Vurdering av personvernkonsekvenser i praksis

Om gjennomføring av vurdering av personvernkonsekvenser etter PVF artikkel 35

Masteravhandling i Forvaltningsinformatikk

Senter for Rettsinformatikk, avdeling for Forvaltningsinformatikk,
Det juridiske fakultet

Kandidatnr. 129395 og 129402

UNIVERSITETET I OSLO

Juni 2020

Sammendrag

I dette arbeidet har vi undersøkt en konsekvensvurdering gjennomført av Brønnøysundregistrene. I undersøkelsen har vi forsøkt å finne ut hvordan en kan gjennomføre en konsekvensvurdering etter PVF artikkel 35 og de organisatoriske forutsetningene for dette. I kapittel 1 går vi gjennom forskningsspørsmålene for dette arbeidet. I kapittel 2 arbeidet vi med å kartlegge relevante bestemmelser og begreper som var nødvendig på grunn av de til dels uklare bestemmelsene i personvernforordningen. Det var viktig å etablere et informasjons- og vurderingsgrunnlag for å kunne analysere funnene våre. I kapittel 3 har vi delt resultatene av undersøkelsen vår inn i tre deler: før, under og etter gjennomføring av konsekvensvurderingen.

Vi har forsøkt å belyse de forskjellige aspektene av en konsekvensvurdering. Dette innebærer at vi først undersøkte hva som var grunnlaget for at konsekvensvurderingen ble gjennomført og hvordan arbeidet ble organisert. Deretter fokuserte vi på hva som i hovedsak ble gjort under arbeidet med konsekvensvurderingen. Vi presenterer selve gjennomføringen av konsekvensvurderingen og trekker særlig frem arbeidet med risikovurdering. Videre presenterer vi eventuelle organisatoriske endringer Brønnøysundregistrene kan ha gjennomført på bakgrunn av arbeidet med konsekvensvurderingen vi har undersøkt. Under analysering av konsekvensvurderingen har vi brukt prosessen vi utledet fra kartleggingen av relevante begreper og bestemmelser i personvernforordningen.

Vi avslutter i kapittel 4 med samlede konklusjoner for funn og det generelle arbeidet vi har gjort. Vi legger også frem våre avsluttende refleksjoner som innebærer tanker vi har gjort oss og utfordringer vi har møtt på underveis. Helt avslutningsvis fremstiller vi våre tanker om hvordan vi ser for oss veien videre for Brønnøysundregistrene i forbindelse med konsekvensvurderinger og personvern generelt.

Forord

Denne oppgaven markerer slutten på fem år med studier for oss begge. Vi har brukt denne tiden til å høste kunnskap om alt fra hullkort til smarte byer. Vi føler vi sitter igjen med et helt unikt perspektiv og har erfart at det i stor grad er et veldig nyttig perspektiv. Vi er takknemlige for muligheten for å lære av så mange av de som vanker i miljøet knyttet til studiet. Fra advokater, skuespillere, utviklere og ikke minst andre forvaltningsinformatikere. Vi vil påstå at studiemiljøet vi har vært en del av de siste fem årene er noe for seg selv både faglig og sosialt. Vi vil savne både Domus Nova og alle de som har vært der for oss under eksamenstid og de litt roligere periodene. Vi har fått støtte og trøst fra både veileder og andre i administrasjonen. Ikke minst er vi takknemlige for den støtten vi har fått fra andre studenter både eldre og yngre, samt før og etter oss i studieløpet. Vi håper å kunne følge eksempelet til de som gikk foran oss og være en støtte for de som kommer etter oss.

Vi vil spesielt takke vår veileder Dag Wiese Schartum for konstruktive og solide tilbakemeldinger under arbeidet vårt med denne undersøkelsen. Vi innrømmer at det har variert mellom følelser av glede og fortapelse etter endte veiledningsmøter, men det har også helt klart brakt oss videre i arbeidet med undersøkelsen. Vi vil også takke for fem år med undervisning der du har vist oss gleden og frustrasjonen som følger med det å være en forvaltningsinformatiker.

Vi ønsker også å takke Synne Solbakken for å sette oss i kontakt med undersøkelsesobjektet vårt og for at du tok deg tid til å korrekturlese og komme med tilbakemeldinger. Du har også vært en konstant kilde til positivitet på “hjemmekontoret” under en vanskelig periode. Vi vil også takke vårt intervjuobjekt i Brønnøysundregistrene for at vi fikk intervjue deg og at du bidro med alle dokumentene til undersøkelsen vår. Vi håper du fortsetter med det viktige arbeidet med personvern i lang tid fremover. Takk også til Espen Holst Møllebak og Petter Ludvig Andersen som undersøkte muligheter for å sette oss i kontakt med potensielle virksomheter vi kunne tatt for oss i undersøkelsen. Til slutt vil vi takke Desireè og Bendik som har holdt ut med oss, spesielt de siste ukene før innlevering.

Oslo, 06. juni 2020

Innholdsfortegnelse

Oversikt over tabeller og figurer

1. Innledning

1.1 Bakgrunn og aktualitet

I 2018 ble lov om behandling av personopplysninger (personopplysningsloven) vedtatt for å inkorporere Europaparlamentets- og Rådsforordning (EU) 2016/679 av 27. april 2016 (generell personvernforordning, heretter PVF). Personvernforordningen ble vedtatt for å erstatte Europaparlamentets- og Rådsdirektiv 95/46/EC av 24. oktober 1995 (heretter «personverndirektivet»).

Etter tidligere personopplysningslov hadde virksomheter melde- og konsesjonsplikt for behandlingsaktiviteter med særlig inngripende karakter. Dette innebar at virksomheten måtte melde fra til eller søke om konsesjon fra Datatilsynet som gjennomførte egne konsekvensvurderinger av den planlagte behandlingen. Etter personvernforordningen har ikke virksomheter lenger en melde- og konsesjonsplikt for de fleste behandlingsaktiviteter.[1] Dette kommer av at lovgiver har plassert ansvaret for vurdering av personvernkonsekvenser hos den enkelte virksomhet. Dette følger av PVF artikkel 35 hvor den behandlingsansvarlig er pliktet til å gjøre en vurdering av personvernkonsekvensene av en behandling, dersom det er sannsynlig at behandlingen vil medføre høy risiko for fysiske personers rettigheter og friheter. Dette er i tråd med ansvarsprinsippet i PVF artikkel 5 (2). Ansvarsprinsippet fastsetter at den behandlingsansvarlige skal sikre og påvise at behandlingen av personopplysninger foregår i overensstemmelse med personvernforordningen, jf. PVF artikkel 24 (1).

I en rekke bestemmelser hvor ansvarsprinsippet materialiseres har den behandlingsansvarlige plikt til å treffe egnede tekniske og organisatoriske tiltak med sikte på å etterleve kravene i forordningen. I vurderingen av hvilke tiltak som er egnede må virksomheter etter personvernforordningen blant annet ta hensyn til risiko av ulik sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter. Dette gjelder ikke bare rettigheter og friheter knyttet til personvern. Det omfatter også grunnleggende rettigheter og friheter etter Den europeiske menneskerettighetskonvensjonen som for eksempel bevegelsesfrihet, retten

[1] Datatilsynet “Om melding og konsesjon”

til å ikke bli diskriminert, ytringsfrihet, osv. se avsnitt 2.5 nedenfor. Den behandlingsansvarlige må først se hvilke mulige konsekvenser behandlingen kan medføre og deretter vurdere hvor høy risikoen for krenkelse av den registrertes rettigheter og friheter er.

Vurdering av personvernkonsekvenser i henhold til PVF artikkel 35 og organisatoriske forutsetninger for dette er et aktuelt tema som er viktig å undersøke ettersom ny teknologi tas i bruk i større grad enn tidligere. Digitalisering medfører nye muligheter for å samle inn, prosessere og lagre større mengder personopplysninger. Nye teknologiske løsninger kan ha en rekke effektivitetsgevinster, samtidig som at dette også kan medføre uforutsette konsekvenser for fysiske personers rettigheter og friheter. Derfor er det viktig, spesielt ved bruk av nye teknologiske løsninger, å vurdere personvernkonsekvenser for å identifisere og håndtere risiko, jf. fortalepunkt 89. En slik vurdering kan også anses som en metode for å sikre og demonstrere regeletterlevelse.

I dette forskningsopplegget vil vi undersøke gjennomføring av en konsekvensvurdering i praksis i en spesifikk virksomhet. I undersøkelsen har vi valgt å undersøke en konsekvensvurdering gjort av Brønnøysundregistrene. Brønnøysundregistrene er et offentlig forvaltningsorgan ansvarlig for mange av landets viktigste registre. Vi har skrevet grundigere om Brønnøysundregistrene i avsnitt 3.2.1 nedenfor. I undersøkelsen vår vil vi se på den faktiske gjennomføringen av og de organisatoriske forutsetningene for å gjøre konsekvensvurderingen i samsvar med kravene i forordningen. Vi baserer selve undersøkelsen på erfaringer de ansatte fra Brønnøysundregistrene fikk fra vurderingen, samt de faktiske resultatene av vurderingen som ble gjennomført. I neste avsnitt vil vi redegjøre for de konkrete problemstillingene for undersøkelsen og diskutere disse nærmere.

1.2 Problemstillinger

Ut fra det vi har redegjort og diskutert i avsnittet ovenfor, har vi formulert en overordnet problemstilling som vi har tatt utgangspunkt i ved utformingen av delproblemstillinger for undersøkelsen. Den overordnede problemstillingen angir temaet for selve arbeidet, mens delproblemstillingene er det vi spesifikt vil undersøke. Disse vil danne bakgrunnen for selve

undersøkelsen og belyse nærmere det vi ønsker å finne ut av. Vi har formulert fire delproblemstillinger med tilhørende forklaringer og diskusjoner.

> *Hvordan gjennomføres en vurdering av personvernkonsekvenser i samsvar med PVF artikkel 35, og hva er de organisatoriske forutsetningene for en slik vurdering?*

Nedenfor har vi formulert mer spesifikke delproblemstillinger for å undersøke de faktiske forholdene i Brønnøysundregistrene. Disse vil danne bakgrunnen for selve undersøkelsen og belyse nærmere det vi ønsker å finne ut av.

1. *Hvordan organiserte Brønnøysundregistrene arbeidet med den konkrete konsekvensvurderingen, og hvem var det som deltok i dette arbeidet?*

Her vil vi se på hvordan oppgavene med konsekvensvurderingen ble fordelt og hva som var begrunnelsen for dette. Med dette sikter vi for eksempel til om den behandlingsansvarlige satt sammen en egen gruppe med ansatte fra ulike avdelinger innad i Brønnøysundregistrene til å jobbe sammen med konsekvensvurderingen eller om de brukte andre eksterne til å gjennomføre vurderingen.

Vi ønsker også å finne ut av hvilke roller den/de som arbeidet med konsekvensvurderingen hadde på tidspunktet vurderingen ble gjennomført. Det er for eksempel stor forskjell på om vurderingene ble gjort av noen som jobber med generell regeletterlevelse (f.eks. compliance) og noen som jobber med mer spesifikk type arbeid. Det er også interessant å se på eventuell sammensetning av ansatte fra ulike avdelinger og om det fantes tydelige forskjeller på hva som ble mest vektlagt under vurderingen. Når dette undersøkes, vil vi også se på hvem i Brønnøysundregistrene som avgjør graden av denne involveringen.

2. *Hvordan kom Brønnøysundregistrene frem til at de var rettslig forpliktet til å gjøre en vurdering av personvernkonsekvenser for den aktuelle behandlingen?*

Med denne delproblemstillingen er vi ute etter å undersøke hva som var begrunnelsen for at Brønnøysundregistrene som behandlingsansvarlig så seg forpliktet til å gjennomføre en konsekvensvurdering for behandlingen. Vi ønsker også å se på hva de baserte denne avgjørelsen på, for eksempel om behandlingen var særlig inngripende. I tillegg ønsker vi å vite hva slags informasjon som var tilgjengelig for den behandlingsansvarlige angående regelverk, retningslinjer og veiledning på dette tidspunktet. Vi ønsker å undersøke hvordan Brønnøysundregistrene har fått oversikt over hvilke behandlinger som krever en konsekvensvurdering etter PVF artikkel 35, og hva de har plikt til å risikovurdere.

Denne delproblemstillingen er viktig for å forstå bakgrunnen for selve konsekvensvurderingen. Vurderingen kan for eksempel ha blitt gjennomført på grunn av frykt for sanksjoner eller omdømmetap dersom de ikke etterlever kravene i forordningen. Delproblemstillingen er også med på å forklare noe om hvordan vurderingen ble gjennomført og eventuelt hvilke forutsetninger som eksisterte i Brønnøysundregistrene i forkant. Dette kan bidra til å skape et helhetlig inntrykk av prosessen med den aktuelle konsekvensvurderingen i virksomheten fra før den er påbegynt til etter den er avsluttet.

3. *Hvordan ble konsekvensvurderingen gjennomført og hva var det som konkret ble vurdert av Brønnøysundregistrene ?*

Med denne delproblemstillingen ønsker vi for det første å undersøke hvordan selve vurderingen ble gjennomført. Vi ser på om det ble benyttet noen spesifikke metoder for å blant annet vurdere risikoen for krenkelse av fysiske personers rettigheter og friheter. Her hadde det vært interessant å finne ut om hvilken metode Brønnøysundregistrene eventuelt brukte. Dersom det ble benyttet en spesifikk metode, er det også hensiktsmessig å se hvilket fagfelt denne er fra og om de som gjennomførte arbeidet har god kjennskap til denne. Dersom det ble brukt en ny metode som ikke har vært brukt av virksomheten tidligere, ønsker vi å undersøke hvorfor akkurat den metoden ble benyttet. For eksempel om metoden de benyttet var anbefalt. Vi vil undersøke erfaringer ved bruken av en slik anbefalt metode. Dette er særlig med tanke på om det var enkelt å lære og anvende metoden i praksis og om resultatene ved bruk av metoden var ansett som pålitelige.

Med denne delproblemstillingen vil vi også undersøke hva som konkret ble vurdert. Det ville for eksempel være interessant å undersøke i hvilken grad Brønnøysundregistrene har vurdert risiko for registrertes rettigheter og friheter. Med dette sikter vi på hvor bred vurdering virksomheten har gjort. Har de bare vurdert risiko for at den registrertes rettigheter etter personvernforordningen ikke blir overholdt eller har de også vurdert risiko for andre rettigheter og friheter? Dette kan blant annet fortelle oss noe om utfordringer en virksomhet kan ha ved å få oversikt over hvilke rettigheter og friheter behandlingen kan medføre konsekvenser for. Hvis Brønnøysundregistrene har valgt å avgrense vurderingen til rettigheter etter personvernforordningen vil vi også undersøke hva som er grunnen til dette. På en annen side kan virksomheten ha for få ressurser til å kunne få en fullstendig oversikt over hvilke rettigheter og friheter den tiltenkte behandlingen vil medføre en risiko for. I tillegg vil det være hensiktsmessig å se nærmere på om Brønnøysundregistrene faktisk har vurdert risiko for fysiske personer eller kun risiko for virksomheten selv. Dette kan blant annet omfatte konsekvenser for Brønnøysundregistrene selv ved brudd på personopplysningssikkerheten.

4. *Har det blitt gjort organisatoriske endringer som følge av erfaringene fra den konkrete konsekvensvurderingen?*

Denne delproblemstillingen tar for seg de eventuelle endringene Brønnøysundregistrene har gjort vedrørende organiseringen av arbeidet med konsekvensvurderingen. Vi vil se på hvordan virksomheten benyttet erfaringene de satt igjen med etter at de gjennomførte konsekvensvurderingen. Vi ønsker for eksempel å se på om det ble opprettet nye retningslinjer eller rutiner for å gjøre risiko- og konsekvensvurderinger, eller om eksisterende retningslinjer og rutiner ble endret og oppdatert. Dette innebærer blant annet å se på om sammensetningen av og kompetansen til de ansatte som arbeidet med gjennomføringen av konsekvensvurderingen var optimal. I tillegg er det interessant om det i etterkant av vurderingen ble utarbeidet en rutine på når personvernombudet skal involveres og i hvilken grad dette skal gjøres.

1.3 Metode

1.3.1 Innledning

I dette avsnittet vil vi gjennomgå organiseringen av forskningsopplegget vårt. Dette innebærer at vi vil gjøre rede for hva slags forskningsopplegg vi har valgt, hvilke datainnsamlingsmetoder vi har valgt og våre begrunnelser for valgene. Vi vil også skrive om hvordan vi har planlagt å gjennomføre undersøkelsen i praksis. Til slutt vil vi skrive om hvilke kildekritiske vurderinger vi har gjort underveis.

1.3.2 Oppsett av forskningsopplegget og valg av metoder

Forskning på vurdering av personvernkonsekvenser i henhold til PVF artikkel 35 er et relativt nytt felt. Særlig den formen vi har valgt hvor vi undersøker gjennomføring av en slik konsekvensvurdering i praksis og de organisatoriske forutsetningene for dette. Som følge av at vi tar for oss et nokså nytt forskningsområde har vi lagt til grunn et eksplorerende forskningsopplegg. Dette innebærer at vi har utviklet utforskende problemstillinger fordi vi ønsker mer kunnskap på et område der det er lite tilgjengelig forhåndskunnskap.[2] Vi ønsker med dette å utvikle ny kunnskap basert på erfaringer fra å gjennomføre en slik konsekvensvurdering i praksis. Vi har derfor ingen klare hypoteser som vi vil teste, men har et mer åpent sinn om hvilke funn vi vil gjøre. Vi har derimot noen forventninger om hvilke funn vi vil gjøre basert på det som er fastsatt i personvernforordningen. For eksempel kan vi se til forordningen for hva en vurdering av personvernkonsekvenser skal inneholde og involvering av personvernombudet i arbeidet, se avsnitt 2.4 nedenfor. Ut fra vår beskrivelse av problemstillingene i avsnitt 1.2 over er det her snakk om et enkelt-case studie. Vi tar for oss en virksomhet hvor det er sannsynlig at vi kan undersøke få enheter og likevel få et klart bildet av virkeligheten. Enkelt-case studie kjennetegnes av at en tar for seg få undersøkelsesenheter og går i dybden.[3] Som følge av dette vil ikke funnene vi gjør ha høy ekstern gyldighet, men vi ser ikke dette som særlig negativt for arbeidet vårt, ettersom vi er ute etter å finne erfaringer fra å vurdere personvernkonsekvenser. Det hadde vært interessant å sammenligne to eller flere virksomheters erfaring rundt konsekvensvurdering og de organisatoriske forutsetningene for

[2] Jacobsen (2018) side 99
[3] Jacobsen (2018) side 99-100

dette. På en annen side ville et slikt forskningsopplegg krevd enda mer tid og ressurser. Vi ser det som hensiktsmessig å begrense oss til én gjennomført konsekvensvurdering fordi vi ikke vet omfanget av funnene vi vil gjøre underveis. Et enkelt-case studie vil også være hensiktsmessig ettersom det kjennetegnes av å være fleksibelt. Det betyr at problemstillingene og forskningsopplegget kan utvikles etter de funnene som gjøres. Nedenfor redegjør vi for våre valg av datainnsamlingsmetoder og vår tilnærming til dette.

1.3.3 Juridisk metode

For å samle inn data- og vurderingsgrunnlag til forskningsopplegget har vi tatt utgangspunkt i hva som er fastsatt i personvernforordningen. Grunnen til dette er at vurdering av personvernkonsekvenser følger av et lovkrav. I PVF artikkel 35 har lovgiver blant annet fastsatt krav til når en er rettslig forpliktet til å gjøre en konsekvensvurdering, og minimumskrav til innholdet av konsekvensvurderingen, se avsnitt 2.4 nedenfor. Det er derfor nødvendig å bruke juridisk metode for å analysere kravene i artikkel 35. I analysen av kravene har vi ikke bare gjennomgått selve bestemmelsen men også Personvernrådets retningslinjer for høy risiko og vurdering av personvernkonsekvenser.[4] Personvernrådet er et uavhengig rådgivende organ for EU kommisjonen for personvernspørsmål. Dette rådet het tidligere Artikkel 29-gruppen (Article 29 Data Protection Working Party).[5] Personvernrådets hovedoppgave er å bidra til konsekvent anvendelse av personvernforordningen i hele EU- og EØS-området, og fremme samarbeid mellom tilsynsmyndighetene i de forskjellig medlemslandene.[6] Rådet består av ledere for hver av de europeiske tilsynsmyndighetene.[7] Personvernrådets oppgaver er fastsatt i PVF artikkel 70 (1). En annen oppgavene de har er blant annet å gi retningslinjer og uttalelser om ulike temaer som for eksempel vurdering av personvernkonsekvenser.[8]

I tillegg til Personvernrådet sine retningslinjer for konsekvensvurderinger har vi også undersøkt veiledningsmateriell om konsekvensvurderinger som Datatilsynet har publisert på deres nettside. Grunnen til dette er fordi Personvernrådets retningslinjer er generelle, men de ulike

[4] WP29 (2017)
[5] Datatilsynet (2016)
[6] European Data Protection Board (2016)
[7] Skullerud m.fl. (2018) side 323
[8] WP29 (2017) side 5

tilsynsmyndighetene kan utarbeide mer konkrete lister og veiledning på bakgrunn av retningslinjene til Personvernrådet. Datatilsynets liste over behandlingsaktivitetene som medfører høy risiko skal sendes til Personvernrådet for godkjenning, jf. PVF artikkel 35 (4). Både før og under undersøkelsen så vi det derfor hensiktsmessig å bruke begge kildene og se dem i sammenheng. Vi har også brukt juridiske litteratur hvor bestemmelsene i personvernforordningen er analysert og diskutert.

Vi har i stor grad valgt å fokusere på forordningen da dette blir vår hovedkilde til juridisk materiale ettersom hovedbestemmelsen vedrørende konsekvensvurderinger finnes her. Vi har forsøkt å analysere sammenhengen mellom PVF artikkel 35 og andre bestemmelser i personvernforordningen, se avsnitt 2.3. Dette har vi gjort som følge av at plikten til å gjøre en konsekvensvurdering etter artikkel 35 må ses i sammenheng med andre krav og plikter i forordningen. Videre har vi sett på muligheten for å benytte forarbeider for å supplere og gi en bredere forståelse av kravene i artikkel 35.

1.3.4 Dokumentstudie

For å kunne undersøke en vurdering av personvernkonsekvenser i Brønnøysundregistrene, vil det være nødvendig å lese en faktisk vurdering.Vi ønsket å få tilgang til all relevant informasjon som kan gi oss et inntrykk av hvordan arbeidet med konsekvensvurderingen ble gjennomført. Det innebærer den aktuelle vurderingen som er gjenstand for vår undersøkelse og dokumentasjonen som ble gjort underveis i arbeidet. Dette er dokumentasjonen som blant annet følger av forordningen, se avsnitt 2.3 nedenfor. I tillegg var det også interessant for oss å få tilgang til supplerende dokumentasjon, f.eks. i form av notater eller tilleggsdokumenter virksomheten selv har valgt å inkludere.

For å få innsyn i dokumentasjonen sendte vi en forespørsel til Brønnøysundregistrene om å få tilgang til en gjennomført konsekvensvurdering. Vår kontaktperson i Brønnøysundregistrene som også var vårt intervjuobjekt sendte oss fem dokumenter:

- Konsekvensvurderingen som ble gjennomført av Brønnøysundregistrene for ny søketjeneste de utarbeidet

- Risikovurdering som ble gjort i forbindelse med konsekvensvurderingen
- Risikorapport som omtalte og forklarte en annen risikovurdering og tilhørende tiltak for å forsøke å redusere risikoene.
- To dokumenter som inneholdt tilleggsinformasjon om konkrete tekniske tiltak for å minimere en bestemt risiko.

Sammen med den oversendte dokumentasjonen fikk vi også nyttig informasjon om bruk av maler og metoder Brønnøysundregistrene benyttet for å gjennomføre konsekvensvurderingen. Dokumentene vi fikk tilgang til må ses i sammenheng med at personvernforordningen inneholder et implisitt krav til dokumentasjon for å kunne påvise etterlevelse, se avsnitt 2.3 nedenfor.

1.3.5 Intervju

Vi ønsket også gjennomføre et semistrukturert intervju for å samle inn data for undersøkelsen. Et semistrukturert intervju kjennetegnes av at temaer og spørsmål som skal gjennomgås under intervjuet er planlagt på forhånd. Den mest praktiske måten å gjennomføre dette på er at en lager en intervjuguide med de planlagte spørsmålene. Samtidig kan en avvike noe fra intervjuguiden ved at man kan stille tilleggsspørsmål dersom intervjuobjektet for eksempel skulle fortelle om noe som er veldig interessant og relevant for undersøkelsen. Fordelene ved denne formen for intervju er at det gir oss fleksibilitet til å avvike fra den opprinnelige planen vår. Det kan også gi oss en mulighet for å undersøke nærmere andre aspekter som vi muligens ikke hadde tenkt så mye over tidligere. Dette er særlig egnet med tanke på at vår problemstilling er utforskende ettersom vi ikke vet helt sikkert hvilke oppdagelser vi vil gjøre, se avsnitt 1.3.2 ovenfor.

Et semistrukturert intervju vil kunne legge til rette for at vi enklere kan strukturere og analysere våre funn. Vi vurderte dette som fordelaktig i forhold til et åpent intervju der det ofte samles inn mye kompleks informasjon som kan være tidkrevende å strukturere i etterkant. Vi valgte å strukturere intervjuet vårt i forkant ved å utforme en intervjuguide. Ved å lage en intervjuguide i forkant av intervjuet hadde vi en plan som vi kan bruke til å holde oversikt over temaer vi skulle dekke i løpet av intervjuet.

Valget vedrørende hvem vi skulle intervjue var avhengig av hvem som hadde anledning, og hvilken kunnskap vedkommende hadde. Ettersom vi skulle undersøke Brønnøysundregistrenes arbeid med konsekvensvurdering, mente vi at det helst burde være en som deltok i dette arbeidet. Vi antok at jo mer involvert vedkommende har vært i arbeidet med konsekvensvurderingen, jo mer relevant kunnskap vil vedkommende mest sannsynligvis ha. Imidlertid måtte vi ta hensyn til hvem som hadde anledning til å stille til et intervju.

Vi ønsket å gjennomføre minst ett intervju i undersøkelsen. Dette som følge av at intervju som datainnsamlingsmetode kan ta mye tid og ressurser. I tillegg vil man som oftest måtte bruke mye tid på å strukturere informasjonen som samles inn under intervjuet. En annen grunn til at vi valgte å kun gjøre ett intervju er fordi undersøkelsen vår ble gjennomført mens vi var i en utfordrende periode grunnet koronavirus-pandemien. Det hadde derfor vært vanskelig for oss å avtale et nytt intervju før innleveringsfristen. Hvis det likevel skulle vise seg at vi ikke fikk samlet inn nok relevant data under intervjuet, og vi så det som nødvendig å samle inn mer data fra andre intervjuobjekter, var vi åpne for å gjennomføre et nytt intervju.

Vi avtalte med intervjuobjektet vårt å ha intervjuet over Microsoft Teams (heretter Teams), ettersom intervjuobjektet vårt befant seg i Brønnøysund. Vi så det som positivt å ha intervjuet over Teams fremfor over telefon ettersom det ville legge til rette for mer flyt i samtalen og bygge større tillit mellom oss og den vi intervjuer. Det er fordi vi da vil kunne se intervjuobjektet og intervjuobjektet vil kunne se oss.[9]

For å samle inn informasjonen under intervjuet planla vi å bruke både lydopptak og skrive notater. Ved å bruke lydopptak sikret vi at vi fikk med oss alt som ble sagt. Forutsetningen for at vi kunne ta lydopptak var at intervjuobjektet ga sitt samtykke til dette. Etter intervjuet skrev vi et referat og sendte til intervjuobjektet vårt for godkjennelse, samt kommentarer og suppleringer. Det kan være krevende å lete frem til spesifikk data i et lydopptak av et intervju med opptil en times varighet. Vi noterte derfor ned hva intervjuobjektet fortalte oss slik at vi senere kunne bruke notatene til å finne frem til informasjonen i lydopptaket. Vi hadde også alle dokumentene vi fikk tilsendt fremfor oss under intervjuet.

[9] Jacobsen (2018) s.148

1.3.6 Kildekritikk

Gjennom hele arbeidet med undersøkelsen har vi forsøkt å være så kildekritiske som mulig. Dette innebærer å vurdere påliteligheten og gyldigheten av kildene vi har brukt i undersøkelsen. Det er viktig med tanke på at konklusjonene vi gjør i undersøkelsen avhenger av hvilke kilder vi har brukt og vår evne til å analysere funnene.[10] Derfor har vi kontinuerlig gjort kildekritiske vurderinger med tanke på påliteligheten av dataene vi samler inn og på kildene våre i denne undersøkelsen. Videre i dette avsnittet vil vi først skrive om hvilke kildekritiske vurderinger vi har gjort under juridisk metode, så dokumentstudie og intervju.

Under juridisk metode har vi primært brukt personvernforordningen for å danne et informasjons- og vurderingsgrunnlag for undersøkelsen vår i kapittel 3. Ettersom forordningen er et nokså nytt, omfattende og komplekst regelverk var det hensiktsmessig for oss å bruke retningslinjer fra både Personvernrådet og Datatilsynet, samt annen juridisk litteratur om personvernforordningen. Som nevnt i avsnitt 1.3.3 ovenfor om juridisk metode har Personvernrådets retningslinjer en nokså stor rettskildemessig vekt. Da vi brukte retningslinjer og veiledningstekster fra Personvernrådet og Datatilsynet passet vi på at materialet var så oppdatert som mulig. Dette innebar å undersøke om Personvernrådet for eksempel hadde publisert noen nye retningslinjer eller uttalelser rundt konsekvensvurderinger. Personvernrådets uttalelser og retningslinjer er, som nevnt tidligere, gjeldende for hele EU og EØS-området. Datatilsynets veiledningsmateriale er basert på disse retningslinjene og uttalelsene, men er mer spesifikt gjeldende for Norge.

Da vi brukte juridisk litteratur vurderte vi blant annet tiden for når det var publisert for å vurdere hvor oppdatert innholdet var. I tillegg vurderte vi hvor dyptgående forfatterne av litteraturen hadde analysert bestemmelsene i personvernforordningen og for hvilke formål. Dette er fordi tolkningen av bestemmelsene kan være skreddersydd for et annet formål enn det vi har for undersøkelsen, derfor var det viktig å ha dette i bakhodet da vi brukte innholdet. Det var også

[10] Jacobsen (2018) side 227-246

viktig å undersøke hvem som var forfatterne for å kunne ta stilling til påliteligheten av innholdet.

Ved innsamling av dokumentene fra Brønnøysundregistrene tok vi særlig hensyn til at dette var sekundærkilder, altså data samlet inn fra andre enn oss selv.[11] Vi måtte også ta hensyn til at det ikke var vi selv som valgte ut hvilke dokumenter som ble undersøkt. Vi la kun noen føringer for hvilke typer dokumenter vi ønsket å undersøke, se avsnitt 3.1. Derfor måtte vi spørre oss om informasjonen i disse dokumentene gjenspeiler virkeligheten. Deretter måtte vi vurdere funnene vi trakk ut fra dokumentene og forsikre oss om at vi hadde forstått innholdet av disse. I den forbindelse var det viktig å hele tiden stille spørsmål ved både dokumentasjonens kvalitet og pålitelighet, samt våre egne oppfatninger. Noe som bidro til å oppklare dette var å fokusere på metodetriangulering som vi vil gjennomgå nærmere i avsnitt 1.3.7 nedenfor. Den supplerende informasjonen bidro til å knytte både dataene til virkeligheten, og gjorde at vi fikk testet om vår oppfatning av informasjonen stemte overens med slik det var tenkt.

Intervju er den eneste datainnsamlingsmetoden hvor vi har brukt primærkilder fordi vi samler inn data direkte fra kilden.[12] Som nevnt i avsnitt 1.3.5 ovenfor valgte vi ut hvem vi skulle intervjue basert på kunnskap vedkommende hadde om konsekvensvurderinger, og hvem som var tilgjengelig. Her var vi nødt til gjøre en avveining mellom hvem som hadde informasjonen vi ønsket å samle inn og hvem som var tilgjengelig for å kunne stille til et intervju. Før og under intervjuet tok vi til betraktning at flere faktorer kan påvirke hvordan intervjuobjektet vårt valgte å svare på spørsmålene våre. For eksempel ønsket vi å ta lydopptak av intervjuet, men bare dersom intervjuobjektet ga sitt samtykke til dette. Vi var også oppmerksomme på at vi under et intervju også samler inn subjektive data som kan være påvirket av bias fra intervjuobjektet vårt. Intervjuobjektet vil dele sine erfaringer ved gjennomføringen av konsekvensvurderingen, som kan være ulik erfaringen andre har fra gjennomføringen. Intervjuobjektet vårt var også ansvarlig for gjennomføringen av konsekvensvurderingen vi undersøkte. Dette kan være med

[11] Jacobsen (2018) s.139-140
[12] Jacobsen (2018) s.139-140

på å påvirke hvordan intervjuobjektet velger å svare, samt at vedkommende kan fremstå mindre kritisk til innholdet i konsekvensvurderingen.

Vi vurderte også om å ha intervjuet over Teams kunne påvirke hvordan intervjuobjektet valgte å svare. Ut fra spørsmålenes art og svarene vi kunne forvente oss, så vi det som forsvarlig å ha intervjuet over Teams. Etter intervjuet sendte vi som nevnt i avsnitt 1.3.5 et referat til intervjuobjektet for å verifisere at vår forståelse stemmer overens med det som ble sagt under intervjuet. Imidlertid fikk vi kun høre og lese ett perspektiv og har ikke hatt noe videre kontakt med andre som var deltakende i arbeidet med konsekvensvurderingen. Dette innebærer at om noe er beskrevet i dokumentasjon eller intervju som ikke stemmer med virkeligheten, hadde vi ingen mulighet til å finne ut av dette. I neste avsnitt vil vi redegjøre nærmere for hvordan vi planla å benytte datainnsamlingsmetodene slik at de utfyller hverandre.

1.3.7 Triangulering av metoder

Som nevnt ovenfor har vi hovedsakelig brukt juridisk metode for å danne et informasjons- og vurderingsgrunnlag for undersøkelsen. Det var viktig at vi hadde tilstrekkelig kunnskap om temaet vi undersøkte. Grunnen til dette var at vi var nødt til å vite hva vi var ute etter og at vi kunne vurdere funnene vi gjorde. For eksempel ville analysering av lovteksten, samt annen litteratur om tolkningen av lovtekst sette oss i bedre stand til å formulere relevante spørsmål til intervjuet. I tillegg gjorde det oss mer egnet til å sette oss inn i dokumentasjonen av konsekvensvurderingen.

Vi ønsket å undersøke dokumentasjonen av konsekvensvurderingen før vi gjennomførte intervjuet. Vi så det som hensiktsmessig å gjøre det på denne måten fordi undersøkelsen av dokumentasjonen kunne gi oss bedre oversikt over hva som var unødvendig å bruke tid på under intervjuet. Dette var også nyttig ved utforming av intervjuguide og strukturering av intervjuet. Det gjorde også at vi kunne fokusere på aspekter som ikke var inkludert i dokumentene, men som vi ønsket å få nærmere utdypet. En annen grunn til at vi ønsket å gjennomføre dokumentstudie først er fordi vi kunne spørre intervjuobjektet vårt om vår tolkning av innholdet var korrekt. Ved å kombinere dokumentstudie og intervju ville funnene våre dermed utfylle hverandre. Vi vil da kunne sammenligne det som er dokumentert med det som

ble sagt. Det vil si å sammenligne objektive data med subjektive data. I tillegg var det interessant å finne ut om funnene vi gjorde under dokumentstudiet og intervjuet avviket fra hverandre.

2. Kartlegging av begreper og krav i personvernforordningen

2.1 Innledende om kartleggingen

I dette kapittelet vil vi gjennomgå kravene i personvernforordningens artikkel 35 hvor vi finner hovedbestemmelsen for vurdering av personvernkonsekvenser. Det er viktig å se bestemmelsen i sammenheng med andre bestemmelser i personvernforordningen, for å forstå nærmere hva artikkelen omhandler. Dette gjør vi ved å skape et helhetlig overblikk over momentene i artikkelen for å få et godt nok grunnlag til å gjennomføre undersøkelsen i kapittel 3. Først vil vi diskutere hva som menes med risiko i personvernforordningen, deretter sette artikkel 35 i sammenheng med andre bestemmelser. For å oppnå dette ser vi først risikobegrepet i forskjellige kontekster og forsøker å oppnå en god forståelse av risiko. Dette gjøres blant annet ved hjelp av å se på ulike modeller for å vurdere risiko. Vi vil så gjennomgå kravene i artikkel 35 systematisk på et overordnet nivå i avsnitt 2.4 nedenfor. Deretter vil vi illustrere og forklare stegene i en konsekvensvurdering på et overordnet nivå. Til slutt vil vi fremheve og redegjøre for vurderingsmomentene for om en tiltenkt behandling medfører høy risiko for fysiske personers rettigheter og friheter.

2.2 Grunnleggende om risiko

2.2.1 Forståelsen av risikobegrepet

Risiko er et begrep som står sentralt i arbeidet med vurdering av personvernkonsekvenser. Lovgiver har fastsatt en rekke kriterier som skal brukes for å vurdere risiko, se avsnitt 2.3 til 2.2.5 nedenfor. Selve innholdet av hva som menes med risiko er ikke definert i forordningen. Risiko er derimot et begrep som er særlig kjent i forbindelse med informasjonssikkerhet og er sentralt for mange standarder i dette feltet.[13] For å diskutere hva som menes med risiko i personvernforordningen vil vi ta utgangspunkt i definisjonen til Personvernrådet i deres retningslinjer om vurdering av personvernkonsekvenser og høy risiko.[14] Grunnen til at vi tar utgangspunkt i definisjonen til Personvernrådet er fordi rådets hovedoppgave er å sikre

[13] ISO 31000:2018 og ISO 27000-familien
[14] WP29 (2017)

harmonisert etterlevelse av personvernforordningen. For å oppnå dette har Personvernrådet i oppgave å blant annet undersøke spørsmål vedrørende anvendelse av personvernforordningen, avgi uttalelser, samt gi anbefalinger og retningslinjer for å fremme en ensartet anvendelse av forordningen, jf. PVF artikkel 70 (1) (e).[15] Nedenfor vil vi sammenligne Personvernrådets definisjon av risiko med elementene risiko består av i ISO 31000-standarden.

ISO (International Organization for Standardization) er en verdensomfattende sammenslutning av nasjonale standardiseringsorganer. ISO utarbeider og publiserer internasjonale standarder som for eksempel ISO 31000-standarden.[16] Dette er en standard for risikostyring som inneholder retningslinjer, prinsipper, rammeverk og prosess for å håndtere risiko. Denne standarden kan også brukes av en hvilken som helst organisasjon, uavhengig av størrelse og sektor.[17] Personvernrådet påpeker i sine retningslinjer for vurdering av personvernkonsekvenser at komponentene av risiko som følger av fortalepunkt 90 i personvernforordningen, overlapper med en rekke definerte komponenter av risikostyring i ISO 31000-standarden.
Personvernrådets definisjon av risiko:

"A "risk" is a scenario describing an event and its consequences, estimated in terms of severity and likelihood."[18]

Det første elementet av risiko som trekkes frem i ISO 31000 er at risiko består av en hendelse, mer nøyaktig en uønsket hendelse.[19] Dette kan være snakk om en hendelse man har en plikt, eller et ønske om, å avverge. For eksempel kan det omfatte villede handlinger som at uvedkommende med intensjon får uautorisert tilgang til personopplysninger. Det kan også være ikke-villede handlinger som følge av svikt i organisatoriske rutiner, som å glemme å logge seg av jobb PCen sin. Det neste elementet er konsekvensene hendelsen medfører.

[15] Skullerud m.fl. (2018) side 325
[16] ISO "What we do"
[17] ISO 31000:2018
[18] WP29 (2017) side 6
[19] ISO 13000:2018 Risk management - Principles and guidelines side 5

Dette kan for eksempel være snakk om en hendelse som for eksempel at personopplysninger kommer på avveie, som medfører tap av tillit, tap av omdømme, osv. Det tredje elementet er risikofaktorene som omhandler beskrivelse av alvorlighetsgraden til konsekvensene og sannsynligheten for de vil inntreffe.[20] Ved å se til hva det er lagt vekt på i ISO 31000 standarden, er det tydelig at Personvernrådets definisjon av risiko bygger på de samme elementene. PVF artikkel 35, samt andre bestemmelser og fortalepunkt i forordningen, inneholder også risikokriterier vedrørende hendelse, konsekvenser og risikofaktorer, se avsnitt 2.3 til 2.5 nedenfor.

I følge Gellert (2017) er det fastsatt en rekke kriterier i personvernforordningen vedrørende hendelser som kan medføre risiko, men ikke særlig mange kriterier som omhandler konsekvenser for fysiske personers rettigheter og friheter. Videre påpeker Gellert (2017) at flere av kriteriene omhandler beregning av risikoenes alvorlighetsgrad, men ikke dens sannsynlighetsgrad. Resultatet av dette er at det foreligger ingen regler for hvordan risiko skal vurderes i praksis.[21] I personvernforordningen har ikke lovgiver fastsatt noen spesifikk metode som den behandlingsansvarlige skal benytte ved gjennomføring av konsekvensvurderingen. Dette henger sammen med Personvernrådets retningslinjer hvor det er fastsatt at personvernforordningen gir den behandlingsansvarlige fleksibilitet, til å bestemme den nøyaktige strukturen og formen til konsekvensvurderingen selv. Formålet med dette er at den behandlingsansvarlige selv skal kunne vurdere hvilken struktur og metode som passer med eksisterende arbeidsprosesser.[22] Personvernforordningens fortalepunkt 90 inneholder komponentene som skal brukes til å vurdere risiko når man gjennomfører en konsekvensvurdering. Dette omfatter å vurdere sannsynligheten for at det vil oppstå høy risiko, dens alvorlighetsgrad og kildene til risikoen(e). Personvernrådet har også understreket at det finnes en rekke ulike etablerte prosesser i EU og over hele verden som tar hensyn til komponentene av risiko slik det er beskrevet i fortalepunkt 90. Uansett hvilken form den har, må en konsekvensvurdering i henhold til personvernforordningen være en unik vurdering av

[20] ISO 13000:2018 Risk management - Principles and guidelines side 4
[21] Gellert (2017) side 287
[22] WP29 (2017) side 17

risiko for fysiske personers rettigheter og friheter, og gjøre den behandlingsansvarlige i stand til å iverksette tiltak for å håndtere risikoen på en tilfredsstillende måte.[23]

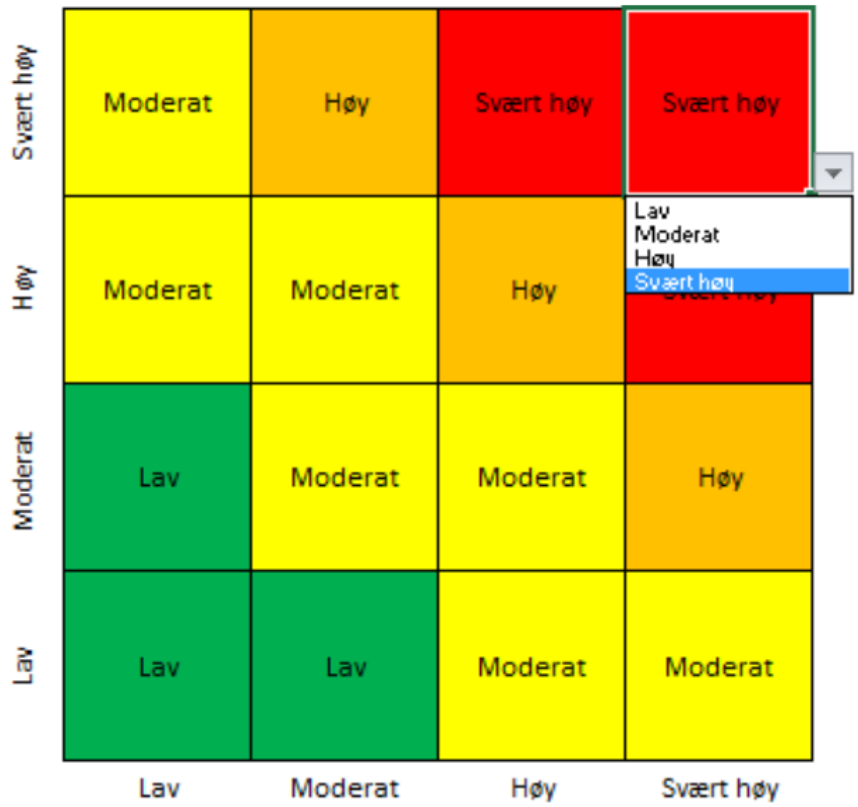
Ved å ta i betraktning det vi har redegjort og diskutert ovenfor vil vi argumentere for at man kan bruke alminnelig forståelse av risikobegrepet i personvernforordningen ettersom risikobegrepet ikke er klart definert. Personvernforordningen viser til momenter av risiko som overlapper med allerede definerte elementer av risiko i alminnelig forstand. Til slutt påpeker også Personvernrådet at det finnes en rekke ulike metoder for å vurdere risiko som tar hensyn til disse momentene. For å forsøke å bedre vår forståelse av begrepet, tok vi i bruk risikomodeller for å forklare nærmere hvordan man kan beregne og arbeide med sannsynlighets- og alvorlighetsgraden av risiko. Vi har valgt å trekke frem to forskjellige risikomodeller og diskutere dem i forhold til hverandre. En risikomodell består av ulike definisjoner av risikofaktorene og forholdene mellom de og kan bidra til bedre forståelse av risiko.[24] Grunnen til at vi har valgt disse risikomodellene er fordi de består av de samme elementene som personvernforordningen viser til i fortalepunkt 90, men på litt ulike måter, se avsnitt 2.2.2.3 nedenfor. Som påpekt ovenfor har ikke lovgiver fastsatt krav til hvordan risikoenes sannsynlighets- og alvorlighetsgrad skal beregnes, bare at de skal vurderes på en objektiv måte.[25]

2.2.2 Risikomodeller

2.2.2.1 Risikomatrisen

Den første risikomodellen vi ønsker å trekke frem er risikomatrisen. Dette er en modell som tar hensyn til en hendelse med en konsekvens og tilhørende alvorlighet- og sannsynlighetsgrad, samt kilden til risikoene. I en risikomatrise blir hvert element vurdert og risikoen blir tilegnet en plass i et diagram som vist i figur 1 nedenfor.

[23] WP29 (2017) side 17
[24] NIST (2012) avsnitt 2.3.1 side 8
[25] Gellert (2017) side 287



Figur 1 Eksempel på risikomatrise[26]

Risikomatriser finnes i flere versjoner og endres etter behov for hver enkelt virksomhet. I hovedsak blir hver konsekvens plassert i diagrammet basert på en vurdering av risikofaktorene som nevnt i avsnitt 2.2.1 ovenfor. Denne vurderingen gjøres, som vist i figur 2 nedenfor, ved å først beskrive hver tenkte hendelse og dens konsekvens(er).

Risikobeskrivelse Stikkord om: (1) innledende hendelse(r) (2) informasjonssikkerhetsbruddet (3) de uønskede konsekvensene som kan oppstå	**Begrunnelse for konsekvensvurdering**	**Konsekvens**	**Tilhørende sannsynlighet**	**Begrunnelse for vurdering av tilhørende sannsynlighet**	**Risikonivå**
Risiko 1		Høy	Svært høy		Høy

[26] Digitaliseringsdirektoratet (2018)

Figur 2 Tabell for å beregne risiko[27]

Deretter vurderer man alvorlighetsgraden for denne konsekvensen. En konsekvens kan vurderes som alt fra svært lav til svært høy. Så vurderes sannsynlighetsgraden på samme skala. Etter at begge risikofaktorene er vurdert, plasseres hver identifiserte risiko på bakgrunn av dette inn i risikomatrisen. For eksempel vil risiko med lav alvorlighetsgrad, men med høy sannsynlighetsgrad bli plassert øverst i venstre hjørne i matrisen og innebære en moderat risiko (se figur 1). Etter at man har plassert alle konsekvensene i diagrammet vil man kunne identifisere både høy og svært høy risiko basert på hvilken plass i matrisen de er tildelt.

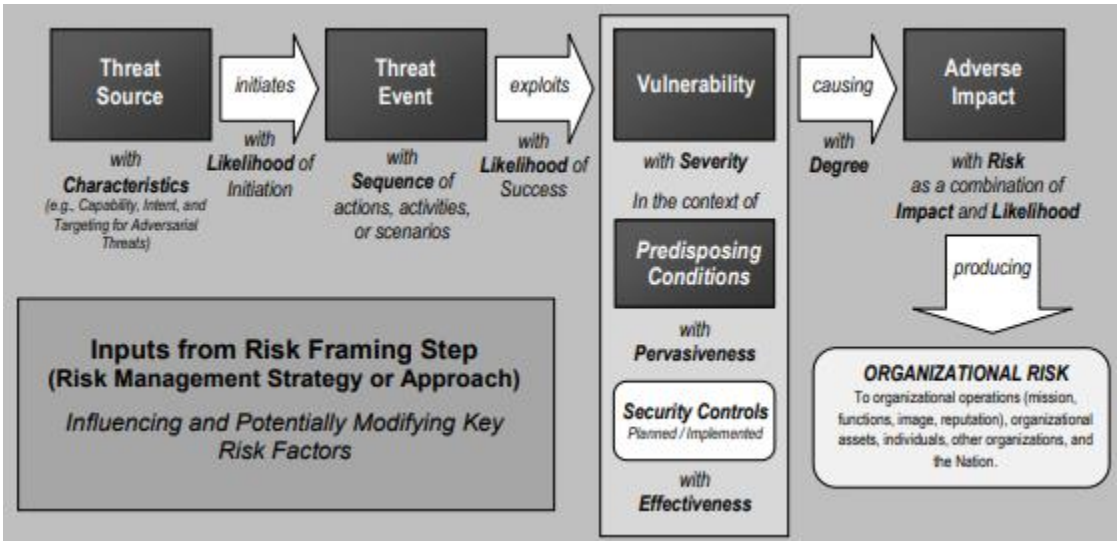
Vurderingene vil variere fra virksomhet til virksomhet, det vil også variere hva som regnes som akseptabel risiko, altså hendelser man ikke plikter til eller ønsker å avverge. Akseptabel risiko kan også innebære en hendelse man ønsker å avverge, men ikke har mulighet til å prioritere. Sannsynlighet- og alvorlighetsgrad er noe som må vurderes ut ifra erfaringer og tidligere hendelser. Det er derfor viktig å komme med en god beskrivelse av hendelse og konsekvens samt at man begrunner de vurderingene som ble gjort for hver enkelt risiko. Dermed er det viktig å benytte gode vurderingsmetoder og rutiner.

2.2.2.2 NIST risikomodell

Den andre risikomodellen vi vil trekke frem er laget av National Institute of Standards and Technology (heretter omtalt som NIST). NIST er et ikke-regulatorisk føderalt byrå innen det amerikanske handelsdepartementet som fremmer vitenskap, standarder og teknologi med ønske å forbedre økonomisk sikkerhet og livskvalitet i Amerika.[28] Risikomodellen vi vil redegjøre for er publisert i NIST sin veileder "Guide for Conducting Risk Assessment". Denne risikomodellen er trukket frem av Digitaliseringsdirektoratet som et eksempel på hva slags risikomodell som kan tas i bruk når man jobber med risiko.[29] Nedenfor, i figur 3 viser vi til risikomodellen som NIST har laget i deres veileder for risikovurdering. I figuren er alle risikofaktorer representert av firkanter og hvite piler som er med på å avgjøre størrelsen på

[27] Digitaliseringsdirektoratet (2018)
[28] NIST (2018)
[29] Digitaliseringsdirektoratet "Hva er risiko?" nr. 3 risikomodeller

risiko. I risikomodellen til NIST nedenfor har risikofaktorene blitt dekomponert til mer detaljerte egenskaper.[30] Vi vil redegjøre risikofaktorene modellen består av under figuren.



Figur 3 NIST sin risikomodell

I NIST sin risikomodell snakker man om trusselfaktoren som omhandler hendelser eller scenarioer med potensielle konsekvenser. I modellen skiller man mellom trusselkilde og trusselhendelse. Trusselkilde er intensjonen eller metoden målrettet mot å utnytte en sårbarhet, som for eksempel et fiendtlig angrep. Det kan også være en situasjon som ved et uhell kan utnytte en sårbarhet. En trusselhendelse er scenarioer eller en serie aktiviteter med potensielle konsekvenser. Et eksempel kan være et datainnbrudd som resulterer i at personopplysninger urettmessig endres eller slettes. I modellen bruker man også sannsynlighetsfaktoren som i likhet med trussel er delt inn i to faktorer. Den ene er sannsynlighet for at hendelsen vil finne sted, den andre er sannsynligheten for at de potensielle konsekvensene av hendelsen vil inntreffe. Etter å ha vurdert sannsynligheten ut fra disse to faktorene separat vil man gjøre en samlet vurdering av sannsynlighet ved å kombinere resultatene fra begge vurderingene.[31]

For å vurdere sannsynligheten for at de potensielle konsekvensene en hendelse medfører vil inntreffe, bruker risikomodellen tre faktorer. Dette omfatter sårbarheter som finnes enten i et

[30] NIST (2012) avsnitt 2.3.1 side 8
[31] NIST (2012) avsnitt 2.3.1 side 8 - 11

informasjonssystem, sikkerhetsprosedyrer, maskinvare, osv.[32] Videre har man disponerende forhold som handler om betingelser innen en organisasjon som kan minimere eller øke sannsynligheten for at konsekvensene en trusselhendelse medfører, materialiseres. For eksempel vil et informasjonssystem uten ekstern nettverkskobling redusere sannsynligheten for å bli utsatt for et nettverksbasert angrep.[33] Den siste faktoren innebærer at en tar i betraktning hvor effektive eksisterende og planlagte kontrolltiltak vil være dersom en trusselhendelse skulle forekomme. Alle disse faktorene er med på å avgjøre alvorlighetsgraden av konsekvensene dersom de skulle finne sted.[34]

Det neste elementet av risikomodellen er konsekvensene, altså resultatene av en trusselhendelse. Alvorlighetsgraden av konsekvensene avhenger av skadens omfang som forventes når en trusselhendelse finner sted. Størrelsen på skade kan måles på ulike måter. For eksempel kan uautorisert tilgang til hundretalls personers helseopplysninger medføre stort skadeomfang ved at det trolig vil resultere i tap av omdømme, økonomisk tap, tap av tillit, osv. Hvis det derimot er snakk om én person sitt personnummer som ble gjort kjent for uvedkommende, kan alvorlighetsgraden bli vurdert som lavere.[35]

2.2.2.3 Diskusjon av risikomodellene

Ovenfor har vi gått gjennom to ulike risikomodeller for å vurdere og forstå risiko. Hvordan en virksomhet velger å benytte seg av slike modeller varierer, men utgangspunktet vil uansett være å kunne identifisere og vurdere risiko knyttet til hendelser og aktiviteter. Den første av de to risikomodellene, altså risikomatrisen, benyttes ofte hos norske virksomheter og særlig i offentlig forvaltning da den er anbefalt av Digitaliseringsdirektoratet.[36] Vi har også redegjort for NIST sin risikomodell som er mer kompleks enn risikomatrisen, da den bruker flere faktorer for å vurdere risiko.

Risikomodellene baserer seg på de samme elementene som ble gjennomgått i avsnitt 2.2.1 ovenfor: hendelse, konsekvens, sannsynlighets- og alvorlighetsgrad og risikokilder. Allikevel

[32] NIST (2012) avsnitt 2.3.1 side 9
[33] NIST (2012) avsnitt 2.3.1 side 10
[34] NIST (2012) avsnitt 2.3.1 side 9
[35] NIST (2012) avsnitt 2.3.1 side 11
[36]Digitaliseringsdirektoratet “Hva er risiko?”

ser man at NIST modellen i stor grad vil fungere som rettesnor for hvordan man skal gå frem og hva man skal ta hensyn til under arbeidet med risikovurderingen. Risikomatrisen, derimot, er mer som et skjema der man fyller ut de ulike feltene og kommer frem til et resultat. En av grunnene til at vi mener risikomatrisen er praktisk å bruke er fordi her benyttes en skala for å vurdere størrelsen på risiko. I risikomodellen til NIST bruker man ikke skala men to ulike sannsynlighetsfaktorer. Dette bidrar også til at NIST modellen fremstår som mer kompleks og mindre "rett frem" enn risikomatrisen. En likhet vil derimot være at ved beregning av sannsynlighet vil man kartlegge trusler man har vært eller særlig er utsatt for, for å avgjøre sannsynlighetsgraden av risiko.

Når det kommer til hvordan vi kan benytte modellene for å definere risikobegrepet tar vi, som nevnt i tekstavsnittet rett ovenfor, utgangspunkt i risikoelementene. Disse elementene benyttes på ulik måte for å vurdere risiko. Risikomatrisen har et fast oppsett som fastsetter at risiko plasseres etter konsekvensens alvorlighetsgrad, samt sannsynligheten for at den inntreffer. NIST modellen er på den andre siden mer åpen for at man kan gjøre egne vurderinger og trekker i tillegg inn flere hensyn. Hensyn som i NIST sin modell trekkes frem er blant annet sårbarhet og hvilke eksisterende forhold som kan gjøre at denne sårbarheten øker. Begge modellene gir en oversikt over hva som kan og bør vurderes i forbindelse med å identifisere, beregne og håndtere risiko.

En annen forskjell mellom risikomodellene ut i fra vår vurdering, er at NIST sin risikomodell er i større grad rettet mot risiko for virksomheter. Dette innebærer at det i NIST sin veileder legges større vekt på hendelser som kan medføre konsekvenser for virksomhetene. Vi vil imidlertid argumentere for at det ikke er noe i veien for å bruke denne risikomodellen i risikovurdering av personvernkonsekvenser. Grunnen til dette er at det i modellen tas hensyn til de samme momentene som lovgiver har fastsatt i fortalepunkt 90, se avsnitt 2.2.1 ovenfor. Som påpekt i avsnitt 2.2.1 har ikke lovgiver fastsatt krav til hvordan risiko skal beregnes, i tillegg har Personvernrådet i sine retningslinjer angitt at risikoprosesser hvor momentene i forordningen er tatt i betraktning, kan tas i bruk.

2.2.2.4 Videre om risikobegrepet

Videre vil vi benytte det vi har redegjort for og diskutert i avsnittene 2.1 til 2.2 når vi analyserer de videre kravene i PVF artikkel 35. Ut i fra det vi har diskutert ovenfor kan vi trekke frem en forståelse av at risiko er et resultat av konsekvensen(e) av en hendelse med tilhørende sannsynlighet- og alvorlighetsgrad. Dermed vil en enkel fremstilling av risikoelementene kunne illustreres slik som i figur 4 nedenfor.

Figur 4: Enkel fremstilling av risikoberegning[37]

I figur 4 går vi ut fra en forenklet vurdering av en hendelse som kan medføre en konsekvens. Sannsynlighetsgraden (sannsynligheten for at hendelsen inntreffer) blir i figuren ganget med konsekvens (og alvorlighetsgrad den medfører) og resulterer i risiko. Slik kan man se for seg at man kan beregne hvor høy risiko en hendelse medfører. Dette er hovedelementene i hva risikobegrepet innebærer og er en konsentrert fremstilling av momentene i en risikovurdering.

Før vi går dypere inn på innholdet av kravene i PVF artikkel 35 vil vi først sette bestemmelsen i sammenheng med andre bestemmelser i forordningen. Dette mener vi er nødvendig for å kunne få bedre forståelse for kravene i artikkelen. Særlig gjelder dette ved forståelse av risiko og hvordan man skal gå frem for å ta stilling til om man er rettslig forpliktet til å gjøre en konsekvensvurdering eller ikke, jf. artikkel 35 (1).

2.3 Ansvarsprinsippet og krav om risikovurderinger

Som nevnt i avsnitt 1.1 ovenfor har lovgiver lagt til grunn en proaktiv tilnærming til etterlevelse av personvernforordningen ved fastsettelsen av ansvarsprinsippet, jf. PVF artikkel 5 (2). Ansvarsprinsippet handler om at den behandlingsansvarlige har ansvaret for og skal kunne

[37] PECB kursmateriale for ISO27001 foundation sertifisering

påvise at behandlingen overholder personvernprinsippene i PVF artikkel 5 (1) (a - f). I personvernforordningen er det en rekke bestemmelser hvor ansvarsprinsippet gjennomføres. Nedenfor vil vi gjennomgå de bestemmelsene som gjennomfører prinsippet hvor den behandlingsansvarlige er pliktet til å risikovurdere. Vi har valgt å redegjøre for artiklene og innholdet i dem samlet fordi bestemmelsene har mye av det samme innholdet. Dette gjelder spesielt for hva som skal vurderes for om det foreligger risiko og vurdering av hvilke tiltak som skal treffes. Bestemmelsene vi vil trekke frem er PVF artikkel 24 (1) om den behandlingsansvarliges ansvar. I denne bestemmelsen er den behandlingsansvarlige pålagt å treffe egnede tiltak for å sikre og påvise at behandlingen skjer i henhold til personvernforordningen. Neste bestemmelse er artikkel 25 (1) om innebygd personvern og personvern som standardinnstilling. I denne bestemmelsen står det skrevet at den behandlingsansvarlige skal treffe tiltak med sikte på å gjennomføre personvernprinsippene og for å integrere de nødvendige garantier i selve behandlingsopplegget. Formålet med denne bestemmelsen er at den behandlingsansvarlige skal vurdere personvernspørsmål allerede før og under utvikling (eller anskaffelse) av systemer eller tjenester som benyttes til å behandle personopplysninger.[38] Den siste bestemmelsen vi vil trekke frem som må ses i sammenheng med plikten til å gjøre en konsekvensvurdering etter PVF 35 (1), er PVF artikkel 32 om sikkerhet ved behandling av personopplysninger. I denne bestemmelsen skal den behandlingsansvarlige treffe tiltak med sikte på å oppnå et egnet sikkerhetsnivå.[39]

Felles for disse bestemmelsene er vurderingsmomentene som skal tas i betraktning ved vurdering av hvilke tiltak som er egnede. Disse omfatter behandlingens art, omfang, formål og sammenhengen den utføres i. I tillegg til dette skal man ta hensyn til "risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter". I PVF artikkel 25 (1) og 32 (1) skal man også ta hensyn til den tekniske utviklingen og gjennomføringskostnadene. Lovgiver har med dette lagt til grunn en risikobasert tilnærming til etterlevelse av personvernforordningen, ettersom risiko er et av de sentrale momentene som skal tas til vurdering vedrørende hvilke tiltak som er egnede. Koplingen mellom risiko og etterlevelse fremheves særlig i fortalepunkt 78 i forordningen. Her har lovgiver fastsatt at vern

[38] Skullerud m.fl. (2018) side 175
[39] Skullerud m.fl. (2018) side 200

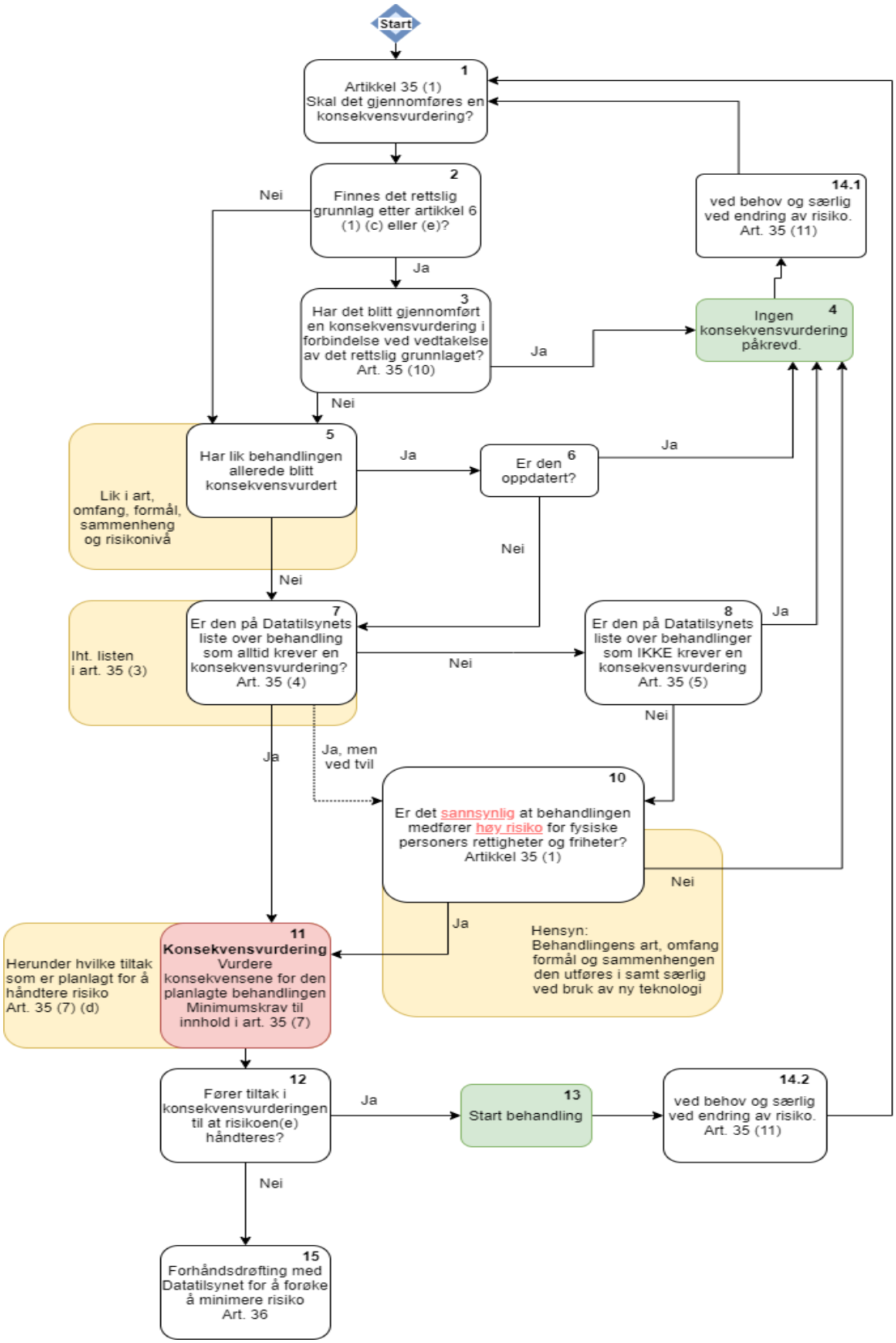
av fysiske personers rettigheter og friheter krever at man treffer egnede organisatoriske og tekniske tiltak for å sikre at kravene i forordningen oppfylles. I vurderingen vedrørende hvilke tiltak som er egnede skal man foreta en forholdsmessighetsvurdering. Altså at tiltakene man har truffet eller planlegger å treffe skal være forholdsmessige til risikoene behandlingen medfører. Dette kan tolkes slik at jo høyere risiko det er snakk om, jo mer omfattende tiltak må en treffe for å håndtere risikoene.[40] Det er ikke fastsatt noen form- eller innholdskrav til vurderingen av risiko etter artikkel 32 (2). Den behandlingsansvarlige må selv vurdere hvordan risikovurderingen skal gjennomføres og omfanget av denne.[41] I artikkel 32 (2) har lovgiver skrevet risikomomenter det særlig skal tas hensyn til ved vurdering av hva som kan sies å være et egnet sikkerhetsnivå. Dette omfatter for eksempel utilsiktet eller ulovlig tilintetgjøring eller tap av personopplysninger. I følge Skullerud, m.fl. (2018) har lovgiver i PVF artikkel 5 (2) fastsatt et implisitt krav om at den behandlingsansvarlige må dokumentere de vurderingene og valgene rundt behandlingen vedkommende har gjort. For eksempel trekker de frem PVF artikkel 5 (1) (f) vedrørende prinsippet om "konfidensialitet og integritet". Etter dette prinsippet skal man sikre at det foreligger tilstrekkelig sikkerhet for personopplysningene som behandles, ved bruk av egnede tekniske og organisatoriske tiltak. Etter PVF artikkel 5 (2) skal den behandlingsansvarlige derfor kunne påvise at vedkommende har truffet egnede tiltak for å oppnå et egnet sikkerhetsnivå. Derfor foreligger det et implisitt krav til at risikovurderinger skal være dokumenterte og etterprøvbare.[42]

Bestemmelsene i forordningens artikkel 24, 25 og 32 kommer til anvendelse for enhver behandling. Det betyr at bestemmelsene ikke avhenger av sannsynlighets- og alvorlighetsgraden til risikoene som behandlingen medfører for fysiske personers rettigheter og friheter.[43] I følge Personvernrådets retningslinjer for vurdering av personvernkonsekvenser bør plikten til å konsekvensvurdere etter artikkel 35 forstås opp mot den generelle plikten den behandlingsansvarlige har til å håndtere risiko etter artikkel 24 (1), 25 (1) og 32.[44] I neste avsnitt vil vi gjennomgå kravene i PVF artikkel 35 på et overordnet nivå.

[40] Skullerud m.fl. (2018) side 169
[41] Skullerud m.fl. (2018) side 204
[42] Skullerud m.fl. (2018) side 204
[43] Skullerud m.fl. (2018) side 175
[44] WP29 (2017) side 6

2.4 Kravene i PVF artikkel 35 på et overordnet nivå

For å redegjøre for sammenhengen med de øvrige kravene i PVF artikkel 35 har vi laget figur 5 nedenfor som er et flytdiagram som illustrerer hele prosessen på et overordnet nivå. Dette mener vi er hensiktsmessig for å sette kravene i artikkelen i kontekst. En annen grunn til at vi har valgt å lage et flytdiagram er for å vise hvordan bestemmelsene henger sammen og for å tydeliggjøre rekkefølgen og relasjonen mellom dem. Vi har altså tatt utgangspunkt i bestemmelsen og laget en prosess for gjennomføringen av en konsekvensvurdering. Vi forklarer alle elementene i flytdiagrammet under selve diagrammet.


Start
1
Artikkel 35 (1)
Skal det gjennomføres en konsekvensvurdering?
2
Finnes det rettslig grunnlag etter artikkel 6 (1) (c) eller (e)?
Nei
Ja
3
Har det blitt gjennomført en konsekvensvurdering i forbindelse ved vedtakelse av det rettslig grunnlaget?
Art. 35 (10)
Ja
4
Ingen konsekvensvurdering påkrevd.
14.1
ved behov og særlig ved endring av risiko.
Art. 35 (11)
Nei
5
Har lik behandlingen allerede blitt konsekvensvurdert
Ja
6
Er den oppdatert?
Ja
Nei
Lik i art, omfang, formål, sammenheng og risikonivå
Nei
7
Er den på Datatilsynets liste over behandling som alltid krever en konsekvensvurdering?
Art. 35 (4)
Nei
8
Er den på Datatilsynets liste over behandlinger som IKKE krever en konsekvensvurdering
Art. 35 (5)
Ja
Nei
Iht. listen i art. 35 (3)
Ja
Ja, men ved tvil
10
Er det sannsynlig at behandlingen medfører høy risiko for fysiske personers rettigheter og friheter?
Artikkel 35 (1)
Nei
Ja
Hensyn:
Behandlingens art, omfang formål og sammenhengen den utføres i samt særlig ved bruk av ny teknologi
Herunder hvilke tiltak som er planlagt for å håndtere risiko
Art. 35 (7) (d)
11
Konsekvensvurdering
Vurdere konsekvensene for den planlagte behandlingen
Minimumskrav til innhold i art. 35 (7)
12
Fører tiltak i konsekvensvurderingen til at risikoen(e) håndteres?
Ja
13
Start behandling
14.2
ved behov og særlig ved endring av risiko.
Art. 35 (11)
Nei
15
Forhåndsdrøfting med Datatilsynet for å forøke å minimere risiko
Art. 36

Figur 5: Flyten i artikkel 35

For å forklare flytdiagrammet på en så oversiktlig måte som mulig har vi nummerert hver boks. Vi vil begynne med boksen helt øverst fra boks 1 og ned til boks 15. Vi har valgt å gjennomgå de ulike delene av diagrammet punktvis.

Det første stadiet

I boks 1 er fasen hvor man skal begynne å vurdere om det er nødvendig å gjøre en konsekvensvurdering eller ikke. For å undersøke dette må man se hva som står skrevet i PVF artikkel 35 (1) hvor plikten til å gjøre en konsekvensvurdering er fastsatt, se avsnitt 2.5 nedenfor. Dette stadiet vil man komme tilbake til som følge av at risikobildet kan endre seg over tid, på grunn av at deler eller hele behandlingsopplegget endres.

Er unntaket etter PVF artikkel 35 (10) aktuelt?

Før man begynner å evaluere om behandlingen oppfyller kriteriene bør man først undersøke hva det rettslige grunnlaget for behandlingen er. I boks 2 tar man stilling til om behandlingen av personopplysninger i henhold til PVF artikkel 6 (1) (c) eller (e) har et rettslig grunnlag i unionsretten eller i medlemsstaten som den behandlingsansvarlige er underlagt, og regulerer hele eller de spesifikke behandlingsaktivitetene. Dersom dette er tilfelle bør man undersøke om unntaket i PVF artikkel 35 (10) er aktuelt. I boks 3 tar man stilling til om det er gjort en vurdering av personvernkonsekvenser som del av lovprosessen ved vedtakelsen av de aktuelle lovreglene. Behandlinger der dette er tilfellet vil ikke medføre et krav om gjennomføring av konsekvensvurdering, med mindre medlemsstatene har fastsatt at det likevel skal gjennomføres.

Har det blitt gjort en konsekvensvurdering for en lignende behandling tidligere?

Hvis det ikke har blitt gjennomført en konsekvensvurdering som del av vedtakelsen av lovreglene, må man ta stilling til om man har gjort en konsekvensvurdering på et tidligere tidspunkt. Dette er illustrert i boks 5 hvor man undersøker om det allerede har blitt gjennomført en konsekvensvurdering på samme behandlingsaktivitet eller en behandling som er svært lik. I følge Datatilsynet er et av formålene med en vurdering av personvernkonsekvenser å sikre

systematisk undersøkelse av *nye* tilfeller som medfører høy risiko for fysiske personers rettigheter og friheter. Dermed er det ikke grunn til å gjennomføre en slik vurdering dersom det ikke er snakk om et nytt tilfelle. Ved vurdering om den planlagte behandlingen er lik en tidligere behandling skal man særlig ta hensyn til behandlingens art, omfang, formål, sammenhengen den utføres i og risikonivået.[45] Hvis man har gjort en vurdering av personvernkonsekvenser for samme, eller i stor grad lik behandling, må man vurdere om resultatene av den er tilstrekkelig oppdaterte. Dette vises i boks 6 hvor man må ta stilling til om man kan bruke den tidligere vurderingen til å evaluere risiko og treffe egnede tiltak for den planlagte behandlingen.

Medfører den planlagte behandlingen høy risiko?

Dersom man kommer frem til at man ikke kan bruke resultatene fra en tidligere vurdering eller at det ikke har blitt utført en konsekvensvurdering tidligere, må man undersøke nærmere om behandlingen medfører høy risiko. Etter PVF artikkel 35 (4) er tilsynsmyndigheten i det enkelte medlemsland pålagt å publisere en liste over behandlingsaktiviteter, hvor man må gjøre en konsekvensvurdering. Dette er altså behandlingsaktiviteter tilsynsmyndigheten har vurdert medfører høy risiko for fysiske personers rettigheter og friheter. Behandlingsaktivitetene i listen er utarbeidet på bakgrunn av kriteriene lovgiver har fastsatt i personvernforordningen, for eksempel PVF artikkel 35 (3) (a-c) og Personvernrådets liste i deres retningslinjer for vurdering av personvernkonsekvenser. Den behandlingsansvarlige må undersøke om den tiltenkte behandlingen faller inn under ett eller flere typetilfeller nevnt i personvernforordningen eller tilsynsmyndighetens liste. Et eksempel på en behandlingsaktivitet fra listen er kameraovervåkning i skoler eller barnehager under åpningstider.

Hvis behandlingen man planlegger å iverksette oppfyller to eller flere av kriteriene på tilsynsmyndighetens liste, kreves det at man gjør en konsekvensvurdering. Dette er illustrert i boks 7 hvor man først undersøker listen, for så å vurdere om den tiltenkte behandlingen oppfyller noen av behandlingsaktivitetene i PVF artikkel 35 (3) (a-c). Datatilsynet anbefaler å undersøke listene de har publisert før man starter en behandlingsaktivitet for å komme frem til om behandlingen sannsynligvis medfører høy risiko for fysiske personers rettigheter og

[45] Datatilsynet (2019)

friheter.[46] På Datatilsynets nettside påpekes det at listen over behandlingsaktivitetene som krever en konsekvensvurdering ikke er uttømmende. Det utelukkes derfor ikke at en planlagt behandling kan medføre høy risiko selv om kriteriene i listen eller i artikkel 35 (3) (a-c) ikke skulle være ansett som oppfylt. I tillegg til å undersøke kriteriene for om det foreligger høy risiko kan det også være hensiktsmessig å undersøke om behandlingen oppfyller noen av kriteriene på listen Datatilsynet har publisert for når det ikke foreligger høy risiko. Dette følger at PVF artikkel 35 (5) hvor tilsynsmyndigheten kan publisere en liste over behandlingsaktiviteter hvor man ikke trenger å gjøre en konsekvensvurdering. Dette er illustrert i boks 8.

I noen tilfeller kan det være at behandlingen ikke er oppført, eller er oppført delvis, på listene nevnt ovenfor. Det kan også være tilfeller hvor noen av kriteriene for høy risiko er oppfylt, men at det likevel kan foreligge tvil om man faktisk er rettslig forpliktet. Slik kan for eksempel være tilfelle hvis den planlagte behandlingen oppfyller kun ett kriterium, men basert på andre hensyn er det likevel tvil om det foreligger høy risiko. Denne situasjonen er illustrert i boks 10. I denne boksen har vi vist til vurderingsmomentene i PVF artikkel 35 (1) hvor man da må vurdere risiko. Dette gjøres ut fra behandlingens art, omfang, formål og kontekst, samt bruk av ny teknologi, se avsnitt 2.5 nedenfor hvor vi har gjennomgått disse vurderingsmomentene.

Gjennomføring av konsekvensvurderingen

Dersom det foreligger høy risiko som følge av vurderinger illustrert i boks 7 eller 10, vil neste steg være å iverksette selve konsekvensvurderingen. Dette er illustrert i boks 11 hvor man må oppfylle kravene etter PVF artikkel 35 (7) (a-d). I denne bestemmelsen har lovgiver listet opp minimumskravene til hva en vurdering av personvernkonsekvenser skal inneholde. I Personvernrådet sine retningslinjer for vurdering av personvernkonsekvenser er det lagt til et vedlegg med kriterier. Disse kriteriene bør den behandlingsansvarlige benytte for å vurdere om en konsekvensvurdering, eller metodikken for å gjennomføre konsekvensvurderingen, er omfattende nok til å etterleve kravene i personvernforordningen. Dette er generelle kriterier for de fire fasene i artikkel 35 (7) (a-d).[47] Nedenfor vil vi gjennomgå kravene i artikkel 35 (7) (a-d)

[46] Datatilsynet (2019)
[47] WP29 (2017) side 22

og trekke frem eksempler på kriterier Personvernrådet mener konsekvensvurderingen bør omfatte i hver fase.

1. En systematisk beskrivelse av behandlingsaktivitetene og formålet med behandlingen. Dersom det er relevant skal man også beskrive hvilke interesser behandlingen bidrar til for den behandlingsansvarlige, jf. artikkel 35 (7) (a). Ved beskrivelsen av behandlingsaktivitetene har Personvernrådet trukket frem at man bør beskrive behandlingens art, omfang, formål og kontekst. Disse momentene har lovgiver fastsatt i fortalepunkt 90 skal brukes til å vurdere graden av risiko. Andre kriterier Personvernrådet har trukket frem er beskrivelse av kategorier av personopplysninger som inngår i behandlingen, lagringstiden og mottakere.[48] Hvor omfattende og detaljert en konsekvensvurdering skal være når det gjelder beskrivelsen av behandlingsaktivitetene og formål, må vurderes ut fra det konkrete tilfellet. En generell hovedregel er at hvis det behandles store mengder personopplysninger, og/eller om behandlingen er relativt ny og/eller særlig inngripende bør konsekvensvurderingen være enda mer omfattende og grundig.[49]
2. Den behandlingsansvarlige skal dokumentere at behandlingsaktivitetene og kategoriene av personopplysningene er nødvendige å behandle for å oppfylle formålet. I tillegg må det også dokumenteres at gevinstene for den behandlingsansvarlige eller samfunnet er proporsjonalt i forhold til krenkelser av personvernet behandlingen medfører for den registrerte, jf. artikkel 35 (7) (b).[50] For å vurdere om tiltakene man planlegger å treffe bidrar til at behandlingen er nødvendig og proporsjonal har Personvernrådet fastsatt at man skal vurdere behandlingen opp mot personvernprinsippene i PVF artikkel 5 (1) (a-e). I tillegg til dette skal man også vurdere i hvilken grad de registrertes rettigheter etter artikkel 12 til 22 er ivaretatt ved behandlingen.[51]
3. Videre skal konsekvensvurderingen inneholde en vurdering av risiko for de registrertes rettigheter og friheter. Som påpekt i avsnitt 2.2.1 ovenfor har ikke lovgiver fastsatt krav

[48] WP29 (2017) side 22
[49] Skullerud m.fl. (2018) side 220
[50] Skullerud m.fl. (2018) side 220
[51] WP29 2017) side 22

til hvordan selve risikovurderingen skal utføres.[52] Personvernrådet har skrevet noen kriterier som bør brukes når man gjennomfører risikovurderingen. Kriteriene i denne fasen er laget ut i fra det lovgiver har fastsatt i fortalepunkt 84 og 90. I fortalepunkt 84 skal man vurdere risikoenes opprinnelse, art, særegenhet og alvorlighetsgrad. I følge Personvernrådet innebærer dette blant annet å identifisere trusler som fører til hendelser med tilhørende konsekvenser for fysiske personers rettigheter og friheter. I samsvar med fortalepunkt 90 skal også kildene til risikoene identifiseres og sannsynlighets- og alvorlighetsgrad skal beregnes.[53]

4. Til slutt skal konsekvensvurderingen inneholde planlagte tiltak for å håndtere de identifiserte risikoene. Dette kan være snakk om rene sikkerhetstiltak som for eksempel kryptering av personopplysninger for å bevare konfidensialitet. Andre tiltak kan omfatte å kontrollere at personopplysningene bare behandles for det fastsatte formålet med behandlingen eller at behandlingen ikke skal gjennomføres.[54] I denne fasen har ikke Personvernrådet etablert mange kriterier annet enn å vise til fortalepunkt 90 hvor lovgiver har fastsatt at tiltakene skal begrense risiko, sikre vern av personopplysninger og påvise etterlevelse av personvernforordningen.[55] Dette er illustrert i boks 12 hvor man må foreta en vurdering om tiltakene bidrar til å håndtere risiko på en tilstrekkelig måte. Dersom man kommer frem til at tiltakene minimerer risikonivået til hva som er ansett som akseptabel risiko, bør dette dokumenteres. Det eksisterer ikke noen eksplisitte krav om at konsekvensvurdering skal dokumenteres skriftlig, men som nevnt i avsnitt 2.3 ovenfor vil det være den mest praktiske måten for den behandlingsansvarlige å påvise etterlevelse av personvernregelverket.

Datatilsynet har på sin nettside publisert en sjekkliste som er laget ut fra kriteriene i veilederen til Personvernrådet. I motsetning til Personvernrådet sine lister med kriterier som skal vurderes

[52] Skullerud m.fl (2018) side 220
[53] WP29 (2017) side 22
[54] Skullerud m.fl. (2018) side 220-221
[55] WP29 (2017) side 22

for om en konsekvensvurdering er i overensstemmelse personvernforordningen, er Datatilsynets sjekkliste enda mer omfattende og detaljert.[56]

Etter PVF artikkel 35 (2) skal den behandlingsansvarlige rådføre seg med personvernombudet dersom dette er utpekt på et tidligere tidspunkt. Et personvernombud er en person i en virksomhet som skal gi råd om hvordan man kan best ivareta personverninteressene rundt behandlingen.[28] I tillegg til plikten en behandlingsansvarlig har etter artikkel 35 (2) skal personvernombudet gi råd og kontrollere gjennomføringen av konsekvensvurderingen på anmodning av den behandlingsansvarlige etter PVF artikkel 39 (1) (c). Personvernombudet skal da kontrollere at konsekvensvurderingen blir gjennomført i henhold til kravene i PVF artikkel 35. Dette omfatter blant annet risikovurdering etter PVF artikkel 35 (7) (c). I tillegg til involveringen av personvernombudet følger det av PVF artikkel 35 (9) at man skal innhente de registrerte (eller en representant for de registrerte) sitt synspunkt på den planlagte behandlingen. Denne plikten gjelder bare i de tilfeller det er relevant, og uten at det berører vernet av de kommersielle eller allmenne interesser eller sikkerheten ved behandlingsaktivitetene. Hvis en virksomhet er eksempel planlegger å sette opp et overvåkningskamera på arbeidsplassen vil typisk være et tilfelle hvor man på forhånd kan få oversikt over hvem som er de registrerte. I en slik situasjon vil man kunne innhente de ansattes eller deres tillitsvalgtes synspunkter på montering av overvåkningskamera. I dette eksempelet må man også se arbeidsmiljølovens bestemmelser om kontrolltiltak på arbeidsplassen i sammenheng med artikkel 35 (9), jf. arbeidsmiljøloven § 9-2.[57] I andre situasjoner kan det være utfordrende å få full oversikt over hvem de registrerte er.

Forhåndsdrøftelse med tilsynsmyndigheten

Dersom man ut fra konsekvensvurderingen ikke har truffet eller er i stand til å treffe egnede tiltak for å håndtere risikoene behandlingen medfører, skal man gjøre en forhåndsdrøftelse med Datatilsynet, etter PVF artikkel 36 (1), dette er illustrert i boks 15. I følge artikkel 36 (2) skal Datatilsynet dersom de kommer frem til at den planlagte behandlingen er i strid med

[56] Datatilsynet “Sjekkliste for vurdering av personvernkonsekvenser (DPIA)” (?)
[57] Skullerud m.fl. (2018) side 221

personvernforordningen og hvor det er relevant, gi skriftlig råd der den behandlingsansvarlige har gjennomført risikovurderinger som er ansett som ikke tilstrekkelige. I tillegg til dette kan Datatilsynet også bruke alle sine fullmakter i henhold til PVF artikkel 58. Dette innebærer at dersom tilsynsmyndigheten kommer frem til at behandlingen vil være i strid med personvernforordningen, vil de kunne åpne en kontrollsak og kan dermed både endre og stoppe den planlagte behandlingen.[58]

En kontinuerlig prosess

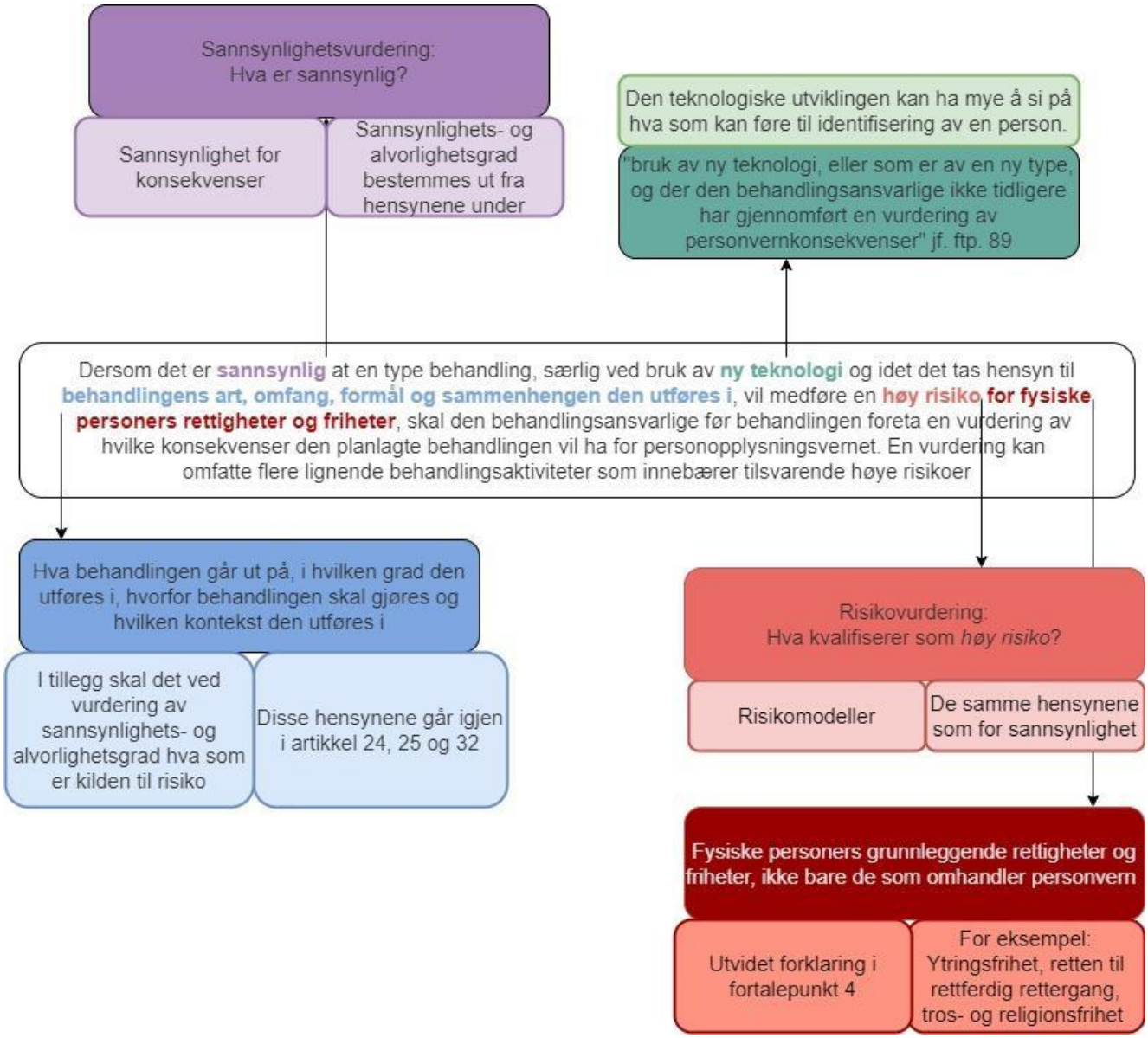
Boks 14.1 og 14.2 illustrerer at arbeidet med konsekvensvurderingen er en kontinuerlig prosess. I PVF artikkel 35 (11) skal den behandlingsansvarlige ved behov evaluere om behandlingen skjer i henhold til konsekvensvurderingen. Gjennomgåelsen bør særlig gjøres i tilfeller hvor risikobildet endrer seg. Faktorer som kan medføre endring av risiko er for eksempel hvis organisatoriske rutiner endres ved at avdelinger slås sammen og ansvarsforholdene endres. Et annet eksempel kan være at man velger å ta i bruk ny teknologi hvor man ikke har gjort en konsekvensvurdering tidligere. Derfor må vurdering av personvernkonsekvenser gjøres kontinuerlig gjennom hele behandlingens levetid. Dette er forsøkt illustrert ved at alle boksene peker tilbake mot boks 1. I neste avsnitt vil vi gå grundigere gjennom boks 10 vedrørende vurderingsmomentene i artikkel 35 (1).

2.5 Kriterier for vurdering av risiko i PVF artikkel 35

For å gjennomgå hvilke kriterier som er skrevet ned i PVF artikkel 35 og i personvernforordningen ved vurdering av risiko vil vi ta utgangspunkt i hva som står skrevet i selve artikkelen. Her oppgis kravet for om en er rettslig forpliktet til å gjøre en vurdering av personvernkonsekvenser. I gjennomgangen vil vi bruke vår forståelse av elementene risiko består av, se avsnitt 2.2.1 ovenfor for å trekke frem kriteriene lovgiver har skrevet ned i personvernforordningen. Vi går gjennom kriteriene fordi det er disse den behandlingsansvarlige må ta stilling til ved behandlingen. De brukes også som veiledning for å avgjøre om vedkommende er rettslig forpliktet til å gjøre en konsekvensvurdering. For å

[58] Skullerud m.fl. (2018) side 221

gjennomgå kriteriene har vi nedenfor laget figur 6 hvor vurderingsmomentene er fremhevet. Vi har lagd denne figuren for å gi et mer oversiktelig bilde over hvor vurderingsmomentene er skrevet ned og hva de omhandler.



Figur 6: Personvernforordningen artikkel 35 (1)

I figur 6 ovenfor har vi plassert innholdet av PVF artikkel 35 (1) i rektangelet i midten av figuren. I lovteksten har vi fremhevet vurderingsmomentene i selve lovteksten ved bruk av ulike farger. Fra hvert vurderingsmoment som er fargelagt er det en pil som peker ut mot bokser i samme farge. I disse boksene har vi skrevet noen utdypninger vedrørende hva vilkårene handler om. For å forklare figuren ovenfor på en oversiktlig og grundig måte vil vi begynne med å forklare boksene over selve lovteksten, for så å punktvis forklare delene under.

Sannsynlighetsvurdering

Øverst til venstre i figur 6 har vi trukket frem "sannsynlighet" som det første vurderingsmomentet ved å farge det i fiolett, og med en pil som peker mot de lilla boksene ovenfor lovteksten. Sannsynlighet i denne sammenhengen går som nevnt ut på å vurdere hvor sannsynlig det er at en uønsket hendelse vil inntreffe. Det finnes flere måter å vurdere sannsynlighet på. I risikomatrisen tildeles hendelsene et tall fra 1 til 5, se 2.2.2.1 ovenfor. Det gjøres for å vise hvor sannsynlig det er at akkurat den hendelsen inntreffer, hvor 1 er lite sannsynlig og 5 er nesten garantert.[59] Ved avgjørelsen om en behandling sannsynligvis vil medføre høy risiko for fysiske personers rettigheter og friheter, må det altså vurderes om det er sannsynlig at en uønsket hendelse med store konsekvenser vil skje. Sannsynlighet er som nevnt et av vurderingsmomentene for å beregne risiko. Økt sannsynlighet er gjerne også økt risiko, men dersom konsekvensen er ubetydelig, er ikke sannsynlighet alene nok for at det foreligger høy risiko. Sannsynlighet vurderes ut fra hensynene som legges frem i artikkel 35 (1) og innebærer at man må se på behandlingens art, omfang, formål og sammenhengen den utføres i. Vi vil komme nærmere inn på disse hensynene nedenfor.

Ny teknologi

Bruk av ny teknologi har lovgiver skrevet ned som et moment for å vurdere om det foreligger høy risiko. Dette er illustrert i figur 6 ovenfor ved at vi har fargelagt "*ny teknologi"* i grønt, og pilen som peker opp mot de grønne boksene ovenfor lovteksten. I de grønne boksene har vi vist til hva som står skrevet i fortalepunkt 89 i personvernforordningen. I fortalepunkt 89 har lovgiver skrevet at ny teknologi kan åpne opp for nye muligheter ved behandling av

[59] Digitaliseringsdirektoratet (2018)

personopplysninger. Dette kan for eksempel omfatte større lagringskapasitet eller analysering av større mengder personopplysninger enn tidligere. Noe som spesielt kan føre med seg endringer er teknologi som tillater behandlingsansvarlig å sammenstille opplysninger. Dette kan resultere i at tidligere "anonym" data er blitt til personopplysninger. Ved bruk av ny teknologi kan det dermed foreligge uvisshet vedrørende om hvilke konsekvenser det kan ha for fysiske personers rettigheter og friheter, dette gjelder særlig dersom det ikke har blitt utført en konsekvensvurdering rundt anvendelse av slik teknologi tidligere.

Behandlingens art, omfang, formål og sammenhengen den utføres i

Videre i PVF artikkel 35 (1) følger det at man ved evaluering av risiko også skal ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i. Dette er fremhevet i figur 6 ved bruk av lyseblå farge. I hver av de tre blå boksene nederst til venstre har vi skrevet sammendrag for hva disse vurderingsmomentene omhandler. For det første er disse hensynene de samme lovgiver har fastsatt i en rekke andre bestemmelser, se avsnitt 2.3 ovenfor. Dette er illustrert i den blå boksen nederst til høyre. I fortalepunkt 76 er det presisert at risikoens sannsynlighets- og alvorlighetsgrad skal bedømmes ut i fra behandlingens art, omfang, formål og kontekst, illustrert i den blå boksen nederst til venstre.

Den siste blå boksen øverst, illustrerer et lite sammendrag av hva de ulike hensynene går ut på. På et overordnet nivå handler disse hensynene om at den behandlingsansvarlige må ha full oversikt over den tenkte behandlingen. Behandlingsansvarlig skal derfor vite hva slags type behandling det er snakk om, om det for eksempel er overvåking, behandling av e-postadresser i et kundeforhold eller behandling av helsedata for forskning. I tillegg skal de vite hvor stort omfanget av behandlingen er. For eksempel om det er snakk om kontinuerlig monitorering av en større gruppe mennesker, eller en engangsbehandling av adresse for å kunne sende en pakke som den registrerte har bestilt. Deretter skal det tas hensyn til formålet for behandlingen. Dette bygger opp under prinsippet om formålsbegrensning i artikkel 5 (1) (b) som handler om at den behandlingsansvarlige er nødt til å ha et uttrykkelig angitt og berettiget formål for behandling av personopplysninger. Formålet er det den behandlingsansvarlige ønsker å oppnå med den gitte behandlingen. Dette kan for eksempel være å ta en avgjørelse basert på innhentede personopplysninger eller kontrollformål. Til slutt kommer hensynet til

sammenhengen behandlingen utføres i, dette handler om at behandlingen skal stemme overens med hva som er forventningene til den registrerte med tanke på personvern. For eksempel har en pasient forventning om at en lege holder helsedata konfidensielt og ikke deler disse med en tredjepart.

Risiko for fysiske personers rettigheter og friheter

Hvis man legger til grunn vår forståelse av hvilke hovedelementer risiko består av, se øverst i avsnitt 2.2.1 ovenfor. Kan vi betrakte "risiko for fysiske personers rettigheter og friheter" som konsekvensene som kan oppstå dersom en uønsket hendelse inntreffer. Et eksempel på en slik uønsket hendelse kan være brudd på personopplysningssikkerheten, jf. PVF artikkel 4 (12) som utløser disse konsekvensene.[60] For å kunne identifisere risiko må en ha forståelse for hva som menes med "risiko for fysiske personers rettigheter og friheter", dette er illustrert i figur 6 ovenfor ved at vi har trukket frem sistnevnte i mørk rød farge. I følge Personvernrådet omfatter ikke dette bare konsekvenser for den enkeltes personopplysningsvern men også andre grunnleggende rettigheter og friheter. Dette fremgår av personvernforordningens fortalepunkt 4 hvor lovgiver har skrevet at retten til personopplysningsvern ikke er en absolutt rettighet og må ses i sammenheng med den funksjonen den har i samfunnet. Rett til personopplysningsvern må veies opp mot andre grunnleggende rettigheter. Derfor må man ikke bare vurdere risiko for den enkeltes personopplysningsvern men også andre rettigheter og friheter som bevegelsesfrihet, ytringsfrihet, retten til å ikke bli diskriminert, osv.[61]

Høy risiko

Den siste delen av figuren vi vil gjennomgå er de lyserød boksene nest nederst til høyre. I disse boksene har vi skrevet ned stikkord vedrørende hvordan man skal komme frem til om det foreligger høy risiko eller ikke. For å vurdere om det foreligger høy risiko kan man ikke bare vurdere hensynene skrevet ned i PVF artikkel 35 (1). Man må i tillegg se de andre kriteriene lovgiver har skrevet ned i forordningen. Nedenfor vil vi gjennomgå kriterier lovgiver har fastsattfor å vurdere om det foreligger risiko, deretter om det foreligger høy risiko.

[60] Gellert (2017) side 282
[61] Bieker m.fl.t (2016) side 25

I personvernforordningen fortalepunkt 75 har lovgiver oppgitt en ikke-uttømmende liste over kriterier for behandlingsaktiviteter og konsekvenser som medfører risiko for fysiske personers rettigheter og friheter. Disse kriteriene gir den enkelte veiledning for å evaluere om det foreligger risiko. I fortalepunktet er det også spesifisert at med konsekvenser for fysiske personer rettigheter og friheter omfattes både fysisk, materiell og ikke-materiell skade. Lovgiver har videre oppgitt en rekke eksempler på konsekvenser som øker risiko. Noen av eksemplene på slike kriterier er tap av omdømme, økonomisk tap, forskjellsbehandling, ID-tyveri, osv.

I tillegg til konsekvenskriterier har lovgiver også oppgitt behandlingsaktiviteter som øker risiko. Nedenfor har vi oppgitt punktvis noen av kriteriene og delt dem inn i art, omfang og formål:

- Art: Behandling av personopplysninger som faller inn under definisjonen av særlige kategorier, jf. PVF artikkel 9 (1) eller straffedommer og lovovertredelser, jf. artikkel 10.
- Formål: Evaluering av personlige aspekter for å kunne forutsi en ansatt sine arbeidsprestasjoner.
- Omfang: behandling av store mengde personopplysninger og/eller personopplysninger om et stort antall registrerte.[62]

Kriteriene vi har trukket frem ovenfor i dette avsnittet skal brukes til å evaluere om det foreligger risiko. Nedenfor skal vi redegjøre for kriteriene som skal brukes til å vurdere om det foreligger høy risiko.

I PVF artikkel 35 (3) (a-c) har lovgiver listet opp behandlingsaktiviteter hvor det vil være særlig nødvendig å gjøre en konsekvensvurdering. I artikkel 35 (3) (a) vil systematisk og omfattende behandling av personlige aspekter med sikte på å ta avgjørelser som kan ha rettslig virkning eller på annen lignende måte påvirke den fysiske personen, være en behandlingsaktivitet hvor man bør gjøre en konsekvensvurdering. Videre i bestemmelsen er også behandling av store mengder særlige kategorier av personopplysninger og/eller straffedommer omfattet, jf. artikkel

[62] Demetzou (2019) side 6

35 (3) (b), og systematisk overvåkning av offentlig område, jf. artikkel 35 (3) (c). I fortalepunkt 91 har lovgiver videre spesifisert kriteriene i artikkel 35 vedrørende om det foreligger høy risiko. For å trekke ut noen eksempler er det presisert nærmere hva som skal vurderes for om det foreligger behandling av personopplysninger i et stort omfang. Her har man pekt på momenter som antall registrerte, antall opplysninger og det geografiske virkeområdet. For eksempel om behandlingen foregår på et regionalt-, nasjonalt-, internasjonalt- eller globalt nivå. I tillegg er særlig behandlingsaktiviteter som hindrer eller gjør det vanskelig for den registrerte å utøve sine rettigheter trukket frem som eksempler der det kan være nærliggende å gjøre en konsekvensvurdering.

2.6 Samlet perspektiv

Ut fra det som er referert til og redegjort for ovenfor, er det vår vurdering at forståelsen av risiko i lys av personvernforordningen er sentralt ettersom det er et av hovedkriteriene for etterlevelse. Dersom man ikke har forståelse for hva høy risiko innebærer kan resultatet være at man unnlater å gjennomføre en konsekvensvurdering der det faktisk foreligger høy risiko. For å kunne evaluere risiko må man derfor ha god oversikt over vurderingskriteriene vi har gjennomgått i avsnitt 2.4 og 2.5 ovenfor. Risikobegrepet kan være vanskelig å definere, spesielt ettersom forordningen i seg selv ikke inneholder en god forklaring på hva risiko skal innebære. Derimot har lovgiver fastsatt momenter som skal tas i betraktning når man vurderer risiko som overlapper med flere etablerte metoder for risikovurderinger.

Videre er det viktig å ha en god forståelse for hva de ulike vurderingsmomentene i personvernforordningen innebærer for å gjøre en så riktig vurdering som mulig. Vi har i avsnitt 2.5 ovenfor forsøkt å illustrere kravene og hensynene i PVF artikkel 35 (1) for å få oversikt over hva som menes med de ulike elementene. I dette kapittelet har vi også illustrert i avsnitt 2.4 ovenfor hvordan kravene i artikkel 35 kan settes i et flytdiagram. Med dette flytdiagrammet forsøker vi å lage en “sti” for hvordan man kan gå frem for å vurdere om bestemmelsen kommer til anvendelse, og hva som er kravene. Til slutt understreker vi også at arbeidet med å gjennomføre en konsekvensvurdering er en kontinuerlig prosess. I undersøkelsen vil vi bruke den teoretiske gjennomgangen til å analysere og drøfte funnene vi gjorde i undersøkelsen vår i kapittel 3 nedenfor. Vi vil hovedsakelig bruke figur 5 i avsnitt 2.4 ovenfor for å analysere og

drøfte funnene. Der det er relevant vil vi også bruke de andre figurene og teorien vi har gjennomgått i kapittel 2 for å vise sammenhenger mellom funnene våre og hva vi har diskutert og drøftet i dette kapittelet.

3. Undersøkelsen

3.1 Innledningsvis om undersøkelsen

I dette arbeidet har vi vært ute etter å undersøke en virksomhets vurdering av personvernkonsekvenser. Som nevnt i avsnitt 1.2 ovenfor ønsker vi å undersøke hvordan en konsekvensvurdering er gjennomført i samsvar med PVF artikkel 35 og organisatoriske forutsetninger for dette. I begynnelsen av undersøkelsen hadde vi ikke en bestemt virksomhet eller sektor vi spesifikt hadde lyst til å undersøke. Vi passet derfor på å lage et undersøkelsesopplegg som var nokså åpent og generelt. Vi hadde sendt flere forespørsler til en rekke virksomheter innen finanssektoren og helse- og omsorgssektoren som i utgangspunktet var positive til å ta del i undersøkelsen. Ved utbruddet av korona - viruset ble det vanskelig for virksomhetene vi hadde kontaktet å ta del i undersøkelsen. Vi kom i kontakt med intervjuobjektet vårt, som er juridisk rådgiver hos Brønnøysundregistrene, gjennom en bekjent av oss. Etter at vi fikk bekreftet at vi kunne få innsyn i en gjennomført konsekvensvurdering og at vår kontaktperson sa seg villig til å stille til et intervju, ble Brønnøysundregistrene vårt undersøkelsesobjekt.

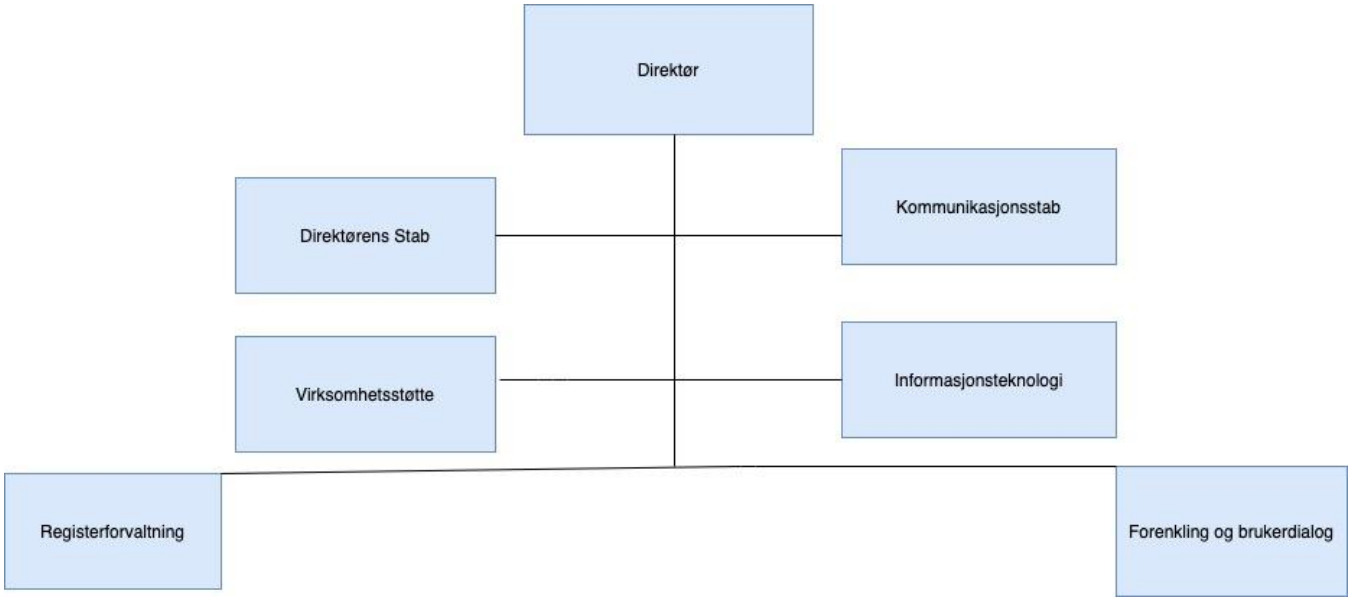
3.2 Om opplegget for og gjennomføringen av undersøkelsen

3.2.1 Om caset

Før vi går inn på gjennomføringen av datainnsamlingsmetodene vil vi først skrive litt generelt om Brønnøysundregistrene og hvilken konsekvensvurdering vi fikk tilgang til å bruke i undersøkelsen vår. Brønnøysundregistrene er et offentlig forvaltningsorgan som utvikler og driver digitale tjenester med mål om å effektivisere, samordne og forenkle dialogen mellom det offentlige og virksomheter, samt privatpersoner.[63] En av hovedoppgavene til Brønnøysundregistrene er forvaltning av landets viktigste registre, som for eksempel enhetsregisteret og fellesregisteret.[64] De fleste av kontorene deres er i Brønnøysund men i tillegg har de kontorer i både Narvik og Oslo og er delt inn i fire avdelinger og to staber.

[63]Brønnøysundregistrene "Om oss"
[64] Brønnøysundregistrene "Oppgavene våre"

Nedenfor har vi lagt inn figur 7 som er Brønnøysundregistrenes organisasjonskart. Vi mener det var hensiktsmessig å legge inn denne oversikten med tanke på at vi senere viser til hvilke avdelinger de som deltok i arbeidet med konsekvensvurderingen hørte til. Dette vil også gjøre det lettere for leseren å få et inntrykk av hvordan arbeidet med konsekvensvurderingen ble organisert. Vi vil forklare alle elementene av organisasjonskartet på et overordnet nivå under figuren.



Figur 7: Brønnøysundregistrenes organisasjonskart

Øverste firkant illustrerer Direktøren som har det overordnede ansvaret for etatens virksomhet. Dette innebærer å sikre god virksomhetsstyring hvor økonomi, resultatmål, prioriteringer og rapporteringskrav ivaretas etter styringsdokumentene fra Nærings- og fiskeridepartementet. Øverste firkant til venstre er Direktørens stab som skal være støtte for både direktøren og resten av toppledelsen. Øverste firkant til høyre er kommunikasjonsstaben som blant annet skal håndtere toppledelsens behov for intern og ekstern kommunikasjon. Kommunikasjonsstaben håndterer også alle mediehenvendelser og er koordinator for andre henvendelser som gjelder Brønnøysundregistrene. Firkantene videre under representerer de fire avdelingene Brønnøysundregistrene består av. Først har vi avdeling for virksomhetsstøtte som skal bidra til at Brønnøysundregistrene når målene sine. Disse målene omfatter blant

annet at virksomheten skal opptre i samsvar med lov- og avtaleverk, og legge til rette for at ledere og ansatte får den støtten de trenger. Avdelingen for informasjonsteknologi har blant annet ansvaret for å fastlegge rammer, utvikle og forvalte egne IT-system innenfor register og forenklingsområdet. Den nederste firkanten til venstre representerer avdeling for registerforvaltning som har ansvaret for og forvalter 14 registre, der den nasjonale felleskomponenten Enhetsregisteret, Foretaksregistere og Konkursregisteret er de største. Til slutt har vi avdeling for forenkling og brukerdialog som representeres av firkanten nederst til venstre. Denne avdelingen arbeider med at samhandlingen mellom næringslivet, frivillig organisasjoner, innbyggere og offentlige etater skal skje på best mulig måte.[65]

Intervjuobjektet vårt tilhørte avdeling for registerforvaltning. Nylig hadde vedkommende ansvaret for arbeidet med konsekvensvurderingen for en ny tjeneste som nylig har blitt lansert. Denne tjenesten er en nettbasert søkeløsning for konkurskaranteneregisteret. Tjenesten skal sørge for offentliggjøring av opplysninger om personer som er ilagt konkurskarantene. Å bli ilagt konkurskarantene innebærer at man ikke kan starte, påta seg eller utøve nye verv i en fastsatt periode. Verv omfatter her for eksempel daglig leder, styreleder, styremedlem eller varamedlem. I enkelte tilfeller kan konkurskarantene innebære at en person også blir fjernet fra eksisterende verv. En person kan bli ilagt konkurskarantene ved at tingretten avsier en kjennelse om konkurskarantene dersom en person er mistenkt for straffbar handling i forbindelse med konkurs eller en virksomhet som har ført til konkursen. Det samme gjelder i tilfeller hvor en person er funnet uskikket til å stifte, utøve eller påta seg verv, som nevnt ovenfor, i et nytt selskap, på grunn av uforsvarlig forretningsførsel.[66] Tjenesten som ble konsekvensvurdert legger til rette for at enkeltpersoner kan søke og få innsyn i konkurskaranteneregisteret ved å logge seg inn ved bruk av ID-porten. For å samle inn data som kunne belyse delproblemstillingene våre, se avsnitt 1.2 ovenfor, tok vi utgangspunkt i konsekvensvurderingen Brønnøysundregistrene hadde gjort før lanseringen av denne søketjenesten.

[65] Brønnøysundregistrene “Organisasjon og ledelse”
[66] Brønnøysundregistrene “Hva er konkurskarantene?”

3.2.2 Forholdet mellom dokumenter og intervju

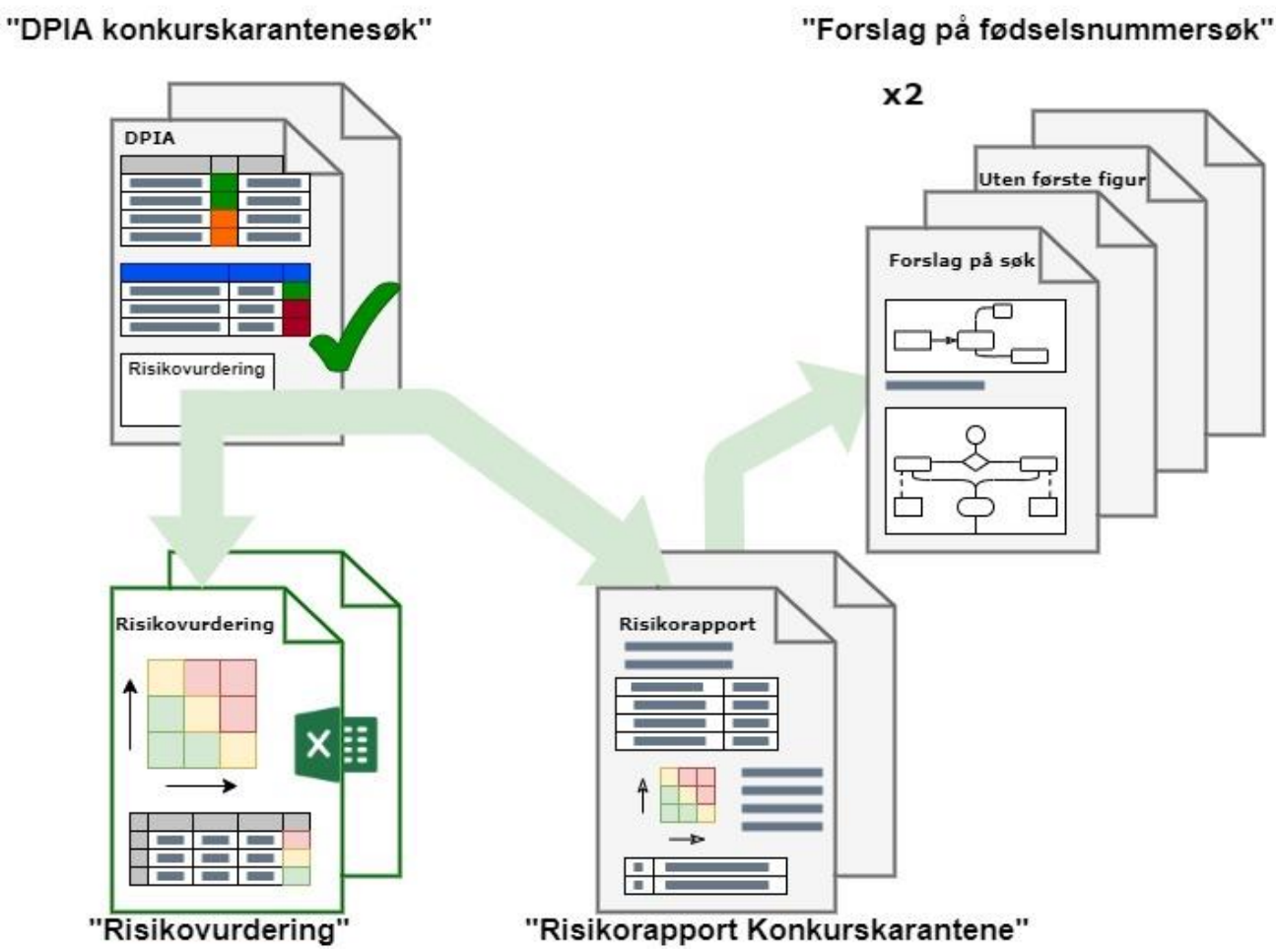
Som nevnt i avsnitt 1.3 ovenfor hadde vi valgt å samle inn data ved bruk av dokumentstudier og ha et intervju i etterkant med en som hadde deltatt i arbeidet med konsekvensvurderingen. Når det gjaldt hvordan vi hadde planlagt å gjennomføre dokumentundersøkelsen og intervjuet var det ingen endringer vi måtte gjøre når det gjaldt selve gjennomføringen. Endringer vi måtte gjøre underveis var tidspunktet for når vi skulle ha intervju. Grunnen til dette var at vi mottok dokumentasjonen av konsekvensvurderingen kort tid før vi hadde avtalt å ha et intervju. Vi utsatte derfor intervjuet, noe som var helt uproblematisk for intervjuobjektet vårt. Ved å utsette intervjuet fikk vi mer tid til å sette oss inn i dokumentasjonen og forberede oss. Vi kunne dermed i større grad gjennomføre den planlagte metodetrianguleringen, se avsnitt 1.3.7 ovenfor. Vår kontaktperson valgte en konsekvensvurdering basert på informasjonen vi hadde gitt vedkommende i forkant om undersøkelsen vår. Dette omfattet hva vi ønsket å undersøke, hva vi ønsket å få tilgang til og utvalgskriterier for hvem vi ønsket å intervjue.

3.2.3 Dokumentstudiet

Gjennomføringen av dokumentstudiet begynte da vi mottok dokumentene fra konsekvensvurderingen vi undersøkte. Våre tidligere erfaringer med å lese gjennomførte konsekvensvurderinger var minimalt. Vi hadde sett på maler som blant annet brukes innenfor helsesektoren.[67] Ellers hadde vi noen egne forventninger om hva dokumentasjonen ville inneholde. Våre forventninger baserte seg, som nevnt tidligere, på kravene i lovteksten slik de er lagt frem i forrige kapittel, samt Datatilsynets veiledning om vurdering av personvernkonsekvenser. Vi hadde ikke fått noen informasjon om hvilke maler eller metoder som ble brukt før vi mottok dokumentene.

Dokumentasjonen vi fikk fra intervjuobjektet vårt inneholdt mye data som vi måtte sette oss inn i før intervjuet. I figur 8 nedenfor har vi laget en forenklet oversikt over dokumentene vi mottok.

[67] FHI (2020)
AccuWeather /Reveal Mobile Case - Hallin (2020)



Figur 8: Forenklet dokumentstruktur

Vi har i figur 8 ovenfor forsøkt å vise dokumentstrukturen for de dokumentene vi mottok fra Brønnøysundregistrene. Det første dokumentet var den dokumenterte konsekvensvurderingen som hadde tittelen “DPIA Konkurskarantenesøk”. Den grønne haken på dokumentet viser til at ledelsen i Brønnøysundregistrene har validert konsekvensvurderingen, som vi vil komme nærmere inn på i avsnitt 3.3.2 nedenfor. I konsekvensvurderingen var det inkludert en del som omhandlet risikovurdering. Her ble det referert til to av de andre dokumentene vi mottok, som vist i figuren ovenfor ved hjelp av to grønne piler fra konsekvensvurderingen. De to dokumentene det ble referert til var risikovurderingen og risikorapporten. Risikovurderingen var en Excel-fil som viste hvordan Brønnøysund hadde vurdert hver enkelt risiko. Risikorapporten inneholdt en gjennomgang av arbeidet med en annen risikovurdering knyttet til samme tjeneste. Her var det videre utdypet tiltak som skulle bidra til å håndtere risikoene. I tillegg viste risikorapporten til andre tiltak som fulgte av vurderingen. Disse tiltakene fantes i to egne

dokumenter kalt “Forslag på fødselsnummersøk”. De to dokumentene var variasjoner av samme foreslåtte løsning.

Vi oppfattet Innholdet av dokumentene vi fikk tilsendt som oversiktlig og systematisert grunnet bruk av tabeller, definisjoner, matriser, forklaringer, osv. Dette gjorde det enklere for oss å få oversikt over for eksempel hvordan risiko og tiltak ble identifisert. Vi fikk innblikk i hva Brønnøysundregistrene la til grunn for hver vurdering og mange av momentene ble grundig forklart. Derimot var det noen dokumenter eller deler av dokumenter som i stor grad var interne og det var vanskelig å se hva som ble referert til. I noen tilfeller var det for eksempel lenket til et dokument vi ikke hadde tilgang til. Det var også utfordrende da det noen ganger ble benyttet forkortelser og navn på systemer vi ikke hadde noen forutsetning for å forstå. Derfor var det hensiktsmessig at vi hadde mulighet til å intervjue noen som hadde deltatt i arbeidet. Vi vil gå gjennom hvordan vi gjennomførte intervjuet i avsnittet nedenfor.

3.2.4 Intervju

Måten vi gikk frem på for å finne ut hvem vi skulle intervjue var først å høre med en bekjent av oss som jobber hos Brønnøysundregistrene, om vedkommende kunne sette oss i kontakt med aktuelle intervjuobjekter. Grunnen til at vi gjorde det på denne måten var fordi personen kjente til virksomheten og hadde bedre oversikt over hvem som jobber eller har jobbet med konsekvensvurderinger tidligere. På denne måten var det også enklere for å oss å komme i kontakt med ansatte i Brønnøysundregistrene som hadde den relevante erfaringen vi var ute etter. Personen vi valgte å intervjue var, som nevnt i avsnitt 3.2 ovenfor, juridisk rådgiver i avdeling for registerforvaltning. Grunnen til at vi valgte å intervjue vedkommende var at vi fikk vite at intervjuobjektet jobbet med personvern og da spesielt med konsekvensvurderinger. I forespørselen vår til intervjuobjektet beskrev vi våre problemstillinger og temaer vi ønsket å snakke om. Med dette gjorde vi det klart hva vi var ute etter og satt intervjuobjektet vårt i stand til å stilling til om hun var “riktig person” å intervjue eller ikke. I tillegg ga dette henne en mulighet til å forberede seg før intervjuet slik at vi kunne være så effektive som mulig.

Intervjuet ble gjennomført som planlagt over Teams.

I forkant av intervjuet hadde vi laget en intervjuguide som vi brukte aktivt under gjennomføringen. I intervjuguiden vår hadde vi delt intervjuet i tre deler: introduksjon, hoveddel og avslutning. Videre delte vi spørsmålene inn i forskjellige temaer som for eksempel organiseringen av arbeidet, beslutningsgrunnlaget for å gjøre en konsekvensvurdering, hvordan den ble gjennomført og om det ble gjort organisatoriske endringer som et resultat av denne vurderingen. Inndelingen av temaene var basert på delproblemstillingene våre, se avsnitt 1.2 ovenfor. Vi begynte å snakke om hvert tema ved å stille et åpent spørsmål. Grunnen til dette er at vi ville få intervjuobjektet vårt til å prate fritt og komme med forklaringer. Vi hadde også formulert oppfølgingsspørsmål for å sikre at vi fikk informasjonen vi var ute etter.

Ved gjennomføringen av intervjuet følte vi at det var god flyt i samtalen. Som nevnt i avsnitt 1.3.5 ovenfor tok vi lydopptak av intervjuet noe som vi fikk inntrykk av ikke påvirket måten intervjuobjektet vårt valgte å svare i særlig stor grad. Intervjuobjektet vårt var positiv til at vi tok lydopptak av samtalen. At vi fikk gjøre lydopptak gjorde det også lettere for oss å holde samtalen gående. Vi noterte i tillegg, noe vi syntes var veldig hjelpsomt. Dette gjelder særlig for å forsikre oss om at vi hadde stilt de spørsmålene vi hadde planlagt. En utfordring med intervjuet var å ha tid til å stille alle spørsmålene vi hadde forberedt innenfor tidsrammen. Vi måtte derfor prioritere de planlagte spørsmålene underveis i intervjuet fremfor temaer vi syntes var veldig interessante.

En annen utfordring var å ha intervjuet over Teams, fordi vi måtte være ekstra oppmerksomme på ikke å snakke over hverandre ved at vi for eksempel stiller hvert vårt spørsmål samtidig. Grunnet at alle tre var på hvert sitt sted, så hakking og treg internettforbindelse kunne føre til at vi avbrøt hverandre. Vi hadde, som nevnt i tekstavsnittet over, delt spørsmålene inn i fire deler og fordelte de mellom oss. På den måten hadde vi ansvar for hvert vårt tema når det kom til å stille, og svare på, spørsmål. I tillegg forsøkte vi alltid å spørre hverandre om vi hadde noe mer vi ønsket å spørre om innenfor hvert tema før vi gikk videre til et annet. Dette syntes vi fungerte veldig bra, særlig i tilfeller hvor den ene ikke kom på flere spørsmål mens den andre hadde ett eller flere tilleggsspørsmål.

Så snart intervjuet var gjennomført satt vi oss sammen for å skrive et referat. Her forsøkte vi å lage et sammendrag der vi fokuserte på de viktigste funnene til hvert tema. Deretter ble referatet sent til intervjuobjektet som hadde to kommentarer. Etter at vi hadde rettet opp i kommentarene, satte vi i gang med å inkludere funnene våre i teksten. En av utfordringene var å finne en god måte å disponere funnene våre på. En annen var at vi i stor grad tok utgangspunkt i referatet og innså etterhvert at det var mye å hente ved å gå tilbake til å lytte til intervjuet og gjennomgå dokumentasjonen flere ganger.

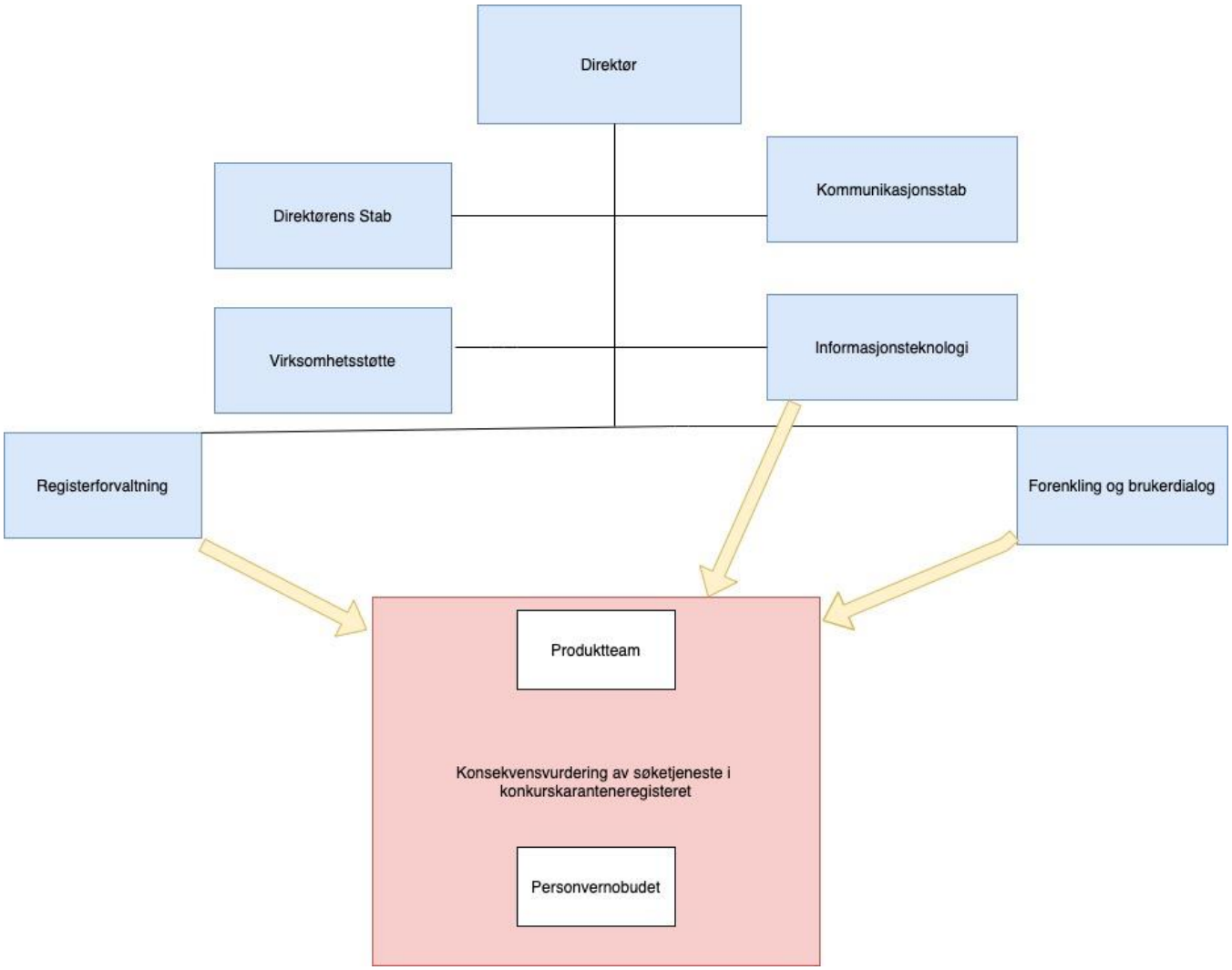
3.3 Før gjennomføring av konsekvensvurderingen

3.3.1 Innledning

I denne delen vil vi presentere hvilke funn vi gjorde i tilknytning til delproblemstillingene 1 og 2, se avsnitt 1.2 ovenfor, vedrørende hva som ble gjort før konsekvensvurderingen ble iverksatt. Dette gjelder hvordan arbeidet med den aktuelle konsekvensvurderingen ble organisert og hvordan man kom frem til at en slik vurdering var påkrevd. For å finne ut av dette undersøkte vi hvem som var involvert i arbeidet, hvilke roller de fikk tildelt og hvilken bakgrunn de hadde. Underveis i undersøkelsen forsøkte vi å følge flyten i figur 5 i avsnitt 2.4 ovenfor for å gå i gjennom dokumentasjon og intervju. Vi brukte altså figur 5 som et utgangspunkt for å analysere funnene våre. Avsnitt 3.3.2 nedenfor omhandler organiseringen av arbeidet med konsekvensvurderingen, mens avsnitt 3.3.3 går ut på hvordan Brønnøysundregistrene avgjorde om de var rettslig forpliktet til gjennomføre en konsekvensvurdering.

3.3.2 Organisering av arbeidet med konsekvensvurdering

For å få en oversikt over organiseringen av gjennomføringen begynte vi å se til blant annet risikorapporten vi fikk tilsendt av intervjuobjektet vårt. Her fant vi en oversikt over et produktteam bestående av åtte personer som var involvert i risikovurderingen. De som var med i produktteamet inkluderte ansatte med kunnskap innenfor IT, jus, samt ansatte fra avdeling for konkursregisteret og fra avdeling for forenkling og brukerdialog. Nedenfor har vi laget figur 9 som er en utvidet versjon av organisasjonskartet til Brønnøysundregistrene, se figur 7, avsnitt 3.2.1 ovenfor. Figuren illustrerer hvor de ansatte som deltok i produktteamet tilhørte.



Figur 9 Organisering av arbeidet med konsekvensvurderingen

De gule pilene illustrerer hvilke avdelinger de som var del av produktteamet tilhørte. Ifølge intervjuobjektet vårt tilhørte de fleste avdelingen for forenkling og brukerdialog ettersom dette var en avgiver tjeneste. I tillegg var det også nevnt at ansatte fra avdeling for informasjonsteknologi som jobbet innen systemutvikling var del av produktteamet.

Det ble forklart av intervjuobjektet vårt at dette produktteamet var de som var med på konsekvensvurderingen. Det ble satt fokus på at denne sammenstillingen av ansatte med ulik bakgrunn bidro positivt til arbeidet. Dette ble begrunnet med at deltakernes ulike synsvinkler resulterte i at de fikk dekket flere områder og at konsevensvurderingen ble mindre snever. Angående den videre organiseringen av arbeidet sto intervjuobjektet vårt for det meste av den

faktiske skrivingen i konsekvensvurderingen. Oppgavene underveis ble også delegert av intervjuobjektet som i all hovedsak hadde ansvaret for selve gjennomføringen og dokumentasjonen av konsekvensvurderingen.

I figur 9 ovenfor illustrerer den nederste hvite firkanten personvernombudets rolle. Personvernombudet deltok i arbeidet ved å gi råd og veiledning, spesielt når det gjaldt tolkningen av sjekklisten til Datatilsynet. Vi vil skrive nærmere om hvordan sjekklisten ble brukt i avsnitt 3.4.2 nedenfor om selve gjennomføringen av konsekvensvurderingen. Intervjuobjektet vårt påpekte under intervjuet at personvernombudet ikke var en del av produktteamet, fordi det var viktig at vedkommende skulle beholde sin uavhengighet. Derfor har vi laget en egen firkant for personvernombudet under og ikke inkludert i firkanten for produktteamet. Etter kravene i forordningen som vi gjennomgikk i figur 5, avsnitt 2.4 ovenfor stilles det ikke noen eksplisitte krav til organisering av arbeidet med tanke på hvem som deltar. Det eneste kravet som kan knyttes til dette er kravet om å rådføre seg med personvernombud dersom dette er en mulighet, jf. PVF artikkel 35 (2). Brønnøysundregistrene har en ansatt i 100% stilling som personvernombud og dermed gjaldt dette kravet under gjennomføring av konsekvensvurderingen.

Som nevnt i avsnitt 3.2.3 ovenfor hadde ledelsen validert konsekvensvurderingen. Derfor ønsket vi å undersøke nærmere rollen ledelsen hadde i arbeidet med konsekvensvurderingen. Under intervjuet fikk vi vite at ledelsen ikke deltok direkte i arbeidet, men fulgte opp jevnlig og validerte konsekvensvurderingen. At ledelsen validerte konsekvensvurderingen henger sammen med sjekklisten til Datatilsynet hvor det fremgår at ledelsen, etter minstekravene i artikkel 35 (7) er gjennomgått, skal evaluere og eventuelt godkjenne. Dette kravet henger også sammen med ansvarsprinsippet ved at selv om ledelsen ikke deltok har de fremdeles det overordnede ansvaret som behandlingsansvarlig. Dersom konsekvensvurderingen skulle vise seg å være mangelfull er det ledelsen som blir holdt ansvarlig.

3.3.3 Hvordan kom Brønnøysundregistrene frem til at en konsekvensvurdering var påkrevd?

Ut fra dokumentasjonen av konsekvensvurderingen så vi at Brønnøysundregistrene hadde brukt Datatilsynets liste over behandlingsaktiviteter som medfører høy risiko. Dette for å begrunne om en konsekvensvurdering var påkrevd. Som påpekt i figur 5,avsnitt 2.4 ovenfor bør man evaluere den tiltenkte behandlingen opp mot tilsynsmyndighetens liste for avgjøre om en konsekvensvurdering er påkrevd eller ikke. Dette gjelder særlig i tilfeller hvor det ikke har blitt gjennomført en konsekvensvurdering for en lignende behandling på et tidligere tidspunkt. Dersom den tiltenkte behandlingen oppfyller to eller flere kriterier på tilsynsmyndighetens liste skal man gjennomføre en konsekvensvurdering. Ut fra dokumentasjonen av konsekvensvurderingen har Brønnøysundregistrene vektlagt at ved tvil vil det være hensiktsmessig å følge “føre-var-prinsippet”. Dette er anbefalt av Datatilsynet, og handler om at dersom det foreligger tvil, burde man gjennomføre en vurdering av personvernkonsekvenser uansett.

I evalueringen konkluderte produktteamet med at konsekvensvurderingen for søketjeneste i konkurskaranteneregisteret oppfylte tre av kriteriene fra Datatilsynets liste. Kriteriene som var vurdert som oppfylt var blant annet behandling av personopplysninger om straffedommer eller lovovertredelser etter PVF artikkel 10. Dette som følge av at personer som ilegges konkurskarantene med skjellig grunn kan mistenkes for å ha gjort straffbare handlinger. Det andre kriteriet var at personopplysninger i konkurskaranteneregisteret kunne brukes av andre aktører til formål som for eksempel å trekke slutninger om en karanteneinnehaver sine økonomiske evner, pålitelighet, adferd, osv. Som angitt i avsnitt 2.5 ovenfor følger det av personvernforordningens fortalepunkt 75 at slike formål skal vurderes som å øke risikoen for fysiske personers rettigheter og friheter. Det tredje kriteriet som var ansett som oppfylt var at behandlingen foregikk i stor skala. Dette fulgte blant annet av at de antok at tjenesten ville bli brukt i stor utstrekning av flere søkere, og at det ville være ca. 600 karanteinnehavere i registeret til enhver tid. Som nevnt i avsnitt 2.5 er behandlingens omfang et vurderingsmoment for om det foreligger høy risiko etter artikkel 35 (1). I vurdering om behandling av personopplysninger foregår i stort omfang har lovgiver fastsatt noen hensyn i fortalepunkt 75 som antall registrerte, antall personopplysninger, osv. I tillegg har lovgiver i fortalepunkt 91

trukket frem at det geografiske virkeområdet skal tas i betraktning ved vurdering om det foreligger behandling av personopplysninger i stort omfang. I dette tilfelle vil det være nærliggende å fastslå at behandlingen foregår på et nasjonalt nivå, ettersom det er snakk om et nasjonalt register. I tillegg til de oppfylte kriteriene nevnt ovenfor var også andre tilfeller som kunne medføre risiko for fysiske personers rettigheter og friheter særlig fremhevet. Dette gjaldt tilfeller hvor personer med identisk navn, kunne forveksles med konkursinnehaveren, som kan potensielt medføre konsekvenser for personen eller søkeren. Et annet hensyn var at personer med fortrolig eller strengt fortrolig adresse kan være gjenstand for behandlingen.

Intervjuobjektet fortalte oss at vurderingen vedrørende om de var rettslig forpliktet til å gjøre en konsekvensvurdering etter Datatilsynets liste ikke ble gjort i forkant av selve konsekvensevalueringen. Det ble gjort senere for å bekrefte at en konsekvensvurdering var påkrevd. Det rettslige grunnlaget for behandlingen er PVF artikkel 6 (1) (e), jf (3). Det supplerende rettsgrunnlaget er konkursloven § 144, jf. konkursregisterforskriften § 10. I tilknytning til dette undersøkte vi om det var gjennomført en vurdering av personvernkonsekvenser i forbindelse med lovprosessen. Dette henger sammen med et av momentene vi har redegjort for i figur 5, avsnitt 2.4 ovenfor. Det handler om unntaket fra å gjøre en konsekvensvurdering dersom PVF artikkel 35 (10) er gjeldende. Intervjuobjektet vårt hadde ikke kjennskap til om det hadde blitt gjort noen formelle konsekvensvurderinger i forkant, eller for eksempel i lovprosessen. Det var heller ikke skrevet noe om dette i dokumentene vi fikk tilsendt. Grunnet mangel på dokumentasjon gikk vi ut fra at artikkel 35 (10) ikke var aktuelt i dette tilfellet.

Konsekvensvurderingen av søketjenesten ble til en viss grad basert på en tidligere konsekvensvurderingen som omhandlet DSOP-prosjektet.[68] Intervjuobjektet påpekte særlig at flere av problemstillingene var ganske like og derfor var det hensiktsmessig å bruke den tidligere konsekvensvurderingen. Dette var særlig gunstig med tanke på at man dermed kunne unngå å gjennomføre samme risikovurdering flere ganger etter hverandre. I figur 5,avsnitt 2.4 ovenfor har vi påpekt at man bør undersøke om det har blitt gjennomført en tidligere

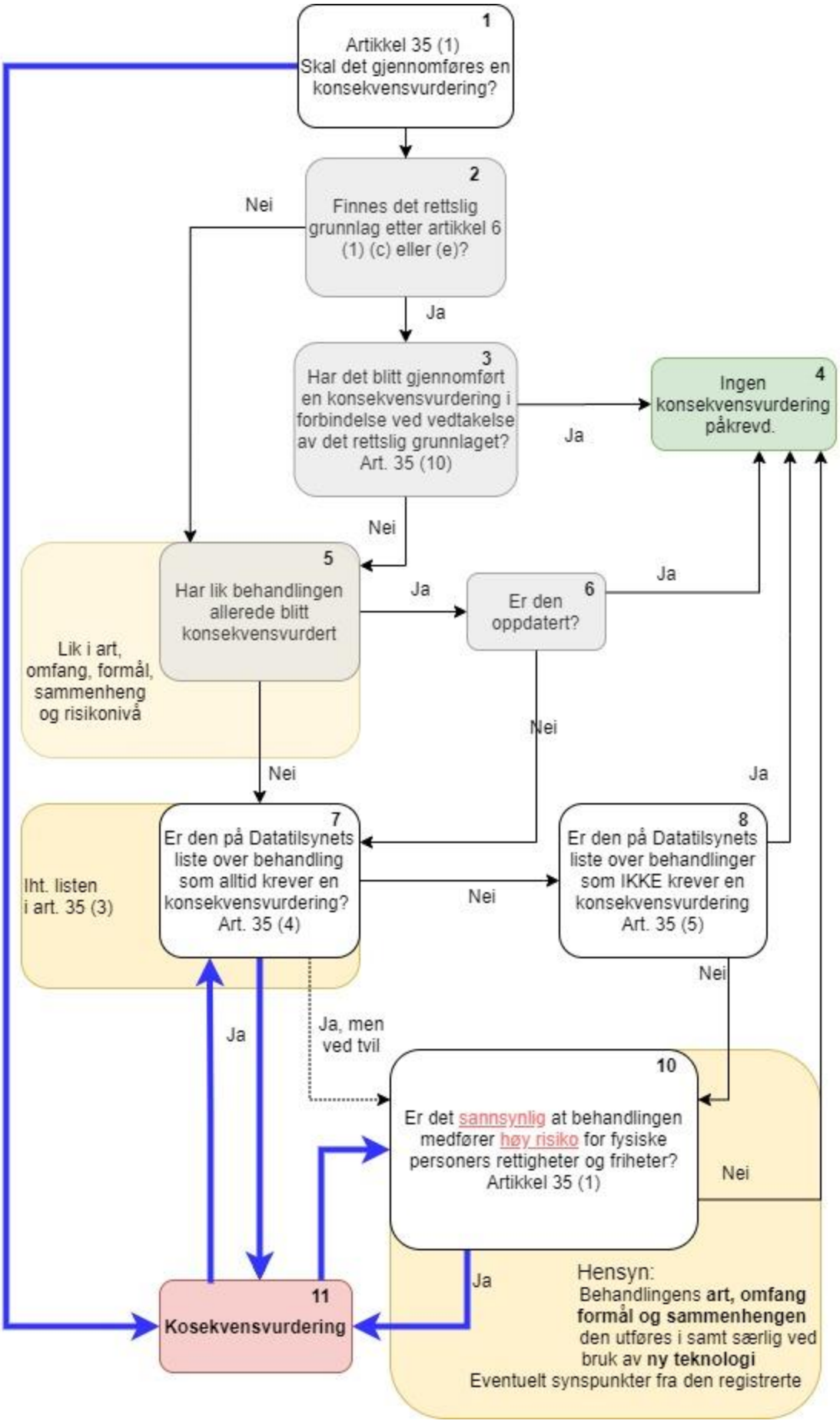
[68] Digital Samhandling Offentlig Privat: Samarbeidsprosjekt mellom offentlig forvaltning og finans norge - Bits (2017)

konsekvensvurdering for den tiltenkte behandlingen, eller en behandling som er svært lik. Hvis man kommer frem til at man har gjort en konsekvensvurdering for en lik behandling på et tidligere tidspunkt må man undersøke om den er tilstrekkelig oppdatert med tanke på at risikobildet kan ha endret seg. For eksempel ved å ta i bruk ny teknologi eller det kan oppstå organisatoriske eller sosiale endringer som medfører at man må gjøre en ny vurdering av personvernkonsekvenser. Det virket ikke som at undersøkelsen av den tidligere konsekvensvurderingen var avgjørende for om en konsekvensvurderingen var påkrevd eller ikke for dette tilfellet.

Avgjørelsen om at konsekvensvurderingen skulle gjennomføres, ble gjort uten en risikovurdering i forkant. Intervjuobjektet vektla særlig to hensyn som avgjorde at konsekvensvurderingen ble vurdert som nødvendig. Disse hensynene omfattet behandlingens art fordi det var snakk om behandling av personopplysninger som faller under PVF artikkel 10, og at det var en helt ny tjeneste. Som nevnt i avsnitt 2.5 ovenfor er behandlingens art et vurderingsmoment lovgiver har fastsatt i artikkel 35 (1), for å evaluere om en planlagt behandling medfører høy risiko. Behandling av personopplysninger om straffedommer og lovovertredelser etter artikkel 10 er trukket frem i fortalepunkt 91 som et hensyn som medfører høy risiko for fysiske personers rettigheter og friheter. I tillegg til dette mente intervjuobjektet i motsetning til hva som er konkludert i dokumentasjonen, at behandlingen ikke foregikk i særlig stor skala. Et vurderingskriterium som er viktig i denne sammenhengen er artikkel 35 (3) (b) hvor lovgiver har fastsatt at behandling i stor skala av personopplysninger om straffedommer og lovovertredelser, er tilfeller hvor en konsekvensvurdering skal være særlig nødvendig.

Når det kommer til hensynet om “ny tjeneste” fikk vi ikke inntrykk av at det var snakk om bruk av ny teknologi. I dokumentasjonen av konsekvensvurderingen var det også konkludert at dette ikke var tilfelle. Intervjuobjektet påpekte at ved bruk av en ny tjeneste hvor ikke alle risikoene er kartlagt på forhånd kan en konsekvensvurdering være et verdifullt verktøy for å identifisere, evaluere og håndtere risiko, samt dokumentere etterlevelse av personvernforordningen. Som angitt i avsnitt 2.3 ovenfor henger plikten til å gjøre konsekvensvurderinger tett sammen med ansvarsprinsippet, jf. artikkel 5 (2).

På neste side har vi laget figur 10 som er et utsnitt av figur 5, avsnitt 2.4 ovenfor for å sammenligne våre funn med prosessen vi utarbeidet ved analyseringen av bestemmelsene i PVF artikkel 35.


1
Artikkel 35 (1)
Skal det gjennomføres en konsekvensvurdering?
2
Finnes det rettslig grunnlag etter artikkel 6 (1) (c) eller (e)?
Nei
Ja
3
Har det blitt gjennomført en konsekvensvurdering i forbindelse ved vedtakelse av det rettslig grunnlaget? Art. 35 (10)
Ja
4
Ingen konsekvensvurdering påkrevd.
Nei
5
Har lik behandlingen allerede blitt konsekvensvurdert
Ja
6
Er den oppdatert?
Ja
Lik i art, omfang, formål, sammenheng og risikonivå
Nei
Nei
7
Er den på Datatilsynets liste over behandling som alltid krever en konsekvensvurdering? Art. 35 (4)
Iht. listen i art. 35 (3)
Nei
8
Er den på Datatilsynets liste over behandlinger som IKKE krever en konsekvensvurdering Art. 35 (5)
Ja
Nei
Ja
Ja, men ved tvil
10
Er det sannsynlig at behandlingen medfører høy risiko for fysiske personers rettigheter og friheter? Artikkel 35 (1)
Nei
Ja
Hensyn:
Behandlingens art, omfang formål og sammenhengen den utføres i samt særlig ved bruk av ny teknologi
Eventuelt synspunkter fra den registrerte
11
Kosekvensvurdering

Figur 10: flyten i artikkel 35 vs. hva vi faktisk fant

I figur 5, avsnitt 2.4 har vi skrevet at man bør undersøke tilsynsmyndighetens liste og behandlingsaktivtetene i PVF artikkel 35 (3) (a-c), for å vurdere om en konsekvensvurdering er påkrevd. Dersom det fremdeles foreligger tvil om en konsekvensvurdering er påkrevd etter denne vurderingen, bør man undersøke nærmere hensynene i artikkel 35 (1). I figur 10 ovenfor har vi laget et par blå tykke piler som illustrerer prosessen i vurderingen om konsekvensvurdering for søketjenesten i konkurskaranteneregisteret var påkrevd eller ikke. Den lengste tykke pilen til venstre del av figur 10, illustrerer at de hadde bestemt seg for å gjøre en konsekvensvurdering på forhånd. Som nevnt ovenfor baserte dette seg på to vurderingsmomenter som kan knyttes til de som er skrevet i boks 10 i figuren ovenfor. Dette er illustrert ved at det er en tykk pil mot boks 10 og tilbake til boks 11. Som nevnt ovenfor ble vurdering av tilsynsmyndighetenes liste av behandlingsaktiviteter som medfører høy risiko vurdert i etterkant av avgjørelsen. Dette er illustrert av en tykk pil fra boks 11 mot boks 7. I figuren er det også to piler fra boks 7 og 10 som peker tilbake til boks 11. Disse pilene illustrerer at produktteamet ut fra vurderingen av listene og hensynene kom frem til at en konsekvensvurdering var påkrevd. I forhold til figur 5 hadde Brønnøysundregistrene i vurderingen om en konsekvensvurdering var påkrevd dermed fulgt en annen rekkefølge enn det vi hadde kommet frem til i vår analyse av bestemmelsene.

3.4 Gjennomføring av konsekvensvurderingen

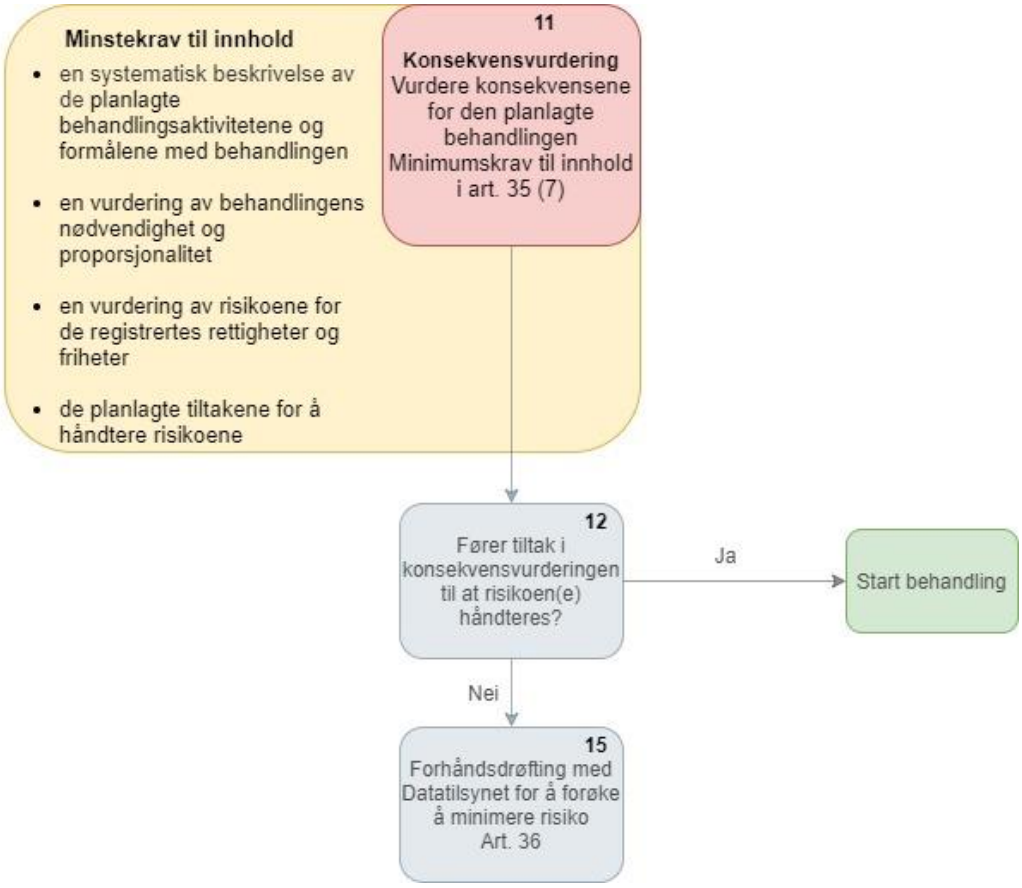
3.4.1 Innledning

Da det ble bestemt at det skulle gjøres en konsekvensvurdering, ble det satt i gang et arbeid med selve gjennomføringen. Vi går gjennom funnene våre av gangen i arbeidet med konsekvensvurderingen i avsnitt 3.4.2 nedenfor. Her fortsetter vi å følge flyten i PVF artikkel 35 som vist i figur 5, avsnitt 2.4 ovenfor. Videre tok vi utgangspunkt i artikkel 35 (7) da vi vurderte informasjonen vi fikk fra Brønnøysundregistrene. Bestemmelsen inneholder krav til hva en

konsekvensvurdering må inneholde. Ett av disse er kravet til risikovurdering som vi var inne på i kapittel 2 ovenfor. Dermed har vi, i avsnitt 3.4.3 nedenfor, gjennomgått risikovurderingen og tiltakene som ble gjort og/eller planlagt for å håndtere risiko(ene).

3.4.2 Beskrivelse av gangen i konsekvensvurderingen

Oppsettet for dokumentasjonen av konsekvensvurderingen var delt i fem deler hvorav den første innebar å undersøke om det i det hele tatt kreves en konsekvensvurdering. Denne delen har vi gjennomgått i avsnitt 3.3.3 ovenfor. De andre delene av konsekvensvurderingen fulgte minimumskravene lovgiver har fastsatt i PVF artikkel 35 (7) (a-d), vedrørende hva en slik vurdering minst skal inneholde. Ved gjennomføringen av konsekvensvurderingen tok Brønnøysundregistrene utgangspunkt i Datatilsynets sjekkliste. Som nevnt i avsnitt 2.4 ovenfor inneholder sjekklisten kriterier som bør tas hensyn til i de ulike fasene av konsekvensvurderingen. Intervjuobjektet fortalte oss at de hadde brukt sjekklisten til Datatilsynet ved arbeidet med flere konsekvensvurderinger. Under har vi i figur 11 laget et utsnitt av figur 5, avsnitt 2.4. Denne figuren illustrerer prosessen vi utarbeidet under analyseringen av kravene i artikkel 35, under figuren redegjør vi for hva vi faktisk fant.

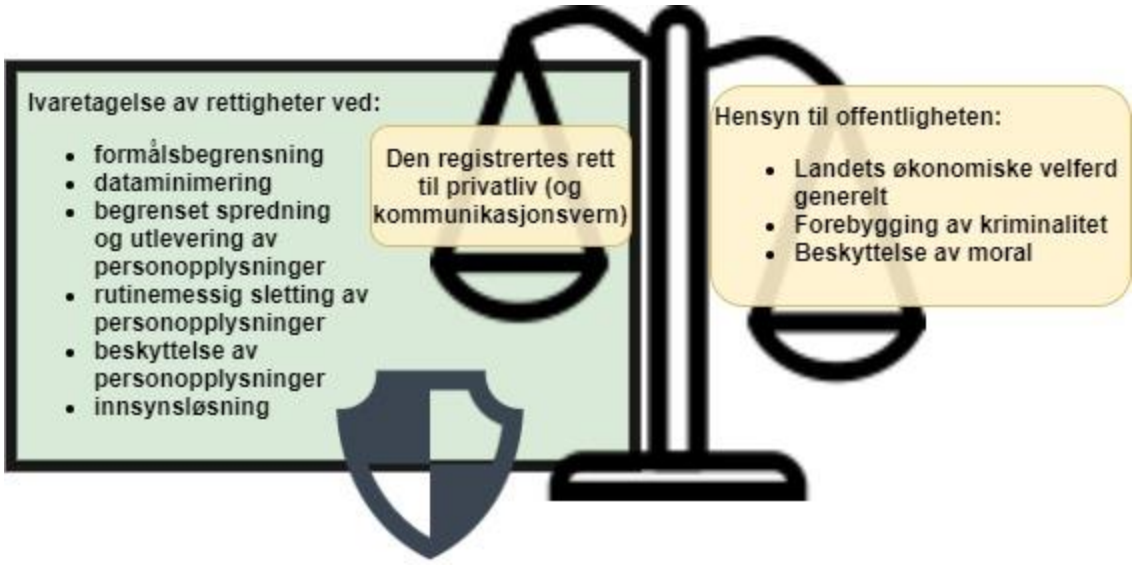


Figur 11: Utsnitt fra flytdiagram som fokuserer på PVF artikkel 35 (7)

Figur 11 ovenfor benyttes i dette avsnittet for å vurdere gjennomføringen av den undersøkte konsekvensvurderingen opp mot kravene som stilles etter forordningen. Figuren fokuserer på de elementene i figur 5, avsnitt 2.4 som omhandler de kravene i artikkel 35 (7) som finnes i den gule boksen. Vi så at neste del i dokumentasjonen inneholdt en systematisk beskrivelse av behandlingsaktiviteter i forbindelse med den nye søketjenesten, og formålet med behandlingen. Dette følger av krav etter PVF artikkel 35 (7) bokstav a. I tillegg fulgte dette av kravet om ansvar etter artikkel 24 (1), ansvarsprinsippet i artikkel 5 (2) og kravet om protokollføring etter artikkel 30. Vi kunne lese i oversikten til denne delen i dokumentasjonen at denne beskrivelsen blant annet innebar: «hvilke personopplysninger vi samler inn, omfanget av dem, hva de brukes til, hvordan de lagres og hvem som har tilgang til dem. Vi må også kunne redegjøre for formålet med behandlingen(e), noe som innebærer at vi må forklare hvorfor vi trenger hver enkelt personopplysning som vi samler inn.»

Videre fulgte tredje del om behandlingens nødvendighet og proporsjonalitet. Dette følger av krav etter PVF artikkel 35 (7) bokstav b. I denne delen ble det vurdert i hvilken grad behandlingen av personopplysninger i forbindelse med søketjenesten var legitim og nødvendig, samt at behandlingen var proporsjonal i forhold til formålet. I denne delen ble det vurdert om den registrertes rettigheter og friheter ble ivaretatt under behandlingsaktivitetene som var planlagt for tjenesten. Det var viktig at vi i den sammenhengen trakk frem fortalepunkt 4 i forordningen som presiserer at retten til personopplysningsvern ikke er en absolutt rettighet. Retten til personopplysningsvern må til enhver tid ses i sammenheng med og veies opp mot eventuelle andre rettigheter og friheter.

I konsekvensvurderingen vi undersøkte ble det først tatt stilling til de fem personvernprinsippene i artikkel 5. Deretter ble det vurdert om dette var relevant i forhold til behandlingen og eventuelt hva det måtte tas hensyn til. Videre ble det tatt stilling til forskjellige rettigheter og friheter for den registrerte. Det var først fokus på rettigheter og friheter etter personvernforordningen som for eksempel retten til innsyn, sletting, dataportabilitet m.v. Deretter fulgte en vurdering om relevante rettigheter og friheter etter EMK var tatt hensyn til i behandlingsopplegget. I følge dokumentasjonen av konsekvensvurderingen var retten til privatliv og kommunikasjonsvern etter EMK artikkel 8, vurdert som den eneste rettigheten behandlingen kunne medføre konsekvenser for. Intervjuobjektet vårt bekreftet dette og sa at det ble konkludert med at de andre rettighetene og frihetene etter EMK ikke var relevante for behandlingen. Dette var fordi behandlingen ikke ble vurdert som særlig inngripende for disse rettighetene. Intervjuobjektet forklarer derimot at retten til privatliv etter artikkel 8 ble vurdert og at den i dette tilfellet måtte veies opp mot hensynet til offentlighet. Nedenfor har vi laget figur 12 som skal illustrere hvordan behandlingens nødvendighet og proporsjonalitet ble vurdert.



Figur 12: Avveining mellom retten til privatliv og offentlig hensyn

I figuren ovenfor har vi trukket ut de hensynene som ble lagt til grunn ved vurderingen om inngripen i retten til den enkeltes privatliv var forholdsmessig. De gule elementene av figuren inneholder de ulike interessene som ble veid opp mot hverandre. I vurderingen ble det konkludert med at interessene som gagnet det offentlige veide tyngre enn den enkeltes privatliv. Dette er illustrert i figuren ovenfor ved at det gule elemente om offentlighet veier tyngre enn den andre gule boksen. Videre var det dokumentert hensyn som allikevel skulle bidra til å ivareta den registrertes rettigheter og friheter. Dette er illustrert i figuren ved hjelp av den grønne boksen som inneholder hensyn som blant annet følger av personvernprinsippene i PVF artikkel 5. Det er også inkludert et skjold i figuren som viser at disse hensynene er til for å verne om rettighetene og frihetene til den registrerte.

I den fjerde delen av konsekvensvurderingen vi undersøkte ble det listet konkrete konsekvenser behandlingen kunne medføre. Dette følger også av kravet til innhold i PVF artikkel 35 (7) bokstav c. Artikkelen viser til at dette dreier seg om de risikoene for fysiske personers rettigheter og friheter, som ble identifisert etter artikkel 35 (1). Dette innebærer altså konsekvenser behandlingen har for personopplysningsvernet. Brønnøysundregistrene vurderte konsekvenser opp mot såkalte “aktuelle personvernrisikoer”. Vi har inkludert et bilde av hvordan dette er strukturert i figur 13 under.

Spørsmål	Svar	Kommentar	Aktuelle personvernrisikoer	Tiltak
			• Tap av konfidensialitet • Tap av integritet • Tap av tilgjengelighet • Brudd på personvernprinsipper og den registrertes rettigheter • Fare for den registrertes liv og helse • Fare for økonomisk tap for den registrerte • Fare for omdømmetap for den registrerte • Fare for tillitstap/omdømmetap for BR	

Figur 13 Utsnitt av tabell i konsekvensvurderingen

Figur 13 viser tabellen der Brønnøysundregistrene undersøkte om tjenesten ville føre til krenkelser av den registrertes rettigheter og friheter. Figuren viser en kolonne i dokumentet der den, eller de som gjennomførte konsekvensvurderingen kunne vurdere hver konsekvens opp mot aktuelle personvernrisikoer, som for eksempel tap av tilgjengelighet eller tap av omdømme for den registrerte. Vi la merke til at det også var inkludert omdømme- og tillitstap for Brønnøysundregistrene som en aktuell personvernrisiko. Dette var noe vi vurderte som lite passende ettersom det her bør tas utgangspunkt i den registrertes synspunkter. Tabellen inneholdt også en kolonne for tiltak med sikte på å håndtere de identifiserte personvernrisikoene. Vi vil komme nærmere inn på risikoer og tiltak i avsnitt 3.4.3 nedenfor, om risikovurderingen.

Den siste delen av konsekvensvurderingen inneholdt selve risikovurderingen etter PVF artikkel 35 (7) (c) og (d). Med risikovurderingen mener vi identifisering av risikoer og evaluering av risikoenes sannsynlighets- og alvorlighetsgrad, samt identifisering av tiltak for å håndtere risikoene. Risikovurderingsdokumentet var her referert og linket til, som vist i figur 8 i avsnitt 3.2.3. ovenfor. Det som var skrevet i konsekvensvurderingen var et sammendrag av risikovurderingen og særlig to risikoer ble trukket frem. Vi vil komme nærmere inn på de konkrete vurderingene nedenfor. Dette følger av samme rekkefølge som sjekklisten til Datatilsynet for gjennomføring av konsekvensvurderinger.

3.4.3 Risikovurdering i Brønnøysundregistrene

Som nevnt i avsnitt 3.4.2 ovenfor innebar siste del av konsekvensvurderingen en oversikt over og vurdering av risikoene for de registrertes rettigheter og friheter. Både i risikovurderingen og risikorapporten ble det identifisert risikoer som kunne knyttes til den nye søketjenesten i konkurskaranteneregisteret. Risikoene ble i hovedsak identifisert under den systematiske gjennomgangen og ved vurderingen av nødvendighet og proporsjonalitet, samt ved selve vurderingen av personvernkonsekvenser, se avsnitt 3.5.1 nedenfor. I risikorapporten ble vi oppmerksomme på at det var gjort workshops i forbindelse med risikovurderingen. Dette var noe intervjuobjektet vårt utdypet videre. Risikovurderingen ble altså innledet med to workshops der produktteamet (se avsnitt 3.3.2 ovenfor) vurderte potensielle risikoer for behandlingen.

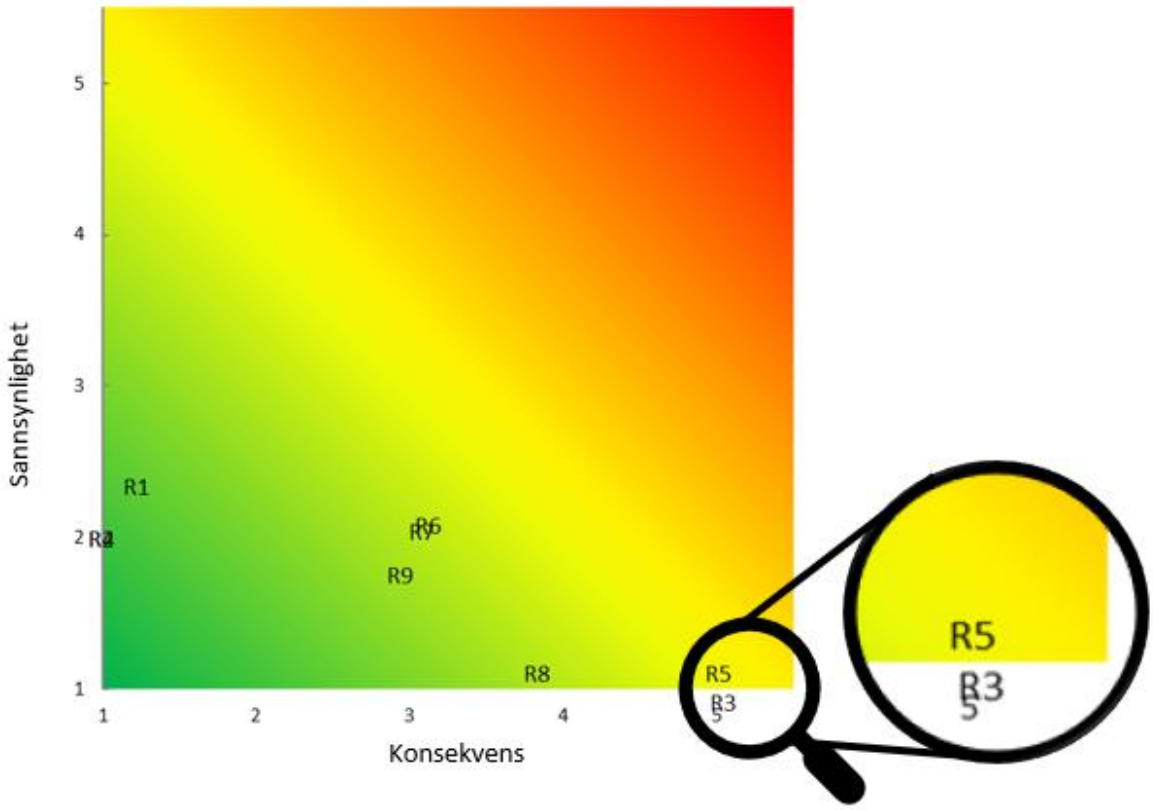
I risikorapporten ble det identifisert 18 risikoer (R1-R18) som angikk både det tekniske og organisatoriske ved løsningen som ble vurdert. Som nevnt i tekstavsnittet ovenfor ble risikoene identifisert i forbindelse med workshops. Her kom produktteamet frem til flere risikoscenarioer, altså mulige hendelser og hvilke konsekvenser det ville ha dersom de inntraff. Risikoene var ikke fordelt inn i organisatoriske eller tekniske risikoer. De var delt inn i fire grupper med en kort beskrivelse. Disse gruppene var:

- Brudd på tilgjengeligheten
- Angrep, tyveri og tekniske svakheter
- Feil bruk av løsningen
- Andre risikoer

Risikoscenarioene omfattet både villede og ikke-villede handlinger. For eksempel var en av risikoene som falt under gruppen “Angrep, tyveri og tekniske svakheter” at det kunne forekomme tyveri av ID-token fra ID-porten som fører til tap av ID-opplysninger for søker. I gruppen “Andre risikoer” hadde produktteamet identifisert risiko som var vurdert som utenfor akseptabel risiko. Denne risikoen handlet om at manglende systemkompetanse rundt søketjenesten kan føre til manglende vedlikehold av tjenesten.

Det neste vi undersøkte var hvilken risikomodell Brønnøysundregistrene benyttet i arbeidet med risikovurderingen. Det var tydelig da vi leste dokumentasjonen at de i dette tilfellet benyttet seg av en risikomatrise, slik som vi gjennomgikk i avsnitt 2.2.2.1 ovenfor. I risikovurderingen tildelte produktteamet hver risiko en verdi på bakgrunn av sannsynlighets- og alvorlighetsgrad. I risikovurderingen vi mottok som inneholdt risikomatrisen var det kun ni risikoer (R1-R9) som var trukket frem til forskjell fra de 18 som var listet i rapporten. Dette tolket vi som at de hadde valgt å gå videre med bare de risikoene som var vurdert som nødvendig å inkludere i konsekvensvurderingen. Det var imidlertid utfordrende å forstå hvordan de har valgt ut disse ni risikoene for vurdering. Risikorapporten inneholdt også en risikomatrise der alle de 18 risikoene (R1-R18) var plassert. Det vi konkluderte med er at det nok ble gjennomført to risikovurderinger i forbindelse med søk i konkurskaranteneregisteret. Denne konklusjonen underbygges bl.a. ved referanse til “den alminnelige risikovurderingen” og lenke til risikorapporten i konsekvensvurderingens siste del, se avsnitt 3.4.2 ovenfor. Under intervjuet forholdt vi oss kun til risikoene og konsekvensene i risikovurderingen og vi vil dermed ta for oss denne først.

Under, i figur 14, har vi inkludert en av figurene fra risikovurderingen som viser en risikomatrise der risikoene R1 til R9 er plassert.



Figur 14: Risikomatrise hentet fra dokumentet Risikovurdering

Intervjuobjektet vårt fortalte oss at de få risikoene som var identifisert var alle på et akseptabelt risikonivå. Altså var det ikke vurdert noen høy risiko. To identifiserte risikoer (R3 og R5) var allikevel plassert i det gule feltet i risikomatrisen, fremhevet av forstørrelsesglasset i figur 14 ovenfor. Dette innebærer at det forelå moderat risiko. Fra risikorapporten og risikovurderingen, samt etter intervjuet, var det tydelig at begge disse risikoene var av et akseptabel nivå ettersom det var vurdert som lite sannsynlig at de skulle inntreffe. Risikoene (R3 og R5) dreide seg om strengt fortrolige adresser og feil bostedskommune ved flytting. Intervjuobjektet vårt fortalte at de hadde vurdert konsekvensene av disse risikoene og veid de opp mot hensynet til åpenhet. Med særlig vekt på den lave sannsynligheten og hensynet til offentligheten kom de frem til at risikoene kunne aksepteres.

Under intervjuet fikk vi vite at fire av de ni risikoene (R6 - R9), som er inkludert i matrisen ovenfor, omhandler risiko for andre enn den registrerte. For eksempel at det foreligger risiko for økonomisk tap eller omdømmetap for andre enn den registrerte som følge av forveksling

grunnet statisk bostedskommune (R6). I følge intervjuobjektet vårt var det uenighet om at disse fire risikoene (R6-R9) i det hele tatt skulle bli inkludert i risikovurderingen. Intervjuobjektet vårt mente at disse risikoene kunne inkluderes i “den alminnelige risikovurderingen” som det vises til i rapporten. Denne uenigheten kan knyttes til at det i risikovurderingen av personvernkonsekvenser er den registrerte som skal være i fokus, som nevnt under figur 13 i avsnitt 3.4.2 ovenfor.

I tillegg til selve risikovurderingen er det i artikkel 35 (7) bokstav d et krav til at konsekvensvurderingen inneholder de planlagte tiltakene for å sikre personvern og påvise etterlevelse av kravene i forordningen. I risikorapporten var det listet tiltak for å håndtere flere av risikoene som ble identifisert i “den alminnelige risikovurderingen”. For risikovurderingen ble det ikke opplyst om noen nye tiltak i dokumentasjonen, men det var inkludert flere eksisterende tiltak som bidro til å minimere risikoene. Under intervjuet ble det også trukket frem to tiltak som skulle bidra til at behandlingen av personopplysninger i søketjenesten virket mindre inngripende i de registrertes rettigheter og friheter. Tiltakene innebar å ha innlogging som en forutsetning for å kunne søke og en begrensning av hvor mange søkeresultater som kan hentes ut. Disse tiltakene ble foreslått for å blant annet hindre utlisting av registeret.

De identifiserte tiltakene i risikorapporten var ikke gruppert inn i organisatoriske eller tekniske tiltak, som i artikkel 24 (1). Tiltakene var presentert ved en tabell som viste hvilke risikoer som skulle minimeres. Etter vår vurdering kan tiltakene grupperes inn i både organisatoriske og tekniske tiltak. For eksempel hadde Brønnøysundregistrene identifisert risiko for at tjenesten ville være utsatt for robottrafikk, som potensielt kunne ført til utlisting av registeret. For å minimere risikoen for dette hadde de blant annet iverksatt tiltak for begrensningsstyrt søk i tjenesten. Dette vil si at en søker kun hadde ett sett med søk vedkommende kunne gjøre i et gitt tidsintervall. Dette tiltaket vurderte vi som et teknisk tiltak som også intervjuobjektet bekreftet. Et annet eksempel på et teknisk tiltak er automatisk feilmelding til brukerne i tilfeller hvor Brønnøysundregistrenes nettside eller ID-porten er nede. Vi fikk ikke et inntrykk av at Brønnøysundregistrene hadde brukt en spesifikk systematikk i arbeidet med å identifisere tiltak som skulle treffes for å håndtere risiko. Tiltak var omtalt i en mer i generell forstand.

3.5 I etterkant av konsekvensvurderingen

3.5.1 Innledning

I denne delen undersøkte vi om arbeidet med konsekvensvurderingen hadde ført til organisatoriske endringer hos Brønnøysundregistrene. I denne delen var vi også ute etter å finne ut hvilke erfaringene de satt igjen med, samt om sammensetningen av de som deltok i arbeidet var ansett som fordelaktig. Vi undersøkte også om det ble opprettet noen nye rutiner rundt involvering av personvernombudet i arbeidet.

3.5.2 Endringer som følge av konsekvensvurderingen

I følge intervjuobjektet vårt hadde ikke konsekvensvurdering av søketjenesten i konkurskaranteneregisteret, ført direkte til noen organisatoriske endringer. Vi fikk heller ikke inntrykk av at det var noen formelle rutiner for arbeidet med konsekvensvurderinger hos Brønnøysundregistrene. Derimot ble vi gjort oppmerksom på at man ved hver konsekvensvurdering tar med seg erfaringer videre. Ved gjennomføring av konsekvensvurderinger i praksis blir det lettere å se hva som fungerer eller ikke fungerer. Fremgangsmåten som er benyttet i caset vårt er et resultat av erfaringer fra tidligere gjennomførte vurderinger. I forbindelse med dette ble vi fortalt om et prosjekt om å lage en felles mal for konsekvensvurderinger. Dette prosjektet innebar i følge intervjuobjektet vårt at denne malen skal benyttes som et rammeverk for arbeidet med konsekvensvurderinger. Ettersom malen ble utarbeidet med et ønske om at den skal fungere som rammeverk, inneholdt den både veiledningstekst og eksempler. Malen var et godt steg mot å utarbeide en felles metode for gjennomføring av konsekvensvurderinger. Dette kommer som følge av et behov for å systematisere arbeidet med vurdering av personvernkonsekvenser i større grad. Malen som ble brukt i den konsekvensvurderingen vi undersøkte, var den de hadde bestemt seg for å bruke ved fremtidige konsekvensvurderinger.

I tillegg var det et behov for å skape en oversikt over tidligere konsekvensvurderinger til gjenbruk. Dette kommer som følge av at det var stort fokus på å høste erfaringer fra hver konsekvensvurdering for å kunne forbedre gjennomføring. I figur 5,avsnitt 2.4 ovenfor har vi angitt at tidligere konsekvensvurderinger av samme eller lik behandling bør brukes til å vurdere

om en ny konsekvensvurdering er påkrevd. I tillegg vil innholdet av den tidligere konsekvensvurderingen kunne brukes på ny. Ved at alle konsekvensvurderingene er samlet på ett sted vil det samtidig legge til rette for at man gjennomgår konsekvensvurderingene hyppigere. Som påpekt i figur 5 er vurdering av personvernkonsekvenser en kontinuerlig prosess, ettersom risikobildet kan endre seg over tid for eksempel som følge av organisatoriske endringer eller ved bruk av et nytt informasjonssystem. Det kan eksempelvis være tilfelle at en ny planlagt behandling som er svært lik en tidligere behandling, kan medføre at en oppdager at en eldre konsekvensvurdering må gjennomgås på nytt.

Intervjuobjektet påpekte at organiseringen og sammensetningen av ansatte fra ulike avdelinger og med forskjellig kompetanse var fordelaktig. Dette var fordi man fikk fremhevet ulike perspektiver, som for eksempel personvernperspektivet og utviklerperspektivet. Disse perspektivene mente intervjuobjektet var viktig å se i sammenheng med hverandre. Vedkommende sa også at disse perspektivene ofte overlappet og at det dermed ble klart hva som burde vektlegges i vurderingen. I tillegg til dette fortalte intervjuobjektet at de arbeider med å etablere interne retningslinjer for når man skal kontakte personvernombudet eller andre som jobber med personvern i Brønnøysundregistrene. Dette kan gjelde tilfeller hvor det er tvil om en konsekvensvurdering er påkrevd eller ikke. I dokumentasjonen var det ikke skrevet noe særlig om organisatoriske endringer konsekvensvurderingen medførte eller andre planlagte tiltak som følge av andre hensyn. Vi måtte derfor basere våre funn på hva intervjuobjektet fortalte oss da vi skulle finne svar på denne delproblemstillingen.

3.6 Samlede tanker om funnene

Både intervju og dokumentstudiet ga oss svar på delproblemstillingene våre. Det var noen få forskjeller på informasjonen vi innhentet ved intervju og dokumentstudie. Blant annet ble behandlingen i dokumentasjonen beskrevet som omfattende, mens intervjuobjektet vårt fortalte oss at det ikke var snakk om behandling i stort omfang. Det er å regne med at informasjonen avviker litt fra det vi fant i dokumentasjonen av konsekvensvurderingen, og at vedkommende ikke har friskt i minne om hva resultatet av hver vurdering ble. Likevel er det verdt å merke seg slike forskjeller. På en annen side supplerte også funnene hverandre. Dette

gjelder særlig når det kom til avgjørelsen for at en konsekvensvurdering skulle gjennomføres. Vi fikk inntrykk av dokumentasjonen at Datatilsynets liste over behandlingsaktiviteter som krever vurdering av personvernkonsekvenser ble undersøkt i forkant. Avgjørelsen ble ifølge intervjuobjektet vårt egentlig basert på en annen fremgangsmåte enn det vi hadde sett for oss.

Ettersom intervjuobjektet vårt både ledet konsekvensvurderingen og var vår kilde til dokumentasjon, var det viktig for oss å vurdere dette i forhold til påliteligheten av funnene våre. Det var særlig viktig fordi intervjuobjektet valgte ut hvilken konsekvensvurdering vi fikk tilgang til og hvem vi skulle intervjue. Derfor kan det være at vedkommende valgte den konsekvensvurderingen som ga oss det beste inntrykke av hvordan arbeidet med konsekvensvurderinger ble gjennomført i Brønnøysundregistrene.

4 Konklusjon

4.1 Samlet oppsummering og konklusjon

I denne undersøkelsen har vi sett på en konkret konsekvensvurdering gjennomført av Brønnøysundregistrene. Vi har fokusert på selve gjennomføringen av arbeidet med konsekvensvurderinger og vurdert funnene opp mot vår analyse av kravene i personvernforordningen. Innledningsvis la vi grunnlaget for oppgaven ved å kartlegge og analysere relevante begreper og bestemmelser. En ting vi har tillagt mye vekt i dette arbeidet er hvordan risiko skal forstås i personvernforordningen. Grunnen til dette er at risiko er et sentralt kriterium som brukes til å vurdere om en konsekvensvurdering er påkrevd, samt for å etterleve forordningen generelt. Deretter lagde vi en prosess basert på artikkel 35 i forordningen og andre tilhørende bestemmelser som forklarer hvordan vi så for oss flyten i bestemmelsen. Alt dette var hensiktsmessig for å kunne både forbedre og besvare problemstillingene våre. Dette mener vi bidro til å gi oss det vi trengte for å kunne analysere og vurdere funnene vi gjorde i undersøkelsen.

Det vi ønsket svar på i dette arbeidet var hvordan en vurdering av personvernkonsekvenser kan gjennomføres i praksis og de organisatoriske forutsetningene for dette. Videre i arbeidet utledet vi fire delproblemstillinger og forklarte våre forventninger til hver av de. Det vi ønsket å få informasjon om var hvordan Brønnøysundregistrene organiserte arbeidet med konsekvensvurderingen, og hvordan de kom frem til at de var nødt til å gjennomføre den. Deretter undersøkte vi hoveddelene av konsekvensvurderingen og hvordan det konkrete arbeidet ble gjennomført. Avslutningsvis ønsket vi å vite hvilke, om noen, organisatoriske endringer som ble gjort etter at arbeidet med konsekvensvurderingen var avsluttet. Vi har underveis i arbeidet måtte endre litt på problemstillingene etter at vi har sett flere sammenhenger. Vi skiftet fokuset fra de organisatoriske forutsetningene for en konsekvensvurdering til å se på det faktiske arbeidet som har blitt gjort og hva som var resultatet.

Noe av det vi kunne trekke ut fra caseundersøkelsen vår, var at en sammensetning av personer med ulik bakgrunn kan virke fordelaktig i arbeidet med konsekvensvurderinger. Vi trakk denne slutningen på bakgrunn av undersøkelsen vi gjorde av denne spesifikke konsekvensvurderingen. Vi forstår imidlertid at dette kan variere fra vurdering til vurdering, men det stemte overens med det vi hadde forventet før vi gjennomførte undersøkelsen. I vår undersøkelse var det snakk om en konsekvensvurdering gjennomført av en virksomhet som utfører oppgaver i allmennhetens interesse ved drift og vedlikehold av nasjonale registre. Derfor hadde vi også en forventning om at arbeidet med konsekvensvurderingen ble gjort på en måte som gjenspeiler dette. Med dette tenkte vi at Brønnøysundregistrene måtte ha tilstrekkelig med ressurser tilgjengelig. Dette omfatter for eksempel ansatte med spesifikk kompetanse innen blant annet jus, systemutvikling, osv. for å kunne være bedre rustet til å gjennomføre konsekvensvurderingen i henhold til personvernforordningen.

En annen slutning vi har trukket ut fra caseundersøkelsen er at virksomheter ikke nødvendigvis undersøker prosessen lovgiver har lagt til grunn i PVF artikkel 35. Vi var åpne for at Brønnøysundregistrene kunne ha bestemt seg for å gjøre en konsekvensvurdering basert på andre vurderinger enn det vi så for oss i vår analyse av bestemmelsene. For eksempel tenkte vi oss at Brønnøysundregistrene hadde egne, formelle retningslinjer for hvilke typer behandling som krever en konsekvensvurdering. Dette var ikke tilfellet og avgjørelsen ble tatt uten å vurdere hverken lister eller lovgivers prosess. Vi vil derimot påpeke at hensynene som intervjuobjektet forklarte at ledet til avgjørelsen om at en konsekvensvurdering skulle gjennomføres, var hensyn lovgiver har listet opp i artikkel 35 (1). Vi vil presisere her at vårt intervjuobjekt hadde en del erfaring med konsekvensvuringer og personvern generelt. Et av hensynene som intervjuobjektet vårt fremhevet som en særlig grunn til å gjennomføre en konsekvensvurdering uansett, var å få kartlagt risiko og krav etter forordningen før behandlingen ble iverksatt. I både Personvernrådets retningslinjer og på Datatilsynets nettsider er konsekvensvurdering omtalt som et verktøy for å kunne oppfylle ansvarsprinsippet, jf. PVF artikkel 5 (2).[69] Vi utledet dermed at terskelen for å gjøre en konsekvensvurdering ikke

[69] WP29 (2017) side 4
Datatilsynet (2019)

nødvendigvis avhenger om det faktisk foreligger høy risiko. Den enkelte virksomhet kan komme frem til at de skal gjennomføre en slik vurdering uansett for å påvise etterlevelse.

Når det kom til selve konsekvensvurderingen hadde vi som nevnt ikke særlig mye kjennskap til tidligere gjennomførte konsekvensvurderinger. Vi hadde noen forventninger basert på innholdskravene etter personvernforordningen og Datatilsynets sjekkliste. Ut ifra funnene vi gjorde var det klart at Brønnøysundregistrene hadde erfaring med bruk av sjekklisten til Datatilsynet og at de hadde lagd malen de brukte ut fra denne. Ved undersøkelsen av hva og hvordan risiko var identifisert, vurdert og hvordan det skulle håndteres, er vi i ingen posisjon til å gjøre noen lovlighetskontroll. Dermed måtte vi være forsiktig med å konkludere om Brønnøysundregistrene har gjennomført en konsekvensvurdering i henhold til artikkel 35 eller ikke. Det vi vil konkludere med er at tilpasning av sjekklisten til Datatilsynet kan bidra til at vurderingen blir mer systematisert. Ved å ta stilling til kriteriene kan en være i bedre stand til å gjøre en omfattende vurdering med sikte på å oppfylle kravene i forordningen. Derimot er det viktig å understreke at sjekklisten ikke er en fasit. Det kom frem at en rekke av innholdet i sjekklisten ble vurdert som ikke relevant for denne konsekvensvurderingen.

Det som også var interessant var at funnene våre viste at det ikke bare hadde blitt vurdert risiko for den registrerte, men også andre enn den registrerte, samt Brønnøysundregistrene. Innenfor vanlige risikovurderinger er det ofte virksomheten som er i hovedfokus. Dette kan komme av gammel vane eller av sanksjonene virksomheten kan bli møtt med dersom behandlingen skulle vise seg å være i strid med forordningen. I en vurdering av personvernkonsekvenser skal man derimot ta hensyn til risiko for fysiske personers rettigheter og friheter. Ved bruk av sjekklisten som et utgangspunkt kan man i større grad bli oppmerksom på hvordan man skal vurdere risiko ut fra de registrerte sitt perspektiv og ikke virksomhetens.

Som nevnt har ikke lovgiver fastsatt noen spesifikk metode som skal brukes til å konsekvensvurdere, eller en definisjon av innholdet i risikobegrepet. Derfor er det opp til virksomheten selv å avgjøre hvilken metode de skal bruke. I dette tilfelle hadde Brønnøysundregistrene brukt risikomatrisen til å vurdere risiko. Denne metoden tar for seg

momentene i fortalepunkt 90. Brønnøysundregistrene kom frem til at det, etter anbefalte tiltak ble gjennomført, ikke forelå høy risiko for den registrertes rettigheter og friheter.

Det ble ikke gjennomført noen organisatoriske endringer som et resultat av konsekvensvurderingen vi undersøkte. Vi var klar over at dette kunne være tilfelle før vi begynte selve undersøkelsen. Derimot ble vi gjort oppmerksom på at det pågår et prosjekt hos Brønnøysundregistrene hvor man arbeidet med standardisering av en felles mal for konsekvensvurderinger. Vi vil dermed konkludere med at selv om ikke denne konsekvensvurderingen ledet til noen direkte endringer, høster man erfaringer fra hver konsekvensvurdering. Malen de brukte i den vurderingen er som nevnt et resultat av behov for systematisering, og erfaringene fra denne konsekvensvurdering vil være med på å danne grunnlaget for en felles mal hos Brønnøysundregistrene. Dette vil legge til rette for at man i større grad kan gjenbruke konsekvensvurderinger, samt gjennomgå dem på nytt dersom dette anses nødvendig.

4.2 Avsluttende refleksjoner

Noe vi anså som særlig utfordrende var å forsøke å systematisere lovkrav etter personvernforordningen og deretter anvende de på et praktisk tilfelle. Her var det ikke vi som gjennomførte konsekvensvurderingen, men vi var nødt til å se for oss hvordan man kan etterleve kravene i forordningen. For å kunne gjøre dette benyttet vi en del litteratur som omhandlet personvernforordningen, ettersom personvernforordningen i stor grad er utformet og formulert på en veldig generell måte med tanke på at den skal gjelde for hele EU- og EØS-området. Dermed er det ikke gitt at forordningen gir klare og konkrete svar på hvordan en konsekvensvurdering skal gjennomføres. Vi har derfor tatt den tilgjengelige litteraturen på området til hjelp for å kunne bearbeide og forstå hva som faktisk menes med risiko, konsekvens o.l. Dette omfatter spesielt retningslinjer fra Personvernrådet om gjennomføring av konsekvensvurdering og sjekklisten som Datatilsynet utledet fra disse retningslinjene. Vi benyttet begge i arbeidet, men vi forsøkte å tenke selvstendig under undersøkelsen, særlig da vi utarbeidet vår egen systematikk for arbeidet.

Noe annet vi oppdaget i arbeidet var behovet for en felles definisjon av risikobegrepet som kan benyttes i forbindelse med konsekvensvurderinger. Det finnes en rekke definisjoner og forklaringer, men det var utfordrende å finne én forklaring som dekket hva risiko innebærer og som samtidig ikke var for komplisert. Dette mener vi kunne være klarere fastsatt i forordningen, blant annet for å sikre en felles og tilstrekkelig forståelse av risiko uansett hvilket land man befinner seg i. Dette kan likevel gjøres i mindre skala ved å ha en felles forståelse av risiko innenfor hver enkelt virksomhet. For eksempel kan virksomheten utlede mer nøyaktige kriterier for hva de skal vurdere som "høy" risiko. Disse kriteriene kan inngå i en felles metode for gjennomføring av konsekvensvurderinger og er en viktig del da risikofortsåelsen legger grunnlaget for hele vurderingen. Det bidrar for eksempel til at man ikke unnlater å gjennomføre konsekvensvurderinger der man vurderer risikoen som lavere enn den faktisk er. Derfor ønsker vi å trekke frem risikoforståelse som noe av det viktigste vi har undersøkt.

Andre ting vi har fokusert på i dette arbeidet var å vurdere påliteligheten til funnene våre. Intervjuobjektet vårt var også vår kilde til dokumenter og dermed var det viktig å være klar over at vi ikke hadde noen mulighet for å etterprøve informasjonen. Vi kunne ved tvil ha tatt kontakt med en annen i Brønnøysundregistrene for å oppklare, men vi anså ikke noen av vurderingene som særlig kontroversielle. I de tilfellene der det oppstod avvik fra dokumentasjon og informasjon fra intervjuet passet vi på å presisere dette i teksten. Derimot kunne det ha vært gunstig å få flere synspunkter på samme sak for å forsikre oss om at funnene våre gjenspeiler virkeligheten. I arbeidet med denne undersøkelsen har vi forsøkt å være så åpne som mulig vedrørende styrker og svakheter ved forskningsopplegget vårt. Dette mener vi er særlig viktig for at den enkelte som leser denne undersøkelsen selv skal kunne være i en posisjon til å ta stilling til kvaliteten på forskningen vår. Vi har også passet på at leseren har så godt utgangspunkt for å kunne forstå hva det er vi har oppdaget og drøftet som mulig. Dette gjorde vi ved å inkludere hva vi har kommet frem til vedrørende hensyn og begreper i personvernforordninger. Vi håper også at de funnene vi har gjort i dette forskningsopplegget kan være nyttig ved undersøkelse av andre gjennomførte konsekvensvurderinger.

4.3 Om veien videre

I dette avsnittet vil vi skrive om hva vi mener kan være den videre utviklingen innenfor arbeidet med konsekvensvurderinger i Brønnøysundregistrene, basert på konklusjonene våre ovenfor. Som nevnt ovenfor fortalte intervjuobjektet vårt om at de arbeidet med å lage en standardisert mal som skulle brukes ved fremtidige konsekvensvurderinger. Dette kom av et behov for mer systematisering av arbeidet, og å samle alle konsekvensvurderingene på ett sted. Et annet formål var at den enkelte skulle kunne høste erfaringer fra tidligere konsekvensvurderinger ved gjennomføring av nye. I denne undersøkelsen har vi bare undersøkt én konsekvensvurdering utført av Brønnøysundregistrene, men vi vil anta at en rekke andre virksomheter kan ha samme behov for å standardisere arbeidet. Standardisering av maler og metoder for gjennomføring av konsekvensvurderinger kan bidra til at man effektiviserer arbeidet med vurdering av personvernkonsekvenser. Det kan også medføre at det er mindre krevende å sette seg inn i tidligere konsekvensvurderinger uten å bruke altfor mye tid på å finne frem til relevant informasjon. For eksempel kan det være tilfelle hvor man jobber med en konsekvensvurdering, og vil bruke deler av andre gjennomførte vurderinger som veiledning. I denne undersøkelsen hadde Brønnøysundregistrene laget en mal ut fra Datatilsynets sjekkliste. Som vårt intervjuobjekt påpekte, arbeider de fremdeles med å lage en felles mal. Selv om bruk av malen var ansett som hensiktsmessig i dette tilfelle, er det ikke dermed sagt at den er like relevant ved konsekvensvurdering av en annen type behandling.

Ved undersøkelsen av denne konsekvensvurderingen oppdaget vi at vurdering av personvernkonsekvenser, er en læringsprosess. Virksomheten tilegner seg nye erfaringer om regelverket, hvor omfattende vurderingen skal være og hvilke risikokriterier en må ta hensyn til. Det er ikke sikkert enhver virksomhet hadde samme utgangspunkt eller forutsetninger da personvernforordningen trådte i kraft til å gjennomføre omfattende konsekvensvurderinger. Fastsettelsen av ansvarsprinsippet i personvernforordningen har flyttet ansvaret over på den enkelte virksomhet til å i større grad sette seg inn i reglene før behandlingen påbegynnes. De må for eksempel avgjøre om en konsekvensvurdering er påkrevd, hvordan den skal gjennomføres, samt hvilke tiltak som skal treffes for at behandlingen skal foregå samsvar med forordningen. Vurdering av personvernkonsekvenser er et rettsområde som er stadig under utvikling. Blant annet utvikles det hele tiden ny teknologi og nye behandlingsaktiviteter som for

eksempel kan inkluderes i tilsynsmyndighetenes lister over behandlingsaktiviteter som krever at det blir utført en konsekvensvurdering for. Det kan også bli truffet rettsavgjørelser vedrørende om en konsekvensvurdering har blitt gjennomført i henhold til PVF artikkel 35 eller ikke. Virksomheter kan da sammenligne og ta stilling til om metoden de bruker for å konsekvensvurdere, samt om deres forståelse av risiko i lys av personvernforordningen, faktisk er i henhold til rettspraksis.

Kildeliste

Rettskilder

2018	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (pol)
2016	EUROPAPARLAMENTETS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer med behandling av personopplysninger og om fri utveksling av slike opplysninger samt oppheving av direktiv 65/46/EF (hjemlet i pol. § 1)
2005	Lov 17. juni 2005 nr. 62 om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)
1984	Lov 8. juni 1984 nr. 58 om gjeldsforhandling og konkurs (konkursloven)

Litteratur

Bøker

- Hallinan, Dara m.fl. “Data Protection and Privacy: Data Protection and Democracy (Computers, Privacy and Data Protection)”. Oxford: Hart Publishing 2020
- Jacobsen, Dag ingvar. “Hvordan gjennomføre undersøkelser?” 3. utg CAPPELEN DAMM AS 2018
- Kuner, Christopher. Bygrave, Lee A. og Docksey, Christopher. “The EU General Data Protection Regulation (GDPR): A Commentary” 1. utg. New York: Oxford University Press 6. februar 2020
- Schartum, Dag Wiese. “Digitalisering av offentlig forvaltning: Fra lovtekst til programkode” 1. utg. Oslo: Fagbokforlaget, 2018
- Schartum, Dag Wiese. “Personvernforordningen – En lærebok” 1. utg. Oslo: Fagbokforlaget 2020

- Skullerud, Åste Marie Bergseng. Rønnevik, Cecilie Lørvik Bødtker. Skorstad, Jørgen og Pellerud, Marius Engh. “Personvernforordningen (GDPR) Kommentarutgaven” 1. utg. Oslo: Forlag: Universitetsforlaget 2018

Offentlig dokumenter

- Article 29 Data Protection Working Party (WP29) “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 WP 248 rev. 01, 4 April. 2017. As last revised and Adopted on 4 October 2017
- International Organization for Standards (ISO) 2018 “ISO 31000:2018 Risk management – Guidelines”
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce. “Information Security: Guide for Conducting Risk assessments” September 2012

Artikler

- Demetzou, Katarina. ”Data Protection Impact Assessment: A tool for accountability and the unclarified concept of ”high risk” in the General Data Protection Regulation” Computer Law and Security Review, vol. 35, Issue. 6 (2019) s.1-14
- Gellert, Raphael. “Understanding the notion of risk in the General Data Protection Regulation” Computer Law and Security Review, vol. 34, issue. 2 (2017) s.279-288
- Bieker, Felix. Friedewald, Michael. Hansen, Marit. Obersteller, Hannah og Rost, Martin. ”A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation” In Privacy Technologies and Policy: 4th annual privacy Forum, APF 2016 Frankfurt/Main, Germany. (2016) s.21-37

Lenker

Brønnøysundregistrene

- Brønnøysundregistrene “Om oss” https://www.brreg.no/om-oss/ (sitert: 08.05.2020)
- Brønnøysundregistrene “Oppgavene våre” https://www.brreg.no/om-oss/oppgavene-vare/ (sitert: 08.05.2020)
- Brønnøysundregistrene “Organisasjon og ledelse” https://www.brreg.no/om-oss/organisasjonen-og-ledelsen/ (sitert: 28.05.2020)
- Brønnøysundregistrene “Hva er konkurskarantene?” https://www.brreg.no/registersok/alle-registersok/om-konkurskarantene/ (sitert: 28.05.2020)

Datatilsynet

- Datatilsynet “Vurdering av personvernkonsekvenser” (2019) https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/ (sitert: 23.05.2020)
- Datatilsynet “Sjekkliste for vurdering av personvernkonsekvenser (DPIA)” (2018) https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf (sitert: 10.02.2020)
- Datatilsynet “Om melding og konsesjon” https://www.datatilsynet.no/regelverk-og-verktoy/konsesjon-og-melding/ (sitert: 30.01.2020)

Øvrige lenker

- Bits “Digital Samhandling Offentlig Privat (DSOP) - Samarbeidserklæring” (2017) https://www.bits.no/wp-content/uploads/2019/08/Samarbeidserkl%C3%A6ring-DSOP.pdf
- Digitaliseringsdirektoratet “Brukerveiledning risikovurderingsverktøy” (Sist endret 2018) https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/brukerveiledning_risikovurderingsverktoy_v1.3.pdf (sitert 20.03.2020
- Digitaliseringsdirektoratet “Hva er risiko?” https://internkontroll-infosikkerhet.difi.no/risikostyring/hva-er-risiko
- European Data Protection Board (EDPB) “About EDPB” https://edpb.europa.eu/about-edpb/about-edpb_en (sitert 27.05.2020)
- Folkehelseinstituttet (FHI) “DPIA Smittestopp” (April 2020) https://www.fhi.no/contentassets/67d72db7c1ba4e2f9a70e9606b1c7ab0/dpia-smittestopp.pdf (sitert 03.05.2020)
- International Organization for Standards https://www.iso.org/what-we-do.html (sitert: 25.05.2020)
- National Institute of Standards and Technology (NIST) “NIST general Information” https://www.nist.gov/director/pao/nist-general-information (sitert: 06.05.2020)

Personlig informasjon

- Intervju med juridisk rådgiver i avdeling for registerforvaltning hos Brønnøysundregistrene, gjennomført 05.05.2020