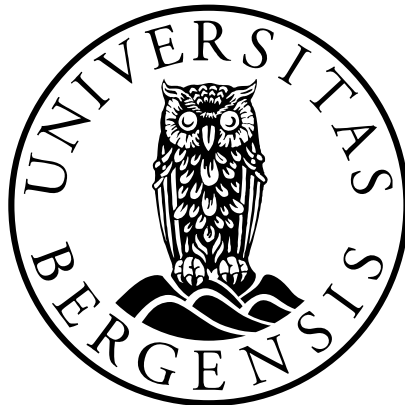


Formålsbegrensningsprinsippet i GDPR

*I hvilken grad kan personopplysninger
viderebehandles for andre formål enn
opprinnelig formål?*

Kandidatnummer: 142

Antall ord: 14802



JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. desember 2020

Innholdsfortegnelse

Innholdsfortegnelse.....	1
1 Innledning.....	3
1.1 Tema og problemstilling.....	3
1.2 Temaets aktualitet.....	4
1.3 Rettskilder og metode.....	6
1.4 Avgrensninger.....	10
1.5 Den videre fremstillingen.....	11
2 Personvernforordningen.....	13
2.1 Personvernforordningen og dens bakteppe.....	13
2.2 Grunnleggende prinsipper for behandlingen av personopplysninger.....	14
2.3 Kravet til behandlingsgrunnlag.....	16
3 Formålsbegrensningsprinsippet.....	18
3.1 Formålsbegrensningsprinsippet i en internasjonal kontekst.....	18
3.2 Formålsbegrensningsprinsippet i personvernforordningen.....	19
3.3 Formålsbegrensningsprinsippetets begrunnelse.....	21
3.4 Prinsippetets første del: personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål.....	22
3.4.1 Innledende.....	22
3.4.2 Formålet skal være spesifikt.....	23
3.4.3 Formålet skal være uttrykkelig angitt.....	24
3.4.4 Formålet skal være berettiget.....	25
3.5 Prinsippetets andre del: personopplysninger skal ikke viderebehandles på en måte som er uforenlig med formålene.....	26
4 Når er viderebehandling av personopplysninger «uforenlig» med opprinnelig formål?.....	28
4.1 Innledende om vilkåret og vurderingen.....	28
4.2 Presentasjon av personvernforordningen artikkel 6 nr. 4.....	29
4.3 Foreløpig oppsummering.....	31
4.4 Vurderingsmomentene i bokstav a-e.....	32
4.4.1 Bokstav a – forbindelsen mellom formålene.....	32
4.4.2 Bokstav b – konteksten for innsamlingen.....	33
4.4.3 Bokstav c – personopplysningenes art.....	34

4.4.4	Bokstav d – mulige konsekvenser.....	35
4.4.5	Bokstav e – sikkerhetstiltak	36
4.4.6	Oppsummering av artikkel 6 nr. 4	38
4.5	Rettspraksis som belyser adgangen til viderebehandling	40
4.6	Øvrig praksis som belyser adgangen til viderebehandling	44
5	Særlig om viderebehandling i Big data-sammenheng	47
6	Avsluttende betraktninger	50
7	Litteraturliste	52
7.1	Direktiver og forordninger	52
7.2	Traktater, konvensjoner m.m.	52
7.3	Norske lover og forskrifter.....	53
7.4	Lovforarbeider	54
7.5	Rettspraksis.....	54
7.5.1	Rettspraksis fra EU-domstolen	54
7.5.2	Rettspraksis fra Den europeiske menneskerettighetsdomstolen	54
7.5.3	Norsk rettspraksis.....	54
7.6	Veiledere	55
7.7	Praksis fra nasjonale tilsynsmyndigheter	55
7.8	Juridisk litteratur	56
7.9	Andre kilder	57
7.9.1	Artikler	57
7.9.2	Internettkilder.....	58
7.9.3	Rapporter.....	59
7.9.4	Offentlige dokumenter	59

1 Innledning

1.1 Tema og problemstilling

Temaet for oppgaven er formålsbegrensningsprinsippet i General Data Protection Regulation¹ (heretter «GDPR», «personvernforordningen» eller «forordningen») og hvilke føringer dette prinsippet legger for behandlingen av personopplysninger. Prinsippet fremgår av GDPR artikkel 5 nr. 1 bokstav b. Det innebærer for det første at personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål. Videre går prinsippet ut på at personopplysninger ikke skal viderebehandles på en måte som er uforenlig med disse formålene.² Formålsbegrensningsprinsippet kan dermed deles inn i to komponenter: kravet til formålsspesifisering og forbudet mot uforenlig viderebehandling.³ GDPR artikkel 6 nr. 4 gir ytterligere veiledning for adgangen til viderebehandling av personopplysninger, herunder vurderingsmomenter som skal inngå i en uforenlighetsvurdering.

Problemstillingen for oppgaven er i hvilken grad personopplysninger kan viderebehandles for andre formål enn det formålet eller de formålene som opplysningene opprinnelig ble hentet inn for. Oppgavens hovedfokus er dermed den delen av formålsbegrensningsprinsippet som knytter seg til viderebehandling av personopplysninger, herunder vilkåret *uforenlig*.

Oppgaven omhandler formålsbegrensningsprinsippet slik det kommer til uttrykk i personvernforordningen. Forordningen er EUs sentrale personvernregelverk. Den ble ansett EØS-relevant og ble inntatt i EØS-avtalen 20. juli 2018.⁴ Forordningen gir et sett med regler som regulerer behandlingen og utvekslingen av personopplysninger. Etter forordningen skal personopplysninger forstås som «enhver opplysning om en identifisert eller identifiserbar fysisk person».⁵ Definisjonen innebærer at forordningen har et bredt anvendelsesområde. Personopplysninger kan være alt fra opplysninger om noens hjemmeadresse og

¹ Europaparlamentets og Rådets forordning (EU) 2016/679 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].

² GDPR artikkel 5 nr. 1 bokstav b. Den engelske versjonen lyder som følger: «Personal data shall be ... collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes».

³ A29 WP Opinion 03/2013 on purpose limitation, s. 3. Inndelingen benyttes også av Christopher Kuner mfl., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press 2020, s. 315.

⁴ EØS-komiteen, Decision of the EEA Joint Committee No 154/2018 of 6 July 2018.

⁵ GDPR artikkel 4 nr. 1.

telefonnummer til opplysninger om bevegelsesmønstre og kjøpevaner. Samtidig innebærer definisjonen at opplysninger som ikke kan knyttes til et individ, som anonymiserte opplysninger, ikke reguleres av forordningen.⁶ Formålet med GDPR er å sikre et effektivt vern av personopplysninger samt å tilrettelegge for fri flyt av personopplysninger i EU og EØS.⁷ Forordningen setter en høy standard for vern av personopplysninger, og formålsbegrensningsprinsippet er en viktig komponent for å sikre denne høye graden av vern. Personvernforordningen vil bli nærmere redegjort for i oppgavens del to.

Formålsbegrensningsprinsippet er ett av flere prinsipper i personvernforordningen som er bestemmende for behandlingen av personopplysninger.⁸ Disse prinsippene er vidt formulert og har vesentlig betydning for all behandling av personopplysninger. Fastlegging av prinsippenes eksakte innhold og rekkevidde kan imidlertid by på utfordringer.⁹ Oppgaven tar sikte på å bidra til avklaring av formålsbegrensningsprinsippet, som ett av disse prinsippene.

1.2 Temaets aktualitet

Personvern og regelverket for ivaretagelsen av personvern er et svært aktuelt tema. Som følge av den teknologiske utviklingen samles og behandles personopplysninger i massiv skala.¹⁰ Internettøkonomien bygger i stor utstrekning på at individer deler opplysninger om seg selv i bytte mot tilgang til tilsynelatende gratis digitale tjenester¹¹ og personopplysninger selges på lik linje med andre handelsvarer.¹² Det enorme omfanget av personopplysninger i omløp nødvendiggjør rettslig regulering av all behandling av personopplysninger. I EU- og EØS er GDPR nåtidens viktigste svar på disse utfordringene.¹³ Andre EU-rettslige rettsakter samt nasjonal lovgivning gir også viktige bidrag innen personvernrettens område gjennom ulike regler knyttet til behandlingen av personopplysninger.¹⁴

⁶ GDPR fortalepunkt 26 nr. 5.

⁷ GDPR artikkel 1.

⁸ Prinsippene fremgår av GDPR artikkel 5.

⁹ Det var lenge uklarerhet knyttet til innholdet i og rekkevidden av formålsbegrensningsprinsippet, med uensartet praktisering av prinsippet blant de ulike EU- og EØS-landene. Denne tematikken behandles nærmere i oppgavens punkt 3.2.

¹⁰ GDPR fortalepunkt 6.

¹¹ Lee A Bygrave, *Data Privacy Law: An International Perspective*, Oxford University Press 2014, s. 5.

¹² Jon Wessel-Aas og Magnus Ødegaard, *Personvern – publisering og behandling av personopplysninger*, Gyldendal 2018, s. 5.

¹³ Alle EUs medlemsland samt EØS-landene Island, Liechtenstein og Norge er tilsluttet GDPR.

¹⁴ Ett eksempel er Direktiv (EU) 2016/680 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av

En særlig utfordring ved vernet av personopplysninger er at slike opplysninger behandles for uendelig mange ulike formål. Eksempelvis vil det være avgjørende å ha tilgang til opplysninger om noens helse- og sykdomshistorikk i behandlingssammenheng, samtidig som slike opplysninger også kan være relevante ved beregningen av prisen for en helseforsikring. Formålsutglidning er fenomenet der personopplysninger benyttes til andre formål enn hva de opprinnelig var myntet på. Et viktig aspekt ved personvernregelverket er derfor formålsbegrensning, som handler om å sikre forutberegnelighet om hvilke formål personopplysninger benyttes til.¹⁵ Formålsbegrensning kan hevdes å være særlig viktig på bakgrunn av den teknologiske utviklingen og muligheten for å sammenstille og bruke enorme mengder personopplysninger i såkalt Big data-sammenheng. Big data kan defineres som store mengder digitale data, både i strukturert og ustrukturert form, som blir analysert for å identifisere trender og sammenhenger.¹⁶ Nye analyseverktøy gjør det mulig å sammenstille og finne relevante og betydningsfulle sammenhenger mellom enda større samlinger av data enn tidligere.¹⁷ Slike sammenstillinger kan være svært hensiktsmessige, eksempelvis i forskningssammenheng, men kan samtidig innebære en risiko for at individet mister kontrollen over personopplysningene sine.

En rekke saker fra nyhetsbildet illustrerer at formålsbegrensning er et viktig ledd i ivaretagelsen av personvernet. I mai 2020 publiserte NRK artikkelen «Avslørt av mobilen», som resultat av et omfattende journalistisk arbeid med å kartlegge fenomenet mobilsporing.¹⁸ I artikkelen avdekkes det at en rekke mobilapplikasjoner som benytter brukerens posisjonsdata selger disse dataene videre til såkalte dataforhandlere, som deretter samler og videreselger dataene til både kommersielle aktører og myndigheter. I slike tilfeller er det nærliggende å anta at brukerne av mobilappene har samtykket til at appen benytter stedtjenester, men ikke til videresalg av disse dataene. I sitt arbeid avdekket NRK at det ved kjøp av kartkoordinater som var tilknyttet en dato, et klokkeslett og en bestemt mobil lot seg gjøre å spore enkeltindivider, selv om posisjonsdataene i utgangspunktet var anonymiserte. Dermed fikk ukjente aktører muligheten til å kartlegge bevegelsesmønstre helt ned på individnivå. Saken er ett av flere eksempler som illustrerer hvorfor det er viktig at aktører som

straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning 2008/977/JIS.

¹⁵ A29 WP Opinion 03/2013, s. 4.

¹⁶ <https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/> (sist besøkt 10.11.20).

¹⁷ Bygrave (2014) s. 153.

¹⁸ <https://www.nrk.no/norge/xl/avslort-av-mobilen-1.14911685> (sist besøkt 21.11.20).

samler inn personopplysninger pålegges å angi hvilke formål opplysningene hentes inn for, samt at de forbyr å benytte opplysningene til formål som ikke er i samsvar med disse.

Et annet eksempel som illustrerer aktualiteten av formålsbegrensning er debatten rundt den mye omtalte smittesporingsappen Smittstopp lansert i april 2020 som ledd i bekjempelsen av koronapandemien.¹⁹ Faren for formålsutglidning var en av flere innvendinger som ble fremlagt i debatten om hvorvidt appen var problematisk fra et personvernrettslig perspektiv. Bekymringen var at myndighetene potensielt kunne bli fristet til å bruke innbyggernes lokasjonsdata for andre formål enn de tiltenkte formålene.²⁰

Selv om personvern er å regne som en grunnleggende verdi i samfunnet er ikke personvern en absolutt rettighet. Hensynet til vern av personopplysninger må balanseres mot andre grunnleggende rettigheter og øvrige interesser i samfunnet.²¹ Personvern og ytringsfrihet er et eksempel på to rettigheter som kan stå i et spenningsforhold.²² En vid ytrings- og informasjonsfrihet anses som en forutsetning for et fungerende demokrati. Samtidig forutsetter et fungerende demokrati også at den enkelte borger har en beskyttet privatsfære.²³ Denne avveiningen mellom vernet av individers personvern og ivaretagelsen av andre interesser og hensyn kan også identifiseres i formålsbegrensningsprinsippet. Det gjelder nemlig ikke noe absolutt forbud mot viderebehandling av personopplysninger for andre formål enn det opprinnelige formålet. Dette tilsier at de ulike interessene som kan tale for viderebehandling også anses relevante og verdifulle. Den videre fremstillingen tar sikte på å illustrere *hvordan* denne avveiningen mellom hensynet til den registrerte og andre interesser skal foretas, gjennom uforenlighetsvurderingen.

1.3 Rettskilder og metode

Oppgavens problemstilling gjelder rekkevidden av formålsbegrensningsprinsippet i personvernforordningen. Personvernforordningen er derfor den primære rettskilden i oppgaven. Ettersom rettsakten er gitt i form av en forordning, har den direkte virkning i alle

¹⁹ <https://www.fhi.no/nyheter/2020/ny-app-fra-folkehelseinstituttet/> (sist besøkt 25.11.20).

²⁰ Se eksempelvis <https://www.aftenposten.no/meninger/kronikk/i/GGLLVm/vi-maa-velge-mellom-pest-og-kolera-appen-smittestopp-kan-vaere-en-midde> og <https://agendamagasinet.no/kommentarer/bekjempe-pandemi-finner-app/> (begge sist besøkt 25.11.20).

²¹ GDPR fortalepunkt 4.

²² Wessel-Aas (2018) s. 35.

²³ Wessel-Aas (2018) s. 44.

EUs medlemsland.²⁴ EU-lovgivning i forordnings form innebærer nemlig at alle medlemslandene følger helt likelydende bestemmelser. Dette ble ansett fordelaktig ved innføringen av et nytt personvernregelverk i EU for å sikre en mest mulig harmonisert og ensartet regulering av personvernreglene innenfor EU og EØS.²⁵

Personvernforordningen er inntatt i EØS-avtalen og «gjelder som lov» etter personopplysningsloven § 1.²⁶ Den norske oversettelsen av personvernforordningen vil benyttes i oppgaven.

Rettskildebildet for øvrig preges av at personvernforordningen er en relativ fersk rettsakt. Som jeg kommer tilbake til i oppgavens del 2, er imidlertid deler av personvernforordningen en videreføring av tilsvarende reguleringer i det tidligere personverndirektivet.²⁷ Dette gjelder blant annet formålsbegrensningsprinsippet. Dermed kan kilder som var av relevans for tolkningen av formålsbegrensningsprinsippet i personverndirektivet, som avgjørelser fra EU-domstolen samt tidligere uttalelser fra Artikkel 29-gruppen, også være relevante i GDPR-sammenheng.²⁸ Artikkel 29-gruppens funksjon forklares nærmere senere i underkapittelet.

Ved at personvernforordningen er en EU-rettsakt, må den tolkes i tråd med EUs tolkningslære. Utgangspunktet for tolkningen er ordlyden.²⁹ EU-lovgivningen eksisterer imidlertid på alle EUs 24 offisielle språk, hvilket medfører en risiko for at forskjellige versjoner kan gi grunnlag for ulike tolkninger. Både kontekst og formål er derfor særlig viktige tolkningsbidrag ved fortolkning av EU-rettslige bestemmelser.³⁰ Av den grunn er personvernforordningens fortale et sentralt tolkningsbidrag for oppgaven.

Personvernforordningens fortale består av 173 fortalepunkt. Den gir anvisning på hva forordningens overordnede formål er, i tillegg til å forklare de enkelte artiklene nærmere.³¹ Fortalen er ikke rettslig bindende,³² og har derfor som utgangspunkt begrenset rettskildemessig verdi. Den vil likevel fungere som et støttemoment, særlig ved mangel på

²⁴ Halvard Haukeland Fredriksen og Gjermund Mathisen, *EØS-rett*, 3. utg., Fagbokforlaget 2018, s. 28.

²⁵ GDPR fortalepunkt 10.

²⁶ Lov 15. juni 2018 nr. 38 om behandling av personopplysninger.

²⁷ Direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

²⁸ Wessel-Aas (2018) s. 128-129.

²⁹ Fredriksen (2018) s. 296.

³⁰ Fredriksen (2018) s. 298.

³¹ Fredriksen (2018) s. 305.

³² *Karen Millen Fashions [C5] C-345/13*, avsnitt 31.

andre klare kilder. Det er særlig forordningens fortalepunkt 50 om «Further Processing of Personal Data» som er av relevans for fremstillingen.

Det er The European Court of Justice (heretter «EU-domstolen») som tolker og avklarer EU-retten, herunder personvernforordningen.³³ EU-domstolens avgjørelser er derfor en sentral rettskilde. Det er imidlertid ingen avgjørelser fra domstolen som direkte bidrar til avklaring av formålsbegrensningsprinsippet rekkevidde, herunder gjennom anvendelse av de opplistede vurderingsmomentene som fremgår av personvernforordningen artikkel 6 nr. 4.

Vern av personopplysninger som en grunnleggende rettighet kommer selvsagt til uttrykk også utenfor personverndirektivet og personvernforordningen, eksempelvis i EUs pakt om grunnleggende rettigheter (heretter «EU-pakten» eller «pakten»)³⁴ og i Den europeiske menneskerettighetskonvensjonen («EMK»)³⁵. Det fremgår av EMK artikkel 8 nr. 1 at «[e]nhver har rett til respekt for sitt privatliv». Artikkelen gir ikke eksplisitt uttrykk for et vern av personopplysninger, men Den europeiske menneskerettighetsdomstolen («EMD») har lagt til grunn at behandling av personopplysninger utgjør et inngrep i retten til privatliv.³⁶ Rettspraksis fra EMD kan derfor være av relevans for oppgavens tema. Praksis fra EMD vektlegges ved tolkning og anvendelse av andre europeiske regelsett, herunder EUs regler om behandling av personopplysninger.³⁷ EU-domstolen har selv henvist til dommer avsagt av EMD i sin praksis.³⁸ Dommer der EMD indirekte eller direkte har befattet seg med formålsbegrensningsprinsippet vil derfor være relevante for fremstillingen.

Article 29 Working Party (heretter «Artikkel 29-gruppen») var EUs rådgivende organ i personvernspørsmål frem til implementeringen av personvernforordningen.³⁹ Gruppen bestod av representanter fra nasjonale tilsynsmyndigheter i medlemslandene. Norges tilsynsmyndighet på personvernområdet, Datatilsynet, var representert i gruppen. Gruppen vedtok uttalelser og anbefalinger om hvordan reglene i det daværende personverndirektivet

³³ Fredriksen (2018) s. 153.

³⁴ Charter of Fundamental rights of the European Union (2012/C 326/02).

³⁵ Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November 1950 (Den europeiske menneskerettighetskonvensjonen).

³⁶ Et eksempel er dommen *S. and Marper v. The United Kingdom* [GC] 2008 nos. 30562/04 og 30566/04: «The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8», avsnitt 67.

³⁷ Wessel-Aas (2018) s. 20.

³⁸ Ett eksempel er *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauer mann v Österreichischer Rundfunk*, C-465/00, C-138/01 and C-139/01, se avsnitt 72-73.

³⁹ Wessel-Aas (2018), s. 94.

burde etterleves og håndheves, samt uttalelser knyttet til den kommende personvernforordningen. Disse uttalelsene og veilederne er ikke juridisk bindende, men fungerer som rådgivende retningslinjer og kan dermed være relevante tolkningsbidrag.⁴⁰

Når det gjelder formålsbegrensningsprinsippet ga Artikkel 29-gruppen den 2. april 2013 en veileder kalt «Opinion 03/2013 on purpose limitation».⁴¹ Veilederen gjelder formålsbegrensningsprinsippet slik det på tidspunktet fremgikk av personverndirektivet. Veilederen redegjør for prinsippet og presiserer dets rekkevidde i tillegg til å gi anbefalinger til den da foreslåtte personvernforordningen. Ettersom personvernforordningen viderefører formålsbegrensningsprinsippet, er veilederen også relevant for formålsbegrensningsprinsippet etter forordningen.

Fra 25. mai 2018 opphørte Artikkel 29-gruppen og European Data Protection Board (heretter «EDPB» eller «Personvernrådet») overtok rollen som rådgivende organ. Datatilsynet er representert i Personvernrådet ved én representant, men uten stemmerett ettersom Norge ikke er et EU-land.⁴² Personvernrådets overordnede oppgave er å sikre ensartet anvendelse av GDPR, jf. forordningens artikkel 70. Personvernrådet har dermed i oppgave å tolke GDPR for å sikre en harmonisert forståelse av forordningen blant medlemslandene. Heller ikke Personvernrådets uttalelser eller veiledere er bindende, men kan på tilsvarende måte som for Artikkel 29-gruppen være relevante tolkningsbidrag. EDPB har gitt sin tilslutning til flere av Artikkel 29-gruppens veiledere.⁴³ Veilederen «Opinion 03/2013 on purpose limitation» er imidlertid ikke blant disse. Bakgrunnen for dette er at veilederen først og fremst tolket formålsbegrensningsprinsippet etter det daværende personverndirektivet, ikke etter den kommende personvernforordningen. Veilederen påpekte imidlertid svakheter ved formålsbegrensningsprinsippet under direktivet samt ga anbefalinger til prinsippets utforming og gjennomføring i den kommende forordningen. I tillegg er GDPR artikkel 6 nr. 4, som gir vurderingsmomenter for adgangen til viderebehandling, basert på veilederen. Retningslinjene i veilederen er derfor verdifulle.

Videre kan retningslinjer og uttalelser fra nasjonale tilsynsmyndigheter få betydning for tolkningen av forordningen. GDPR artikkel 51 pålegger hver medlemsstat å opprette

⁴⁰ Wessel-Aas (2018) s. 94.

⁴¹ A29 WP Opinion 03/2013.

⁴² https://edpb.europa.eu/about-edpb/board/members_en (sist besøkt 22.11.20).

⁴³ EDPBs nettsider angir hvilke av Artikkel 29-gruppens veiledere som er tilsluttet: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (sist besøkt 22.11.20).

uavhengige tilsynsorgan som skal føre tilsyn med at forordningen følges. Uttalelser fra slike tilsynsmyndigheter har begrenset rettskildemessig vekt, men kan likevel gi veiledning for hvordan forordningens bestemmelser skal forstås ved at de viser hvordan ulike lands tilsynsmyndigheter tolker personvernforordningen. Datatilsynet er Norges tilsynsmyndighet. Datatilsynets vedtak kan klages inn for Personvernemnda, jf. personopplysningsloven § 22. Praksis fra Datatilsynet og Personvernemnda benyttes i oppgaven.

Øvrige internasjonale regelverk, som OECD retningslinjer for beskyttelse og utveksling av personopplysninger over landegrensene («OECD-retningslinjene») og Europarådets Konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger («Europarådskonvensjonen»), vil også bli omtalt i oppgaven. Disse regelverkene gir uttrykk for et formålsbegrensningsprinsipp, og vil derfor bli benyttet for å belyse hvordan formålsbegrensningsprinsippet kommer til uttrykk utenfor personvernforordningen.

Endelig vil avgjørelser fra Norges Høyesterett bli anvendt i oppgaven. Norsk rettspraksis har ingen direkte rettskildemessig verdi for hvordan personvernforordningen skal forstås, men kan illustrere hvordan formålsbegrensningsprinsippet har blitt og blir tolket.

1.4 Avgrensninger

Oppgaven omhandler formålsbegrensningsprinsippet i personvernforordningen, med særlig vekt på prinsippets andre del, som gjelder adgangen til viderebehandling av personopplysninger. Hovedformålet med oppgaven er å vurdere i hvilken grad personopplysninger kan viderebehandles for andre formål enn det formålet opplysningene opprinnelig ble hentet inn for.

Som jeg kommer tilbake til senere i oppgaven henger flere av grunnprinsippene i personvernforordningen artikkel 5 tett sammen. Selv om formålsbegrensningsprinsippet har nær tilknytning til og kan sees i lys av enkelte andre grunnprinsipper, skal jeg i begrenset grad behandle disse i oppgaven.

Det avgrenses videre mot de særlige reglene som gjelder for behandling og viderebehandling av personopplysninger for etterforskningsformål. Det er gitt et eget EU-direktiv som regulerer

denne tematikken.⁴⁴ Direktivet er gjennomført i norsk rett ved politiregisterloven og politiregisterforskriften.⁴⁵

Endelig avgrenses oppgavens behandling av formålsbegrensningsprinsippet mot eventuelle endringer i rettsstilstanden etter torsdag 26. november 2020. Oppgaven bygger på rettskildebildet frem til denne datoen. Eventuelle rettskilder som offentliggjøres etter denne datoen anvendes ikke i fremstillingen.

1.5 Den videre fremstillingen

Problemstillingen for oppgaven er som nevnt i hvilken grad personopplysninger kan viderebehandles for andre formål enn det formålet eller de formålene som opplysningene opprinnelig ble hentet inn for. For å plassere oppgavens problemstilling i kontekst gis det i del 2 av oppgaven en kort redegjørelse for personvernforordningen og forordningens bakteppe, herunder forholdet mellom personvernforordningen og det tidligere personverndirektivet. I tillegg gis en kort presentasjon av de grunnleggende prinsippene for behandling av personopplysninger som forordningen opererer med.

Videre, i del 3, gjøres det grundig rede for formålsbegrensningsprinsippet, både slik det kommer til uttrykk som et generelt personvernrettslig prinsipp i ulike internasjonale kilder og som ett av grunnprinsippene i personvernforordningen. Som nevnt kan prinsippet deles inn i to komponenter. Selv om oppgavens problemstilling gjelder viderebehandling av personopplysninger, og dermed knytter seg til prinsippets andre del, vil også formålsbegrensningsprinsippetets første del gjøres rede for. De to komponentene henger tett sammen, og det anses derfor hensiktsmessig å redegjøre for den første delen for å sikre best mulig forståelse for den delen som gjelder viderebehandling.

Opgavens del 4 foretar en grundig analyse av vilkåret «uforenlig» i personvernforordningen artikkel 5 nr. 1 bokstav b. Vilket utgjør skranken for viderebehandling av personopplysninger og er langt på vei bestemmende for i hvilken grad viderebehandling av personopplysninger er lovlig. Fremstillingen tar sikte på å avklare hvordan vilkåret skal

⁴⁴ Direktiv (EU) 2016/680 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffefølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning 2008/977/JIS.

⁴⁵ Lov 21. juni 2017 nr. 94 om endringer i politiregisterloven mv. (gjennomføring av direktiv (EU) 2016/680 mv.).

forstås, herunder hvordan uforenlighetsvurderingen skal foretas. Personvernforordningen artikkel 6 nr. 4 angir en rekke vurderingsmomenter som skal inngå i uforenlighetsvurderingen. Disse momentene undersøkes grundig. Rettspraksis fra domstoler og avgjørelser fra tilsynsmyndigheter som bidrar til forståelsen av uforenlighetsvurderingen gjøres rede for.

Del 5 omhandler formålsbegrensningsprinsippet og Big data. Adgangen til viderebehandling av personopplysninger i Big data-sammenheng drøftes, herunder i hvilken grad formålsbegrensningsprinsippet hindrer slik bruk av personopplysninger.

Avslutningsvis oppsummeres hovedtrekkene og funnene som er gjort gjennom oppgaven i del 6.

2 Personvernforordningen

2.1 Personvernforordningen og dens bakteppe

Personvernforordningen er EUs sentrale personvernregelverk. Forordningen gir et sett med regler som regulerer behandlingen av personopplysninger. Den ble vedtatt i 2016 og trådte i kraft i EU den 25. mai 2018.⁴⁶ I Norge ble forordningen gjennomført gjennom inkorporasjon ved personopplysningsloven § 1, som angir at personvernforordningen «gjelder som lov». Personopplysningsloven for øvrig gir supplerende nasjonale bestemmelser om behandling av personopplysninger innenfor det handlingsrommet forordningen angir.⁴⁷

Formålet med GDPR er å sikre et effektivt vern av personopplysninger samt å tilrettelegge for fri flyt av personopplysninger i EU og EØS.⁴⁸ Forordningen sikrer en harmonisert regulering av personvernreglene innenfor EU og EØS ved at virksomheter som behandler personopplysninger kan forholde seg til like regler uansett hvilket land de opererer i, i tillegg til at borgerne vet at de nyter samme personvern og har de samme rettighetene uansett hvilket medlemsland en tjenestetilbyder er etablert i.⁴⁹ Ettersom rettsakten er gitt som en forordning har den direkte virkning i alle EUs medlemsland.⁵⁰ EU-lovgivning i forordnings form innebærer som nevnt at alle medlemslandene følger helt likelydende bestemmelser.⁵¹ Forordninger benyttes derfor særskilt i tilfeller hvor EU øker ambisjonsnivået for regulering av særlige spørsmål.⁵²

Da personvernforordningen ble vedtatt var den ikke noen fullstendig nyvinning, men en modernisering og utvikling av et eksisterende personvernregelverk.⁵³ Forordningen erstattet den tidligere EU-rettsakten Direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger

⁴⁶ GDPR artikkel 99 nr. 2.

⁴⁷ Åste Marie Bergseng Skullerud mfl., *Personvernforordningen (GDPR) Kommentartutgave*, Universitetsforlaget 2018, s. 35.

⁴⁸ GDPR artikkel 1.

⁴⁹ Skullerud (2018) s. 35.

⁵⁰ Fredriksen (2018) s. 28.

⁵¹ GDPR gir imidlertid rom for enkelte nasjonale tilpasninger, slik at visse regler kan være ulike blant medlemslandene. Eksempelvis angir GDPR artikkel 88 at nasjonale myndigheter kan gi særlige regler om vern av arbeidstakeres personopplysninger i arbeidssammenheng. Et annet eksempel er GDPR artikkel 8, som åpner for at medlemsstatene ved lov kan fastsette en aldersgrense for barns samtykke i forbindelse med informasjonssamfunnstjenester.

⁵² Fredriksen (2018) s. 29.

⁵³ Wessel-Aas (2018) s. 25.

(videre «personverndirektivet»). I motsetning til GDPR var dette tidligere regelverket gitt i direktivs form. Direktiver innebærer at medlemsstatene pålegges å vedta nasjonale regler med et bestemt innhold, hvilket medfører at det kan oppstå visse forskjeller blant medlemsstatene ved utformingen og håndhevelsen av reglene.⁵⁴

Det følger av personvernforordningen artikkel 2 nr. 1 at forordningen får anvendelse på «behandling av personopplysninger». Personopplysninger defineres som nevnt som «enhver opplysning om en identifisert eller identifiserbar fysisk person». Etter artikkel 4 nr. 2 skal begrepet «behandling» forstås som «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke»,⁵⁵ for eksempel innsamling, strukturering, lagring, bruk eller utlevering. I praksis betyr dette at nesten all befatning med personopplysninger utgjør «behandling».⁵⁶ Personvernforordningen har dermed et svært vidt anvendelsesområde. Den er teknologinøytral, hvilket skal hindre omgåelse av regelverket, i tillegg til å gi fleksibilitet til å møte nye behandlingsmåter som oppstår som følge av den teknologiske utviklingen.⁵⁷

2.2 Grunnleggende prinsipper for behandlingen av personopplysninger

De fleste nasjonale og internasjonale personvernregelverk bygger på et sett grunnleggende prinsipper for vern av personopplysninger. Prinsippene kan anses som generelle rettslige normer om personvern. Disse overordnede normene kommer til en viss grad til uttrykk i lovgivningen som fullgode rettsregler, men fungerer også som retningslinjer ved skjønsmessige interesseavveininger.⁵⁸ Prinsippene er fleksible ved at de kan anvendes innenfor ulike teknologiske, økonomiske og sosiale rammer.⁵⁹ De tilrettelegger dermed for en dynamisk tolkning av den aktuelle rettsakten slik at personopplysningsvernet utvikles i tråd med samfunnsutviklingen.

⁵⁴ Fredriksen (2018) s. 28-29.

⁵⁵ For at ikke-automatisert behandling av personopplysninger skal anses som behandling i forordningens forstand er forutsetningen at opplysningene inngår i eller skal inngå i et register, jf. GDPR artikkel 2 nr. 1.

⁵⁶ GDPR artikkel 2 oppstiller visse andre begrensninger i forordningens saklige virkeområde. Disse er ikke relevante for oppgaven, og vil ikke bli omtalt nærmere.

⁵⁷ GDPR fortalepunkt 15. Se også Skullerud (2018) s. 44.

⁵⁸ Dag Wiese Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, Fagbokforlaget 2016, s. 113-114.

⁵⁹ Kuner (2020) s. 311.

Personvernforordningen opererer også med slike grunnleggende prinsipper. Forordningens artikkel 5 nr. 1 angir en rekke prinsipper som legger føringer for behandlingen av personopplysninger i tråd med forordningen. Dette er prinsippene om lovlighet, rettferdighet og åpenhet, formålsbegrensning, dataminimering, riktighet, lagringsbegrensning og integritet og konfidensialitet. Flere av prinsippene henger tett sammen. Når det gjelder formålsbegrensningsprinsippet kan dette blant annet sees i sammenheng med prinsippet om åpenhet. Formålet med behandlingen av personopplysninger må være synlig for aktuelle parter, som den registrerte og datatilsynsmyndigheter, for at nødvendige garantier skal kunne ivaretas fullt ut. Åpenhet rundt formålet eller formålene for behandling er avgjørende for å sikre forutberegnelighet samt legge til rette for brukerkontroll.⁶⁰ All behandling av personopplysninger skal som utgangspunkt skje i tråd med prinsippene. Eventuelle unntak fordrer hjemmel i forordningen.⁶¹ Prinsippene fungerer som sentrale tolkningsfaktorer ved tolkningen av personvernforordningens øvrige bestemmelser.⁶²

Det er den behandlingsansvarlige som har ansvar for at de grunnleggende prinsippene overholdes.⁶³ Den behandlingsansvarlige er den fysiske eller juridiske personen eller organet som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.⁶⁴ I motsatt ende har man den fysiske personen som de aktuelle personopplysningene angår og som er rettighetssubjektet etter personvernforordningen. Forordningen omtaler denne som «den registrerte».⁶⁵

Personvernforordningen artikkel 5 bygger i stor grad på personverndirektivet artikkel 6, som ga uttrykk for tilnærmet de samme prinsippene under tittelen «Principles relating to data quality». GDPR innebar ingen fundamental revisjon av disse, kun visse justeringer og tilføyelser.⁶⁶ Når det gjelder formålsbegrensningsprinsippet fremgikk dette av personverndirektivet artikkel 6 nr. 1 bokstav b. Prinsippet lød som følger: «personal data must be ... collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes». Ordlyden er så godt som identisk med personvernforordningens formulering av prinsippet. Som nevnt innledningsvis vil kilder

⁶⁰ A29 WP Opinion 03/2013, s. 13.

⁶¹ Skullerud (2018) s. 74.

⁶² Skullerud (2018) s. 75.

⁶³ GDPR artikkel 5 nr. 2.

⁶⁴ GDPR artikkel 4 nr. 7.

⁶⁵ GDPR artikkel 4 nr. 1.

⁶⁶ Kuner (2020) s. 311.

tilknyttet formålsbegrensningsprinsippet etter personverndirektivet være relevante for oppgavens behandling av prinsippet ettersom forordningen viderefører direktivets prinsipp.

Det er likevel visse forskjeller mellom formålsbegrensningsprinsippet i personverndirektivet og i personvernforordningen. Personverndirektivet hadde ingen særskilt regulering av adgangen til viderebehandling av personopplysninger tilsvarende reguleringen i personvernforordningen artikkel 6 nr. 4. Som nevnt gir artikkelen en rekke vurderingsmomenter som skal inngå i vurderingen av hvorvidt viderebehandling er uforenlig med opprinnelig formål. Disse momentene klargjør innholdet i uforenlighetsvurderingen og bidrar til en mer enhetlig praktisering av prinsippet. På dette punktet innebar GDPR dermed en viktig presisering av prinsippets anvendelse. Bakgrunnen for og konsekvensene av denne tilføyelsen behandles nærmere i oppgavens del 3.2.

2.3 Kravet til behandlingsgrunnlag

En svært sentral regel i personvernforordningen er kravet til behandlingsgrunnlag, som følger av GDPR artikkel 6 nr. 1 samt av prinsippet om lovlighet i artikkel 5 nr. 1 bokstav a. Kravet innebærer at behandling av personopplysninger kun er lovlig når den behandlingsansvarlige kan bygge behandlingen på et av seks angitte behandlingsgrunnlag. Disse listes opp i artikkel 6 nr. 1 bokstav a-f. De mulige behandlingsgrunnlagene er samtykke (bokstav a), avtale som den registrerte er part i eller skal inngå (bokstav b), oppfyllelse av en rettslig forpliktelse (bokstav c), vern av vitale interesser (bokstav d), utførelse av oppgave i allmennhetens interesse eller utøvelse av offentlig myndighet (bokstav e) og berettiget interesse (bokstav f).

Selv om den behandlingsansvarlige kan påvise at behandlingen av personopplysninger bygger på et lovlig behandlingsgrunnlag, må også de grunnleggende prinsippene, herunder formålsbegrensningsprinsippet, være tilfredsstillt. Dette betyr at dersom behandlingen av personopplysninger eksempelvis skjer på bakgrunn av en avtale mellom den behandlingsansvarlige og den registrerte, og dermed har avtalen som behandlingsgrunnlag, må behandlingen likevel oppfylle spesifiserte, uttrykkelig angitte og berettigede formål. Som jeg kommer tilbake til senere i oppgaven, må formålet være angitt senest når innsamlingen av de aktuelle opplysningene finner sted.⁶⁷

⁶⁷ Se oppgavens del 3.2.1.

Forholdet mellom kravet til behandlingsgrunnlag og formålsbegrensningsprinsippets tematiseres nærmere senere i oppgaven.

3 Formålsbegrensningsprinsippet

3.1 Formålsbegrensningsprinsippet i en internasjonal kontekst

Formålsbegrensning er et sentralt personvernrettslig prinsipp som er fremtredende i de internasjonale personvernregelverkene. Prinsippet omtales også som 'finalitetsprinsippet' eller 'formålsspesifiseringsprinsippet'.⁶⁸ Prinsippet kan gjenfinnes i de tidlige personvernregelverkene som OECD-retningslinjene⁶⁹ og Europarådskonvensjonen.⁷⁰ Det følger av OECD-retningslinjene artikkel 9 at

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Videre følger det av retningslinjene artikkel 10 at personopplysninger «should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9» uten «the consent of the data subject» eller «by the authority of law». I Europarådskonvensjonen fremgår det av artikkel 5 bokstav b at «[p]ersonal data undergoing automatic processing shall be (...) stored for specified and legitimate purposes and not used in a way incompatible with those purposes». Gjengangeren er begrepet *incompatible*, som på norsk kan oversettes til *uforenlig*. Dette vilkåret er avgjørende for adgangen til viderebehandling også etter personvernforordningen.

Den europeiske menneskerettskonvensjonen artikkel 8 gir uttrykk for retten til respekt for privatlivet. Som nevnt i del 1.3 tolkes artikkelen slik at den også hjemler et vern av personopplysninger. Etersom konvensjonsteksten er såpass knapp som den er, gir den ikke uttrykk for særlige personvernrettslige prinsipper. Det er dermed opp til den Den europeiske menneskerettighetsdomstolen å utpense innholdet i konvensjonens vern av

⁶⁸ Bygrave (2014) s. 153.

⁶⁹ OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23. september 1980.

⁷⁰ Europarådet, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28. januar 1981.

personopplysninger. Formålsbegrensningsprinsippet har i liten grad blitt vist til eksplisitt, men domstolen har indirekte anvendt aspekter ved prinsippet slik det kommer til uttrykk i personvernlovgivning. Et eksempel er dommen *M.S. v Sweden*,⁷¹ som jeg gjør rede for i oppgavens del 4.5.

Vernet av personopplysninger kommer videre til uttrykk i EUs pakt om grunnleggende rettigheter artikkel 8.⁷² Det fremgår av artikkelen at «[e]veryone has the right to the protection of personal data concerning him or her» og videre at «[s]uch data must be processed fairly for specified purposes». Det siste gir uttrykk for første del av formålsbegrensningsprinsippet, nemlig at personopplysninger skal samles inn for spesifiserte formål. Pakten artikkel 8 regulerer imidlertid ikke prinsippets andre del, det vil si adgangen til viderebehandling av personopplysninger.

Formålsbegrensningsprinsippets rolle som sentralt personvernrettslig prinsipp har også blitt bekreftet av Høyesterett. I dommen inntatt i Rt. 2013 s. 143 uttalte Høyesterett at formålsbegrensning «regnes internasjonalt som et fundamentalt og viktig prinsipp på personopplysningsrettens område».⁷³ Denne dommen behandles nærmere i oppgavens del 4.5.

Gjennomgangen illustrerer at formålsbegrensningsprinsippet er et sentralt og viktig prinsipp på personvernrettens område. Men selv om formålsbegrensningsprinsippet har en betydelig utbredelse, er det ikke en uten videre enkel jobb å avklare prinsippets eksakte innhold. Særlig uforenlighetsvurderingen byr på utfordringer i praksis.⁷⁴ I det videre fokuseres det på formålsbegrensningsprinsippet i GDPR. I årene frem mot personvernforordningen hadde det oppstått behov for avklaring av prinsippets innhold og rekkevidde. Dette tematiseres i neste underkapittel.

3.2 Formålsbegrensningsprinsippet i personvernforordningen

I personvernforordningen kommer formålsbegrensningsprinsippet som nevnt til uttrykk i artikkel 5 nr. 1 bokstav b, hvor det heter at personopplysninger skal «samles inn for

⁷¹ *M.S. v. Sweden* [J] 1997, no. 20837/92.

⁷² Charter of Fundamental rights of the European Union (2012/C 326/02).

⁷³ Rt. 2013 s. 143, avsnitt 47.

⁷⁴ Bygrave (2014) s. 153.

spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene». Prinsippet kan deles inn i to komponenter, der den første knytter seg til selve innsamlingen av personopplysninger, mens den andre gjelder viderebehandling av personopplysninger. En slik inndeling støttes av Artikkel 29-gruppen, som konstaterer at konseptet formålsbegrensning består av «two main building blocks».⁷⁵

Formålsbegrensningsprinsippet i GDPR er en videreføring av det tilsvarende prinsippet i forordningens forgjenger, personverndirektivet. Formuleringen av selve prinsippet er som vist tilnærmet identisk. Det ble imidlertid gjort visse tilføyelser ved overgangen til personvernforordningen. Det fantes ikke klare retningslinjer for hvordan personverndirektivets formålsprinsipp skulle forstås og anvendes i praksis. Ettersom prinsippet er relativt åpent og vagt formulert, ble prinsippet derfor tolket på flere måter og fikk ulik rekkevidde i medlemsstatene.⁷⁶ Særlig uforenlighetsvurderingen ble praktisert ulikt. Risikoen for uensartet anvendelse tematiseres av Artikkel 29-gruppen i veilederen om formålsbegrensningsprinsippet, hvor denne problematikken også fremheves som årsaken til at gruppen utga en omfattende veileder om prinsippet.⁷⁷ I veilederen poengterer artikkel 29-gruppen at utviklingen av ny teknologi som medfører at personopplysninger kan behandles for stadig flere formål, samt muligheten til gjenbruk av personopplysninger i Big data-sammenheng, også var faktorer som nødvendiggjorde en grundig analyse av formålsbegrensningsprinsippet.⁷⁸ I veilederen påpekte Artikkel 29-gruppen at uklarhet rundt prinsippets anvendelse både kan medføre svekket vern for den registrerte, men også unødvendige regulatoriske byrder for virksomheter og andre som operere på tvers av landegrenser.

I arbeidet frem mot personvernforordningen var det derfor viktig å etablere en klarere og mer ensartet forståelse av formålsbegrensningsprinsippet og dets rekkevidde. Det ble ansett nødvendig for å sikre en mer harmonisert tolkning og anvendelse av prinsippet blant EUs medlemsland ved innføringen av personvernforordningen.⁷⁹

Særlig uforenlighetsvilkåret byr som nevnt på tolkningstvil. Vilkåret «uforenlig» er ikke definert nærmere i GDPR artikkel 5 nr. 1 bokstav b enn hva som var tilfelle for

⁷⁵ A29 WP Opinion 03/2013, s. 3.

⁷⁶ A29 WP Opinion 03/2013, s. 5.

⁷⁷ A29 WP Opinion 03/2013, s. 5.

⁷⁸ A29 WP Opinion 03/2013, s. 14.

⁷⁹ A29 WP Opinion 03/2013, s. 5.

personverndirektivet. Uklarheten knyttet til innholdet i uforenlighetsvurderingen avhjelpest imidlertid av artikkel 6 nr. 4, som ble innført ved GDPR. Bestemmelsen bidrar til klargjøring av hva som utgjør kompatibel viderebehandling, men angir også visse unntak der viderebehandling er lovlig til tross for at behandlingen som utgangspunkt er uforenlig med opprinnelig formål. Det konkrete innholdet i artikkel 6 nr. 4 presenteres og behandles i oppgavens del 4.2.

3.3 Formålsbegrensningsprinsippets begrunnelse

Det er flere årsaker til at personvernregelverkene opererer med et formålsbegrensningsprinsipp. Formålsbegrensningsprinsippet begrunnes særlig i hensynet til forutberegnelighet. Prinsippet sikrer forutberegnelighet ved at både selve behandlingen av personopplysninger og utfallet av behandlingen skal være i samsvar med den registrertes forventninger.⁸⁰ Når man deler personopplysningene sine har man sannsynlighet en forventning om hvilke formål opplysningene skal benyttes til. Eksempelvis vil en person som deler helseopplysninger til et forsikringselskap ved tegning av helseforsikring neppe forvente at opplysningene senere skal videreformidles til en leverandør av skreddersydde helsereiser for at denne skal benytte opplysningene i målrettet markedsføring. En slik behandling av opplysningene er dermed i strid med den registrertes forventninger. Ved å ivareta slike forventninger sikres tillit og forutberegnelighet. I tillegg bidrar prinsippet til åpenhet og rettssikkerhet.⁸¹ Artikkel 29-gruppen tar til orde for at formålsbegrensningsprinsippet derfor er å regne som en hjørnestein i personvernet.⁸² Formålsbegrensningsprinsippet er utvilsomt et særlig viktig prinsipp.

På den andre siden kan personopplysninger som allerede er innhentet åpenbart være av vesentlig betydning også for andre formål enn det opprinnelige formålet. Eksempelvis kan det fremstå hensiktsmessig at helseopplysninger samlet inn i behandlingssammenheng senere kan benyttes til medisinsk forskning for å kartlegge og bekjempe sykdommer. På bakgrunn av slike betraktninger kan det være verdifullt å tillate noe videre bruk, innen tydelig definerte rammer.⁸³ Ved at formålsbegrensningsprinsippet i personvernforordningen kun forbyr viderebehandling til formål som er *uforenlige* med det opprinnelige formålet, tillates en viss

⁸⁰ Bygrave (2014) s. 153.

⁸¹ A29 WP Opinion 03/2013, s. 11.

⁸² A29 WP Opinion 03/2013, s. 4.

⁸³ A29 WP Opinion 03/2013, s. 4.

grad av videre bruk av personopplysninger. Prinsippet kan derfor sies å gi uttrykk for en balansert tilnærming til viderebehandling. Prinsippet ivaretar hensynet til og behovet for forutberegnelighet i behandlingen av personopplysninger, samtidig som det åpner for en pragmatisk tilnærming og en viss fleksibilitet i adgangen til viderebehandling.⁸⁴ Dette kan sees i sammenheng med at personvern ikke er en absolutt rettighet, som tematisert i oppgavens del 1.2. Ivaretagelsen av den enkeltes personvern må vurderes i lys av funksjonen denne rettigheten har i samfunnet og balanseres mot andre fundamentale rettigheter.⁸⁵

I det følgende skal det redegjøres nærmere for formålsbegrensningsprinsippetets to sider og hvilken praktisk betydning prinsippet har for de som behandler personopplysninger. Som påpekt anses forståelse av prinsippetets første del som hensiktsmessig for forståelsen av adgangen til viderebehandling av personopplysninger.

3.4 Prinsippetets første del: personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål

3.4.1 Innledende

Formålsbegrensningsprinsippetets første del går ut på at personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål. Denne delen av prinsippet kan omtales som formålsspesifiseringsdimensjonen.⁸⁶

Ved at forordningen angir at personopplysningene skal «samles inn» for spesifikke, uttrykkelig angitte og berettigede formål, må den behandlingsansvarlige avgjøre formålet for behandlingen av personopplysninger før, og i alle tilfeller ikke etter, innsamlingen av opplysningene finner sted. En slik forståelse bekreftes av fortalen, hvor det fremgår at «the specific purposes for which personal data are processed should be explicit and legitimate and determined *at the time of the collection of the personal data*» (min utheving).⁸⁷ I tillegg er beskrivelsen av formålet med behandlingen en forutsetning for at den registrerte skal kunne gjøre et informert valg om å samtykke til behandlingen i tilfeller der behandlingen bygger på

⁸⁴ A29 WP Opinion 03/2013, s. 5.

⁸⁵ GDPR fortalepunkt 4.

⁸⁶ Kuner (2020) s. 315.

⁸⁷ GDPR fortalepunkt 39 nr. 6.

samtykke som behandlingsgrunnlag. Slik beskrivelse må derfor skje før behandlingen finner sted.

Prinsippet forutsetter at behandling av personopplysninger skjer for ett eller flere formål. Hva som er formålet i en gitt behandlingssituasjon vil generelt være svaret på spørsmålet om *hvorfor* personopplysningene blir behandlet.⁸⁸ Formålsspesifiseringsdimensjonen, som behandles i det følgende, illustrerer at det er viktig å ha en klar forestilling om hvorfor personopplysninger behandles.

3.4.2 Formålet skal være spesifikt

Personopplysninger skal for det første samles inn for spesifikke formål. Kravet om at formålet skal være spesifikt betyr at det må være konkret angitt.⁸⁹

Artikkel 29-gruppen har fremhevet at formålet må være spesifisert på en slik måte at det er mulig å avgjøre hvilke typer behandling som dekkes og ikke dekkes av formålet. I tillegg skal formålet være tilstrekkelig spesifikt angitt slik at det er mulig å vurdere hvorvidt behandlingen er lovlig, herunder om behandlingen er tillatt under relevant personvernlovgivning og om nødvendige personverngarantier er oppfylt. Generelle eller vagt formulerte formål, eksempelvis «å bedre brukeropplevelsen» eller «markedsføringsformål» vil ofte ikke nå opp til terskelen uten at nærmere forklaring gis. Detaljgraden vil imidlertid avhenge av de konkrete omstendighetene ved innsamlingen og karakteren av personopplysningene.⁹⁰

Artikkel 29-gruppens veileder gir eksempler som illustrerer vilkårets relative karakter. For eksempel vil en lokal butikk i en liten by hvor kundene i hovedsak er lokalbefolkningen, som kun samler inn enkelte opplysninger om kundene, ikke måtte spesifisere formålene for behandlingen like inngående som et stort detaljhandelsselskap som selger varer via internett og bruker avanserte analyseverktøy for å utarbeide personlige tilbud og andre former for målrettet markedsføring til kundene.⁹¹

⁸⁸ A29 WP Opinion 01/2010 on the concepts of "controller" and "processor", s. 13.

⁸⁹ Skullerud (2018) s. 76.

⁹⁰ A29 WP Opinion 03/2013, s. 15-16.

⁹¹ A29 WP Opinion 03/2013, s. 51.

Bruk av såkalt *layered notice* kan være et grep for å spesifisere formål på en hensiktsmessig måte.⁹² Det er ikke nødvendigvis slik at omfattende og detaljerte redegjørelser av formålet er den mest hensiktsmessige måten å formidle formålene på. Tvert imot kan omstendelige forklaringer innebære en risiko for at spesifiseringen av formålet oppfattes som lite tilgjengelig. Metoden med *layered notice* går derfor ut på den aller mest sentrale informasjonen formidles på en presis og brukervennlig måte, mens tilleggsinformasjon tilbys for de som ønsker ytterligere forklaring. Tilleggsinformasjonen kan for eksempel formidles gjennom en lenke til en nettside som gir en mer inngående beskrivelse av hvordan personopplysningene skal behandles og til hvilke formål.

I tilfeller der personopplysninger samles inn for mer enn ett formål, bør hvert enkelt formål spesifiseres i slik detaljgrad det er mulig å vurdere hvorvidt innsamling for dette formålet er lovlig. Den behandlingsansvarlige må i alle tilfeller unngå å angi ett overordnet formål for å forsøke å åpne døren for fremtidige behandlingsaktiviteter som i realiteten er fjernt relaterte til det faktiske formålet.⁹³

3.4.3 Formålet skal være uttrykkelig angitt

Videre fremgår det av formålsbegrensningsprinsippet at formålet skal være «uttrykkelig angitt». Ved at formålet skal være uttrykkelig angitt, må det formidles tydelig og kan ikke være underforstått.⁹⁴ Det er ikke tilstrekkelig at den behandlingsansvarlige formulerer spesifikt angitte formål og er bevisst på disse overfor seg selv, formålene må også formidles.

I veilederen om formålsbegrensning fremhever Artikkel 29-gruppen at det overordnede siktemålet med kravet om at formålet skal være uttrykkelig angitt er å sikre at formålene spesifiseres uten uklarhet eller tvetydighet. Hva som er ment fra den behandlingsansvarliges side må være klart, slik at det ikke oppstår tvil eller vanskeligheter rundt forståelsen. Slik fremmes åpenhet og forutberegnelighet.⁹⁵

Formålene må videre formidles eller uttrykkes på en måte som er forståelig for alle involverte parter. Dette innebærer at det ikke er tilstrekkelig at formålet er forståelig for den

⁹² A29 WP Opinion 03/2013, s. 16.

⁹³ A29 WP Opinion 03/2013, s. 16.

⁹⁴ Skullerud (2018) s. 76.

⁹⁵ A29 WP Opinion 03/2013, s. 17.

behandlingsansvarlige og eventuelle databehandlere.⁹⁶ Formålet må formidles på en slik måte at det forstås av den registrerte, uavhengig av forhold som språklig eller kulturell bakgrunn, kunnskapsnivå og eventuelle særlige behov.⁹⁷ Eksempelvis må en nettside som gir rådgivning til eldre eller mentalt syke personer ta i betraktning alderen til individene de retter seg mot og eventuelle særlige behov disse har.⁹⁸

3.4.4 Formålet skal være berettiget

Formålsspesifiseringsdimensjonen oppstiller også et krav om at formålet skal være «berettiget». Kravet om at formålet skal være berettiget innebærer at behandlingen må skje i samsvar med gjeldende lovgivning, samt tilfredsstille andre samfunnskrav.⁹⁹ Formålet kan ikke innebære et uforholdsmessig inngrep i rettighetene og interessene som står på spill for den registrerte, kun for at den behandlingsansvarliges interesser skal ivaretas. Vilkåret innebærer at formålet må være berettiget når den registrertes rettigheter avveies mot den behandlingsansvarliges eller samfunnet for øvrig sine interesser.¹⁰⁰

Behandlingen må for det første skje på bakgrunn av ett av de seks angitte behandlingsgrunnlagene i GDPR artikkel 6 nr. 1 for å være lovlig. I tillegg må formålene være i tråd med personvernregelverket for øvrig, samt lovgivning på andre rettsområder, eksempelvis arbeidsrett, kontraktsrett og forbrukerbeskyttelse.¹⁰¹ Vilkåret skal forstås vidt, slik at alt fra formelle lover og rettsavgjørelser til mer generelle rettslige prinsipper kan være bestemmende for lovligheten. Vurderingen av hva som er et berettiget formål vil kunne endres med tiden, i takt med den vitenskapelige og teknologiske utviklingen og generelle oppfatninger i samfunnet.¹⁰²

⁹⁶ Med «databehandler» menes en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. definisjonen i GDPR artikkel 4 nr. 8.

⁹⁷ A29 WP Opinion 03/2013, s. 17.

⁹⁸ A29 WP Opinion 03/2013, s. 51.

⁹⁹ Skullerud (2018) s. 76.

¹⁰⁰ Kuner (2020) s. 315.

¹⁰¹ GDPR artikkel 88 åpner eksempelvis for at nasjonale myndigheter kan gi særlige regler om vern av arbeidstakers personopplysninger i arbeidssammenheng. «Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale» (FOR-2018-07-02-1108) er et eksempel på en nasjonal regulering om behandling av personopplysninger.

¹⁰² A29 WP Opinion 03/2013, s. 19-20.

3.5 Prinsippets andre del: personopplysninger skal ikke viderebehandles på en måte som er uforenlig med formålene

Formålsbegrensningsprinsippet går videre ut på at personopplysninger ikke skal viderebehandles på en måte som er uforenlig med opprinnelig formål. Denne delen av formålsbegrensningsprinsippet kan kalles forenlighetsdimensjonen.¹⁰³

Innledningsvis er det hensiktsmessig å avklare *hva* som utgjør viderebehandling. Viderebehandling foreligger med en gang en annen behandlingsaktivitet enn innsamling utføres. Forordningen skiller nemlig ikke mellom behandling for opprinnelig angitte formål og senere angitte formål, men derimot mellom innsamling, som den aller første operasjonen som gjøres med personopplysninger, og alle videre operasjoner, eksempelvis strukturering, lagring og bruk. Dette betyr at all behandling etter selve innsamlingen skal regnes som viderebehandling og derfor må tilfredsstille kravet til forenlighet.¹⁰⁴

Det nærmere innholdet i uforenlighetsvilkåret behandles inngående i del 4 av oppgaven. Innholdet av vilkåret er avgjørende for i hvilken grad det er adgang til å viderebehandle personopplysninger. GDPR artikkel 6 nr. 4 har en viktig funksjon for denne delen av formålsbegrensningsprinsippet, ved at artikkelen angir en rekke vurderingsmomenter som skal inngå i vurderingen av uforenlighet.

Uforenlighetsvurderingen aktualiseres imidlertid ikke i ethvert tilfelle. Viderebehandling for visse formål er nemlig unntatt uforenlighetsvurderingen som artikkel 5 nr. 1 bokstav b legger opp til. Etter artikkelen skal viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål per definisjon ikke anses uforenlig med de opprinnelige formålene som opplysningene ble hentet inn for. Dette er dermed lovlige sekundærformål. Artikkel 89 oppstiller krav til «nødvendige garantier» ved behandling for disse formålene. Etter artikkel 89 nr. 1 kan slike tiltak omfatte pseudonymisering eller anonymisering.¹⁰⁵ Disse garantiene skal sikre ivaretagelse av den registrertes rettigheter og friheter, særlig ved å sikre at prinsippet om dataminimering

¹⁰³ Kuner (2020) s. 315.

¹⁰⁴ A29 WP Opinion 03/2013, s. 21.

¹⁰⁵ Artikkel 29-gruppen har gitt en egen veileder om anonymiseringsteknikker: A29 WP Opinion 05/2014 on Anonymisation Techniques. Begrepene pseudonymisering og anonymisering forklares nærmere i oppgavens del 4.5.5.

overholdes. Prinsippet om dataminimering går ut på at personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.¹⁰⁶

Ettersom viderebehandling for arkivformål, forskningsformål eller statistiske formål ikke skal anses uforenlig med opprinnelig formål, vil ikke uforenlighetsvilkåret være relevant for adgangen til viderebehandling for disse formålene. Unntaksregelen kan imidlertid være relevant for adgangen til viderebehandling av personopplysninger i Big data-sammenheng. Denne tematikken behandles nærmere i oppgavens del 5.

¹⁰⁶ GDPR artikkel 5 nr. 1 bokstav c.

4 Når er viderebehandling av personopplysninger «uforenlig» med opprinnelig formål?

4.1 Innledende om vilkåret og vurderingen

Etter personvernforordningen artikkel 5 nr. 1 bokstav b skal personopplysninger ikke viderebehandles på en måte som er «uforenlig» med opprinnelig formål. Etter en naturlig språklig forståelse henviser vilkåret «uforenlig» til formål som ikke lar seg forene med eller ikke er i samsvar med det opprinnelige formålet. Ordlyden tilsier følgelig at det må foretas en vurdering av i hvilken grad de aktuelle formålene er kompatible. Motsetningsvis tilsier bestemmelsen at viderebehandling for nye, ikke-uforenlige formål er tillatt, selv uten et eget rettsgrunnlag for viderebehandlingen.¹⁰⁷ Det er imidlertid ikke uten videre klart hva som utgjør uforenlig viderebehandling. Som diskutert i kapittel 3.2 ble vilkåret «uforenlig» i personvernforordningens forgjenger, personverndirektivet, tolket ulikt blant EUs medlemsland, slik at formålsbegrensningsprinsippet fikk uensartet rekkevidde blant medlemslandene.

Et vesentlig forhold ved uforenlighetsvilkåret er at det er gitt i form av et såkalt dobbelt negativ. Forordningen forbyr viderebehandling for formål som er uforenlige med det opprinnelige formålet, i motsetning til kun å tillate viderebehandling for formål som er forenlige. Ved at viderebehandling kan være lovlig så lenge behandlingen ikke er uforenlig med opprinnelig formål, synes lovgiver å ha ment å åpne for en viss fleksibilitet hva gjelder videre bruk.¹⁰⁸ Standarden kan antas å være mindre streng enn dersom kravet til viderebehandling var at denne måtte være *forenlig* med opprinnelig formål.¹⁰⁹ Jeg omtaler derfor vurdering som foretas for å avgjøre viderebehandlingens lovlighet som *uforenlighetsvurderingen*, selv om vurderingen ofte omtales som en *forenlighetsvurdering* i praksis og juridisk teori.

¹⁰⁷ En slik tolkning bekreftes av GDPR fortalepunkt 50 nr. 2.

¹⁰⁸ A29 WP Opinion 03/2013, s. 21.

¹⁰⁹ Bygrave (2014) s. 156.

I veilederen om formålsbegrensningsprinsippet angir Artikkel 29-gruppen at det er to måter å foreta uforenlighetsvurderingen på når den behandlingsansvarlige eller en tilsynsmyndighet skal ta stilling til om viderebehandling er lovlig: vurderingen kan være formell eller materiell.¹¹⁰ Ifølge veilederen innebærer en vurdering av formell karakter å ta utgangspunkt i det skriftlige formålet opprinnelig angitt av den behandlingsansvarlige og sammenligne dette med de mulige videre bruksområdene. Siktemålet er å avgjøre om disse direkte eller indirekte dekkes av det opprinnelige formålet. En vurdering av materiell karakter vil på sin side rekke lenger enn å analysere det formelt angitte formålet. Den materielle vurderingen innebærer å identifisere og analysere både det nye og det opprinnelige formålet, herunder ved å se formålene i lys av både kontekst og andre forhold. Artikkel 29-gruppen angir at selv om den første fremgangsmåten potensielt fremstår mer objektiv og nøytral, kan den lett bli rigid. I tillegg kan en slik fremgangsmåte potensielt gi den behandlingsansvarlige et insentiv til å angi det opprinnelige formålet på en tvetydig eller uklar måte for å sikre et større spillerom for viderebehandling. Dette på bekostning av å ivareta hensynet til individet som personopplysningene angår. Den materielle vurderingen er på sin side mer fleksibel og pragmatisk. I tillegg er den mer effektiv, ved at den åpner for tilpasninger i takt med samfunnsutviklingen. Utfordringen er imidlertid å avgjøre hvilke kriterier som er relevante for å avgjøre når et formål for viderebehandling er uforenlig. Her aktualiseres vurderingsmomentene i personvernforordningen artikkel 6 nr. 4 bokstav a-e.¹¹¹

4.2 Presentasjon av personvernforordningen artikkel 6 nr. 4

Som nevnt innledningsvis i oppgaven gir personvernforordningen artikkel 6 nr. 4 nærmere regler om adgangen til behandling av personopplysninger for andre formål enn det de opprinnelig ble innhentet for. Tittelen på artikkel 6 i sin helhet er «[b]ehandlingens lovlighet».

Artikkel 6 nr. 4 gir før det første uttrykk for en rekke momenter som den behandlingsansvarlige skal ta i betraktning ved vurderingen av uforenlighet. Dette er momenter som «blant annet» skal hensyntas, og listen er dermed ikke uttømmende. Momentene behandles inngående i oppgavens punkt 4.3.1 til 4.3.5. Personverndirektivet inneholdt ikke en slik presisering av hvilke forhold som kan være relevante ved

¹¹⁰ A29 WP Opinion 03/2013, s. 21.

¹¹¹ A29 WP Opinion 03/2013, s. 22.

uforenlighetsvurderingen. Som omtalt i del 3.2 ble momentene innført ved personvernforordningen. Ettersom deling og gjenbruk av personopplysninger skjer i stadig økende grad, ble det ansett nødvendig med veiledning om hva som skal betraktes som forenlig videre bruk.¹¹²

I tillegg til å angi relevante momenter for uforenlighetsvurderingen, følger det av artikkel 6 nr. 4 at dersom det nye formålet ikke er forenlig med innsamlingsformålet, kan viderebehandlingen likevel være lovlig dersom behandlingen har grunnlag i «den registrertes samtykke» eller «unionsretten eller medlemsstatenes nasjonale rett». For at det skal foreligge et gyldig samtykke til viderebehandlingen må samtykket oppfylle vilkårene for samtykke etter forordningen artikkel 7. Dette innebærer at samtykket må være frivillig, spesifikt, informert, utvetydig og dokumenterbart, i tillegg til at det må være gitt gjennom en aktiv handling og med mulighet til å trekke det tilbake like lett som det ble gitt.¹¹³ For viderebehandling med grunnlag i lov må slike lovbestemmelser utgjøre «et nødvendig og forholdsmessig tiltak i et demokratisk samfunn for å sikre oppnåelse av målene nevnt i artikkel 23 nr. 1». I slike tilfeller er formålet vurdert som såpass viktig for samfunnet at viderebehandlingen tillates.¹¹⁴ Siden det er *viderebehandlingen* som må ha grunnlag i lov eller samtykke, må lovgrunnlaget eller samtykket knytte seg til viderebehandlingen for uforenlige formål. Det må være et rettslig grunnlag for selve viderebehandlingen.¹¹⁵

Det er et interessant poeng at EU-kommisjonens opprinnelige forslag til personvernforordningen artikkel 6 nr. 4 åpnet for en langt mer omfattende adgang til viderebehandling enn hva personvernforordningen i dag tillater. Den foreslåtte formuleringen av artikkel 6 nr. 4 lød:

*Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.*¹¹⁶

¹¹² Kuner (2020) s. 327.

¹¹³ GDPR artikkel 7 og GDPR fortalepunkt 32.

¹¹⁴ Skullerud (2018) s. 92.

¹¹⁵ Prop. 56 LS (2017-2018) s. 37.

¹¹⁶ EU-kommisjonen, Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011.

Kommisjonen foreslo følgelig at viderebehandling for uforenlige formål skulle tillates dersom viderebehandlingen kunne forankres i ett av behandlingsgrunnlagene angitt i artikkel 6 nr. 1 bokstav a-e. Dermed ville det ha vært mulig å avhjelpe eventuell uforenlighet kun ved å påvise et nytt grunnlag for behandlingen.¹¹⁷ En slik regel ville i realiteten ha medført en uthuling av formålsbegrensningsprinsippet.¹¹⁸ Forslaget ble kritisert, eksempelvis av Artikkel 29-gruppen. Gruppen påpekte at kravet til behandlingsgrunnlag og forbudet mot uforenlig viderebehandling må anses som kumulative vilkår.¹¹⁹ En løsning der det hadde vært mulig å omgå eventuell uforenlighet ved å påvise et nytt behandlingsgrunnlag ville derfor ha medført en lavere grad av beskyttelse enn etter personverndirektivet. Den nevnte passasjen ble forkastet av Europaparlamentet.¹²⁰ Den endelige løsningen er redegjort for ovenfor – viderebehandling for uforenlige formål er kun tillatt dersom den registrerte samtykker til det eller viderebehandlingen er hjemlet i unionsretten eller medlemsstatenes nasjonale rett i tråd med forordningen artikkel 23 nr. 1.

4.3 Foreløpig oppsummering

For å samle trådene gis en foreløpig oppsummering av formålsbegrensningsprinsippet. Formålsbegrensningsprinsippet innebærer for det første at personopplysninger skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål. Denne delen av prinsippet gjelder uten unntak. Videre innebærer formålsbegrensningsprinsippet at personopplysninger ikke skal viderebehandles på en måte som er uforenlig det opprinnelige formålet. Det må foretas en vurdering av uforenlighet, og her får vurderingsmomentene i artikkel 6 nr. 4 anvendelse. Dersom viderebehandlingen av personopplysningene ikke anses uforenlig, kan slik behandling skje uten at det kreves et nytt behandlingsgrunnlag. Dersom viderebehandlingen derimot er uforenlig, kan personopplysningene som utgangspunkt ikke viderebehandles for andre formål enn det opprinnelige. Det gjelder imidlertid visse unntak fra dette utgangspunkt.

For det første kan viderebehandling være lovlig dersom slik behandling skjer for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål. Viderebehandling for slike formål skal uten videre anses som forenlig med

¹¹⁷ A29 WP Opinion 03/2013, s. 36.

¹¹⁸ Kuner (2020) s. 316.

¹¹⁹ A29 WP Opinion 03/2013, s. 36-37.

¹²⁰ Europaparlamentet, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

de opprinnelige formålene, og er dermed unntatt uforenlighetsvurderingen. Lovligheten beror imidlertid på om viderebehandlingen skjer i samsvar med artikkel 89.

Videre kan viderebehandling være lovlig dersom den registrerte har samtykket til viderebehandlingen. Viderebehandling kan også være lovlig dersom behandlingen har grunnlag i unionsretten eller medlemsstatenes nasjonale rett for å ivareta viktige allmenne hensyn i samsvar med artikkel 23. Dette er blant annet hensynet til den nasjonale sikkerhet og hensynet til forebygging, etterforskning, avsløring eller straffeforfølgning av straffbare forhold. I fortalen fremgår det i tillegg at formålsbegrensningsprinsippet ikke hindrer den behandlingsansvarlige fra å gi informasjon om mulige straffbare gjerninger eller sikkerhetstrusler til nasjonale sikkerhetsmyndigheter. Slik utlevering av informasjon er likevel ikke lovlig dersom det er uforenlig med en lovbestemt, profesjonsbasert eller annen bindende taushetsplikt.¹²¹

Dersom ingen av unntakene gjør seg gjeldende, beror adgangen til viderebehandling som nevnt på at slik behandling ikke er uforenlig med det formålet opplysningene opprinnelig ble samlet inn for. I det følgende gis en redegjørelse av vurderingsmomentene i artikkel 6 nr. 4 bokstav a-e, som gir føringer for uforenlighetsvurderingen.

4.4 Vurderingsmomentene i bokstav a-e

4.4.1 Bokstav a – forbindelsen mellom formålene

Etter artikkel 6 nr. 4 bokstav a skal det for det første tas hensyn til enhver forbindelse mellom formålene som personopplysningene har blitt samlet inn for og formålene med den tiltenkte viderebehandlingen. Forbindelsen mellom opprinnelig formål og formålene ved viderebehandlingen kan sies å ligge i kjernen av uforenlighetsvurderingen.¹²²

I Artikkel 29-gruppens veileder fremheves det at det er innholdet i formålene og i selve relasjonen mellom disse, og ikke den språklige utformingen av formålene, som står sentralt

¹²¹ GDPR fortalepunkt 50 nr. 9 og 10.

¹²² A29 WP Opinion 03/2013, s. 23.

ved vurderingen. Hovedfokuset er hva sammenhengen mellom det opprinnelige formålet og formålene for viderebehandlingen går ut på.¹²³

Utgangspunktet er at jo større avstand det er mellom innsamlingsformålet og videre formål, desto mer problematisk vil det være å konstatere forenlighet.¹²⁴ Gjenbruk til ulike kontrollformål må antageligvis anses som en type bruk som sjeldent har nær sammenheng med det opprinnelige formålet. Et eksempel er der en arbeidstakers datatrafikk loggføres og overvåkes for å forhindre dataangrep. Kontrollformål kan i et slikt tilfelle være å benytte datatrafikken for å undersøke om arbeidstakeren jobber tilstrekkelig effektivt eller undersøke om det skjer klanderverdige forhold på arbeidsplassen. Slik bruk vil antageligvis ikke være påregnelig for den registrerte dersom bruken ikke er opplyst om på forhånd. Viderebehandling av personopplysninger til kontrollformål vil som utgangspunkt derfor vanskelig være forenlig med opprinnelig formål.¹²⁵

4.4.2 Bokstav b – konteksten for innsamlingen

Videre følger det av artikkel 6 nr. 4 bokstav b at det skal tas hensyn til konteksten personopplysningene har blitt samlet inn i, med særlig henblikk på forholdet mellom den registrerte og den behandlingsansvarlige. I fortalen fremgår det at det er relevant hvilke rimelige forventninger forholdet til den behandlingsansvarlige gir den registrerte om hva personopplysningene skal benyttes til.¹²⁶ Spørsmålet er særlig hvilke berettigede forventninger den aktuelle innsamlingskonteksten gir den registrerte om bruken. Jo mer overraskende den videre bruken er i lys av konteksten, desto mer sannsynlig er det at viderebehandlingen må anses uforenlig.¹²⁷ Dette henger sammen med hensynet til forutberegnelighet, som formålsbegrensningsprinsippet søker å ivareta.

Det følger uttrykkelig av bokstav b at forholdet mellom den registrerte og den behandlingsansvarlige er relevant for uforenlighetsvurderingen. Det er dermed sentralt å vurdere hva som er alminnelig og forventet praksis for typen relasjon som foreligger mellom den behandlingsansvarlige og den registrerte. Det er for eksempel relevant om den registrerte

¹²³ A29 WP Opinion 03/2013, s. 23.

¹²⁴ A29 WP Opinion 03/2013, s. 24.

¹²⁵ Skullerud (2018) s. 93.

¹²⁶ GDPR fortalepunkt 50 nr. 6.

¹²⁷ A29 WP Opinion 03/2013, s. 24.

var rettslig forpliktet til å dele de aktuelle personopplysningene.¹²⁸ Dersom innsamlingen av personopplysningene derimot bygger på et kontraktsforhold, vil styrkeforholdet mellom den behandlingsansvarlige og den registrerte være særlig relevant. Herunder kan det være betydningsfullt hvor enkelt det vil være for den registrerte å avslutte kontraktsforholdet og finne en alternativ leverandør av den aktuelle tjenesten. En annen konstellasjon foreligger der innsamlingen av personopplysninger bygger på den registrertes samtykke. I så fall kan omstendigheter som graden av frivillighet og hvor informert samtykket var, være av relevans.¹²⁹

Et interessant spørsmål er om det påvirker vurderingen dersom den registrerte er mindreårig, herunder om forholdet mellom den behandlingsansvarlige og den registrerte i så fall må vurderes annerledes. Svaret er antageligvis ja. Artikkel 29-gruppen angir at vurderingen av forholdet mellom den registrerte og den behandlingsansvaret bør innebære en evaluering av styrkeforholdet mellom disse.¹³⁰ Generelt må det sies å være et skjevere styrkeforhold i tilfeller der den registrerte er et barn. I slike tilfeller bør dette derfor tas høyde for i vurderingen av hvorvidt viderebehandling er uforenlig med opprinnelig formål.

4.4.3 Bokstav c – personopplysningenes art

Etter artikkel 6 nr. 4 bokstav c skal det også legges vekt på personopplysningenes art. Det er særlig relevant om opplysningene som behandles inngår i «særlige kategorier av personopplysninger» etter artikkel 9 eller om opplysningene gjelder straffedommer og lovovertridelser i henhold til artikkel 10.

Personvernforordningen artikkel 9 angir at personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering inngår i det som kalles «særlige kategorier av personopplysninger». Denne typen opplysninger kan også omtales som *sensitive*

¹²⁸ A29 WP Opinion 03/2013, s. 24.

¹²⁹ A29 WP Opinion 03/2013, s. 24.

¹³⁰ A29 WP Opinion 03/2013, s. 24.

personopplysninger.¹³¹ Eksempler på slike personopplysninger er opplysninger om legebesøk, graviditet eller hvilket parti noen stemte på ved forrige stortingsvalg.

Vet at de nevnte kategoriene personopplysninger er eksplisitt angitt er det naturlig å forstå bestemmelsen slik at det stilles strengere krav til uforenlighetsvurderingen ved viderebehandling av slike personopplysninger enn andre typer personopplysninger.¹³² Dette kan også antas å henge sammen med at den registrerte antageligvis har en større forventning om konfidensialitet i slike tilfeller enn der det er tale om mindre beskyttelsesverdige opplysninger.¹³³ Samtidig må artikkel 6 nr. 4 bokstav c forstås slik at viderebehandling av særlige kategorier av personopplysninger ikke kategorisk utelukkes. Generelt vil det være slik at jo mer sensitive personopplysninger det er tale om, desto snevrere er adgangen til viderebehandling.¹³⁴ Ved behandling av særlige kategorier av personopplysninger oppstiller artikkel 9 særlige krav til behandlingen, hvilket også kan fungere som en skranke mot viderebehandling. Disse særlige kravene behandles ikke nærmere her.

4.4.4 Bokstav d – mulige konsekvenser

Et ytterligere moment som skal hensyntas i uforenlighetsvurderingen er de mulige konsekvensene den tiltenkte viderebehandlingen kan medføre for de registrerte, jf. artikkel 6 nr. 4 bokstav d. Nasjonale og internasjonale regelverk om vern av personopplysninger, herunder personvernforordningen, tar sikte på å beskytte individer mot ulike konsekvenser av feilaktig eller overflødig bruk av personopplysninger. Dermed er det naturlig at de mulige konsekvensene ved viderebehandling er et sentralt moment i uforenlighetsvurderingen.¹³⁵

Både positive og negative konsekvenser skal tas i betraktning.¹³⁶ Mulige konsekvenser ved viderebehandling kan knytte seg til handlinger eller avgjørelser som gjøres i fremtiden eller som treffes av tredjeparter. Andre konsekvenser kan være at behandlingen fører til utelukkelse eller diskriminering av individer. Konsekvensene kan også relatere seg til *måten* personopplysningene viderebehandles på, eksempelvis dersom opplysningene blir publisert

¹³¹ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/spesielt-om-sarlige-kategorier-av-personopplysninger-sensitive-personopplysninger-og-unntak/> (sist besøkt 04.11.20).

¹³² Skullerud (2018) s. 93.

¹³³ Skullerud (2018) s. 93.

¹³⁴ A29 WP Opinion 03/2013, s. 25.

¹³⁵ A29 WP Opinion 03/2013, s. 25.

¹³⁶ A29 WP Opinion 03/2013, s. 25.

offentlig eller på annen måte tilgjengeliggjort for en stor personkrets eller dersom opplysningene blir sammenstilt med andre opplysninger, eksempelvis for profilerings- eller markedsføringsformål. Slike konsekvenser er særlig relevante dersom de fremstod lite forutsigbare på innsamlingstidspunktet.¹³⁷

Antageligvis vil viderebehandling som oftest innebære en risiko for negative konsekvenser for den registrerte, men det kan også tenkes tilfeller der viderebehandling har positive følger. Et eksempel som illustrerer dette er dersom en bilprodusent oppdager en alvorlig produksjonsfeil i en bil som allerede er på markedet og får tilgang til en liste over aktuelle bileiere hentet ut fra et offentlig kjøretøyregister for å varsle disse. Det er åpenbart i de registrertes, i dette tilfellet bileiernes, interesse å bli varslet om risikoen for å havne i alvorlige ulykker som følge av produksjonsfeilen. Viderebehandling av eieropplysningene til dette formålet har dermed positive konsekvenser for de registrerte. Andre omstendigheter må selvsagt også tas i betraktning, som risikoen for at bilprodusenten misbruker opplysningene for andre formål eller lagrer opplysningene på en uforsvarlig måte, men eksempelet illustrerer likefullt at viderebehandling kan være i den registrertes interesse.¹³⁸

Ifølge artikkel 29-gruppen skal også konsekvenser av følelsesmessig karakter tas i betraktning ved vurderingen av hvilke konsekvenser viderebehandling kan medføre. Som eksempel på følelsesmessige konsekvenser nevnes den irritasjonen eller frykten eller det ubehaget som kan oppstå som følge av at den registrerte opplever at hun eller han mister kontroll over personopplysningene sine.¹³⁹

Generelt må utgangspunktet være at jo mer negative og uforutsigbare konsekvenser viderebehandlingen kan ha for den registrerte, desto mer sannsynlig er det at viderebehandlingen anses som uforenlig.¹⁴⁰

4.4.5 Bokstav e – sikkerhetstiltak

Etter artikkel 6 nr. 4 bokstav e skal det også tas hensyn til om det foreligger «nødvendige garantier». Kryptering og pseudonymisering angis som eksempler på tiltak som kan utgjøre tilfredsstillende personverngarantier. Disse begrepene forklares nærmere lenger ut i

¹³⁷ A29 WP Opinion 03/2013, s. 26.

¹³⁸ Eksempelet er hentet fra A29 WP Opinion 03/2013, s. 63-64.

¹³⁹ A29 WP Opinion 03/2013, s. 26.

¹⁴⁰ A29 WP Opinion 03/2013, s. 26.

underkapittelet. Bokstav e tilsier at det er relevant for uforenlighetsvurderingen hvilke sikkerhetstiltak som har blitt gjort eller kan gjøres av den behandlingsansvarlige for å sikre forsvarlig behandling, herunder ved unngå unødvendige konsekvenser for den registrerte som følge av viderebehandlingen. Dersom andre aspekter ved uforenlighetsvurderingen tilsier at viderebehandling er uforenlig, kan dette i noen tilfeller avhjelpest ved at det iverksettes tiltak som sikrer ivaretagelsen av den registrertes personvern. Dermed kan tilstrekkelig gode sikkerhetstiltak i prinsippet kompensere for svakheter på andre områder.¹⁴¹

Nødvendige garantier kan skje i form av at den behandlingsansvarlige foretar informasjonssikkerhetstiltak til den registrertes fordel. Det kan eksempelvis være tale om en streng etterlevelse av prinsippene om åpenhet og dataminimering, slik at behandlingen preges av transparens og er begrenset til hva som er strengt nødvendig, eller gjennom tydeliggjøring av den registrertes rett til å protestere.¹⁴²

Nødvendige garantier kan også skje gjennom tekniske tiltak. Slike tekniske tiltak gjør det mulig å beskytte personvernvernet bedre, i tillegg til at man potensielt kan dra nytte av personopplysninger selv om hjemmelen for å behandle opplysninger i identifiserbar form ikke foreligger.¹⁴³ Kryptering angis som et mulig tiltak som kan bøte på eventuelle negative konsekvenser ved viderebehandling av personopplysninger. Kryptering er betegnelsen på tiltak som kan benyttes for å gjøre personopplysninger vanskelig tilgjengelig for uvedkommende.¹⁴⁴ Det er tale om systemtekniske tiltak som omformer data slik at uvedkommende ikke kan forstå dataenes semantiske innhold, det vil si selve informasjonen som dataene uttrykker. For å få tilgang på innholdet må dataene dekrypteres med en kjent nøkkel.¹⁴⁵

Et annet tiltak som nevnes eksplisitt i artikkel 6 nr. 4 bokstav e er pseudonymisering. Pseudonymisering går ut på å behandle personopplysninger på en slik måte at personopplysningene ikke kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger. Slike tilleggsopplysninger må lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert

¹⁴¹ A29 WP Opinion 03/2013, s. 26.

¹⁴² A29 WP Opinion 03/2013, s. 26.

¹⁴³ Eva Jarbekk og Simen Sommerfelt, *Personvern og GDPR i praksis*, Cappelen Damm 2019, s. 184.

¹⁴⁴ Schartum (2016) s. 306.

¹⁴⁵ Schartum (2016) s. 307.

eller identifiserbar fysisk person.¹⁴⁶ Pseudonymisering kan gjøres enkelt, eksempelvis ved å bytte navn på en person eller skifte ut et personnummer.¹⁴⁷ Pseudonymisering er et nyttig sikkerhetstiltak, men sikrer imidlertid ikke fullstendig anonymisering, ettersom det fortsatt kan være mulig å identifisere individer.¹⁴⁸ I en egen veileder om anonymisering har Artikkel 29-gruppen påpekt at oppfatningen om at pseudonymiserte datasett er anonymiserte er en «common mistake(..)».¹⁴⁹

Anonymisering fordrer nemlig irreversibel aidentifisering, hvilket innebærer at anonymiseringsprosessen ikke skal kunne reverseres.¹⁵⁰ Med aidentifisering menes her tilfeller der navn, personnummer eller andre personentydige kjennetegn er fjernet.¹⁵¹ Det er følgelig en høy terskel for når personopplysninger kan anses å være anonymiserte. Det viser seg også at opplysninger i datasett som i utgangspunktet hevdes å være anonymiserte, i noen tilfeller likevel kan knyttes tilbake til enkeltindivider. Et eksempel er tilfellet nevnt innledningsvis, der NRK avdekket at lokasjonsdata, som i utgangspunktet var anonymiserte, kunne sammenholdes og slik benyttes til å identifisere enkeltindivider og kartlegge bevegelsesmønstrene deres. I slike tilfeller var det antageligvis aldri tale om reell anonymisering. Dette understreker at graden av reell beskyttelse i de ulike sikkerhetstiltakene som den behandlingsansvarlige iverksetter må tas i betraktning.

På bakgrunn av dette kan vurderingen etter artikkel 6 nr. 4 bokstav e sies å skille seg fra vurderingene som de øvrige bokstavene i artikkelen gir anvisning på. Vurderingen etter bokstav e handler ikke om sammenhengen mellom det opprinnelige formålet og viderebehandlingen, men om i hvilken grad iverksettelse av tiltak kan bøte på de negative konsekvensene ved viderebehandling.¹⁵² I hvilken grad slike tiltak kan resultere i at viderebehandling likevel ikke er å regne som uforenlig er imidlertid uklart. Momentet må i alle tilfeller inngå i den helhetsvurderingen som artikkel 6 nr. 4 legger opp til.

4.4.6 Oppsummering av artikkel 6 nr. 4

¹⁴⁶ Definisjonen fremgår av GDPR artikkel 4 nr. 5.

¹⁴⁷ Jarbekk (2019) s. 184.

¹⁴⁸ GDPR fortalepunkt 26 nr. 2.

¹⁴⁹ A29 WP Opinion 05/2014, s. 21.

¹⁵⁰ A29 WP Opinion 05/2014, s. 7.

¹⁵¹ <https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/> (sist besøkt 10.11.20).

¹⁵² Skullerud (2018) s. 94.

På bakgrunn av gjennomgangen av vurderingsmomentene er det klart at uforenlighetsvurderingen i svært stor grad bygger på de konkrete omstendighetene i den aktuelle behandlingssituasjonen, og at uforenlighet dermed må avgjøres individuelt i det enkelte tilfelle.

Dersom den behandlingsansvarlige kan konkludere med at viderebehandling ikke er uforenlig med det opprinnelige formålet opplysningene ble samlet inn for, kreves ikke noe nytt behandlingsgrunnlag.¹⁵³ Dette kan anses å følge av en betraktning om at så lenge det nye behandlingsformålet er ikke er uforenlig med det opprinnelige formålet, vil det opprinnelige behandlingsgrunnlaget være dekkende for den videre behandlingen.¹⁵⁴ Dersom viderebehandling derimot anses uforenlig foreligger ikke rettslig grunnlag for viderebehandlingen, med den følge at opplysningene må samles inn på nytt dersom de skal kunne behandles for det nye formålet.¹⁵⁵

Dersom en behandlingsansvarlig baserer seg på forenlighet som grunnlag for viderebehandling må vedkommende kunne vise at det har blitt foretatt en uforenlighetsvurdering der alle relevante omstendigheter har blitt tatt i betraktning, herunder påvise at momentene som er angitt i artikkel 6 nr. 4 har blitt overveid.¹⁵⁶ Listen med momenter angitt i artikkel 6 nr. 4 er ikke uttømmende, og det kan dermed være relevant å ta høyde for andre omstendigheter ved uforenlighetsvurderingen.

Visse aspekter ved reguleringen i artikkel 6 nr. 4 er fremdeles uavklarte. Et eksempel er hvorvidt momentene i artikkel 6 nr. 4 kan tas til inntekt for at viderebehandling kan være tillatt selv om et nytt formål i liten grad korrelerer med opprinnelig formål, gitt at tilstrekkelige beskyttende garantier har blitt iverksatt, eksempelvis pseudonymisering.¹⁵⁷ Det er usikkert i hvilken grad slike sikkerhetstiltak kan avhjelpe svakhet på andre punkter i uforenlighetsvurderingen. Videre er det eksempelvis også uklart i hvilken grad viderebehandling av «særlige kategorier av personopplysninger» fordrer en særlig nær forbindelse mellom opprinnelig formål og formålene ved viderebehandlingen eller særlig tilfredsstillende sikkerhetstiltak for ikke å være uforenlig med opprinnelig formål. Begge disse eksemplene knytter seg til hvordan de ulike vurderingsmomentene skal balanseres opp

¹⁵³ GDPR fortalepunkt 50 nr. 2.

¹⁵⁴ Skullerud (2018) s. 95.

¹⁵⁵ Prop. 56 LS (2017-2018) s. 37.

¹⁵⁶ Kuner (2020) s. 343.

¹⁵⁷ Kuner (2020) s. 343.

mot hverandre. Slike spørsmål vil antageligvis avklares etterhvert som personvernforordningen får mer solid fotfeste og forordningens regler prøves av EU-domstolen.

4.5 Rettspraksis som belyser adgangen til viderebehandling

Som nevnt innledningsvis har jeg ikke lyktes i å finne rettspraksis fra EU-domstolen, norske domstoler eller andre lands domstoler som gjelder formålsbegrensningsprinsippet etter GDPR og som dermed berører selve vurderingen av når viderebehandling for andre formål er uforenlig med det opprinnelige formålet, herunder ved anvendelse av GDPR artikkel 6 nr. 4.¹⁵⁸ EU-domstolen synes faktisk ikke å ha behandlet eller tatt i betraktning uforenlighetsvilkåret i formålsbegrensningsprinsippet i det hele tatt. I tilfeller der domstolen kunne ha tematisert forbudet mot uforenlig viderebehandling for å vurdere om det foreligger brudd på retten til respekt for privatlivet etter EU-pakten, har domstolen heller fokusert på andre aspekter.¹⁵⁹

Ettersom personvernforordningens formålsbegrensningsprinsipp er en videreføring av et eksisterende prinsipp, vil det imidlertid være relevant å analysere rettspraksis som gjelder formålsbegrensningsprinsippet forut for personvernforordningen. Denne rettspraksisen viser hvordan domstoler har forholdt seg til og forholder seg til formålsbegrensningsprinsippet. Ved at det er tale om rettspraksis forut for personvernforordningen, anvendes ikke momentene i forordningen artikkel 6 nr. 4 direkte. Dommene illustrerer likevel hvilke omstendigheter som har blitt ansett som sentrale i vurderingen.

Den europeiske menneskerettsdomstolen har til en viss grad befattet seg med formålsbegrensningsprinsippet. Domstolen har ikke vist til prinsippet direkte, men i saker som omhandler viderebehandling av personopplysninger har domstolen anvendt flere av de

¹⁵⁸ Det finnes imidlertid forespørsler om forhåndsavgjørelser som er forelagt for EU-domstolen hvor domstolen bes klargjøre tolkningen av GDPR artikkel 5 nr. 1 bokstav b. Et eksempel er forespørsel om slik forhåndsavgjørelse i saken *B v Latvijas Republikas Saeima* (Case C-439/19).

¹⁵⁹ Betragtningen er hentet fra en doktorgradsavhandling om formålsbegrensningsprinsippet. Forfatteren skriver følgende om tematikken: «*From the case law investigated for this study the following conclusion can be drawn: In the assessment of the establishment of an interference with and the impact on the rights protected under the Charter the CJEU has never taken into account the role of the non-incompatibility requirement*» (side 139). Merel Elize Koning, *The purpose and limitations of purpose limitation*, 2020, tilgjengelig på https://merelkoning.nl/wp-content/uploads/2020/10/M.Koning_The-purpose-and-limitations-of-purpose-limitation_thesis.pdf (sist besøkt 25.11.20).

samme vurderingsmomentene som de som nå fremgår av GDPR artikkel 6 nr. 4 i vurderingen av om retten til respekt for privatlivet er krenket. Et eksempel er dommen *M.S. v Sweden*.¹⁶⁰ Dommen gjaldt et tilfelle der et sykehus hadde formidlet helseopplysninger om en kvinnelig pasient, uten kvinnens samtykke, til den svenske *Försäkringskassan*. *Försäkringskassan* benyttet deretter opplysningene i forbindelse med avgjørelsen av kvinnens søknad om erstatning under yrkesskadeforsikringslovgivningen. Søknaden ble avslått. Kvinnen klaget saken inn for EMD under henvisning til at utleveringen av helseopplysningene krenket retten til respekt for privatlivet etter EMK artikkel 8 nr. 1. Retten fant at det dreide seg om viderebehandling av de aktuelle personopplysningene utover hva den registrerte kunne forvente, og at dette medførte krenkelse av kvinnens rett til respekt for sitt privatliv:

*The Court notes that the medical records in question contained highly personal and sensitive data about the applicant, including information relating to an abortion. Although the records remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants (...). Moreover, whilst the information had been collected and stored at the clinic in connection with medical treatment, its subsequent communication had served a different purpose, namely to enable the Office to examine her compensation claim. It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office (...). Having regard to these considerations, the Court finds that the disclosure of the data by the clinic to the Office entailed an interference with the applicant's right to respect for private life guaranteed by paragraph 1 of Article 8 (min understrekning).*¹⁶¹

Dommen anvender hverken formålsbegrensningsprinsippet eksplisitt eller bidrar til å avklare rekkevidden av adgangen til viderebehandling, men illustrerer likefullt at domstolen var bevisst den registrertes berettigede forventninger rundt bruken av personopplysningene i vurderingen av hvorvidt retten til respekt for privatlivet var krenket.¹⁶² EMD konkluderte imidlertid med at den aktuelle behandlingen var lovlig etter EMK artikkel 8 nr. 2.

¹⁶⁰ *M.S. v. Sweden* [J] 1997, no. 20837/92.

¹⁶¹ Dommens avsnitt 35.

¹⁶² Bygrave (2014) s. 154.

En annen dom fra EMD er *S. and Marper v. The United Kingdom*.¹⁶³ Heller ikke denne gjelder formålsbegrensningsprinsippet direkte, men dommen viser hvordan EMD har anvendt både de mulige konsekvensene ved eventuell viderebehandling og personopplysningenes art som momenter i vurderingen av om retten til respekt for privatlivet er krenket. Dommen gjaldt spørsmål om hvorvidt det å beholde DNA-prøver av arresterte personer som senere blir frifunnet eller hvor tiltalen droppes innebærer en krenkelse av retten til respekt for privatlivet. Retten tematiserte blant annet «the rapid pace of developments in the field of genetics and information technology», hvilket etter rettens syn innebar en mulighet for at «the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today».¹⁶⁴ Retten foretok med dette en vurdering av hvilke mulige konsekvenser eventuell viderebehandling av DNA-prøvene kunne få i fremtiden. Videre viste retten til at DNA-prøver er av «highly personal nature» og at slike prøver «contain much sensitive information about an individual, including information about his or her health».¹⁶⁵ Personopplysningenes art ble dermed også vektlagt i vurderingen av om det forelå en krenkelse.

En sak fra norske domstoler er Avfallsservice-dommen.¹⁶⁶ I dommen vurderte Høyesterett blant annet lovligheten av gjenbruk av innsamlede opplysninger for andre formål enn det opprinnelige formålet. En sjåfør ansatt i renovasjonsfirmaet Avfallsservice AS ble sagt opp på grunnlag av avvik mellom timelistene og bilens elektroniske logg. Vedkommende anførte at det forhold at hans timelister ble sammenholdt med de elektroniske rapportene for å avdekke eventuelle brudd på arbeidspliktene innebar en ny type bruk av hans personopplysninger, i strid med personopplysningsloven. Vurderingen av hvorvidt viderebehandlingen var lovlig ble foretatt etter den dagjeldende personopplysningsloven § 11.¹⁶⁷ Lovens § 11 første ledd bokstav c påla den behandlingsansvarlige å sørge for at personopplysninger som behandles «ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker». Bestemmelsen ga følgelig uttrykk for formålsbegrensningsprinsippet.

¹⁶³ *S. and Marper v. The United Kingdom* [GC] 2008 nos. 30562/04 og 30566/04.

¹⁶⁴ Dommens avsnitt 71.

¹⁶⁵ Dommens avsnitt 72.

¹⁶⁶ Rt. 2013 s. 143.

¹⁶⁷ Lov 14. april 2000 nr. 31 om behandling av personopplysninger. Loven gjennomførte personverndirektivet i norsk rett.

Spørsmålet retten tok stilling til var om formålet med behandlingen var «uforenlig» med det opprinnelige formålet. Retten konstaterte først at kontroll av en arbeidstaker i den hensikt å avdekke mulige brudd på vedkommendes arbeidsplikter var et annet formål enn det opprinnelige.¹⁶⁸ Høyesterett viste så til at «kontrolltiltak ikke bare kunne være en ulempe for den som har noe å skjule, men også for den som ikke har noe å skjule», og at «generell overvåkning i arbeidslivet vil være en belastning».¹⁶⁹ Deretter foretok retten en nyansert vurdering av ulempene for arbeidstakeren. Her pekte retten på at opplysningene i loggen utelukkende var knyttet til vedkommendes arbeidsoppgaver, og at det således ikke dreide seg om informasjon av privat eller personlig karakter.¹⁷⁰ Dette illustrerer at retten vurderte personopplysningenes art, og at opplysningene ikke var av en slik karakter at arten alene talte for at viderebehandling var uforenlig. Videre ble den registrertes rimelige forventninger anvendt som vurderingsmoment. Retten uttalte at bruk av de aktuelle opplysningene til generell kontroll av de ansatte klart ville ha ligget utenfor hva A hadde rimelige forventninger om. Videre pekte retten på at hensynet til tillit i arbeidsforhold tilsier at en arbeidstaker som utgangspunkt bare kan forvente at personopplysninger brukes til kontrollformål «dersom det er gjort uttrykkelig oppmerksom på det på forhånd».¹⁷¹ Etter en samlet vurdering konkluderte retten med at viderebehandlingen av personopplysningene var uforenlig, med særlig vekt på at kontrollformålet skilte seg markert fra det opprinnelige formålet.

Dommen har som nevnt ikke rettskildemessig verdi for hvordan formålsbegrensningsprinsippet i personvernforordningen skal forstås. Den er likevel et eksempel hvordan en domstol har foretatt en bred helhetsvurdering for å avgjøre hvorvidt viderebehandling er uforenlig med opprinnelig formål. I tillegg illustrerer dommen hvordan ivaretagelsen av forutberegnelighetshensyn kan anvendes som et sentralt aspekt i vurderingen, ettersom den registrertes forventinger fremheves i dommen.

Videre finnes norsk rettspraksis som ikke tematiserer formålsbegrensningsprinsippet direkte, men som illustrerer diskusjonen rundt formålsbegrensning som ideal. Et eksempel er HR-2020-1776-A, en kjennelse som gjaldt spørsmålet om det var adgang til å pålegge en forskningsbiobank ved NTNU å utlevere vevsprøver fra et avdødt barn til bruk i

¹⁶⁸ Dommens avsnitt 55.

¹⁶⁹ Dommens avsnitt 56.

¹⁷⁰ Dommens avsnitt 58.

¹⁷¹ Dommens avsnitt 61.

etterforskning.¹⁷² Universitetet nektet å utlevere materialet under henvisning til helseforskningsloven § 27, hvor det fremgår at «[h]umant biologisk materiale fra forskningsbiobanker kan ikke utleveres i forsikringsøyemed, til arbeidsgiver, til påtalemyndighet eller til domstol, selv om den materialet stammer fra samtykker til det». Ved vurderingen av spørsmålet om helseforskningsloven § 27 var til hinder for utlevering av materialet pekte førstvoterende på at flere omstendigheter talte i favør av utlevering, blant annet hensynet til barnets beste.¹⁷³ Førstvoterende konkluderte likevel med at bestemmelsen ikke kunne tolkes innskrenkende. Ut over det forhold at lovens ordlyd var helt klar, fremhevet førstvoterende risikoen for formålsutglidning: «[f]or det andre kan utlevering i enkelttilfeller uten klar forankring i helseforskningsloven § 27 åpne for formålsutglidning og en generell svekkelse av tilliten til medisinsk- og helsefaglig forskning og forskningsbiobanker». Dommen fremhever risikoen for formålsutglidning som en uheldig konsekvens, som potensielt svekker befolkningens tillit til primærformålet. Selv om kjennelsen ikke bidrar til avklaring av formålsbegrensingsprinsippets rekkevidde, viser den at hensynet til å ivareta tilliten til den primære behandlingsaktiviteten kan være et sentralt argument ved spørsmål tilknyttet adgangen til viderebehandling av personopplysninger.

4.6 Øvrig praksis som belyser adgangen til viderebehandling

Datatilsynet er som nevnt Norges tilsynsmyndighet når det gjelder å sikre etterlevelsen av personvernforordningen. Personvernemnda er klageorgan for vedtak fattet av Datatilsynet. Vedtak fra nasjonale tilsynsmyndigheter har som påpekt i oppgavens del 1.3 begrenset rettskildemessig vekt. I vedtakene som det redegjøres for i det følgende tolket Datatilsynet og Personvernemnda norsk rett som var basert på personverndirektivet. Vedtakene illustrerer hvordan den aktuelle tilsynsmyndigheten har forholdt seg til formålsbegrensingsprinsippet.

I et relativt ferskt vedtak fra Datatilsynet ble Statens Vegvesen ilagt et overtredelsesgebyr for å ha behandlet personopplysninger til formål som var uforenlige med det opprinnelige formålet.¹⁷⁴ Det aktuelle bruddet skjedde før personopplysningsloven av 2018 trådte i kraft, og uforenlighetsvurderingen ble dermed foretatt etter personopplysningsloven av 2000 § 11

¹⁷² HR-2020-1776-A.

¹⁷³ Dommens avsnitt 38.

¹⁷⁴ Datatilsynets referanse 20/02199-1.

første ledd bokstav c. De aktuelle personopplysningene i saken var videoopptak fra fastmonterte veikameraer. Statens Vegvesen hadde ansvaret for disse kameraene. Formålet med kameraovervåkingen var trafikkavvikling og trafikksikkerhet. Det ble imidlertid avdekket at opptak fra veikameraene i omfattende grad hadde blitt brukt for å overvåke kontraktsparter, ansatte, underleverandører og ansatte hos underleverandørene i oppfølgingen av en kontrakt med selskapet Veidrift AS. Et av spørsmålene Datatilsynet måtte ta stilling til var dermed hvorvidt den nye bruken av opptakene fra veikameraene var uforenlig med det opprinnelige formålet. I uforenlighetsvurderingen viste Datatilsynet særlig til at den nye bruken var til betydelig ulempe for kontraktøren og hans ansatte, og lå betydelig utenfor hva kontraktøren kunne forvente at personopplysningene skulle brukes til.¹⁷⁵ Under henvisning til Avfallsservice-dommen viste Datatilsynet også til at hensynet til tillit i arbeidsforhold som utgangspunkt tilsier at man bare kan forvente at personopplysninger brukes til kontrollformål dersom den registrerte er gjort uttrykkelig oppmerksom på det på forhånd.¹⁷⁶ Datatilsynet konkluderte med at bruken av opplysningene til kontraktsoppfølging var uforenlig med det opprinnelige formålet.

Videre finnes det praksis fra Personvernemnda hvor nemnda har anvendt vurderingsmomentene i personvernforordningen artikkel 6 nr. 4. Et tilfelle gjald sletting av personopplysninger i en personalmappe etter avsluttet arbeidsforhold.¹⁷⁷ Det opprinnelige formålet med arbeidsgivers behandling av den registrertes personopplysninger var personaladministrasjon og ivaretagelse av arbeidsgivers plikter og den registrertes rettigheter etter arbeidsmiljøloven kapittel 2. Arbeidsforholdet opphørte, men arbeidsgiver beholdt opplysningene. Formålet med videre lagring var begrunnet i arbeidsgivers behov for å dokumentere saksbehandlingshistorikken i saken, særlig ved eventuelle senere klager eller søksmål, samt potensiell bruk i en senere søknadsprosess dersom arbeidstakeren søkte om ny ansettelse. Personvernemnda tok stilling til om disse nye formålene var forenlige med det opprinnelige formålet. Nemnda konkluderte positivt på dette spørsmålet. I begrunnelsen ble det for det første fremhevet at det var «nær forbindelse mellom de opprinnelige personaladministrative forholdene som begrunnet innsamling av personopplysningene og de nye forholdene som knytter seg til å dokumentere saksbehandlingen i det tidligere arbeidsforholdet, både ved en eventuell senere klage eller søksmål fra A samt ved en eventuell

¹⁷⁵ Vedtaket side 7.

¹⁷⁶ Vedtaket side 9.

¹⁷⁷ PVN-2018-15.

ny arbeidssøknad fra ham», ettersom opplysningene fortsatt skulle brukes «i den samme sammenhengen, dvs. arbeidsgiver-/arbeidstakerrelasjonen». Videre vurderte nemnda personopplysningenes art, og viste til at opplysningene «i svært liten grad representer[te] særlige kategorier av personopplysninger». Når det gjaldt mulige konsekvenser av viderebehandlingen viste nemnda til at disse ville gå ut på «å sikre en mer fullstendig opplysning av saksforholdet, både ved et eventuelt søksmål eller i en ny ansettelsesprosess». I den forbindelse uttalte nemnda at det ikke kunne tillegges avgjørende vekt dersom dette eventuelt resulterte i et dårligere resultat for den registrerte. Endelig pekte nemnda på at det var «lav risiko for at disse opplysningene spres videre til uvedkommende». Konklusjonen ble som nevnt at viderebehandlingen ble ansett forenlig med opprinnelig formål. Avgjørelsen fra nemnda er et pedagogisk og nyansert eksempel på hvordan uforenlighetsvurdering kan foretas.

5 Særlig om viderebehandling i Big data-sammenheng

En særlig problemstilling reises ved viderebehandling av personopplysninger i såkalt Big data-sammenheng. Som forklart innledningsvis i oppgaven refererer Big data, eller stordata, til behandling av store mengder data som blir analysert for å identifisere trender og sammenhenger. Ved å sammenstille opplysninger fra en rekke ulike kilder blir det mulig å oppdage nye mønstre og sammenhenger.¹⁷⁸ Stordatanalyser benyttes av både selskaper, myndigheter og andre organisasjoner, eksempelvis i forbindelse med helsetjenester, markedsføring, infrastruktur og mobiltelefoni. Sammenstilling av personopplysninger på nye måter gjør det mulig å levere bedre og mer effektive tjenester. Slike analyser gir følgelig et stort potensial for innovasjon.¹⁷⁹ Samtidig kan Big data utgjøre en risiko for vern av personopplysninger og retten til respekt for privatlivet. Artikkel 29-gruppen har fremhevet flere risikopunkter, blant annet risikoen for at sikkerheten ved behandlingen svekkes jo større mengder data det er tale om, manglende åpenhet for den registrerte og økte muligheter for overvåkning fra myndighetsorganer.¹⁸⁰

I en rapport om Big data forfattet av Datatilsynet vises det til at Big data «i stor grad [handler] om å hente ut sekundærverdi av innsamlede data», og at Big data derfor kan utfordre formålsbegrensningsprinsippet.¹⁸¹ På tilsvarende måte som for annen type viderebehandling er det i utgangspunktet uforenlighetsvurderingen som avgjør om viderebehandling i Big-data sammenheng er lovlig. Momentene i artikkel 6 nr. 4, som er behandlet inngående i oppgavens del 4.4, legger føringer for vurderingen. De konkrete omstendighetene avgjør om viderebehandling er å anse som uforenlig.

Som omtalt tidligere i oppgaven fremgår det av personvernforordningen artikkel 5 nr. 1 bokstav b at viderebehandling anses forenlig med det opprinnelige formålet dersom slik behandling skjer for vitenskapelig eller historisk forskning, statistiske formål eller arkivformål i allmennhetens interesse. Personopplysninger kan viderebehandles for slike

¹⁷⁸ Bart Custers og Helena Ursic, «Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection» *International Data Privacy Law*, 6 (2016) nr. 1, s. 4-15, på s. 5.

¹⁷⁹ A29 WP Opinion 03/2013, s. 35.

¹⁸⁰ A29 WP Opinion 03/2013, s. 35.

¹⁸¹ Datatilsynet, Big Data – personvernprinsipper under press (2013), s. 24. Tilgjengelig på https://www.datatilsynet.no/globalassets/global/dokumenter-pdf/rettigheter-og-plikter/rapporter/big-data_web.pdf (sist besøkt 23.11.20).

formål såfremt behandlingen tilfredsstillende «nødvendige garantier» etter forordningens artikkel 89. Disse formålene kan regnes som privilegerte formål («privileged purposes») i den europeiske personvernlovgivningen.¹⁸² Formålenes særstilling kan knyttes til ideen om kunnskapssamfunnet, med forventninger om stadig økt kunnskap og opplysning.¹⁸³ I tillegg er det en kjensgjerning at det kan være vanskelig å forutse, og dermed spesifisere, all fremtidig, ønskelig bruk allerede på innsamlingstidspunktet. På bakgrunn av unntaksregelen i artikkel 5 nr. 1 bokstav b vil formålsbegrensningsprinsippet ikke være til hinder for Big data-analyser som innebærer viderebehandling av personopplysninger for vitenskapelige eller statistiske formål, forutsatt at kravet til nødvendige garantier er oppfylt.¹⁸⁴

Formålsbegrensningsprinsippetets første dimensjon, nemlig kravet til at behandlingens formål er spesifikt, uttrykkelig angitt og berettiget på innsamlingstidspunktet, må imidlertid fortsatt være tilfredsstillende.

Unntaket i GDPR artikkel 5 nr. 1 bokstav b for viderebehandling til vitenskapelig eller historisk forskning, statistiske formål eller arkivformål vil ikke kunne anvendes i tilfeller der viderebehandlingen utelukkende er kommersielt begrunnet. Formålsbegrensningsprinsippet vil derfor særlig kunne representere en skranke for kommersielle Big data-analyser.¹⁸⁵

Eventuell viderebehandling til Big data-formål beror på om slik viderebehandling er uforenlig med det opprinnelige formålet. Her vil blant annet forbindelsen mellom formålene være et sentralt vurderingsmoment, samt om det er mulig å iverksette sikkerhetstiltak for å verne den registrertes personvern, eksempelvis gjennom pseudonymisering.

Formålsbegrensningsprinsippetets krav til formålsspesifisering, herunder kravet om at formålet må være spesifikt angitt, forhindrer at behandlingsansvarlige kan forsøke å omgå hele uforenlighetsproblematikken ved å angi formålet for den opprinnelige behandlingsaktiviteten på en vid eller vag måte.

I kommersielt begrunnede Big data-analyser vil antageligvis den beste – og ofte eneste – løsningen være å innhente et separat samtykke som omfatter analyseformålene. Slik blir bruken av personopplysninger i analysesammenheng også mest mulig forutberegnelig og åpen for den registrerte. Et eksempel er dersom en sosiale medier-plattform innhenter samtykke til

¹⁸² Forgó, Nikolaus, Hänold, Stefanie og Schütze, Benjamin, «The principle of purpose limitation and big data», i *New Technology, Big Data and the Law*, Marcelo Corrales, Mark Fenwick og Nikolaus Forgó (red.), Springer 2017, s. 17-42, på s. 36.

¹⁸³ Koning (2020) s. 189.

¹⁸⁴ Forgó (2017) s. 40.

¹⁸⁵ Datatilsynet (2013) s. 39.

å benytte brukernes personopplysninger til egne formål, eksempelvis å utarbeide forslag til grupper eller arrangementer som den aktuelle brukeren antas å være interessert i, samt et separat samtykke til å kunne benytte og dele personopplysningene med tredjeparter i analysesammenheng. En utfordring i slike tilfeller er riktignok at det på innsamlingstidspunktet kan være uklart hvilke formål det er ønskelig å benytte opplysningene til på et senere tidspunkt. Formålsbegrensningsprinsippet gir dermed en klar oppfordring til å avklare eventuell videre bruk allerede på innsamlingstidspunktet. En annen utfordring er å sikre at samtykket er tilstrekkelig informert. Det kan være krevende å informere om komplekse dataanalyser, samt typer databehandling og kunnskapsinnhenting som potensielt ikke eksisterer på samtykketidspunktet, på en tilstrekkelig god måte.¹⁸⁶

En alternativ løsning for å kunne benytte personopplysninger til sekundærformål gjennom Big data-analyser uten å krenke formålsbegrensningsprinsippet er å sørge for anonymisering av opplysningene.¹⁸⁷ Anonymiseringen må være reell. Dersom opplysningene ikke lenger kan knyttes til en identifisert eller identifiserbar person, er det ikke tale om personopplysninger i forordningens forstand og behandlingen er ikke lenger regulert av personvernforordningen.¹⁸⁸ Her må imidlertid faren for re-identifikasjon tas høyde for. Videre faller selve anonymiseringen av personopplysninger innunder definisjonen av «behandling» i GDPR artikkel 4 nr. 2 og fordrer dermed et behandlingsgrunnlag.

Uansett er det på høy tid med ytterligere diskusjon rundt formålsbegrensningsprinsippet og ny teknologi, herunder Big data-analyser. Slike analyser kan være verdifulle på mange samfunnsområder, og det er som nevnt et stort potensial for innovasjon.

Formålsbegrensningsprinsippet strengt praktisert legger åpenbart en demper for muligheten for slik innovasjon og utvikling. Kanskje er dette riktig, nettopp fordi personvern er en grunnleggende verdi og forutberegnelighet for enkeltindividet når det gjelder bruken av dets personopplysninger et viktig ideal. Formålsbegrensningsprinsippet bidrar unektelig til å fremme individets kontroll over sine personopplysninger i slike sammenhenger.

¹⁸⁶ Custers (2016) s. 11.

¹⁸⁷ Datatilsynet (2013) s. 40.

¹⁸⁸ GDPR fortalepunkt 26 nr. 5.

6 Avsluttende betraktninger

Gjennom oppgaven har innholdet i og rekkevidden av formålsbegrensningsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav b blitt gjort rede for. Fremstillingen har vist at det ikke er mulig å gi et entydig svar på oppgavens problemstilling, nemlig i hvilken grad personopplysninger kan viderebehandles for andre formål enn det opprinnelige formålet. Årsaken er at det må foretas en konkret vurdering i det enkelte viderebehandlingstilfelle, der en rekke omstendigheter skal tas i betraktning for å avgjøre om viderebehandlingen er uforenlig. Fremstillingen har imidlertid forsøkt å avklare innholdet i vilkåret *uforenlig*, hvilket er et viktig skritt i avklaringen av formålsbegrensningsprinsippet innhold, herunder adgangen til viderebehandling.

Det er utvilsomt at innføringen av vurderingsmomentene i forordningens artikkel 6 nr. 4 har bidratt til klargjøring av innholdet i uforenlighetsvurderingen og dermed også rekkevidden av adgangen til viderebehandling. Listen er ikke uttømmende, men momentene viser likefullt hvilke aspekter som er av betydning ved vurderingen av hvorvidt viderebehandling til nye formål er forenlig eller uforenlig. Det at disse momentene nå er inntatt i forordningen bidrar forhåpentligvis til økt oppmerksomhet rundt uforenlighetsvurderingen, i tillegg til å lette etterlevelsen av formålsbegrensningsprinsippet forbud mot uforenlig viderebehandling.

Selv om personvernforordningen på denne måten har bidratt til avklaring av rekkevidden av adgangen til viderebehandling av personopplysninger, gjenstår noe usikkerhet tilknyttet anvendelsen, eksempelvis vedrørende hvordan de ulike momentene i uforenlighetsvurderingen skal veies mot hverandre. Det er blant annet usikkert i hvilken utstrekning ulike sikkerhetstiltak, for eksempel pseudonymisering, kan avhjelpe svak forbindelse mellom opprinnelig formål og formålet for viderebehandlingen. Det er behov for rettspraksis som klargjør rettstilstanden ytterligere. EU-domstolen har imidlertid ikke befattet seg med formålsbegrensningsprinsippet etter personvernforordningen hittil, og dermed heller ikke foretatt noen uforenlighetsvurdering hvor momentene i artikkel 6 nr. 4 har blitt anvendt.

Opgaven har videre vist at formålsbegrensningsprinsippet kan vanskeliggjøre Big data-analyser, ettersom slike analyser dreier seg om å hente ut sekundærverdi av allerede innsamlede data. I mange tilfeller vil den behandlingsansvarlige antageligvis ikke kunne

basere seg på at viderebehandlingen ikke er uforenlig etter en uforenlighetsvurdering, og et samtykke som dekker analyseformålene kan derfor være avgjørende for lovligheten.

Uansett er det klart at uforenlighetsvurderingen må sees i lys av de hensyn som begrunner formålsbegrensningsprinsippet, særlig forutberegnelighet. Videre må vurderingen også ta høyde for forordningens formål og de øvrige grunnprinsippene for behandling av personopplysninger. Disse omstendighetene kan, ved siden av vurderingsmomentene i artikkel 6 nr. 4, gi veiledning for vurderingen av når viderebehandling av personopplysninger er forenlig eller uforenlig med opprinnelig formål.

7 Litteraturliste

7.1 Direktiver og forordninger

- Personverndirektivet** Europaparlamentets og Rådets direktiv 95/46/EF av 24 oktober 1995 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.
- Personvernforordningen** Europaparlamentets og Rådets forordning (EU) 2016/679 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.
- Direktiv (EU) 2016/680** Europaparlamentets og Rådets direktiv (EU) 2016/680 av 27. april 2016 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning 2008/977/JIS.

7.2 Traktater, konvensjoner m.m.

- EMK** Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 (Den europeiske menneskerettighetskonvensjonen).

OECD-retningslinjene	OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23. september, 1980.
Europarådskonvensjonen	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28. januar, 1981.
EU-Pakten	Charter of Fundamental rights of the European Union (2012/C 326/02) (EUs pakt om grunnleggende rettigheter).

7.3 Norske lover og forskrifter

Personopplysningsloven 2000 Lov 14. april 2000 nr. 31 om behandling av personopplysninger.

Endringslov til politiregisterloven mv. Lov 21. juni 2017 nr. 94 om endringer i politiregisterloven mv. (gjennomføring av direktiv (EU) 2016/680 mv.).

Personopplysningsloven 2018 Lov 15. juni 2018 nr. 38 om behandling av personopplysninger.

Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale
Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale 2. juli 2018 nr. 1108.

7.4 Lovforarbeider

Prop. 56 LS (2017–2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.

7.5 Rettspraksis

7.5.1 Rettspraksis fra EU-domstolen

Dom av 20. mai 2003 [GC], *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauerermann v Österreichischer Rundfunk*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294.

Dom av 19. juni 2014 [C5], *Karen Millen Fashions*, C-345/13, EU:C:2014:2013.

Forespørsel om forhåndsuttalelse av 11. juni 2019, *B v Latvijas Republikas Saeima*, C-439/19).

7.5.2 Rettspraksis fra Den europeiske menneskerettighetsdomstolen

M.S. v. Sverige [J], ECHR:1997:0827JUD002083792.

S. and Marper v. The United Kingdom [GC], ECHR:2008:1204JUD003056204.

7.5.3 Norsk rettspraksis

Rt. 2013 s. 143 A.

HR-2020-1776-A.

7.6 Veiledere

Article 29 Data Protection Working Party, *Opinion 01/2010 on the concepts of "controller" and "processor"*, 00264/10/EN WP 169 [Tilgjengelig på https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf] (sist besøkt 1. desember 2020).

Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 00569/13/EN WP 203 [Tilgjengelig på https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf] (sist besøkt 1. desember 2020).

Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216 [Tilgjengelig på https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf] (sist besøkt 1. desember 2020).

7.7 Praksis fra nasjonale tilsynsmyndigheter

Datatilsynet, vedtak om overtredelsesgebyr av 25. august 2020, 20/02199-1.

Personvernemnda, avgjørelse av 18. mars 2019, PVN-2018-15.

7.8 Juridisk litteratur

- Bygrave (2014)** Bygrave, Lee A, *Data Privacy Law: An International Perspective*, Oxford University Press 2014.
- Custers (2016)** Custers, Bart og Ursic, Helena, «Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection» *International Data Privacy Law*, 6 (2016) nr. 1, s. 4-15.
- Forgó (2017)** Forgó, Nikolaus, Hänold, Stefanie og Schütze, Benjamin, «The principle of purpose limitation and big data», i *New Technology, Big Data and the Law*, Marcelo Corrales, Mark Fenwick og Nikolaus Forgó (red.), Springer 2017, s. 17-42.
- Jarbekk (2019)** Jarbekk, Eva og Sommerfelt, Simen, *Personvern og GDPR i praksis*, Cappelen Damm 2019.
- Fredriksen (2018)** Fredriksen, Halvard Haukeland og Mathisen, Gjermund, *EØS-rett*, 3. utg., Fagbokforlaget 2018.
- Koning (2020)** Koning, Merel Elize, *The purpose and limitations of purpose limitation*, 2020, [Doktorgradsavhandling], [tilgjengelig på https://merelkoning.nl/wp-content/uploads/2020/10/M.Koning_The-purpose-and-limitations-of-purpose-limitation_thesis.pdf] (sist besøkt 25. november 2020).

- Kuner (2020)** Kuner, Christopher, Bygrave, Lee A, Docksey, Christopher og Drechsler, Laura, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press 2020.
- Schartum (2016)** Schartum, Dag Wiese og Bygrave, Lee A, *Personvern i informasjonssamfunnet*, Fagbokforlaget 2016.
- Skullerud (2018)** Skullerud, Åste Marie Bergseng, Rønnevik, Cecilie, Skorstad, Jørgen og Pellerud, Marius Engh, *Personvernforordningen (GDPR) Kommentarutgave*, Universitetsforlaget 2018.
- Wessel-Aas (2018)** Wessel-Aas, Jon og Ødegaard, Magnus, *Personvern – publisering og behandling av personopplysninger*, Gyldendal 2018.

7.9 Andre kilder

7.9.1 Artikler

Furuly, Trude, Lied, Henrik og Gundersen, Martin «Avslørt av mobilen», NRK, 9. mai 2020, <https://www.nrk.no/norge/xl/avslort-av-mobilen-1.14911685> (sist besøkt 21. november 2020).

Indregard, Sigve «Bekjempe pandemi? «Det finnes en app for det»», Agenda Magasin, 30. mai 2020 <https://agendamagasin.no/kommentarer/bekjempe-pandemi-finnes-app/> (sist besøkt 25. november 2020).

Mestad, Adele og Skre, Alf Butenschøn «Vi må velge mellom pest og kolera. Appen Smittestopp kan være en middelvei», Aftenposten, 17. apr. 2020 <https://www.aftenposten.no/meninger/kronikk/i/GGLLVm/vi-maa-velge-mellom-pest-og-kolera-appen-smittestopp-kan-vaere-en-midde> (sist besøkt 25. november 2020).

7.9.2 Internettkilder

Datatilsynet, *Ordlister*, u.å., <https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/> (sist besøkt 10. november 2020).

Datatilsynet, *Spesielt om særlige kategorier av personopplysninger (sensitive personopplysninger) - forbud og unntak*, sist endret 8. august 2019, <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/spesielt-om-sarlige-kategorier-av-personopplysninger-sensitive-personopplysninger-og-unntak/> (sist besøkt 4. november 2020).

European Data Protection Board, *GDPR: Guidelines, Recommendations, Best Practices*, u.å., https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (sist besøkt 22. november 2020).

European Data Protection Board, *Members*, u.å., https://edpb.europa.eu/about-edpb/board/members_en (sist besøkt 22. november 2020).

Folkehelseinstituttet, *Smittestopp – ny app fra Folkehelseinstituttet*, 16. april 2020 <https://www.fhi.no/nyheter/2020/ny-app-fra-folkehelseinstituttet/> (sist besøkt 25. november 2020).

7.9.3 Rapporter

Datatilsynet, *Big Data – personvernprinsipper under press* (2013) [Tilgjengelig på https://www.datatilsynet.no/globalassets/global/dokumenter-pdf-skjema-ol/rettigheter-og-plikter/rapporter/big-data_web.pdf] (sist besøkt 23. november 2020).

7.9.4 Offentlige dokumenter

EU-kommisjonen, Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 [Tilgjengelig på <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en>] (sist besøkt 1. desember 2020).

Europaparlamentet, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Tilgjengelig på <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014AP0212>] (sist besøkt 2. desember 2020).

EØS-komiteen, Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 [Tilgjengelig på <https://www.efta.int/sites/default/files/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018 - English/154-2018.pdf>] (sist besøkt 2. desember 2020).