ikke hvordan opplysninger om deres besøk på Nettstedet kan bli brukt i fremtiden. Tilgjengeliggjøringen innebar derfor store personvernkonsekvenser for de berørte.

De som besøkte Nettstedet hadde en berettiget forventning om fortrolighet. I den sammenheng vektlegger vi også at det ble påstått at besøk på Nettstedet var anonymt, noe som ikke stemte.

Datatilsynet vektlegger videre at det er mye å bebreide kommunen for da den tok i bruk sporingsverktøyene på denne typen nettsted. I lys av den offentlige oppmerksomheten rundt

sporing på nett, at Nettstedet retter seg mot barn og Nettstedets sensitive tematikk, så burde ikke behandlingen ha funnet sted.

Datatilsynet vektlegger også allmennpreventive hensyn. Det er viktig at offentlige tjenester som ønsker å nå ut til befolkningen gjør dette på en måte som ivaretar befolkningens personvern. Spesielt offentlige organer som behandler opplysninger om sårbare personer må være bevisste om deres ansvar. Alle må kunne søke informasjon hos, og motta hjelp fra, offentlige organer uten frykt for personvernbrudd.

Ileggelsen av et overtredelsesgebyr skal være virkningsfullt, forholdsmessig og avskrekkende. Overtredelsene er alvorlige, og gebyret må derfor være av en viss størrelse for å være virkningsfullt.

Det er mange nettsider som bruker de samme sporingsverktøyene som Nettstedet har brukt. Derfor er det viktig å statuere et eksempel i denne saken, noe som tilsier at gebyret må settes høyt for å fungere som effektiv avskrekking for andre behandlingsansvarlige.

Samtidig har kommunen erkjent alvoret i saken, og den har satt i gang flere tiltak for stanse behandlingen og å hindre lignende hendelser i fremtiden, som forklart ovenfor. I avviksmeldingen 1. april 2025 skrev kommunen at den oppdaget flere forhold som ikke hadde direkte sammenheng med tilsynet som den nå jobber med å utbedre.

Kommunen har også opplyst om at den har gjennomgått andre nettsted som den driver som ikke er omfattet av dette tilsynet.

Dette bør vektlegges i en formildende retning.

Forholdsmessighetsvurderingen tar utgangspunkt i alvoret og karakteren av overtredelsen. Samtidig har vi lagt stor vekt på at det er snakk om en viktig tjeneste som er ment å hjelpe sårbare barn, som tilsier at gebyret heller ikke må settes for høyt. Vi har også lagt betydelig vekt på kommunens pressede økonomi i utmålingen. Videre har vi også særlig vektlagt kommunens tiltak for å rydde opp og hindre at lignende overtredelser skjer igjen.

Etter en totalvurdering har vi kommet til at kommunen ilegges et overtredelsesgebyr på **250 000 NOK**.

8. Anbefalinger til oppfølging

I brevet 30. april 2025 ber kommunen om veiledning om hvordan den kan innhente samtykke fra mindreårige.

Fra og med 1. januar 2025 gjelder det et krav om å innhente samtykke for å lagre eller å lese av informasjon i brukers enheter. Dette følger av ekomloven § 3-15 første avsnitt. Det presiseres i bestemmelsen at vilkårene for et gyldig samtykke er de samme som følger av personvernforordningen. Andre avsnitt i bestemmelsen slår samtidig fast at kravet om

samtykke ikke gjelder for lagring av eller tilgang til opplysninger i enheten som er «strengt nødvendig» for at nettsiden skal fungere.³⁵

Ifølge personopplysningsloven § 5, jf. artikkel 8 (1) i personvernforordningen, kan ikke barn under 13 år samtykke til behandlingen av deres personopplysninger i forbindelse med bruk av tjenester på internett, uten samtykke fra deres foresatte. Artikkel 8 (2) slår fast at dersom en behandlingsansvarlig baserer behandlingen på samtykke, så må vedkommende treffe rimelige tiltak for å kontrollere at samtykket er gitt av den foresatte.

Siden en viktig del av Nettstedets målgruppe er barn og unge som ikke ønsker å snakke om vanskelige tema med sine foresatte, så virker det vanskelig å lage en samtykkeløsning hvor foresatte samtykker på vegne av barn under 13 år. I tillegg vil en slik løsning kreve bruk av verktøy som skiller mellom barn over og under 13 år. Bruken av slike verktøy er et nytt behandlingsformål som vil kreve nye vurderinger fra kommunen.

I prinsippet er det ikke noen rettslige hindre mot at kommunen kan bruke sporingverktøy som krever samtykke etter ekomloven § 3-15, så lenge vilkårene om gyldig samtykke er oppfylt.³⁶ Samtidig virker det upraktisk å innhente samtykke for et nettsted som gir et lavterskel hjelpetilbud som Alarmtelefonen.

Sporingsteknologier som ikke krever lagring eller avlesing av opplysninger i brukerens enhet faller utenfor virkeområdet til ekomloven § 3-15. Bruken av slike teknologier, for eksempel til å skille mellom brukere for å måle trafikk på Nettstedet, krever derfor ikke samtykke etter denne bestemmelsen. Behandlingen av personopplysningene må likevel ha et behandlingsgrunnlag etter personvernforordningen artikkel 6, og den må følge de øvrige reglene i forordningen.

En slik behandling kan i prinsippet forankres i en interesseavveining etter artikkel 6 nr. 1 bokstav f). Kommunen må i så fall vurdere hvilke opplysninger som er nødvendige å samle inn for behandlingsformålet. Denne vurderingen må gjøres i lys av dataminimeringsprinsippet og lagringsbegrensningen i forordningens artikkel 5 nr. 1 bokstav c) og e). Kommunen må også vurdere om behandlingen er forenlig med de registrertes interesser og rettigheter. I den sammenheng må kommunen særlig ta hensyn til at de fleste besøkende til Nettstedet vil være barn som strever med ulike vanskelige situasjoner. Kommunen kan for eksempel vurdere om det finnes tiltak som reduserer mulige personvernkonsekvenser som aidentifisering av dataene eller pseudonymisering av personopplysninger. Det vil også være nødvendig å gi informasjon om behandlingen etter artikkel 13. Informasjonen må være lett tilgjengelig med et forståelig språk for målgruppen til Nettstedet.

I brevet 30. april 2025 skrev kommunen at den har fjernet alle sporingsteknologier fra Nettstedet som ikke var nødvendige for at den skulle fungere. Likevel er det et «cookie-

³⁵ Det er Nasjonal kommunikasjonsmyndighet (NKOM) som har ansvar for å vurdere om plasseringen er «strengt nødvendig» etter § 3-15 (2) bokstav b). Se forskrift 20. desember 2024 nr. 3413 om delegering av myndighet etter lov om elektronisk kommunikasjon (ekomloven), avsnitt 12, bokstav b).

³⁶ Datatilsynet har laget en veileder for å innhente gyldig samtykke ved bruk av informasjonskapsler og andre sporingsteknologier: [Bruk av informasjonskapsler og andre sporingsteknologier | Datatilsynet](#).

banner» på forsiden som ber besøkende om å samtykke til behandling av personopplysninger til de følgende formålene: «egenskaper», «statistikk» og «markedsføring». Siden Nettstedet tilsynelatende ikke bruker sporingsverktøy som krever samtykke etter ekomloven eller behandler personopplysninger på grunnlag av samtykke, så blir informasjonen i «cookie-banneret» upresis. Datatilsynet anbefaler kommunen å fjerne det inntil den har avklart hvilke formål personopplysningene skal behandles for og hva behandlingsgrunnlaget er.

I avviksmeldingen 1. april 2025 skrev kommunen at den hadde oppdaget mangler ved behandlingen i lys av artikkel 24 og 30 i personvernforordningen. Vi oppfatter kommunen slik at den har satt i gang med tiltak for å utbedre dette, og Datatilsynet kommer ikke til å gjøre nærmere undersøkelser i disse forholdene i forbindelse med dette tilsynet. Vi viser ellers til veiledning på våre nettsider, herunder i kategorien «Virksomhetenes plikter», som kan inneholde relevant informasjon for kommunen.

9. Klagerett

Kristiansand kommune kan klage på vedtaket om overtredelsesgebyr. En eventuell klage må sendes til Datatilsynet **innen tre uker etter at dette brevet er mottatt**, jf. forvaltningsloven §§ 28 og 29. Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernemnda for klagebehandling.

Oppfyllelsesfristen for et vedtak om overtredelsesgebyr er fire uker fra vedtaket er endelig.

10. Innsyn og offentlighet

Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige, jf. offentlighetsloven § 3. Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentet fra offentlig innsyn ber vi dere om å begrunne dette.

Hvis dere har spørsmål om saken, kan dere ta kontakt på e-post, postkasse@datatilsynet.no.

Vennlig hilsen

Tobias Judin
seksjonssjef

Svein Gjørtz
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer