UiO : Det juridiske fakultet

Den behandlingsansvarliges dokumentasjon etter personvernforordningen art. 24.

Kandidatnummer: 594.

Leveringsfrist: 25.11.2021.

Antall ord: 15199

Innholdsfortegnelse

1 Innledning

1.1 Tema og bakgrunn

Temaet for oppgaven er påvisning av etterlevelse av personvernforordningen, nærmere bestemt de kravene som kan stilles til behandlingsansvarliges dokumentasjon etter personvernforordningens art 24.

I lys av at retten til personvern ble inntatt i TFEU art. 16 i 2009, ble det reist spørsmål om det daværende personverndirektivet 1995 (DPD) fortsatt holdt tritt med dagens samfunn. De foregående årene var preget av raske teknologiske fremskritt, og behandling av personopplysninger skjedde nå i en helt annen skala enn tidligere.[1] Konklusjonen var at selv om de grunnleggende prinsippene som lå bak direktivet fortsatt var gjeldende, var det behov for en mer enhetlig og harmonisert personvernlovgivning, som kunne holde tritt med den teknologiske utviklingen og effektivt beskytte enkeltpersoners friheter og rettigheter.[2]

Et fokusområde ved utviklingen av den nye forordningen var aktørenes ansvar, eller «accountability». Article 29 Working Party hadde i 2009 pekt på at virksomheter ikke i tilstrekkelig grad internaliserte sine plikter etter det daværende direktivet.[3] DPD inneholdt et krav om rapportering til tilsynsmyndigheten i forkant av behandlingen etter art. 18 og 19, men denne plikten kunne gi behandlingsansvarlige inntrykk av at de var fritatt noe av ansvaret etter denne rapporteringen ble gjennomført. Det ble derfor foreslått et forsterket fokus på ansvarsmekanismer i en eventuell ny lovgivning.

Med den nye personvernforordningen (GDPR) ble behandlingsansvarlige, både i og utenfor Europa, pålagt nokså omfattende plikter når det gjaldt deres behandling av personopplysninger. Sentralt i forordningen ligger det nå et krav om proaktivitet fra den behandlingsansvarlige, i at denne skal drive såkalt «internkontroll» med egne personopplysningsbehandlinger. Målet med å få behandlingsansvarlige til å drive egenkontroll med behandlingen, var å sikre en slik internalisering av deres plikter som til noen grad var fraværende etter DPD. Gjennom å bevisstgjøre behandlingsansvarlige på disse pliktene, er håpet at enkeltpersoners rettigheter og friheter ivaretas i større grad og på et tidligere tidspunkt i behandlingen enn tidligere.

Det er innenfor de nye internkontrollreglene at vi finner art. 24 om den behandlingsansvarliges ansvar. Bestemmelsen legger opp til at den behandlingsansvarlige plikter å gjennomføre tiltak som skal sørge for at behandlingen skjer i overensstemmelse med forordningen, men også for å påvise slik etterlevelse.

---

[1] COM(2012) 11 s. 1.

[2] COM(2012) 11 s. 2.

[3] WP29 (2009) s. 19.

Håndhevingsmekanismene som skal sørge for etterlevelse av disse reglene ble samtidig oppdaterte og styrket for å sørge for at pliktene til de behandlingsansvarlige ble fulgt. Blant annet ble tilsynsmyndighetenes oppgaver og myndighet klargjort og utvidet, og det ble vedtatt et svært høyt sanksjonsnivå for overtredelser av GDPR. Omfanget av det nye håndhevingsregimet kan illustreres ved at flesteparten av de nasjonale tilsynsmyndighetene rapporterte at overgangen fra DPD til GDPR innebar et behov for en 30-50% økning i deres årlige budsjetter.[4]

Disse nye pliktene, samt risikoen for høye gebyr, innebærer at det er et stort behov for behandlingsansvarlige å påvise sin etterlevelse av forordningen. En svært praktisk måte å gjøre dette på er gjennom å inneha dokumentasjon om forhold ved behandlingen av personopplysningen. Det er likevel knyttet noen usikkerheter til hvordan aktører kan og skal innrette denne dokumentasjonen.

1.2 Problemstilling og avgrensinger

Hovedproblemstillingen for oppgaven er: «Hvilke krav stiller artikkel 24 til den behandlingsansvarliges dokumentasjon av etterlevelse av personvernforordningen». Forordningens art. 24 stiller et krav til at behandlingsansvarlige skal kunne påvise at personopplysningsbehandlingen skjer i samsvar med forordningens øvrige bestemmelser. Dette kravet er imidlertid ikke presisert noe nærmere i verken ordlyden eller rettspraksis. Jeg ønsker derfor å drøfte dokumentasjonens rolle som påvisningsverktøy etter art. 24, for å finne ut hvordan dokumentasjonen skal innrettes. Jeg utelukker med dette ikke at påvisning kan skje på andre måter enn ved hjelp av dokumentasjon. Dokumentasjon er imidlertid den mest praktiske formen for påvisning av etterlevelse etter min mening, slik at oppgavens hovedfokus vil ligge på dette.

For å kunne besvare den vide problemstillingen jeg oppstiller, er det nødvendig å drøfte flere ulike sider ved dokumentasjonen. Bestemmelsen er taus om en rekke forhold som vil være av stor betydning for hvordan behandlingsansvarlige skal innrette seg etter art 24. Jeg vil derfor særlig fokusere på tre aspekter ved den behandlingsansvarliges dokumentasjon: dokumentasjonens type, dokumentasjonens omfang og dokumentasjonens form. Uten en klar formening om disse sidene ved dokumentasjonen vil det være vanskelig å bruke dokumentasjon som et effektivt påvisningsverktøy etter art. 24.

I vurderingene av ovennevnte aspektene vil jeg også drøfte hvordan andre regler spiller inn. Særlig interessant i denne sammenhengen er hvordan reglene om overtredelsesgebyr kan brukes ved vurderingen av disse aspektene ved dokumentasjonen. Jeg stiller derfor opp et eget spørsmål om reglene om overtredelsesgebyr kan benyttes for å ta stilling til innholdet i

[4] EDPB (2019a) s. 7.

dokumentasjonsplikten etter art. 24. Spørsmålet er lite drøftet i rettspraksis og teori, og vil derfor i stor grad bero på system- og formålsbetraktninger.

1.3 Rettskildebildet og metode

Oppgaven bygger i det vesentlige på en analyse og drøftelse av personvernforordningens regler.

Norge er, som medlem i EØS, forpliktet til å lojalt gjennomføre EØS-relevante rettsakter som vedtas i EU jf. EØS-avtalen art. 3. Ettersom Norge ikke har overgitt formell lovgivningskompetanse ved sitt medlemskap i EØS, må slike rettsakter gjennom to ledd før de får virkning internrettslig.

Det første leddet er at rettsakten må tas inn i EØS-avtalen ved beslutning av EØS-komiteen jf. EØS-avtalen art. 102 nr. 1. Denne innlemmingen beror på enighet mellom EU på den ene siden, og enstemmighet fra EFTA-statene jf. art. 93 nr. 2 på den andre siden. Denne prosessen sørger for at rettsakten er folkerettslig bindende for Norge, men den utløser ikke direkte rettsvirkninger i norsk rett. Dette følger av at det norske rettssystemet er basert på dualisme, altså at internasjonal og nasjonal rett anses som to separate rettssystemer, hvor traktatforpliktelser må innlemmes i norsk rett for å kunne anvendes direkte.[5]

Det andre leddet er derfor nasjonal gjennomføring av disse forpliktelsene. Dette skjer typisk gjennom transformasjon, inkorporasjon eller konstatering av rettsharmoni.[6] Artikkel 7 foreskriver hvordan ulike typer rettsakter skal gjennomføres. I motsetning til personverndirektivet 1995, som la opp til at statene selv skulle omskrive og tilpasse reglene til nasjonale forhold, måtte personvernforordningen gjennomføres «som sådan» jf. art. 7 bokstav a. Dette innebar at inkorporasjon var eneste aktuelle gjennomføringsalternativ for forordningen jf. Prop. 56 LS (2017-2018) s. 15.

Forordningen er derfor inkorporert i norsk rett gjennom personopplysningsloven § 1, og oversatt til norsk. Forordningen har, ved motstrid, forrang foran nasjonale regler som regulerer samme forhold jf. EØS-loven § 2. Den norske versjonen av personvernforordningen er autoritativ ved at den er inntatt i EØS-tillegget til Den europeiske unions tidende jf. EØS-avtalen art. 129 nr. 1, og er derfor slik likestilt med de mange andre offisielle språkversjonene.

Det at personvernforordningen har så mange autoritative språkversjoner byr på enkelte metodiske utfordringer og særegenheter. For det første er det ingen garanti for at ordene som brukes har likt meningsinnhold på tvers av disse versjonene. For det andre er det slik at det er EU som

[5] Ruud (2014) s. 52.

[6] Ruud (2014) s. 59.

har ansvaret for EU-landenes språkversjoner, mens de norske og islandske språkversjonene er utarbeidet av statene selv.[7] Det er derfor en risiko for at forståelsen av begrepene som brukes ikke er fullt ut harmonisert på tvers av EU og Norge og Island.

Likevel skal tolkningen skje i henhold til det sentrale rettskildeprinsippet i EØS-retten, nemlig homogenitetsmålsetningen jf. EØS-avtalen art. 1(1) og fortalen til EØS-avtalen (fjerde ledd). I denne ligger det en forutsetning om at EØS-regler skal tolkes likt på tvers av EU- og EFTA-statene, og at de skal håndheves og praktiseres likt.[8] Dette utgjør generelt en metodisk utfordring ved tolkningen av primær- og sekundærlovgivningen i EØS.

Dersom det foreligger motstrid mellom to eller flere språkversjoner, vil domstolene strekke seg langt for å komme til et tolkningsresultat som er harmonisert. Dette kan typisk gjøres ved å legge mindre vekt på den konkrete ordlyden i de ulike versjonene, og heller benytte formålet og systembetraktninger for å finne en harmonisert tolkning av de konkrete bestemmelsene, jf. C-419/10 avsn. 68.

De mange språkversjonene påvirker også tolkningen ved at de ulike språkversjonene må ses i sammenheng. Siden omfanget er så stort som det er, kan det være vanskelig å få med alle nyansene i de ulike versjonene. Dette kan også begrunne at det legges noe mindre vekt på den eksakte ordlyden enn det som er normalt etter alminnelig norsk rettskildelære.[9]

Ettersom norsk er det språket jeg er mest komfortabel med, har jeg i oppgaven tatt utgangspunkt i den norske språkversjonen av personvernforordningen som autoritativ rettskilde. Dette har jeg gjort fordi det er lettest for meg å finne nyanser i den norske ordlyden til GDPR. Andre språkversjoner, primært svensk, dansk og engelsk, har jeg benyttet der tolkningen levner usikkerhet, eller der språkversjonene er egnet til å vise andre aspekter ved ordlyden enn det som kommer fram i den norske versjonen. Slik har jeg forsøkt å unngå noen av de ovennevnte problemene. Det er likevel en mulighet for at jeg har mistet nyanser som kommer frem i andre språkversjoner enn de nevnte. Ved å legge mindre vekt på den konkrete ordlyden, og ved å benytte andre rettskilder i tolkningen, vil risikoen imidlertid reduseres noe.

En normalt tungtveiende rettskilde vil være rettspraksis fra EU- og EFTA-domstolen. Mange av reglene i personvernforordningen viderefører tidligere regler fra DPD, slik at rettspraksis om disse reglene fortsatt er relevante ved tolkningen av bestemmelsene. For denne oppgaven, som har sin hovedvekt på et nytt aspekt ved forordningen, har jeg undersøkt databasene til EUR-lex

[7] Arnesen (2015) s. 345.
[8] Sejersted (2014) s. 87.
[9] Sejersted (2014) s. 45.

og eftacourt.int for å finne relevante dommer. Jeg har i disse søkene ikke lykkes å finne dommer som berører spørsmålet om påvisningsaspektet i forordningens art. 24. Tosoni mfl. har også lagt ut en oversikt over saker som er oppe for CJEU, EFTA og nasjonale domstoler som berører personvernrettslige problemstillinger.[10] Heller ikke i denne oversikten har jeg funnet noen direkte relevante saker for spørsmålet om den behandlingsansvarliges dokumentasjon.

Mye av tolkningen er derfor nødvendigvis basert på andre kilder, særlig formålsbetraktninger, systembetraktninger og litteratur. Når det gjelder litteratur vil særlig retningslinjer, veiledninger og andre uttalelser fra European Data Protection Board (EDPB, Personvernrådet) kunne bidra. Gruppen har som oppgave å sikre ensartet anvendelse av forordningen jf. GDPR art. 70(1), og deres uttalelser vil kunne tillegges tung vekt ved tolkning av forordningen.[11] Personvernrådet har også gitt tilslutning til enkelte uttalelser fra dens forgjenger, Article 29 Working Party (WP29) i EDPB Endorsement 1/2018, som innebærer at noen av de eldre uttalelsene fortsatt er av betydning.

En siste rettskilde som er verdt å vie oppmerksomhet, er fortaler. Etter TEUF art. 296(2) skal rettsakter «state the reasons on which they are based». Dette skjer for traktater, forordninger og direktiver typisk ved at teksten innledes med en fortale, også kalt preambel. Denne forklarer hjemmelen rettsakten bygger på, og formålene bak de etterfølgende bestemmelsene, og fyller en lignende (men ikke lik) funksjon som forarbeider gjør i norsk rett.[12] Det kan ikke utledes konkrete rettigheter eller plikter fra fortalene, men de kan spille en stor rolle når det gjelder den nærmere tolkningen av rettsreglene.[13]

1.4 Den videre fremstillingen

I det følgende har jeg delt oppgaven inn i tre deler.

I kapittel 2 presenterer jeg de grunnleggende reglene av betydning for den behandlingsansvarliges ansvar. Redegjørelsen vil her først gjelde noen av de overordnede prinsippene som ligger til grunn for forordningen, før jeg går over til en tolkning av innholdet i plikten etter art. 24. Fokuset vil ligge på rammene for den behandlingsansvarliges påvisning av at behandlingen skjer i overenstemmelse med forordningen. Funnene som gjøres her vil danne grunnlaget for drøftelsen i kapittel 3.

[10] Tosoni (2021) s. 289 flg.
[11] Skullerud (2019) s. 44.
[12] Sejersted (2014) s. 53.
[13] Sejersted (2014) s. 57.

I kapittel 3 vil jeg drøfte en rekke spørsmål for å avdekke det nærmere innholdet av den behandlingsansvarliges påvisning etter art. 24. Her vil jeg først vurdere hvordan reglene om overtredelsesgebyr kan spille inn på forståelsen av innholdet i dokumentasjonsplikten. Deretter vil jeg se på de kravene som kan stilles til dokumentasjonens type, omfang og form. Dette ser jeg særlig i lys av reglene om overtredelsesgebyr jf. kapittel 3.1 og egenskaper ved dokumentasjonen jf. redegjørelsen i kapittel 2.3.3.

I kapittel 4 vil jeg kort oppsummere de funnene jeg har gjort i kapittel 3, og nevne noen av de utfordringene som temaet avdekker angående kildematerialet.

2 Den behandlingsansvarliges ansvar

2.1 Grunnleggende prinsipper med betydning for dokumentasjonsplikten

Personvernforordningen art. 5 inneholder de fleste sentrale prinsippene som ligger til grunn for de øvrige bestemmelsene i GDPR. Prinsippene bidrar både til å forklare og til å begrunne de reglene som er inntatt i forordningen. Ettersom domstolene ved tolkning av EØS-rett generelt tillegger prinsipper stor vekt, vil disse kunne være viktige rettskildefaktorer ved tolkningen av konkrete regler i GDPR.[14]

Prinsippene har et noe vagt formulert innhold, og det er levnet rom for nokså skjønnsmessige avveininger. Dette gjør det vanskelig å tillegge prinsippene i art. 5 et presist innhold uten autoritative uttalelser fra domstolen. Det er likevel ikke sånn at prinsippene bare har verdi ved tolkningen av andre regler. Dersom prinsippene ikke overholdes, vil man risikere å bli møtt med overtredelsesgebyr jf. art. 83(5)(a).

Prinsippene jeg har valgt å presentere er prinsippet om lovlighet, rettferdighet og åpenhet etter art. 5(1)(a), og ansvarsprinsippet slik det kommer til uttrykk i art. 5(2). Bakgrunnen for valget av prinsipper er at disse virker inn på pliktene etter art. 24 på ulike måter. Ved at behandlingsansvarlige tvinges til å påvise sin etterlevelse, vil både den registrerte og tilsynsmyndighetene lettere kunne se om forordningen overholdes og avdekke eventuelle brudd. Åpenhet rundt behandlingen kan slik sies å forutsette, og begrunne, regler om påvisning og dokumentasjon. Prinsippet vil derfor være av betydning for drøftelsen av dokumentasjonskrav.

Denne gjennomsiktigheten rundt behandlingen vil videre ha en side mot behandlingens lovlighet og rettferdighet, ved at den tvinger eventuelle ulovligheter og urettferdige behandlinger frem i lyset. Behandlingsansvarlige kan dermed bli oppmuntret til å sikre at disse prinsippene blir overholdt, i frykt for at eventuelle overtredelser blir oppdaget.

[14] Sejersted (2014) s. 45.

Ansvarsprinsippet gjelder spesifikt prinsippene i art. 5(1), men er også særlig relevant i relasjon til kravet om påvising av etterlevelse av GDPR etter art. 24(1). Bestemmelsen i art. 24(1) er på mange måter en videreføring av de grunnleggende betraktningene som er lagt til grunn i ansvarsprinsippet, og er myntet på å oppfylle dette. Forholdet mellom de to er derfor også viet et eget punkt i kapittel 2.2.1.

2.1.1 Lovlighet, rettferdighet og åpenhet

Prinsippet om lovlighet, rettferdighet og åpenhet er som nevnt fastsatt i personvernforordningen art. 5(1)(a). Lovgiver har her samlet disse tre elementene til ett prinsipp. Innholdet til forutsetningen om lovlighet er imidlertid noe forskjellig fra innholdet til kravet om åpenhet, som igjen er noe forskjellig fra kravet om rettferdighet. I det følgende vil jeg derfor behandle dem hver for seg for å få frem særegenhetene ved deres innhold. Det er ikke dermed sagt at disse delene av prinsippet er totalt uavhengige av hverandre. De vil til en viss grad kunne bidra til forståelsen av hverandre, noe som er bakgrunnen for at de er samlet i et prinsipp i lovteksten.

Det første elementet av prinsippet i art. 5(1)(a) er kravet om lovlighet eller lovlig behandling. Denne delen av prinsippet i art. 5(1)(a) er særdeles viktig, noe som er gjenspeilet av at lovlighetskravet var inntatt i både DPD art. 6(1)(a) og OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) nr. 7. Lovlighetskravet kan på mange måter hevdes å være en grunnsten for all personvernslovgivning, i den forstand at det omfatter alle de andre prinsippene som legger grunnlaget for regler om personopplysningsbehandling.[15]

Denne delen av prinsippet krever at all behandling av personopplysninger skal skje på lovlig måte. Dette må ses i sammenheng med at behandling av personopplysninger som utgangspunkt er i strid med enkeltpersoners rett til personvern etter art. 16(1) TFEU og art. 8(1) ECFR, med mindre det foreligger et særlig rettslig grunnlag for behandlingen. Lovlighetskravet kan derfor sies å henvise til forordningens egne krav om rettslig grunnlag for personsopplysningsbehandling, for eksempel i art. 6. Dette gir imidlertid kravet om lovlig behandling et noe snevert virkeområde. Mer naturlig er det å se denne delen av prinsippet som et krav om lovlighet i relasjon til alle relevante rettslige krav.[16] Det forutsettes da at behandlingen skjer i tråd med andre rettsregler, som EU-retten og menneskeretter som ytringsfrihet og vern om barnets personlige integritet.

Kravet om rettferdig behandling av personopplysninger er et av de mer skjønnsmessig utformede delene av art. 5. Det gis lite veiledning hva gjelder dette kravets konkrete innhold, men det er essensielt snakk om et krav til at det ikke er benyttet urettferdige eller uærlige metoder

[15] Bygrave (2014) s. 146.

[16] de Terwangne (2020) s. 314.

for å skaffe personopplysningene. Rettferdighetskravet legger også opp til en forholdsmessighetsvurdering mellom de formålene som opplysningene skal brukes til, og de konkrete interessene til den registrerte. Denne delen av prinsippet i art. 5(1)(a) kan ses på som den andre siden til kravet om lovlig behandling av personopplysninger. Der lovlighet sikter til konkrete rettsregler, vil prinsippet om rettferdighet sikte til interesseavveininger. [17]

Kravet om åpenhet rundt behandlingen av personopplysninger var tidligere sett på som en integrert del av prinsippet om rettferdighet slik dette kom til uttrykk i DPD art. 6(1)(a). Dette ble uttrykkelig nevnt i fortalen til personverndirektivet, hvor det i punkt 38 ble sagt at «rettferdig behandling av opplysninger forutsetter at den registrerte kan få kjennskap til at en slik behandling eksisterer» og «nøyaktige og fullstendige opplysninger om de nærmere omstendighetene ved innsamlingen». Disse to delene av art. 5(1)(a) er tett knyttet opp mot hverandre, da rettferdig behandling ikke kan skje uten åpenhet rundt behandlingen. Dette kan begrunnes i at en registrert som ikke er kjent med innholdet i behandlingen av hans eller hennes personopplysninger, ikke kan vite om denne skjer i strid med deres interesser og på en rettferdig måte.

Åpenhetskravet er i dag nærmere forklart i fortalens punkt 39, hvor det legges særlig vekt på at den registrerte har krav på at en rekke opplysninger om behandlingen er gitt på «lett tilgjengelig og lettfattelig» måte, og at språket som brukes i denne kommunikasjonen er «klart og enkelt». Disse elementene av prinsippet ivaretas gjennom at det stilles en rekke krav både til behandlingsansvarlige og til informasjonen som gis den registrerte i art. 12-15.

Denne delen av prinsippet etter art. 5(1)(a) er særdeles viktig for at den registrerte skal kunne utøve sine rettigheter til blant annet sletting etter art. 17 og retting etter art. 16. Disse rettighetene kan vanskelig ivaretas og håndheves dersom den registrerte mangler kjennskap til, eller har fått utilstrekkelig eller uklar informasjon om, behandlingen. Slike krav fra den registrerte forutsetter at den behandlingsansvarlige selv innehar informasjon om behandlingen.

2.1.2 Ansvarsprinsippet

Prinsippet om ansvar er hjemlet i personvernforordningen art. 5(2). Artikkelen bestemmer at det er den «behandlingsansvarlige» som er «ansvarlig for og skal kunne påvise at nr. 1 overholdes».

At den behandlingsansvarlige er det primære ansvarssubjektet i GDPR er gjenspeilet i mange av de autoritative språkversjonene til GDPR. På norsk kalles denne personen «behandlingsansvarlig», i den tyske språkversjonen kalles denne personen «verantwortlicher», som kan

[17] Schartum (2020) s. 89.

oversettes til «den som er ansvarlig» og på fransk er personen «responsable du traitement», eller «ansvarlig for behandlingen».

«Behandlingsansvarlig» er den fysiske eller juridiske personen som, alene eller sammen med andre, bestemmer formålet med og midlene for behandlingen av personopplysninger jf. art. 4(7). Bestemmelsen nevner også eksplisitt at offentlige myndigheter, institusjoner og andre organer kan regnes som behandlingsansvarlige.

At den behandlingsansvarlige skal bestemme «formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes» innebærer essensielt at den ansvarlige bestemmer hvorfor og hvordan behandlingen skal skje. Det er denne personen som regnes som behandlingsansvarlig etter definisjonen i art. 4(7). Ordlyden skiller ikke mellom «formålet» og «midler», slik at det gis inntrykk av at dette er kumulative vilkår for å regnes som behandlingsansvarlig.

Det viktigste er imidlertid at den behandlingsansvarlige er den som bestemmer hvorfor behandlingen skal skje, altså formålet med behandlingen. Dette er av praktiske årsaker. Den behandlingsansvarlige kan nemlig inngå databehandleravtaler etter art. 28(3), hvor den ansvarlige kan delegere deler av oppgaven med å bestemme hvilke konkrete midler som skal benyttes til databehandleren. Det er sikker rett at dette kan gjøres uten at dette medfører at personen mister status som behandlingsansvarlig.[18] Dette er begrunnet i at den behandlingsansvarlige ikke alltid har den tekniske kompetansen som kreves til å angi midlene som skal brukes på en tilstrekkelig presis måte. Det er likevel ikke slik at hele denne oppgaven kan delegeres. Delegasjonen av valg av midler kan bare gjøres for de midlene som regnes som ikke-essensielle, i den forstand at de ikke har en sterk tilknytning til formålet med behandlingen.[19] Dersom databehandler får delegert en slik oppgave, vil denne fort kunne regnes som behandlingsansvarlig jf. art. 28(10).

Ved fastleggelsen av hvem som er behandlingsansvarlig, skal begrepet tolkes i lys av det bakenforliggende formålet om å sikre en effektiv og fullstendig beskyttelse av den registrertes rettigheter. Dette betyr at begrepet skal tolkes vidt, slik at man sikrer et høyt beskyttelsesnivå hva gjelder fysiske personers rettigheter (C-131/12 *Google Spain* (premiss 34), C-210/16 *Wirtschaftsakademie* (premiss 26-28) og C-40/17 *Fashion ID* (premiss 65-66)).

Videre skal vurderingen baseres på de reelle, heller enn de formelle, forholdene ved behandlingen. Denne funksjonelle forståelsen følger ikke direkte av ordlyden. Det er imidlertid sikker rett at denne forståelsen av begrepet skal legges til grunn, se WP29 Opinion 01/2010, hvis

[18] EDPB (2020a) s. 13.

[19] EDPB (2020a) s. 14.

forståelse også ble lagt til grunn i de oppdaterte EDPB Guidelines 07/2020, og i Generaladvokat P. Mengozzis forslag til avgjørelse i C-25/17 *Jehovan Todistajat* (para. 68). Løsningen er også implisert i art. 28(10), som fastsetter at en databehandler som selv bestemmer formål og midler med behandlingen, vil regnes som behandlingsansvarlig etter art. 4(7).

Ettersom et av de grunnleggende formålene med personvernforordningen er å sørge for en effektiv og fullstendig beskyttelse av fysiske personers rettigheter, er det av sentral betydning at noen står ansvarlig for behandlingen. Den vide og funksjonelle forståelsen av begrepet skal derfor sørge for at det alltid vil være noen som blir ansett som behandlingsansvarlig, for å unngå et lovtomt rom der behandling av personopplysninger skjer uten at noen står ansvarlig for denne. Definisjonen skal således sørge for at ansvaret plasseres hos den som har avgjørende innflytelse på personopplysningsbehandlingen.[20]

Prinsippet om den behandlingsansvarliges ansvar i art. 5(2) har to sider ved seg. Den første er at den pålegger den behandlingsansvarlige å sikre at prinsippene som ligger til grunn for GDPR er overholdt. Denne ivaretakelsesplikten er etter ordlyden begrenset til de prinsippene som er nevnt i art. 5(1). For noen av disse prinsippene innebærer dette relativt klare forpliktelser for den behandlingsansvarlige. Som eksempel er prinsippet om lagringsbegrensing nokså presist formulert, noe som gjør dette prinsippet enklere å overholde enn et prinsipp som for eksempel «rettferdighet», som ikke er nærmere forklart i verken art. 5(1)(a) eller andre bestemmelser jf. redegjørelsen ovenfor. Denne uklarheten i innholdet i noen av prinsippene levner rom for nokså vide og skjønnsmessige tolkninger, og bidrar til å gjøre ivaretakelsesplikten i art. 5(2) noe uklar.

Dette overholdelseaspektet ved ansvarsprinsippet er en videreføring av prinsippet slik det kom til uttrykk i DPD art. 6(2). Det som er nytt med GDPR, er at den behandlingsansvarlige nå også er eksplisitt pålagt å kunne «påvise» denne etterlevelsen. Ordlyden er taus om hvordan denne påvisningen skal skje, men plikten må ses i sammenheng med andre ansvarsbestemmelser i GDPR, særlig art. 24 om den behandlingsansvarliges ansvar.[21] Denne sammenhengen og innholdet i art. 24 er temaet for det neste kapittelet.

2.2 Den behandlingsansvarliges ansvar etter art. 24

2.2.1 Forholdet til art. 5(2)

Art. 24 om den behandlingsansvarliges ansvar er tett knyttet opp mot ansvarsprinsippet slik det kommer til uttrykk i art. 5(2). De to artiklene har lagt på vei et lignende innhold. Begge bestemmelsene krever at behandlingsansvarlig skal både sikre og påvise egen etterlevelse, og begge plasserer ansvaret for dette på den behandlingsansvarlige.

[20] EDPB (2020a) s. 9

[21] de Terwangne (2020) s. 319

Det er imidlertid noen forskjeller mellom de to bestemmelsene. Ansvarsprinsippet i art. 5(2) har avgrenset sitt virkeområde til prinsippene som ligger til grunn for personvernforordningen jf. art. 5(1). Artikkel 24 omfatter på den andre siden «tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning» jf. art. 24(1) første punktum. Etter ordlyden vil dette gjelde enhver bestemmelse i forordningen av betydning for behandlingen den ansvarlige foretar, herunder de ovennevnte prinsippene i art. 5(1). Det er derfor mulig å se art. 24 som en videreføring eller presisering av ansvarsprinsippet i art. 5(2).[22]

Det kan argumenteres for at en sikring og påvisning av at reglene for behandlingen i GDPR er fulgt jf. art. 24(1), i praksis betyr at de bakenforliggende prinsippene i art. 5(1) er ivaretatt. Det kan nemlig være vanskelig å tenke seg en situasjon hvor den behandlingsansvarlige har gjennomført egnede tiltak for å sikre og påvise at behandlingen er utført i samsvar med GDPR jf. art. 24, men likevel handler i strid med prinsippene i art. 5(1).

Det vil derfor være naturlig å se disse bestemmelsene i sammenheng med hverandre. Pliktene i art. 24 er særlig relevant ved tolkningen av innholdet i art. 5(2), og art. 24 må ses i lys av art. 5(2) og det ansvaret som der legges på etterlevelsen av personvernsprinsippene spesifikt.[23]

2.2.2 Risikovurdering

Innebygd i art. 24(1) ligger det et krav til at det foretas en vurdering av virksomhetens risikonivå som skal begrunne de tiltakene som iverksettes. Resultatet av en slik vurdering vil ha betydning både for tiltakene som skal sikre etterlevelsen av forordningen, og for hvor mye som kreves av den behandlingsansvarliges påvisning av at behandlingen skjer i overenstemmelse med forordningen. Der det foreligger liten risiko knyttet til virksomheten, vil det ikke stilles like strenge krav til dokumentasjonen av behandlingen som det vil dersom behandlingen er svært risikofylt.

Det kan være et betydelig sprik mellom omfanget til ulike virksomheter som behandler personopplysninger og den risikoen som er knyttet til behandlingen deres. Kravene til tiltakene som skal gjennomføres er derfor skalerte, ved at det er skal tas hensyn til «behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter» jf. art. 24(1) når behandlingsansvarlig skal ta stilling til hvilke tiltak som skal iverksettes for å sikre og påvise etterlevelse.

Som nevnt i personvernforordningens fortale punkt 4, er ikke retten til vern om personopplysninger absolutt. Den må veies opp mot eventuelle inngrep i andre rettigheter, for eksempel

[22] Jarbekk (2021) art. 24 note 2.

[23] Schartum (2020) s. 247.

retten til å drive næringsvirksomhet. For enkelte mindre bedrifter som driver med enkel, lavrisiko personopplysningsbehandling kan det være lite hensiktsmessig å kreve dyre og omfattende ansvarstiltak.[24] I realiteten vil det å pålegge slike selskaper å gjennomføre de samme tiltakene som multinasjonale teknologigiganter, uten å ta hensyn til særtrekkene ved virksomheten, kunne være uforholdsmessig tyngende. Det er heller ingen garanti for at omfattende tiltak vil øke beskyttelsesgraden nevneverdig, når det uansett er knyttet lite risiko til personopplysningsbehandlingen.

Ordet «risiko» er ikke definert i art. 24(1), men begrepet kan defineres på flere ulike måter. I flere norske forarbeider er begrepet blitt definert som produktet av sannsynligheten for at en hendelse inntreffer og konsekvensen av at dette skjer, se for eksempel NOU 2018:17 s.147 og NOU 2016:19 s.41. En slik definisjonen er antatt av blant andre Schartum at kan legges til grunn også i tolkningen av risikobegrepet etter personvernforordningen.[25] Aven og Renn har argumentert for en definisjon hvor tallfestingen ikke er like fremtredende. De definerer risiko som «uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value».[26]

Det avgjørende når man vurderer risiko, vil være at det foretas en vurdering av særtrekkene ved behandlingen og virksomheten, for å fastslå hvor alvorlig risikoen for den registrertes rettigheter og friheter er, og hvor sannsynlig det er at truslene mot disse frihetene og rettighetene realiseres jf. fortalens punkt 76. Hvor alvorlig risikoen er vil baseres på en analyse av sannsynligheten for at behandlingen fører til «fysisk, materiell eller ikke-materiell skade» jf. fortalens punkt. 75. Resultatet av risikovurderingen vil så informere valget av de «egnede» tiltakene etter art. 24(1).

Art. 24(1) gir liten veiledning når det gjelder den konkrete risikovurderingen, men legger opp til en skjønnsmessig vurdering av noen oppstilte momenter. Denne skaleringen skal baseres på «behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter». Denne formuleringen går igjen i en rekke andre bestemmelser som omhandler iverksetting av tiltak. En lignende skalering følger også av blant annet av art. 25(1) om innebygd personvern og art. 32(1) om sikkerhetstiltak. Forståelsen av hva som ligger i denne formuleringen etter disse bestemmelsene kan dermed tjene også i forståelsen av den samme formuleringen etter art. 24(1).

[24] WP29 (2014) s. 3.

[25] Schartum (2020) s. 238.

[26] Aven (2009) s. 6.

De nevnte momentene i disse bestemmelsene presiseres også noe i fortalens punkt. 75. Her forklares til en viss grad innholdet i noen av momentene, samtidig som det legges frem enkelte andre eksempler og momenter av betydning for risikovurderingen.

Med «behandlingens art» jf. art. 24(1) siktes det særlig til typen personopplysninger som behandles, spesielt om det gjelder behandling av særlige kategorier personopplysninger etter art. 9(1) jf. definisjonene i art. 4(13) - 4(15).

Formålet med behandlingen kan spille inn på risikovurderingen i skjerpende retning dersom behandlingen tar sikte på å behandle opplysninger for å treffe juridisk bindende beslutninger for de registrerte. Eksemplene fra fortalens punkt 75 er personopplysninger som skal benyttes i analyser av den registrertes arbeidsprestasjoner eller økonomiske situasjon. Dette er personopplysningsbehandling som berører mange av de grunnleggende prinsippene bak GDPR, særlig prinsippet om riktighet i art. 5(1)(d) jf. også bestemmelsene om retting og sletting av personopplysninger jf. art. 16 og art 17, samt det ulovfestede prinsippet om den registrertes innvirkning på egne personopplysninger.[27]

Virksomhetens «omfang» som moment i risikovurderingen vil særlig være et aktuelt moment for å innføre strengere tiltak. Dette vil spesielt være aktuelt dersom det behandles store mengder personopplysninger som berører mange registrerte, eller det behandles personopplysninger over lang tid. I litteraturen er det også hevdet at dersom det er få registrerte, men personopplysningene om disse få er detaljerte og mangfoldige, vil lignende betraktninger kunne gjøre seg gjeldende.[28]

Også om behandlingen omhandler barn vil her kunne være av betydning. Barn er en særlig sårbar gruppe som har vanskelig for å orientere seg om egne rettigheter, og deres personopplysninger «fortjener et særlig vern» jf. fortalens punkt 38. Det at forordningen anerkjenner denne gruppen som særlig sårbar, kan begrunne at det har betydning ved risikovurderingen om virksomheten i stor grad behandler opplysninger om barn. Schartum har tatt til orde for at de underliggende betraktningene som gjør seg gjeldende for barn, blant annet manglende konsekvenstenkning og manglende forståelse av egne rettigheter, også vil gjøre seg gjeldende der behandlingen for eksempel gjelder demente eller andre med alvorlige kognitive nedsettelser.[29]

Tilsynelatende er det mange av de samme momentene som skal vurderes etter bestemmelsene i art 24, 25 og 32. Det er imidlertid ikke gitt at risikovurderingen som foretas på bakgrunn av

[27] Bygrave (2014) s. 158 flg.
[28] Schartum (2020) s. 242.
[29] Schartum (2020) s. 242.

disse momentene vil slå ut likt på tvers av bestemmelsene, og at man vil få like resultater. Det er snakk om bestemmelser som skal oppfylle forskjellige formål og som skal lede til ulike typer tiltak. Artikkel 25(1) krever en risikovurdering for å vurdere hvilke innebygde tiltak i systemer, løsninger og lignende som skal gjennomføres for å ivareta personvernprinsipper som dataminimering jf. art. 5(1)(c). På den andre siden krever art. 32(1) at en risikovurdering tas for å finne egnende sikkerhetstiltak for å ivareta hensynene til integritet og konfidensialitet ved behandling av personopplysninger jf. prinsippet i art. 5(1)(f). Dette tilsier at risikovurderingen ikke vil være helt lik.

Både art. 25(1) og art. 32(1) peker også på momenter som ikke er nevnt i art. 24(1), for eksempel at «gjennomføringskostnadene» er relevante momenter i vurderingen. Dette tilsier at det ikke er anledning etter art. 24(1) å vektlegge den behandlingsansvarliges kostnader i relasjon til internkontrolltiltakene som skal gjennomføres. Selv om enkelte av momentene er like, viser dette også at det ikke vil være tilstrekkelig for en behandlingsansvarlig å nøye seg med å foreta én risikovurdering for å begrunne tiltakene etter art. 24 og etter art. 25 og art. 32.

Det er behandlingsansvarlig selv som skal foreta en slik analyse av risikoen ved egen virksomhet. Etter ordlyden er det ikke klart når denne skal foretas. Siden tiltakene etter art. 24(1) skal være på plass gjennom hele behandlingen,[30] vil det imidlertid virke mot sin hensikt å foreta den første risikovurdering etter at behandlingen har begynt. Mangelen på risikovurdering vil da utgjøre en trussel for den registrertes rettigheter og friheter, siden den behandlingsansvarlige ikke kan vite om det skal gjennomføres andre tiltak for å redusere denne risikoen.

Det vil være naturlig at virksomheter og teknologi utvikler seg, og at man får inn ny informasjon om effektiviteten ved tiltakene over tid. Det holder derfor ikke å bare foreta én risikovurdering. Tiltakene som iverksettes «skal gjennomgås på nytt og skal oppdateres ved behov» jf. art. 24(1) siste punktum, for å sikre at beskyttelsesnivået ligger konsekvent høyt. For å iverksette nye tiltak kan det være nødvendig å foreta en ny risikovurdering, siden de aktuelle, nye tiltakene skal gjennomføres med bakgrunn i en risikovurdering jf. første punktum. For å ivareta den registrertes rettigheter og friheter på best mulig måte, kan det derfor være nødvendig å foreta en ny risikovurdering etter en hendelse har inntruffet eller i tråd med virksomhetens utvikling.

2.2.3 Tolkning av «egnede tekniske og organisatoriske tiltak»

Etter at risikovurderingen er gjennomført, må behandlingsansvarlig vurdere hvilke tiltak som skal iverksettes etter art. 24 for å redusere risikonivået til et akseptabelt nivå. Det er disse tiltakene som danner kjernen i internkontrollplikten.

[30] Docksey (2020) s. 560.

Tiltak som begrep er ikke forklart nærmere i art. 24(1). En normal språklig forståelse av et «tiltak» er at det er noe man foretar for å oppfylle et bestemt formål. En slik forståelse er veldig vid, og krever ytterligere presisering.

I den engelske versjonen til GDPR art. 24(1) er uttrykket «measures» brukt. Dette kan direkte oversettes til «tiltak». Den danske og svenske språkversjonen har benyttet begreper med et litt annet innhold. På dansk er begrepet «foranstaltninger» brukt, og på svensk er begrepet «åtgärder». Begrepene på dansk og svensk kan også oversettes med tiltak, men her det kanskje mer naturlig å bruke det norske ordet «forholdsregler». Dette viser en side av bestemmelsen som er tydelig av konteksten, men ikke ordlyden direkte, nemlig at tiltakene for å sikre og påvise etterlevelsen av forordningen skal foreligge før behandlingen starter.

Sammenhengen ordet er brukt i, «egnede tekniske og organisatoriske tiltak», snevrer forståelsen noe inn. Det som vil være påbudt er etter ordlyden bare de tiltakene som er av teknisk eller organisatorisk karakter. Dette vil typisk kunne være bruk av systemer for avvikshåndtering eller rollefordelinger internt i virksomheten. Et spørsmål som dukker opp i denne sammenhengen er om det er grunn til å kreve andre typer tiltak av den behandlingsansvarlige enn de som er av teknisk eller organisatorisk natur.

En vid tolkning av art. 24(1) vil bety at også andre typer tiltak, for eksempel juridiske eller pedagogiske tiltak, vil kunne være påbudt.[31] En slik forståelse har ikke direkte hold i ordlyden i art. 24(1). En formålsbasert tolkning av art. 24(1) taler likevel for en slik løsning. Hvis det pålegges andre typer tiltak, vil dette kunne sørge for en sterkere etterlevelse av GDPR siden behandlingsansvarlig er pålagt å se videre enn bare de tiltakene som er av teknisk og organisatorisk natur.

Schartum peker i sin bok på at det vil tale mot art. 24 sin hensikt om en behandlingsansvarlig kan unngå å iverksette et effektivt tiltak som vil sikre etterlevelse av prinsippene i art. 5(1) og reglene i personvernforordningen jf. art. 24(1) fordi det effektive tiltaket ikke strengt tatt er teknisk eller organisatorisk[32]. En slik formålsbasert tolkning av begrepet har god dekning i den metodiske tradisjonen innenfor EU-retten, som i noe større grad baserer sine tolkninger på formålsbetraktninger enn hva som er vanlig etter norsk rettstradisjon.[33]

EDPB har i sine retningslinjer for forståelsen av art. 25 uttalt at «[t]echnical and organizational measures […]can be understood in a broad sense as any method or means that a controller may

[31] Schartum (2020) s. 244.
[32] Schartum (2020) s. 246.
[33] Sejersted (2014) s. 66-67.

employ in the processing».[34] Begrepet i art. 25(1) er likt formulert som begrepet i art. 24(1). Denne forståelsen av begrepet relaterer seg imidlertid til såkalt innebygd personvern, som er noe annet enn tiltak for å sikre og påvise etterlevelse av alle reglene i GDPR. Artikkel 25(1) henviser imidlertid tilbake til de prinsippene som ligger til grunn for GDPR, som søker å beskytte den registrertes rettigheter. Artikkel 24(1) jf. art. 5(2) bygger på de samme formålene, noe som taler for å ilegge tiltaksbegrepet den samme forståelsen.

Begrepet kan derfor etter min mening ikke begrenses til å bare gjelde «tekniske og organisatoriske tiltak».

Tiltakene som gjennomføres av behandlingsansvarlig skal være «egnede». Etter ordlyden skal altså tiltakene som iverksettes være skikket til å oppnå formålet, nærmere bestemt enten å sikre eller å påvise etterlevelsen av personvernforordningen. Hva som er «egnet» må også ses i sammenheng med risikovurderingen som skal ligge til grunn for tiltakene.

I at tiltakene skal «sikre» etterlevelsen av forordningen ligger det at den behandlingsansvarlige skal gjennomføre tiltak som sørger for at behandlingen av personopplysningene skjer i tråd med reglene i GDPR. Dette omfatter en rekke ulike typer tiltak. Sentralt i plikten ligger tiltak som skal redusere risikonivået som er avdekket gjennom utføringen av risikovurderingen. Dette kan være alt fra å oppnevne en sikkerhetsansvarlig til å sørge for fri informasjonsutveksling innad i virksomheten. På den tekniske siden kan dette være tiltak for å sikre dataminimering, for eksempel å implementere hjelpetekster til bruker ved innregistrering av personopplysninger. Slike tekniske tiltak vil imidlertid ofte være mer aktuelt å gjennomføre i henhold til bestemmelsen i art. 25(1), siden de har en side til innebygd personvern og ivaretakelse av personvernprinsippene etter art. 5(1).

Mange tiltak vil naturlig falle inn under både behandlingsansvarliges plikter etter art. 24(1) og etter andre bestemmelser – særlig art. 25(1) (men også art. 32(1)). Dette gjør det uklart om enkelte tiltak, som utpeking av ansvarlig for sikring av registrertes rettigheter, omfattes av art. 24(1) eller art. 25(1). [35] Denne uklarheten angående virkeområdet til de to artiklene skyldes at ordlyden i art. 25(1) ikke eksplisitt knytter tiltakene mot programvaren eller systemene som benyttes i behandlingen. EDPB knytter heller ikke tiltakene til systemløsninger i sin veileder fra 2019, ettersom forordningen ikke benytter systembegreper.[36] Løsningen er her uklar.

[34] EDPB (2019b) punkt 8.

[35] Schartum (2020) s. 253-254.

[36] EDPB (2019b) punkt 7-8.

Utover å gjennomføre tiltak for å sikre etterlevelse av GDPR, skal behandlingsansvarlig også gjennomføre tiltak for å «påvise» denne etterlevelsen. I «påvise» ligger det etter en naturlig språklig forståelse at den behandlingsansvarlige skal kunne bevise eller demonstrere at forordningens bestemmelser er fulgt. Jeg vil komme tilbake til det nærmere innholdet i dette begrepet i kapittelet om dokumentasjon som påvisningsverktøy.

Formålet med kravet er mangedelt. Primært skal påvisningskravet sørge for at tilsynsmyndighetenes tilsynsoppgaver etter art. 57(1) gjøres lettere, men kravet skal samtidig sørge for å beskytte den behandlingsansvarlige mot sanksjoner. En annen side ved kravet er at den registrerte beskyttes gjennom at den behandlingsansvarlige får et bevisst forhold til behandlingen og risikoen tilknyttet denne, og slik kan ta proaktive steg for å minimere risiko.

Personvernforordningen legger opp til flere ulike måter den behandlingsansvarlige kan påvise etterlevelse på. I art. 24(3) legges det opp til at virksomheter kan overholde godkjente atferdsnormer eller sertifiseringsmekanismer for å påvise etterlevelse. Slike normer og mekanismer kan få stor betydning i fremtiden. Alternativene er imidlertid lite aktuelle for norske virksomheter per dags dato, siden det foreløpig finnes svært få slike veiledere.[37] Disse vil likevel kunne få en mye større rolle etter hvert som det utvikler seg flere slike mekanismer og normer.

Overholdelse av, og formell tiltredelse til, slike atferdsnormer og sertifiseringsmekanismer etter art. 24(3) er imidlertid ikke alene tilstrekkelig for å kunne påvise etterlevelse av art. 24(1). Dette følger av ordlyden i nr. 3, som sier at overholdelsen av art. 40 og art. 42 kan brukes som «en faktor for å påvise at den behandlingsansvarliges forpliktelser overholdes». Det er selve resultatet av tiltredelsen av atferdsnormene eller sertifiseringsmekanismene som er av rettslig betydning etter art. 24. I det følgende vil jeg derfor redegjøre for dokumentasjon og den rollen den vil ha i den behandlingsansvarliges påvisning av at behandlingen skjer i henhold til forordningen.

2.3 Dokumentasjon

2.3.1 Hva er dokumentasjon?

Oppgavens hovedproblemstilling dreier seg om behandlingsansvarliges «dokumentasjon». For å kunne undersøke nærmere hvilke krav som stilles til denne, kan det være hensiktsmessig å først redegjøre for hva dokumentasjon er.

Dokumentasjon kan defineres som «bevisføring ved hjelp av dokumenter».[38] Et dokument er i dagligtalen sett på som en skriftlig fremstilling som er av betydning for en sak. I offentleglova

[37] Jarbekk (2021) art. 24 note 4.

[38] NAOB (u.å. a)

§ 4 første ledd er begrepet definert noe videre, som «ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lytting, framsyning, overføring eller liknande». Denne definisjonen er teknologinøytral, og innebærer at også bilder, tegninger, modeller eller lignende vil være omfattet jf. Ot.prp. nr. 102 (2004-2005) s. 120.

I NOU: 2019:9 *Fra kalveskinn til datasjø* ble det i kapittel 4.2.3 foreslått en noe mer presist avgrenset definisjon. Utvalget baserte seg i dette forarbeidet blant annet på internasjonale arkivstandarder for å fastlegge innholdet i dokumentasjonsbegrepet, og de landet på følgende definisjon:

a) dokumentasjon: informasjon som løpende bekrefter hvordan en virksomhet, organisasjon eller person har handlet, utøvd myndighet eller utført tjenester og andre oppgaver. Dette omfatter blant annet prosesser, beslutninger, handlinger med rettslige virkninger, samt vesentlige hendelser og forhold.

Denne definisjonen, som riktignok er en legaldefinisjon i en lov som gjelder noe litt annet enn påvisning av etterlevelse av personvernforordningen, har også en side til personvernlovgivningen, særlig art. 30. Dette er noe som drøftes nærmere i forarbeidets kapittel 10. Definisjonen er etter min mening uansett godt egnet til å illustrere hva dokumentasjon er, også i sammenheng med art. 24(1).

2.3.2 Hjemler art. 24 et selvstendig dokumentasjonskrav?

Ordet «dokumentasjon» er ikke brukt i art. 24. Kravet som stilles er bare at det implementeres tiltak for å påvise etterlevelse av GDPR. Den eneste referansen til dokumentasjon i relasjon til den behandlingsansvarliges ansvar er i art. 33(5), men denne handler om dokumentasjon av en rekke forhold i etterkant av et brudd på personopplysningssikkerhet.

Selve begrepet «påvise» i art. 24(1) forstås etter en normal språklig forståelse som å godtgjøre eller bevise noe.

Dette vil være synonymt med de definisjonene av dokumentasjon som er presentert ovenfor, slik at det kan hevdes at art. 24(1) inneholder et krav om å inneha dokumentasjon. Dette synet støttes av blant andre Schartum, som tolker «påvise» dithen at det inneholder et krav til at det skal foreligge dokumentasjon,[39] og Jarbekk, som mener bestemmelsen må tolkes slik at den oppstiller en svært omfattende dokumentasjonsplikt.[40] Det ble også lagt til grunn i EDPBs

[39] Schartum (2020) s. 247 og 296.

[40] Jarbekk (2021) art. 24 note 2.

anbefaling 01/2020, som i en fotnote henviste til art. 5(2) og 24(1) når det var snakk om dokumentasjon av vurderinger som ble tatt i relasjon til dataoverføringer til en tredjestat.[41]

Det er likevel ikke slik at påvisningsplikten utelukkende kan oppfylles ved å inneha dokumentasjon. Dette gjenspeiles bedre i andre språkversjoner enn den norske (og danske). På engelsk er påvisningsplikten en plikt til å «be able to demonstrate» etterlevelse, og på svensk skal man kunne «visa» slik etterlevelse. Dette fanger i større grad opp et aspekt ved plikten enn den norske versjonen, nemlig at det kan være mulig å vise etterlevelse av forordningen ved å, for eksempel, demonstrere funksjoner i et system. Dokumentasjon er likevel en klart mer praktisk og egnet måte å påvise etterlevelse på i de fleste tilfeller, og det er derfor dokumentasjon som vil være det primære fokuset i det følgende.

Det er også andre bestemmelser i forordningen som inneholder lignende krav som art. 24(1). Spørsmålet er da om det er behov for en selvstendig dokumentasjon etter art. 24(1), eller om andre bestemmelser oppfyller dette behovet.

Det nærmeste et eksplisitt krav til dokumentasjon som finnes i GDPR etter art. 33(5), er art. 30. Bestemmelsen, som i utkastet til GDPR fra 2012 hadde overskriften «documentation»,[42] pålegger behandlingsansvarlig (og representanter og databehandlere) å føre «protokoll over behandlingsaktiviteter som utføres under deres ansvar». Denne bestemmelsen har i norsk oversettelse overskriften «Protokoller over behandlingsaktiviteter». En protokoll kan enkelt forklares som et dokument hvor «noe» skal føres inn.[43] I engelsk versjon er overskriften «Records of processing activities». «Records» er blant annet innenfor arkivfaget sett på synonymt med «dokumentasjon» jf. NOU 2019:9 s. 48. Selv om ordet ikke er benyttet i disse språkversjonene, er det likevel klart at protokollplikten er en plikt til å inneha dokumentasjon.

Etter GDPR art. 30(1) er dette «noe» som skal føres inn i dokumentet grunnleggende informasjon om behandlingen av personopplysninger som utføres jf. bokstav a til g. Formålet med å føre protokoll er å kunne drive kontroll med behandlingens lovlighet i ettertid, samtidig som den skal sikre at behandlingsansvarlige har et bevisst forhold til behandlingen.[44]

Ved første øyekast virker det som at å føre protokoll jf. art. 30(1) kan være et tilstrekkelig tiltak for å påvise etterlevelse etter art. 24(1), slik at det ikke er et selvstendig behov for å tolke inn

[41] EDPB (2020b) s. 10.
[42] COM(2012) 11 s. 61.
[43] NAOB (u.å. b).
[44] Skullerud (2019) s. 304-305.

en videre plikt til dokumentasjon i art. 24(1). Det er imidlertid en del forskjeller mellom de to artiklene.

For det første krever art. 24(1) at det påvises at behandlingen er i overenstemmelse med alle forordningens regler. Artikkel 30(1) inneholder noen grunnleggende mangler for å kunne påvise dette. Mest graverende er det at art. 30(1) ikke krever at behandlingsgrunnlaget registreres, slik at protokoller som følger opplistingen i art. 30(1) ikke vil kunne bevise at behandlingen er lovlig jf. art. 6(1). Det norske Datatilsynet anbefaler av denne grunn at virksomheter bruker deres maler, som inneholder noen flere punkter enn de som er lovpålagt.[45] Denne anbefalingen støttes også av flere, herunder det danske Datatilsynet og britiske ICO. [46, 47]

Den andre forskjellen ligger i virkeområdet til bestemmelsene. Der art. 24 gjelder enhver behandlingsansvarlig, vil art. 30 som utgangspunkt gjelde større virksomheter. Art. 30(5) unntar nemlig enkelte mindre virksomheter fra protokollplikten. En virksomhet vil være unntatt plikten dersom den har færre enn 250 ansatte, gitt at den bare behandler personopplysninger leilighetsvis, behandlingen ikke sannsynligvis medfører risiko for den registrertes rettigheter og det ikke behandles opplysninger jf. art. 9(1) og art. 10. Forskjellen i virkeområdet mellom art. 24 og art. 30 må imidlertid ikke overdrives. Vilkårene om at behandlingen ikke sannsynligvis medfører risiko og at den bare må skje leilighetsvis er imidlertid såpass vide at det må antas at veldig få virksomheter kan benytte seg av unntaket for å unngå protokollplikten. I praksis vil derfor de færreste som driver personopplysningsbehandling kunne unngå å føre protokoll.

Disse forskjellene innebærer at det vil være et selvstendig behov for dokumentasjon utover det som følger av art. 30. Denne plikten er imidlertid betydelig mindre håndfast enn den som følger av art. 30, noe som nødvendiggjør en drøftelse av dennes omfang og karakter.

2.3.3 Egenskaper ved dokumentasjonen

Dokumentasjonen som skal foreligge etter art. 24 vil tjene flere av aktørene i GDPR. Primært er kravet til å inneha dokumentasjon for å påvise etterlevelse et krav som skal sikre at tilsynsmyndighetene kan utføre sine oppgaver etter art. 57(1) på en tilfredsstillende måte. Men også andre aktører vil tjene på at det foreligger dokumentasjon. Den behandlingsansvarlige vil kunne bruke dokumentasjonen for å unngå eller redusere sitt ansvar etter kapittel 8 GDPR. Samtidig vil det at den behandlingsansvarlige dokumenterer en rekke forhold rundt behandlingen sørge for at virksomheten får et bevisst forhold til reglene som gjelder behandlingen, og slik vil kunne innrette sin virksomhet slik at risikoen for den registrertes rettigheter og friheter minimeres. På

[45] Datatilsynet Norge (2018)

[46] Datatilsynet Danmark (2020) s. 6 og 8.

[47] ICO (u.å.).

denne måten tjener også den registrerte på at det foreligger dokumentasjon. Videre vil en utstrakt dokumentasjonsplikt kunne gjøre enkelte plikter etter GDPR lettere å oppfylle, for eksempel innsynsbegjæringer fra enkeltpersoner etter art. 15(1).

For at dokumentasjon skal være et effektiv påvisningsverktøy, og slik kunne ivareta disse hensynene, er det enkelte kvaliteter ved dokumentasjonen som bør være på plass. Standarden ISO 30300, som gjengitt i NOU 2019:9 på s. 52, peker særlig på fire slike kvaliteter eller «grunnleggende egenskaper» ved god dokumentasjon.

Den første er at dokumentasjonen må være pålitelig. Dette innebærer at dokumentasjonen har et innhold som man kan stole på, altså at den er sann, korrekt og oppdatert.[48] Hvis dokumentasjonen til en behandlingsansvarlig ikke er pålitelig, vil den ikke kunne tjene til å påvise et visst faktum.

Den andre er at dokumentasjonen må være autentisk. Autentisitet betyr i bunn og grunn at dokumentasjonen er ekte, altså at den er oppstått under de forholdende som er anført og har den hjemmel og opprinnelse som påberopt.[49] Hvis det blir spørsmål om dokumentasjonens autentisitet, vil dette kunne svekke tilliten både til behandlingsansvarlig og til innholdet til dokumentasjonen.

Den tredje kvaliteten er at dokumentasjonen må ha integritet. Dette betyr at dokumentasjonen er uendret og fullstendig. Integriteten til dokumentasjonen er knyttet til de andre kvalitetene, da endringer etter dokumentasjonen har skjedd er egnet til å svekke tiltroen til både innhold og autentisitet.

Det siste elementet for å sikre god dokumentasjon er at den er anvendbar. I dette ligger det at dokumentasjonen må kunne gjenfinnes og leses på nytt. Uten anvendbarhet vil dokumentasjonen miste sin funksjon over tid, siden den ikke lenger vil kunne påvise etterlevelsen. Dette vil ha betydning for hvordan dokumentasjonen lagres.

ISO-standarden har i utgangspunktet ingen rettskildemessig vekt ved tolkningen av kravet i art. 24, ettersom den dreier seg om noe annet enn påvisning etter personvernforordningen. Den belyser imidlertid viktige elementer ved dokumentasjon som har betydning utover dens direkte virkeområde. Etter min mening er argumentasjonsverdien til standarden stor, slik at denne kan fungere på lignende måte som juridisk litteratur ved tolkningen av art. 24(1). De ovennevnte elementene sikrer at dokumentasjonen som fremlegges har kvaliteter som sikrer at de kan

[48] NOU 2019:9 s. 53.
[49] NOU 2019:9 s. 53.

brukes til å påvise etterlevelse. Dersom det sås tvil ved eksempelvis dokumentasjonens integritet, er denne uegnet til å påvise etterlevelse, siden det vil være knyttet usikkerhet til om den gir uttrykk for hvordan virksomheten faktisk opererer.

3 Innholdet i dokumentasjonsplikten

Plikten til å påvise etterlevelse etter art. 24 har et uklart innhold etter sin ordlyd. Når ulike virksomheter skal innordne seg etter denne plikten, møter de på en rekke spørsmål som lovteksten ikke gir klart svar på. Som vist i kapittel 2.2, innebærer plikten til å påvise etterlevelse at behandlingsansvarlig skal gjennomføre egnede tiltak, og i kapittel 2.3 er det vist at et slikt egnet tiltak kan være dokumentasjon. Særlig er spørsmålet om innordningen av den behandlingsansvarliges dokumentasjon vanskelig å få tak på etter ordlyden alene.

Grunnet at regelen om påvisning av etterlevelse etter GDPR er såpass ny, foreligger det ennå ikke klarhet rundt innholdet i denne plikten etter art. 24(1). Det er heller ikke sikkert at denne plikten kommer til å konkretiseres noe særlig, i hvert fall ikke i rettspraksis. Art. 24 er nemlig ikke omfattet av bestemmelsen om overtredelsesgebyr, som er den mest aktuelle sanksjonshjemmelen ved overtredelser av GDPR. Dette vil kunne redusere sannsynligheten for at CJEU vil vurdere det konkrete innholdet i bestemmelsen, siden saksforholdet neppe vil dreie seg direkte om denne bestemmelsen. Tre år etter forordningens ikrafttredelse foreligger det ennå ingen autoritative tolkninger av bestemmelsen.

Når ordlyden til bestemmelsen i art. 24 er såpass vid som den er, jf. redegjørelsen i kapittel 2.2, blir det praktisk vanskelig å få grep om hva som skal dokumenteres, og hvordan dette skal gjennomføres. Når det heller ikke foreligger rettspraksis om art. 24(1)’s rekkevidde, blir det nødvendig å benytte andre tolkningsmomenter for å klargjøre innholdet.

I det følgende vil jeg først redegjøre for håndhevelsesregimet etter GDPR. Dette gjør jeg for å lede opp til et spørsmål om disse reglene, nærmere bestemt reglene om overtredelsesgebyr, kan benyttes for å fastlegge innholdet i dokumentasjonsplikten etter art. 24.

3.1 Kan regelen om overtredelsesgebyr benyttes for å vurdere innholdet i dokumentasjonsplikten etter art. 24?

Prinsippet om den behandlingsansvarliges ansvar og presiseringen av ansvaret i art. 24(1) er uløselig knyttet til reglene om sanksjoner i kapittel 8, særlig reglene om overtredelsesgebyr. Dette sier seg selv, uten sanksjoner til å følge opp ansvaret til den behandlingsansvarlige, mister disse reglene sin reelle betydning. I tråd med at behandlingsansvarlige er blitt pålagt en rekke nye og utvidede plikter, har det derfor vært sentralt å sørge for en styrking av håndhevingsregimet i GDPR.

Denne styrkingen skjedde på to måter. For det første gjennom en klargjøring og utviding av oppgavene og kompetansene til de nasjonale tilsynsmyndighetene jf. forordningens art. 57 og art. 58. Målet med dette var å sørge for en håndhevelse av reglene som ga klare incentiver til etterlevelse. Videre ble det viktig å sørge for et samarbeid om anvendelsen og håndhevingen av personvernforordningen jf. art 57(1)(g), for å ivareta formålet om et ensartet personverns- og håndhevingsregime innenfor EU og EFTA.

Den andre var gjennom en økning av sanksjonsnivået i forhold til DPD, for å sikre etterlevelsen av forordningen. En av de mest sentrale oppgavene og kompetansene til tilsynsmyndigheten er derfor blitt å ilegge overtredelsesgebyr jf. art. 58(2)(i).

3.1.1 Vilkårene for å ilegge overtredelsesgebyr etter art. 83

Ilegging av overtredelsesgebyr er regulert i personvernforordningens art. 83. Et overtredelsesgebyr forstås som en administrativ reaksjon som ilegges ved brudd på en bestemmelse, og innebærer at en person skal betale et beløp til det offentlige jf. Prop. 60 L (2017-2018) s. 17. Sanksjonen er svært lik strafferettslige bøter, med den forskjellen at overtredelsesgebyr ilegges av forvaltningen, i dette tilfellet Datatilsynet som norsk tilsynsmyndighet jf. personopplysningsloven § 20(1).

Overtredelsesgebyr er ikke regnet som en strafferettslig reaksjon etter norsk nasjonal rett. Etter EMK er imidlertid slike administrative sanksjoner å regne som straff.[50] Denne forståelsen er anerkjent av Høyesterett i Rt. 2012 side 1556 avsn. 39 og Rt. 2011 s. 910 avsn. 48. Dette betyr at det må tas hensyn til en rekke grunnleggende rettsikkerhetsgarantier ved ileggelsen av overtredelsesgebyr etter art. 83 GDPR, som *retten til å ikke bli stilt for retten eller straffet to ganger* jf. EMK protokoll 7 art 4 nr. 1 (ne bis in idem), *retten til en rettferdig rettergang* jf. EMK art. 6 og *legalitetsprinsippet* i art. 7. Utøvelse av myndighet må skje i samsvar med slike prosessuelle garantier jf. GDPR art. 83(8) og art. 58(4).

Ileggelse av overtredelsesgebyr er etter norsk rett generelt regulert i forvaltningsloven (fvl.) § 44 jf. § 43. Bestemmelsene i forvaltningsloven er ikke selv hjemmel for å ilegge overtredelsesgebyr, men gir regler der slik hjemmel følger av særlovgivning. De reglene som er gitt her, må ses i sammenheng med de særlige vilkårene og reglene for skjønnsutøvelsen som er gitt i personvernforordningen art. 83.

Den direkte hjemmelen for ileggelse av overtredelsesgebyr er personvernforordningen art. 83. Bestemmelsen gir regler om hvordan tilsynsmyndigheten kan utøve den myndighet som er lagt til dem i art. 58(2)(i). Det sentrale vilkåret for å ilegge overtredelsesgebyr, er at det foreligger

[50] Prop. 60 L (2017-2018) s. 19.

et brudd på en av de opplistede bestemmelsene i art. 83(4) og (5). Denne listen må tolkes uttømmende, i lys av hjemmelskravene i EMK art. 7(1), Grl. § 113 og fvl. § 44. Det er likevel i GDPR art. 84(1) gitt hjemmel for nasjonale myndigheter til å også gjøre andre overtredelser sanksjonerbare. Etter norsk rett innebærer dette at brudd på art. 10 og art. 24 også er tilknyttet sanksjoner, på tross av at art. 83 ikke lister opp disse. Ansvaret for brudd på disse bestemmelsene følger av personopplysningsloven § 26. Denne særregelen er ikke å finne igjen i de andre nordiske persondatalovene.[51]

Ved spørsmålet om det skal ilegges gebyr, og ved utmåling av størrelsen av overtredelsesgebyret, skal tilsynsmyndigheten sikre at sanksjonen er «virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende» jf. art. 83(1).

At sanksjonen skal være virkningsfull innebærer i hovedsak en oppfordring til tilsynsmyndigheten om å faktisk ilegge overtredelsesgebyr der vilkårene for det er oppfylt, slik at håndhevingen av personvernforordningen er og oppfattes effektiv. Dette må ses i sammenheng med at overtredelsesgebyret skal være «avskrekkende». Hvis aktørene opplever at det gis gebyr ved overtredelser, kan art. 83 fungere som et «ris bak speilet» for å sikre etterlevelse. Samtidig skal størrelsen på gebyrene være store nok til at gebyret oppleves som et onde.

Det er to situasjoner hvor overtredelsesgebyr er aktuelt. Den første er der det foreligger et brudd på en eller flere av de opplistede bestemmelsene i art. 83(4) eller (5). Etter ordlyden holder det at det konstateres brudd, uten at det er tilknyttet andre vilkår. I denne vurderingen inngår en rekke forskjellige vurderingsmomenter jf. art. 83(2)(a) - (k). Disse momentene utgjør grensene for skjønnsutøvelsen til tilsynsmyndigheten. Listen oppgir de viktigste momentene. Det er likevel en nokså vid adgang til å legge vekt på andre momenter, ettersom bokstav k legger opp til at «enhver annen skjerpende eller formildende faktor ved saken» kan vektlegges.

Der en aktør ikke overholder, eller har nektet å etterkomme, et pålegg fra tilsynsmyndigheten jf. art. 58(2) kan det også være aktuelt å ilegge et overtredelsesgebyr jf. art. 83(6). Det er da de samme momentene som legger rammene for skjønnsutøvelsen.

Bestemmelsen i art. 83 legger opp til at det er en rekke aktører som kan ilegges overtredelsesgebyr. De mest sentrale rettssubjektene er behandlingsansvarlig og databehandlere, ettersom disse gruppene er pålagt en rekke krav og plikter etter forordningen, men også sertifiseringsorganer og kontrollorganer kan straffes jf. art. 83(4)(b) og (c).

[51] Prop. 56 LS (2017-2018) s. 137.

Der sanksjonen skal ilegges et foretak, har ikke lovteksten definert hvilke juridisk personer som er omfattet. Det følger imidlertid av fortalens punkt 150, som sier at begrepet skal forstås likt som «undertakings»-begrepet i Roma-traktaten art. 101 og 102. Heller ikke her er begrepet definert. Bestemmelsene dreier seg om konkurranserett. Innenfor konkurranseretten er begrepet tolket vidt, slik at det omfatter virksomheter «udoever oekonomisk virksomhed, uanset denne enheds retlige status og dens finansieringsmaade.» jf. C-41/90 avsn. 21, og at dette også gjelder når «denne økonomiske enhed juridisk set udgøres af flere fysiske eller juridiske personer» jf. C-217/05 avsn. 40. Jeg forstår henvisningen til Roma-traktaten slik at det er denne vide forståelsen, slik den er utviklet i rettspraksis, det siktes til.

3.1.2 Betydningen av reglene om overtredelsesgebyr ved tolkningen av art. 24

Bestemmelsene om overtredelsesgebyr er tett knyttet til reglene om ansvarlighet. Begge regelsettene handler som vist ovenfor grunnleggende om å plassere ansvar og sørge for at reglene i personvernforordningen er effektive og håndhevbare. Art. 24 vil være uten reell betydning dersom etterlevelsen ikke følges opp av tilsynsmyndigheter med «*meaningful powers of sanction*»,[52] og tilsynsmyndigheten vil ikke kunne beskytte den registrertes rettigheter på en tilfredsstillende måte uten at ansvaret for ivaretakelsen av disse rettighetene er plassert. Denne tette tilknytningen mellom regelsettene taler etter min mening klart for at reglene har relevans ved fastleggelsen av innholdet av dokumentasjonsplikten.

En effektiv måte å sørge for at behandlingsansvarlige etterlever personvernforordningen er å få dem til å selv drive en egenkontroll med sine rutiner og praksiser. Dette er et av formålene med art. 24. En vid og uoversiktlig plikt til dokumentasjon kan imidlertid føre til at denne internaliseringen av egne plikter feiler. Dokumentasjonen kan få et slikt omfang at den ansvarlige ikke evner å få et bevisst forhold til sin egen etterlevelse, eller det kan bli så lite omfattende at den ikke er egnet til å beskytte den behandlingsansvarlige mot sanksjoner.

Det vil gjøre det lettere for den enkelte ansvarlige å drive effektiv og presis dokumentasjon av sin etterlevelse, dersom denne kan innrettes med utgangspunkt i et regelsett som det allerede er incentiver til å ha kjennskap til, nemlig sanksjonsreglene. Å kunne dra veksler på hva som bør bevises i en eventuell erstatnings- eller overtredelsesgebyrsak er således en nokså lettvint løsning, og sørger for en indre sammenheng i regelverket. En slik løsning har altså også en pedagogisk verdi.

Løsningen med å bruke reglene om overtredelsesgebyr for å forstå innholdet i dokumentasjonsplikten etter art. 24 er også foreslått i juridisk litteratur. I boken «Personvernforordningen – En

[52] WP29 (2010) s. 17.

lærebok» av Dag Wiese Schartum foreslås det å bruke sanksjonsreglene, særlig art. 83(2), for å «*konkretisere behov og ideer for dokumentasjon*»[53]. Artikkel 83(2) oppstiller de momentene som skal inngå i skjønnsutøvelsen til tilsynsmyndigheten ved ileggelsen av overtredelsesgebyr. Momentene gir ikke i seg selv en konkret veiledning for innrettelsen av dokumentasjonen, men som det blir påpekt i boken er tilnærmingen «*mer en støtte for tanken enn noe som gir direkte og enkle svar*»[54].

I General Data Protection Regulation (GDPR) – A Commentary av Kuner og Bygrave m.fl. argumenteres det ikke direkte for en slik løsning, men det blir uttalt at eksistensen av sanksjonsreglene har «an important role in encouraging accountability» gjennom å både fungere avskrekkende og oppmuntrende.[55] Det pekes her på den tette tilknytningen som finnes mellom reglene om sanksjoner og ansvar, men det tas ikke standpunkt til om sanksjonsreglene kan bidra til å informere innholdet i dokumentasjonsplikten som ledd i påvisningen av etterlevelsen. Dette har nok sammenheng med at boken er skrevet fra et generelt perspektiv. I motsetning til Norge foreslo som nevnt verken Danmark, Sverige eller Finland å gjøre det sanksjonerbart å misligholde pliktene etter art. 24, jf. uttalelser i Prop. 56 LS (2017-2018) s. 137.

Disse argumentene, sett i sammenheng, viser etter min mening at art. 83 er et relevant utgangspunkt for forståelsen av art. 24(1).

Det er likevel ikke slik at denne tolkningen av innholdet i art. 24(1) basert på art. 83 alene kan gi tilfredsstillende svar. På dette stadiet av personvernforordningens levetid, i mangel på autoritative rettsavgjørelser om påvisningsplikten, er det derfor nødvendig å se hen til en rekke andre kilder for å få en helhetlig forståelse av det ansvaret som er pålagt den behandlingsansvarlige.

En annen sentral kilde som kan bidra til forståelsen av art. 24(1) er retningslinjene til WP29 og EDPB, som gir anvisning på hvordan Personvernrådet forstår innholdet i de konkrete bestemmelsene. Slike retningslinjer er ikke bindende på noen måte. I forarbeidene til personopplysningsloven ble det uttalt at det likevel er «grunn til å anta at uttalelsene i praksis vil bli tillagt stor vekt».[56]

Også uttalelser fra nasjonale tilsynsmyndigheter og nasjonal rettspraksis kan etter omstendighetene ha betydning ved tolkningsspørsmålet. Grunnen til at disse har betydning er at nasjonal

[53] Schartum (2020) s. 297.
[54] Schartum (2020) s. 297.
[55] Docksey (2020) s. 567.
[56] Prop. 56 LS (2017-2018) s. 168.

praksis sier noe om hvordan den enkelte staten forstår sine forpliktelser etter GDPR. Ettersom en harmonisert personvernlovgivning er et uttrykt mål med GDPR jf. fortalens punkt 3, vil særlig en konsekvent forståelse på tvers av landegrenser kunne være et aktuelt moment ved forståelsen av de innholdsmessige forpliktelsene i art. 24(1).

3.2 Typer av dokumentasjon

Dokumentasjon som begrep er som vist tidligere i kapittel 2.3 nokså vidt. Når det gjelder påvisning av etterlevelse etter GDPR kan begrepet med fordel deles inn i to hovedgrupper for å illustrere noen grunnleggende forskjeller.

Den første hovedgruppen (hovedgruppe 1), er den gruppen dokumentasjon som viser hvordan en virksomhet og behandlingen av personopplysninger formelt er organisert. Denne gruppen kan sies å omfatte påvisning av at ulike rutiner og systemer er på plass, samt andre formelle forhold ved virksomheten.[57] Innenfor denne gruppen finner man for eksempel krav til dokumentasjon av interne retningslinjer etter art. 24(2), og dokumentasjon av formell overholdelse av atferdsnormer eller sertifiseringsmekanismer etter art. 24(3).

Den andre hovedgruppen (hovedgruppe 2) er dokumentasjon av handlinger foretatt av virksomheten eller automatiske systemer, og hendelser under behandlingen. Dette er dokumentasjon som er viser hvordan behandlingen *faktisk* skjer.

De to hovedgruppene er avhengige av å eksistere samtidig for å få en fullgod dokumentasjon av den behandlingsansvarliges etterlevelse. Dokumentasjon av rutiner og retningslinjer er i seg selv bare en form for ønsketenkning om hvordan behandlingen bør skje. Der man bare har dokumentert formelle forhold vil man ikke vite noe om hvordan behandlingen av personopplysninger faktisk skjer.[58] En registrert vil ikke kunne føle seg trygg på at hans eller hennes personopplysninger, rettigheter og friheter er ivaretatt dersom den behandlingsansvarlige ikke samtidig kan påvise at disse tiltakene rent faktisk er effektive.

Her fungerer den andre hovedgruppen som bevis på at tiltakene faktisk er effektive. Ved at handlingene som foretas dokumenteres, kan behandlingsansvarlig selv kontrollere at behandling skjer i overenstemmelse med gjeldende regler og interne retningslinjer.

En aktuell måte å dokumentere faktiske forhold på, er gjennom logging. Logging er et begrep som ikke er nevnt i forordningen, mye grunnet den generelle naturen til GDPR og at

[57] Schartum (2020) s. 297.

[58] Schartum (2020) s. 297.

forordningen skal treffe behandlingsansvarlige som behandler personopplysninger på ulike måter, i ulikt omfang og med ulik risiko.

Logging skjer ved at et system blir utsatt for en form for hendelse, og deretter genererer en beskjed som typisk gir informasjon om når hendelsen skjedde, hva kilden til hendelsen var og en rekke andre typer data.[59] Hvilke typer data det dreier seg om vil variere, men kan typisk være IP-adresser, brukernavn, hvor en fil ble sendt, hvem som sendte en forespørsel eller tilsvarende.

Ved at hendelser blir logget, får den behandlingsansvarlige lagret en rekke data rundt det som skjedde. Hvilke hendelser det er som utløser loggingen vil variere. Dette kan tilpasses slik at det skapes logger ved hendelser av betydning for forpliktelsene etter art. 24 eller 32. For eksempel kan hendelsen være at en innsynsforespørsel etter art. 15 blir innsendt, eller at en spesiell mappe eller fil åpnes.

Det er gode grunner til å vie oppmerksomhet til denne måten å påvise etterlevelse på. Logging resulterer i dokumentasjon som sier noe om de faktiske forholdene, ved at den gir et øyeblikksbilde av situasjonen når den utløsende hendelsen inntreffer.

Hvis logging vurderes opp mot de kvalitetene ved dokumentasjon som ble redegjort for i kapittel 2.3.3, viser logging stort potensiale som påvisningsverktøy. Under forutsetning av at loggene er uendrede etter de oppstår, vil dokumentasjonen både gi autentisk og pålitelig informasjon i den forstand at resultatene er korrekte, og er oppstått til det gitte tidspunktet og under de gitte forholdene. Loggens integritet kan også sikres på flere måter. Enkle tiltak som at loggene lagres flere steder enn der de oppstår, vil kunne sikre at eventuelle modifikasjoner fanges opp når loggene holdes opp mot hverandre.[60] Hvor mye som skal gjøres for å sikre loggingens integritet vil imidlertid bero på risikovurderingen i art. 24(1), og det er derfor ikke gitt at en slik sikring er nødvendig i alle tilfeller.

At logging er svært godt egnet for påvisning kan også illustreres ved en sak fra det norske Datatilsynet, som endte i et vedtak om overtredelsesgebyr mot St. Olavs hospital. Enkeltstående forvaltningspraksis er absolutt ingen tungtveiende rettskilde med mindre denne gir uttrykk for en harmonisert forståelse av den konkrete bestemmelsen. Her bruker jeg imidlertid saken for å vise Datatilsynets syn på logging som påvisningsverktøy.

Saken handlet om at flere titalls tusen rapporter som inneholdt sensitive personopplysninger lå tilgjengelig for alle autoriserte brukere i Helse Midt-Norge RHF. Dette gjaldt blant annet

[59] Chuvakin (2013) s. 2 og 6.

[60] Chuvakin (2013) s. 314.

pasientenes redegjørelse for egen tilstand, navn på utførende lege og sykepleier, samt eventuelle komplikasjoner.

Særlig interessant i denne sammenheng er drøftelsen i punkt 5.2 hvor Datatilsynet vurderte betydningen av at St. Olavs ikke hadde logget aktiviteten på fil/mappeområdet. Datatilsynet uttalte at manglende logging gjorde det umulig å «bekrefte og/eller avkrefte om ansatte har benyttet seg av tilgangene», og at dette førte til en økt risiko for at hospitalet mistet oversikt over hvor journalene befant seg.[61] Datatilsynet konkluderte derfor med at manglende logging i seg selv utgjorde et brudd på kravene til «tekniske og organisatoriske tiltak» for å påvise etterlevelse i både personvernforordningen art. 24(1) og art. 32(1), samt pasientjournalloven § 23.

Det fremgår ikke direkte av vedtaket, men et underliggende moment i saken, som talte for at logging burde vært implementert, var den høye risikoen virksomheten opererte med. Særlig er det av betydning at behandlingen gjaldt sensitive personopplysninger jf. GDPR art. 9, at det var mange registrerte og at en rekke av de registrerte var barn. Dette er momenter som ved risikovurderingen etter art. 24(1) tilsier en skjerping i hva som kreves av den behandlingsansvarlige, jf. fortalens punkt 75 og gjennomgangen av denne i kapittel 2.2.2.

I punkt 5.4 i vedtaket til Datatilsynet ble manglende logging drøftet på nytt, men denne gangen som et moment i vurderingen av om overtredelsesgebyr skulle ilegges. Her ble det vektlagt at det ikke fantes en logg for to av de tre avvikene, og dette ble sett på som en skjerpende omstendighet etter art. 83(2)(a). Dette viser igjen den tette tilknytningen mellom ansvars- og sanksjonsreglene.

I litteraturen er også logging fremhevet som et særlig godt egnet virkemiddel for å påvise etterlevelse. Chuvakin fremhever logging som «a primary means of IT accountability» og «a perfect compliance technology».[62] Chuvakin vurderer riktignok logging i relasjon til amerikansk personvernslovgivning, men også i relasjon til GDPR er logging blitt nevnt som et nyttig påvisningsverktøy. Schartum peker på at denne typen dokumentasjon typisk vil kunne ha større bevismessig betydning enn dokumentasjonen av formelle forhold og lignende, og at det derfor bør vies «spesiell oppmerksomhet» til muligheten til å logge.[63]

En side ved logging som kan være verdt å nevne, er at logging i seg selv kan innebære en personopplysningsbehandling. Avhengig av hva som registreres av aktivitet, vil en logg etter hvert kunne inneholde nokså omfattende personopplysninger om enkeltpersoner. Dette vil blant

[61] Datatilsynet (20.09.2021) s. 8.
[62] Chuvakin (2013) s. 366.
[63] Schartum (2020) s. 297.

annet ha betydning for adgangen til å drive logging og spørsmålet om dokumentasjonens lagringstid. Dette kommer jeg tilbake til i kapittel 3.4.2.

Logging er ikke alene tilstrekkelig for å demonstrere den behandlingsansvarliges etterlevelse etter art. 24. Uten at loggen sammenholdes med annen dokumentasjon, vil loggen kunne være noe intetsigende. Et komplett bilde av den behandlingsansvarliges behandling av personopplysninger vil man først få der det fremvises dokumentasjon på formelle forhold som er gjennomført, som deretter blir holdt opp mot faktisk informasjon som påviser at disse tiltakene overholdes i virkeligheten. Både bruk av hovedgruppe 1 og hovedgruppe 2 er således nødvendig for å ivareta pliktene etter art. 24.[64]

3.3 Omfanget av dokumentasjonsplikten etter art. 24

Omfanget av dokumentasjonen er et spørsmål om rekkevidden av den behandlingsansvarliges påvisning av etterlevelsen, nærmere bestemt hvilke rettsregler som omfattes av plikten i art. 24.

Artikkel 24 kaster et bredt nett, ved å si at behandlingsansvarlig skal kunne «påvise at behandlingen utføres i samsvar med denne forordning». I dette ligger det at den behandlingsansvarlige må kunne påvise etterlevelse av enhver bestemmelse i personvernforordningen som pålegger positive eller negative plikter, og som har behandlingsansvarlig som pliktsubjekt. Dette inkluderer hovedsakelig reglene i kapittel 2 til 5. Det er altså snakk om en omfattende og svært vid påvisningsplikt for den behandlingsansvarlige.

Samtidig må pliktens omfang ses i sammenheng med andre prinsipper og friheter av betydning for personopplysningsbehandling, herunder prinsippet om proporsjonalitet og friheten til å drive næringsvirksomhet. Disse prinsippene taler for at dokumentasjonsplikten ikke kan være så vid at den i vesentlig grad vil hindre aktører å drive næringsvirksomhet innenfor forordningens virkeområde. Det er fortsatt ønskelig med fri flyt av data, og at virksomheter skal kunne drive med personopplysningsbehandling der denne tjener menneskeheten jf. fortalens punkt 4.

Tilsynsmyndigheten kan når som helst be om at den behandlingsansvarlige skal legge frem «all informasjon», herunder dokumentasjonen til den behandlingsansvarlige, som ledd i sine oppgaver etter personvernforordningen art. 58(1)(a). Tilsynsmyndighetens adgang til å kreve slik framleggelse gjelder så lenge den ber om informasjon den «trenger» for å utøve sine oppgaver.

Hva som ligger i at tilsynsmyndigheten «trenger» dokumentasjonen er skjønnsmessig, og vil bero på tilsynets egne vurderinger av hva som er nødvendig for å utøve sine oppgaver, primært da for å sikre at behandlingsansvarlig har opptrådt i overenstemmelse med GDPR. Dette bidrar

[64] Schartum (2020) s. 297.

til å legge et press på den behandlingsansvarlige, siden det ligger en bakenforliggende trussel i at tilsynsmyndigheten kan kreve dokumentasjon på overholdelsen av enhver bestemmelse som er omfattet av artikkelen.

Denne bakenforliggende trusselen bidrar til at behandlingsansvarlig oppmuntres til å sørge for at det foreligger nokså store mengder dokumentasjon til enhver tid. Særlig for behandlingsansvarlige som er dekket av personopplysningslovens virkeområde jf. § 4, vil omfanget av dokumentasjonen kunne oppfattes som krevende, siden Datatilsynet kan ilegge overtredelsesgebyr for manglende påvisning.

De færreste som driver med personopplysningsbehandling, vil imidlertid være omfattet av plikter etter samtlige bestemmelser i de aktuelle kapitlene. Dersom behandlingen ikke bruker samtykke som lovlig behandlingsgrunnlag, vil for eksempel art. 7, som pålegger behandlingsansvarlig å kunne påvise at det er innhentet lovlig samtykke, ikke være aktuell.

Behandlingsansvarlig vil ikke ha incentiv til å dokumentere etterlevelse av bestemmelser det ikke er knyttet sanksjoner til, siden ekstra dokumentasjon utgjør ekstra kostnader som virksomheten ikke vil få igjen som fortjeneste i form av ekstra sikring mot ansvar. Art. 83 gir likevel ikke her så mye veiledning i sin oppramsing av hvilke bestemmelser det er aktuelt å sanksjonere brudd på.

Listen i art. 83(4) og (5) er i det vesentlige sammensvarende med det som er nevnt ovenfor, ved at nærmest alle bestemmelsene i kapittel 2 til kapittel 5 er omfattet. Det er imidlertid noen unntak. Blant annet gjelder dette art. 10, som gjelder behandling av personopplysninger knyttet til straffedommer og lovovertredelser. Her er det imidlertid klart at en overtredelse, mest praktisk at en behandlingsansvarlig behandler slike opplysninger uten hjemmel i unionsretten eller nasjonal rett, automatisk vil være i strid med lovlighetsprinsippet i art. 5(1)(a) og reglene om gyldig behandlingsgrunnlag i art. 6, slik at overtredelsesgebyr uansett er aktuelt.

Selv om disse reglene ikke gir mye veiledning når det gjelder omfanget av dokumentasjonen, kan art. 83(4) og (5) likevel bidra noe. Hvis man ser på art. 83(4), som angir de «mindre alvorlige» overtredelsene, gjelder dette art. 8, 11, 25-39, 42 og 43. De «alvorligste» overtredelsene er av bestemmelsene i art. 5-7, 9, 12-22, 44-49 og eventuelle nasjonale regler jf. art. 83(5). Dette gir en pekepinn på hvilke bestemmelser det er «viktigst» å dokumentere etterlevelse av.

Omfanget av dokumentasjonsplikten kan også påvirkes av resultatet av risikovurderingen som er foretatt. Som vist i kapittel 2.2.2 vil risikovurderingen spille inn på de kravene som kan stilles til påvisingen av at behandlingen skjer i overenstemmelse med forordningen. Der risikoen er lav og behandlingen skjer i lite omfang kreves det ikke like mye av dokumentasjonen, herunder

når det gjelder hvor mye som må påvises. For slike mindre virksomheter med liten grad av risiko knyttet til behandlingen, kan dokumentasjonens omfang i større grad styres av den enkeltes risikovillighet enn de lavere kravene til omfanget av dokumentasjonen som vil følge av risikovurderingen etter art. 24.

Det er også slik at enkelte av disse punktene allerede omfattes av andre typer dokumentasjonskrav. Artikkel 30 vil som nevnt kunne tjene som dokumentasjon på etterlevelse av noen av kravene i GDPR, gjennom kravet til å ha tilgjengelig en rekke opplysninger om behandlingen. Artikkel 7 krever på sin side selvstendig dokumentasjon på at den enkelte registrerte har samtykket til behandlingen. Dette vil bidra til å redusere det konkrete omfanget av dokumentasjonsplikten etter art. 24(1), ettersom dobbeldokumentering ikke vil være mer egnet til å påvise etterlevelse i større grad enn å ikke gjøre det.

En ytterligere måte å redusere omfanget av dokumentasjonen på, er gjennom å ha et bevisst forhold til hvilke regler som gjelder særlig for den konkrete virksomheten. Som eksempel er det ikke nødvendig å kunne dokumentere at det foreligger gyldig samtykke fra den registrerte jf. art. 7(1) dersom dette ikke er et aktuelt behandlingsgrunnlag. Her kan bruk av styrende dokumentasjon være aktuelt for å begrense omfanget. Styrende dokumentasjon er en type dokumentasjon som skal gi et overordnet blikk på hvordan virksomheten er organisert og hvilke krav og plikter denne er underlagt.[65] Slike styrende dokumenter kan typisk kalles retningslinjer, policy eller standard, og er viktige for å legge grunnlaget for virksomhetens videre behandlingsrutiner.[66] Styrende dokumentasjon havner inn under hovedgruppe 1.

Slik styrende dokumentasjon er det i utgangspunktet lagt opp til at virksomheten må ha på plass dersom det står i «rimelig forhold til behandlingsaktivitetene» jf. art. 24(2). Det er ikke knyttet noen særlige vurderingsmomenter til denne rimelighetsvurderingen, men trolig vil de samme momentene som i første ledd kunne være veiledende også i denne sammenhengen, slik at jo større risiko som knyttes til virksomheten, jo større krav er det til å utarbeide slike interne retningslinjer.[67]

Gevinsten av å inneha slik styrende dokumentasjon er nokså stor. Utover at den veileder valg av tiltak etter art. 24(1), vil den også kunne fungere som dokumentasjon for de valgene som er foretatt, særlig når det gjelder hvilke regler virksomheten mener er relevante for dem. Det er samtidig ikke et veldig krevende tiltak å gjennomføre, slik at det kan være god grunn til å

[65] Datatilsynet Norge (2018).
[66] Skullerud (2019) s. 278.
[67] Skullerud (2019) s. 278

benytte slik dokumentasjon, selv der art. 24(2) ikke krever det. Dette gjenspeiles i fortalens punkt 78, som peker på at den behandlingsansvarlige «bør […] vedta interne retningslinjer».

Eksistensen av slik styrende dokumentasjon er likevel ikke alene tilstrekkelig for å påvise etterlevelse, da det er de reelle forholdene ved virksomheten som vil være avgjørende. Men det vil likevel kunne bidra til påvisningen dersom virksomheten samtidig kan vise at den i realiteten følger disse retningslinjene gjennom annen dokumentasjon, jf. drøftelsen om logging i kapittel 3.2.

3.4 Dokumentasjonens form og innhold

3.4.1 Formkrav til dokumentasjonen

Det er ikke uvanlig at det stilles krav til dokumenters form. Slike krav kan bidra til at dokumentasjonen kan systematiseres mer effektivt, og kan sikre notoritet rundt dokumentene.

Andre bestemmelser om dokumentasjon inneholder eksplisitte formkrav. Artikkel 30(3) krever at protokollene skal være «skriftlige, herunder elektroniske». Skriftlighetskravet er i seg selv ikke overraskende – skriftlighet ligger i kjernen av dokument-begrepet som nevnt i kapittel 2.3.

Både den norske og engelske språkversjonen av art. 30 er etter min mening noe uklar om hvorvidt det også er et krav om at protokollen skal være elektronisk. Bruken av ordet «herunder» i den norske versjonen kan tolkes som at elektronisk form også anses som skriftlig, altså at skriftlighetskravet kan oppfylles ved å ha en elektronisk protokoll uten å samtidig ha et fysisk eksemplar. Den engelske versjonen har formulert kravet som at protokollen «shall be in writing, including in electronic form». Ordet «including» heller etter min mening mer mot at det også er et krav om protokollen skal være elektronisk i tillegg til skriftlig.

I litteraturen er det heller ikke entydig hvilken løsning som gjelder. Jarbekk ser ut til å legge seg på den første linjen, uten at det drøftes noe videre.[68] Skullerud mfl. mener på den andre siden at protokollen skal kunne «sammenstilles og leveres ut på et lesbart og elektronisk format ved behov», og tar dermed til orde for den andre tolkningen.[69]

Formålet med bestemmelsen er å sikre ansvar og etterlevelse av GDPR.[70] Oppgaven med håndhevelsen av denne forpliktelsen er lagt til tilsynsmyndigheten jf. redegjørelsen i kapittel 3.1. For at disse skal kunne utføre sine tilsynsoppgaver på en effektiv måte, er de avhengig av at arbeidsmengden ikke blir så stor at det går ut over den registrertes rettigheter. En

[68] Jarbekk (2021) art. 30 note 4.
[69] Skullerud (2019) s. 305.
[70] Kotschy (2020) s. 618.

effektivitetsbetraktning i lys av formålet til bestemmelsen taler for at behandlingsansvarlig skal ha protokollen tilgjengelig elektronisk.

Basert på dette tolker jeg bestemmelsen dithen at den stiller et krav om både skriftlighet og elektronisk form.

Artikkel 24 gir ikke direkte anvisning på noen lignende formkrav. Dette kan begrunnes i at bestemmelsen har latt det stå åpent hvordan den behandlingsansvarlige skal påvise etterlevelsen av forordningen. Den mest praktiske formen for påvisning skjer imidlertid ved hjelp av dokumentasjon jf. drøftelsen i kapittel 2.3. Denne er det behov for å presisere formen av. Et krav til skriftlighet ligger her implisitt i at det er snakk om dokumentasjon, jf. redegjørelsen i kapittel 2.3.1.

Spørsmålet er om art. 24 kan tolkes slik at den også krever at dokumentasjonen skal foreligge elektronisk.

Ordlyden er taus om spørsmålet. Det er imidlertid et krav om at dokumentasjonen skal være egnet til å påvise etterlevelsen. Kravet om egnethet gjelder særlig to aspekter ved dokumentasjonen. For det første skal den være egnet til å redusere den risikoen som ligger innbakt i personopplysningsbehandlingen. I dette ligger det at dokumentasjonen skal kunne bidra til en risikoreduksjon. Dette vil være tilfellet dersom dokumentasjonen kan bidra til å plukke opp hendelser, og der dokumentasjonen har en opplærende og pedagogisk funksjon overfor behandlerne, ved at den gir dem et bevisst forhold til behandlingen og dens lovlighet. Det er også risikoreduserende at tilsynsmyndighetene kan benytte denne dokumentasjonen som grunnlag for tiltak etter art. 58(2) eller for å ilegge overtredelsesgebyr, da dette kan tvinge virksomheten til etterlevelse.

For det andre skal dokumentasjonen være egnet til å oppnå det tilsiktede formålet. I dette ligger det at den behandlingsansvarlige skal kunne påvise etterlevelse av forordningen. Dersom dokumentasjonen nedtegnes i et format som er utilgjengelig for tilsynsmyndigheten, vil den ikke være egnet til å påvise etterlevelse med mindre den kan omgjøres til et format som kan avleses. Dette må ses i sammenheng med de kvalitetene som kreves for god dokumentasjon, jf. redegjørelsen i kapittel 2.3.3. Dersom dokumentasjon er lagret i et slikt format som ikke kan omgjøres, vil dokumentasjonen ikke være anvendbar og miste sin funksjon som påvisningsverktøy.

Disse aspektene kan også ses i lys av prinsippet om åpenhet i art. 5(1)(a). Prinsippet skal sørge for at behandling av personopplysninger skjer på en slik måte at den registrerte får tilgang til nøyaktige og presise opplysninger om behandlingen, på en «lett tilgjengelig og lettfattelig måte» jf. fortalens punkt 39, jf. kravene i art. 12(1). Dersom dokumentasjonen ikke kan leveres

ut til den registrerte uten at den vanskeliggjør den registrertes utøvelse av sine rettigheter etter art. 16 flg., vil dokumentasjonen fort være uegnet til å redusere risikoen for overtredelser, siden den registrerte ikke kan drive en form for etterkontroll med behandlingen.

En tolkning av «egnede […] tiltak» vil ikke alene kunne begrunne at dokumentasjonen skal være tilgjengelig elektronisk. Dokumentasjon som bare foreligger skriftlig i form av papirdokumenter er ikke automatisk uegnet til å kunne påvise etterlevelse av forordningens regler. Et papirdokument kan for eksempel vise at det er gjennomført interne retningslinjer i virksomheten, og hvem sine personopplysninger som er behandlet kan nedtegnes for hånd.

Det er likevel slik at dokumentasjon i utelukkende fysisk form har en rekke ulemper ved seg. Det representerer en utgift for virksomheten og tilsynsmyndighetene om denne skal sendes via post eller om tilsynsmyndigheten må sende personell for å undersøke denne der dokumentasjonen er lagret. Det kan også bli spørsmål om notoritet rundt dokumentene dersom disse bare foreligger i ett eksemplar som må kopieres en rekke ganger.

Det er en rekke likheter mellom art. 24(1) og art. 30 som kanskje kan begrunne analogisk anvendelse av art. 30's formkrav på art. 24(1). For det første utgjør begge bestemmelsene en del av ansvarsreglene som er plassert i samme kapittel. Kravet til dokumentasjon i art. 24(1) og kravet til protokollering er nokså like i den forstand at art. 30 gir uttrykk for en type dokumentasjonskrav, men med klarere rammer enn dokumentasjonskravet i art. 24(1). Bestemmelsene søker også å oppfylle de samme grunnleggende formålene, nærmere å dokumentere etterlevelse av forordningen og sikre den registrertes rettigheter.

Det er også normalt lite krevende å ha dokumentasjon tilgjengelig elektronisk, eller i hvert fall å ha mulighet til å gjøre fysisk dokumentasjon tilgjengelig elektronisk.

Disse momentene taler etter min mening for at behandlingsansvarlige plikter å ha dokumentasjonen tilgjengelig elektronisk. De lege ferenda vil en slik løsning kunne lette arbeidet til tilsynsmyndighetene, og det kan være mer effektivt for den behandlingsansvarlige å ha dokumentasjonen tilgjengelig elektronisk.

Å bruke analogi for å begrunne et tolkningsresultat bør det imidlertid vises forsiktighet med. Som nevnt i kapittelet om overtredelsesgebyr, er sanksjonen å regne som straff etter EMK, slik at legalitetsbetraktninger trer inn for fullt. Det kreves klar hjemmel for å kunne ilegge overtredelsesgebyr. Etter GDPR vil det ikke automatisk være problematisk å innfortolke et slikt formkrav i art. 24(1). Ettersom art. 24 ikke er nevnt i bestemmelsen i art. 83(4) eller (5) kreves det ikke en like stor tilbakeholdenhet ved en slik tolkning.

Problemet er at Norge har fastslått at overtredelser av art. 24 i seg selv kan begrunne ansvar etter art. 83(4) jf. personopplysningsloven § 26 første ledd. Dette innebærer at det må utvises en større tilbakeholdenhet ved tolkningen og anvendelsen av bestemmelsen enn dersom det ikke var tilknyttet straffansvar til den. Det er generelt knyttet lite forutberegnelighet til en situasjon hvor en behandlingsansvarlig (som omfattes av personopplysningsloven virkeområde) kan straffes med overtredelsesgebyr for å ikke ha dokumentasjon tilgjengelig elektronisk, når art. 24 ikke eksplisitt setter dette som et krav. Dette taler sterkt mot at det oppstilles et generelt krav til elektronisk form på dokumentasjonen.

Rettskilder som reelle hensyn, formålsbetraktninger og en vid tolkning av ordlyden kan etter min mening ikke begrunne et generelt krav om elektronisk form ved all dokumentasjon etter art. 24(1).

Dette tolkningsresultatet er likevel ikke i veien for at spesielle dokumentasjonstyper bare anses egnet dersom de eksisterer i elektronisk form. Der risikovurderingen etter art. 24 tilsier at det skal implementeres slike dokumentasjonsløsninger, vil det samtidig kreves at denne dokumentasjonen er tilgjengelig i elektronisk form. For noen typer dokumentasjon, for eksempel logging, vil dette være særlig aktuelt jf. drøftelsen i kapittel 3.2.

3.4.2 Hvor lenge skal dokumentasjonen lagres?

En siste utfordring etter art. 24 jeg vil se på, er spørsmålet om hvor lenge en behandlingsansvarlig skal lagre dokumentasjonen.

Spørsmålet løses ikke direkte av den vide ordlyden i art. 24. Lagringstid må imidlertid ses i sammenheng med at dokumentasjon skal være egnet til å påvise etterlevelse av forordningen jf. art. 24(1) og gjennomgangen i kapittel 2.2.3. Dersom dokumentasjonen slettes for fort, vil den ikke kunne påvise eventuell etterlevelse, og vil dermed ikke være et egnet tiltak.

Spørsmålet om lagringstid er et spørsmål som avhenger av to ting. For det første må det tas stilling til når den behandlingsansvarlige senest kan inneha dokumentasjonen. For det andre må det tas stilling til tidspunktet hvor den behandlingsansvarlige ikke lenger plikter å inneha denne.

Når det gjelder det første spørsmålet, vil dette naturligvis bero på hvilken type dokumentasjonen det er snakk om.

Plikten til å gjennomføre egnede tiltak for å påvise etterlevelse gjelder gjennom hele behandlingen. Ettersom tilsynsmyndigheten kan be om "all informasjon" jf. art 58(1)(a) når som helst i løpet av behandlingen, vil utgangspunktet være at dokumentasjon på etterlevelsen må eksistere ved behandlingens oppstart. Dette gjelder imidlertid bare de dokumentasjonstypene som ligger

til hovedgruppe 1, som nevnt ovenfor i kapittel 3.2. Dette kan begrunnes i praktiske årsaker. Det vil tross alt ikke være mulig å inneha dokumentasjon som sier noe om faktiske forhold, før slike forhold har inntruffet. Systemene og tiltakene for å innhente denne dokumentasjonen må imidlertid være på plass ved behandlingens oppstart. Dokumentasjon som hører til hovedgruppe 1 er således mye lettere å ha på plass ved behandlingens oppstart. Dette gjelder for eksempel interne retningslinjer.

Dette utgangspunktet angående hovedgruppe 1 vil imidlertid modifiseres noe ved at kravene til påvisning, herunder dokumentasjon, kan endre seg i takt med at virksomheten utvikler seg over tid og at risikonivået varierer jf. drøftelsen i kapittel 2.2.2. Kravet til å inneha dokumentasjon vil da først inntreffe når risikoen ved behandlingen endrer seg nok til å begrunne nye påvisningstiltak. Dette har den konsekvensen at en behandlingsansvarlig som ikke er bevisst på slike endringer, vil kunne plikte å inneha dokumentasjon før den behandlingsansvarlige har rukket å foreta en ny risikovurdering og gjennomgå tiltakene etter art 24(1).

Når det gjelder spørsmålet om når plikten til å ha dokumentasjonen lagret opphører, er det flere momenter som må tas i betraktning.

Også her vil regler angående tilsynsmyndighetenes adgang til å ilegge overtredelsesgebyr kunne spille inn. Denne gangen er det imidlertid et annet aspekt ved håndhevelsesregimet som kan få betydning, nemlig foreldelsesreglene. Forordningen har ingen egen bestemmelse om foreldelse. I Norge er det inntatt en egen bestemmelse om dette i personopplysningsloven § 28. Her angis det at adgangen til å ilegge overtredelsesgebyr foreldes fem år «etter overtredelsen er opphørt». Denne fristen kan avbrytes ved at Datatilsynet kan foreta fristavbrytende grep. Dette skjer ved at Datatilsynet enten forhåndsvarsler om at den kommer til å vedta å ilegge overtredelsesgebyr, eller ved at Datatilsynet faktisk vedtar å ilegge gebyr.

Hvordan en overtredelse opphører kan skje på flere ulike måter, for eksempel ved at den behandlingsansvarlige har fattet grep for å bringe virksomheten i overenstemmelse med reglene. Et mer praktisk alternativ er at overtredelsen opphører fordi personopplysningsbehandlingen opphører.

Den primære motivasjonen for å lagre dokumentasjon vil for de fleste behandlingsansvarlige være å unngå ansvar og overtredelsesgebyr. Foreldelsesreglene vil derfor kunne gi en pekepinn på hvor lenge det er aktuelt å inneha dokumentasjonen. Ved at lagringstiden settes likt med foreldelsesfristen, under forutsetning av at et brudd vil ha opphørt dersom behandlingen opphører, vil lagring i minimum fem år etter opphørt personopplysningsbehandling kunne være et godt utgangspunkt.

Der dokumentasjonen i seg selv inneholder personopplysninger, som nevnt i kapittel 3.2 om logging, vil også prinsippet om lagringsbegrensing påvirke hvor lenge dokumentasjon kan lagres. Prinsippet kommer til uttrykk i art. 5(1)(e). Etter denne skal personopplysninger «lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene» som begrunner behandlingen. Dette innebærer i korte trekk at behandlingsansvarlige har en slettingsplikt etter en viss periode, og denne inntreffer når behandlingen ikke lenger er nødvendig for å oppfylle nærmere definerte formål. Det er likevel ingen bestemmelse i forordningen som setter en konkret tidsramme for hvor lenge personopplysninger kan lagres, selv om flere bestemmelser, herunder art. 13 og art. 14, synes å forutsette at en slik ramme er satt.[71]

Dersom dokumentasjonen inneholder personopplysninger, for eksempel ved at IP-adresser lagres i en logg, vil dokumentasjonen måtte slettes når den ikke lenger er nødvendig for å oppfylle behandlingsformålet. Dersom formålet utelukkende er å påvise etterlevelse av forordningen, vil lagringsbegrensingsprinsippet tilsi at dokumentasjonen slettes når den ikke lenger er egnet til slik påvisning. Hvis dette ses i sammenheng med foreldelsesreglene vil dette innebære at sletting senere enn 5 år etter behandlingen opphører, kan komme på kant med lagringsbegrensingsprinsippet.

Her er rettstilstanden usikker, men det er etter min mening gode grunner til å ta utgangspunkt i foreldelsesregelens femårsgrense. Det er imidlertid i denne sammenheng verdt å merke seg at ettersom forordningen er taus om spørsmålet, kan det være nasjonale særregler som setter rammer for lagringstiden for dokumentasjonen.

4 Avslutning

Utgangspunktet for den behandlingsansvarliges plikter etter art. 24(1) er at den ansvarlige skal kunne påvise etterlevelse av forordningen. En praktisk viktig måte å gjennomføre dette på er gjennom å inneha dokumentasjon. Oppgaven har forsøkt å gi svar på spørsmålet om hvilke krav som kan stilles til denne dokumentasjonen jf. drøftelsen i kapittel 3. Denne har vist at det er nokså mange elementer ved dokumentasjonen av etterlevelsen som det må tas stilling til når en behandlingsansvarlig skal vurdere gjennomføringen av dokumentasjon som tiltak etter art. 24. Dette gjelder særlig dokumentasjonens type, omfang og form. Forordningen er taus om en rekke spørsmål, for eksempel hva gjelder lagringstiden til denne dokumentasjonen og eventuelle formkrav. Ordlyden gir alene liten veiledning, samtidig som andre sentrale kilder som rettspraksis tilsynelatende ennå ikke har vurdert temaet.

[71] Schartum (2020) s. 168.

Temaet er samtidig av stor betydning for alle behandlingsansvarlige, men særlig for behandlingsansvarlige som opererer innenfor jurisdiksjoner som har knyttet overtredelsesgebyr til overtredelsen av art. 24. For de som foretar personopplysningsbehandlinger innenfor slike land, for eksempel Norge, er det etter min mening et stort behov for en nærmere klargjøring av disse pliktenes rettslige innhold, enten ved at det gis ut egnede retningslinjer fra EDPB etter art. 70(1)(e) eller ved at spørsmålet blir vurdert nærmere av domstolene.

Kildeliste

Litteratur

Arnesen (2015) — Arnesen, Finn. «Om den babelske vending i norsk rett» *Lov og rett* årg. 54 nr. 6 (2015) s. 344-362 [Lest i lovdata.no]

Aven (2009) — Aven, Terje og Renn, Ortwin. On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, vol. 12 nr. 1 (2009) s. 1-11.
DOI: 10.1080/13669870802488883

Butin (2014) — Butin, Denis og Le Métayer, Daniel. «Log Analysis for Data Protection Accountability» I *FM 2015: Formal Methods. 19th International Symposium Singapore, May 12-16, 2014 – Proceedings*. Cliff Jones, Jun Sun og Pekka Pihlajasaari red., Cham: Springer, 2014, s. 163-178. DOI: 10.1007/978-3-319-06410-9_12

Bygrave (2014) — Bygrave, Lee. *Data Privacy Law: An International Perspective.* Oxford: Oxford University Press, 2014.

Chuvakin (2013) — Chuvakin, Anton, Schmidt, Kevin, Phillips, Chris. *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Saint Louis: Elsevier Science & Technology Books, 2013. [https://doi.org/10.1016/C2010-0-65241-2]

Datatilsynet Danmark (2020) — Datatilsynet. «Vejledning om fortegnelse» (2020) https://www.datatilsynet.dk/Media/E/5/Fortegnelse%20(3).pdf, hentet 07.11.2021.

Datatilsynet Norge (2018) — Datatilsynet. «Internkontrollens struktur» (sist endret 30.10.2018). https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/internkontrollens-struktur/, hentet 07.11.2021.

de Terwangne (2020) — de Terwangne, Cècile. «Article 5 Principles relating to processing of personal data». I *The General Data Protection Regulation (GDPR): A Commentary*. Kuner, Christopher, Bygrave,

Lee A., Docksey, Christopher red., Oxford: Oxford University Press, 2020, s. 309-320

Docksey (2020) — Docksey, Christopher. «Article 24 Responsibility of the Controller». I *The General Data Protection Regulation (GDPR): A Commentary*. Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher red., Oxford: Oxford University Press, 2020, s. 555-570.

ICO (u.å.) — Information Commissioner's Office. «Documentation» (u.å.) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/, hentet 07.11.2021.

Jarbekk (2021) — Jarbekk, Eva. «Karnov lovkommentar til Personvernforordningen» i *Lovdata Pro* (2021), hentet 29.10.2021.

Kotschy (2020) — Kotschy, Waltraut. «Article 30 Records of Processing Activities». I *The General Data Protection Regulation (GDPR): A Commentary*. Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher red., Oxford: Oxford University Press, 2020, s. 616-624.

NAOB (u.å. a) — Det Norske Akademis ordbok. «Dokumentasjon» (u.å.) https://naob.no/ordbok/dokumentasjon, hentet 05.11.2021.

NAOB (u.å. b) — Det Norske Akademis ordbok. «Protokoll» (u.å.) https://naob.no/ordbok/protokoll, hentet 05.11.2021.

Ruud (2014) — Ruud, Morten og Ulfstein, Geir. *Innføring i folkerett*. 4. utg., Oslo: Universitetsforlaget, 2014.

Schartum (2020) — Schartum, Dag. *Personvernforordningen – en lærebok*. Bergen: Fagbokforlaget, 2020.

Sejersted (2014) — Sejersted, Fredrik. «Del I Bakgrunn og hovedtrekk». I *EØS-rett*. Føhn, Merethe, Sveen, Eline Ova red., 3.utg., Oslo: Universitetsforlaget, 2014, s. 21-120.

Shepherd (2003) Shepherd, Elizabeth og Yeo, Geoffrey. *Maintaining Records: A Handbook of Principles and Practice.* London: Facet Publishing, 2003. [lest i scholar.google.com]

Skullerud (2019) Skullerud, Åste Marie, Rønnevik, Cecilie, Skorstad, Jørgen mfl. *Personopplysningsloven og personvernforordningen (GDPR): Kommentarutgave*. Oslo: Universitetsforlaget, 2019.

Tosoni (2021) Tosoni, Luca. «Appendix 1: Data Protection Case Law Chart». I *The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update.* Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher red., 10.05.2021, s. 289-326. http://dx.doi.org/10.2139/ssrn.3839645, hentet 02.11.2021.

Norske rettskilder

Lover

1814 Lov 17. mai 1814 Kongeriket Norges Grunnlov [Grunnloven].

1967 Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker [forvaltningsloven].

1992 Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. [EØS-loven].

2018 Lov 15. juni 2018 nr. 38 om behandling av personopplysninger [personopplysningsloven].

Forarbeider

Ot.prp.nr.79 (1991-1992) *Om lov om gjennomføring i norsk rett av hoveddelen i Avtale om Det europeiske økonomiske samarbeidsområde (EØS), mv.*

Ot.prp. nr. 102 (2004-2005) *Om lov om rett til innsyn i dokument i offentleg verksemd (offentleglova).*

NOU 2016: 19 *Samhandling for sikkerhet: Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.*

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*.

Prop. 60 L (2017-2018) *Endringer i alkoholloven, atomenergiloven, folkehelseloven, legemiddelloven, lov om medisinsk utstyr, strålevernloven og tobakksskadeloven mv. (overtredelsesgebyr mv.).*

NOU 2018: 17 *Klimarisiko og norsk økonomi.*

NOU 2019: 9 *Fra kalveskinn til datasjø – Ny lov om samfunnsdokumentasjon og arkiver.*

Rettspraksis og forvaltningsvedtak

Rt. 2011 s. 910 *Tine*

Rt. 2012 side 1556 *Gran & Ekran*

Datatilsynet (20.09.2021) Datatilsynet. *Vedtak om overtredelsesgebyr – St. Olavs hospital HF*. 20. september 2021. Dokumentnummer 20/01813-4 [https://www.datatilsynet.no/contentassets/447e5ad0c7f346fc9cc1c0d62d023bba/vedtak-om-overtredelsesgebyr--st.-olavs-hospital-hf.pdf]

Internasjonale rettskilder

Regelverk og forarbeider

COM(2012) 11 *Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse).*

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

ECFR	*Charter of the Fundamental Rights of the European Union* 2016 (C 202/02).
EMK	*Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter*, Roma 4. november 1950 [norsk oversettelse].
EØS-avtalen	*Avtale om Det europeiske økonomiske samarbeidsområde*, Oporto 2. mai 1992.
Forordning 2016/679	*Europaparlamentets- og rådsforordning (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 (generell personvernforordning)*. [norsk versjon]
Forordning 2016/679	*Europa-parlamentets og rådsforordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)* [dansk versjon].
Förordning 2016/679	*Europaparlamentets och Rådets förordning (EU) 2016/679av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)* [svensk versjon]
Regulation 2016/679	*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [engelsk versjon]
Règlement 2016/679	*Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive*

	95/46/CE (règlement général sur la protection des données) [fransk versjon]
Verordnung 2016/679	*Verordnung (EU) 2016/679 des Europäishen parlaments und des rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)* [tysk versjon]
TFEU	*The Treaty on the Functioning of the European Union*. Consolidated version 2016 (C 202/01).

Rettspraksis

Case C-41/90 Höfner and Elser v Macrotron GmbH.	ECLI:EU:C:1991:161
Case C-217/05 Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española de Petróleos SA	ECLI:EU:C:2006:784
Case C-419/10 Wolfgang Hofmann v. Freistaat Bayern	ECLI:EU:C:2012:240
Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González	ECLI:EU:C:2014:317
Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH	ECLI:EU:C:2018:388
Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV	ECLI:EU:C:2019:629
Opinion of Advocate General P. Mengozzis on case C-25/17 Jehovan Todistajat	ECLI:EU:C:2018:57

Retningslinjer og veiledninger

OECD (1980) Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23.09.1980) https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, hentet 09.11.2021.

WP29 (2009) *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*. 02356/09/EN. 01.12.2009. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf, hentet 28.10.2021.

WP29 (2010) Article 29 Working Party. *Opinion 1/2010 on the concepts of "controller" and "processor"*. 00264/10/EN. 16.02.2010 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, hentet 09.11.2021.

WP29 (2014) Article 29 Working Party. *Statement on the role of a risk-based approach in data protection legal frameworks.* 14/EN. 30.05.2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf, hentet 13.11.2021.

EDPB (2018) EDPB. *Endorsement 1/2018* Brussel: 25.05.2018. https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf, hentet 15.10.2021.

EDPB (2019a) EDPB. *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*. 26.02.2019.https://edpb.europa.eu/sites/default/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf, hentet 20.11.2021.

EDPB (2019b) EDPB. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0* Guidelines 4/2019. 20.10.2020.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, hentet 14.11.2021.

EDPB (2020a) EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0*. Guidelines 07/2020 07.07.2021. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf, hentet 09.11.2021.

EDPB (2020b) EDPB. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0*. Recommendations 01/2020. 18.06.2021. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, hentet 16.11.2021.