Høringssvar til det Europæiske Databeskyttelsesråd (EDPB) vedr. *'Guidelines 02/2026 on Anonymisation'*

Indledning og generelle bemærkninger

Indledning

Aarhus Universitet (herefter 'universitetet', 'vi', 'vores') takker for muligheden for at afgive høringssvar til EDPB's kommende vejledning om anonymisering *'Guidelines 02/2016 on Anonymisation'* (herefter 'Vejledningen'). Vejledningen er af stor betydning for og udgør et væsentligt bidrag til forståelsen af anonymisering i en databeskyttelsesretlig kontekst, herunder i relation til behandling af personoplysninger til forskningsformål.

Universitetet finder det positivt, at Vejledningen inddrager og forsøger at operationalisere den seneste retspraksis samt adresserer væsentlige problematikker, som kunstig intelligens, deling af data og reidentifikationsteknikker.

Imidlertid finder vi samtidig anledning til at fremhæve en række problemstillinger, som er særlige relevante i en forskningskontekst, hvor foranstaltninger som pseudonymisering og anonymisering er af afgørende karakter til beskyttelse af den registrerede i forbindelse med udførslen af behandlingsaktiviteter i forskningsprocessen, f.eks. i forbindelse med forskningssamarbejder og publicering

Henvisninger til præambelbetragtninger og artikler i det følgende uden nærmere præcisering sker til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (herefter "GDPR").

Høringssvaret er struktureret efter Vejledningens struktur og kronologi.

Generelle bemærkninger om samspillet mellem EDPB's vejledninger

EDPB vedtog retningslinjer for pseudonymisering i 2025 *'Guidelines 01/2025 on Pseudonymisation'*. Fælles for den vejledning og Vejledningen er, at information kan være personoplysninger for nogen (pseudonym), mens det er gjort anonymt for andre. Det er derfor i vid udstrækning de samme teknikker, som anvendes i pseudonymiserings- og anonymiseringsprocesser.

Forskningsdatakontoret
Aarhus Universitet
Inge Lehmanns Gade 10
8000 Aarhus C

Det er vigtigt, at Vejledningen og *'Guidelines 01/2025 on Pseudonymisation'* bringes i overensstemmelse, bl.a. i lyset af EU-Domstolens retspraksis.

Det bør derudover overvejes, om det kunne være mere hensigtsmæssigt at behandle det i én samlet vejledning eller som et klarere integreret rammeværk, hvorved det bliver tydeligere, at der er tale om et kontinuum.

Aarhus Universitet anbefaler desuden, at EDPB overvejer, om den endelige version af Vejledningen giver anledning til ændringer i *'Guidelines 1/2026 on processing of personal data for scientific research purposes (herefter 'Guideline 01/2026)'*. Vi finder det hensigtsmæssigt, at det i Guideline 01/2026 præciseres, at vurderingen af anonymisering er relativ. Det kunne f.eks. tydeliggøres ved at indsætte følgende passus i Guidelines 01/2026, punkt. 162:" Whether *data should be considered anonymised should be assessed from the perspective of the relevant recipient in accordance with Guidelines 02/2026 on Anonymisation*."

Bemærkninger til Vejledningens afsnit 1: 'Introduction'

GDPR omtales i litteraturen og af praktikere under tiden som "*The law of everything*". Den Europæiske Unions Domstol (herefter 'EU-domstolen') har i sin praksis fortolket personoplysningsbegrebet bredt med henvisning til EU-lovgivers hensigt ved formuleringen 'enhver information' i definitionen af personoplysningsbegrebet (artikel 4, nr. 1).

Ved en læsning af præambelbetragtning 26 er det vores klare overbevisning, at lovgiver ikke har haft til hensigt at udvide definitionen af personoplysningsbegrebet til at omfatte enhver oplysning, som relaterer sig til en fysisk person, hvis identifikation af en fysisk person *ikke er* eller *ikke længere er* mulig. Dette støttes bl.a. af EU-domstolens praksis i C-413/23 P (herefter 'EDPS vs SRB') præmis 80:

> *"As the Advocate General observed, in essence, in point 51 of his Opinion, those clarifications relating to the assessment of whether or not the data subject is identifiable would be deprived of any practical effect if pseudonymised data were to be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725.*[1]*"*

Det er derfor væsentligt, at der ikke i Vejledningen indfortolkes krav, der går videre end, hvad der er følger af præambelbetragtning 26, herunder at vurderingen af, hvad der er rimelige midler, ikke udstrækkes unødigt.

[1] Det bemærkes, at EU-domstolen har fastslået, at personoplysningsbegrebet skal fortolkes ensartet og sammenhængende på tværs af EU-retten. Det er derfor i denne kontekst underordnet, at dommen behandler en behandling, som er underlagt forordning 2018/1725.

Bemærkninger til Vejledningens afsnit 2 "Legal analysis"
Ad Vejledningens punkt 2.2. " Identifying the applicable perspective(s)"

Momenter i vurderingen af det relevante perspektiv bør uddybes
Universitetet finder det positivt, at Vejledningen behandler betydningen af den relative tilgang til identificerbarhed som følger af GDPR's præambelbetragtning 26.

EU-domstolen har i dommen EDPS vs SRB lagt vægt på, at der skal fortages en vurdering af det relevante perspektiv i forbindelse med reidentifikationsvurderingen. Da vurderingen af det relevante perspektiv er afgørende for, om oplysninger behandles som personoplysninger eller som anonyme oplysninger, er det af væsentlig betydning for dataansvarlige og registrerede, at vurderingen er korrekt. På den baggrund bør Vejledningen udbygges med flere eksempler som belyser betydningen af de momenter, som EU-domstolen inddragede i sagen C-413/23 P ved vurderingen af det eller de relevante perspektiver, herunder bl.a.:

- Retsforholdet
- Beskyttelseshensyn
- Tidspunktet for vurderingen

Ændringer i de databeskyttelsesretlige rollers betydning
I Vejledningens punkt 15 anføres det, at det relevante perspektiv i en databehandlerkonstruktion vil være *den dataansvarliges perspektiv. Dette* med henvisning til en teleologisk anvendelse af GDPR. Hvis denne fortolkning lægges til grund, bør EDPB præcisere, at dette ikke kan udstrækkes længere end til ophør af behandlingen af personoplysninger, som databehandleren udfører på vegne af den dataansvarlige. Hvis der efterfølgende sker en videregivelse til et selvstændigt formål til den aktør, der tidligere agerede databehandler, må vurderingen af det relevante perspektiv skulle foretages i den nye kontekst. Dette kan illustreres ved et eksempel:

> *Dataansvarlig A indgår aftale med Databehandler B om en række dataanalyser på baggrund af et aggregeret datasæt. Dataansvarlig A er i besiddelse af det originale datasæt og kender de metoder, der er anvendt ved aggregeringen. Datasættet udgør derfor personoplysninger for Dataansvarlig A.*
>
> *Databehandler B er ikke i besiddelse af oplysninger, som gør Databehandler B i stand til at identificere fysiske personer i datasættet. Databehandler B sletter datasættet efter aflevering af dataanalyserne til Dataansvarlig A.*
>
> *I forbindelse med udvikling i virksomheden ønsker B at bruge datasættet fra A til eget formål. A vurderer, at B ikke er i stand til at identificere fysiske personer i datasættet. A videregiver datasættet til B til B's eget formål.*

Datasættet udgør ikke personoplysninger for B, når B ikke længere handler på A's vegne, og det må derfor i denne kontekst være B's perspektiv, der er relevant for reidentifikationsvurderingen.

Identifikation af det eller de relevante perspektiver i forskningskontekster
Anvendelsen af pseudonymisering og anonymisering er særligt relevant i forskningssammenhænge, idet mange videnskabelige forskningsområder beskæftiger sig med sammenhænge og mønstre. I sådanne tilfælde er identifikation af det enkelte individ ikke hverken ønskelig eller relevant for forskningen, men data vil ofte indeholde personhenførbare oplysninger på indsamlingstidspunktet. Endvidere består forskningssamarbejder, forskningsmiljøer og infrastrukturer af mange aktører, som kan have forskellige retlige og tekniske muligheder.

Universitetet anbefaler derfor, at EDPB supplerer Vejledningen med flere eksempler fra forskningsverdenen, herunder både kvantitative og kvalitative forskning, idet vurderingen her kompliceres af, at aktørerne vil have væsentligt forskellige muligheder for identifikation henholdsvis reidentifikation.

Ad Vejledningens punk 2.3 " relates to"
I Vejledningens punkt 17 fremhæves det, at visse typer af information kan relatere sig til en fysisk person, selvom det ikke synes umiddelbart, eller det vil indebære en yderligere behandling for at identificere 'relationen' mellem informationen og individet (i den forbindelse henvises der til aggregerede datasæt som eksempel). Universitetet er enige i, at det efter omstændighederne kan være muligt at udlede oplysninger om enkeltindivider i aggregerede data i visse tilfælde. Det er dog væsentligt, at det fremhæves, at der skal være tale om en reel sandsynlighed for reidentifikation for, at data ikke betragtes som gjort anonyme.

Ad Vejledningens punkt 2.4 "Whether the natural person is "identified or identifiable"
Det er universitetets bekymring, at Vejledningens beskrivelse i pkt. 20-21 kan lede til en for vidtrækkende kæde af enheder og tredjemænd, hvilket kan føre til at data i praksis aldrig kan anonymiseres. Det bør derfor understreges, at en hypotetisk mulighed for identifikation, herunder reidentifikation, ikke i sig selv udgør identifikation.

Ad Vejledningens punkt 2.4.2 "Means resonably likely to be used"
Universitetet anerkender, at det kan være nødvendigt at undersøge, hvad der udgør rimelige midler for andre enheder samt om adgang til reidentifikation eller midler til reidentifikation kan opnås igennem tredjeparter.

Det er imidlertid væsentligt, at vurderingen af, hvad der udgør rimelige midler, tager højde for, at det kan være vanskeligt at afdække hele 'kæden' af aktører, og at dette i sig selv kan medføre, at der ikke er tale om rimelige midler.

Forskning sker ofte i forskningssamarbejder, herunder samarbejder inden for EU/EØS og øvrige internationale samarbejder, i konsortier med mange aktører. Derfor vil det også her være hensigtsmæssigt med en række eksempler, som belyser ovenstående i en forskningskontekst, herunder med blik for forskelle på kvantitativ og kvalitativ forskning.

EDPB opfordres til at præcisere, hvilke krav der stilles til den dataansvarliges vurdering af tredjemands adgang til identifikationsmidler. Det fremgår ikke klart, hvor langt den dataansvarlige forventes at undersøge modtagers faktiske og fremtidige muligheder for (re)-identifikation. EDPB opfordres endvidere til, gennem eksempler, at illustrere, hvornår hjælpemidler ikke bør anses for rimelige, fordi det vil indebære en uforholdsmæssig indsats med hensyn til tid, omkostninger og ressourcer.
Endeligt ønskes det præciseret, hvilke krav der stilles til dokumentation af vurdering af tredjemands brug af identifikationsmidler, herunder hvornår dokumentationen anses for tilstrækkelig.

Fremtidig teknologi som en objektiv faktor

I Vejledningens punkt 29 e henviser EDPB til fremtidige teknologier som med rimelighed kan forudses. I den forbindelse opfordres EDPB til også her at inddrage betydningen af udviklingen på området for kunstig intelligens med henblik på at belyse, hvilke implikationer dette måtte have, herunder i hvilken grad dataansvarlige forventes at kunne forudse udviklingen.

Vurdering af relevante enheder

I Vejledningens punkt 30 behandles spørgsmålet om, hvilke enheder der bør indgå i vurderingen af, hvem der kan besidde rimelige midler. I Vejledningen fremhæver EDPB bl.a. medarbejdere, der handler i strid med instrukser, efterretningstjenester, uetiske virksomheder, cyberkriminelle o.lign.

Universitetet anerkender, at der kan være tilfælde, hvor det kan være relevant at overveje sådanne enheders mulighed for reidentifikation. Det er samtidig universitetets opfattelse, at også denne vurdering må bero på en vurdering af sandsynlighed, herunder sandsynligheden for at den pågældende enhed med rimelighed kan tænkes at ville søge at tilvejebringe de nødvendige supplerende informationer med henblik på at identificere individer.

Her bringes General Advokatens udtalelse i C-582/14 ('Breyer') i erindring. Det fremgår af generaladvokatens forslag til afgørelse i 'Breyer'-sagen, punkt 65:

> *"Den maksimalistiske fortolkning ville i praksis føre til, at alle former for information ville blive klassificeret som personoplysninger, uanset hvor lidet brugbar den måtte være i forbindelse med identificeringen af en bruger. Det kan aldrig med 100% sikkerhed fastslås, at der ikke er en tredjemand, der er i besiddelse af yderligere oplysninger, der kan kombineres med denne viden, og som dermed kan anvendes til at afsløre identiteten på en person."*

Af punkt 68 fremgår det yderligere:

> *"Ligesom 26. betragtning ikke henviser til alle mulige hjælpemidler, der kan tænkes bragt i anvendelse (...), skal det også forstås således, at lovgiver henviser til "tredjemænd", som den registeransvarlige, der søger at indhente yderligere oplysninger med henblik på identificering, ligeledes med rimelighed, kan henvende sig til." (vores understregning)*

EDPB opfordres til overveje om, eksemplifikationen i Vejledningens punkt 30 er hensigtsmæssigt udformet i lyset af, at også spørgsmålet om, hvad der udgør relevante enheder, bør foretages ud fra en rimelighedsvurdering.

På samme måde er det universitetets opfattelse, at *'motivated intruder-test'*, der i Vejledningens punkt 31 beskrives som "*lack of motivation*", kan bidrage til vurderingen af relevante enheder, dog uden at dette nødvendigvis kan være eneste afgørende moment.

Identifikation forbudt ved lov eller ved aftale

I Vejledningens punkt 32-33 behandles EU-domstolens bemærkninger i retspraksis om betydningen af lovlige midler ved vurderingen af, om en person anses for identificerbar. Ved læsning af den relevante retspraksis kan spørgsmålet om '*lovlige midler*', som behandles i Vejledningens punkter, imidlertid forstås på flere måder. EDPB opfordres derfor til at bidrage til yderligere klarhed over, hvordan "*prohibited by law*" skal fortolkes i denne sammenhæng, herunder hvordan et retligt forbud mod identifikation indgår, og samspillet med den generelle risikovurdering og de tekniske og organisatoriske foranstaltninger, der måtte være implementeret.

I punkt 34 i Vejledningen anerkender EDPB, at kontraktretlige forpligtelser kan have en betydning for vurderingen af rimelige midler til reidentifikation. EDPB opfordres til supplere Vejledningen med eksempler, som der illustrerer vægtningen af kontraktretlige forpligtelser/garantier fra modtageren om ikke at forsøge at foretage reidentifikation i den samlede reidentifikationsvurdering set i forhold til øvrige tekniske og organisatoriske foranstaltninger.

I den forbindelse ville et eksempel om såkaldte 'sikre forskningsmiljøer' (etablerede lukkede datamiljøer med eller uden lovgivningsmæssige begrænsninger for brug af data, datas karakter og uddatakontrol) være værdifuldt. I sådanne miljøer kombineres

tekniske, kontraktuelle og organisatoriske foranstaltninger ofte med det formål at begrænse adgang til data, herunder gennem eksplicitte forbud mod reidentifikation.

Sandsynlighed for reidentifikation stiger over tid
I Vejledningens punkt 35 fremhæver EDPB, at sandsynligheden for reidentifikation stiger over tid. Aarhus Universitet har under Danske Universiteters GDPR-arbejdsgruppe tidligere rejst spørgsmål vedrørende de praktiske implikationer af tidsmæssige aspekter i et høringssvar til det danske datatilsyn.

I den forbindelse opfordrede arbejdsgruppen Datatilsynet til at forholde sig til omfanget og udstrækningen af en given vurdering af den teknologiske fremdrift og udvikling, som kan påvirke mulighederne for reidentifikation.

Eftersom vurderingen af oplysningernes karakter baserer sig på rimelighedsvurderinger og sandsynligheden for reidentifikation, vil den dataansvarlige kunne nå frem til, at oplysningerne er effektivt anonymiseret for modtagere på tidspunktet. Hvilken konsekvens vil det have, hvis reidentifikation viser sig mulig om ti år, men det ikke var muligt på tidspunktet for anonymiseringen at forudse?

Spørgsmålet kan illustreres gennem et eksempel:

> *"Dataansvarlig 1 anonymiserer et datasæt med henblik på at dele det med en bestemt modtager. Dataansvarlig 1 er i besiddelse af, to nøgler, der skal bruges for at gennemføre en reidentifikation. Der er ikke nogen lovlige muligheder for Dataansvarlig 1 til at dele nøglerne.*
>
> *Det er på tidspunktet for anonymiseringen vurderet, at det heller ikke vil være praktisk muligt at foretage en reidentifikation i lyset af den tilgængelige teknologi på behandlingstidspunktet og forventningerne til den teknologiske udvikling. Dataansvarlig 1 transmitterer derfor det anonyme datasæt Y til modtageren.*
>
> *Ti år senere beslutter den danske regering at indføre en ny lov grundet en verdensomspændende krise. Med loven kan Dataansvarlig 1 nu lovligt udlevere de to nøgler, som er forudsætningen for reidentifikation.*

Betydningen af den tidsmæssige udstrækning i eksemplet rejser afledte spørgsmål som:

- Har lovændringen den konsekvens, at oplysningerne, der nu ikke længere kan anses for anonyme, må anses for at have været personoplysninger i hele perioden eller må oplysningerne først anses for igen at være personoplysninger på det tidspunkt, hvor det bliver faktisk muligt at få adgang til oplysningerne, der skal muliggøre reidentifikation (lovændringen)?

- Hvis ovenstående spørgsmål besvares således, at oplysningerne må anses for effektivt anonymiseret i den periode, hvor det hverken er lovligt eller praktisk gennemførligt at foretage en reidentifikation, hvilke forpligtelser påhviler da den dataansvarlige, herunder i forhold til ansvarlighedsprincippet?
- Hvis spørgsmålet straks ovenfor besvares således, at oplysningerne må anses for effektivt anonymiseret i den periode, hvor det hverken er lovligt eller praktisk gennemførligt at foretage en reidentifikation, hvilke forpligtelser påhviler modtageren i forhold til at sikre, at oplysningerne fortsat er anonyme

EDPB opfordres til at forholde sig til eksemplet og de afledte spørgsmål og udbygge vejledningen om implikationerne af ændringer i oplysningers karakter som følge af det tidsmæssige aspekt. Desuden vil det styrke Vejledningen, hvis EDPB inddrager andre omstændigheder, som ikke har en objektiv karakter, f.eks. adgangen til nye tekniske muligheder eller ændrede forhold hos modtageren, som den oprindelige afgiver ikke bliver bekendt med.

EDPB bør i den forbindelse have for øje, at en løbende forpligtelse til at revurdere oplysningers karakter medfører en meget stor byrde for de dataansvarlige. For forskningsinstitutioner vil det forudsætte en stillingtagen til en udvikling i teknologi og datamængder/datakvalitet, som kan være svær at forudse, særligt også i forhold til datasæt, der kan være placeret i et repositorium (open science) i anonymiseret form på et tidspunkt, der ligger langt tilbage i tid.

Ad Vejledningens punkt 2.5.2 "GDPR compliance and the anonymisation process"
Behandlingsgrundlag
I Vejledningens punkt 38 behandler EDPB den dataansvarliges pligt til at have et lovligt behandlingsgrundlag for den behandlingsaktivitet, som anonymiseringsprocessen udgør. Vi anerkender, at alle behandlingsaktiviteter skal være hjemlet. Det er dog væsentligt, at det understreges endnu tydeligere, at der som alt overvejende hovedregel vil være hjemmel til anonymisering i det eksisterende behandlingsgrundlag, og at der således i udgangspunktet ikke kræves et særskilt grundlag for anonymiseringen.

Det er ligeledes væsentligt, at det fremgår tydeligt, at de øvrige databeskyttelsesretlige forpligtelser ophører på tidspunktet for videregivelsen af oplysningerne, der på dette tidspunkt er vurderet anonyme for modtageren.

Dokumentationskrav
Vi anerkender, at der ud fra ansvarlighedsprincippet i artikel 5, stk. 2 skal ske dokumentation af væsentlige forhold omkring anonymiseringsprocessen. Vi finder dog anledning til at kommentere på Vejledningens punkt 41, da det er vigtigt, at dokumentationsbyrden ikke gøres unødig byrdefuld, ligesom det er væsentligt, at dokumentationen i sig selv ikke kan bruges som værktøj til at identificere individer.

Vi opfordrer til, at EDPB inddrager disse perspektiver.

Implikationerne af hændelser
I Vejledningens punkt 42 fremgår det, at sikkerhedshændelser kan medføre, at oplysninger vil kunne betragtes som personoplysninger, idet der efter hændelsen med rimelige midler vil kunne ske identifikation. EDPB bedes uddybe implikationerne i et sådant tilfælde, herunder gerne gennem et eksempel.

Bemærkninger til Vejledningens afsnit 3 "The technical Analysis of anonymisation
Ad afsnit 3.4.2 'No linkage' og afsnit 3.4.3 'No inference'
I afsnittet behandles rammerne for, hvornår kriteriet 'No linkage' er opfyldt. I den forbindelse anfører EDPB i punkt 60, at

> "*The No Linkage criterion is met if the data does not contain an individual's record which could be linked to another record which (a) also relates (with certainty or high likelihood) to that same individual, and (b) comes from a different dataset.*"

Formuleringer som "high likelihood" (høj sandsynlighed for at relatere sig til) giver anledning til at anmode EDPB om yderligere præcisering af, hvilken betydning kvalificerede "gæt" har i anonymiseringsvurderingen.

Vejledningen baserer anonymiseringsvurderingen på begreber som "high likelihood", "reasonably likely" og "realistic means", som alle forudsætter kvalificerede skøn over fremtidige identifikationsmuligheder.

Det forekommer derfor uklart, hvilke konsekvenser det vil have for en dataansvarlig, der har foretaget en grundig, saglig og veldokumenteret analyse af oplysningerne, der på vurderingstidspunktet med rimelighed kan føre til den konklusion, at et datasæt er anonymt, hvis det viser sig mulig at gætte identiteten.

Denne afklaring ses også at være relevant i relation til inferenskriteriet.

Afsluttende bemærkninger
Sammenfattende ser Aarhus Universitet positivt på bestræbelserne om at skabe mere klarhed over, hvad der udgør anonyme oplysninger.

Samtidig er det afgørende, at fortolkningen af GDPR sker i lyset af den teknologiske om samfundsmæssige udvikling. Vejledningen spiller derfor en væsentlig rolle i at understøtte en praktisk, risikobaseret og operationel anvendelse af reglerne, der på den

ene side sikrer beskyttelse af de registrerede, men som samtidig skaber mulighed for anvendelse af data til samfundsvigtige formål.

Aarhus Universitet står gerne til rådighed med viden og erfaringer fra forskningssektoren, og vi opfordrer til, at forskningsinstitutioners behov og perspektiver inddrages aktivt, hvor høringsprocessen viser sig at rejse spørgsmål.