

Når er opplysninger anonyme? EDPB foreslår nye retningslinjer om anonymisering

Av Håvard Sveier Ottemo og Line Helen Haukalid

I en ny veileder klargjør EDPB at anonymitet ikke bare avhenger av datasettet, men også av hvem som har tilgang til opplysningene, hvilke identifikasjonsmidler som er tilgjengelige, og hvor sannsynlig det er at disse vil bli brukt. Veilederen presiserer også hvilke GDPR-forpliktelser som gjelder under anonymiseringsprosessen, og hvordan virksomheter bør vurdere, teste og dokumentere at opplysningene faktisk er anonyme.

Den 7. juli 2026 sendte EDPB *Guidelines 02/2026 on Anonymisation* for offentlig høring. Veilederen oppdaterer Artikkel 29-gruppens uttalelse 05/2014 om anonymisering i lys av nyere rettspraksis og den rettslige og teknologiske utviklingen. Den bygger særlig på EU-domstolens dom i sak C-413/23 P, EDPS mot SRB, og innebærer en tydelig presisering og videreutvikling av EDPBs syn på anonymitet. Høringsfristen er 30. oktober 2026.

EDPS mot SRB gjaldt personvernreglene for EUs institusjoner, men EDPB anvender dommens *resonnement* i sin analyse av anonymitet etter GDPR. I saken skulle opplysningsplikten vurderes på innsamlingstidspunktet og fra den behandlingsansvarliges perspektiv. Fordi opplysningene da var personopplysninger for den behandlingsansvarlige, måtte de registrerte informeres om mottakerne. Dette gjaldt selv om opplysningene senere kunne være anonyme for mottakeren. Et sentralt poeng var altså at anonymitet må vurderes fra det relevante aktørperspektivet.



Håvard Sveier Ottemo

Anonymitet må vurderes fra riktig perspektiv

EDPB tar utgangspunkt i definisjonen av personopplysninger i GDPR artikkel 4 nr. 1 og stiller to spørsmål: (1) Er opplysningene «om» en fysisk person, og (2) er personen «identifisert eller identifiserbar»? Hvis svaret på ett av spørsmålene er nei, skal opplysningene anses som anonyme. Svaret kan variere mellom aktører: De samme opplysningene kan være personopplysninger for én aktør, men anonyme for en annen.

Ved bruk av databehandlere skal vurderingen foretas fra den behandlingsansvarliges perspektiv. Er opplysningene personopplysninger for den behandlingsansvarlige, må databehandleren behandle dem som personopplysninger selv om databehandleren ikke selv kan identifisere de registrerte. Den behandlingsansvarlige kan dermed ikke omgå GDPR ved å overlate behandlingen til en aktør med færre identifikasjonsmidler.



Line Helen Haukalid

Når er opplysninger «om» en identifiserbar person?

Opplysninger kan være «om» en person på grunn av sitt innhold, formål eller sin virkning. Tilknytningen trenger ikke være umiddelbart synlig, men kan avdekkes gjennom videre behandling. Også aggregerte opplysninger kan derfor være personopplysninger dersom de kan brukes til å utlede informasjon om enkeltpersoner.

Det neste spørsmålet er om personen er identifisert eller identifiserbar ved hjelp av midler som med rimelighet kan forventes brukt. Identifikasjon innebærer at personen kan skilles fra andre i en bestemt sammenheng på en måte som gjør det mulig å behandle vedkommende annerledes. Det er ikke nødvendig at én aktør alene råder over alle nødvendige opplysninger eller identifikasjonsmidler. Personen kan også være identifiserbar dersom opplysninger som flere aktører kontrollerer, med



Illustrasjon: Colorbox/ ChatGPT

rimelighet kan forventes kombinert. Ved vurderingen skal det tas hensyn til alle objektive faktorer som påvirker både tilgangen til identifikasjonsmidlene og sannsynligheten for at de faktisk vil bli brukt.

Manglende motivasjon for å identifisere personen er ikke i seg selv avgjørende. Et lovforbud kan tale for at et identifikasjonsmiddel ikke med rimelighet kan forventes brukt, med mindre det foreligger en konkret risiko for lovbrudd. Et kontraktsforbud har ikke samme vekt, men kan inngå i vurderingen.

GDPR gjelder frem til opplysningene er anonyme

At opplysningene er anonyme for mottakeren, fritar ikke avsenderen dersom denne fortsatt kan identifisere personene. Avsenderen må fortsatt behandle dem som personopplysninger og oppfylle sine forpliktelser etter GDPR.

Anonymiseringen må ha behandlingsgrunnlag etter artikkel 6 og eventuelt oppfylle et unntak etter

artikkel 9 nr. 2. Anonymisering kan dessuten være et moment i favør av den behandlingsansvarlige i en interesseavveining.

Den behandlingsansvarlige må også oppfylle åpenhetsforpliktelsene etter GDPR artikkel 5 nr. 1 bokstav a og artikkel 12–15 ved anonymiseringen. EDPB fremhever at de registrerte klart bør informeres om at personopplysningene vil bli behandlet for å fremstille anonyme opplysninger som deretter faller utenfor GDPRs virkeområde.

Anonymiseringsprosessen og testing av resultatet bør dokumenteres på en egnet måte, slik at den behandlingsansvarlige både kan påvise at anonymiseringsprosessen skjer i samsvar med GDPR og at anonymiseringen faktisk er effektiv. Dokumentasjonen bør oppbevares også etter at anonymiseringsprosessen er avsluttet.

To måter å vurdere anonymitet på

EDPB beskriver to tilnærminger til vurderingen av om anonymisering av personopplysninger har vært vellykket:

Den **kontekstuelle tilnærmingen** bygger på den rettslige analysen og tar hensyn til hvilke identifikasjonsmidler hver relevant aktør har eller kan få tilgang til og sannsynligheten for at midlene vil bli brukt.



Anonymiseringsprosessen og testing av resultatet bør dokumenteres på en egnet måte, slik at den behandlingsansvarlige både kan påvise at anonymiseringsprosessen skjer i samsvar med GDPR og at anonymiseringen faktisk er effektiv.

Den **forenklede tilnærmingen** vurderer muligheten for reidentifikasjon uten å skille mellom aktørenes ulike muligheter til å få tilgang

til datasettet, tilleggsopplysninger og andre nødvendige ressurser. Vurderingen tar dermed utgangspunkt i om opplysningene kan knyttes til enkeltpersoner når alle relevante identifikasjonsmidler tas i betraktning, ikke hva den enkelte aktøren med rimelighet kan forventes å gjøre. Dette er ikke en alternativ rettslig standard, men et frivillig og mer forsiktig analyseverktøy.

Tilnærmingene kan kombineres. Ved begge undersøkes tre forhold: om datasettet inneholder en unik kombinasjon av opplysninger om én person (No Record Isolation), om opplysningene med sikkerhet eller høy sannsynlighet kan kobles til opplysninger om samme person i et annet datasett (No Linkage), og om det kan utledes spesifikke og meningsfulle opplysninger om en identifisert eller identifiserbar person (No Inference).

Eksempelvis kan et datasett inneholde opplysninger om alder, yrke, bosted og bevegelsesmønster:

- En opplysningskombinasjon – 47 år, tannlege og bosatt i en bestemt kommune – er unik i datasettet og gjelder én enkeltperson (brudd på No Record Isolation).
- Opplysningene kan kobles til en navngitt tannlege i et offentlig register (brudd på No Linkage).

- Bevegelsesmønsteret viser regelmessige besøk på en kreftklinikk og kan gi grunnlag for å utlede at personen mottar kreftrelatert behandling (brudd på No Inference).

Dersom ett eller flere kriterier ikke er oppfylt, betyr det ikke automatisk at opplysningene er personopplysninger. Bruddets betydning må vurderes nærmere for å avgjøre om opplysningene likevel kan anses som anonyme. Ved brudd på No Inference er EDPB strengere: Dersom kriteriet ikke er oppfylt under den kontekstuelle tilnærmingen, bør opplysningene ikke anses som anonyme fra minst ett relevant perspektiv.

EDPB går i veilederen særlig detaljert gjennom begge tilnærmingene og kriteriene, og gjennomgangen bør leses i sin helhet.

Hva betyr veilederen i praksis?

Veilederen innebærer neppe nye plikter, men tydeliggjør hva virksomheter må vurdere og dokumentere ved anonymisering.

For det første må virksomheten vurdere anonymitet i den konkrete sammenhengen. Det er ikke tilstrekkelig å undersøke datasettet isolert. Virksomheten bør også kartlegge hvem som kan få tilgang til opplysningene, hvilke tilleggsopplysninger

de har eller kan få tilgang til, og hvilke metoder de med rimelighet kan forventes å bruke for å identifisere enkeltpersoner.

For det andre må avsenderens og mottakerens perspektiv vurderes separat. Et datasett kan være anonymt for mottakeren, men fortsatt inneholde personopplysninger for avsenderen. Avsenderen må da fortsatt oppfylle sine GDPR-forpliktelser ved anonymiseringen og utleveringen.

For det tredje bør vurderingen dokumenteres og oppdateres dersom teknologien, tilgangen til tilleggsopplysninger eller andre relevante forhold endrer seg. Et datasett som er anonymt i dag, kan senere måtte anses som personopplysninger dersom reidentifikasjon blir tilstrekkelig sannsynlig.

Veilederen er fortsatt på høring, men viser hvordan EDPB tolker dommen i *EDPS mot SRB*, og gir virksomheter mer konkrete holdpunkter for anonymitetsvurderingen.

Håvard Sveier Ottemo, advokatfullmektig, Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immateriell rett.

Line Helen Haukalid, Managing Associate, Advokatfirmaet Wiersholm.