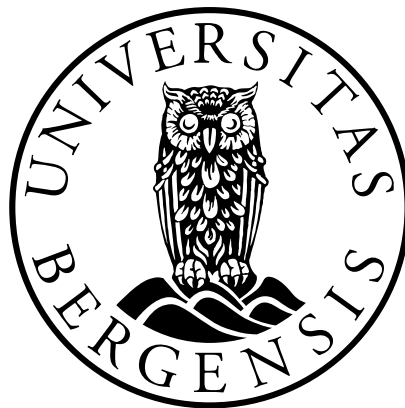


Et sterkere vern av særlige kategorier personopplysninger?

En rettslig analyse av GDPR artikkel 9 (1)

Kandidatnummer: 6

Antall ord: 14 063



JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10.05.2023

Innholdsfortegnelse

1 INNLEDNING	4
1.1 TEMA OG PROBLEMSTILLING	4
1.2 AVGRENSNINGER	6
1.3 METODE OG RETTSKILDER	7
1.4 OPPGAVENS STRUKTUR	9
2 GDPR OG PERSONOPPLYSNINGER	10
2.1 GDPR GENERELT	10
2.2 ALMINNELIGE PERSONOPPLYSNINGER	12
2.3 HVA ER BEHANDLING AV PERSONOPPLYSNINGER?	15
2.4 SÆRLIGE KATEGORIER PERSONOPPLYSNINGER GENERELT	16
2.5 SÆRLIGE KATEGORIER PERSONOPPLYSNINGER – EN KORT HISTORIKK	18
2.5.1 Europarådets personvernkonvensjon	19
2.5.2 Direktiv 95/46/EF	20
3 NÆRMERE OM GDPR ARTIKKEL 9 (1)	22
3.1 KATEGORIENE I GDPR ARTIKKEL 9 (1)	22
3.2 «PERSONAL DATA REVEALING» OG «PERSONAL DATA CONCERNING»: EN VID TOLKNING AV GDPR ART. 9 (1)?	24
3.3 FOTOGRAFIER OG VIDEO	26
3.4 BEHANDLINGSFORMÅL SOM BEGRENSNING AV ART. 9 (1)	29
3.5 FORDELER OG ULEMPER VED BEHANDLINGSFORMÅL SOM BEGRENSNING	32
3.6 FORMÅLSTOLKNING OG KONTEKSTBASERT TILNÆRMING TIL ART.9 (1)	34
4 SAK C-184/20: KAN ET NAVN VÆRE EN ARTIKKEL 9-OPPLYSNING?	37
4.1 SAKENS BAKGRUNN OG EU-DOMSTOLENS KONKLUSJONER	37
4.2 ER PERSONOPPLYSNINGER SOM ER EGNET TIL Å INDIREKTE AVSLØRE SEKSUELL ORIENTERING OMFATTET AV BEHANDLINGSFORBUDET I GDPR ARTIKKEL 9(1)?	40
4.3 PROPORSJONALITETSTESTEN: KAN PERSONOPPLYSNINGER OM PRIVATE INTERESSER PUBLISERES PÅ INTERNETT?	43
4.3 KONSEKVENSER AV DOMMEN: EN DYNAMISK OG FLEKSIBEL TOLKNING AV GDPR ARTIKKEL 9 (1)	46
4.3.1 Skjerpet ansvar ved behandling som involverer publisering og offentliggjøring på internett	48
5. KONKLUSJON	51
6 LITTERATURLISTE	53
6.1 NORSKE LOVER OG FORARBEIDER	53
6.2 EU-RETTSAKTER OG AVTALER	53
6.3 RETTSPRAKSIS FRA EU-DOMSTOLEN OG GENERALADVOKATENS INNSTILLINGER	54
6.4 VEILEDERE, UTTALELSER OG RAPPORTER	55

6.5 JURIDISK LITTERATUR	56
6.5.1 Bøker	56
6.5.2 Artikler.....	57
6.6 ØVRIGE KILDER.....	58
6.6.1 Internasjonale traktater.....	58
6.6.2 Nettsider.....	58

1 Innledning

1.1 Tema og problemstilling

I takt med den teknologiske utviklingen øker presset på den enkeltes personvern. Enorme mengder personopplysninger registreres, samles inn, brukes og gjenbrukes i det uendelige.¹ Den utstrakte bruken av smarttelefoner gir oss døgnkontinuerlig tilgang til apper og internett. Samtidig fører dette til at vi legger igjen digitale spor hele tiden. Personopplysninger om hva man handler, hvilke TV-serier man ser på, hvor man bor eller hvilke steder man besøker i løpet av en dag, lagres og sammenstilles av globale aktører og teknologiselskaper som Meta og Amazon.² Det er en flodbølge av informasjon som behandles, og omfattende behandling av personopplysninger har blitt normalt i det datadrevne, digitale samfunnet vi lever i.

Som følge av dette har behovet for et sterkere personvern vokst, og EU innførte sin nye personvernforordning, General Data Protection Regulation³ (heretter GDPR eller personvernforordningen), som trådte i kraft i mai 2018.⁴ GDPR erstattet EUs personverndirektiv.⁵ Formålet med GDPR er å verne fysiske personer i forbindelse med behandling av personopplysningene deres, og å sørge for fri utveksling av personopplysninger mellom medlemslandene i EU. GDPR innebærer dessuten full harmonisering av regler om personvern innen EU/EØS.⁶ Utgangspunktet er dermed at det ikke er adgang til å fravike eller

1 NOU 2022:11 Ditt personvern – vårt felles ansvar s. 9

2 NOU 2022:11 Ditt personvern – vårt felles ansvar s. 46

3 Europaparlamentets- og Rådsforordning (EU) 2016/579 av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [GDPR].

4 Jf. GDPR artikkel 99 (2).

5 Europaparlamentets- og Rådsdirektiv 95/46/EF av 24.oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

6 Wessel-Aas og Ødegaard (2018) s. 25.

supplere reglene, men GDPR åpner for at det kan gis nasjonale regler i noen tilfeller.⁷ GDPR er et teknologinøytralt regelverk⁸ og det betyr at det kan anvendes på behandling av personopplysninger uansett teknologi. En utfordring er imidlertid at ordlydene er abstrakte og generelle nettopp for å sikre stor fleksibilitet og et bredt vern av fysiske personer, og at det derfor kan være krevende å klarlegge den nærmere rekkevidden av bestemmelsene i konkrete situasjoner.

Bedre teknologi i form av økt datakraft og avanserte maskinlæringssystemer skaper situasjoner som utfordrer anvendelsen av GDPR. Personopplysningene som samles inn om oss av store teknologiselskaper kan videreselges til tredjeparter og brukes til å skreddersy budskap, lage profiler av enkeltindivider, drive målrettet markedsføring og tilpasse tjenester.⁹ Noen databehandlinger innebærer bare at man lagrer eller flytter informasjon, men i mange sammenhenger samler aktører informasjon med formål om å utlede nye opplysninger om oss. Gjennom analyser av bevegelsesmønster og lokasjonsdata, kan det for eksempel utledes hvor man bor og jobber, eller om man har en religiøs tilhørighet.¹⁰ Det betyr at opplysninger som i utgangspunktet verken er veldig sensitive eller avslørende, potensielt kan brukes til å utlede svært privat informasjon om enkeltpersoner uten at de er klar over det. Det kan få alvorlige føler for enkeltpersoners rettigheter og friheter dersom opplysningene kommer på avveie eller misbrukes. Nylig avdekket for eksempel The Washington Post hvordan en gruppe konservative katolikker i Colorado hadde kjøpt appsporingsdata som identifiserte prester som brukte homofile datingapper for så å dele informasjonen med biskoper rundt i landet.¹¹

7 Schartum (2020) s. 40.

8 Schartum (2020) s. 29.

9 NOU 2022:11 s. 50.

10 NOU 2022:11 s. 50.

11 Michelle Boorstein og Heather Kelly, «Catholic group spent millions on app data that tracked gay priests», The Washington Post, 19.mars 2023, <https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/>, (lest 05.05.23).

Nettopp for å sikre at sensitive opplysninger nyter tilstrekkelig vern, opererer GDPR med et skille mellom alminnelige personopplysninger i artikkel 4 (1) og en særregulering for «særlige kategorier personopplysninger»¹² i artikkel 9 (1). I artikkel 9 (1) oppstilles en lukket liste av kategorier det i utgangspunktet er forbudt å behandle, slik som opplysninger om religiøs oppfatning og seksuell orientering. Ordlydene er imidlertid vagt angitt, og de mange mulighetene teknologien gir til å sammenstille opplysninger for å utlede ny informasjon representerer en utfordring for rekkevidden av art. 9 (1). Slik eksempelet overfor viser, er det i lys av nåtidens enorme informasjonsmengder, avanserte behandlingsmåter og ny teknologi, ofte lite som skal til for at det kan utledes særlige kategorier personopplysninger fra alminnelige personopplysninger.

Spørsmålet denne oppgaven skal forsøke å besvare er: Hvilke personopplysninger omfattes av GDPR artikkel 9 (1)? Hvilken rekkevidde har bestemmelsen? En sentral tese i oppgaven er at artikkel 9 (1) omfatter både særlige kategorier personopplysninger av direkte og indirekte karakter. Jeg vil spesielt se på de indirekte tilfellene der sensitiv informasjon kan utledes fra alminnelige personopplysninger, og drøfte hvordan den nærmere grensdragningen for når det skjer en behandling av artikkel 9-opplysninger er foretatt i rettskildene. Deretter spør jeg hvilke konsekvenser EU-domstolens nylige avsagte sak *C-184/20 OT v Vyriausioji tarnybinės etikos komisija*¹³ har for tolkningen av artikkel 9 (1) og vurderingen av når en behandling av personopplysninger faller innenfor bestemmelsen.

1.2 Avgrensninger

Opgaven vil undersøke innholdet av ordlyden i artikkel 9 (1) og det avgrenses dermed mot behandlingsgrunnlag for særlige kategorier personopplysninger etter GDPR artikkel 9 (2). Videre oppstår en rekke kompliserte spørsmål i tilknytning til de tre legaldefinerte

¹² Jeg bruker det norske uttrykket «særlige kategorier» fremfor det engelske uttrykket «special categories» i oppgaven for lesbarhetens skyld.

¹³ Dom av 1.august 2022 [GC], *OT v Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601.

kategoriene «genetic data», «biometric data» og «data concerning health»¹⁴ som er for omfattende å behandle i lys av oppgavens størrelse. Det vil imidlertid foretas en kort redegjørelse for biometriske opplysninger i relasjon til behandling av foto og video.

1.3 Metode og rettskilder

I denne oppgaven har jeg valgt å bruke EU-rettslig metode og rettskilder fra EU-retten ettersom jeg blant annet analyserer en avgjørelse fra EU-domstolen. Imidlertid er det viktig å presisere at EU-retten påvirker norsk rett fordi Norge er bundet av EØS-avtalen.¹⁵ Dermed er problemstillingene i oppgaven utvilsomt relevante også i en norsk kontekst.

I tråd med EU-rettslig metode vil jeg i oppgaven ta utgangspunkt i en naturlig språklig forståelse av ordlyden sammen med tolkningsmomenter som den aktuelle bestemmelsens kontekst og formål. For å sikre EU-rettens grunnforutsetning om en ensartet fortolkning i et EU med 24 offisielle språk, er nettopp kontekst og formål sentralt.¹⁶ Kontekstuell fortolkning innebærer at man tolker en bestemmelse ut fra sammenhengen den inngår i, og i lys av overordnede bestemmelser og EU-retten generelt.¹⁷ På den måten foretar man en dynamisk tolkning som skjer i relasjon til den teknologiske utviklingen. Videre innebærer formålsoverordnet fortolkning at bestemmelsene fortolkes slik at formålet med dem fremmes i størst mulig grad.

Opgavens primære rettskilde er den engelske språkversjonen av GDPR. Som resultat av at EU-domstolen undersøker språklige nyanser i sin tolkning av art. 9 (1) i avgjørelsen jeg drøfter i kapittel 4, har jeg valgt å forholde meg til den engelske språkversjonen av GDPR.

¹⁴ De tre kategoriene er en del av GDPR artikkel 9 (1) og er legaldefinert i henholdsvis GDPR artikkel 4 (13), 4 (14) og 4 (15).

¹⁵ Jf. § 1 og § 2 i Lov 27.november 1992 om nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven eller EØSL).

¹⁶ Fredriksen og Mathisen (2018) s. 296.

¹⁷ Fredriksen og Mathisen (2018) s. 299.

Jeg vil supplere med norske oversettelser underveis der det er hensiktsmessig. En metodisk utfordring i oppgaven er at GDPR er et ungt regelverk og at tilfanget av autoritative rettskilder derfor er begrenset. GDPR inneholder mange generelle og vage ordlyder som hittil i liten grad er blitt avklart i rettskildene, og derfor vil personvernforordningens fortale være et viktig verktøy for å presisere og gi begrunnelser for bestemmelsene til tross for at den ikke er juridisk bindende.¹⁸

Videre vil jeg bruke uttalelser og retningslinjer fra EUs tidligere rådgivende organ i personvernspørsmål, Article 29 Working Party (heretter «Artikkel 29-gruppen») i oppgaven. Anbefalingene er ikke juridisk bindende, men er likevel sentrale for å klarlegge innholdet i GDPR og gir dessuten en pekepinn på hvilke instruksjoner datatilsynsmyndighetene i medlemslandene har fått. Jeg vil også benytte uttalelser fra European Data Protection Board (heretter «Personvernrådet»), som er opprettet i medhold av GDPR og erstatter Artikkel 29-gruppen. Personvernrådet har utgitt sparsomt med egne retningslinjer, men har gitt tilslutning til flere av Artikkel 29-gruppens veiledere.¹⁹ Retningslinjene har begrenset rettskildemessig vekt, men bidrar likevel til å klargjøre innholdet i artikkel 9 (1) på måter jeg mener er produktive for drøftelsene i oppgaven. Samtidig er det problematisk at retningslinjene er svært detaljerte og inneholder utfyllende regler og eksempler, og man kan stille spørsmål ved overføringsverdien til andre tilfeller.²⁰

EU-domstolens avgjørelser er rettskilder som klart er autoritative og har betydning for tolkningen av GDPR.²¹ Hittil er det én avgjørelse i sak C-184/20 fra EU-domstolen som vurderer rekkevidden av artikkel 9 (1) inngående og følgelig vil avgjørelsen være en viktig

18 Schartum (2020) s. 23.

19 En oversikt over veiledere Personvernrådet har gitt sin tilslutning til finnes her: https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en

20 Schartum (2020) s. 25.

21 Schartum (2020) s. 24.

rettskilde i oppgaven. Samtidig er mange av bestemmelsene fra personverndirektivet²² direkte videreført i GDPR, og rettspraksis om direktivet fra EU-domstolen er fremdeles viktig og vil brukes for å klarlegge definisjoner i GDPR. Jeg vil også bruke generaladvokatens innstilling som en kilde til forståelse av EU-domstolens rettspraksis i sak C-184/20 fordi generaladvokatens argumentasjon gir nyttig bakgrunnsinformasjon om argumentene som har vunnet frem. Sist, men ikke minst vil argumentasjon og synspunkter fra juridisk litteratur i lys av det spinkle rettskildebildet brukes i drøftelsen av tolkningsspørsmål knyttet til artikkel 9 (1).

1.4 Oppgavens struktur

Videre i oppgavens kapittel to vil jeg redegjøre for GDPR og personopplysninger, behandling og skillet mellom alminnelige og særlige kategorier personopplysninger. Jeg vil gi en introduksjon til særlige kategorier personopplysninger generelt, samt en kort historikk bak tilblivelsen, og en redegjørelse for sentrale hensyn bak artikkel 9 (1) og GDPR som risikobasert regelverk. I kapittel tre vil jeg foreta en analyse av den nærmere rekkevidden av artikkel 9 (1). Jeg vil se på særlige kategorier personopplysninger av indirekte karakter og drøfte hvordan personopplysninger i form av fotografier og video skaper vanskelige avgrensningsspørsmål. Deretter vil jeg drøfte ulike innfallsvinkler knyttet til spørsmålet om hvordan artikkel 9 (1) kan avgrenses. Jeg vil spesielt se på hvordan behandlingsformål er brukt som avgrensningskriterium i retningslinjer fra Personvernrådet. I kapittel fire vil jeg foreta en analyse av EU-domstolens avgjørelse C-184/20 og drøfte hvilke konsekvenser dommen har for tolkningen av artikkel 9 (1). Avslutningsvis vil jeg i konklusjonen i kapittel fem oppsummere oppgavens funn.

22 Direktiv 95/46/EF.

2 GDPR og personopplysninger

2.1 GDPR generelt

Som nevnt innledningsvis er et av formålene med GDPR å verne fysiske personer i forbindelse med behandling av personopplysningene deres. For å kunne oppnå dette oppstiller GDPR først og fremst en rekke plikter *den behandlingsansvarlige* må overholde for å kunne behandle personopplysninger, og en rekke rettigheter for *den registrerte*. *Den behandlingsansvarlige* er en fysisk eller juridisk person som er ansvarlig for behandlingen av opplysningene og bestemmer formålet med behandlingen og midlene som skal benyttes.²³ *Den registrerte*²⁴ er betegnelsen på fysiske personer som får behandlet personopplysninger om seg.

GDPR er et risikobasert regelverk og det innebærer at den behandlingsansvarlige ved enhver behandling skal gjennomføre tiltak som motvirker forhold som gir risiko for fysiske personers rettigheter og friheter, og spesielt forhold som kan krenke personvernet.²⁵ Dette følger blant annet av artikkel 5 (2) der det uttrykkes at den behandlingsansvarlige er ansvarlig og skal kunne påvise at de generelle personvernprinsippene i artikkel 5 (1) overholdes både før, under og etter behandlingen.²⁶ Risikovurderinger er den behandlingsansvarliges hovedverktøy for å sikre at kravene i GDPR innfris. En risikobasert tilnærming betyr at man tilpasser hvor sterkt personopplysningene beskyttes i tråd med hvor stor risiko den konkrete behandlingen utgjør for den registrertes personvern.²⁷ Ordet risiko nevnes flere steder i GDPR, men er ikke definert noe sted. Risiko kan defineres som en funksjon av sannsynlighet og konsekvens av en

23 Schartum (2020) s. 61 og GDPR artikkel 4 (7).

24 Jf. GDPR artikkel 4 (1).

25 Schartum (2020) s. 237.

26 Wessel-Aas og Ødegaard (2018) s. 129.

27 Kuner mfl. (2020) s. 26.

eller flere hendelser.²⁸ Enhver databehandling vil ha påvirkning på den registrerte, og i risikovurderinger dreier det seg gjennomgående om å unngå negativ påvirkning og at skadelige konsekvenser materialiserer seg for den registrerte.²⁹

Et sentralt trekk ved GDPR er at det oppstilles et skille mellom alminnelige personopplysninger³⁰ og særlige kategorier personopplysninger.³¹ Som konsekvens av at GDPR er et risikobasert regelverk, stilles det strengere krav til behandlingen av særlige kategorier personopplysninger fordi disse er av mer privat karakter enn ordinære personopplysninger. Dermed har de registrerte behov for sterkere vern.³² Når alminnelige personopplysninger behandles kreves det kun at den behandlingsansvarlige har et legitimt formål og hjemmel i en av behandlingsgrunnlagene som oppstilles i artikkel 6 (1) bokstav a-f. Nærmere bestemt må den behandlingsansvarlige etter artikkel 6 (1) veie interessen for å sette i gang behandlingsaktiviteten opp mot personverninngrepet for den registrerte.³³

Særlige kategorier personopplysninger er på sin side i utgangspunktet forbudt å behandle etter GDPR artikkel 9 (1), og dersom man skal foreta behandling er kravene til behandlingsgrunnlag som er nedfelt i artikkel 9 (2) mer restriktive enn grunnlagene i artikkel 6 (1). I teorien er det dessuten antatt at det kreves kumulativt rettsgrunnlag i både artikkel 9 (2) og i artikkel 6 (1) for å behandle særlige kategorier.³⁴ I tillegg kan skillet få konsekvenser for den behandlingsansvarliges vurdering av personvernkonsekvenser, da behandling av store mengder artikkel 9-opplysninger kan regnes som høyrisiko og det stilles mer omfattende krav

28 Schartum (2020) s. 238.

29 AP29WP Opinion 06/2014 s. 36

30 Jf. GDPR Artikkel 4 (1).

31 Jf. GDPR Artikkel 9 (1).

32 Wessel-Aas og Ødegaard (2018) s. 107.

33 Wessel-Aas og Ødegaard (2018) s. 148.

34 Schartum (2020) s. 110.

til denne vurderingen etter artikkel 35 og man også kan måtte utpeke personvernombud i henhold til artikkel 37.³⁵

2.2 Almennelige personopplysninger

Definisjonen av «personal data» (heretter «personopplysning») fremgår av GDPR art. 4 (1):

‘personal data’ means **any information relating to an identified or identifiable natural person** (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Det avgjørende kriteriet for at noe skal være en personopplysning som omfattes av GDPR er at det med stor grad av sikkerhet er mulig å fastslå hvilken fysisk person man har personinformasjon om. I tråd med Artikkel 29-gruppens inndeling av definisjonen³⁶ til artikkel 4 (1) GDPR er det fire kumulative vilkår som må være innfridd, og spesielt vilkåret «identified or identifiable» gjør at personopplysningsbegrepet favner vidt.

Ordlyden «any information» tilsier at det er tilstrekkelig at det er en opplysning.

Opplysningene GDPR regulerer kan dessuten uttrykkes på en hvilken som helst måte i nærmest alle mulig tenkelige former som skrift, lyd, bilder, tegning, video, biometri, registrering ved sensorer eller på annet vis.³⁷ Synspunktet bekreftes i Peter Nowak-dommen der EU-domstolen uttalte at en vid forståelse «[...] reflects the aim of the EU legislature to assign a wide scope to that concept».³⁸ I samme dom uttalte EU-domstolen også at personopplysninger potensielt omfatter all slags informasjon som er «[...] not only objective

35 Schartum (2020) s. 277.

36 A29WP Opinion 4/2007 s. 6.

37 Schartum (2020) s. 48.

38 Sak C-434/16, avsnitt 34.

but also subjective, in the form of opinions and assessments, provided that it ‘relates’ to the data subject». ³⁹ Med andre ord kan personopplysninger i utgangspunktet omfatte alt fra objektive og sikre fakta, til slutninger, verdivurderinger, meninger og gjetninger utledet fra informasjon den behandlingsansvarlige allerede besitter. ⁴⁰

Videre innebærer vilkåret «natural person» at det må behandles opplysninger om en fysisk person. Vilket «relating to» tilsier ut fra ordlyden at opplysningene må ha en viss tilknytning til den fysiske personen, men ingenting om hvor sterk tilknytning som kreves. Igjen tjener Peter Nowak-dommen som et utgangspunkt for å anta at vilkåret som hovedregel tolkes vidt, da EU-domstolen har uttalt at vilkåret «is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person». ⁴¹ Dette betyr at både tilfeller der informasjonen gjennom sitt innhold er om en bestemt person, f. eks i form av et identitetskort, og også tilfeller med fjernere tilknytning, slik som behandlinger der informasjonen gjennom formålet eller virkningen er å påvirke eller evaluere et individ og også behandlinger der informasjonen kun har potensial til det, er omfattet. ⁴²

Det siste vilkåret for at noe skal kunne regnes som en personopplysning, er at informasjonen må omhandle en «identified or identifiable» fysisk person. At en person er «identifiserbar» innebærer at det er mulig å skille personen fra alle andre medlemmer i en gruppe. ⁴³

Først og fremst åpner ordlyden i artikkel 4 (1) for en fleksibel tilnærming til hvordan identifisering kan skje. En person er identifiserbar dersom vedkommende «can be identified, directly or indirectly, in particular by reference to an identifier». Eksempler på identifikatorer som nevnes i GDPR er blant annet navn, identifikasjonsnummer og lokasjonsdata.

39 Sak C-434/16, avsnitt 34.

40 Hallinan og Borgesius (2020) s. 4-5.

41 Sak C-434/16, avsnitt 35.

42 A29WP Opinion 4/2007 s. 9-12.

43 A29WP Opinion 4/2007 s. 12.

Når artikkel 4 (1) nevner både direkte og indirekte identifisering, er konsekvensen i praksis at det er stort rom for å bruke skjønn når man vurderer hvorvidt en opplysning er en personopplysning, spesielt i situasjoner der identifiseringen er indirekte. Direkte identifisering skjer i de tilfellene der informasjonen eksplisitt og direkte identifiserer en person. Typiske eksempler er navn og fingeravtrykk. Som regel er det snakk om informasjon som alene gir tilstrekkelig sikker identifikasjon.⁴⁴

Indirekte identifisering innebærer på sin side at informasjonen har en fjernere og mindre umiddelbar tilknytning til personen, og er som oftest aktuelt i situasjoner der én opplysning alene ikke er nok til å identifisere personen. Dermed sammenstiller man informasjonen med annen tilleggsdata fra flere kilder. For eksempel kombinerer man navn og boligadresse for å identifisere en person. Indirekte identifisering kan også vise til at man kan knytte opplysninger til en person gjennom flere ledd. En personopplysning gjennom flere ledd kan oppstå når et trafikkovervåkingskamera registrerer karakteristikkene ved en bestemt bil, og denne informasjonen viser til et bilutleiefirma som har tilknytning til en bedriftskunde som igjen er tilknyttet en bestemt sjåfør. På bakgrunn av resonnetet kan man fastslå at kameraet registrerer en personopplysning om sjåføren.⁴⁵

Ordlyden «identified or identifiable» medfører dessuten at terskelen for identifiserbarhet er lav. Ut fra ordlyden er det tilstrekkelig at det er et potensial for at personen kan identifiseres. Fortalepunkt 26 oppstiller en identifiserbarhetstest. Ifølge denne skal man i vurderingen av om en person er identifiserbar ta hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk, og momenter som inngår er blant annet kostnader, tidsbruk, tilgjengelig teknologi på behandlingstidspunktet og den teknologiske utviklingen. I tillegg kan EU-domstolens standpunkt i Breyer-dommen⁴⁶ tas til

44 Schartum (2020) s. 44.

45 Schartum og Bygrave (2016) s. 138.

46 Sak C-582/14, avsnitt 49.

inntekt for at opplysningene som gjør identifisering mulig ikke trenger å være i besittelsen til kun én person.

2.3 Hva er behandling av personopplysninger?

Begrepet «processing» defineres i GDPR art. 4 (2) som «any operation or sets of operations which is performed on personal data or sets of personal data, whether or not by automated means». Ordlyden tilsier at bestemmelsen omfatter absolutt alt man kan gjøre med en personopplysning både manuelt og automatisk. Videre lister bestemmelsen opp en rekke eksempler på behandling, deriblant innsamling, registrering, gjenfinning og lagring.

Listen er ikke uttømmende, og det fremgår av fortalepunkt 15 at «in order to prevent a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used». Det betyr med andre ord at «processing» tolkes vidt for å kunne anvendes på nye behandlingsmåter og ny teknologi. «Processing» kan være én eller flere handlinger, og handlingene kan være både enkle og komplekse. På denne måten kan alt fra behandlingsaktiviteter som å sende salgsfremmende e-poster, til å samle inn informasjon fra digitale kilder som man senere sammenstiller med andre opplysninger, eller bare det å legge ut et bilde av en person på et nettsted, være behandlinger som omfattes av GDPR. Videre er et viktig poeng at hvilke opplysninger som utledes av dataene man besitter avhenger av både formålet for bruken, den konkrete behandlingsaktiviteten og konteksten ellers. Ulike behandlingsansvarlige kan bruke den samme informasjonen til ulike formål og eksempelvis foreta ulike gjetninger, slutninger og antakelser basert på samme informasjon.

Samlet sett viser gjennomgangen av vilkårene i definisjonen av personopplysninger, at GDPR opererer med en svært vid forståelse av hvilken informasjon som omfattes av ordlyden. Særlig spørsmålet om identifisering befinner seg i et dynamisk felt fordi man hele tiden vurderer opplysningene i lys av den konkrete konteksten og behandlingssituasjonen, samt at man tar høyde for fremtidig forventet teknologisk utvikling. GDPR tar sikte på å regulere et enormt spekter av både behandlingsmåter og personopplysninger på en fleksibel måte, og et sentralt

hensyn bak den teknologinøytrale innfallsvinkelen er å unngå at det oppstår alvorlig risiko for at bestemmelsene i GDPR omgås.⁴⁷

2.4 Særlige kategorier personopplysninger generelt

GDPR artikkel 9 (1) oppstiller et forbud mot behandling av særlige kategorier personopplysninger og har følgende ordlyd:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Listen over særlige kategorier personopplysninger er uttømmende og behandling av kategoriene er i utgangspunktet alltid forbudt med mindre man har kumulativt hjemmelsgrunnlag i art. 9 (2) og art. 6 (1). Kategoriene er i stor grad en videreføring av Direktiv 95/46/EF artikkel 8 nr.1 med unntak av «genetic data» og «biometric data» som ble tilføyd med vedtakelsen av GDPR. Tidligere ble uttrykket «sensitive personopplysninger» brukt og uttrykket er synonymt med det vi i dag kaller særlige kategorier. Uttrykket «sensitive personopplysninger» er en fellesnevner for særlig følsomme personopplysninger som bør gis et særlig vern.⁴⁸ At en personopplysning kan karakteriseres som «sensitiv» innebærer vanligvis at den har et privat og personlig innhold som gjør at den registrerte personen ønsker å holde informasjonen for seg selv og beskytte den ekstra godt.⁴⁹ Behandlingen av slike opplysninger vil ofte medføre ekstra risiko for den registrerte fordi utilsiktet spredning og tilgjengeliggjøring kan gi uønskede følger av forskjellig art og styrke for personen i det virkelige liv. Den forhøyede risikoen tilsier at det er behov for strengere krav til behandling

47 GDPR fortalepunkt 5.

48 NOU 1997:19 s. 73.

49 Schartum og Bygrave (2016) s. 143-144.

av personopplysninger i slike situasjoner for å sikre tilstrekkelig beskyttelse av den registrertes rettigheter.

Ser man til fortalepunkt 51,71 og 75 legges det opp til en svært vid beskyttelse av de registrerte. Lest i sammenheng indikerer fortalepunktene at sentrale hensyn som motiverer et særskilt vern er at opplysningenes sensitive karakter utgjør en særlig risiko for den enkeltes rettigheter og friheter. I fortalepunkt 51 heter det at slike opplysninger er «particularly sensitive in relation to fundamental rights and freedoms» og at de «merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms». Referansen til «fundamental rights and freedoms» må leses som en anvisning til EUs charter om grunnleggende rettigheter der retten til privatliv og personvern er nedfelt i artikkel 7 og 8.⁵⁰ Videre nevner fortalepunkt 71 i relasjon til behandlinger som angår profilering, at den behandlingsansvarlige i helautomatiserte prosesser må forhindre risikoen for «discriminatory effects» når særlige kategorier personopplysninger behandles.

Risikoen det refereres til i GDPR er dessuten relevant å lese i lys av fortalepunkt 75, der risiko kobles til ulike former for realisering av skade: «The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage». Eksempler på skader som nevnes er blant annet «[...] where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy[...]», samt «any other significant economic or social disadvantage». Med andre ord er det et bredt spekter av risiko for negativ påvirkning på den registrerte som skal vurderes i henhold til GDPR, og hva gjelder artikkel 9-opplysninger kan man se for seg svært mange ulike alvorlige og negative konsekvenser dersom slike opplysninger kommer på avveie eller misbrukes.

50 Charter on The Fundamental Rights of the European Union, 18.12.2000, 2000/C 364/01.

2.5 Særlige kategorier personopplysninger – en kort historikk

Den någjeldende grensedragningen mellom alminnelige og særlige kategorier av personopplysninger i GDPR har en historikk som strekker seg flere tiår tilbake i tid. Siden fremveksten av tidlig lovgivning rundt databeskyttelse har spørsmålet om hvordan man best kan klassifisere og sørge for tilfredsstillende beskyttelse av sensitive personopplysninger vært en rød tråd i personverndebatter.⁵¹ De første internasjonale personverndebattene dreide seg blant annet om hvorvidt sensitivitet var et egnet kriterium for å avgjøre behandlingsbetingelsene for særlig følsomme opplysninger.⁵² Det var enighet om at noen opplysningstyper var mer beskyttelsesverdige enn andre, men det var sprikende praksis.

En av aktørene som tidlig anerkjente behovet for ekstra beskyttelsestiltak for bestemte kategorier av sensitive opplysninger var OECD (Organisasjonen for økonomisk utvikling og samarbeid). OECDs retningslinjer om personvern og utveksling av personopplysninger over landegrensene av 23. september 1980 var ikke bindende, men introduserte et begrep om sensitive opplysninger for medlemslandene som likevel har påvirket nasjonal lovgivning i flere land. Imidlertid utdypet retningslinjene i liten grad innholdet av begrepet og forsøkte heller ikke å presisere hvilke opplysningstyper som skulle betraktes som sensitive.⁵³ Isteden understreket retningslinjene at «[...] It is probably not possible to define a set of data which are universally regarded as being sensitive».⁵⁴

51 Simitis (1999) s. 1.

52 Simitis (1999) s. 2.

53 Quinn og Malgieri (2021) s. 1587.

54 Quinn og Malgieri (2021) s. 1587.

2.5.1 Europarådets personvernkonvensjon

Først med vedtakelsen av Europarådets personvernkonvensjon av 28.januar 1981⁵⁵ oppsto et vendepunkt som fikk store konsekvenser internasjonalt og på mange måter var avgjørende for at sensitive opplysninger ble etablert som et rettslig begrep i flere land.⁵⁶

Europarådets personvernkonvensjon baserte seg på en forutsetning om at noen personopplysninger er ekstra beskyttelsesverdige og dermed kun kan behandles på bakgrunn av bestemte formål og under spesielle forhold. Konvensjonens artikkel 6 angir en forhåndsinn delt liste over spesifiserte kategorier av opplysninger som skal defineres som sensitive, og regulerer «special categories of data». Listen innbefatter kategoriene «personal data revealing racial origin, political opinions or religious or other beliefs» og «personal data concerning health or sexual life». Konvensjonen var bindende, men statene hadde selv mulighet til å opprette flere kategorier med basis i nasjonal lovgivning og dette ga stor fleksibilitet.⁵⁷

Europarådet begrunnet behovet for styrket beskyttelse av sensitive opplysninger etter konvensjonen artikkel 6 med at behandlingen av slike opplysninger «[...] may lead to encroachments on interests, rights and freedoms».⁵⁸ Videre fremhevet Europarådet at inngrep i den enkeltes interesser og rettigheter som kunne utgjøre en potensiell risiko for diskriminering eller skade på en persons verdighet eller fysiske integritet var spesielt viktig å verne. Både tilfeller der en persons mest intime sfærer blir berørt, i form av hans eller hennes sexliv eller seksuelle legning, samt tilfeller der behandling av personopplysninger kan påvirke uskyldspresumsjonen, ble nevnt som sentrale situasjoner som nødvendiggjør ekstra beskyttelse.⁵⁹

55 Convention for the Protection of Individuals with regard to the Automatic Processing for Personal Data, Strasbourg, 28. januar 1981 (CETS no. 108).

56 Simitis (1999) s. 1.

57 Quinn og Malgieri (2021) s. 1588.

58 Europarådet (1981) s. 10.

59 Europarådet (1981) s. 10.

2.5.2 Direktiv 95/46/EF

Direktiv 95/46/EF som ble vedtatt i 1995, bygget på og videreførte katalogiseringen fra Europarådets personvernkonvensjon, men den store forskjellen var at direktivet hadde en restriktiv innfallsvinkel ved å oppstille et absolutt forbud mot behandling av personopplysninger gjennom ordlyden «Member states shall prohibit the processing of [...]». Selv om listen i utgangspunktet var uttømmende ga EU-direktivet likevel medlemsstatene en viss mulighet til å tilføye egne kategorier. Resultatet var lovgivning som sprikte i flere retninger på tvers av medlemsstatene. Enkelte land for eksempel oppstilte genetiske opplysninger, biometriske opplysninger, privatliv og avhengighet som sensitive kategorier.⁶⁰

Hensynene bak beslutningen om å regulere bestemte kategorier av personopplysninger i EU-direktivet er i stor grad sammenfallende med Europarådets begrunnelser. I sin veiledning om særlige kategorier av personopplysninger uttaler Artikkel 29-gruppen at en sentral motivasjon bak den styrkede beskyttelsen er antagelsen om at misbruk av slike opplysninger til forskjell fra misbruk av annen vanlig personinformasjon «[...] could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination».⁶¹ Videre understreker Artikkel 29-gruppen at «Misuse of sensitive data, such as health data or sexual orientation (e.g. if publicly revealed), may be irreversible and have long-term consequences for the individual as well as his social environment».⁶²

Slik det fremgår av Artikkel 29-gruppens veiledning er opplistingen av særlige kategorier personopplysninger i det tidligere direktivet et kompromiss mellom flere land, og kun én av flere mulige innfallsvinkler for å regulere særlig beskyttelsesverdige opplysninger. Artikkel 29-gruppen uttalte at en svakhet ved reguleringen av særlige kategorier personopplysninger i direktivet var at «[...] A closed list is inflexible and unable to react to the context of

60 Simitis (1999) s. 4 og 7.

61 A29WP 04/2011 s. 4.

62 A29WP 04/2011 s. 4.

processing as well as new forms of processing which might occur in the course of ongoing technological developments».63 Artikkel 29-gruppen adresserte problematikken gjennom en analyse av alternative tilnæringer, og skisserte i tillegg til direktivets fremgangsmåte blant annet en kontekstbasert tilnærming.

Her er det særlig interessant å merke seg fleksibiliteten en kontekstbasert tilnærming ville ha åpnet for. Den kontekstbaserte tilnærmingen oppstiller et generelt forbud nesten identisk med direktivets, men overlater større skjønnsrom for medlemsstatene til å tilføye flere kategorier. Den vil også inneholde et tillegg med en generelt utformet ordlyd som omfatter konteksten informasjonen behandles i: «Sensitive personal data are personal data, which are capable by their nature or by the context in which they are processed of infringing fundamental freedoms or privacy or which have an especially discriminatory effect on the data subject».64 En slik ordlyd ville i større grad ha åpnet for å ta hensyn til konteksten når man avgjør hvorvidt personopplysningene man behandler skal omfattes av artikkel 9 (1). I tillegg kunne formuleringen trolig muliggjort at opplysninger som ikke har noen tilknytning til de særlige kategoriene i dagens bestemmelser i GDPR likevel kunne fått et særskilt vern dersom hensynet til den registrerte i en konkret situasjon tilsa slik beskyttelse.

63 A29WP 04/2011 s. 13.

64 A29WP 04/2011 s. 12.

3 Nærmere om GDPR artikkel 9 (1)

I det følgende vil jeg redegjøre for vilkårene i art. 9 (1) for å klarlegge den nærmere materielle rekkevidden av bestemmelsen. Jeg vil først kort redegjøre for de ulike særlige kategoriene bestemmelsen oppstiller, før jeg vil drøfte vilkårene «revealing» og «concerning». Slik drøftelsen vil vise reiser art. 9 (1) en rekke uavklarte tolkningsspørsmål, og det er flere utfordringer knyttet til å avgjøre når det faktisk skjer en behandling av artikkel 9-opplysninger. I den sammenhengen er et sentralt spørsmål om også opplysninger som ikke direkte omhandler noen av de særlige kategoriene likevel kan være omfattet av art. 9 (1).

3.1 Kategoriene i GDPR artikkel 9 (1)

Den vage ordlyden i GDPR art. 9 (1) kan forstås som et uttrykk for et ønske om å sikre et bredt vern for personopplysninger som representerer en særlig stor risiko for den enkeltes grunnleggende rettigheter og friheter.⁶⁵ EU-rettens lovgivningsteknikk med utstrakt bruk av vide og abstrakte ordlyder, samt det sparsommelige tilfanget av rettskilder gjør imidlertid at det lett kan oppstå usikkerhet knyttet til hvorvidt en personopplysning er omfattet av art. 9 (1) i konkrete behandlingssituasjoner.

Hver av de opplistede kategoriene i art. 9 (1) kan betraktes som nærmere definerte grupperinger av sensitive egenskaper og opplysningstyper. Det er kun «genetic data», «biometric data» og «data concerning health» som er legaldefinert i henholdsvis art. 4 (13), art. 4 (14) og art. 4 (15).⁶⁶ Et fellestrekk ved alle opplysningstypene i art. 9 (1) er at de har vage og vide ordlyder. Dermed oppstår det avgrensingsproblemer i praksis når man skal

⁶⁵ GDPR fortalepunkt 51.

⁶⁶ Som nevnt innledningsvis avgrenser oppgaven mot en detaljert behandling av disse ettersom definisjonene reiser mange kompliserte spørsmål.

vurdere om en konkret opplysning bør omfattes av art. 9 (1). Helseopplysninger⁶⁷ kan for eksempel være alt fra opplysninger om en vanlig forkjølelse til stigmatiserende informasjon om sykdommer eller funksjonsnedsettelse, og utgangspunktet er at det trengs lovhjemmel i en av de alternative grunnlagene i art. 9 (2) for å behandle opplysningene i begge tilfeller til tross for forskjellen i alvorlighetsgrad.⁶⁸

De fem andre resterende kategoriene i art. 9 (1) innbefatter «racial or ethnic origin» (rasemessig eller etnisk opprinnelse), «political opinions» (politisk oppfatning), «religious or philosophical beliefs» (religion eller filosofisk overbevisning), «trade union membership» (fagforeningsmedlemskap) og «data concerning a natural person's sex life or sexual orientation» (opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering). Ingen av dem er legaldefinert i GDPR, og det er få rettskilder som gir veiledning. De vide formuleringene kan i utgangspunktet romme svært mye.

Kategorien «racial or ethnic origin» må regnes for å dekke informasjon om minoritetstilhørighet og hudfarge⁶⁹, og det understrekes i fortalepunkt 51 at EU ikke godtar teorier om at det finnes ulike menneskeraser. Kategorien «political opinions» tilsier ut fra en ordlydstolkning at det er snakk om ytringer som forteller noe om politisk tilhørighet. Det er antatt at «political opinions» omfatter både tilknytning til et politisk parti, deltakelse i demonstrasjoner og politiske uttalelser eller publikasjoner.⁷⁰ Hva gjelder kategorien «religious or philosophical beliefs» tilsier ordlyden at det inkluderer opplysninger om medlemskap i organisasjoner som fokuserer på religion eller filosofisk tro, og tekst som uttrykker religiøs eller filosofisk overbevisning, samt forskjellige typer atferd som uttrykker dette⁷¹, slik som å

67 EU-domstolen tolker helseopplysninger vidt. I sak C-101/01 Bodil Lindqvist uttalte domstolen at «the expression personal data concerning health must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual» (avsnitt 50).

68 A29WP 04/2011 s. 8.

69 Kuner mfl. (2020) s. 374.

70 Kuner mfl. (2020) s. 375.

71 Kuner mfl. (2020) s. 375.

ha på seg et kors eller unngå visse typer matvarer. Kategorien «trade union membership» tilsier på sin side enhver opplysning som gir holdepunkter for at noen har et slikt medlemskap.

Kategorien «data concerning a natural person's sex life or sexual orientation» må i likhet med de ovennevnte kategoriene antas å romme mye. «Sexual orientation» tilsier opplysninger om alle typer legninger, mens «sex life» trolig kan tolkes enda bredere til å omfatte opplysninger om seksuell praksis, sivilstand og intime opplysninger om f. eks endring av kjønn.⁷² Slik denne raske skisseringen av kategoriene i art. 9 (1) illustrerer kan personopplysninger komme til uttrykk i mange former (f. eks atferd, skrift, utseende) og danne utgangspunkt for mer eller mindre sikre slutninger av sensitiv karakter. Dersom vi trekker linjer tilbake til den vide definisjonen av «personal data» i kapittel 2.2, kreves det heller ikke at slutningene eller antakelsene er sanne for at de skal regnes som en personopplysning.

3.2 «Personal data revealing» og «personal data concerning»: En vid tolkning av GDPR art. 9 (1)?

Den uttømmende listen av særlige kategorier i art. 9 (1) kan imidlertid ikke leses isolert fra resten av ordlyden. Utgangspunktet etter art. 9 (1) er at både ordlyden «personal data concerning» og «personal data revealing» uttrykker et krav til forbindelsen eller tilknytningen mellom *innholdet* i en personopplysning og en av de særlige kategoriene i en konkret behandlingssituasjon. Ordet «concerning» kan oversettes til «angående», «om» eller «omhandler», mens ordet «revealing» på sin side kan oversettes til «avslørende», «avslører» eller «røper».

Ut fra en naturlig ordlydstolkning tilsier både «revealing» og «concerning» at bestemmelsen i art. 9 (1) i utgangspunktet gjelder for alle personopplysninger som klart, utvetydig og direkte omhandler en av de nærmere angitte kategoriene i listen. Altså må personopplysninger som

⁷² Kuner mfl. (2020) s. 375.

direkte gjelder sensitive egenskaper omfattes. For eksempel er uttalelser om at en person er medlem av et trossamfunn eller et politisk parti en personopplysning som helt direkte, klart og utvetydig omhandler de særlige kategoriene «religious beliefs» eller «political opinions». Slike opplysninger kan beskrives som artikkel 9-opplysninger med en klar og direkte tilknytning til de særlige kategoriene og er i utgangspunktet omfattet av bestemmelsen.

Imidlertid kan man spørre seg om de to ordlydene «concerning» og «revealing» indikerer at lovgiver har ønsket å markere en nyanseforskjell. Ordlyden av «concerning» i betydningen «om» og «omhandler» kan forstås som et språklig uttrykk som oppstiller et strengere og mer skjerpert krav til innholdet i personopplysningene og tilknytningen til de særlige kategoriene for at de skal omfattes av art. 9 (1) enn det «revealing» gjør. Ordlyden «revealing» forstått i betydningen opplysninger som «avslører» eller «røper» oppstiller på sin side tilsynelatende rent språklig en lavere terskel for at personopplysninger har et innhold som faller innenfor art. 9 (1). I lys av ordlyden «revealing» er spørsmålet med andre ord om også personopplysninger som på en indirekte måte gir uttrykk for sensitive egenskaper skal omfattes av art. 9 (1) og hvor den nedre grensen skal trekkes.

Artikkel 29-gruppens tilnærming i *Advice paper on special categories of data* tyder på at ordlyden «personal data revealing» i art. 9 (1) GDPR skal tolkes vidt. Artikkel 29-gruppen uttaler at «The term “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership”» skal forstås som at «not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual **can** be concluded».⁷³ Uttalelsen kan tas til inntekt for at artikkel 9 (1) altså ikke bare omfatter direkte sensitive opplysninger, men også personopplysninger og informasjon som i utgangspunktet ikke er sensitiv, men som det kan utledes informasjon om sensitive egenskaper eller forhold fra på en mer indirekte måte gjennom en behandling. Ordet «can» indikerer dessuten at det er nok at det finnes en slik mulighet i opplysningene.

73 A29WP 04/2011 s. 5.

Synspunktet har fått bred støtte i teorien, og Kuner presiserer at ordlyden «revealing» innebærer at «the list includes not just direct indications of sensitive data, but also information that can be used to indicate them indirectly». ⁷⁴Opplysninger som indirekte avslører en særlig kategori er hensiktsmessig å forstå i lys av identifikasjonskravet som oppstilles i definisjonen av personopplysninger i artikkel 4 (1) GDPR. Poenget er at akkurat som man kan foreta indirekte identifisering gjennom å sammenstille informasjon med fjern tilknytning til en person, så kan man gjennom å sammenstille informasjon fra flere kilder eller i flere ledd, ofte også utlede opplysninger som indirekte avslører sensitive egenskaper om en person samtidig som det er tilstrekkelig at det er mulig å identifisere personen.

Et eksempel på personopplysninger som røper noe om sensitive forhold på en indirekte måte, er dersom en religiøs sekt har opprettet nettsider som er rettet mot medlemmene av sekten. ⁷⁵ Informasjonen om at en bestemt person har brukt sektens nettsted er ikke en direkte opplysning om personens tro, men likevel kan man tolke informasjonen om nettbruken som en sterk indikasjon på personens religiøse tilhørighet og stille spørsmål ved om tilfellet bør omfattes av art. 9 (1). Et annet eksempel er at man gjennom å studere transaksjonsdetaljene i en persons bankutskrift, f. eks kan trekke slutninger, altså utlede opplysninger, om at personen er medlem i en fagforening.

3.3 Fotografier og video

Samtidig skaper den brede definisjonen som er skissert hittil av art. 9 (1) flere komplekse tolkningsspørsmål. Nærmere bestemt er det i lys av rettskildene uklart hvordan den nedre grensen for hvilke opplysninger som omfattes av bestemmelsen skal trekkes. Når personopplysninger kan uttrykkes i mange medier både gjennom video, fotografi og lyd, er en

⁷⁴ Kuner mfl. (2020) s. 373.

⁷⁵ Bygrave og Schartum (2016) s. 145.

naturlig konsekvens at svært mye kan røpes om forhold eller egenskaper som faller innenfor en av de særlige kategoriene.

Avhengig av behandlingssituasjon og behandlingsformål, er det mulig å utlede ulike opplysninger fra ett og samme datasett. De samme opplysningene kan altså behandles på ulike måter av forskjellige behandlingsansvarlige til ulike formål. Ofte vil det være en viss risiko for at en behandlingsansvarlig prosesserer andre opplysninger og også opplysninger av særlige kategorier, i tillegg til de opplysningene den behandlingsansvarlige har som formål å behandle. Å tenke seg et skille mellom aktiv og passiv behandling kan bidra til å klargjøre problemstillingen. Den «aktive» behandlingen består av informasjonen den behandlingsansvarlige har formål og behandlingsgrunnlag til å behandle, mens den «passive» behandlingen er all informasjonen som følger med.

Fotografier og video er et godt eksempel på en type personopplysninger det ofte vil være mulig å dedusere opplysninger om forhold knyttet til en eller flere av de særlige kategoriene i art. 9 (1) fra på en indirekte måte. Fotografier vil nesten bestandig gi en indikasjon på hudfarge og etniske trekk, og i noen tilfeller også religion dersom vedkommende bærer et religiøst symbol eller plagg. Artikkel 29-gruppen har utpekt fotografier og personbilder, enten de er publisert på internett eller tatt av trafikkovervåkningskameraer eller andre overvåkningskameraer, som spesielt problematiske. De har uttalt at «[...] images can reveal information about an individual's ethnic origin or health status, for example, they may be considered sensitive data as defined in Art. 8 (1) of the Directive, with the result that these data may not be processed without the individual's consent».⁷⁶ Uttalelsen har begrenset vekt ettersom den er gjort i forbindelse med Direktiv 95/46/EF, og definisjonen av «biometric data» var ikke inntatt i direktivet på det tidspunktet, men likevel tjener den som eksempel på at Artikkel 29-gruppen anerkjente at bilder som avslører en av de særlige kategoriene kunne kvalifisere som artikkel 9-opplysninger uavhengig av behandlingens formål.

76 A29WP 04/2011 s. 8.

En løsning der alle personbilder i form av fotografier og malerier skal regnes for å tilhøre art. 9 (1) er upraktisk fordi det i realiteten betyr at det bestandig er forbudt å behandle disse opplysningene med mindre den behandlingsansvarlige f. eks har samtykke etter art. 9 (2). Med ikrafttreddelsen av GDPR har det derfor blitt foretatt en presisering som avgrenser rekkevidden av art. 9 (1) noe. Det fremgår av fortalepunkt 51 at behandling av fotografier «should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person».

Fortalepunkt 51 kan forstås som at fotografier som hovedregel bare skal regnes som artikkel 9-opplysninger når de omfattes av definisjonen av «biometric data for the purpose of uniquely identifying a natural person». Biometriske kjennetegn kan beskrives som kjennetegn som utgår fra kroppen, som er unike for hver enkeltperson og samtidig permanente eller stabile over tid.⁷⁷ Et hovedhensyn bak unntaket for biometriske opplysninger er trolig å forhindre at fotografier og visuelt materiale automatisk betraktes som artikkel 9-opplysninger.⁷⁸

I lys av ordlyden av «biometric data» i art. 9 (1) og ordlyden av legaldefinisjonen i art. 4 (14) kreves det at opplysningene relaterer seg til fysiske, fysiologiske eller atferdsmessige egenskaper hos en fysisk person, at selve identifiseringen skjer gjennom en særskilt teknisk behandling («specific technical means») og at formålet med behandlingen er å entydig identifisere en fysisk person for at et fotografi skal omfattes av definisjonen av biometri.

⁷⁹Dette betyr at et fotografi eller et videoopptak som ikke har gjennomgått en særskilt teknisk behandling for å identifisere én bestemt person faller utenfor definisjonen selv om materialet avslører sensitive egenskaper.

⁷⁷ Kuner mfl. (2020) s. 212.

⁷⁸ Quinn og Malgieri (2021) s. 1595.

⁷⁹ Personvernrådet 3/2019 s. 18.

3.4 Behandlingsformål som begrensning av art. 9 (1)

Personvernrådet har i sine *Guidelines 3/2019 on processing of personal data through video devices* behandlet spørsmålene nærmere. Her adresserer de utfordringen når videoovervåkningssystemer samler inn enorme mengder personopplysninger som potensielt kan avsløre informasjon som faller innenfor de særlige kategoriene i art. 9 (1).

Videoovervåkning fører til at ikke-signifikant data kan brukes til å utlede annen informasjon for å oppnå et annet formål, for eksempel med hensikt om å kartlegge en persons vaner.

Personvernrådet uttaler at «Video footage showing a data subject wearing glasses or using a wheel chair are not per se considered to be special categories of data».⁸⁰ Imidlertid bemerker de at «However, if the video footage is used to deduce special categories of data Article 9 applies». Videre nevner Personvernrådet to eksempler på behandlingssituasjoner de mener omfattes av art. 9 (1). Det ene eksempelet er at dersom videoopptak behandles med formål om å dedusere politiske meninger fra bilder som viser identifiserbare datasubjekter som deltar i et politisk arrangement eller en streik, så må tilfellene omfattes av art. 9 (1). Det andre eksempelet er at dersom et sykehus installerer et videokamera med formål om å overvåke helsetilstanden til en pasient, så må det anses for å være behandling av særlige kategorier av personopplysninger etter art. 9 (1).⁸¹

Eksemplene indikerer Personvernrådet anser behandlingsformål som en relevant måte å avgrense hvilke behandlinger av personopplysninger som omfattes av art. 9 (1), i alle fall i behandlingssituasjoner som gjelder videoovervåkning. Tilfeller der den behandlingsansvarlige har som formål å utlede særlige kategorier av personopplysninger fra alminnelige personopplysninger er med andre ord behandlinger som klart faller innenfor bestemmelsen.

⁸⁰ Personvernrådet 3/2019 s. 17.

⁸¹ Personvernrådet 3/2019 s. 17.

Tilfeller der den behandlingsansvarlige ikke behandler personopplysninger som helt eksplisitt og direkte omfattes av art. 9 (1) og ikke har oppgitt et behandlingsformål som relaterer seg til en av de særlige kategoriene i art. 9 (1) faller derimot tilsynelatende utenfor. Dette til tross for at det skulle vise seg at særlige kategorier av personopplysninger er en mer eller mindre tilfeldig «bifangst» av den primære behandlingsaktiviteten man gjennomfører, og dermed fremgår på en indirekte måte. Utgangspunktet er at en slik situasjon ikke i seg selv omfattes av artikkel 9 (1), selv om den behandlingsansvarlige trolig sitter på store mengder informasjon det potensielt kan utledes artikkel 9-opplysninger fra, for eksempel dersom en kirke installerer overvåkningskameraer på eiendommen sin. For å sikre tilstrekkelig vern av opplysningene som samles inn må den behandlingsansvarlige i slike tilfeller ta hensyn til dataminimeringsprinsippet og «try to minimize the risk of capturing footage revealing other sensitive data (beyond Article 9), regardless of the aim».⁸² En måte å minimere risikoen for å avsløre annen sensitiv informasjon, er for eksempel å ikke lagre mer data enn det som er strengt nødvendig for formålet, og å begrense lagringstiden til et absolutt minimum.

Et liknende standpunkt om betydningen av behandlingsformål som avgrensningskriterium for hva skal regnes som artikkel 9-opplysninger er uttrykt av Personvernrådet i *Guidelines 8/2020 on the targeting of social media users*. I retningslinjene utgjør profilering en særskilt form for behandling som aktualiserer situasjoner der artikkel 9-opplysninger av indirekte karakter oppstår.

Profilering⁸³ er i denne sammenhengen forstått som analysering av personopplysninger med formål om å avdekke atferd, preferanser, evner eller behov. Store mengder personopplysninger kan gjennom maskinlæring og sporingsteknologi brukes til å lage omfattende profiler om enkeltindivider.⁸⁴ I den aktuelle veilederen deles artikkel 9-opplysninger inn i «explicit special categories of data» og «inferred and combined special

⁸² Personvernrådet 3/2019 s. 17.

⁸³ Jf. definisjonen av profilering i GDPR artikkel 4 (4).

⁸⁴ NOU 2022:11 s. 50.

categories of data». Førstnevnte er direkte sensitive opplysninger som klart og eksplisitt gir uttrykk for informasjon som omfattes av artikkel 9 (1).⁸⁵ Sistnevnte er artikkel 9-opplysninger av indirekte karakter nettopp fordi de oppstår som resultat av at det sammenstilles og utledes informasjon fra alminnelige personopplysninger. Personvernrådet uttaler at «profiling can create special category of data by inference from data which is not special category data in its own right, but becomes so when combined with other data».⁸⁶ Et eksempel på dette er at når man utleder opplysninger om noens helsetilstand gjennom å kombinere informasjon om matinnkjøp med informasjon om matens kvalitet og energiinnhold. Her er formålet å utlede helseopplysninger og følgelig er opplysningene omfattet av art. 9 (1).⁸⁷

Videre uttaler Personvernrådet at behandlingen av en enkelt uttalelse eller en enkelt stedsdata som avslører at en person har besøkt et sted som typisk besøkes av grupper med en bestemt religiøs tro, ikke generelt i seg selv vil bli ansett som behandling av artikkel 9-opplysninger. Imidlertid bemerker de at «However, it may be considered as processing of special categories of data if these data are combined with other data or because of the context in which the data are processed or the purposes of which they are being used».⁸⁸ Uttalelsen tyder på at hva gjelder profilering og targeting, så er ikke behandlingsformål alene avgjørende for å bestemme hvilke opplysninger som omfattes av art. 9 (1), man må også se på konteksten opplysningene behandles i. Samtidig understrekes det at når en leverandør av sosiale medier behandler store mengder informasjon som potensielt kan brukes til å utlede personopplysninger av særlige kategorier, fører ikke dette automatisk til at behandlingen omfattes av art. 9 (1). Artikkel 9 blir altså ikke aktualisert dersom «the processing does not

85 Personvernrådet nevner en uttalelse i sosiale medier om at man er medlem av et politisk parti som et eksempel på «explicit special categories of data», jf. Personvernrådet 8/2020, s. 32.

86 Personvernrådet 8/2020 s. 32.

87 Personvernrådet 8/2020 s. 32.

88 Personvernrådet 8/2020 s. 33.

result in inference of special category data».⁸⁹ Her vil personvernprinsippene og risikovurderingene i GDPR art. 32 og eventuelt art. 35 fungere som sikkerhetsmekanismer.

3.5 Fordeler og ulemper ved behandlingsformål som begrensning

Etter dette er det klart at ordlydene «revealing» og «concerning» i utgangspunktet åpner for en vid tolkning av artikkel 9 (1) GDPR. Imidlertid viser gjennomgangen av retningslinjene i punkt 3.4 at rekkevidden av artikkel 9 (1) ikke er like stor som ordlyden indikerer, og at det er usikkerhet knyttet til hvordan den nærmere grensedragningen skal foretas. Personvernrådets uttalelser i *Guidelines 3/2019 on processing of personal data through video devices* tyder på at i alle fall behandlingssituasjoner som starter med alminnelige personopplysninger, men der man har som formål å utlede personopplysninger av særlige kategorier, bør omfattes. Altså må formålet med behandlingen være tilknyttet den særlige kategorien. I det følgende vil det redegjøres nærmere behandlingsformål som et avgrensningskriterium for å definere når det skjer behandling av artikkel 9-opplysninger, og fordeler og ulemper ved en slik innfallsvinkel.

Et behandlingsformål defineres av den behandlingsansvarlige før behandlingen av personopplysningene starter og er viktig for å sikre at behandlingen er lovlig. Med behandlingsformål menes den spesifikke årsaken til at personopplysninger behandles av en behandlingsansvarlig. Behandlingsformålet er altså målet eller intensjonen den behandlingsansvarlige har.⁹⁰ Formålsbegrensningsprinsippet er en av de seks grunnleggende personvernprinsippene som er nedfelt i art. 5 (1) GDPR og går ut på at personopplysninger kun skal samles inn for spesifikke, uttrykkelig angitte og legitime formål.⁹¹ Formålsbegrensningsprinsippet er samtidig en rettsregel om at det ikke er bare er lov å samle inn personopplysninger før et eller flere behandlingsformål er bestemt slik GDPR krever.⁹² En

⁸⁹ Personvernrådet 8/2020 s. 33.

⁹⁰ Wessel-Aas og Ødegaard (2018) s. 148.

⁹¹ NOU 2022:11 s. 40.

⁹² NOU 2022:11 s. 40.

annen viktig side ved formålsbegrensningsprinsippet som sikrer vern for den registrerte er at adgangen til viderebehandling av opplysningene er begrenset etter nærmere angitte kriterier i art. 5 (1) b.

Behandlingsformålet danner dessuten en referanseramme for de andre vurderingene etter personvernprinsippene i art. 5 (1), slik som dataminimeringsprinsippet.

Formålsbegrensningsprinsippet og dataminimeringsprinsippet henger tett sammen, da sistnevnte innebærer at en ikke skal behandle flere opplysninger enn det som er strengt nødvendig med utgangspunkt i formålet, og at opplysninger ikke må brukes i større utstrekning enn nødvendig.

På den ene siden fremstår det å bruke behandlingsformål som begrensning for når det foregår behandling av personopplysninger som omfattes av art. 9 (1) som en praktisk og anvendelig løsning som forhindrer at bestemmelsen får en altfor omfattende materiell rekkevidde. Man fanger dessuten opp mange forskjellige behandlinger ved å inkludere tilfeller der personopplysninger av særlige kategorier oppstår som et resultat av behandlingen og følgelig har tilknytning til en av de særlige kategoriene. Sett fra den behandlingsansvarliges perspektiv sikrer man dessuten forutberegnelighet ettersom kun behandlinger der formålet eksplisitt er å behandle særlige kategorier omfattes. Dermed faller også en rekke ubetydelige tilfeller med minimale personvernulemper for den registrerte utenfor art. 9 (1). Dersom man trekker linjer tilbake til eksempelet med videoovervåking av en kirke, vil dessuten dataminimeringsprinsippet redusere mengden personopplysninger som innhentes og behandles.

På den andre siden kan behandlingsformål som avgrensningskriterium føre til at risikoen for at lite gjennomtenkte eller uaktsomme behandlinger av personopplysninger øker.⁹³ Fordi det kan være vanskelig å bevise hva intensjonene til den behandlingsansvarlige er i en konkret behandlingssituasjon, kan man se for seg mange omgåelsestilfeller. Den

93 Quinn og Malgieri (2021) s. 1592.

behandlingsansvarlige kan oppgi et behandlingsformål, men likevel behandle opplysninger med viten og vilje for å utlede personopplysninger av særlige kategorier. I tillegg vil situasjoner der behandlingsformålene er mer abstrakt angitt heller ikke fanges opp av art. 9 (1). Hvis den behandlingsansvarlige for eksempel er et forsikringselskap som behandler kundeopplysninger med formål om å bestemme hvilke kunder som skal få bedre forsikringsvilkår, er det ikke usannsynlig at behandlingsmåten gjør at det utledes personopplysninger av særlige kategorier.

3.6 Formålstolkning og kontekstbasert tilnærming til art.9 (1)

I forlengelsen av dette kan det argumenteres for at behandlinger der det prosesseres mye data (f. eks gjennom innsamling) som gjør det mulig å utlede opplysninger av særlige kategorier, uansett vil representere en potensiell risiko for den registrertes vern helt uavhengig av om formålet og resultatet med behandlingen er å utlede slike opplysninger eller ikke. For at artikkel 9 (1) skal komme til anvendelse er det heller ikke nødvendig å bevise at behandlingen fører til skade for den registrerte, det er tilstrekkelig at det er en forhøyet risiko.⁹⁴

Behandlinger som representerer en stor risiko for den enkelte, er for eksempel innsamling av data fra offentlige sosiale medier for å generere profiler. Her inngår opplysningene gjerne i en omfattende behandling og brukes til vurdering eller bedømmelse av en enkeltperson, samtidig som datasett gjerne kombineres og matches og det ofte utledes artikkel 9-opplysninger.⁹⁵

Dag Wiese Schartum argumenterer for at hensynet til den registrerte, som nettopp er at GDPR skal sikre et høyt beskyttelsesnivå for «fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger»,⁹⁶ tilsier at formålstolkning er relevant for å løse spørsmål knyttet til grensdragningen av hvilke opplysninger som faller

94 GDPR fortalepunkt 51.

95 Datatilsynet, «Vurdering av personvernkonsekvenser og forhåndsdrøftelse», 17.07.2019, <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/> (lest 26.04.23).

96 Jf. GDPR art. 1 (2).

innenfor art. 9 (1).⁹⁷ Gjennom formålstolkning ser man GDPR, bestemmelsen og uttrykket som tolkes i sammenheng med formålet som skal realiseres og tolker slik at formålet fremmes så mye som mulig. Schartum foreslår å se på betydningen personopplysningen har for vernet av den registrertes rettigheter og friheter i den konkrete situasjonen for å avgjøre om f. eks et bilde av personer som bærer et kors bør omfattes av art. 9 (1). Ifølge Schartum vil man da komme til at f. eks et personbilde som viser hudfarge er uten betydning i noen sammenhenger, mens det i andre sammenhenger kan ha stor betydning.⁹⁸

Hva slags type behandling personopplysningene utsettes for og konteksten, altså sammenhengen behandlingen utføres i, spiller med andre ord også en viktig rolle for med hvilken styrke den registrertes rettigheter og friheter gjør seg gjeldende. Quinn og Malgieri foreslår at en kontekstbasert tilnærming til GDPR art. 9 (1). Det innebærer at når man behandler informasjon så ser man på flere momenter for å avgjøre om opplysningene bør omfattes av bestemmelsen. Relevante momenter er «[...] the specific interests of the controller, as well as of the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the persons involved».⁹⁹

Gjennom å bruke en kontekstbasert tilnærming for å vurdere hvilke personopplysninger som bør omfattes av art. 9 (1) GDPR ser man på spesifikke særtrekk ved opplysningene som behandles og måten de behandles på, fremfor å kun ta hensyn til intensjonene til den behandlingsansvarlige. Fordelene ved en slik innfallsvinkel er at den harmonerer godt med den risikobaserte tilnærmingen GDPR legger opp til. Ifølge fortalepunkt 76 skal man i vurderingen av hvor sannsynlig og alvorlig risikoen er for den registrertes rettigheter og friheter, se på behandlingens art, omfang, formål og sammenhengen den utføres i. På den

97 Schartum (2020) s. 47.

98 Schartum (2020) s. 47. Schartum presiserer imidlertid ikke nærmere hvilke kriterier som skal brukes for å avgjøre hvorvidt en artikkel 9-opplysning har betydning i en bestemt kontekst.

99 Quinn og Malgieri (2021) s. 1591.

måten kan man blant annet vurdere den totale informasjonsmengden den behandlingsansvarlige har tilgang til. Dermed kan man for eksempel komme frem til at en leverandør av sosiale medier som behandler store mengder informasjon som potensielt kan brukes til å utlede personopplysninger av særlige kategorier foretar en behandling som bør omfattes av art. 9 (1). Samtidig vil ulempen ved en slik tilnærming være at pliktene for en rekke behandlingsansvarlige kan bli uforholdsmessig omfangsrike og det kan være vanskelig i praksis å skaffe tilstrekkelig oversikt over den totale mengden informasjon som inngår i behandlingen. En annen utfordring Quinn og Malgieri har pekt på, er at man med en vid tolkning av GDPR artikkel 9 (1) kan risikere en inflasjonseffekt på sikt der stadig flere typer behandlinger og personopplysninger regnes for å omfattes av særlige kategorier, og at GDPR dermed blir vanskelig å håndheve i praksis.¹⁰⁰

100 Quinn og Malgieri (2021) s. 1583.

4 Sak C-184/20: Kan et navn være en artikkel 9-opplysning?

4.1 Sakens bakgrunn og EU-domstolens konklusjoner

Slik den foreløpige analysen av art. 9 (1) GDPR har vist er rekkevidden av bestemmelsen uklar, og rettskildene gir ufullstendig veiledning. *OT v Vyriausioji tarnybinės etikos komisija* i avgjørelsen C-184/20 som EU-domstolen avsa 1. august 2022 bidrar imidlertid til en klargjøring av hvor de nærmere grensene for hvilke opplysninger som omfattes av GDPR artikkel 9 (1) går og er hittil den første og eneste dommen fra EU-domstolen som behandler artikkel 9 (1) i detalj.

Dommen er en forhåndsavgjørelse i medhold av TEUV artikkel 267.¹⁰¹ Ordningen med forhåndsavgjørelser innebærer at medlemsstater har rett til å legge fram EU-rettslige tolkningsspørsmål for EU-domstolen, og videre at domstoler som dømmer i siste instans har plikt til dette.¹⁰² Formålet med ordningen er å sikre ensartet fortolkning av EU-retten.¹⁰³ Hva gjelden den konkrete avgjørelsen er det verdt å merke seg at dommen er avsagt av storkammeret med 15 dommere. Dette gir avgjørelsen ekstra tyngde, og det er grunn til å anta at den grundige behandlingen er et resultat av at EU-domstolen anser rekkevidden av GDPR artikkel 9 (1) som et spørsmål av stor prinsipiell betydning.

Saksforholdet¹⁰⁴ gjaldt en nasjonal lov i Litauen som pålegger personer som mottar offentlige EU-midler å sende inn erklæringer om private interesser til den øverste etiske kommisjonen i landet. Den etiske kommisjonen er en offentlig myndighet som arbeider for å hindre

101 Traktaten om Den europeiske unions virkeområde.

102 Fredriksen og Mathisen (2018) s. 260.

103 Fredriksen og Mathisen (2018) s. 261.

104 Jf. Sak C-184/20.

korrupsjon, og interesseerklæringene er et viktig ledd i arbeidet med korrupsjonsbekjempelse. OT, en direktør for en organisasjon med tilknytning til miljøvernfeltet, nektet derimot å sende inn en slik erklæring.

Bakgrunnen for at OT nektet, var at han etter loven ikke bare var pålagt å oppgi informasjon om seg selv, men også opplysninger om partnere, samboere eller ektefeller. Den strenge informasjonsplikten den litauiske antikorrupsjonsloven oppstiller innebærer med andre ord at den etiske kommisjonen får tilgang til detaljert informasjon om blant annet gaver og økonomiske transaksjoner om den registrerte, i tillegg til tilsvarende opplysninger om vedkommendes ektefelle. En sentral dimensjon ved saken var dessuten at den etiske kommisjonen i tråd med loven er pålagt å publisere opplysningene på et offentlig nettsted for å sikre krav om gjennomsiktighet og åpenhet knyttet til visse opplysningstyper som et ledd i det nasjonale antikorrupsjonsarbeidet. Gjennom publisering på nett ble informasjonen fra interesseerklæringene dermed tilgjengelig for en allmenn offentlighet.

Da OT nektet å inngi erklæringen, traff den etiske kommisjonen avgjørelse om at han hadde brutt et lovpålegg for å hindre interessekonflikter. OT protesterte og klaget på avgjørelsen. Han anførte at han ikke var omfattet av personkretsen som etter litauisk lov er pålagt å opplyse om private interesser, og at organisasjonen han arbeidet for i kraft av å være en frivillig organisasjon uansett utøver virksomheten sin uavhengig av offentlige myndigheter. Videre anførte han at en publisering av innholdet i interesseerklæringen på kommisjonens nettsted blant annet representerte en krenkelse av respekten for privatlivet hans, og for personvernet til både ham selv og partneren.

EU-domstolen vurderte to spørsmål relatert til saksforholdet. Det første rettsspørsmålet gjaldt hvorvidt GDPR artikkel 6 (1) bokstav c og e og artikkel 6 (3) lest i lys av artikkel 7 og 8 i EU-charteret, må tolkes slik at det er til hinder for nasjonal lovgivning som åpner for at personopplysninger om private interesser publiseres på internett.¹⁰⁵

105 Sak C-184/20, avsnitt 60.

Det andre rettsspørsmålet omhandlet artikkel 9-opplysninger spesifikt og gjaldt hvorvidt GDPR artikkel 9 (1) må tolkes slik at opplysningene i interesseerklæringen som ble publisert på kommisjonens nettsted og som inneholder informasjon om ektefelle, samboer eller partner, og som dermed var egnet til å indirekte avsløre seksuell orientering, kunne anses å falle innenfor «særlige kategorier av opplysninger».¹⁰⁶

Hva gjelder det første spørsmålet, konkluderte EU-domstolen med at til tross for at tiltaket var motivert i et legitimt formål, sikret den nasjonale antikorrupsjonsloven likevel ikke en tilfredsstillende balanse mellom allmennhetens interesse i korrupsjonsbekjempelse og den registrertes rett til vern av personopplysninger.¹⁰⁷ Videre var konklusjonen på det andre spørsmålet at offentliggjøring av en ektefelles navn på et nettsted utgjør behandling av særlige kategorier personopplysninger etter art. 9 (1) GDPR når informasjonen gjør det mulig å utlede opplysninger om en persons seksuelle orientering.¹⁰⁸

For på best mulig måte å få frem bredden av aspekter en behandlingsansvarlig må ta hensyn til ved behandling av personopplysninger som potensielt kan falle innenfor art. 9 (1), vil jeg i det følgende først drøfte dommens andre rettsspørsmål, og deretter dommens første rettsspørsmål. Både den spesifikke behandlingen, formålet og de motstående interessene er momenter som spiller inn i vurderingen EU-domstolen gjør av begge rettsspørsmålene. Særlig mener jeg det er nyttig å undersøke proporsjonalitetstesten EU-domstolen foretar i dommens første rettsspørsmål fordi det utgjør en parallell til den skjønsmessige vurderingen den behandlingsansvarlige selv må gjøre av berettiget interesse som lovlig behandlingsgrunnlag.

106 Sak C-184/20, avsnitt 117.

107 Sak C-184/20, avsnitt 116.

108 Sak C-184/20, avsnitt 128.

4.2 Er personopplysninger som er egnet til å indirekte avsløre seksuell orientering omfattet av behandlingsforbudet i GDPR artikkel 9(1)?

Opplysningene i interesseerklæringen som ble publisert på den etiske kommisjonens nettsted inneholdt informasjon som indirekte kunne avsløre personopplysninger av særlige kategorier fordi ektefellens etternavn var egnet til å fortelle noe om kjønn og seksuell legning lest i sammenheng med OTs navn. Kort sagt skal det lite til for å anta at begge har homofil legning når en mannlig direktør oppgir en partner med et alminnelig mansnavn i interesseerklæringen. Man kan altså indirekte utlede sensitiv informasjon gjennom denne sammenstillingen. EU-domstolen understreker at personopplysningene som er obligatoriske å oppgi i interesseerklæringen i henhold til den litauiske loven «[...] are not, inherently, sensitive data for the purpose of Directive 95/46 and the GDPR». ¹⁰⁹ Utgangspunktet er nettopp at verken navn eller de andre opplysningene som innhentes i interesseerklæringen er direkte omfattet av de særlige kategoriene i artikkel 9 (1).

Imidlertid påpeker EU-domstolen at «[...] it is possible to deduce from the name-specific data relating to the spouse, cohabitee or partner of the declarant certain information concerning the sex life or sexual orientation of the declarant and his or her spouse, cohabitee or partner». ¹¹⁰ På denne måten klargjør domstolen at også personopplysninger av indirekte karakter kan falle innenfor bestemmelsen i tilfeller der det er mulig å utlede informasjon knyttet til kategoriene i artikkel 9 (1). På bakgrunn av dette var spørsmålet ifølge EU-domstolen om «[...]whether data that are capable of revealing the sexual orientation of a natural person by means of an intellectual operation involving comparison or deduction fall within the special categories of personal data». ¹¹¹

109 Sak C-184/20, avsnitt 119.

110 Sak C-184/20, avsnitt 119.

111 Sak C-184/20, avsnitt 120.

Ved å formulere uttrykket «by means of an intellectual operation involving comparison or deduction» retter EU-domstolen blikket mot hvordan den spesifikke behandlingen av informasjon gjennom sammenstilling og deduksjon har betydning for hvilke opplysninger det er mulig å utlede fra ett og samme datasett. Ordet «operation» er nærliggende å lese som en referanse til «processing» slik det er legaldefinert i GDPR artikkel 4 (2) som «any operation or set of operations which is performed on personal data [...]». Domstolen gir imidlertid ikke her noen nærmere forklaring på hva «an intellectual operation involving comparison or deduction» innebærer i praksis, men understreker at i tolkningen av artikkel 9 (1) må ordlyden, konteksten og formålet med GDPR tas i betraktning.¹¹²

Deretter foretar domstolen en isolert tolkning av ordlydene «revealing» og «concerning»¹¹³ og påpeker med henvisning til generaladvokatens innstilling at «revealing» er «consistent with the taking into account of processing not only of inherently sensitive data, but also of data revealing information of that nature indirectly, following an intellectual operation involving deduction or cross-referencing».¹¹⁴ Med andre ord tolker domstolen «revealing» vidt til å omfatte særlige kategorier av personopplysninger som fremgår både direkte og indirekte. Videre påpeker domstolen hvordan «concerning» har en snevrere ordlyd, da ordlyden virker å «signify the existence of a more direct and immediate link between the processing and the data concerned».¹¹⁵ Imidlertid tilbakeviser EU-domstolen raskt holdbarheten av en tolkning som trekker et skille etter hvilke typer sensitive opplysninger det dreier seg om.

Isteden fremhever EU-domstolen at det må foretas en kontekstuell tolkning der uttrykkene «revealing» og «concerning» ses i sammenheng, og kommer til at begge uttrykk skal tolkes

112 Sak C-184/20, avsnitt 121.

113 I artikkel 9 (1) GDPR er ordlyden «concerning» plassert foran kategoriene «health» og det heter videre «data concerning a natural person's sex life or sexual orientation». Ordlyden «revealing» er på sin side plassert foran kategoriene «racial or ethnic origin, political opinions» etc.

114 Sak C-184/20, avsnitt 123.

115 Sak C-184/20, avsnitt 123.

vidt. For å begrunne dette, argumenterer domstolen med å vise til nettopp hvordan «data concerning health» gis en vid legaldefinisjon i GDPR art. 4 (15) der det er tilstrekkelig at opplysningene røper informasjon om noens helsetilstand. For ytterligere å underbygge den vide tolkningen henvises det også til definisjonen av helseopplysninger i fortalepunkt 35.¹¹⁶

Det andre sentrale argumentet i EU-domstolens analyse er at en vid tolkning av «særlige kategorier personopplysninger» er i tråd med formålet til GDPR og Direktiv 95/46/EF. Reglene i GDPR som gjennomfører rettighetene i EU-charteret artikkel 7 og 8, må tolkes i lys av charteret og retten til respekt for privatlivet er en grunnleggende rettighet i charteret som må tillegges stor vekt. Domstolen poengterer at GDPR særlig har som formål å sikre et høyt beskyttelsesnivå av fysiske personers grunnleggende rettigheter og friheter i behandlingen av personopplysninger.¹¹⁷ Videre poengterer domstolen at dette spesielt gjør seg gjeldende ved behandling av artikkel 9-opplysninger fordi slike behandlinger kan utgjøre et stort inngrep i individers rettigheter og friheter.

Domstolen legger dermed avgjørende vekt på hensynet til en effektiv og fullstendig beskyttelse av grunnleggende personvernrettigheter sammen med de grunnleggende rettighetenes høye beskyttelsesnivå i tolkningen av artikkel 9 (1). Konklusjonen er at behandling av «personal data that are liable indirectly to reveal sensitive information concerning a natural person» ikke kan unntas fra det styrkede beskyttelsesregimet GDPR legger opp til.¹¹⁸ Å unnta slik informasjon fra artikkel 9 (1) vil gå på bekostning av effektiviteten til regimet og beskyttelsen av de grunnleggende rettighetene og frihetene til de fysiske personene GDPR skal verne.¹¹⁹ I EU-domstolens vurdering spiller den spesifikke behandlingen som ble gjort av opplysningene dessuten en viktig rolle. Det at artikkel 9-

116 Sak C-184/20, avsnitt 124.

117 Sak C-184/20, avsnitt 125-126.

118 Sak C-184/20, avsnitt 127.

119 Sak C-184/20, avsnitt 127.

opplysningene ble publisert og offentliggjort på en internettside og slik ble fullt tilgjengelig til viderebruk for tredjeparter, ga en forhøyet risiko for personvernulemper.

4.3 Proporsjonalitetstesten: Kan personopplysninger om private interesser publiseres på internett?

I behandlingen av det første rettsspørsmålet foretok EU-domstolen i tråd med EU-rettslig metode en vurdering av hvorvidt publiseringen av navnet til OTs ektefelle på internett tjente til å oppnå et legitimt formål, samt hvorvidt dette tiltaket var i overensstemmelse med proporsjonalitetsprinsippet. Proporsjonalitetstesten er en treleddet vurdering der domstolen først vurderer om tiltaket er egnet til å oppnå det angitte formålet, deretter om tiltaket er nødvendig for å oppnå formålet, og til slutt en vurdering av proporsjonalitet *stricto sensu* som går ut på å gjøre en balansetest av interessene som står i konflikt med hverandre.¹²⁰

Hva gjelder kravet om at tiltaket må tjene til å oppnå et legitimt formål, presiserte domstolen at dette klart var innfridd, ettersom både å forhindre interessekonflikter og korrupsjon i offentlig sektor, er mål som er av allmenn interesse og følgelig legitimt.¹²¹ Videre kom domstolen til at publisering på internett var et egnet tiltak for å oppnå formålet om å bekjempe korrupsjon med begrunnelse om at publiseringen bidrar til å avsløre mulige interessekonflikter hos offentlige ansatte og slik sikrer åpenhet.¹²² I vurderingen av om publiseringen av personopplysningene på internett var nødvendige for å oppnå formålet, var EU-domstolen derimot langt mer kritiske. I nødvendighetskravet ligger det at man vurderer om målsetningen kunne vært oppnådd gjennom mindre inngripende tiltak, også om disse er mer ressurskrevende å gjennomføre.¹²³

120 Fredriksen og Mathisen (2018) s. 119.

121 Sak C-184/20, avsnitt 75-77.

122 Sak C-184/20, avsnitt 83.

123 Fredriksen og Mathisen (2018) s. 121.

I dommen påpeker EU-domstolen at nødvendighetskravet må ses i sammenheng med dataminimeringsprinsippet i GDPR artikkel 5 (1) bokstav c, og kritiserer at den litauiske lovgivningsmyndigheten ikke har undersøkt om publisering av personopplysningene med ubegrenset tilgang for tredjeparter er strengt nødvendig, eller om formålene kan oppnås like effektivt dersom kun en begrenset personkrets har tilgang på informasjonen.¹²⁴ Det er verdt å merke seg at domstolen her trekker et skille i behandlingsaktiviteter mellom innsamlingen av personopplysningene og publiseringen på internett. Ifølge domstolen kan en behandling i form av innsamling av personopplysninger som gjør det mulig å identifisere den opplysningspliktige og opplysninger om virksomheten til personens ektefelle i en interesseerklæring være hensiktsmessig. Imidlertid strekker det seg utover det strengt nødvendige når man foretar en behandling der man offentliggjør og publiserer navnet til den opplysningspliktiges ektefelle på internett. Med henvisning til generaladvokatens innstilling bemerker domstolen dessuten at målsetningen kunne være oppnådd gjennom et mindre inngripende tiltak, f. eks ved å oppgi et generisk navn på ektefellen.¹²⁵

I interesseavveiningen ser EU-domstolen på alvorligheten av inngrepet i den enkeltes personvern og veier det opp mot formålet med tiltaket. Her påpeker domstolen at i avgjørelsen av hvor inngripende tiltaket er for retten til personvern, må man vurdere «[...] the nature of the personal data at issue, in particular of any sensitivity of those data, and of the nature of, and specific methods for, the processing of the data at issue, in particular of the number of persons having access to those data and the methods of accessing them».¹²⁶

Personvernulempene knyttet til offentliggjøring av opplysningene på nett som domstolen trekker frem i denne vurderingen har alle en side til dataminimeringsprinsippet i GDPR. For det første er offentliggjøringen av navn egnet til å avsløre meget sensitive opplysninger om den registrertes privatliv, slik som seksuell legning. Domstolen fremhever også hvordan

124 Sak C-184/20, avsnitt 92 og 93.

125 Sak C-184/20, avsnitt 96.

126 Sak C-184/20, avsnitt 99.

krenkelsens alvorlighetsgrad dessuten kan forsterkes gjennom den kumulative effekten som oppstår når alle personopplysningene kombineres og slik muliggjør at tredjeparter kan danne seg et detaljert bilde av den registrertes privatliv.¹²⁷ Når opplysningene publiseres offentlig får en ubegrenset personkrets tilgang til dem og dette fører igjen til at risikoen for viderebehandling for annet enn det opprinnelige formålet øker.¹²⁸ EU-domstolen understreker spesielt hvordan personvernulemper knyttet til viderebehandling i regi av ukjente tredjeparter utgjør et alvorlig inngrep i personvernet ettersom «[...] publication of those data is liable, for example, to expose the persons concerned to repeated targeted advertising and commercial sales canvassing, or even to risks of criminal activity».¹²⁹ Publiseringsen medfører med andre ord stor risiko for misbruk og negative konsekvenser for den registrerte. Domstolens argument er her relevant å se i lys av generaladvokatens innstilling. Generaladvokaten fremhever nemlig hvordan struktureringen og aggregeringen av informasjon på internett i høy grad påvirkes av søkemotorer som muliggjør at tredjeparter får «[...] a structured overview of the information».¹³⁰ De spesifikke måtene opplysningene kan behandles på når de publiseres på internett skaper dermed store muligheter til å sammenkoble informasjon på kryss og tvers gjennom få tastetrykk.

I den endelige avveiningen av de motstående interessene, fremhever EU-domstolen at selv om det skal tas hensyn til at den allmenne interessen i at personopplysningene offentliggjøres vil variere avhengig av hvilken betydning og funksjon den registrerte har for forvaltning av offentlige midler i virksomheten, oppfyller likevel ikke publiseringen på nett av flertallet av opplysningene i interesseerklæringen kravet til forsvarlig balanse.¹³¹ Det avgjørende for EU-domstolen er at de nasjonale myndighetene ikke har gjort nok for å minske risikoen for misbruk av opplysningene og heller ikke overholder dataminimeringsprinsippet når de

127 Sak C-184/20, avsnitt 101.

128 Sak C-184/20, avsnitt 103.

129 Sak C-184/20, avsnitt 104.

130 Generaladvokatens innstilling (2021), avsnitt 78.

131 Sak C-184/20, avsnitt 112.

publiserer navnespesifikk informasjon om ektefellen. Helhetlig er det altså behandlingstypen og de store personvernulempene den medfører som blir utslagsgivende for resultatet.

4.3 Konsekvenser av dommen: En dynamisk og fleksibel tolkning av GDPR artikkel 9 (1)

Slik gjennomgangen av dommen viser foretar EU-domstolen en vid tolkning av artikkel 9 (1). På den måten sikres formålet i GDPR om å ivareta en høy beskyttelse av sensitive opplysninger, og det er grunn til å anta at den enkeltes personvernrettigheter er styrket som følge av avgjørelsen. Selv om opplysningene i erklæringen ikke omhandlet OTs seksuelle forhold eller seksuelle orientering direkte, var de likevel omfattet av «særlige kategorier» og følgelig forbudt å behandle. Det betyr at det er tilstrekkelig at man kan utlede personopplysninger av særlige kategorier på en indirekte måte for at en behandling omfattes av artikkel 9 (1). Dermed kan alminnelige personopplysninger være omfattet av særlige kategorier dersom det er mulig å dedusere seg fram til opplysninger som avslører noe om kategoriene i artikkel 9 (1). Dette medfører at svært mange behandlinger kan omfattes av artikkel 9 (1). Konklusjonen harmonerer med det mange har påpekt som en sentral tendens i EU-domstolens tolkning av GDPR, nemlig at stadig flere opplysningstyper regnes som personopplysninger.¹³²

På mange måter er avgjørelsen et uttrykk for at EU-domstolen utnytter den dynamiske og fleksible tilnærmingen det teknologinøytrale regelverket muliggjør. Ved å introdusere uttrykket «an intellectual operation involving comparison or deduction» åpnes det potensielt for at svært mange typer behandlinger der særlige kategorier personopplysninger utledes på en indirekte måte vil være omfattet av art. 9 (1) i fremtiden. En måte å forstå uttrykket på, er å se det i lys av definisjonen av «identifiable natural person» i art. 4 (1) GDPR slik generaladvokaten gjør i sin innstilling.¹³³ Poenget her er at identifikasjon kan skje både

¹³² Purtova (2018) s. 40.

¹³³ Generaladvokatens innstilling (2021), avsnitt 87.

direkte og indirekte gjennom sammenstillingen av mange identifikatorer, og den samme logikken man bruker i spørsmålet om hva som utgjør alminnelige personopplysninger, vil kunne anvendes på spørsmålet om særlige kategorier personopplysninger.

Men hvilken overføringsverdi har dommen til andre tilfeller der det kan utledes personopplysninger av særlige kategorier på en indirekte måte? Dersom man ser domstolens vurderinger i lys av rettskildene som er blitt gjennomgått tidligere i oppgavens kapittel tre, ser man at EU-domstolen ikke tar hensyn til at den etiske kommisjonens behandlingsformål ikke var knyttet til artikkel 9 (1), og at den etiske kommisjonens intensjon heller ikke var å behandle artikkel 9-opplysninger. For det første tilsier dette at EU-domstolen tar til orde for et sterkt beskyttelsesregime for artikkel 9-opplysninger. For det andre tilsier det at formålet med behandlingen ikke er et gjeldende kriterium alene for å avgrense hvilke behandlinger av personopplysninger som faller innenfor artikkel 9 (1). Dersom den etiske kommisjonen skulle behandlet opplysningene i den aktuelle saken måtte de trolig basert seg på et av de rettslige grunnlagene i artikkel 9 (2). Unntaket i GDPR artikkel 9 (2) bokstav g for «substantial public interest» kunne for eksempel vært aktuelt.

Konsekvensene av et styrket beskyttelsesregime for artikkel 9-opplysninger, er at den behandlingsansvarlige sannsynligvis må vurdere den totale informasjonmengden som behandles uavhengig av hva formålet med behandlingen er. I alle fall er oppfordringen til å foreta en slik vurdering styrket i lys av EU-domstolens konklusjoner i dommen. Det betyr at selv om formålet bare er å behandle alminnelige personopplysninger, må den behandlingsansvarlige likevel være bevisst på risikoen for at artikkel 9-opplysninger kan deduseres ut fra all informasjonen som allerede behandles og vurdere mulighetene for at slike opplysninger kan utledes. Dette har en klar side til dataminimeringsprinsippet som krever at man kun innhenter, lagrer og behandler opplysninger i den grad det er nødvendig for å oppnå formålet. Kravene til risikovurderinger for behandlingsansvarlige er dermed trolig skjerpet, og konteksten ved behandlingssituasjonen må hensyntas. Kanskje skal det mindre til for at man regner en behandlingsaktivitet for å medføre høy risiko for de registrertes rettigheter og friheter slik at det må gjennomføres en vurdering av personvernkonsekvenser (DPIA) etter GDPR artikkel 35 fremfor en alminnelig risikovurdering etter GDPR artikkel 32. Den behandlingsansvarlige må altså vurdere både opplysningene som eksplisitt behandles og opplysningene som implisitt behandles. Hvis dommen tjener som eksempel er den eksplisitte

informasjonen navnet på OT og ektefellens navn, mens den implisitte informasjonen er sammenstillingen av to navn som det kan utledes informasjon om kjønn og legning fra.

4.3.1 Skjerpet ansvar ved behandling som involverer publisering og offentliggjøring på internett

Med henblikk på at indirekte identifisering av særlige kategorier kan skje på flere måter, både ved at opplysninger knyttes til en person gjennom flere ledd eller gjennom sammenstilling av opplysninger fra mange kilder, er det imidlertid uklart ut fra dommen hvor grensen skal trekkes for når den indirekte identifiseringen blir for fjern. I dommens saksforhold var det ikke nødvendig med noen avansert behandling av informasjonen for at tredjeparter skulle klare å utlede opplysninger om seksuell orientering. Det kreves ikke spesielt omfattende innsats for å anta at OT og partneren var homofile, og en enkel lesning av navnene i sammenheng var tilstrekkelig for å utlede informasjonen. Selv om domstolen understreker de alvorlige personvernulempene knyttet til den offentlige publiseringen av ektefellens navn fordi det gir tredjeparter tilgang til sensitiv informasjon, kan man derfor spørre hvor langt ansvaret overfor tredjeparter strekker seg.

Ut fra hvordan EU-domstolen ordlegger seg i begrunnelsen når den uttaler at publiseringen på nettsiden må tolkes slik at «[...] personal data that are liable to disclose indirectly the sexual orientation of a natural person constitutes processing of special categories of personal data» er det tilstrekkelig at muligheten til å indirekte utlede personopplysninger av særlige kategorier for tredjeparter er til stede.¹³⁴ Vurderingen må trolig gjøres konkret i den enkelte sak, og måten opplysningene behandles på har stor betydning for vurderingen. Dommen gir holdepunkter for at den behandlingsansvarliges ansvar er spesielt skjerpet i tilfeller der det er tale om publisering og offentliggjøring på internett. Fordi opplysningene som avslører sensitiv informasjon blir tilgjengelig for en ubegrenset personkrets når opplysningene publiseres på internett, er risikoen for negativ påvirkning for den registrerte større enn i mange andre

¹³⁴ Sak C-184/20, avsnitt 128.

behandlinger ettersom mulighetene for bruk i andre behandlinger til andre formål av andre aktører er stor.

Artikkel 29-gruppen har tidligere uttalt at i tilfeller der personopplysninger tilgjengeliggjøres for en stor personkrets eller når store mengder personopplysninger behandles eller kombineres med annen informasjon i stor skala slik at det kan utledes flere sensitive opplysninger kan dette «[...] lead to uncanny, unexpected, and sometimes also inaccurate predictions, for example, concerning the behaviour or personality of the individuals concerned».¹³⁵ Dette er spesielt aktuelt når artikkel 9-opplysninger offentliggjøres på internett. Det skapes en uoversiktlig situasjon for den registrerte, og det kan oppstå svært mange situasjoner der tredjeparter i teorien kan utøve handlinger og ta beslutninger som påvirker den registrertes rettigheter og friheter i større eller mindre grad. I dommen nevnes risikoen for at viderebehandling skjer f. eks gjennom målrettet reklame,¹³⁶ og i slike tilfeller mister den registrerte muligheten til å samtykke, protestere på behandlingen og ellers utøve rettighetene sine i tråd med GDPR fordi vedkommende ikke er informert om at behandlingen skjer. Generelt kan det argumenteres for at risikoen for negativ påvirkning og negative konsekvenser for den registrerte er store ved internettpublisering av personopplysninger av særlige kategorier.

En uavklart spørsmål er imidlertid hvilke konsekvenser EU-domstolens løsning av rettsspørsmålet i dommen har for behandlingen av eksempelvis video og bilder, samt biometriske opplysninger. Slik gjennomgangen i kapittel tre har vist, tilsier Personvernrådets retningslinjer at behandlingsformål er et relevant avgrensningskriterium for å avgjøre når videoer og bilder omfattes av artikkel 9 (1). I lys av den vide tolkningen til EU-domstolen kan man imidlertid spørre om også bilder og video som avslører noe som kan knyttes til de særlige kategoriene i artikkel 9 (1) har fått et sterkere vern. I så fall innebærer det at behandlingsansvarlige oftere enn før må ta utgangspunkt i at publisering av slike bilder er

135 A29WP 06/2014 s. 39.

136 Sak C-184/20, avsnitt 128.

forbudt med mindre den registrerte f. eks gir samtykke i tråd med unntaket for behandling i artikkel 9 (2) bokstav a. Det er nærliggende å anta at Personvernrådet vil følge opp med en avklaring av spørsmålene i nye retningslinjer i framtiden.

Til tross for at saksforholdet i dommen gjaldt en offentlig aktør og en privatperson, er EU-domstolens standpunkt i dommen naturlig å betrakte i lys av den utstrakte og voksende bruken av analyser av Big Data¹³⁷ de siste årene blant store private aktører i form av internettplattformer som Facebook, Google, Microsoft og Twitter.¹³⁸ Facebook kan ut fra opplysningene de har tilgang til være i stand til å utlede alt fra forestående selvmordsforsøk til seksuell legning, politiske meninger og andre artikkel 9-opplysninger, mens tredjeparter på sin side har brukt opplysninger fra Facebook til å bestemme hvorvidt kunder er kvalifisert til å få lån, og til å kartlegge holdninger til abort.¹³⁹ Selv om Big Data stort sett går ut på å analysere anonyme eller anonymiserte data, vil det likevel ofte være risiko for reidentifisering slik at anonymiserte data reverseres til identifiserende opplysninger som direkte eller indirekte kan knyttes til en enkeltperson.¹⁴⁰ Sett i lys av de mange uoversiktlige personvernkonsekvensene som kan oppstå i kjølvannet av en slik utvikling, åpner EU-domstolens vide tolkning av GDPR artikkel 9 (1) for en rettsutvikling som strammer grepet for hva som utgjør lovlig behandling av personopplysninger.

137 Big Data er store og komplekse datasett og refererer både til dataene i seg selv og aktiviteten knyttet til å samle inn, lagre og analysere dem. I takt med stadig mer avansert teknologi blir mulighetene for sammenstilling av opplysninger større og flere, jf. Datatilsynet (2013) s. 7.

138 For eksempel har de irske datatilsynsmyndighetene ilagt Facebook og Instagram et overtredelsesgebyr på 390 millioner euro for brudd på GDPR, se <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/overtredelsesgebyr-til-facebook-og-instagram/>

139 Wachter og Mittelstadt (2019) s. 506-507.

140 Datatilsynet (2013) s. 8.

5. Konklusjon

I denne oppgaven har jeg undersøkt hvilke personopplysninger som omfattes av GDPR artikkel 9 (1) og hvilken rekkevidde bestemmelsen har. Etter introduksjonen i kapittel en, redegjorde jeg i kapittel to for GDPR og alminnelige personopplysninger, før jeg rettet blikket mot særlige kategorier personopplysninger generelt, historikken bak tilblivelsen til særlige kategorier, og ga et riss av sentrale hensyn bak GDPR artikkel 9 (1).

I det tredje kapittelet foretok jeg en analyse av den nærmere rekkevidden av artikkel 9 (1). Jeg kom frem til at utgangspunktet etter ordlyden, formål og uttalelser fra Artikkel 29-gruppen er at bestemmelsen skal tolkes vidt. Deretter viste jeg hvordan spesielt særlige kategorier personopplysninger av indirekte karakter kan være vanskelig å trekke de nærmere grensene for, og drøftet hvordan personopplysninger i form av bilder og video skaper utfordringer i anvendelsen av artikkel 9 (1). Videre diskuterte jeg ulike uttalelser fra Personvernrådet og undersøkte hvordan behandlingsformål har blitt brukt som avgrensningskriterium for artikkel 9-opplysninger av indirekte karakter. Deretter redegjorde jeg for henholdsvis formålstolkning og en kontekstbasert tilnærming som alternativer i vurderingen av hva som utgjør artikkel 9-opplysninger.

I kapittel fire foretok jeg en analyse av EU-domstolens avgjørelse C-184/20 og drøftet hvilke konsekvenser dommen har for rekkevidden og tolkningen av artikkel 9 (1). Mine hovedfunn var at EU-domstolen foretar en vid tolkning av artikkel 9 (1), og på den måten sikrer formålet i GDPR om å ivareta en høy beskyttelse av sensitive opplysninger. EU-domstolens standpunkt innebærer at personopplysninger kan være omfattet av særlige kategorier dersom det er mulig å dedusere seg fram til opplysninger som avslører noe om en av kategoriene i artikkel 9 (1).

På bakgrunn av dette kom jeg fram til at den enkeltes personvernrettigheter er styrket som følge av avgjørelsen. Gjennom min lesning av dommen konkluderte jeg med at formålet med behandlingen ikke i seg selv er tilstrekkelig for å avgrense hvilke behandlinger av personopplysninger som faller innenfor art. 9 (1), og at konsekvensene av dommen sannsynligvis er en generell skjerpelse av de behandlingsansvarliges plikter etter GDPR. Jeg påpekte at dommens rekkevidde er noe usikker på flere punkter, men at den alt i alt må forstås

i lys av EUs forsøk på å adressere trusselen de siste årenes enorme teknologiske utvikling gjennom blant annet Big Data utgjør for den enkeltes personvern.

6 Litteraturliste

6.1 Norske lover og forarbeider

EØS-LOVEN	Lov 27.november 1992 om nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven eller EØSl.)
NOU 1997:19	NOU 1997:19 Et bedre personvern – forslag til lov om behandling av personopplysninger
NOU 2022:11	NOU 2022:11 Ditt personvern – vårt felles ansvar

6.2 EU-rettsakter og avtaler

EUs charter om grunnleggende rettigheter	Charter on the Fundamental Rights of the European Union, 18.12.2000, 2000/C 364/01
DIREKTIV 95/46/EF	Europaparlamentets- og Rådsdirektiv 95/46/EF av 24.oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, EUT L 281/31, 23.11.1995
GDPR	Europaparlamentets- og Rådsforordning (EU) 2016/579 av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [GDPR], EUT L 119/1, 04.05.2016

6.3 Rettspraksis fra EU-domstolen og generaladvokatens innstillinger

Sak C-184/20	Dom av 1. august 2022 [GC], <i>OT v Vyriausioji tarnybinės etikos komisija</i> , C-184/20, ECLI:EU:C:2022:601.
Sak C-436/16 Peter Nowak	Dom av 20. desember 2017 [C3], <i>Peter Nowak v Data Protection Commissioner</i> , C-434/16, ECLI:EU:C:2017:994.
Sak C-101/01 <i>Bodil Lindqvist</i>	Dom av 6. november 2003, Criminal proceedings against Bodil Lindqvist, C-101/01, ECLI:EU:C:2003:596.
Sak C-582/14 <i>Breyer</i>	Dom av 19. oktober 2016, <i>Patrick Breyer v Bundesrepublik Deutschland</i> , C-582/14, ECLI:EU:C:2016:779.
Generaladvokatens innstilling (2021)	Opinion of Advocate General P. Pikamäe delivered on 9 December 2021. Case C-184/20 OT v Vyriausioji tarnybinės etikos komisija. EU:C:2021:991

6.4 Veiledere, uttalelser og rapporter

- A29WP Opinion 4/2007 Article 29 Data Protection Working Party «Opinion 4/2007 on the concept of personal data», 01248/07/EN WP 136 [Tilgjengelig på: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm] (lest 05.01.23)
- A29WP Opinion 04/2011 Article 29 Data Protection Working Party «Advice paper on special categories of data (“sensitive data”) 04/2011» [Tilgjengelig på: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf] (lest 04.01.23)
- A29WP Opinion 06/2014 Article 29 Data Protection Working Party «Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC», **844/14/EN WP 217** [Tilgjengelig på: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm] (lest 03.01.23)
- Datatilsynet (2013) Datatilsynet. *Big Data – personvernprinsipper under press.* 2013. [Tilgjengelig på: <https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/big-data/>] (lest 03.02.23)

- Europarådet (1981) Concil of Europe «Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data», Strasbourg, 28.I.1981, [Tilgjengelig på: [https://rm.coe.int/16800ca434.](https://rm.coe.int/16800ca434)] (lest 12.01.23)
- Personvernrådet 3/2019 European Data Protection Board «Guidelines 3/2019 on processing of personal data through video devices Version 2.0», [Tilgjengelig på: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm] (lest 07.01.23)
- Personvernrådet 8/2020 European Data Protection Board «*Guidelines 8/2020 on the targeting of social media users* Version 2.0» [Tilgjengelig på: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en] (lest 02.01.23)
- Simitis (1999) Mr. Spiros Simitis «Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24-26 November 1999). [Tilgjengelig på: <https://rm.coe.int/09000016806845af>] (lest 06.01.23)

6.5 Juridisk litteratur

6.5.1 Bøker

- Fredriksen og Mathisen (2018) Fredriksen, Halvard Haukeland, og Gjermund Mathisen. *EØS-rett*. 3. utgave. Bergen: Fagbokforlaget, 2018.

- Kuner mfl. (2020) Drechsler, Laura, Christopher Kuner, Lee A. Bygrave og Christopher Docksey. *The EU General Data Protection Regulation (GDPR) : A Commentary*. Oxford: Oxford University Press, 2020.
- Schartum (2020) Schartum, Dag Wiese. *Personvernforordningen : En Lærebok*. 1. utgave. Bergen: Fagbokforlaget, 2020.
- Schartum og Bygrave (2016) Schartum, Dag Wiese, og Lee A. Bygrave. *Personvern i informasjonssamfunnet : En Innføring i vern av personopplysninger*. 3. utgave. Bergen: Fagbokforlaget, 2016.
- Wessel-Aas og Ødegaard (2018) Wessel-Aas, Jon, og Magnus Ødegaard. *Personvern : Publisering og behandling av personopplysninger*. 1. utgave. Oslo: Gyldendal, 2018.

6.5.2 Artikler

- Hallinan og Borgesius (2020) Hallinan, Dara og Frederik Zuiderveen Borgesius. "Opinions Can Be Incorrect (in Our Opinion)! On Data Protection Law's Accuracy Principle." *International Data Privacy Law* 10, no. 1 (2020): 1-10.
- Purtova (2018) Purtova, Nadezhda. "The Law of Everything.: Broad Concept of Personal Data and Future of EU Data Protection Law." *Law, Innovation and Technology* 10, no. 1 (2018): 40-81.
- Quinn og Malgieri (2021) Quinn, Paul, og Gianclaudio Malgieri. "The Difficulty of Defining Sensitive Data—The Concept of Sensitive

Data in the EU Data Protection Framework." *German Law Journal* 22, no. 8 (2021): 1583-1612.

Wachter og Mittelstadt (2019) Wachter, Sandra, og Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review* 2019, no. 2 (2019): 494.

6.6 Øvrige kilder

6.6.1 Internasjonale traktater

Europarådets
personvernkonvensjon (1981) Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Strasbourg, 28.januar 1981 (CETS no. 108)

6.6.2 Nettsider

Datatilsynet, «Overtredelsesgebyr til Facebook og Instagram», 05.01.23, <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2023/overtredelsesgebyr-til-facebook-og-instagram/> (lest 07.05.23).

Datatilsynet, «Vurdering av personvernkonsekvenser og forhåndsdrøftelse», 17.07.2019, <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-er-risiko-hoy/> (lest 26.04.23).

Michelle Boorstein og Heather Kelly, «Catholic group spent millions on app data that tracked gay priests», The Washington Post, 09.03.23, <https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/>, (lest 05.05.23).