UiO : Det juridiske fakultet

Avdeling for forvaltningsinformatikk

Risikovurdering av et av Statens vegvesens fagsystem etter krav i personvernforordningen

Kandidatnummer: 129399

Leveringsfrist: 01.07.2020

Antall ord: 18455

Innholdsfortegnelse

1. Innledning

1.1 Bakgrunn og aktualitet

Risikovurderinger skal bidra til å forebygge uønskede hendelser eller mangler ved behandling av personopplysninger i virksomheter. En risikovurdering er både et kartleggingsverktøy og et forbedringsverktøy som omfatter hele virksomheten. En risikovurdering inkluderer både organisering, ansvarsfordeling og rutiner for det daglige virket. Risikovurderingen skal kunne synliggjøre risikobildet og gi et grunnlag for å mestre risikoen ved å planlegge og iverksette "egnede tekniske og organisatoriske tiltak".[1]

Personvernregelverket forutsetter gjennomføring av risikovurdering ved at det tas hensyn til "risikoene av varierende sannsynlighets- og alvorlighetsgrad".[2] Resultatet av en risikovurdering vil danne grunnlag for etablering av tilfredsstillende sikkerhetstiltak og er nødvendig for dokumentering av etterlevelse av kravene etter personvernforordningen.

Det er mange tilgjengelige metodikker som kan brukes for å gjennomføre en risikovurdering, og akkurat dette skaper forvirring. Til og med når metodikken er valgt, kan resultatet variere ut fra forståelsen av risiko. Metoden som velges bør være skalerbar i forhold til virksomhetenes størrelse og sikkerhetsbehov.

Denne masteroppgaven tar sikte på å undersøke hvordan en risikovurdering er gjennomført i praksis i et bestemt offentlig forvaltningsorgan. Forvaltningsorganet jeg har valgt er Statens vegvesen, og jeg vil undersøke hvordan rettslige krav i personvernforordningen håndteres for å risikovurdere et av deres fagsystemer. Jeg vil også undersøke hvordan arbeidet med en risikovurdering blir organisert og hvilken fremgangsmåte som blir anvendt når et fagsystem gjennomgår en risikovurdering.

Oppgaven tar utgangspunkt i fire bestemte bestemmelser som inneholder krav om risikovurdering. Nesten alle bestemmelsene viser også til PVF art. 40 og art. 42 om godkjente atferdsnormer og sertifiseringsmekanismer som en faktor for å påvise at disse forpliktelsene overholdes. Jeg kommer ikke til å se nærmere på disse bestemmelsene fordi det faller utenfor oppgavens ramme som omhandler selve risikovurderingen.

[1] Forordning 679/2016/EU art. 24, 32 (heretter forkortet PVF).
[2] Personvernforordningen art. 24, 25, 32 og 35.

1.2 Problemstilling

1.2.1 Innledning

Det å gjennomføre en risikovurdering kan for mange virke komplisert og vanskelig. Mange har begrenset innsikt i hva som ligger i en risikovurdering og foretrekker å bruke eksterne ressurser. Datatilsynets årsrapport viser at det er stor usikkerhet vedrørende gjennomføring av risikovurdering: 29 prosent av henvendelsene i 2018[3] og 34 prosent av henvendelsene i 2019[4] til Datatilsynets veiledningstjenesten var spørsmål om risikovurderinger og andre temaer knyttet til informasjonssikkerhet.

Til tross for eksisterende usikkerhet og manglende kunnskap, er det likevel nødvendig å gjennomføre en risikovurdering av behandlingen. I og med at behandlingen av personopplysninger vanligvis skjer i et informasjonssystem, velger man ofte å risikovurdere systemet som behandler disse opplysningene før systemet tas i bruk. I tilfeller der systemet allerede var i bruk før personvernforordningen trådte i kraft, er det likevel nødvendig å gjennomføre en ny risikovurdering for å undersøke om personopplysningene behandles i tråd med det nye regelverket.

1.2.2 Problemstillinger og avgrensning

Ved å undersøke relevante rettskilder og gjennomføre en case-studie hvor jeg undersøker hvordan bruken av et fagsystem blir risikovurdert, ønsker jeg å belyse følgende problemstillinger:

1) Hvilke rettslige krav stiller personvernforordningen til vurdering av risiko for behandling av personopplysninger?

Vilkår som er fastsatt i regelverket for at handlinger eller prosesser skal regnes som gyldige, defineres som rettslige krav. Personvernforordningen stiller krav til å gjennomføre risikovurderingen som skal relateres til *behandlingen* av personopplysninger, ikke til et bestemt fagsystem som behandler personopplysninger. En risikovurdering representerer en kartlegging og vurdering av alle mulige farer og problemer og en vurdering av risikoen knyttet vurderingsområdet. Vurdering av personvernrisiko innebærer en verdivurdering og en trusselvurdering relatert til de registrertes rettigheter og friheter. Kravet til risikovurdering er fastsatt i flere bestemmelser.

I dette forskningsprosjektet ønsker jeg å identifisere hvilke bestemmelser som regulerer risikovurderinger. Videre vil jeg kartlegge de rettslige kravene som stilles til risikovurderinger og til de aktørene som behandler personopplysninger.

[3] Meld. St. 28 (2018–2019), s. 32.
[4] Datatilsynets årsrapport for 2019, s. 53.

2) Hvordan organiserte Statens vegvesen arbeidet med å risikovurdere arkivsystemet Memi 360?

For å svare på dette forskningsspørsmålet, vil jeg undersøke praksis for risikovurdering i Statens vegvesen og se hvordan rettslige krav håndteres for å gjennomføre en risikovurdering. Forskningen tar utgangspunktet i arkivsystemet Memi 360 som ble risikovurdert på nytt etter at personvernforordningen trådte i krav. Den første risikovurderingen ble gjort før systemet ble tatt i bruk, og denne risikovurderingen var basert på rettslige krav i EUs tidligere personverndirektiv.[5] Denne risikovurderingen tar jeg ikke i betraktning. Dette forskningsspørsmålet har som formål å kartlegge erfaringer med gjennomføring av risikovurderinger og fordeler og ulemper av organiseringen ved gjennomføring av en bestemt risikovurdering.

3) Hvilken fremgangsmåte ble anvendt da arkivsystemet Memi 360 ble risikovurdert?

Det eksisterer varierende metodikker og veiledninger som er ment å bidra til forståelse av hvordan man gjennomfører en risikovurdering. Gjennom forskningen vil jeg undersøke hvilken fremgangsmåte Statens vegvesen har valgt for å gjøre en risikovurdering av sitt arkivsystem. Jeg vil finne ut om det ble brukt metodikk som er utarbeidet av Difi, Nasjonal sikkerhetsmyndighet (NSM) eller Datatilsynet eller om det er utarbeidet en intern mal for en slik prosess. Vegvesenets fremgangsmåte vil også bli sammenlignet med de rettslige kravene i forordningen.

I og med at en standard metode som kan brukes av alle for å gjennomføre en risikovurdering ikke finnes, må Statens vegvesen trolig tilpasse sitt arbeid med risikovurdering til det som passer virksomhets behov og muligheter best. En mulig mangel på ressurser og kapasitet i virksomheter, særlig når det gjelder vurdering av personvernrisiko, er antakelig utfordring i forvaltningsorganet og kan påvirket en risikovurderingsprosess.

I denne masteroppgaven skal jeg kun fokusere på arkivsystemet Memi 360 som det har blitt gjennomført en risikovurdering av i Staten vegvesen. Hvis systemet er for omfattende og kompleks, er det mulig å se på et avgrenset antall prosesser som er inkludert i systemet.

1.3 Metode

1.3.1 Innledning

Vitenskapelig metode skal være et middel for å svare på forskningsspørsmålene. Det er også en mulighet til å referere til et verktøy som skal benyttes for å samle inn informasjon man trenger for å svare på en problemstilling. Nedenfor vil jeg beskrive mitt metodevalg samt forklare hvorfor

[5] EUs personverndirektiv (95/46/EF).

akkurat de aktuelle metodene er egnet for å kunne besvare forskningsspørsmålene mine. Metodene jeg skal bruke for å svare på forskningsspørsmål er rettsdogmatisk analyse og intervju. En del av denne oppgaven tar for seg en case-studie av Statens vegvesens risikovurdering av et arkivsystem.

Hensikten med metodene jeg har valgt er å finne frem til hovedtrekkene i den rettslige reguleringen av risikovurderinger i forordningen og fremstille et praktisk eksempel på anvendelse av disse kravene for å gjennomføre en risikovurdering. I og med at personvernforordningen inneholder flere krav enn det tidligere regelverket og etablert praksis må tilpasses etter gjeldende rett, er det spesielt viktig å både undersøke og understreke utfordringene knyttet til nettopp dette.

Opplegget var tilstrekkelig til å belyse forskningsspørsmålene. Rettsdogmatisk metode har laget et grunnlag og bakgrunn for intervju og systemanalyse. For å lage intervjuopplegget var det nødvendig først å analysere rettskilder. I tillegg at intervju har dekket det som har ikke gitt systemanalyse og har gitt en utdypet forståelse av fremgangsmåte og metode for risikovurderinger i Statens Vegvesen.

1.3.2 Rettskilder og rettsdogmatisk analyse

Rettsdogmatisk analyse innebærer at innholdet i kravet om risikovurdering fastlegges ved å identifisere relevante rettskilder, tolke innholdet i disse kildene, for etterpå å avveie rettsreglene mot hverandre ved hjelp av rettskildeprinsipper.[6] Med andre ord angir metoden en fremgangsmåte for å ta standpunkt til hvilke rettsregler som gjelder for risikovurdering etter personvernforordningen.

Den rettslige analysen i oppgaven baserer seg på personvernforordningen. Personvernforordningen regulerer behandlingen av personopplysninger og stiller flere krav til en slik behandling. Analysen har som formål å klargjøre og systematisere kravene etter personvernforordningen ved å «gjøre rede for hva man bygger på, og hvordan man resonnerer når man tar standpunkt til rettsspørsmål de lege lata».[7] Gjennom å tolke bestemmelsene som relevante for oppgaven i lys av hverandre vil det kunne føre til et konkret tolkningsalternativ. De overordnede personvernprinsippene i artikkel 5, herunder særlig prinsippet om ansvarlighet, vil blant annet ha betydning for tolkningen av risikovurderingen. Lovforarbeider, slik som en utredning[8] eller høring om utkast til ny personopplysningslov,[9] bidrar til en mer utdypende forståelse av regelverket. Det er foreløpig manglende rettspraksis som kan slå fast betydningen av

[6] Eckhoff (2001) s. 17-18.
[7] Eckhoff (2001) s. 15.
[8] NOU 2016: 19.
[9] Prop. 56 LS (2017–2018).

en risikovurdering, men avgjørelser om tidligere krav til risikovurderinger kan gi innspill til tolkning.

Både veiledninger og uttalelser fra Datatilsynet, vil være relevant for denne masteroppgaven og kan bidra til forståelse av bestemmelsene når det er ikke klart ut fra lovteksten.

Oppgaven vil trekke frem flere avgjørelser fra nasjonale tilsynsmyndigheter. Det er spesielt aktuelt å se på én avgjørelse[10] fra Datatilsynet som definerer hvordan tilsynsmyndigheten vil tolke krav til risikovurdering etter forordningen. Det er til tross for at varsel om overtredelsesgebyr ble sendt før forordningen trådte i kraft. Det hadde også vært relevant å se på avgjørelser fra tilsynsmyndigheter fra andre land. Men fordi tilsynsmyndighet publiserer avgjørelser på nasjonalt språk, avgrenser jeg min forskning til avgjørelser fra det norske Datatilsynet. Av spesiell interesse ved kartleggingen av myndighetspraksis er uttalelser fra Det europeiske personvernrådet[11] som har betydning for praksisutøvelse ved behandling av personopplysninger. Uttalelser fra Personvernrådet skal ha en betydelig vekt ved tolkning av bestemmelser i personvernforordningen, fordi en av Personvernrådets oppgaver er å sikre "ensartet, riktig anvendelse av forordningen, jf. PVF art. 70. Uttalelsen fra Personvernrådet er i utgangspunktet ikke bindende, men de nasjonale tilsynsmyndigheter er pålagt å ta størst mulig hensyn til uttalelsen.[12]

Juridisk teori vil ha en støttefunksjon i oppgaven når det gjelder forståelsen av bestemmelsene eller som bakgrunnsinformasjon.

Det er ikke formålet å finne frem til gjeldende rett, og jeg skal ikke gjøre legalitetskontroll av vegvesenets praksis heller. På grunn av kompleksiteten av en slik mulig tilnærming har jeg valgt å finne frem til hovedtrekkene i den rettslige reguleringen av risikovurderinger i forordningen.

1.3.3 Intervju

Kvalitativt intervju er den andre metoden jeg vil bruke i denne oppgaven for å besvare problemstillingene mine. Individuelle dybdeintervjuer fører til en dypere forståelse av problemstillingen og skal brukes som supplement til rettsdogmatisk metode. Funnene jeg gjør gjennom kvalitative intervjuer viser til sammenhengen mellom gjeldende rett og praksis. Jeg har valgt å gjennomføre individuelt dybdeintervju i min forskning fordi det gir dybdekunnskap om gjennomføring av risikovurderinger med Memi 360 som eksempel. Gjennom slike intervjuer er det mulig å få kunnskap om både hendelsesforløp, vurderinger før og under prosessen, argumenter,

[10] Datatilsynet (2017), varsel om gebyr 16/01531-45/GRA.
[11] Oversatt fra engelsk - European Data Protection Board (EDPB).
[12] Prop. 56 LS (2017-2018) s. 168.

beslutninger, ulike tiltak eller utviklingstrekk. Å gjennomføre et strukturert intervju med respondenten gjør prosessen for innsamling av informasjon enklere og informasjonen jeg innhenter gjennom intervju vil være relevant for oppgaven. Systemansvarlig og systemeier som er kjent med prosessen og systemkravene kan dele erfaringer og rutinemessige spørsmål knyttet til risikovurdering. Intervjuene har som primærfunksjon å bringe større klarhet i forhold til området som skal undersøkes. Hovedtemaene ble på forhånd satt opp i en intervjuguide. Denne tilnærmingen var valgt fordi jeg har et ønske om å oppnå en så åpen samtale som mulig, der det er mulig å forfølge interessante spor som dukket opp i løpet av samtalene. Samtidig er det viktig å komme innom visse temaer.

Først ble det gjennomført et innledende intervju med personvernombudet, der fokus var å ha en åpen samtale om tema for masteroppgave, diskusjon om et case der vi var enige om valg av systemet. Det ble også fullført gjennomgang av systemet som ble risikovurdert og de systemene som ble brukt som en del av fremgangsmåte og metode. Der deltok personvernombudet og informasjons- og IKT-sikkerhetsrådgiver. Neste og mest omfattende intervju jeg gjennomførte ble gjort digitalt. Intervjuobjektet er seksjonsleder for en enhet i Statens vegvesen som har foretatt risikovurderingen og er systemeier for Mime 360 og underliggende systemer. Tema for intervjuet var personvernrisikovurdering av et fagsystem. Som eksempel på et fagsystem ble det tatt utgangspunktet i systemet Memi 360. Formålet med intervjuet var å undersøke en risikovurderingsprosess, metode, fremgangsmåte som ble brukt og hvilke utfordringer som ble oppdaget underveis.

Samtykke for opptak av intervjuet ble innhentet på forhånd av møtet. Fordelen med å ta opp intervjuet er at det er mulig å få med alt som har blitt sagt. Dernest åpner det muligheten for å kunne konsentrere seg mer om å holde øyekontakt og få en god flyt i samtalen.

I begynnelsen av intervjuet ble masteroppgave presentert inkludert tema og problemstilling, og jeg forklarte også hvordan materialet skulle brukes.

Intervjuobjektet var bevisst på at møtet er basert på frivillig deltakelse og at samtykke kan trekkes og intervjuet kunne avsluttes når som helst samt at informasjonen som blir gitt kan trekkes. Jeg opplyste også om at opptaket og intervjureferatet ville bli anonymisert.

Resultatene av intervjuet vil vise forholdet mellom tolkning av bestemmelsene om risikovurderinger og praktisering av kravene etter personvernforordningen. Ved å supplere intervjuresultatene med systemgjennomgang, oppfattes resultatene som riktige og gir grunnlag for å mene at virkeligheten samsvarer med beskrivelse.

1.3.4 Dokumentundersøkelse og systemgjennomgang

Et intervju jeg gjennomførte handlet om gjennomgang av systemer som representerer et verktøy for å ha oversikt over systemer og behandlinger som skjer i systemet. Intervju handlet om etablert metodikk og verktøy for verdivurderinger og behandlinger av personopplysninger. Vi diskuterte oversikten over hvor de ulike verdiene finnes og hvilke behandlinger som gjennomføres. Systemer vi gikk gjennom danner også et grunnlag for risikovurderinger. Kunnskapen jeg fikk fra intervju fra informasjons- og IKT-sikkerhetsrådgiver og personvernombudet var relevant for videre arbeidet med oppgave.

Jeg har også fått tilgang til malen som brukes for risikovurderinger etter PVF art. 32. Både systemoversikt og malen bidro til at jeg har fått bedre kjennskap i interne prosesser vedrørende risikovurdering av systemer og fremgangsmåten for risikovurderinger. Det hjalp meg å gjennomføre intervju vedrørende risikovurderingsprosess som gjaldt Memi 360.

1.4 Oversikt over fremstillingen

Videre i oppgaven vil jeg først i kapittel 2 redegjøre for kravene til risikovurdering i personvernforordningen ved å først gi en generell beskrivelse av kravene og deretter en detaljert beskrivelse etter hver relevant bestemmelse. I kapittel 3 vil jeg presentere case-studien jeg gjennomførte, og resultatene av de gjennomførte intervjuene. Dette innebærer en fremstilling av systemer som er avgjørende for en risikovurderinger: Behandlingsoversikten og det integrerte systemet Verdivurdering. Jeg vil også gjennomgå hvordan Statens vegvesen gjennomfører en risikovurdering av arkiv- og saksbehandlingssystemet Memi 360. På denne måten vil jeg gi en helhetlig oversikt over både rettslige krav og min undersøkelse av hvordan disse kravene etterleves i praksis. Avslutningsvis vil jeg presentere mine konklusjoner i kapittel 4.

2. Oversikt over kravene til risikovurdering i personvernforordningen

2.1 Innledning

Jeg vil i det følgende kapittelet gi en oversikt over risikovurderinger generelt og risikovurdering i personvernforordningen spesielt, herunder hvilke generelle og spesielle krav som gjelder for risikovurderinger i personvernforordningen. Ettersom en risikovurdering innen informasjonssikkerhet er et kjent område, er det særlig aktuelt å se nærmere på prosessen og innholdet av den. En slik vurdering skal ses i sammenheng med tidligere praksis og gjeldende krav.

2.2 Generelt om risikovurdering sett i sammenheng med personvernrisikovurdering

2.2.1 De generelle kravene

Risikovurderinger er et kjent krav fra flere saksområder og har vært en kjent praksis i mange år.[13] Risikovurderinger er bl.a. omtalt i forskrifter som har hjemmel i arbeidsmiljøloven.[14] I tillegg omtales risikovurderinger i internkontrollforskriften,[15] sikkerhetsloven[16] og virksomhetsikkerhetsforskriften[17] mv. Arbeidet med risikovurderinger kan virke både omfattende, komplisert og tidskrevende. Til tross for dette er det viktig å anerkjenne at det finnes ulike farer og trusler som kan bli sett på som en risiko. Dette kan være alt fra vanlige menneskelige feil eller andre uforutsette omstendigheter til målrettet angrep fra eksterne trusselaktører. Risiko for tapte muligheter eller mangel realisering av sine rettigheter og friheter for den registrerte må også tas i betraktning.

Det finnes en rekke veiledninger som hjelper med vurdering av risiko, både de som inneholder generelle retningslinjer for prosessen og de som er tilrettelagt for et bestemt området, slik som eksempelvis informasjonssikkerhet, HMS, innen helseområdet, fiskeproduksjon og andre saksområder. Felles for mange av disse veiledningene er at de er svært omfattende, med fokus på detaljert og formell metodikk. Blant de mest kjente er veiledninger fra Digitaliseringsdirektoratet,[18] Datatilsynets veileder om risikovurdering, og risikometodikken fra Nasjonal sikkerhetsmyndighet. Verktøy som ofte brukes for å gjennomføre en risikovurdering er

[13] For eksempel helse, miljø og sikkerhet (HMS).
[14] Forskrift om utførelse av arbeid §23-1 og Forskrift om organisering, ledelse og medvirkning kap. 7.
[15] Internkontrollforskriften §5.
[16] Sikkerhetsloven § 4-2.
[17] Virksomhetsikkerhetsforskriften § 12.
[18] Digdir, før januar 2020 var det Direktoratet for forvaltning og IKT (Difi).

sjekklister og excel-filer eller matriser. Private organisasjoner og konsulenter tilbyr også metoder og verktøy som kan tilpasses etter kundenes behov.

Det er også flere standarder som retter seg mot risikostyring. Disse beskriver ulike metoder, både generelle og bransjespesifikke. En sentral internasjonal standard er ISO 31000,[19] som beskriver prinsipper og fremmer en veileder for risikovurdering. To andre er norske standarder for krav til alle typer risikovurderinger, NS 5814[20] og NS 5832.[21] Standardene beskriver prinsipper for gjennomføring av analyse av risiko knyttet til tilsiktede uønskede handlinger. De overnevnte standardene er blant de mest kjente. I tillegg er ISO 27000[22] og ISO 27007[23] også er viktige standarder. Disse retter seg mot informasjonssikkerhet og risikovurdering av system.

Standarder er ofte bransje- eller sektorrettet og viser til forskjellige måter å gjennomføre risikovurderinger på, men kan likevel være et godt utgangspunkt for mange aktører utenfor bransjen. Å følge en standard kan likevel bringe en falsk trygghet om at risikoer er under kontroll fordi uansett hvilken metode som velges eller hvilket verktøy som brukes for å gjennomføre en risikovurdering er det alltid en sjanse for at noe går galt. Disse standardene inneholder varierende detaljeringsgrad og perspektiv, men likevel handler en risikovurdering om sannsynlighets- og alvorlighetsgrad for at uønskede hendelser skjer, og hvilke risikoreduserende tiltak som er nødvendig for å oppnå et akseptabelt sikkerhetsnivå. Uansett hvilken metode som velges for gjennomføring av en risikovurdering, må metoden tilpasses virksomhetens behov, muligheter og forholdene innad i virksomheten.[24] Det er ikke et krav at offentlige virksomheter skal sertifisere seg etter standardene. Offentlige virksomheter heller ikke pålagt å være i samsvar med noen av standardene.[25] Pålegget er å basere seg på "anerkjente standarder".[26] Likevel oppfordrer personvernforordningen til "at det opprettes mekanismer for personvernsertifisering, jf. PVF art. 42 (1), og "sertifisering skal være frivillig", jf. PVF art. 42 (3). Uansett er en sertifisering begrenser ikke ansvar for å oppfylle kravene i forordningen[27]

Innholdet i begrepet "risiko" kan variere avhengig av risikodefinisjon som presenteres i forskjellige standarder, veiledninger, fagområder og miljøer. Derfor kan resultatet varierer ut fra forståelsen av risiko. Den enkleste og tradisjonelle måten å beskrive risiko på, er som en

[19] ISO 31000: 2018 Risk management.
[20] NS 5814:2008 Krav til risikovurderinger.
[21] NS 5832:2014 Samfunnssikkerhet.
[22] NS-EN ISO/IEC 27000:2017 Informasjonsteknologi.
[23] NS-ISO/IEC 27007:2020 Informasjonssikkerhet, cybersikkerhet og personvern.
[24] Datatilsynet. *Risikovurdering av informasjonssystem* (u.å.) s. 4.
[25] Digitaliseringsdirektoratet. *Hva sier ISO/IEC 27001?* (u.å.).
[26] eForvaltningsforskriften §15.
[27] PVF art. 42 (4).

kombinasjon mellom sannsynlighet og konsekvens. Det er også mulig å se på risiko som noe som består av en trussel, verdi og verdiens sårbarhet. Denne siste tilnærmingen kalles gjerne for trefaktormodellen. Denne modellen definerer risiko som et "uttrykk for forholdet mellom *trusselen* mot en gitt *verdi* og denne verdiens *sårbarhet* ovenfor den spesifiserte trusselen". [28] Trefaktormodellen er utviklet for å definere trusselaktør og er en anerkjent metode for risikovurdering. Å se på risiko fra sannsynlighets- og konsekvensesperspektiv er likevel mer aktuelt når verdien er personopplysninger. Særlig fordi personvernforordninger antyder relevansen av denne tilnærmingen ved å bruke formuleringen "varierende sannsynlighets- og alvorlighetsgrad". På den ene siden kan trefaktormodellen være aktuell å bruke i tilfeller hvor risiko vurderes med hensyn til personopplysningssikkerhet.[29] På den andre siden er det vanskelig å forholde seg til trusler i tilfeller hvor det vurderes risiko som er knyttet til om behandlingen skjer i tråd med regelverket[30] eller med sikte på en effektiv gjennomføring av personvernprinsippene.[31]

Den tradisjonelle forståelsen av en risikovurdering som er kjent fra annet regelverk og praksis fra andre områder kan også anvendes på en personvernmessig risikovurdering. Til forskjell fra en tradisjonell risikovurdering, hvor det tas hensyn til virksomhetens interesser som verdier, er at det i en personvernfokusert risikovurdering er individets friheter og rettigheter som er sentralt. Fordi de samme tiltakene i noen tilfeller kan dekke både kommersiell- og personvernrisiko, kan de tiltakene som er ment for å beskytte bedriftens hemmeligheter også være egnet for å etablere og opprettholde personopplysningssikkerhet. Slike egnede tiltak som passer for både personopplysninger og for bedriftens hemmeligheter kan eksempelvis være tilgangskontroll, sikkerhetskopiering, loggføring og signering av taushetsplikterklæring.[32]

Bestemmelsene om risikovurdering innen personvern er ikke nye og gjaldt også før personvernforordningen trådte i kraft. Krav til å gjennomføre en risikovurdering har vært en grunnleggende forutsetning for enhver behandling av personopplysninger i mange år og dette var svært tydelig i det tidligere regelverket. Det kan være nyttig å ta et tilbakeblikk på hvordan reglene om dette har vært formulert i mange år. Dette kan gi forståelse for hvorfor personvernrelatert risikovurdering skjer på akkurat den måten det gjør. Personopplysningsforskriften[33] etter det tidligere regelverket inneholdt følgende formulering:

"§2-4 Risikovurdering:

[28] NS 5830:2012, s. 5.
[29] PVF art. 32.
[30] PVF art. 24.
[31] PVF art. 25.
[32] Jarbekk (2019) s. 129.
[33] Personopplysningsforskriften av 15.desember 2000 nr. 1265.

Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.

Den behandlingsansvarlige skal gjennomføre risikovurdering for å kartlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endring som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. første ledd og §2-2.
Resultatet av risikovurderingen skal dokumenteres."

I forskriftens § 2-1 ble det presisert at sikkerhetstiltakene skulle stå i forhold til sannsynligheten og konsekvensen av et sikkerhetsbrudd. Som vi kan se ble det allerede i 2000 bestemt at man må ha oversikt over personopplysninger, fastlegge kriterier for akseptabel risiko forbundet med behandlingen av disse personopplysningene og gjennomføre en risikovurdering.

Kravet til å gjennomføre en risikovurdering er videreført i personvernforordningen fra det tidligere regelverket, men er ikke nedfelt i en bestemt artikkel. Det er heller spredt utover flere artikler, og fremstår muligens ikke like klart som tidligere. Plikten til å gjennomføre en risikovurdering etter personopplysningsforskriften var begrenset til informasjonssikkerhetsområdet[34]. Forordningen har ikke noe definert ord for vurderingen som skal gjøres, selv om det er implisitt at en slik vurdering må foretas.[35]

Personvernforordningen gir ikke en detaljert beskrivelse av krav til risikovurdering, men det er enklere for mange å fortsette med risikovurderinger på sammen måte som før da personvernforskriften trådte i kraft, med den forutsetning at det allerede finnes kunnskap og erfaring med risikovurderinger.

Personvernforordningen gir kun rammer og sikter på resultat, det vil si gjennomføring av egnede tiltak, uten at det foreligger noen formkrav eller detaljert beskrivelse om hvordan risikovurderinger skal skje. Årsaken til dette at forordningen er av generell karakter[36] og det forventes mer detaljert regulering som gjelder et bestemt området.[37]

Før en risikovurdering er det viktig å definere hvilken verdi som skal beskyttes. Verdivurderinger er grunnleggende for videre beskrivelse av mulige uønskede hendelser sentralt. En verdivurdering

[34] "Kartlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd".
[35] PVF art. 24, 25, 34, 35.
[36] The **General** Data Protection Regulation.
[37] Slik som for eksempel The ePrivacy Regulation ville være lex specialis for personvernforordningen.

blir definert som en "kartlegging og rangering av en entitets verdier".[38] Kartlegging av verdier i personvernsammenheng forutsetter en oversikt over behandlingsaktiviteter, jf. PVF art. 30. En slik oversikt over hvilke opplysninger som behandles, hva de brukes til og hvor de oppbevares mv, kan bidra til at sårbarhetene blir mer synlige. Eksempelvis kan informasjon om hvilke systemer behandlinger skjer i, føre til at det er behov å foreta en gjennomgang av sikkerhetsnivået i systemet, tilgangsstyringen eller å sjekke om det er innebygd personvern i slike systemer. I sin vurdering om overtredelsesgebyr til Sykehuset i Vestfold HF la Datatilsynet til grunn at kartleggingen av personopplysninger er nødvendig for å gjennomføre en tilstrekkelig risikovurdering.

En verdivurdering som identifiserer hvilken potensiell skade som kan oppstå ved misbruk av personopplysninger, er også viktig. Datatilsynet understreker at det er flere aspekter som skal tas hensyn til ved analysering av risiko, ikke minst at risikobildet stadig er i endring, og at nye risikoer kontinuerlig må vurderes. [39]

Hvor omfattende og detaljert en risikovurdering må være er avhengig av flere faktorer. Omfanget av risikovurderingen avhenger blant annet av om det er opplysninger av særlig kategori som skal behandles, om behandling er rettet mot barn, om personopplysninger behandles i stor skala eller om personopplysninger flyttes mellom flere aktører og systemer. Slike behandlinger er ofte kompliserte og derfor kan risikovurderinger knyttet til dette kreve at det involveres flere fagpersoner og bruk av mer tid enn en enkel oversiktlig behandlingsprosess.

I og med at forordningen ikke stiller formkrav til risikovurderingsprosessen, kan den variere. Det finnes ingen riktig eller gal måte å vurdere risiko på, så lenge risikoen er identifisert, sannsynlighets- og alvorlighetsgrad er fastsatt og risikoreduserende tiltak er angitt. Derfor er det mulig å velge malverk som passer for egen virksomhet eller lage et eget opplegg for risikovurdering.

Vurdering av risiko er en dynamisk prosess og krever oppdateringer, gjennomgåelser og revidering. Dette gjelder både når risikobildet forandres over tid på grunn av endringer i behandlingen, ved innføring av ny teknologi eller ved lovendring som regulerer risikovurderingen. Det er også en oppfordring om fornyelse av risikovurderinger i personvernforordningen, jf. PVF art. 24 og 32. Kontinuerlig oppfølging av en risikovurdering kan føre til bedre etterlevelse av regelverket, gjennom at det kontrolleres at planlagte tiltak senker sannsynligheten for en risiko til et akseptabelt nivå eller at det iverksettes andre tiltak hvis det er behov for dette.

[38] NS 5830: 2010, s 4.
[39] Datatilsynet 82017). Varsel om overtredelsesgebyr 16/01531-45/GRA s. 13-14.

2.2.2 Risikovurdering etter personvernforordningen

Ved behandling av personopplysninger[40], skal det tas stilling til hvordan opplysningene skal behandles for å være sikker på at håndtering av personopplysninger er i tråd med personvernregelverket. Behandling av personopplysninger forutsetter gjennomføring av en vurdering av *hvilke tiltak som må til* for at behandlingen skal være lovlig.[41]

Selv om begrepet "risikovurdering" ikke benyttes i personvernforordningen, gjenspeiler kravene tilsvarende risikovurdering, med den forskjellen at nå er det fokus på tiltak.

Forordningen stiller krav til gjennomføring av risikovurderinger gjennom flere bestemmelser. PVF art. 24 stiller krav til risikovurdering som er nødvendig for å identifisere tiltak som igjen er nødvendig "for å sikre og påvise at behandlingen utføres i samsvar med denne forordning." PVF art. 32 er brukbar for å se om et bestemt system har et egnet sikkerhetsnivå. En risikovurdering er grunnlag for å bestemme hvilke tiltak som er nødvendige for å integrere personvernprinsippene i behandlingen etter PVF art. 25. Ikke minst er det resultatet av en risikovurdering som viser om behandlingen innebærer høy risiko som fører til krav om vurdering av personvernkonsekvenser etter PVF art. 35. Derfor er de fire artiklene egnet for å regnes som de viktigste for risikovurdering.

Selv om bestemmelsene regulerer ulike forhold, er ett fellestrekk i disse at det stilles krav til en vurdering av risiko som gjelder de registrertes rettigheter og friheter. Personvernforordningen presiserer ikke om rettigheter og friheter er utelukkende personvernrelaterte. Jeg antar at kravet omfatter også andre grunnleggende rettigheter ut fra personvernforordningens formål, jf. PVF art. 1.[42] I tillegg tydeliggjør fortalepunkt 4 at "forordningen overholder alle grunnleggende rettigheter".[43] Personvernforordningen regulerer ivaretakelse av «rettigheter og friheter» i artiklene 12-22. Datatilsynet påpeker[44] at følgende rettigheter og friheter skal være omfattet etter personvernforordningen: Privatliv, kommunikasjonsvern, ytringsfrihet, religionsfrihet, retten til å organisere seg, retten til ikke å bli diskriminert mv. Dette er forskjellige rettigheter og friheter som følger av ulike konvensjoner.[45] En rekke andre bestemmelser har mer indirekte betydning for

[40] Saklig virkeområde etter PVF: "helt eller delvis automatisert behandling av personopplysninger og ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register," jf. PVF art. 2.
[41] Jarbekk (2019) s. 126.
[42] Jf. PVF art. 1: "Denne forordning sikrer vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger".
[43] Fortalepunkt 4: "Særlig med hensyn til privatliv og familieliv, hjem og kommunikasjon, vern av personopplysninger …".
[44] Datatilsynet. Risiko og risikovurdering (2019).
[45] Den europeiske menneskerettighetskonvensjon (EMK), FNs konvensjoner om henholdsvis sivile og politiske rettigheter (SP), og økonomiske, sosiale og kulturelle rettigheter (ØSK), EUs Charter om grunnleggende rettigheter.

"rettigheter og friheter", og kan derfor ikke ekskluderes fra risikovurderingene, jf. kap. V om overføring av personopplysninger til tredjestater eller internasjonale organisasjoner.

Et nøkkelelement i de ulike bestemmelsene i personvernforordningen som inneholder krav til risikovurderinger er formuleringen "*ta hensyn til risikoene* for fysiske personers rettigheter og friheter" Denne formuleringen kan tolkes som en pekepinn for å vise hvordan det er ønskelig at forordningen skal etterleves, både når det kommer til iverksetting av tiltakene for å sikre etterlevelse av kravene, men også oppnåelse av resultater gjennom disse tiltakene. [46] Med andre ord er det risikoene for fysiske personers rettigheter og friheter som skal identifiseres, og etterpå skal disse risikoene håndteres.

Risikobegrepet i personvernforordningen har med dette et bredt omfang ved at det refererer til flere rettigheter og friheter enn bare personvern. Risiko brukes som et kriterium for å danne juridiske forpliktelser slik som for eksempel krav til vurdering av personvernkonsekvenser etter PVF art. 35. Risikovurdering fungerer som oppfyllelse av ansvar og dokumentasjonsplikt for vurderinger som er foretatt dersom det oppstår et avvik eller i tilfelle tilsyn fra myndighet.

Tabellen nedover viser sammenhengen mellom de artiklene som inneholder krav til risikovurdering. Tabellen viser hvilke punkter som er avgjørende for hver bestemmelse samt variasjon mellom disse.

Formulering	**art. 24**	**art. 25**	**art. 32**	**art. 35**
hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i	x	x	x	x
hensyn til den tekniske utviklingen, gjennomføringskostnadene		x	x	
risikoene av varierende sannsynlighets- og alvorlighetsgrad	x	x	x	
eksempel på risikoene			x	x
fysiske personers rettigheter og friheter	x	x	x	x
gjelder behandlingsansvarlige	x	x	x	x

[46] Quelle (2017) s. 44.

gjelder databehandler			x	
egnede tekniske og organisatoriske tiltak	x	x	x	
eksempel på tiltak		x	x	x
skal gjennomgås på nytt og oppdateres ved behov	x			x
tidspunkt for risikovurdering		x		x
ref. til prinsippene		x		

Figur 1 - Sammenheng mellom bestemmelsene som inneholder krav til risikovurderinger

Som tabellen ovenfor viser har bestemmelsene mange elementer med lik formulering, men hver bestemmelse har fokus på et bestemt område, men alle har samtidig en risikobasert tilnærming.

Jeg vil videre gjennomgå noen av hovedtrekkene jeg har presentert i tabellen ovenfor, forklare hvilke krav de stiller til risikovurdering og forklare hvordan artiklene henger sammen og eventuelt overlapper.

I vurderingen av risiko skal det blant annet tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i,[47] og den verdien som skal beskyttes ved iverksetting av tiltak er fysisk personers rettigheter og friheter. Dette presenteres i de horisontale kolonnene, kolonne nr. 2 og nr. 6. Ved å ta hensyn til behandlingens art skal det tas i beregning om det er ordinære personopplysninger eller opplysninger av særlig kategori som behandles. Særlig hensyn skal tas når behandlingen gjelder barn[48]. Ekstra hensyn og særlig vern under risikovurdering fortjener også andre sårbare personer og utsatte grupper, slik som for eksempel demente som ikke kan ivareta egne interesser på tilsvarende nivå som andre.[49] Hvor detaljert, omfattende eller langvarig behandlingen er, kan være avgjørende for betydning om størrelse av risiko og det påvirker hvor krevende risikovurderingen skal være. Som tabellen ovenfor viser inneholder alle fire bestemmelsene samme formulering på disse to punktene. Det betyr at risikovurdering og risikoreduserende tiltak må tilpasses behandlingen av personopplysninger. En risikovurdering er en objektiv vurdering hvor formålet er å fastslå om behandlingen av personopplysninger først og fremst innebærer en risiko i det hele tatt, for å så ta standpunkt til om risikoen er høy.[50]

[47] PVF art. 24, 25, 32 og 35.
[48] Fortalepunkt 38 presiserer at barns personopplysninger fortjener et særlig vern.
[49] Schartum (2020) s. 242.
[50] Fortalepunkt 76.

Som tidligere nevnt, stiller ikke personvernforordningen eksplisitte krav til akkurat hva en personvernrisikovurdering skal inneholde, men det fremkommer av ordlyden i flere artikler at "*Risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter", jf. PVF art. 24, 25 og* 32. Jeg tolker dette som at en risikovurdering må bestå av to parametere, både hvor sannsynlig det er at en uønsket hendelse inntreffer og hvor alvorlig denne uønskede hendelsen eventuelt vil være for den registrerte. Hvis både sannsynlighetsgraden er høy, og alvorlighetsgraden er høy, indikerer dette også at risikoen er høy. En kjent metode for å vurdere dette er ved bruk av en matrise, som jeg vil gjennomgå nærmere i kapittel 2. Formulering i PVF art. 35 er noe annerledes. Artikkel 35 sier at dersom det er sannsynlig at behandlingen vil medføre en høy risiko for fysiske personers rettigheter og friheter, må den behandlingsansvarlige før behandlingen gjøre en vurdering av hvilke konsekvenser behandlingen vil ha for personopplysningesvernet. En slik vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.

En annen artikkel som retter seg mot risiko er PVF art. 30 som omhandler føring av protokoll over behandlingsaktiviteter[51]. Hovedregelen er at det skal føres protokoll over behandlingsaktiviteter, men artikkelen åpner for å frita noen virksomheter fra å føre protokoll, *men mindre* behandlingen som utføres sannsynligvis vil medføre en risiko for de registrertes rettigheter og friheter, jf. PVF art. 30 nr. 5. Det er viktig å legge merke til at det er flere vilkår for at fritak kunne gjelde. Den behandlingsansvarlige og eventuell databehandler skal blant annet gjøre en vurdering av om det er sannsynlig at behandlingen vil medføre risiko. Det kan diskuteres om det kan i praksis foreligge en situasjon der behandlingen ikke vil innebære risiko, verken enten høy eller lav.

Risiko for de registrertes rettigheter og friheter er også avgjørende for vurderingen av om det er krav til å melde brudd på personopplysningssikkerheten til tilsynsmyndigheten etter PVF art. 33, samt om det er krav til å informere de registrerte om bruddet på personopplysningssikkerheten[52]. Det er kun sannsynlighetsgrad som er avgjørende for unntaket etter PVF art. 30, 33 og 34.

Personvernforordningen viser til konkrete risikoer som er relevante i bestemte situasjoner, samt at det gis eksempel på konkrete tiltak som kan være relevante. Eksempelvis gir PVF art. 32 eksempler på tiltak som kan gjennomføres, slik som pseudonymisering og kryptering av personopplysninger. Artikkel 35 nr. 3 gir konkrete eksempler på særlig nødvendige tilfeller hvor man må vurdere personvernkonsekvenser. Et poeng som kan trekkes frem her kan være at eksempelvis PVF art. 24 er noe generell og vag når det kommer til den behandlingsansvarliges ansvar, da artikkelen i høy

[51] PVF art. 30 (5): "En generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene".
[52] PVF art. 34.

grad er vurderingspreget. Formuleringer som «dersom det står i *rimelig* forhold til behandlingsaktiviteten» og «gjennomføre egnede tekniske og organisatoriske tiltak» gir lite henvisning på hva som faktisk må gjøres, og forordningen gir spillerom for behandlingsansvarlig til selv å vurdere hvilke tiltak som skal iverksettes for å påvise at behandlingen utføres i samsvar med forordningen.

Kravet til å gjennomføre en risikovurdering og vurdering av personvernkonsekvenser gjelder alltid for den behandlingsansvarlige. Databehandler skal kun forholde seg til instrukser fra den behandlingsansvarlige og krav til personopplysningssikkerhet. Derfor må databehandler gjøre egen risikovurdering kun etter PVF art. 32. Det er kun behandlingsansvarlig som må "sikre og påvise" etterlevelse av kravene. Databehandler kan likevel ha oppgaver for å etterleve slike krav hvis det er fastsatt i databehandleravtale eller er beskrevet i instruks.

Det er kun PVF art. 24 og 35 som fastsetter tydelig at en vurdering jevnlig skal gjennomgås og eventuelt endres ved endringer i behandlingen. Bestemmelsen om sikkerhet ved behandlingen antyder til jevnlige oppdateringer av risikovurderinger ved å bruke ordet "vedvarende", jf. PVF art. 32 (1) (b). Typiske situasjoner når det er behov for oppdatering vil være når behandlingssystemet utvider omfanget av personopplysninger eller ved at kraftig oppdatering av funksjonell del av systemet som ikke var planlagt under gjennomføring av risikovurdering. Også når det skjer leverandørbytter kan det være aktuelt å se på risikovurderings-rapporten på nytt. Endring av regelverket er også et eksempel på et behov for gjennomgåelse av risikovurderingen. Det er likevel flere andre tilfeller som er aktuelle for at en ny risikovurdering skal gjennomføres.

Selv om ikke alle bestemmelser har klare henvisninger til tidspunktet for når risikovurderinger skal gjennomføres samt at kun en bestemmelse referer til kobling til personvernprinsippene, er det en klar mulighet for analogisk tolkning. Det vil si at risikovurdering skal gjennomføres før behandlingen starter og oppdateres ved behov og at ved gjennomføring av risikovurdering skal personvernprinsippene alltid tas i betraktning. Datatilsynet har uttalt seg om at personvernforordningens formulering av krav til risikovurdering skiller seg fra det gamle regelverket, men bestemmelsene skal likevel tolkes analogisk når det gjelder risikovurderingens *formål og tidspunkt* for gjennomføring av risikovurderinger.[53]

Kravet til en vurdering av personvernkonsekvenser kan oppleves som noe mer klart, da bestemmelsen inneholder krav om i hvilke tilfeller vurderingen skal gjennomføres og hva vurderingen minst skal inneholde, samt andre hensyn man må ta.

[53] Datatilsynet (2017). Varsel om overtredelsesgebyr til Sykehuset i Vestfold HF 16/01531-45/GRA s. 18.

Fortalens punkter 75 og 76 gir en mer konkret veiledning for selve risikovurderingen. Disse punktene viser til at det er nødvendig å være oppmerksom på situasjoner som kan føre til fysisk, materiell eller ikke-materiell skade.

Risikovurderingen danner grunnlag for:

- ivaretakelse av den behandlingsansvarliges ansvar
- sikring av innebygd personvern
- sikring av tilstrekkelig sikkerhet ved behandlingen
- vurdering av personvernkonsekvenser.[54]

En risikovurdering har som hensikt å identifisere de hendelsene som representerer farene eller truslene for de registrertes rettigheter og friheter. Risikovurdering gir et godt grunnlag for å håndtere risikoene gjennom tiltak og være forberedt til potensielle uønskede hendelser som innebærer trusler for de registrertes rettigheter og friheter.

Ansvarlighet går som en rød tråd gjennom hele personvernforordningen. Prinsippet krever at den behandlingsansvarlige beviser overholdelse av personvernprinsippene,[55] jf. PVF art. 5 nr. 2, og de utfører behandlingen i samsvar med forordningen, PVF art. 24 (1). I praksis betyr dette at behandlingsansvarlige blant annet må gjennomføre en risikovurdering og vurdere personvernkonsekvenser av en behandling hvor dette er pålagt.

Risikovurderingen kan vise om det er avvik i forhold til forordningens krav, om disse kravene integreres i behandlingen, samt at sikkerheten opprettholdes. Etablering av rutiner eller "etablering av egnede retningslinjer"[56] kan være en del av tiltak som reduserer risiko og som en del av internkontroll i virksomheten.

Risikovurderingsprosessen etter personvernforordningen kan være preget av frykt for at en uønsket hendelse resulterer i tap av omdømme og ikke minst et mulig overtredelsesgebyr i tillegg til bestemte konsekvenser som kan påvirke de registrertes rettigheter og friheter. Antakelse om omdømme kan føre til at en beskrivelse av flere mulige sikkerhetsbrudd tas i betraktning under vurdering og flere tiltak som kan tenkes å iverksette. Selv om ilagt overtredelsesgebyr kan tåles av de fleste, kan fare for omdømme øke antall risikoreduserende tiltak som vil bli iverksatt, som også forbedrer beskyttelse av de registrertes rettigheter og friheter.

[54] Jarbekk (2019) s. 127.
[55] Gimmingsrud (2017) s. 234.
[56] PVF art. 24 (2).

2.2.3 Sannsynlighet

Personvernforordningen nevner direkte sannsynlighet som et av de to parameterne for å vurdere risiko. Likevel er jeg enig med Jarbekk[57] i at det ikke alltid er hensiktsmessig å både inkludere konsekvens og sannsynlighet i en matrise der individets personvern står i fokus. Uansett sannsynlighetsgrad for en risiko relatert til den registrerte, skal tiltakene iverksettes hvis konsekvensene blir alvorlige. Sannsynligheten kan derimot bidra til bedre identifisering av mulige situasjoner som både har høy konsekvens og høy sannsynlighet, slik at de kommer øverst på virksomhetens prioriteringsliste og viser til behov for vurdering av personvernkonsekvenser.

For en personvernrettet risikovurdering er det behov for å gjennomføre vurdering ut fra den registrertes perspektiv[58] om lovlig, rettferdig og åpen behandling og det er mulig å hevde at graden av sannsynlighet er mindre relevant. Årsaken er det at det enkelte individ som er i fokus og det spiller ingen rolle for det enkelte individ om at det er lite sannsynlig at det blir brudd på den enkeltes rettigheter og friheter. Ikke minst kan katastrofale konsekvenser være farlige for den enkelte selv om det er lite sannsynlig at hendelsen inntreffer. Det er derfor mulig å gjennomføre en risikovurdering og bare å fokusere på konsekvens og ikke sannsynlighet.

Tabellen nedenfor viser et eksempel på en overordnet risikovurdering som kan gjelder for eksempel for et system:

	Konfidensialitet	**Integritet**	**Tilgjengelighet**	**Robusthet**
Katastrofal				
Stor				
Moderat				
Liten				

Figur 2 – Overordnet vurdering[59]

På bakgrunn av hvilken risiko de ulike systemene potensielt har i forhold til konsekvens, kan det gjøres en vurdering av hvilke tiltak som er nødvendig. Systemer hvor uønskede hendelser kan

[57] Jarbekk (2019) s. 131.
[58] PVF art. 24 (1).
[59] Mal er utarbeidet av Datatilsynet.

inntreffe med katastrofale konsekvenser, har trolig behov for risikoreduserende tiltak uavhengig av sannsynlighetsgrad.

Den tradisjonelle forståelsen for risikovurdering er å definere tall for sannsynlighet. Gjennom å sette et tall på sannsynligheten for at en uønsket hendelse inntreffer, definerer man hvor ofte slik hendelse kommer til å forekomme. Slike tall baserer seg som regel på tidligere historikk.
Ved manglende historikk er det også mulig å fastsette et tall på sannsynlighet ut fra kunnskap om systemet og erfaring av deltakere. Da er det viktig at forståelsen av risiko legges til grunn for prosessen.

Det er også viktig å stille spørsmål om hva som menes når man prøver å definere sannsynlighetsgrad. Forståelse av begrepet kan føre til ulike resultater: En ting er om det er antall henvendelser for en periode, en annen ting er om det er sannsynlig at en hendelse inntreffer i det hele tatt. Det er også hensiktsmessig å vurdere å ta sannsynlighet i betraktning for ulike grader av konsekvensvurderinger av den samme hendelsen, eller gjøre kun sannsynlighetsvurdering av det verst tenkelige utfallet.

Likevel nevner personvernforordningen også sannsynlighetsgrad i bestemmelsene som tillater meg å tolke bestemmelsene slik at sannsynlighetsgrad er viktig å inkludere i vurderingen av risiko også når det gjelder den enkeltes rettigheter og friheter. Dessuten pålegger forordningen ikke "risikofri" behandling og ved å ta hensyn til sannsynlighet kan virksomheten prioritere egnede risikoreduserende tiltak mer effektivt.

2.2.4 Matrise

Som hjelpemiddel til å uttrykke risikonivå og akseptkriterier benyttes ofte matriser. Matriser blir ofte presentert i et Excel-verktøy, og er ment å fungere som støtteverktøy til metoden for å gjennomføre en risikovurdering. Det er opp til hver enkel virksomhet å vurdere å bruke matrise, i og med at det ikke er noe krav etter personvernregelverket å bruke en matrise i risikovurdering. Samtidig hjelper en matrise ofte å visualisere en risikofare og definere et akseptabelt risikonivå, samt fastsette risikoreduserende tiltak.
Matrise er et verktøy som kan visualisere risiko og hjelper med å sortere disse med tanke på om det er behov for tiltak eller om en risiko kan aksepteres eller ignoreres.

Tabellen under kan benyttes for å beskrive hendelser hvor man aksepterer risikoen, som er de hvite feltene, og hendelser hvor man ikke aksepterer risikoen for, disse er de grå feltene. Det er viktig å justere akseptabel risiko i hvert enkelt tilfelle. Tiltak skal så planlegges og gjennomføres for å redusere risikoen for at uakseptable hendelser skal inntreffe, det vil si flytte hendelsene over fra grått område til hvitt område.

Konsekvens: **Sannsynlighet:**	**Liten**	**Moderat**	**Stor**	**Katastrofal**
Svært høy				
Høy				
Moderat				
Lav				

Figur 3 – Matrise som et verktøy til å uttrykke risikonivå og akseptkriterier[60]

De hvite feltene representerer akseptabel risiko, og de grå feltene representerer uakseptabel risiko.

Det er også mulig å bruke farger i matrise, der fargekoden angir prioriteringen:

- Grønn farge viser akseptabel risiko. Hendelser som er plassert i grønt område er med lav risiko og risikoreduserende tiltak er normalt ikke nødvendig.
- Gul farge viser til middels risiko. Hendelser som er plassert i gult område er med middels risiko og risikoreduserende tiltak bør vurderes.
- Rød viser til uakseptabel risiko. Hendelser som er plassert i rødt område er med høy risiko og risikoreduserende tiltak skal innføres.

Når flerfarget matrise brukes er det særlig viktig å definere området med akseptabel risiko. Etter det skal virksomheten da først håndtere de situasjonene som er oransje eller røde. Etter min mening kan fargekoden gi falsk trygghet i tilfeller når det ikke fastsettes et akseptabelt risikonivå og tiltak fastsettes avhengig av farge hendelsen plassert i matrisen. I tillegg er det ikke alle matriser setter med rødt når risiko inneholder en hendelse som er svært lite sannsynlighet og med katastrofale konsekvenser. Det kan være en personvernkonsekvenser å akseptere hendelser som potensielt har høy risiko. Mange risikovurderinger bruker bare tre inndelinger, men det blir ofte en for overfladisk inndeling. Det er også mulig å innføre en femte kategori ”ubetydelig risiko,” som den laveste risikoen.

[60] Mal er utarbeidet av Datatilsynet.

En slik matrise gir mulighet å akseptere flere uønskede hendelser og inkludere flere situasjoner når det er lite omfang av opplysninger som behandles eller det eneste som behandles er kontaktopplysninger.

Det er vanlig praksis at risiko fremstilles som tall, men det er også mulig å angi som beskrivende ord. Tallverdiene må likevel redegjøres for å kunne se svakheter, avhengigheter og utfordringer i sammenheng ved kartlegging av risikoer og sårbarheter.[61]

Det kan være en diskusjon hvorvidt det er mulig å bruke matrise som verktøy for å vurdere om behandlingen er lovlig (etter PVF art. 24) eller om det er mulig å bygge personvern inn i behandlingen (etter PVF art. 25), men den er absolutt hensiktsmessig å bruke for å vurdere sikkerhetsrisikoer etter PVF art. 32.

Å definere et risikonivå kan være krevende for de som deltar i risikovurdering. For å kunne angi nivå som er tilnærmet realiteten, forutsetter det tilgjengelighet av historiske data og erfaring samt kunnskap om behandlingen som risikovurderes. Hele personvernforordningen skal tolkes som den risikobaserte tilnærmingen og det innebærer at risikoer tas i betraktning under behandlingen av personopplysninger. Forestillingen om risiko er dermed det viktigste referansepunktet for tolkning og implementering av personvernforordningen.

Noe som kan være en ubetydelig risiko, for eksempel en lekkasje av personopplysninger som allerede er godt kjent i offentligheten eller at en type informasjon kan virke veldig ufarlig. Det vil i mange tilfeller være en ubetydelig risiko at noens navn og adresse lekker, men dersom den aktuelle personen er registrert på en hemmelig adresse, vil det likevel kunne ha stor betydning for vedkommende. Dette viser at hver situasjon må vurderes separat og ut fra den kontekst man behandler personopplysninger.

Etter at det ble definert et akseptabelt risikonivå, skal videre uønskede hendelser identifiseres. Dessuten skal årsaker, samt risikoreduserende tiltak og gjennomføringsplan beskrives. Risikohåndtering må iverksettes når avdekket risiko er høyere enn akseptabelt risikonivå. Selv om bestemmelsene som omhandler risikovurdering kun nevner tekniske og organisatoriske tiltak, er det ikke grunnlag for å avgrense tiltak til slike som kan kun klassifiseres som tekniske eller organisatoriske.[62] I tillegg bør økonomiske, pedagogiske, juridiske og andre tiltak vurderes, jf. "holdningsskapende tiltak" etter PVF art. 39 (1)(b).

[61] Bergsjø (2020) s. 191.
[62] Schartum (2020) s. 245.

2.2.5 De spesielle kravene etter PVF art. 24, 25, 32, 35

Disse fire bestemmelser angir viktige forpliktelser til å vurdere risiko og vurderingen etter bestemmelsene skal være grunnlag for iverksetting av tiltak.

Selv om det er samme formuleringen i ulike bestemmelser, er risikovurdering noe som skal gjennomføres ved å ta ulike hensyn. Etter PVF art. 24 er risikovurdering nødvendig for å se om behandlingen er lovlig. PVF art. 25 forutsetter at risikovurdering sikrer innebygd personvern og personvern som standardinnstilling. PVF art. 32 viser til risikovurdering som er nødvendig for oppnåelse av et egnet sikkerhetsnivå i behandlingen av personopplysninger. PVF art. 35 (7)(c) sier eksplisitt at *"en vurdering av risikoene"* skal være en del av vurdering av personvernkonsekvenser.

Videre skal jeg presentere de spesielle kravene etter hver bestemmelse i personvernforordningen som regulerer en risikovurdering.

2.2.5.1 Den behandlingsansvarlige ansvar etter PVF art. 24

Bestemmelse om behandlingsansvarliges ansvar er mest omfattende når det gjelder hvilke risikoer som skal tas i betraktning og hva som skal risikovurderes. Artikkel 24 handler om behandlingsansvarliges ansvar og er knyttet til PVF art. 5 (2). Ansvarsprinsippet handler om ansvarlighet etter PVF art. 5 at behandlingsansvarlig og databehandler tar ansvar for personopplysningene de behandler. PVF art. 24 beskriver den behandlingsansvarliges ansvar gjennom krav til at behandlingsansvarlig vurderer og iverksetter passende og effektive tiltak for å sikre og påvise overholdelse av prinsippene og forpliktelsene angitt i personvernforordningen.[63]

Ansvarsprinsippet går som en rød tråd gjennom hele forordningen og pålegger at den behandlingsansvarlige skal sikre etterlevelse av kravene i personvernforordningen. I praksis betyr det at en risikovurdering skal avdekke risiko for at forordningen ikke etterleves, og en risikovurdering skal dekke alle bestemmelsene som er rettet mot behandlingsansvarlige. Bestemmelsen viser overordnet til risikovurderingen som skal ta utgangspunkt i behandlingen og basere seg på risikoer for fysiske personers rettigheter og friheter. Bestemmelsen gjelder kun den behandlingsansvarlige og gjelder *sikring* av "samsvar med denne forordningen". *Sikring* av samsvar skal skje gjennom å treffe tiltak, og tiltakene "skal omfatte utarbeidelse av retningslinjer", jf. PVF art. 24 (2). *Påvise* samsvar kan innebære å dokumentere at risikovurdering er gjennomført og tiltakene er truffet. Overholdelse av godkjente atferds- og sertifiseringsnormer kan brukes også for å påvise samsvar, se PVF art. 24 (3). Ansvarsprinsippet overlater friheten å definere

[63] WP29 (2010) s. 4.

tilfredsstillende tiltak til behandlingsansvarlig, med forbehold om muligheten til enhver tid å bli bedt om å demonstrere etterlevelse av kravene.

Forordningen nevner kun ”tekniske og organisatoriske tiltak” som kreves i henhold til prinsippet om ansvarlighet, og presiserer kun at tiltakene må være "egnede”. Jeg antar at det ikke er nødvendig å begrense tiltakene til kun tekniske og organisatoriske. Forordningen viser til holdningsskapende tiltak, jf. PVF art. 39 (1) (b), men det er mulig å tenke at man kan iverksette andre typer tiltak, så lenge de fører til at behandlingen skjer i samsvar med forordningen. Fortalepunkt 74 forklarer at "sannsynligheten for og alvorlighetsgraden av risikoen for de registrerte rettigheter og friheter bør bestemmes med henvisning til behandlingens art, omfang, kontekst og formål, det vil si at resultatet av risikovurderingen må ses i sammenheng med behandlingen som planlegges. Og tiltakene skal være “egnede og effektive” og skal defineres basert på den vurderingen.

Fortalepunkt 75 presiserer at risikoen "kan være resultatet av behandling av personopplysninger som kan føre til fysisk, materiell eller ikke-materiell skade". Fortalepunkt inneholder en omfattende liste over eksempler på behandling som kan føre til slike risikoer, og som derfor bør huskes.

Fortalepunkt 77 viser til kartlegging av risikoer og nevner at risikovurdering skal ta hensyn til risikoens “opprinnelse, art, sannsynlighet og alvorlighetsgrad”. Det styrker tolkning om at risikovurdering skal være skriftlig for at behandlingsansvarlig kunne påvise overholdelse av personvernforordningen.

Tiltak som følger av gjennomføring av risikovurdering “skal gjennomgås på nytt og oppdateres ved behov”, jf. PVF art. 24 (1). Jeg tolker det slik at risikovurderingen som er grunnlag for tiltak også skal gjennomføres på nytt for å se om det er endring i risikobildet og om det er behov for endring av tiltak.

Risiko av varierende sannsynlighets- og alvorlighetsgrad viser til at en metode for risikovurdering skal inneholde begge kriterier. Bestemmelsen viser også til mulige eksempler på tiltak, men det er viktig at disse “står i et rimelig forhold til behandlingsaktiviteter”, altså retningslinjer skal være “egnede” til typen behandling.

Jeg tolker formuleringen om å ta hensyn til “behandlingens art, omfang, formål og sammenhengen den utføres i” som et krav til at utgangspunktet skal tas i behandlingen og ikke i systemet personopplysningene behandles i. Det skal foretas en risikovurdering hvor forholdene ved behandlingen og risikoen ved denne (altså sannsynligheten for brudd i forhold til konsekvensene

ved brudd) skal vurderes mot personvernhensynet til de registrerte. Med andre ord skal en risikovurdering vise om behandlingen er lovlig, at prinsipper for behandling av personopplysninger gjennomføres og at personopplysningssikkerhet opprettholdes.

PVF art. 24 inneholder kun krav som retter seg mot behandlingsansvarlig, men tar hensyn til alle stadier i behandlingen, fra begynnelse til slutt.[64]

Bestemmelsen gir ingen henvisninger til når risikovurdering skal skje.

2.2.5.2 Innebygd personvern og personvern som standardinnstilling etter PVF art. 25

Bestemmelse om innebygd personvern og personvern som standardinnstilling er bygd opp slik at en samlet vurdering av forholdene som inkluderer risikoene danner grunnlag for nødvendige tiltak for "å integrere de nødvendige garantier i behandlingen". Jeg tolker denne bestemmelsen slik at en risikovurdering ligger til grunn for å kunne oppfylle kravene i forordningen etter PVF art. 25. En slik risikovurdering skal kun behandlingsansvarlig gjennomføre. I tillegg til at det er fastsatt et tidspunkt for risikovurdering. Som i bestemmelsen om behandlingsansvarliges ansvar etter PVF art. 24, skal en risikovurdering inkludere sannsynlighets- og alvorlighetsgrad, samt risiko for fysiske personers rettigheter og friheter. Risikovurderingen skal også ta hensyn til behandlingens kontekst: Art, omfang og sammenhengen den utføres i, slik som PVF art. 24 forutsetter. Men kravet om innebygd personvern legger også til grunn den tekniske utviklingen og gjennomføringskostnadene. Teknisk utvikling, kostnadene som er nødvendige for gjennomføring, og risikoene er blant de faktorene som er avgjørende for å definere hvilke konkrete tiltak skal fastsettes for å oppfylle kravet til innebygd personvern og personopplysningssikkerhet. I praksis betyr det at det er avgjørende for risikovurdering å følge med på den tekniske utviklingen og diverse moderne teknologi og se på behandlingens art som dynamisk konsept[65]. Slik som for eksempel bruk av systemer som ikke er i stand til å integrere etterlevelse av krav[66], øker kraftig risiko. Det er likevel alltid en avveining mellom mulighet til å bruke moderne teknologi og kostnadene som følger med gjennomføringen en bedrift kan bruke. Ved planlegging av tiltak som er nødvendige for å senke risiko til akseptabelt nivå er det behov å definere balansen mellom den tekniske utviklingen og omkostningene bedriften kan tåle. Etter min tolkning skal systemene personopplysningene behandles i tas i betraktning i en risikovurdering, samt personvernprinsipper og rettighetene etter kap. III i forordningen. Resultatet av risikovurdering skal vise til hvilke tiltak som er egnede og som kan bidra til "effektiv gjennomføring av prinsippene" og for å "integrere de nødvendige garantier i behandlingen".

[64] Kuner (2020) s. 560.
[65] EDPB (2019) s. 8.
[66] For eksempel manglende muligheten for de registrerte å gjøre innsyn eller sletting av personopplysninger er kun mulig manuelt og ikke automatisk.

Bestemmelsen definerer planleggingsfasen som et passende tidspunkt for gjennomføring av risikovurdering,[67] samt peker på at tiltak skal gjennomføres også under behandlingen.[68] Dette betyr at en risikovurdering som gir grunnlag for tiltak skal være gjennomført før behandlingen starter.

2.2.5.3 Sikkerhet ved behandlingen etter PVF art. 32

Bestemmelsen om sikkerhet ved behandlingen gir mer detaljerte regler vedrørende risikovurdering, jf. PVF art. 32(2). Bestemmelsen stiller krav til både behandlingsansvarlig og databehandler og er knyttet til prinsippet om integritet og konfidensialitet, jf. PVF art. 5(1)(f). Bestemmelsen er bygd opp slik at den representerer veksling mellom tiltak for å oppnå et sikkerhetsnivå, sikkerhetsobjekt, evner til å sikre og risikoer. Jeg antar at de behandlingsansvarlige og databehandlere som har gjennomført en risikovurdering før personvernforordningen trådte i kraft, kjenner igjen kravene etter den bestemmelsen ved å trekke paralleller til personopplysningsforskriften fra 2000.

PVF art. 32 pålegger den behandlingsansvarlige å oppnå et sikkerhetsnivå gjennom å iverksette tekniske og organisatoriske tiltak som er "egnet" for risikoen ved behandlingen av personopplysninger. For å etterleve disse kravene, må man først identifisere og vurdere de spesielle risikoer som blir presentert av databehandlingen, det vil si gjennomføre en risikovurdering. Ettersom bestemmelsen har fokus på personopplysningssikkerhet er det sikkerhetstiltak som skal bidra til et egnet sikkerhetsnivå i behandlingen.

Bestemmelsen gir en liste over kriterier som skal tas i betraktning og viser til eksempler på sikkerhetstiltak som er blant de som kan bidra til å oppnå et egnet sikkerhetsnivå. Listen er ikke-uttømmende, dette kommer frem gjennom uttrykket "herunder blant annet". PVF art. 32 (2) spesifiserer videre de risikoene som er viktig å ta hensyn til ved en risikovurdering. Det er de risikoene som regnes som mest sannsynlige og alvorlige som må reduseres gjennom tiltak.[69] Disse eksemplene viser noen likhetstrekk med kriteriene som skal brukes for å bestemme om det skal utføres en vurdering av personvernkonsekvenser (DPIA[70]) i henhold til PVF art. 35 GDPR, og Artikkel 29-gruppen har understreket viktigheten av sikkerhet i sammenheng med DPIA.[71] PVF art. 32 (2) er knyttet til en av personvernprinsippene som handler om tilstrekkelig sikkerhet for personopplysninger, jf. PVF art. 5 (1)(f).

[67] PVF art. 25: "På tidspunktet for fastsettelse av midlene".
[68] PVF art. 25: "På tidspunktet for selve behandlingen".
[69] Kuner (2019) s. 636.
[70] Forkortelse etter engelsk Data Protection Impact Assessment.
[71] WP29 (2017).

Fortalepunkt 83 henviser til risikovurdering som nødvendig for å opprettholde personopplysningssikkerheten og en lovlig behandling av personopplysninger. I tillegg kommer det frem i fortalepunktet at under en risikovurdering bør det tas hensyn til tilgjengelighet, integritet og konfidensialitet og de risikoene som "særlig kan føre til fysisk, materiell eller ikke-materiell skade".

Personopplysningssikkerhet forutsetter risikostyring, det vil si sikring av opplysninger. I utgangspunktet går risikostyring ut på at blant annet systemene der opplysningene behandles skal være sikre nok i forhold til akseptabelt risikonivå som er satt. For å vurdere risikonivå, er det behov for å se på behandlingens art, omfang, formål og ikke minst sammenhengen den utføres i, men inkluderer også hensyn til den tekniske utviklingen og gjennomføringskostnadene.

Det som er spesielt for PVF art. 32 er at risikovurderingen som gjennomføres skal ta utgangspunkt i risikoen for tap, uautorisert endring, eller tilgang til personopplysninger mv, det vil si uønskede hendelser som fører til brudd på konfidensialitet, integritet, tilgjengelighet eller robusthet. Etter at sikkerhetsrisiko blir identifisert er det behov for iverksettelse av sikkerhetstiltak som en formildende respons. Ordet "egnede" brukes flere ganger i PVF art. 32 (1): "... skal den behandlingsansvarlige og databehandleren gjennomføre *egnede* tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er *egnet* med hensyn til risikoen, herunder blant annet, alt etter hva som er *egnet*. Dette indikerer at behandlingsansvarlig og databehandler først må identifisere risikoer.[72]

Etter at en risikovurdering er gjennomført, må virksomheten treffe tiltak for å sørge for at sikkerhetsnivået opprettholdes. PVF art. 32 gir eksempler på tiltak som kan bidra til å oppnå "et sikkerhetsnivå som er egnet".[73] Listen er ikke uttømmende, og dette kan også innebære menneskelige tiltak, for eksempel opplæring og kulturbygging. Det kan også være tekniske tiltak, for eksempel logging og kryptering, eller organisatoriske tiltak, for eksempel ansvarsfordeling, rutiner eller prosedyrer. Tiltakene skal senke risikoen, men også være forebyggende eller oppdagende.[74] Tiltakene skal være kostnadseffektive, jf. begrepet "gjennomføringskostnadene". En oversikt over truslene som oppdages ved en risikovurdering gir også mulighet for å identifisere trusselaktørene. Det hjelper når det er nødvendig å fastsette hvilke tiltak som kan bidra til å redusere risiko.

[72] Kuner (2019) s. 635.
[73] PVF art. 32(1)(a): "Pseudonymisering og kryptering".
[74] Bergsjø (2020) s. 122.

Å opprettholde et egnet sikkerhetsnivå er relevant for både behandlingsansvarlig og databehandler. Personvernforordningen viser koblingen med disse to rollene, og begge to skal gjennomføre sikkerhetsrelatert, inkludert egnede tiltak. Koblingen mellom de to rollene og samarbeid mellom dem vises gjennom databehandleravtale-ordningen, jf. PVF art. 28. Databehandleravtaler som regulerer forholdet mellom disse rollene skal inneholde krav om at databehandleren treffer tiltak som er nødvendig i henhold til PVF art. 32, jf. PVF art. 28 (3) (c). I tillegg skal databehandler også bistå ved overholdelse av forpliktelsene i henhold til bl.a. PVF art. 32, jf. PVF art. 28 (3) (f). I forbindelse med dette vil en behandlingsansvarlig ofte ha behov for bistand fra sine databehandlere for å gjennomføre en risikovurdering.

Bestemmelsen gir ikke klar henvisning til tidspunktet for gjennomføring av en risikovurdering.

2.2.5.4 Vurdering av personvernkonsekvenser etter PVF art. 35

Artikkel 35 fokuserer på innvirkningen på personopplysningsvern for behandlingen av personopplysninger. Artikkel 35 viser til mer en omfattende risikovurderinger og har fokus på "høy risiko" i behandlingen. Bestemmelsen understreker at vurderingen skal gjennomføres i planleggingsfasen og før behandlingen starter og gir klare eksempler når slik vurdering er absolutt nødvendig, for eksempel "ved bruk av ny teknologi" eller ved automatiserte individuelle avgjørelser eller behandling av store mengder av særlige kategorier av opplysninger, jf. PVF art. 35 (3). Basert på de nevnte eksemplene antar jeg at vurdering av personvernkonsekvenser er særlig aktuelt for offentlig sektor.

Hovedregelen er at det er et krav til å foreta en vurdering av personvernkonsekvenser, ofte også kalt DPIA, hvis behandlingen av personopplysningene medfører en høy risiko for rettighetene eller frihetene til den registrerte. Vurderingen etter PVF art. 35 begrenser seg ikke kun til de tilfellene bestemmelsen viser til, og det er heller ikke nok å sjekke en liste fra Datatilsynet som definerer hvilke andre behandlingen krever slik vurdering. Personvernforordning har pålagt (jf. ordet "skal") tilsynsmyndigheter å utarbeide en liste over behandlingsaktiviteter som omfattes av kravet om vurdering av personvernkonsekvenser, jf. 35 (4). I tillegg er personvernforordningen åpen for (jf. ordet "kan") at tilsynsmyndigheter utarbeider en liste over behandlingsaktiviteter som ikke fører til slik vurderingen, jf. PVF art. 35 (5).

En risikovurdering etter PVF art. 24, 25 eller 32, eventuelt etter en samlet vurdering avhengig av hvordan en virksomhet organiserer sitt arbeid knyttet til en risikovurdering, viser at hele behandlingen eller noen aktiviteter i behandlingen medfører en høy risiko er grunnlag til vurdering etter PVF art. 35. Dette innebærer at en vurdering av risikoer uansett er en del av vurderingen av personvernkonsekvenser, se PVF art. 35 (7) (c). I tillegg finnes det noen situasjoner hvor Artikkel

29-gruppen[75] har angitt at det bør gjennomføres en slik vurdering. WP29 har utgitt en egen veileder om når og hvordan vurderingen etter PVF art. 35 skal gjennomføres.[76]

Fortalepunkt 76 nevner også at risikovurdering som "en objektiv vurdering der det fastslås om behandlingen av personopplysningene innebærer en risiko eller en høy risiko". Ved å avgrense mellom en ordinær risiko og høy risiko, kobles på den måten andre artiklene som handler en risikovurdering til art. 35. Personvernforordningen definerer rammer for vurderinger av personvernkonsekvenser og gir relativt klare eksempler på situasjoner når en slik vurderingen er nødvendig.

Den generelle referansen til "fysiske personers rettigheter og friheter" betyr at vilkårene som gjør det nødvendig å gjennomføre en vurdering av personvernkonsekvenser, gjelder også andre grunnleggende rettigheter og friheter, som frihet til uttrykk eller bevegelsesfrihet, ikke bare personopplysningsvernet.[77]

Bestemmelsen gir klare regler om at vurdering skal foretas før behandlingen starter. Når vi snakker om risikovurderinger for å vurdere risikoen for informasjonssikkerhet, er dette ofte koblet mot beskyttelse av verdier. Innen personvern er den verdien som skal beskyttes de registrertes rettigheter og friheter. I delkapittelet nedenfor vil jeg redegjøre nærmere for informasjonssikkerhet i tilknytning til risikovurderinger.

2.3 Informasjonssikkerhet

Jeg ønsker å redegjøre for informasjonssikkerheten separat, fra det avsnittet som handler om rettslige kravene til risikovurderingen etter PVF art. 32, på grunn av en spesiell karakter av fenomenet informasjonssikkerhet som er mer omfattende enn personopplysningssikkerhet. Risikovurdering knyttes ofte til informasjonssikkerhet, både når det gjelder personopplysninger og annen informasjon, for eksempel bedriftens hemmeligheter. I praksis betyr det at det er systemet som risikovurderes med utgangspunktet av omfanget av informasjon systemet behandler.

Typiske årsaker som fører til uønskelige hendelser er fortsatt menneskelig svikt. Dette kan eksempelvis være vedlegg som åpnes av en ansatt som fører til brudd på både tilgjengelighet, konfidensialitet, integritet og robusthet. Også dårlige rutiner og utilstrekkelig tilgangskontroll kan føre til brudd på informasjonssikkerheten. Samtidig at for strenge sikkerhetskrav til pålogging og/eller registrering, kan også føre til slurv med bruk av systemet. For eksempel hvis det er

[75] Forkortet WP29, den ble erstattet med European Data Protection Board (EDPB) etter 25. mai 2018.
[76] WP29 (2017).
[77] Kuner (2020) s. 671.

vanskelig for en bruker å registrere seg eller være pålogget i et system og rutinene for sikkerhet oppleves som et unødvendig styr, kan det føre til at påloggingsinformasjon kan deles mellom flere brukere.

Informasjonssikkerhet kan møte utfordringer både internt og eksternt. Eksempel på ekstern trussel er hackerangrep, mens utro medarbeiderne og manglende kompetanse er et eksempel på intern trussel.

Risikovurderinger innen informasjonssikkerhet krever IT-sikkerhetskompetanse og forståelse av hvilke svakheter systemet som risikovurderes har. Teknisk kompetanse bidrar til iverksetting av tilfredsstillende tiltak som redusere risiko og oppnår ønskelig sikkerhetsnivå i en prosess og et system samt tilhørende prosedyrer, rutiner og retningslinjer.

Systemer er ofte koblet sammen og overfører opplysninger. En svakhet i et system kan føre til brudd av informasjonssikkerhet i alle andre systemer. For å lage en god risikovurdering av komplekse systemer er det helt grunnleggende at det finnes en oversikt over opplysningene som behandles i systemet og at det er en forståelse av hvordan systemene kommuniserer med hverandre, samt hvilke svakheter systemene har.

Sikkerhet kan defineres som en tilstand med fravær av uønskede hendelser, frykt og fare.[78] En risikovurdering er nødvendig for å ha oversikt over mulige uønskede situasjoner og redusere risiko til et akseptabelt nivå, samt tiltak som bidrar til dette. Målene med tiltakene i informasjonssammenheng kalles sikkerhetsmål, og innen informasjonssikkerhet er konfidensialitet, integritet og tilgjengelighet viktige mål.

Informasjonssikkerheten og personvern er to begrep som ofte er avhengig av hverandre. Hvis en uønsket hendelse fører til brudd på informasjonssikkerheten i systemet som behandler personopplysninger, er det ofte brudd på personopplysningssikkerheten også. Dette går også andre veien, når personvernet blir svekket, er det ofte et system som er involvert i avvik og det er manglende sikkerhetstiltak som igjen førte til dårlig personvern. Informasjonssikkerhet handler om vern av alle typer informasjon mot uautorisert utlevering, endring eller tap. Kjernen er at informasjonen skal beskyttes mot uautorisert bruk. Personopplysningsvern handler om sikring av konfidensialitet, integritet, tilgjengelighet og robusthet.[79]

[78] NS 5830: 2012.
[79] Bergsjø (2020) s. 112.

Konfidensialitet knyttes ofte til informasjon som er underlagt taushetsplikt. Innen informasjonssikkerhet er det et mål at opplysninger ikke blir kjent for uvedkommende. Snoking er et eksempel på brudd på konfidensialitet. Tilgangsstyring og sterk autorisering er eksempel på tiltak for å oppnå konfidensialitet.

Videre knyttes ofte *integritet* til noe eller noen vi kan stole på. Innen informasjonssikkerhet er det et mål å verne opplysninger mot uønsket endring. Kryptering og sikkerhetskopiering er eksempel på sikkerhetstiltak for å oppnå god integritet.

Tilgjengelighet knyttes ofte til tilgang til noe når det er behov for det. Innen informasjonssikkerhet er det et mål at informasjonen er tilgjengelig for autoriserte når det er behov. Utløpt sertifikat som gjør systemet utilgjengelig er eksempel på brudd av tilgjengelighet. Sikkerhetskopiering er eksempel på tiltak for å oppnå tilgjengelighet.

Robusthet knyttes ofte til evnen til å tåle påkjenninger og stress som kan føre til skader og tap.[80] Innen informasjonssikkerhet er det et mål at systemer er i stand til å motsette seg for eksempel stor overlasting. Planlegging av design og arkitektur som kan tåle slike påkjenninger er eksempel på tiltak som bidrar til robusthet.

Uønskede hendelser vil i de fleste tilfeller være knyttet til at uvedkommende får tilgang til informasjon (brudd på konfidensialitet), at uvedkommende sletter eller endrer informasjon (brudd på integriteten) eller at informasjonen ikke er tilgjengelig for rettmessige brukere (brudd på tilgjengeligheten) samt tapte opplysninger som resultat av et ikke bærekraftig system (brudd på robusthet). Brudd på informasjonssikkerheten skjer når systemet utsettes for dataangrep, at utenforstående får tak i brukernavn og passord eller at noen kan urettmessig endre eller slette personopplysningene. Det er hensiktsmessig at virksomheten gjennomfører en risikovurdering i eksempelvis en workshop for å gå gjennom hva slags uønskede hendelser det er relevant å liste opp i en risikovurdering.

På informasjonssikkerhetsområdet er det ofte samme kategorier av uønskede hendelser som er relevant å huske på under flere risikovurderinger. Uønskede hendelser kan variere, men de knyttet ofte blant annet til rutinebrudd, pålogging, dataangrep eller sikkerhetskopiering. Risikoer som er relevante for den eller andre kategorier er ofte lik for flere vurderinger. Rutinebrudd kan føre til at personopplysninger kommer på avveie eller snoking i opplysninger. Risikoen som er knyttet til pålogging er ofte passord som deles med uvedkommende.

[80] Store norske leksikon (2020).

2.4 Samlet perspektiv

En risikovurdering er helt nødvendig å gjennomføre for de som behandler personopplysninger. Både fordi en risikovurdering gir et grunnlag for andre forpliktelser, men også fordi den bidrar til en helhetlig oversikt over behandlinger som skjer i virksomheten og at behandlingen skjer i tråd med regelverket.

Hver enkelt virksomhet kan fritt velge selv hvilken fremgangsmåte de vil bruke for å gjennomføre en risikovurdering, forutsatt at vurderingen skjer innen lovpålagte rammer. Denne friheten gir mulighet for å tilpasse prosessen etter virksomhetens behov og ressurser. Det som kan være utfordrende for virksomheten å skifte fokus fra informasjonssikkerhetsperspektivet, hvor det er bedriftens egne verdier som skal sikres, til den registrertes perspektiv hvor det er verdiene ”grunnleggende rettigheter og friheter” som skal sikres. Det er også viktig å huske på at det er selve behandlingen av personopplysninger som skal risikovurderes og ikke selve system som brukes for å behandle personopplysninger.

Det er mulig å gjennomføre en risikovurdering etter hver enkelt bestemmelse jeg har presentert i dette kapittelet, og virksomheten kan også velge å foreta en samlet vurdering av risiko ved å ta i betraktning alle bestemmelser på en gang.

Et åpent spørsmål er hvorvidt en matrise er et behjelpelig verktøy for vurdering av risiko etter andre bestemmelser enn personopplysningssikkerhet. Også hvorvidt sannsynlighetsgraden som skal være en del av vurderingen i de tilfellene der lovlighet av behandlingen eller integrering av prinsippene i løsningen, bør vurderes. Som tidligere nevnt kan det ha katastrofale følger for den registrerte hvis en uønsket hendelse inntreffer, selv om sannsynlighetsgraden for at denne hendelsen inntreffer er ”lav”.

Det er fortsatt slik at informasjonssikkerhet er mer knyttet til risikovurdering enn andre perspektiver som behandlingens lovlighet og innebygd personvern. Det at de fleste standarder og veiledninger viser til risikovurdering av informasjonssikkerhet kan føre til en feil forståelse av regelverket og falsk trygghet for at virksomheten etterlever kravene.

I neste kapittel vil jeg beskrive undersøkelsen jeg har gjennomført basert på et praktisk eksempel av en risikovurdering. Videre vil jeg se nærmere på hvordan kravene i personvernforordningen faktisk blir forstått, og implementeres i virkeligheten.

3. En case-studie av Statens vegvesens risikovurdering av et arkivsystem

3.1 Innledning

I dette kapittelet vil jeg presentere Statens vegvesens risikovurdering av arkivsystemet Mime 360. Undersøkelse omfatter analyse av blant annet hvilken metodikk som er anvendt i risikovurdering, hvordan arbeidet ble organisert, hvem som var med på arbeidet med videre. Analysen er basert på gjennomføring av flere intervjuer og gjennomgang av relevante dokumentasjon og verktøy som viser noe om gjennomføringen av risikovurderingen.

3.2 Om Statens vegvesens organisering, oppgaver og deltakelse i en risikovurdering

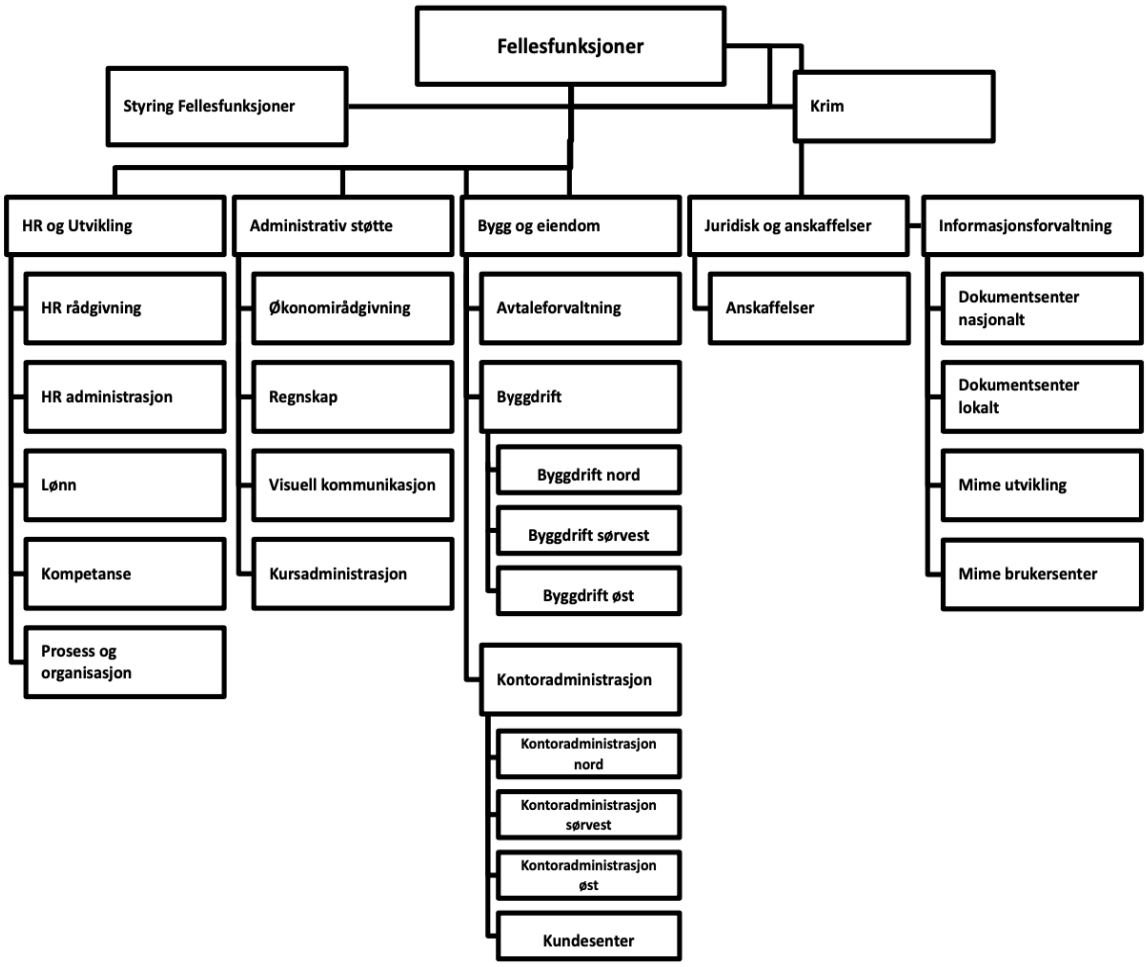
Statens vegvesen har nasjonalt ansvar for beredskap på veiene i Norge og for gjennomføringen noen av Norges største samferdselsprosjekter, samt mindre prosjekter som har stor betydning for samfunnet. I forbindelse med dette lager Vegvesenet et helhetlig, enkelt og sikkert transportsystem, uavhengig av hvem som eier eller drifter veien.[81]

Statens vegvesen består av ett Vegdirektorat og seks divisjoner:

Figur 4 – Statens Vegvesens organisasjonskart

[81] Statens vegvesen (2020).

Det er divisjonen «Fellesfunksjoner» som har ansvar for Mime 360. Divisjonen dekker funksjoner med tilhørende oppgaver, tjenester og leveranser ut mot alle enheter i Statens vegvesen.



Figur 5 – Organisering av divisjonen som har ansvar for Mime 360

I divisjon "Fellesfunksjoner" er avdelingene «Informasjonsforvaltningen» og seksjonen «Mime utvikling» som har foretatt risikovurderingen.

For å utøve sine oppgaver har Statens vegvesen utviklet en omfattende IKT-infrastruktur, hvor det inkluderes et stort antall systemer: Ulike selvbetjeningsløsninger, driftssystemer og andre transporttjenester. Statens vegvesen er ansvarlig for applikasjoners funksjonalitet. Statens vegvesen bestemmer ofte formålet med behandlingen og midlene for behandlingen i ulike systemene. Da må Statens vegvesen som behandlingsansvarlig gjennomføre en risikovurdering av behandlingen og systemet behandlingen skjer i. Statens vegvesens kompliserte infrastruktur fører til at det er nødvendig å ha oversikt over de ulike systemene og de forskjellige vurderingene som blir gjort i tilknytning til behandling av personopplysninger. Dette gjøres ved å ta i utgangspunkt

i kravene i personvernforordningen. Vegvesenet bruker et IT-system som gir en fullstendig oversikt over alle behandlingsaktiviteter og IT-løsninger som er både verdivurdert og risikovurdert. Delsystemer som inkluderes i det overordnet systemet bidrar til etterlevelse av personvernkravene.[82]

3.3 Om Mime 360

Mime 360 er Statens vegvesen sitt arkiv- og saksbehandlingssystem som ble innført i 2015. Mime 360 er basert på et hyllevaresystem (Public 360) med noen få tilpasninger for Statens vegvesen. Alle offentlige etater er pålagt å benytte systemer som er NOARK godkjente.[83] NOARK er en norsk standard for dokumentasjonsforvaltning. Memi 360 er et NOARK-godkjent system.

Statens vegvesen har utviklet et sett med gjenbrukbare integrasjonstjenester som fagsystemer kan ta i bruk for å «snakke» med saksarkivløsningen Memi 360. På denne måten har Memi 360 mange integrasjoner med andre fagsystemer. Enkelte fagsystemer håndterer journalpliktig dokumentasjon og bruker integrasjonstjenestene for å bl.a. lagre til Memi 360. Memi 360 inneholder all journalpliktig informasjon og det betyr at løsningen også inneholder personopplysninger. All dokumentasjon fra Memi 360 er ute på offentlig journal. Det er svært viktig at Statens vegvesen har kontroll på informasjonen som legges ut på offentlig journal. Derfor er det viktig med sikre systemer og ha gode kontrollrutiner.

Regelverket for offentlige arkiv er arkivlov med forskrifter. Alle inn- og utgående dokumenter og alle notater med høy dokumentasjonsverdi skal journalføres i sakarkivløsningen. Offentliglova og arkivlova legger premisser for allmennhetens innsynsrett og arkivplikt.

M360 ble risikovurdert for første gang før systemet ble tatt i bruk. Systemet ble risikovurdert på nytt etter at personvernforordningen trådte i kraft. Videre skal jeg beskrive siste risikovurdering av Memi 360.

3.4 Organisering av risikovurderingen og metode for risikovurderingen av Memi 360

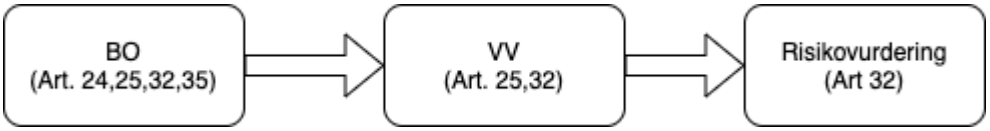
3.4.1 Innledning

Nedenfor følger en beskrivelse av organiseringen av risikovurderingen som er felles for alle systemer i Statens vegvesen. Risikovurderingen av Memi 360 har fulgt denne organiseringen og

[82] Fra intervju med Statens vegvesens personvernombudet.
[83] Forskrift om offentlege arkiv §11.

fraviker ikke fra beskrevet metode. Selv om det kommer en generell beskrivelse av metode, kommer jeg med presiseringer og eksempler som er relevant for caset.

Statens vegvesen bruker to IT-systemer som verktøy som formidler innebygd metode for risikovurderingen. Disse IT-systemene legger til rette for en fremgangsmåte som vil bli beskrevet nedenfor i oppgaven. Nedenfor følger en visualisering av fremgangsmåte for risikovurderingen. Risikovurderingen starter ved kartlegging av behandlinger i systemet Behandlingsoversikten.[84] I Verdivurdering[85] skjer registrering av alle IT-løsninger. Registreringsprosessen avsluttes med en risikovurdering av informasjonssikkerheten i systemet. Nedenfor følger en figur som viser en fremgangsmåte med henvisning til de aktuelle bestemmelsene i forordningen. Risikovurderinger av Memi 360 har skjedd i samsvar med Vegvesenets metode.



Figur 6 – Fremgangsmåte av risikovurderingen

Videre skal jeg redegjøre for fremgangsmåten av risikovurderingen. Redegjørelse inkluderer beskrivelse av verktøyer og metoden inkludert arbeidsoppgaver og avhengigheter og iterasjoner som eksisterer i prosessen.

3.4.2 Kartlegging av behandlinger

3.4.2.1 Om verktøyet

Et system med navnet som Behandlingsoversikten brukes for å holde oversikt over alle behandlingsaktiviteter og erstatter den vanlige måten å føre protokoll med Excel-filer. Det som kreves etter PVF art. 30, det vil si protokoll, er en del av Behandlingsoversikten. Systemet viser grafisk visualisering av behandlinger og personopplysninger som behandles samt det rettslige grunnlaget for behandling. Behandlingsoversikten er koblet til prosesser som skjer i Statens vegvesen, som for eksempel utsendelse av førerkort. I tillegg er hver prosess knyttet til et IT-system som behandler opplysningene. Behandlingsoversikten inneholder også en kobling til risikovurdering av systemer som behandler opplysningene. Behandlingsoversikten har som formål å dokumentere behandlingen av personopplysninger. I systemet registrertes både behandlinger der Statens vegvesen er behandlingsansvarlig og databehandler. Eksempel på at Statens vegvesen er databehandler er behandling av prikkbelastningen som registreres i et sentralt register i Statens vegvesen. Politi er da behandlingsansvarlig for behandlingen, mens Statens vegvesen er

[84] Forkortet BO i tabeller.
[85] Forkortet VV i tabeller.

databehandler som behandler personopplysninger på vegne av politiet. Ved utviklingen av spørsmålene som besvares under registreringen av behandlingen er det tatt utgangspunkt i forordningen og veiledninger fra Datatilsynet. Vegvesenet har også sett på hva andre etater har utarbeidet for å få innspill.

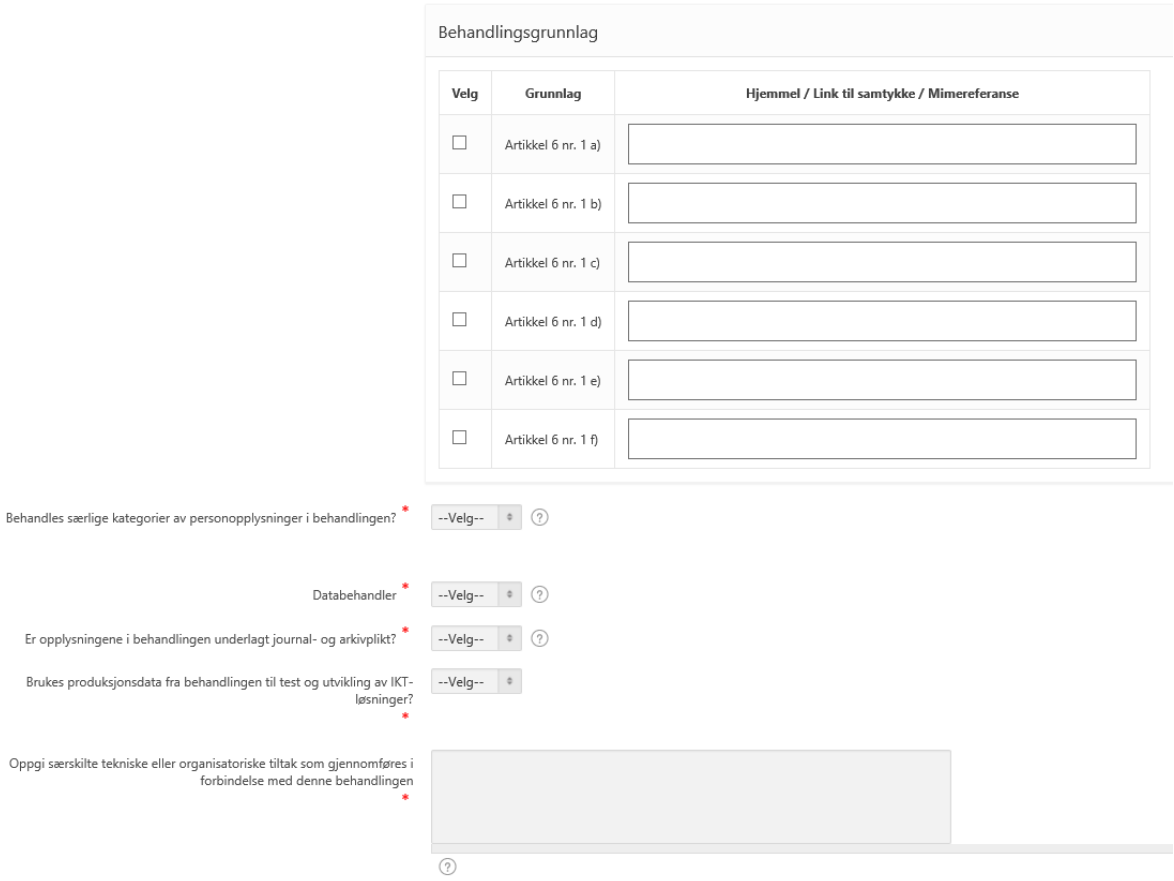
Figur 7 – Hovedelementene Behandlingsoversikten består av

Videre vil jeg gjennomgå arbeidsprosesser som er knyttet til systemet Behandlingsoversikten i den grad er det aktuelt for metode av risikovurderingen, og hvilke prosesser og aktiviteter som inngår i dette systemet.

3.4.2.2 Registreringsprosess

Det er prosesseier som er ansvarlig for å registrere og holde oppdatert prosess og behandlinger denne prosessen innebærer. Prosesseier kan redigere sin prosess, men alle medarbeidere har kun lesetilgang til Behandlingsoversikten ved behov.

Hele risikovurdering av Memi 360 begynte med registrering av en ny behandling i Behandlingsoversikten. Registreringen er bygd opp slik at Behandlingsoversikten har listet mulige typer av personopplysninger som behandles og IT-løsninger som involveres. På den måten utelukker systemeier varierende beskrivelse av like behandlingene. Det er likevel mulig å registrere ny prosess i systemet. Ny behandlingsaktivitet registreres på den måten at prosesseier svarer på spørsmål, fyller ut informasjon eller velger gjeldende informasjon som er listet på forhånd. Slik registrering tilsvarer ikke kun kravene etter PVF art. 30, men omfatter også registrering av andre aspekter som påvirker etterlevelse av krav etter andre bestemmelser. Et eksempel er spørsmål om arkivplikt eller om personopplysninger benyttes for et annet enn opprinnelig formål eller om personopplysningene overføres utenfor EØS-området.

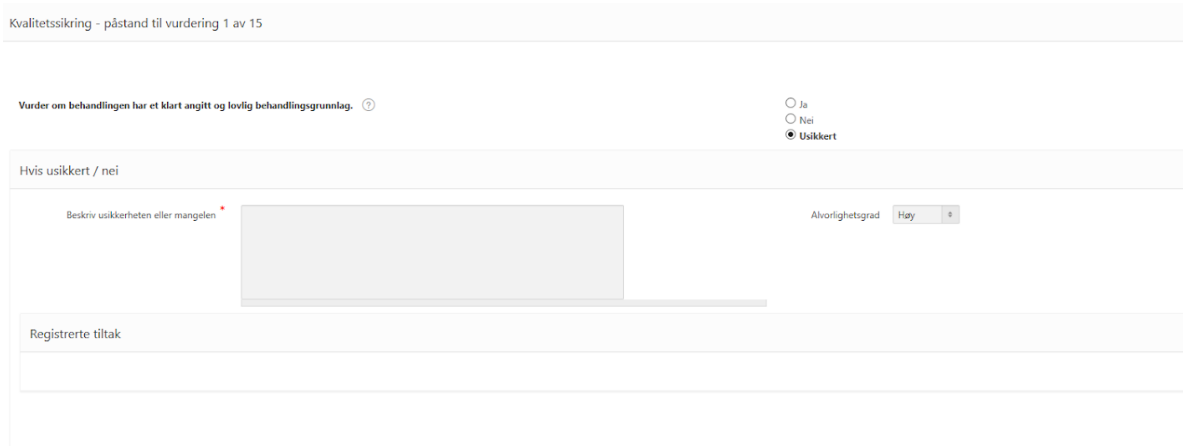


Figur 8 – Registrering av en ny behandling

Som skjermbilde ovenfor viser skal informasjon om tekniske *eller* organisatoriske tiltak som gjennomføres i forbindelse med behandlingen oppgis allerede ved registrering av en ny behandling.

Forordningens krav til risikovurdering varierer ut fra rolle en virksomhet har. Derfor er det ekstra viktig å definere om Statens vegvesen er behandlingsansvarlig eller databehandler for behandlinger i ulike systemer. I Behandlingsoversikten registreres rollene.

Registrering av prosessen avsluttes med 15 spørsmål som skal kvalitetssikre registreringen og eventuelt identifisere og dokumentere tiltak for å lukke avvik. Kvalitetssikring hjelper å avdekke om det er behov for avklaring eller rådføre seg med personvernombudet. Eksempler på andre spørsmål er blant annet oppfordring for vurdering om behandlingen har et tydelig og klart formål, om opplysningene slettes når de ikke lenger er nødvendige for formålet, om den registrerte kan bruke sine rettigheter, slik som rett til få innsyn i sine opplysninger, retting, sletting og andre rettighetene etter Kap. III i forordningen.



Figur 9 – Avsluttende kvalitetssikring av behandlingen ved registrering

Skjermbildet viser at selv om det er et obligatorisk felt for å definere et rettslig grunnlag, stilles det ekstra spørsmål om det for å bekrefte at det ikke ble gjort feil. Samtidig fastsettes alvorlighetsgrad som gjenspeiler krav i bestemmelsene[86] om risikovurdering i forordningen. Videre svarer en prosesseier på spørsmål som avviser eller bekrefter nødvendighet til å gjennomføre vurdering av personvernkonsekvenser etter PVF art. 35. Sjekkliste er basert på anbefalingene fra Det europeiske personvernrådet.

Videre er det fremlagt 22 forhåndsdefinerte risikoer med konsekvenser for den registrerte som fører til at PVF art. 35 kommer til anvendelse. Eksempler på en slik risiko er mangende reell medbestemmelse, manglende reell åpenhet, teknologi eller teknisk tilgang og sikkerhet.

[86] Risikoene av varierende sannsynlighets- og alvorlighetsgrad i PVF art. 24, 25 og 32.

Prioritet 1

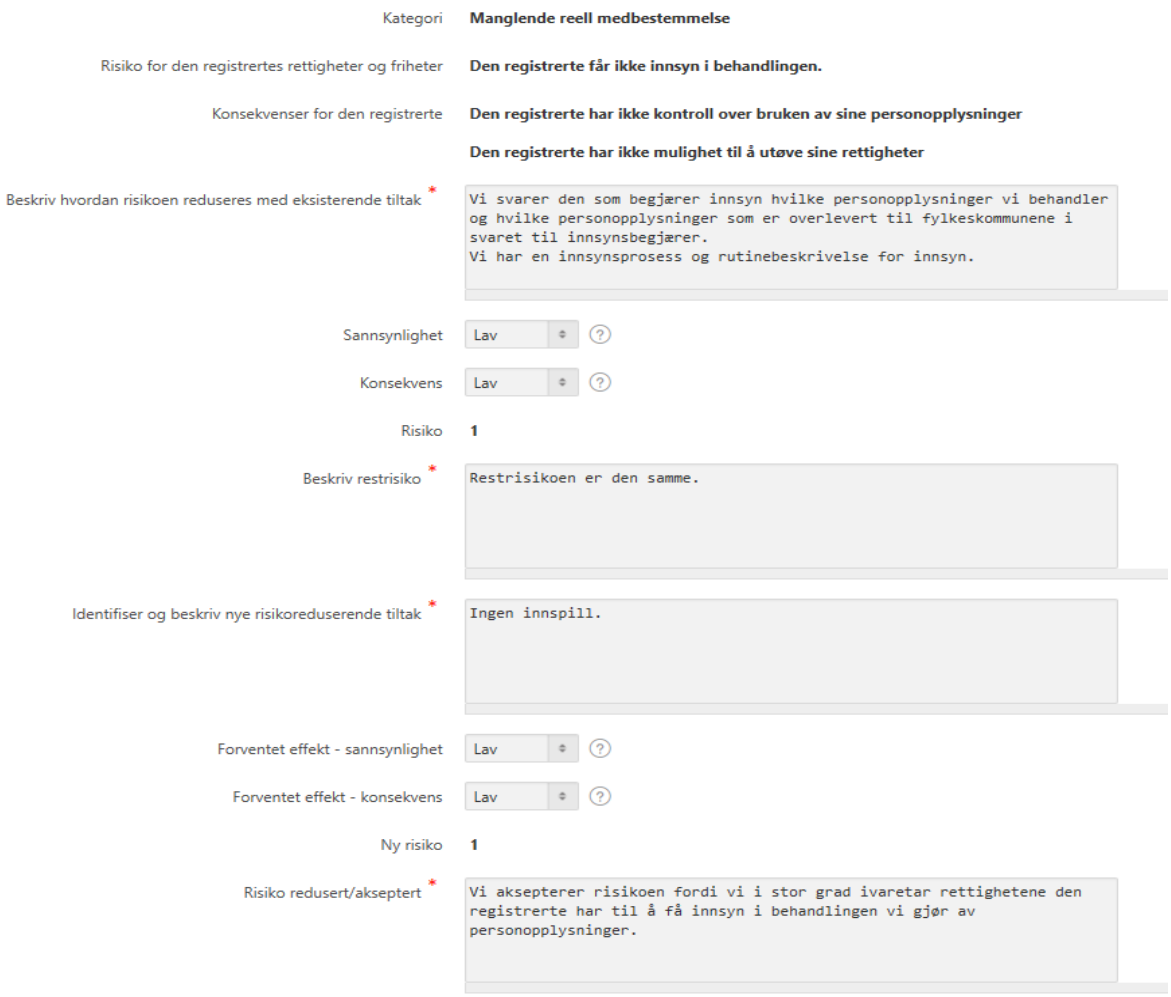
Spørsmål	Beskrivelse
Er behandlingen en evaluering eller poengvurdering?	Inkludert profilering og forutsigelse, spesielt «aspekter som gjelder arbeidsprestasjoner, økonomisk situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser» (fortalepunkt 71 og 91).
Innebærer den systematisk overvåking?	Behandlingsaktiviteter som brukes for å observere, overvåke eller kontrollere de registrerte, inkludert opplysninger som har blitt samlet inn gjennom nettverk eller «en systematisk overvåking i stor skala av et offentlig tilgjengelig område» (artikkel 35 nr. 3 c).
Involverer den særlige kategorier av personopplysninger?	Dette omfatter særlige kategorier av personopplysninger (tidligere kalt sensitive personopplysninger) som er definert i artikkel 9 (for eksempel informasjon om enkeltpersoners politiske meninger), samt personopplysninger vedrørende straffedommer og lovovertredelser som definert i artikkel 10.

Prioritet 2

Spørsmål	Beskrivelse
Omfatter den personopplysninger om registrerte med særskilt beskyttelsesbehov?	Sårbare registrerte kan omfatte barn (de kan anses å ikke være i stand til på en bevisst og gjennomtenkt måte å motsette seg eller gi samtykke til behandling av sine personopplysninger), arbeidstakere, mer sårbare befolkningsgrupper som behøver sosial beskyttelse (psykisk syke personer, asylsøkere, eldre personer, pasienter og så videre), samt i de situasjoner der det foreligger en ubalanse i forholdet mellom den registrerte og den behandlingsansvarlige
Vil konteksten for behandlingen begrense muligheten de registrerte har til å utøve sine rettigheter?	Dette omfatter behandlinger som tar sikte på å tillate, endre eller nekte den registrerte tilgang til en tjeneste eller inngå en avtale. For eksempel når en bank kredittvurderer sine kunder mot en database for å avgjøre om de skal tilbys lån.
Vil to eller flere datasett sammenstilles?	Fra to eller flere databehandlingsoperasjoner som gjennomføres med ulike formål og/eller av ulike behandlingsansvarlige på en måte som overstiger den registrertes rimelige forventninger.
Omfatter behandlingen automatiserte avgjørelser?	Behandling som har som formål å ta beslutninger om den registrerte som har «rettsvirkning for den fysiske personen» eller «på lignende måte i betydelig grad påvirker den fysiske personen» (artikkel 35 nr. 3 a).
Tar den i bruk ny teknologi eller brukes eksisterende teknologi til nye formål?	Bruk av ny teknologi som defineres «i samsvar med det oppnådde nivået av teknisk kunnskap» (fortalepunkt 91), kan medføre behov for å gjennomføre en vurdering av personvernkonsekvenser. Grunnen til dette er at anvendelse av ny teknologi kan medføre nye former for innsamling og bruk av personopplysninger, eventuelt med høy risiko for den enkeltes rettigheter og friheter.
Vil behandlingen innebære at personopplysningene blir flyttet til et sted utenfor EU/EØS	Informasjon som SVV gjennom eksempelvis en Databehandler og eller andre samarbeidspartnere (herunder andre stater)
Dreier det seg om en behandling av personopplysninger i stor skala?	a. Antallet registrerte som berøres, enten som et spesifikt antall eller som en andel av den relevante populasjonen. b. Mengden og/eller spennvidden i personopplysningene som behandles. c. Databehandlingens varighet eller regelmessighet. d. Behandlingens geografiske omfang.

Figur 10 – Forhåndsdefinerte risikoer med konsekvenser for den registrerte

Ved registrering av Memo 360 ble hver av de 22 risikoene dokumentert tilsvarende som en «normal» risikovurdering: Mulige uønskede hendelse er identifisert, risiko for den registrerte, samt konsekvenser og risikoreduserende tiltak ble beskrevet, og sannsynlighets og alvorlighetsgrad er fastsatt. Skjermbilde nedenfor viser et eksempel på gjennomgang av en av de 22 risikoene.



Figur 11 – Vurdering av risiko som potensielt kan være høy

Under kartlegging av Memi 360 ble oppdaget en høy risiko på en av behandlingene som utføres i systemet: I forbindelse med dette ble det kjørt vurderingen av personvernkonsekvenser (DPIA) kun på denne behandlingen. Behandlingen som inngår i Memi 360 og som innebærer en høy risiko for de registrertes rettigheter og friheter er tilgjengeliggjøring av dokumenter i forbindelse med regionreformen:

Regionreformen trådte i kraft 1. januar 2020 og innebærer blant annet at sams (felles) vegadministrasjon etter veglova §10 opphører, dvs. at fylkesvegadministrasjonen blir overført fra Statens vegvesen til fylkeskommunene. Statens vegvesen skal dermed ikke lenger utføre fylkesvegoppgaver på vegne av fylkeskommunene. Ansvaret for regnskapsføring for fylkesveg overføres også til de respektive fylkeskommunene.[87] Alle fylkesveiene som ble forvaltet av Statens

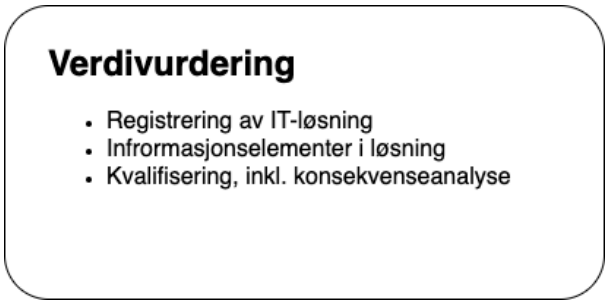
[87] Statens vegvesens brev til Fylkesmannen 19/355002-1 av 09.12.2019.

vegvesen tidligere, gikk over til fylkeskommunene. I den forbindelse skulle alle dokumenter tilgjengeliggjøres (mange inneholdt personopplysninger og en annen sensitiv informasjon) fra Mime 360 og det tidligere arkivet som var knyttet til prosessen. Derfor ble det bestemt å kjøre DPIA på behandlingen med tilgjengeliggjøring av dokumenter. Å gjennomføre DPIA var krevende og tok en ukes tid. Da ble også personvernombudet involvert i DPIA. Rapporten etter denne vurderingen ligger tilgjengelig i Behandlingsoversikten.

3.4.3 Videre risikovurderingsprosess

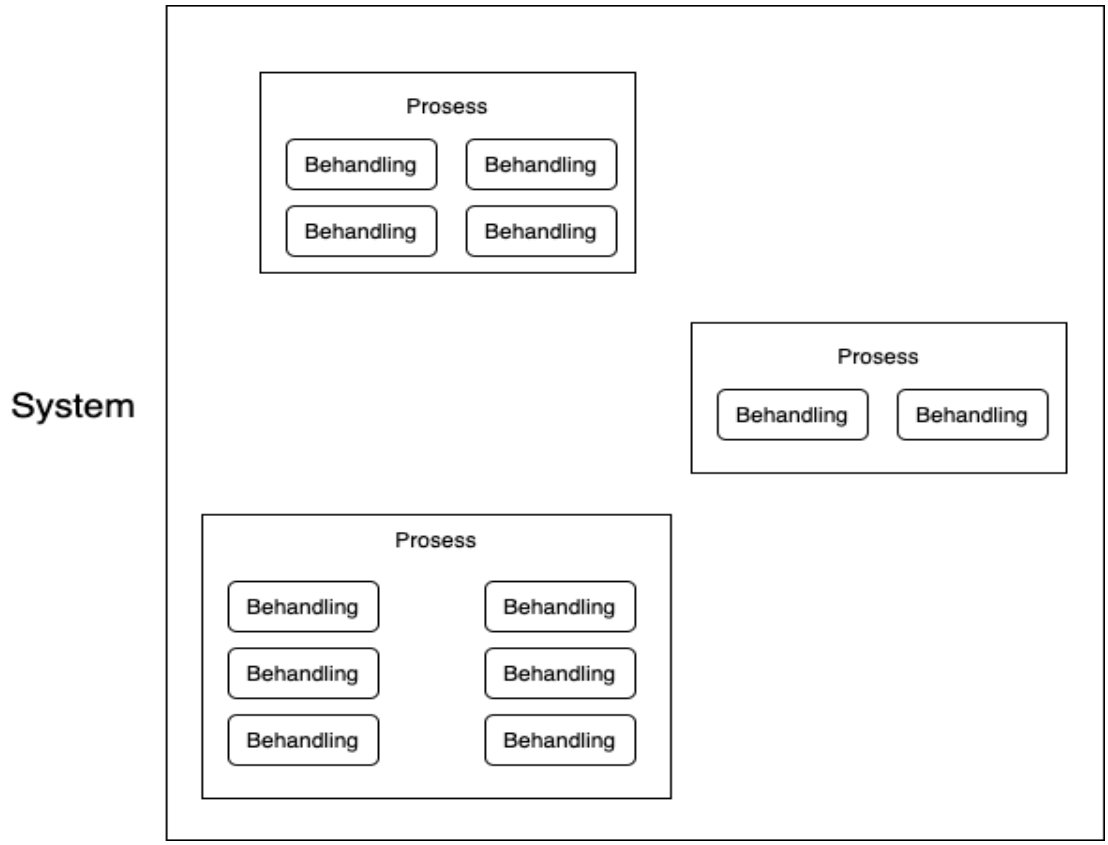
3.4.3.1 Om verktøyet

Behandlingsoversikten er knyttet til et annet IT-system som kalles Verdivurdering. Verdivurderingen baserer seg på NSM sin veileder for verdivurdering og inneholder informasjon om alle IT-løsningene som brukes av Statens vegvesen.



Figur 12 – Hovedelementene Verdivurderingen består av

Bilde nedenfor viser skissering av de enkelte "enhetene" et system kan bestå av. Et system inneholder vanligvis flere behandlingsprosesser, og hver prosess innebærer flere behandlinger. Et eksempel for en slik prosess er fylkesvegadministrasjonen som inkluderer flere fylkesvegoppgaver som Statens vegvesen utførte på vegne av fylkeskommunene.



Figur 13 – En skissering av enhetene et system kan bestå av

3.4.3.2 Verdivurderingsprosess

Systemeier holder prosessen vedkommende er ansvarlig for oppdatert i Verdivurdering. Systemeier er også ansvarlig for at det blir gjort verdivurdering av IT-løsninger.

I risikovurderingsprosess som inkluderer verdivurdering for Memi 360 deltok flere personer:

- Systemeier som kjenner systemet, hvilken informasjon som ligger der, hva slags rutiner som ligger til grunn og hvilke prosesser som skjer og hvilke tilgangsstyringer som eksisterer. Systemeier er ansvarlig for å utvikle, forvalte og drifte et informasjonssystem.[88]
- Systemforvalter som er teknisk ansvarlig for systemet
- IT-sikkerhetsansvarlig
- Ansvarlig for deling av data

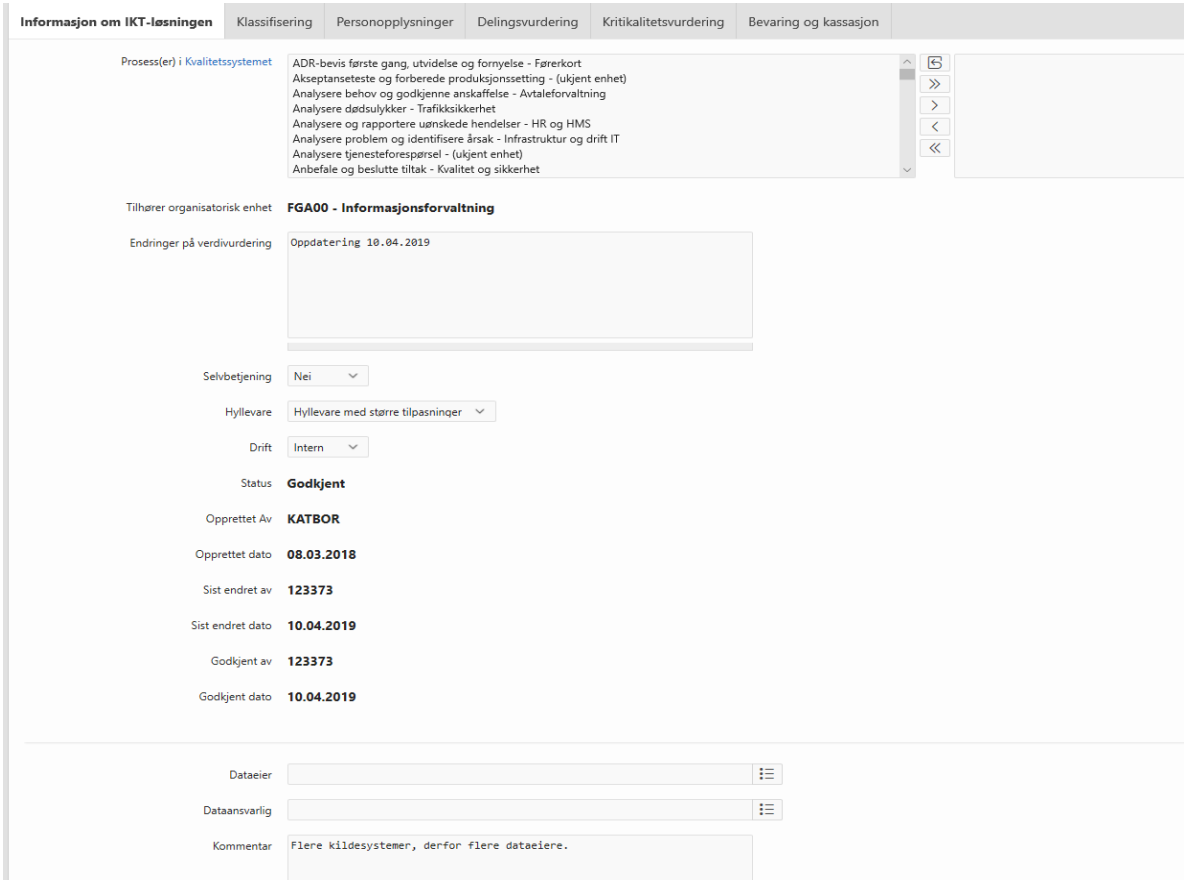
Personvernombudet deltok ikke i risikovurdering, og gjør ikke det ellers i andre risikovurderinger.

Fordi Memi 360 innebærer mange fagprosesser, tok gjennomgåelse av verdivurderingen noe lengre tid enn vanlig. For å gjennomføre dette ble systemet Verdivurdering brukt, der det

[88] Digitaliseringsdirektoratet Begrepsliste - Systemeier (u.å.).

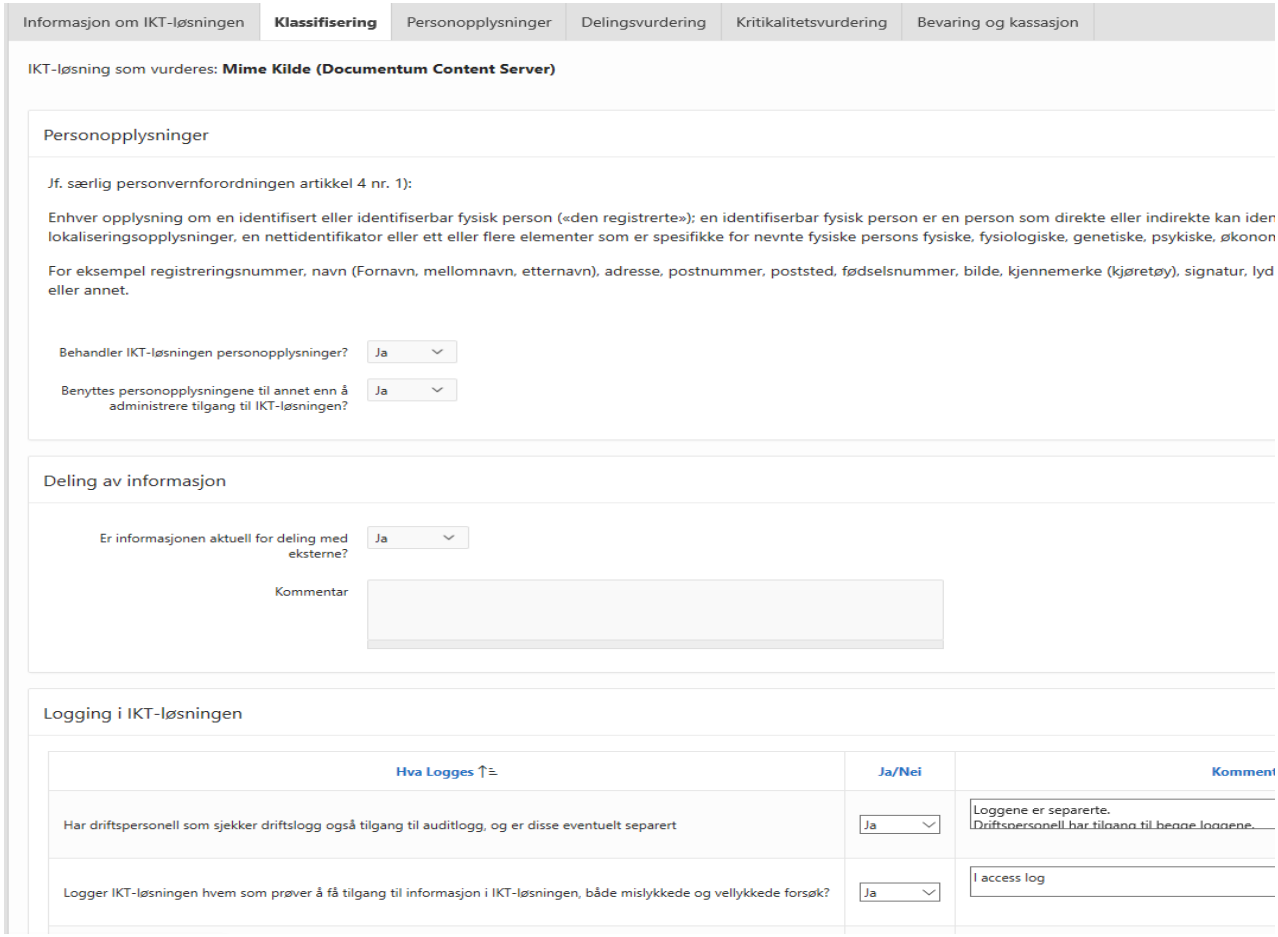
gjennomgås hvilken informasjon som er om løsningen, klassifisering av løsningen, hvilke personopplysninger løsningen inneholder, en delingsvurdering samt en kritikalitetsvurdering.

Slik det gjøres med alle andre IT-løsninger, ble registrering av Memi 360 i Verdivurdering begynt med en beskrivelse av selve løsningen. Beskrivelsen inneholder informasjon om hvilke opplysninger som behandles i systemet som verdivurderes, hvilke prosesser som skjer i systemet mv. I Verdivurdering registreres både personopplysninger og opplysninger som ikke kan knyttes til den registrerte. Som en del av verdivurdering ble det registrert blant annet lagringstid, informasjon om tjenestebehov som gir grunnlag for tilgangsstyring mv. i Memi 360.



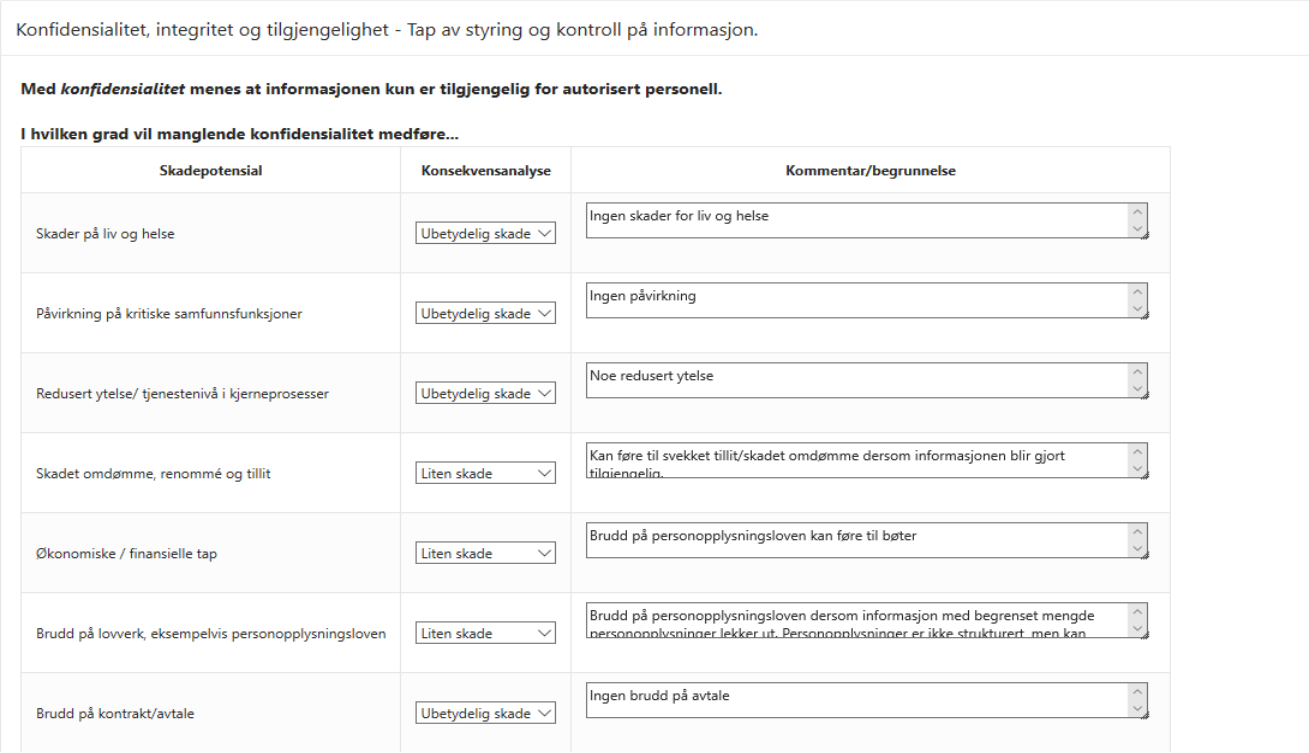
Figur 14 – Registrering av Memi 360 i Verdivurderingen

Kvalifisering som en del av verdivurdering skjer ved å identifisere blant annet om systemet behandler personopplysninger, om informasjonen er aktuell for deling med eksterne aktører, hva slags logging som foretas og hvilke opplysninger som brukes for testing.



Figur 15 – Kvalifisering av Memi 360

Verdivurdering inkluderer konsekvensanalyse som innebærer analyse av risiko de ulike systemene potensielt har i forhold til konsekvens knyttet til informasjonssikkerhet. Konsekvensanalyse inkluderer ikke sannsynlighetsvurdering og det planlegges ikke tiltak i samme prosess, fokuset er kun på å identifisere uønskede hendelser og vurdering av alvorlighetsgrad hvis disse hendelse eventuelt inntreffer. Konsekvensanalysen fra Verdivurderingen inkluderer konsekvenser som fører til brudd på konfidensialitet, integritet og tilgjengelighet ved tap av styring og kontroll på informasjon. Under konsekvensanalysen av Memi 360 ble det vurdert blant annet at manglende konfidensialitet kan medføre redusert ytelse i kjerneprosesser og brudd på personvernregelverket dersom opplysninger lekker ut, manglende integritet kan medføre brudd på arkivloven og manglende tilgjengelighet kan medføre svekket omdømme dersom Statens vegvesen ikke kan fremskaffe historiske data. Konsekvensanalysen av Memi 360 representerer mer omfattende analyse og ikke er utelukkende basert på personopplysningssikkerhet.



Konfidensialitet, integritet og tilgjengelighet - Tap av styring og kontroll på informasjon.

Med *konfidensialitet* menes at informasjonen kun er tilgjengelig for autorisert personell.

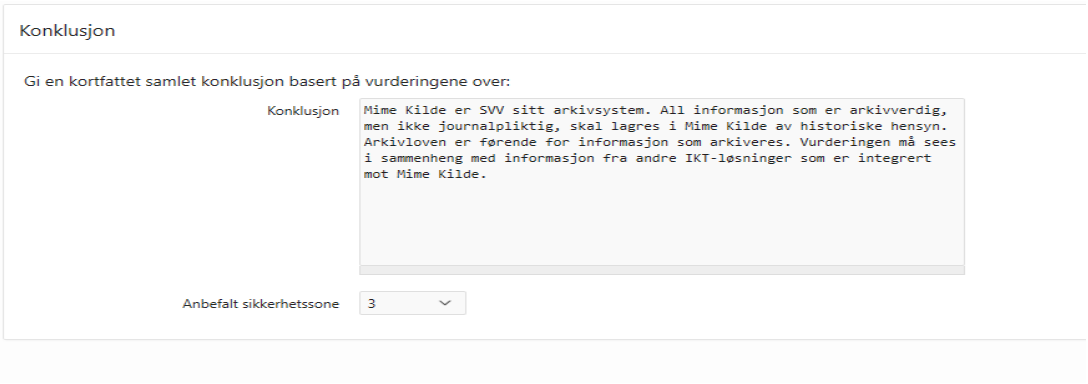
I hvilken grad vil manglende konfidensialitet medføre...

Skadepotensial	Konsekvensanalyse	Kommentar/begrunnelse
Skader på liv og helse	Ubetydelig skade	Ingen skader for liv og helse
Påvirkning på kritiske samfunnsfunksjoner	Ubetydelig skade	Ingen påvirkning
Redusert ytelse/ tjenestenivå i kjerneprosesser	Ubetydelig skade	Noe redusert ytelse
Skadet omdømme, renommé og tillit	Liten skade	Kan føre til svekket tillit/skadet omdømme dersom informasjonen blir gjort tilgjengelig.
Økonomiske / finansielle tap	Liten skade	Brudd på personopplysningsloven kan føre til bøter
Brudd på lovverk, eksempelvis personopplysningsloven	Liten skade	Brudd på personopplysningsloven dersom informasjon med begrenset mengde personopplysninger lekker ut. Personopplysninger er ikke strukturert, men kan
Brudd på kontrakt/avtale	Ubetydelig skade	Ingen brudd på avtale

Figur 16 – Konsekvensanalyse av Memi 360

Analysen inneholder forklarende tekst på hva hvert enkelt brudd kan potensielt føre til og foreslår en liste over skadepotensiale med kommentarfelt som kan brukes ved behov. Skadepotensialet illustrerer potensielle risikoer og er mer omfattende enn kun risiko for de registrertes rettigheter og friheter.

Det er anbefales sikkerhetsnivå som må vurderes, og dette inkluderer 4 sikkerhetsnivåer. For eksempel er det vanlig at personopplysninger har sikkerhetsnivå 3, mens personopplysninger av særlig kategori har sikkerhetsnivå 4. Nivå hjelper til å definere tilfredsstillende tiltak for å opprettholde nødvendig personopplysningssikkerhet.



Konklusjon

Gi en kortfattet samlet konklusjon basert på vurderingene over:

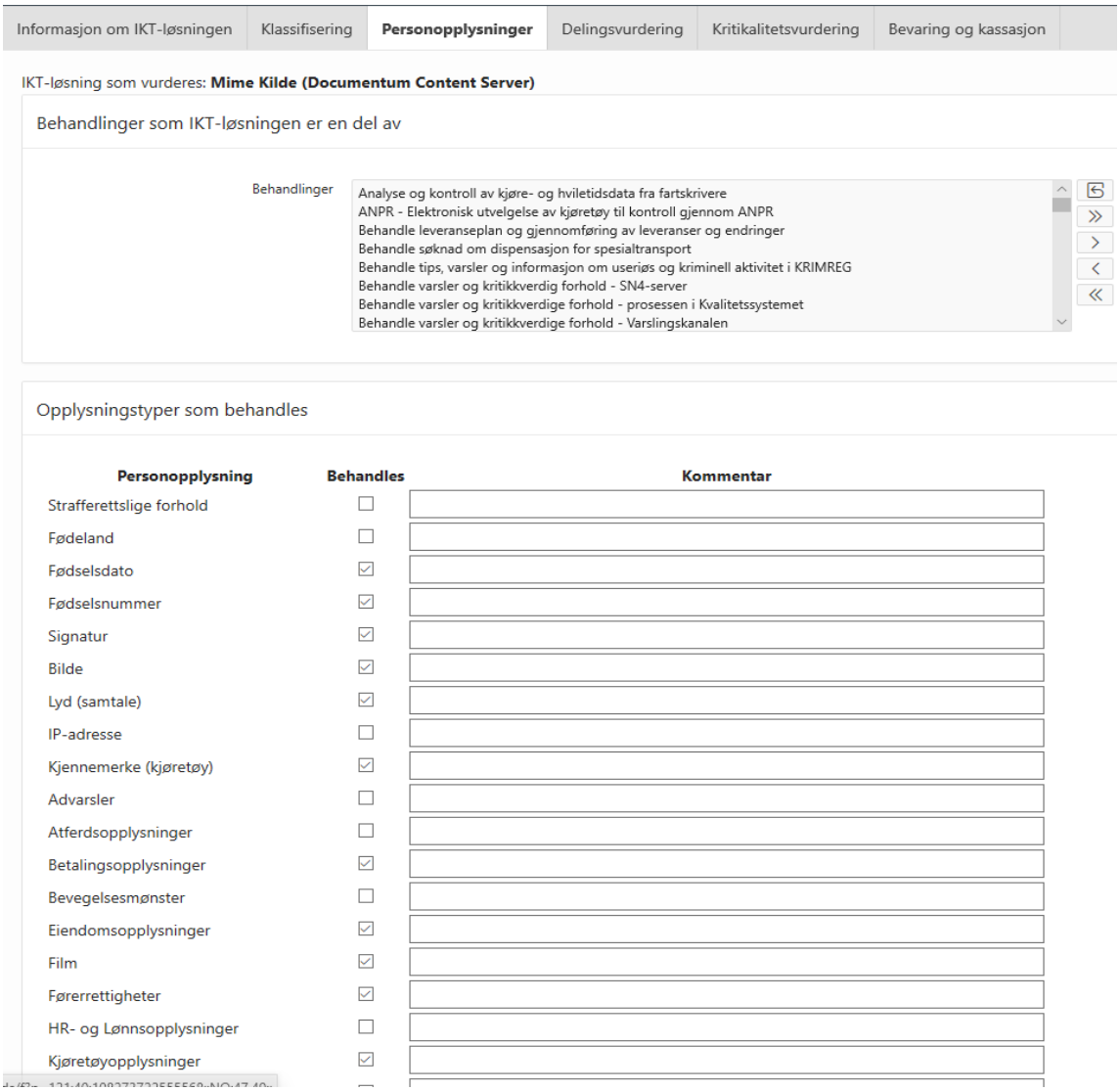
Konklusjon: Mime Kilde er SVV sitt arkivsystem. All informasjon som er arkivverdig, men ikke journalpliktig, skal lagres i Mime Kilde av historiske hensyn. Arkivloven er førende for informasjon som arkiveres. Vurderingen må sees i sammenheng med informasjon fra andre IKT-løsninger som er integrert mot Mime Kilde.

Anbefalt sikkerhetssone: 3

Figur 17 – Konklusjon basert på konsekvensanalyse

Konklusjonen etter konsekvensanalysen viser til anbefalt sikkerhetssone. Skjermbilde ovenfor viser til hvilken sikkerhetssone som er anbefalt for Memi 360 og hva er grunnlaget for anbefaling.

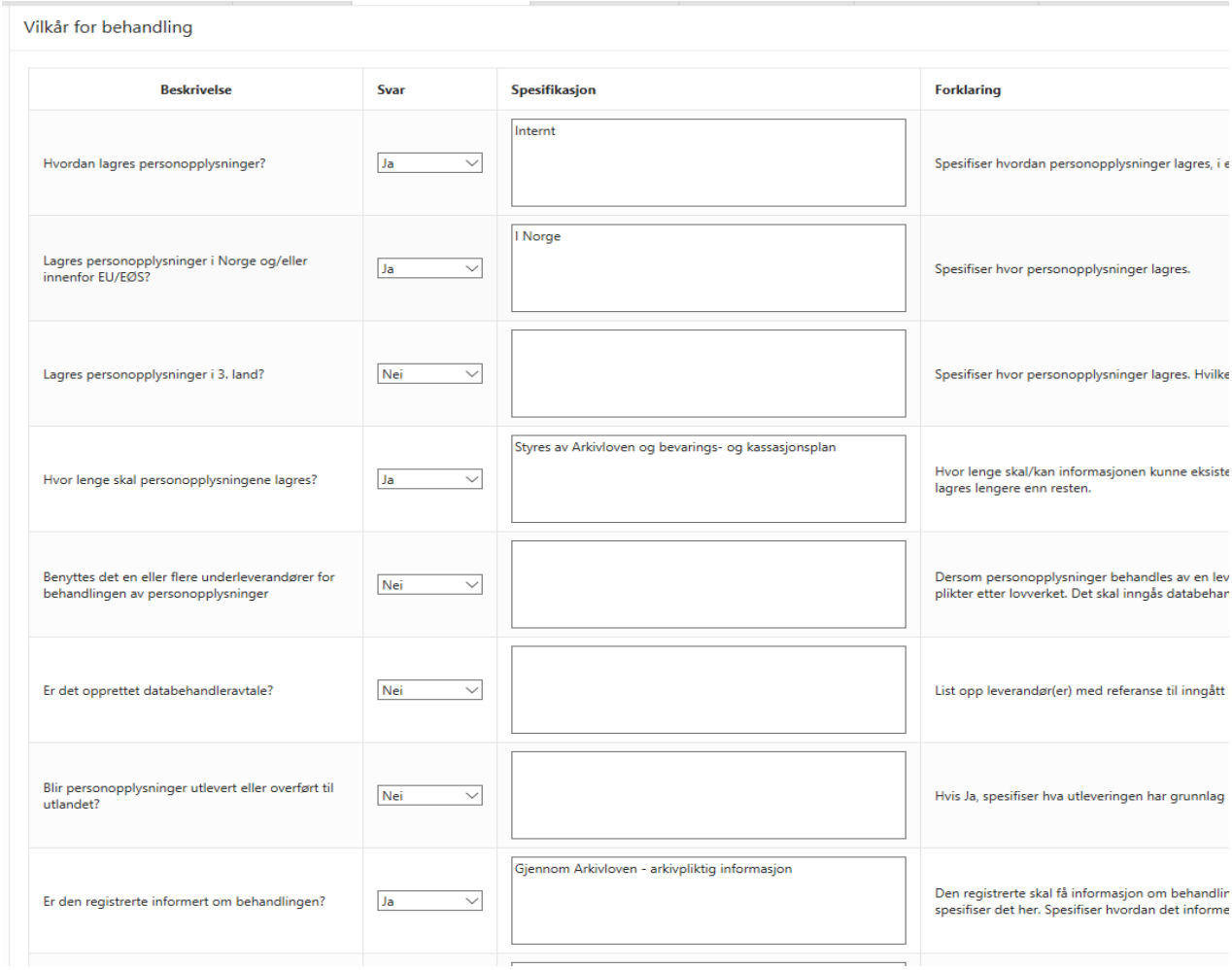
Videre beskrives hvilke behandlinger som inngår i systemet som verdivurderes og personopplysninger som inngår i behandlinger. Verdivurdering lister mulige behandlinger og foreslår personopplysninger som bare skal velges hvis de er relevante for det bestemte systemet. Skjermbilde nedenfor viser kartleggingen av Memi 360.



Figur 18 – Kartlegging av behandlingene som skjer i Memi 360

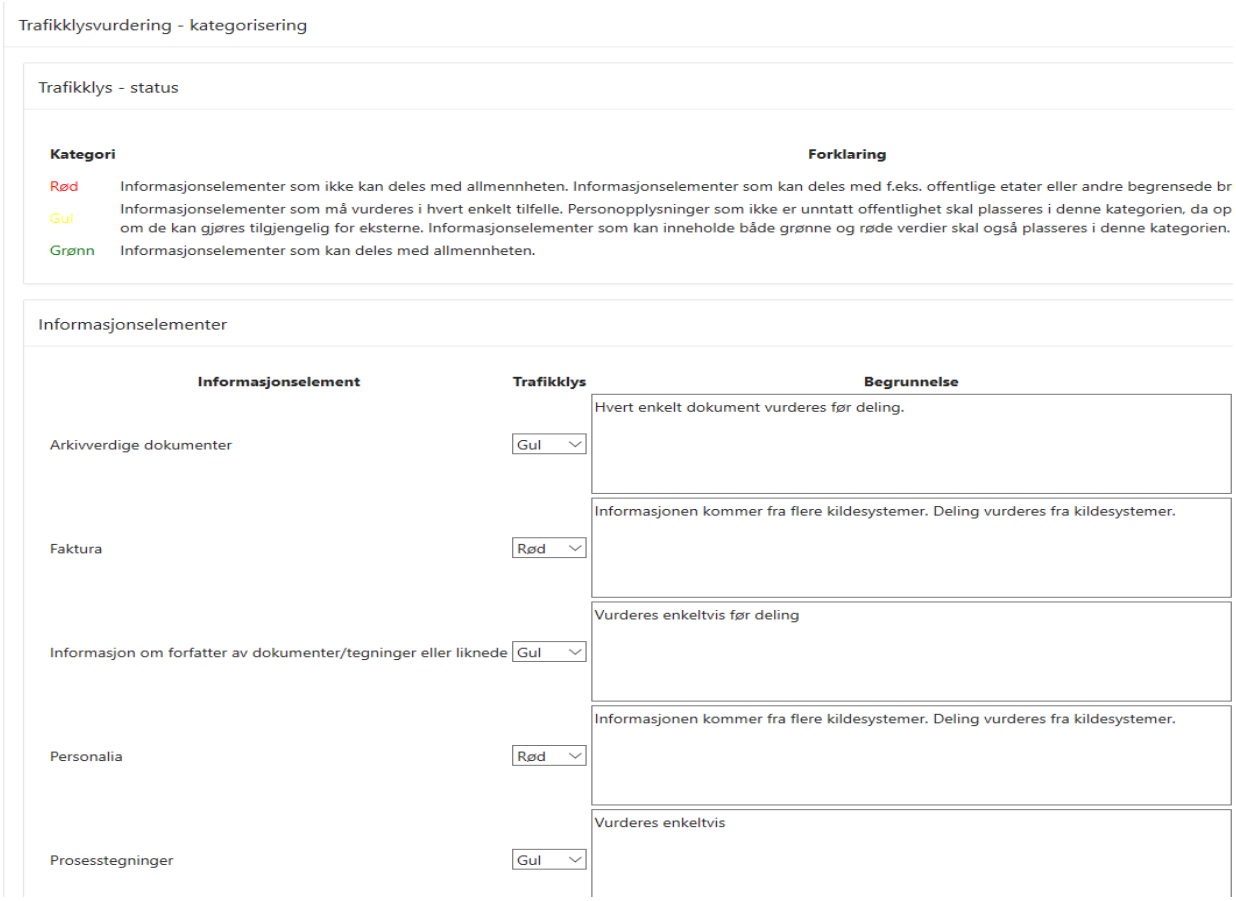
Om opplysninger av særlig kategori er relevante, skal de også merkes, samt kategorier av de registrerte og andre IT-løsninger opplysningene flyttes mellom. I og med at Mime 360 er et arkiv- og saksbehandlingssystem, vil det også inneholde særlige kategorier av personopplysninger.

Ikke minst beskriver systemet også andre vilkår som er relevante for behandlingen og som kan være grunnlag for å se om behandlingen utføres i samsvar med personvernforordningen. Dette innebærer informasjon om lagring, databehandleravtaler, om informasjon til de registrerte, samt om personvernprinsippene er integrert i løsninger om det er nødvendige rutiner på plass.



Figur 19 – Ytterlige informasjon om behandlinger i Memi 360

En separat vurdering i en helhetlig verdivurdering handler om datadeling. Vurderingen inneholder forklarende tekst og spørsmål om behandlingen i forbindelse med deling eller offentliggjøring av informasjon. Til slutt vises det til kategorisering av data med eksempler på farger på trafikklys, altså rødt, gult og grønt. Slik er det intuitivt forståelig hvilke opplysninger som kan deles.

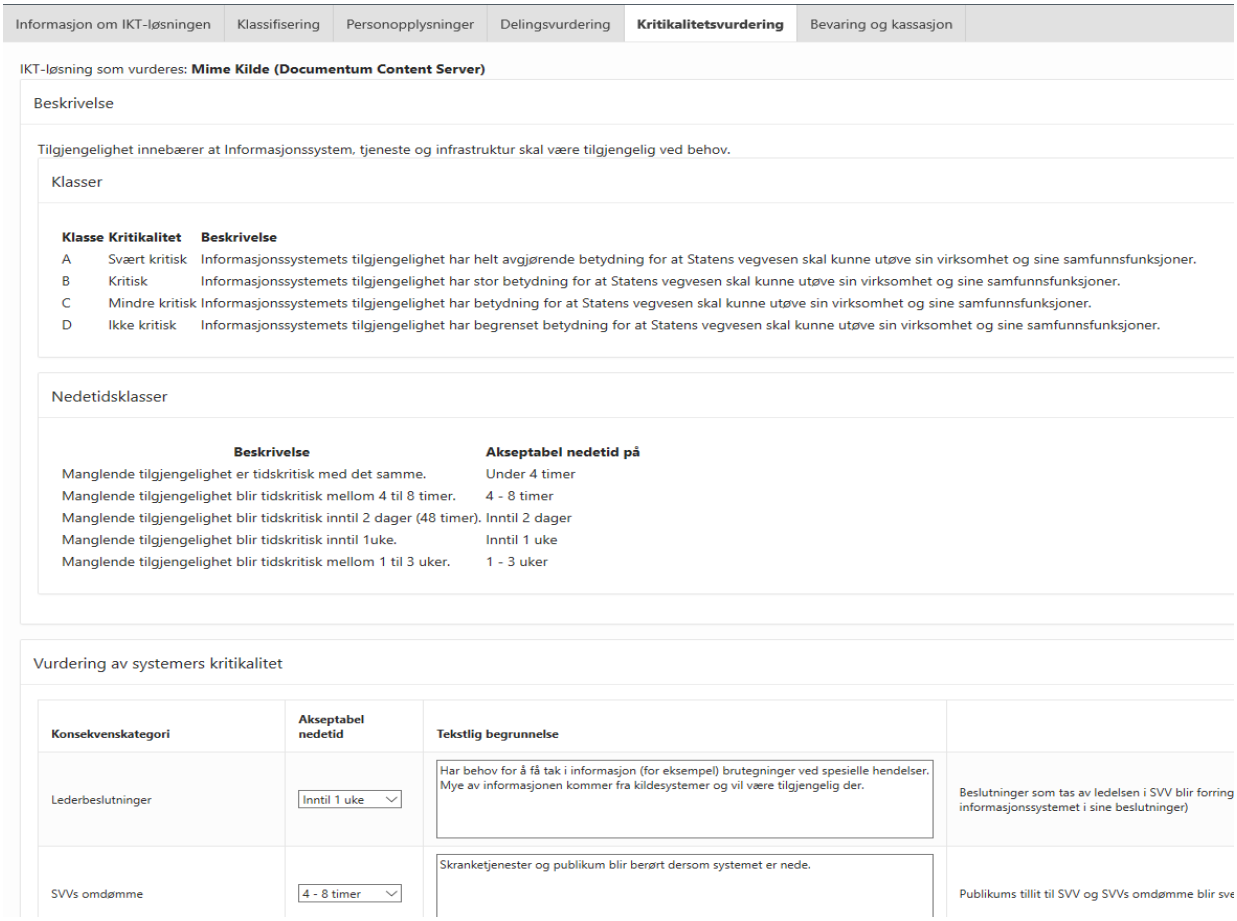


Figur 20 – En vurdering av datadeling i Memi 360

Konklusjonen beskriver en refleksjon vedrørende deling av data og kategorisering av slik informasjon, hvor kategoriene er rød (informasjon som ikke kan deles med allmennheten), gul (informasjon som må vurderes i hvert enkelt tilfelle) og grønn (informasjon som kan deles med allmennheten). Skjermbildet ovenfor viser en konklusjon om datadeling for Memi 360.

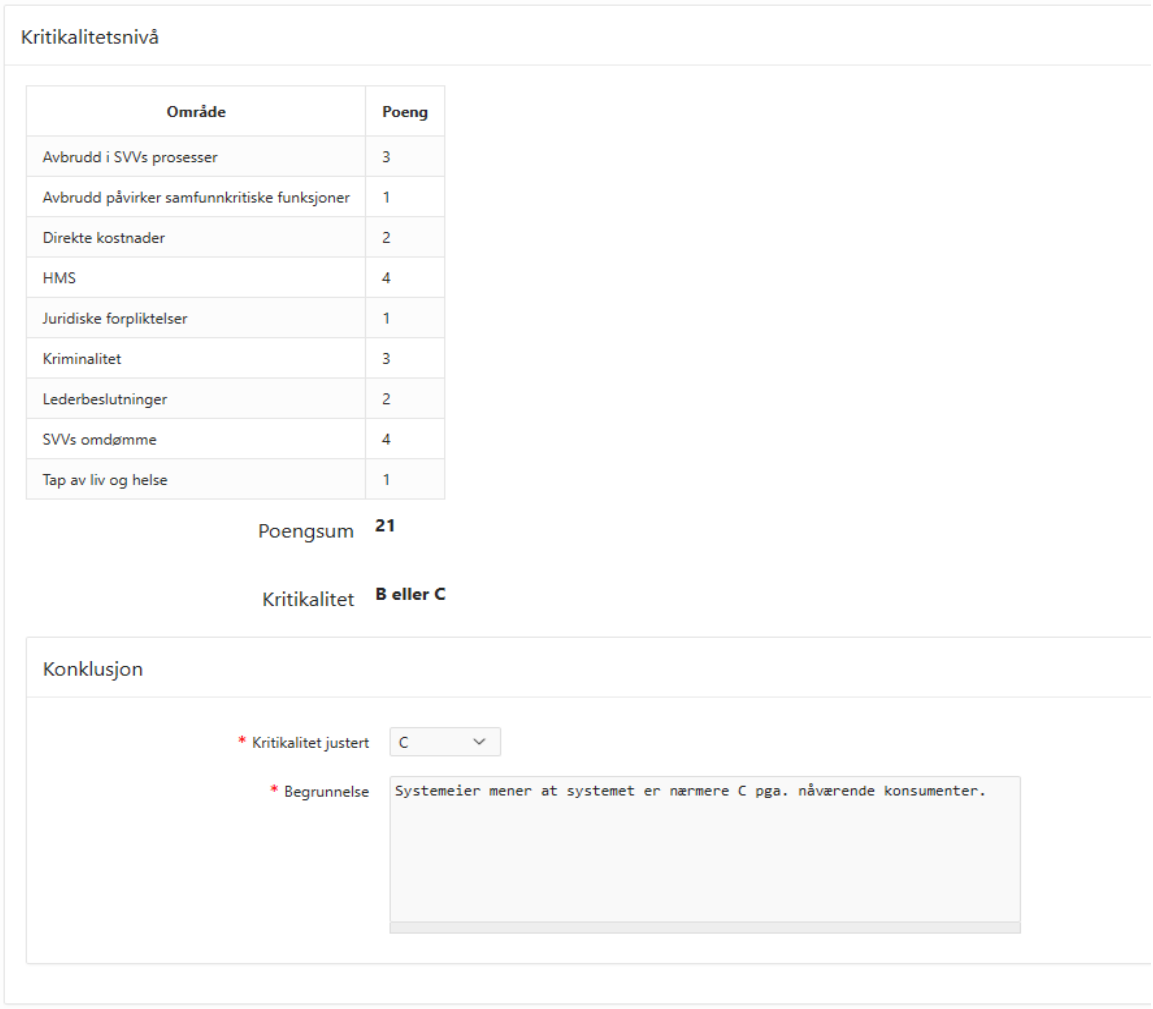
En adskilt funksjon i systemet Verdivurdering er muligheten for å gjennomføre en kritikalitetsvurdering. Denne kritikalitetsvurderingen skal sikre at informasjonssystemet, tjenester og infrastrukturen skal være tilgjengelig ved behov. Kritikalitetsvurderingen inneholder altså en tilgjengelighetsvurdering til løsningen og inneholder en fordeling på fire klasser. Disse fire klassene kategoriserer hvor viktig det er at informasjonssystemet er tilgjengelig for at Statens vegvesen skal kunne utøve sin virksomhet og sine samfunnsfunksjoner. Klasse A er svært kritisk fordi informasjonssystemets tilgjengelighet har helt avgjørende betydning for Vegvesenet Klasse D er vurdert til å være ikke kritisk fordi informasjonssystemets tilgjengelighet har begrenset

betydning for Vegvesenet. Det er også fastsatt nedetidsklasser og akseptabel nedetid. Det kan være avgjørende for påfølgende risikovurdering og planlegging av risikoreduserende tiltak.



Figur 21 – Vurdering av risiko knyttet til systemets utilgjengelighet

Kritikalitetsvurdering av Memi 360 er basert på konsekvenskategori, hvor man velger akseptabel nedetid, begrunnelse og beskrivelse av denne. Systeminformasjonens tilgjengelighet inkluderer ikke personvernområdet, men er avgjørende for andre området, slik som HMS, kriminalitet og Vegvesenets omdømme. Kritikalitetsnivå fastsettes på bakgrunn av samlet poengsum.

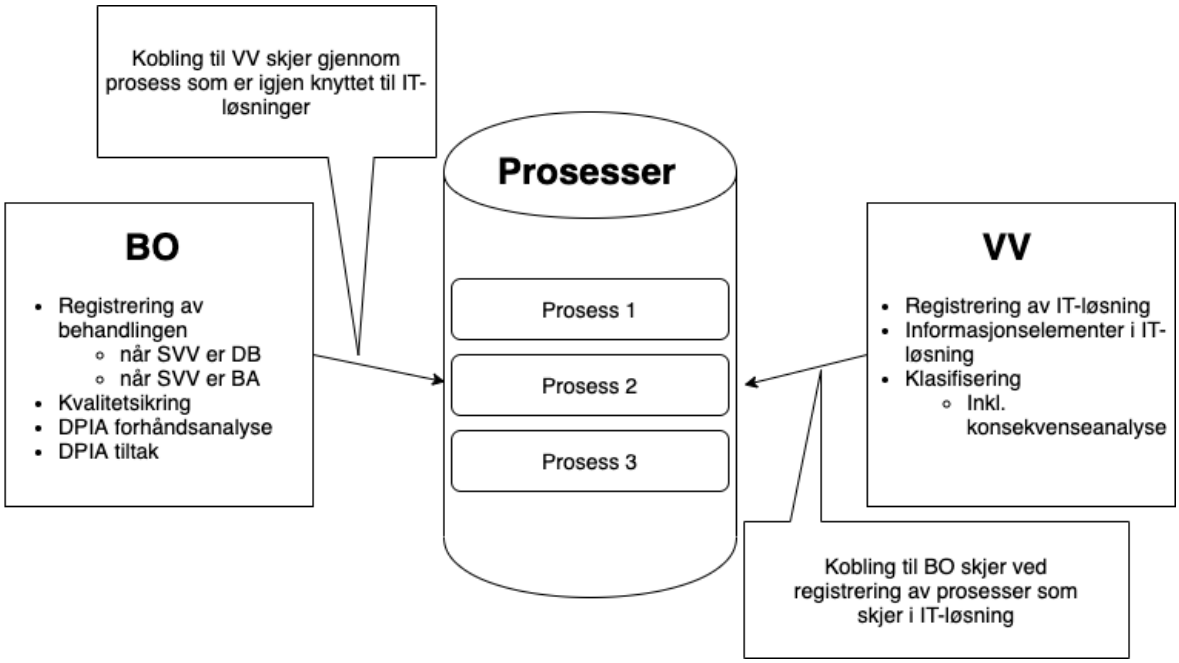


Figur 22 – Resultat av kritikalitetsvurderingen av Memi 360

Det defineres akseptabel risiko under verdivurdering. Verdivurderingsresultatet sendes til en database og brukes ved implementering av nye systemer. Skjermbildet ovenfor viser konklusjon for Memi 360.

3.4.4 Kobling mellom systemene

Behandlingsoversikten er koblet til prosesser som skjer i Statens vegvesen, som for eksempel utsendelse av førerkort. I tillegg er hver prosess knyttet til et IT-system som behandler opplysningene. Behandlingsoversikten inneholder også en kobling til risikovurdering av systemer som behandler opplysningene. Verdivurdering er koblet til Behandlingsoversikten via prosessene som er registrerte i begge systemene.

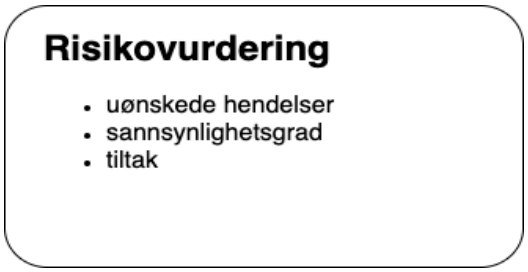


Figur 23 – Kobling mellom Behandlingsoversikten og Verdivurdering

3.4.5 Risikovurdering etter PVF art. 32

Systemeier har ansvar for risikovurderingen.

Etter at risikovurderings gruppa gikk gjennom verdivurderingen av systemet, gjennomføres en risikovurdering som siste steg der verdivurderingsresultat er hentet og risikovurderingen fortsettes basert på verdivurderingen. Da er det sannsynlighetsgrad som vurderes og hvilke tiltak som kan senke risiko. Uønskede hendelser defineres og sannsynligheten fastsettes.



Figur 24 – Hovedelementene risikovurdering består av

Verktøyet har en liste over forslag til uønskede hendelser, som for eksempel trussel og risikoreduserende tekniske- og organisatoriske tiltak.

Malen inneholder forklarende informasjon om hva en uønsket hendelse er og en Excel-fil (5x5 matrise) for visualisering av risiko og om risikoen er akseptabel eller ikke. Matrise innebærer 3

faner (Informasjon, analyse, oppsummering) der det gås gjennom sannsynlighet og konsekvens for uønskede hendelser og tiltak. Uønskede hendelser listes med tanke på konfidensialitet, integritet og tilgjengelighet. Hvis det eksempelvis er mulig at personopplysninger kommer på avveie er det flere forslag til uønskede hendelser og forslag til tiltak i malen som er utarbeidet til dette nettopp formålet. Risikoreduserende tiltak fastsettes uavhengig av risikostørrelse. Risikovurderingen tok utgangspunkt i informasjonssikkerhet og de har på forhånd definert en liste med mulige uønskede hendelser som gir mulighet for å velge de hendelsene som passer for det aktuelle systemet og slippe å finne på de selv. Ifølge intervjuobjektet kan systemer i seg selv være likt med tanke på uønskede hendelser. Det gjenstår å fokusere på spesielle aspekter ved Memi 360 som risikovurderes.

Excel-filer brukes, men Statens vegvesen planlegger å droppe Excel når denne modulen blir tilgjengelig som en del av Verdivurderingen. Det tas ikke hensyn til sannsynlighet før man ser på tiltak.

I utgangspunktet risikovurderes et fagsystem, ikke enkelt behandling, men man tenker behandlingsprosesser som er inkludert i systemet. En IT-løsning kan være knyttet til flere behandlinger og vurderingen må besvares for hver behandling.

Hele prosessen (både verdivurdering av systemet og risikovurdering) tok to ganger to-timers møter.

Risikovurderingsprosessen for Memi 360 er ikke annerledes enn andre risikovurderinger som blir gjennomført for andre systemer. Metoden som er tilpasset for Statens vegvesen gjør det mulig at alle systemene kan risikovurderes på lik linje og man trenger ikke juridisk bistand for denne prosessen. Det ble ikke involvert eksterne ekspertene for gjennomføring av risikovurdering og intervjuobjektet opplever at det var ingen spesielle utfordringer rundt risikovurdering av Memi 360, selv om prosessen innebar en del diskusjon. Intervjuobjektet forteller at de ikke manglet juridisk- eller en annen kompetanse under denne risikovurderingsprosessen fordi det ble gjort en uttømmende forklaring på forhånd om hvordan man gjør en risikovurdering. I tillegg gjorde bruk av malverk og god IT-sikkerhets kompetanse at risikovurderingen ikke var vanskelig for systemeiere, forteller intervjuobjektet.

Det som er viktig for en risikovurdering er å følge den opp i etterkant. Etter at personvernforordningen trådte i kraft og med nye rutiner i Statens vegvesen er det mer fokus på dette nå.

Ifølge Statens vegvesens rutiner er det anbefalt å gjennomføre risikovurdering på nytt hvert år.

4. Drøftelse og delkonklusjoner knyttet til problemstillingene

4.1 Drøftelse og delkonklusjoner om rettslige krav som stiller personvernforordningen til risikovurdering

Min første problemstilling hadde som mål å identifisere hvilke rettslige krav personvernforordningen stiller til vurdering av risiko for behandling av personopplysninger. Tolkning av bestemmelser i sammenheng med veiledninger og uttalelser fra ulike kompetente instanser ga en god oversikt over et det rettslige bildet på hvilke krav som gjelder for risikovurderinger. Det er fortsatt mye som er uklart på grunn av den generelle karakteren på regelverket og manglende rettspraksis, men det er tydelig at risikovurdering er nødvendig for å planlegge tiltak som reduserer risiko for manglende etterlevelse av forordningen, behov for innebygd personvern eller for å sikre behandlingen.

Personvernforordningen gir flere "knagger" som hjelper å forstå hva som kreves for en risikovurdering. Blant annet hvilke hensyn som skal tas, hvilke formål risikovurdering har og hva som skal risikovurderes. Det er likevel naturlig å ha et verktøy for risikovurdering og manglende entydig mening om hvordan risikovurdering skal skje kan føre til en noe overfladisk vurdering eller at risikovurdering oppleves som unødvendig styr og byråkratisk hinder for behandling av personopplysninger. Det er helt avgjørende at virksomheten har tilgang til ressurser som forstår kravene i personvernforordningen på grunn av kompleksiteten av regelverket og som kan bistå med en klargjøring av regelverket og tilpasning til virksomhetens behov ved gjennomføring av en risikovurdering. På den måten bidrar risikovurderingen til at behandlingen av personopplysninger skjer i tråd med regelverket og risiko for uønskede hendelser reduseres til et akseptabelt nivå.

4.2 Drøftelse og delkonklusjoner om organisering av arbeidet med risikovurdering av Statens vegvesens arkivsystem Memi 360

Formålet med andre problemstillingen var å undersøke praksis for risikovurdering i Statens vegvesen.

Det er systemeier som er ansvarlig for at behandlinger som skjer i underordnede systemet er blitt risikovurdert. Ved å plassere det ansvaret hos en som er ansvarlig for utvikling, forvaltning og drift av systemet, er det enklere for forvaltningsorganet å ha oversikt om ulike kravene etterleves, selv om personvernforordningen gir ikke klare føringer om organiseringen, bortsett fra at ansvaret for etterlevelse av regelverket ligger hos behandlingsansvarlig.

Risikovurderingen er basert på og begynner med kartleggingen av behandlinger og registrering av IT-løsningene behandlingene skjer i. Selv om verktøyene Behandlingsoversikten og

Verdivurdering kartleggingen skjer i er knyttet til hverandre, mener jeg at prosesseier som er ansvarlig for registrering og oppdatering av behandlingen, samt gjennomføring av DPIA, skal også delta i risikovurderinger. Prosesseier kan gjøre risikovurderingsgruppa oppmerksom på nyanser i behandlingen og spesielle aspekter som er nødvendig å ta hensyn til under risikovurderingen. Eksempler på særlige hensyn kan være varighet av behandlingen, detaljeringsgrad av behandlingen mv.

En risikovurdering av Mime 360 etter kravene i PVF art. 32 skjer separat fra en risikovurdering etter andre bestemmelsene i forordningen og omfatter en klassisk forståelse av fremgangsmåten med bruk av Excel-filer og matrise. Statens vegvesen har organisert arbeidet slik at det involveres verken en personvernjurist eller personvernombud i prosessen. Jeg antar at ville vært nyttig å involvere en ekspert innen personvern eller en som har inngående forståelse av personvern, særlig når det gjelder bestemmelse av konsekvensgrad. I risikovurdering av Memi 360 deltok fagpersoner som kjenner prosesser i systemet og det kan være en bemerkning at manglende involvering av personvernekspert kan føre til en mindre helhetlig risikovurdering. Det kan være aktuelt å diskutere hvorvidt informasjonsbokser og forklarende tekst kan erstatte løpende rådgiving av noen som kan bidra med vurdering av konsekvensgrad for de registrerte ved potensielt uønskede hendelser. Det er mulig at mangel på andre personer enn de som kan mye om systemprosesser potensielt kan føre til en overfladisk risikovurdering, for vurderingen skal omfatte risikoer for de registrertes rettigheter og friheter. Kunnskapen om hvilke konsekvenser for de ulike rettighetene er krevende for fullstendig vurdering av risiko. Det faktum at det er kun de fagpersoner som kjenner systemer fra teknisk side som deltar i risikovurderinger, kan være en svakhet i organiseringen. Manglende deltakelse av de som har juridisk bakgrunn er forsøkt kompensert med tilrettelagt metode for gjennomføring av slik systemet. På den måten at det er laget spørsmål og forklarende tekst som gjør det unødvendig å ha juridisk kompetanse. Det at det er IT-sikkerhetsansvarlig på plass under vurdering av informasjonssikkerhet styrker mening om at en juridisk kompetanse er nødvendig for en helhetlig risikovurdering. I tillegg kan det også være aktuelt at ordinære brukere som også kan gjøre innspill i prosessen.

Statens vegvesen har fastslått at en ny risikovurdering skjer hvert år uten at det tas hensyn til andre refleksjoner som kan føre til behovet å oppdatere risikovurderingen, slik som for eksempel endringer av risikobildet eller andre "behov" personvernforordninger referer til[89]. Jeg antar at byrde for å passe på det kan ligge hos personvernombudet, men det kan være komplisert for personvernombudet å følge opp alle systemer fordi ulike hensyn kan være knyttet til forskjellige systemer og tidspunkter for aktuelle vurderinger kan være forskjellige.

[89] "Skal gjennomgås på nytt og oppdateres ved behov," jf. personvernforordningen PVF art. 24 og 35.

4.3 Drøftelse og delkonklusjoner om fremgangsmåte som ble anvendt da arkivsystemet Memi 360 ble risikovurdert

Gjennom intervjuer ville jeg også undersøke hvilken fremgangsmåte som ble anvendt da arkivsystemet Memi 360 ble risikovurdert.

Statens vegvesen har valgt å implementere en risikovurderingsprosess inn til en helhetlig oversikt over eksisterende systemer. Behandlingsoversikten registrerer informasjon som kreves etter PVF art. 30 og omfatter beskrivelse av behandlinger både når Vegvesenet er behandlingsansvarlig og når de er databehandler. Behandlingsoversikten baserer seg ikke kun på kravene i forordningens PVF art. 30. I de tilfellene der Statens vegvesen er databehandler inneholder Behandlingsoversikten mer omfattende kartlegging enn det som kreves etter personvernforordningen, slik som for eksempel hvilke opplysninger som behandler på vegne av behandlingsansvarlig, og hvilke IKT-løsninger som behandler disse. Behandlingsoversikten er mer detaljert når Statens vegvesen er behandlingsansvarlig. Den inkluderer krav etter PVF art. 30 om føring av protokoll, men inneholder mer informasjon enn det, for eksempel har Behandlingsoversikten også informasjon om rettslig grunnlag og særlige kategorier av personopplysninger. Jeg har ikke vurdert om Behandlingsoversikten etterlever kravene etter PVF art. 30 fullt ut, fordi det går utover problemstillingene jeg har formulert for min forskning. Likevel viser Behandlingsoversikten at Statens vegvesen har en god ordning på behandlinger når Vegvesenet er både behandlingsansvarlig databehandler. Å kartlegge behandlinger gjennom rolleidentifisering gir videre mulighet til å risikovurdere behandlingen på en mer ryddig måte. Det er fordi personvernforordningen setter flere krav til risikovurdering til behandlingsansvarlig enn databehandler.

Statens vegvesen er behandlingsansvarlig for behandlinger som skjer i arkivsystemet Mime 360. Behandlingsoversikten og særlig delen med 15 spørsmål for kvalitetssikring av behandlingen gir grunnlag for videre risikovurdering. Kvalitetssikring av behandlingen i Mime 360 gir mulighet for å identifisere og dokumentere tiltak for å utelukke avvik etter PVF art. 24 og 25. Ved for eksempel utydelig formål eller manglende rettslig grunnlag eller manglende ivaretakelse av de registrertes rettigheter og friheter viser systemet at det er risiko ved behandlingen. Kvalitetssikringsspørsmål har likevel også usikkerhets- og alvorlighetsgrad og beskrivelse av tiltak, noe som gjenspeiler krav etter PVF art. 24 og 25. Ved å først registrere Mime 360 i Behandlingsoversikten, får Statens vegvesen en full oversikt over behandlingen i systemet og eventuelle risiko for de registrertes rettigheter senkes betydelig. Kartlegging for å identifisere om det er krav etter PVF art. 35 tilsvarer forhåndsdefinerte risikoer som kan potensielt føre til krav om å gjennomføre en vurdering av personvernkonsekvenser, men tilsvarer en «normal» risikovurdering med sannsynlighets- og konsekvensvurdering og identifisering av tiltak, samt kartlegging av restrisiko.

Ved registrering av behandlingen oppgis blant annet informasjon om tekniske eller organisatoriske tiltak som gjennomføres i forbindelse med behandlingen. På den måten vises det klart sammenheng mellom risikovurderingen og Behandlingsoversikten gjennom registrering av egnede tiltak som skal bli identifisert og planlagt under en risikovurdering. Personvernforordningen presiserer imidlertid at tiltak som iverksettes skal være både tekniske og organisatoriske, og ikke være begrenset til de to typene, men flere. Statens Vegvesen har gitt mulighet å identifisere og planlegge kun en av type som ikke er riktig.

Beskrivelse av systemet og hvilke personopplysninger som behandlingen omfatter, registreres i systemet Verdivurdering. Informasjon i Verdivurdering representerer et grunnlag for videre risikovurdering, for konsekvensgrad baserer seg på flere kriterier. Detaljeringsgrad av personopplysninger, omfanget av personopplysninger og av de registrere og om det er sårbare eller utsatte grupper som er blant registrerte, samt om opplysninger av særlig kategori behandles er avgjørende for vurdering av hvor store konsekvenser for de registrertes rettigheter og friheter uønskede hendelser kan føre til.

Intervjuer har vist at Statens vegvesen har risikovurdert Mime 360 etter PVF art. 24 og 25 gjennom et system som omfatter både behandlingsoversikt og verdivurdering, samt at det vurderes om det er behov for vurdering av personvernkonsekvenser etter PVF art. 35. Risikovurdering etter PVF art. 32 skjer ved bruk av Excel-fil og risikomatrise. Statens vegvesen har utarbeidet både informasjonsbokser med forklarende tekst og lister over mulige uønskede hendelser og risikoreduserende tiltak, samt kriterier for sannsynlighet og konsekvenser. Det fører til tid- og ressurssparing, forutsatt at listene er omfattende nok for å unngå situasjoner der man mister en potensielt uønsket hendelse. For å utelukke slike tilfeller skal det være mulig å legge til en uønsket hendelse eller tiltak. I Excel-filen som brukes nå antar jeg at det er uproblematisk å legge til en manglende hendelse eller tiltak.

Det er viktig å legge merke til at fokus i risikovurderingen er systemet, selv om prosessene ikke glemmes og tenkes hele risikovurderingsprosessen. Jeg mener at det er nødvendig for å ta i utgangspunktet behandlinger i systemet, hvilke personopplysninger som behandles og behandlingens "art, omfang, formål og sammenhengen den utføres i" og andre hensyn som kan påvirke risikostørrelse. Det viktig å påpeke at å ha fokus på prosesser som skjer i systemet er et riktig fokus i en risikovurdering, for personvernforordningen stiller krav til risikovurdering av behandlingen og ikke systemer behandlingen skjer i.

Ved vurdering av risiko for behandlinger i Memi 360, vurderte Statens vegvesen sannsynlighetsgrad ut fra antagelser. Om det i hele tatt kan finnes muligheter for at en uønsket

hendelse inntreffer så må det vurderes. Med andre ord antar man hvor stor sannsynlighet for at hendelse inntreffer ut fra en alminnelig forståelse om sannsynlighet.

For å fastsette alvorlighetsgrad, eller størrelse på konsekvenser, er det heller ikke klare kriterier for definering av graden. Ved risikovurdering av Memi 360 tok man i utgangspunktet en alminnelig forståelse av fare og konsekvenser for de registrerte.

4.4 Samlet drøftelse av funnene

Forskningen min har vist at Statens vegvesen i sitt arbeid med kartlegging av behandlingen og risikovurdering av systemer og prosesser førte til at forvaltningsorganet skaffer seg en oversikt over prosesser, personopplysninger og IT-løsninger. Oversikten og etterfølgende verdivurdering danner et grunnlag for risikovurdering og identifisering av forpliktelser etter regelverket. Statens vegvesen har valgt å ta utgangspunkt kun i NSM sin veileder for verdivurderingen, men ikke for etterfølgende risikovurderingen. Fremgangsmåte imidlertid baserer seg på kravene i personvernregelverket. Siden Statens vegvesen er et forvaltningsorgan legges det også frem premisser i regelverket som er rettet mot offentlig sektor, slik som journalføring og arkivering.

Selv om det er en Excel-fil som brukes som verktøy for risikovurdering er grunnlaget allerede tilrettelagt for mer effektiv prosess. Sannsynlighet og konsekvens vurderes likevel kun på risiko knyttet til brudd på tilgjengelighet, konfidensialitet og integritet. Det er imidlertid behov for å inkludere brudd på robusthet som er nødvendig del av risikovurdering når det gjelder informasjonssikkerhet.

Jeg anser også at ved identifikasjon av uønsket hendelse og konsekvensgrad er det lurt å tenke "worst case". Det kan føre til høy risiko på mange områder, men samtidig åpnes muligheter for å forutsi flere hendelser og identifisere flere tiltak. Slike omstendigheter som påvirker risikostørrelse er særlig viktig når behandlingen gjelder sensitive opplysninger eller omfatter en stor mengde personopplysninger eller berører et stort antall registrerte. Ved å ta utgangspunkt i verste tilfelle, er det mulig å identifisere flere hendelser eller iverksette andre tiltak som ikke kunne har blitt tenkt på før, fordi risikoen er blitt vurdert som ubetydelig.

Fremgangsmåten til Statens vegvesen viser noen uklarheter. Jeg ser behovet for definering av kriterier for sannsynlighetsgrad og konsekvenser som avgjørende for at risikovurderingsprosess skal kunne regnes som helhetlig og troverdig. Det er helt nødvendig å avgrense når graden av sannsynlighet er for eksempel på 3 eller hvilke utfall for uønsket hendelse fører til alvorlige og hva skal egentlig regnes som en alvorlig konsekvens.

I tabell som er fremlagt nedenfor følger risikoakseptkriterier for sannsynlighet som kan være et eksempel for anvendelse av grunnlaget for risikovurderingen. Et eksempel på kriterier for sannsynlighet er følgende:

Sannsynlighet	**Historiske data**	**Kriterier**
Meget liten	Sjeldnere enn en hendelse pr. 10.år	a) Skjer kun unntaksvis b) Ingen kjente tilfeller (aldri hørt om) c) Svært lite sannsynlig d) < 10 %
Liten	1 gang pr. 10. år eller oftere	a) Skjer sjelden b) Kjenner tilfeller (år) c) Lite sannsynlig d) 10-30 %
Moderat	1 gang pr. 2. år eller oftere	a) Skjer av og til b) Flere enkelttilfeller (6 måneder) c) Mindre sannsynlig d) 30-50 %
Stor	1 gang pr. år eller oftere	a) Skjer ganske ofte b) Periodevis, lengre varighet (måned) c) Sannsynlig d) 50-90 %
Meget stor	10 ganger pr. år eller oftere	a) Skjer som regel/forventes å skje b) Kontinuerlig (daglig/ukentlig) c) Svært sannsynlig d) > 90 %

Figur 25 – Risikoakseptkriterier for sannsynlighet[90]

På den måten er det enklere å se om risiko er endret siden sist og om det er behov for oppdatert risikovurdering og iverksetting nye tiltak.

[90] UiB (2018) og Busmundrud (2018).

Statens vegvesen har definert skadepotensial ved brudd på informasjonssikkerheten ved konsekvensanalyse. Eksempel på det er brudd på personopplysningsloven[91] hvor det defineres hvor betydelig skaden er med et tilhørende felt for begrunnelse. Likevel viser ikke kommentaren til betydelige kriterier som ble anvendt for å definere skadepotensial.

Det er mulig å ta utgangspunktet i godt etablert praksis for risikovurdering innen HMS for å definere kriterier for konsekvenser. I tabell som er fremlagt nedenfor har jeg beskrevet kriterier innen personvern som kan være eksempel for konsekvens og er følgende:

Konsekvens	**Personskade (HMS)**	**Personvern**
Ubetydelig skade I svært liten grad	Ingen personskade	Avvik fra krav (Vilkår: Kun pseudonymiserte opplysningene, kun enkelte registrerte som er involvert)
Liten skade I liten grad dette lever vi godt med	Mindre skade som fører til førstehjelpstiltak/behandling	Avvik fra krav (Vilkår: Kun navn og kontaktinfo, lite antall registrerte som er involverte, kortvarig skade, ikke sårbare personer, ikke utsatte grupper)
Betydelig skade I noen grad kan være uheldig	En alvorlig personskade eller skade på flere, sykehusopphold	Avvik fra krav (Vilkår: Mer detaljert personopplysninger, større omfang av de registrerte/opplysninger er involvert, langvarig skade, sårbare personer, utsatte grupper, barn).
Svært alvorlig skade I stor grad	Kan resultere i langvarig sykehusopphold eller invaliditet	Brudd på personvernregelverket som fører til gebyr
Katastrofalt utfall I svært stor grad	Kan resultere i en eller flere døde	Brudd på personvernregelverket som fører til gebyr om omdømme/tillitstap

Figur 26 – Risikoakseptkriterier for konsekvens[92]

[91] Antar det omfattes både personopplysningsloven og personvernforordningen.
[92] UiB (2018) og Busmundrud (2018).

Som eksempel viser er det behov for klare kriterier for fastsettelse av konsekvensgrad. Tabellen ovenfor viser er det mulig å fastsette klare kriterier for grad av konsekvenser. Det er imidlertid vanskeligere å definere samme klare vilkår for personvernkonsekvenser. Det som er mulig er å liste noen kriterier som skal tas i betraktning under en risikovurdering.

Når det er klare vilkår for definering av graden til sannsynlighet og konsekvens er risikovurdering mer pålitelig. Det er også mer troverdig at risiko vil bli spesifisert mer nøyaktig.

Etter Statens vegvesen sine rutiner skal en risikovurdering gjennomgås hvert år. Jeg antar da at det er en risikovurdering etter PVF art. 32 som skal oppdateres. Personvernforordningen krever å opprettholde et egnet sikkerhetsnivå og det skal tolkes slik at det ikke er tilstrekkelig å kun oppdatere en risikovurdering etter en gitt tidsperiode. Etter min mening er det også viktig å gjøre en ny risikovurdering i tilfeller hvor fagpersoner, enten sikkerhetsansvarlige eller personvernombudet, har fått kunnskap om en trusselrisiko eller at rettslig praksis er oppdatert. Typiske eksempel på slike situasjoner er at en bedrift ble rammet av hackerangrep[93] som viser at det er behov for gjennomgåelse av systemsikkerhet, eller at en nasjonal tilsynsmyndighet varslet om et gebyr til en bedrift, som viser til en liknende situasjon i flere bedrifter.[94] Det er også nødvendig å fastsette kriterier eller en fast tidsperiode for å gjennomgå både systemet Behandlingsoversikten og systemet Verdivurdering som representerer en faktisk risikovurdering etter PVF art. 24 og 25. På den måten sikres etterlevelsen av krav og en lovlig behandling ellers.

[93] Hydro (2019).
[94] Datatilsynet (2020). Varsel om overtredelsesgebyr 19/01478-6/KBK.

5. Avsluttende kommentarer

Godt personvern er viktig forutsetning for offentlig forvaltning. Siden mye av innsamlingen av personopplysninger i offentlig sektor ikke er basert på samtykke, er det ekstra viktig at systemene som brukes er sikre nok og etterlever kravene i personvernforordningen. Risikovurdering kan føre til at man oppdager svakheter og avvik i systemet, men ved å etablere egnede tekniske og organisatoriske tiltak er det mulig å senke risikoen til et akseptabelt nivå. Både offentlig og privat sektor har en lang erfaring med risikovurderinger, men tidligere fokus har vært på informasjonssikkerhet. Personvernforordningen har innført krav til risikovurdering som gjelder andre aspekter, slik som innebygd personvern eller lovlighet av behandlingen.

Siden personvernforordningen trådte i kraft er det allerede flere eksempler på ikke tilfredsstillende ivaretakelse av informasjonssikkerhet og personvern. Disse eksemplene er kjent på grunn av gebyr nasjonale tilsynsmyndigheter gir til ulike virksomheter.

Allerede i 2018 fikk Norge eksempler på at ivaretakelsen av informasjonssikkerhet og personvern generelt ikke var tilfredsstillende. Det førte til ileggelse av overtredelsesgebyr for ikke å ha oppfylt pliktene til sikkerhetsledelse, risikovurderinger og tilgangsstyring i forbindelse med tjenesteutsetting av IKT-drift til utlandet.

Utfordringer knyttet til risikovurderinger, internkontroll og oversikt over hvilke personopplysninger virksomheter behandler var uakseptable. Gebyrene er følger av blant annet manglende risikovurderinger.[95] Men ikke minst er det de registrerte som opplever tap av rettigheter og friheter, misbruk av deres personopplysninger og mister tillit til de som behandler deres personopplysninger. Personvernidealet tilsier at tilliten til de som behandler personopplysninger er nødvendighet uavhengig av det rettslige grunnlaget behandlingen baserer seg.[96] Og det gjelder særlig offentlig sektor, fordi behandlingen av personopplysninger ofte hjemlet i lov, og ikke er basert på "frivillig, spesifikk, informert og utvetydig viljestyring.[97]

Et vesentlig argument for viktighet av gjennomføring av risikovurdering er Datatilsynets varsel om overtredelsesgebyr ved manglende risikovurdering og vurdering av personvernkonsekvenser.[98] Grunnlaget for varsling om gebyr er manglende gjennomføring av risikovurdering av personopplysninger og manglende gjennomgang av personvernkonsekvensene av behandlingen, jf. PVF art. 32, 35 og 5 nr 2. Saken er avgjørende for implementering av rettslig teori i praksis og

[95] Datatilsynet (2017). Varsel om overtredelsesgebyr til Akershus universitetssykehus HF 16/01531-53/GRA og andre helseforetak i Helse Sør-Øst.
[96] Regjeringen.no (2019).
[97] PVF art. 4 nr. 11: Vilkår for gyldig samtykke.
[98] Datatilsynet (2020). Varsel om overtredelsesgebyr 19/01478-6/KBK.

viser til hvilke kriterier som er definitive for tilsynsmyndigheten ved avgjørelse om det foreligger brudd på personvernregelverket og hvor grovt brudd er.

Statens vegvesen har valgt å kombinere etterlevelse av flere krav etter personvernforordningen gjennom systemene Behandlingsoversikt, Verdivurdering og til slutt en risikovurdering og etterfølgende implementere etterlevelse av kravene i systemer. Ved registrering av en behandling, føres samtidig protokoll over behandlingsaktiviteter og det dannes et grunnlag for å sikre at behandlingen er i tråd med regelverket. Med slik kartlegging dannes også et grunnlag for å ta hensyn til "behandlingens art, omfang, formål og sammenhengen den utføres i". Tekniske og organisatoriske tiltak som iverksettes skal imidlertid være basert på en risikovurdering. Ved fastsetting av kriterier for sannsynlighets- og alvorlighetsgrad, forsterkes grunnlaget for nødvendige tiltak.

Det er imidlertid veldig viktig å ha fokus på selve behandling av personopplysninger, og ikke systemet opplysningene behandles i, ved en risikovurdering. I tillegg er det de registrertes perspektiv som skal være utgangspunktet, ikke konsekvenser for bedriften. Fokus i risikovurdering skal være på konsekvensene for de registrerte i forbindelse med uønskede hendelser. I tillegg til klassiske sikkerhetsbrudd, slik som tap av konfidensialitet for taushetsbelagte personopplysninger, uautorisert oppheving av pseudonymisering mv, skal også andre ulemper inkluderes ved definering av risiko: Hendelser når de registrerte kan bli fratatt sine rettigheter og friheter eller bli hindret i å utøve kontroll over egne personopplysninger.

Gjennomføring av risikovurdering er en krevende prosess, men når en virksomhet lykkes med det, bidrar risikovurderingen til en helhetlig kontroll over behandlingsaktiviteter, sikrer et godt personvern ved at behandlingen er lovlig og at virksomheten ellers behandler personopplysninger i tråd med regelverket.

Funnene jeg har gjort er interessante, da det foreløpig er noe manglende erfaring på feltet for å gjennomføre en risikovurdering med fokus på personvern og ikke direkte på informasjonssikkerhet.

Kildeliste

Litteratur

Bergsjø (2020) — Bergsjø, Håkon, Ronny Windvik og Lasse Øverlier (red.). *Digital Sikkerhet. En innføring.* 1.utg., Oslo: Universitetsforl., 2020.

Busmundrud (2019) — Busmundrud, Odd. *Sannsynligheter og usikkerheter - begrepsavklaring i forbindelse med risikovurderinger* (FFI-rapport 18/02058). Kjeller: Forsvarets forskningsinstitutt, 2019.

Eckhoff (2001) — Eckhoff, Torstein. *Rettskildelære.* 5. utg., ved Jan Helgesen, Oslo: Universitetsforl., 2001.

Gimmingsrud (2017) — Gimmingsrud, Kari. "*En ny tidsalder for personvern i Europa."* Arbeidsrett vol. 14 nr. 2 (2017) s. 220–240 doi: 10.18261/issn.1504-3088-2017-02-03.

Jarbekk (2019) — Jarbekk, Eva, Simen Sommerfeld. *Personvern og GDPR i praksis.* 1.utg., Oslo: Cappelen Damm, 2019.

Kuner (2020) — Kuner, Christopher (red.) mfl. *The EU general data protection regulation (GDPR): A commentary.* Oxford University press, 2020.

Quelle (2017) — Quelle, Claudia. *«The «Risk Revolution» in EU Data Protection Law: We can't Have Our Cake and Eat it, Too»* i Data Protection and Privacy, Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth & Paul De Hert, Oxford and Portland, Oregon, Hart Publishing. 2017.

Schartum (2020) — Schartum, Dag Wiese. *Personvernforordningen - En lærebok.* Bergen: Vigmostad & Bjørke AS, 2020.

Rettskilder

1995	EUROPAPARLAMENTS- OG RÅDSDIREKTIV 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (Personverndirektivet).
1996	Forskrift 06. desember 1996 nr. 1127 om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (Internkontrollforskriften).
2000	Forskrift 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften)
2000	Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
2004	Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).
2011	Forskrift 06. desember 2011 nr. 1355 om organisering, ledelse og medvirkning.
2011	Forskrift 06. desember 2011 nr. 1357 om utførelse av arbeid, bruk av arbeidsutstyr og tilhørende tekniske krav (forskrift om utførelse av arbeid).
2016	EUs personvernforordning (EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av

	direktiv 95/46/EF (generell personvernforordning).
2017	Forskrift 15. desember 2017 nr. 2105 om offentlege arkiv.
2018	Forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).
2018	Lov 01. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).
2018	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).
Meld. St. 28 (2018–2019)	Datatilsynets og Personvernnemndas årsrapporter for 2018.
NOU 2016: 19	*Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.*

Andre kilder

Datatilsynet (2017)	*Varsel om overtredelsesgebyr 16/01531-45/GRA.*
Datatilsynet (2017)	*Varsel om overtredelsesgebyr 16/01531-53/GRA.*
Datatilsynet (2020)	*Varsel om overtredelsesgebyr 19/01478-6/KBK.*
Datatilsynet (2020)	Årsrapport for 2019. *Tall og tendenser fra Datatilsynets virksomhet.*
Datatilsynet (2018)	Risiko og risikovurdering. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-

personvernkonsekvenser/risikovurdering/ hentet 15.02.2020.

Datatilsynet. (u.å.) Risikovurdering av informasjonssystem. https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/risikovurdering_veileder.pdf hentet 02.02.2020.

Digitaliseringsdirektoratet. (u.å.) *Begrepsliste - Systemeier*. https://internkontroll-infosikkerhet.difi.no/begrepsliste-systemeier hentet 15.06.2020.

Digitaliseringsdirektoratet. (u.å.) *Hva sier ISO/IEC 27001?* https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001 hentet 04.06.2020.

EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

Hydro. *Cyberangrep på Hydro* (2020) https://www.hydro.com/no-NO/media/on-the-agenda/cyberangrep-pa-hydro/ hentet 24.06.2020.

Regjeringen.no *Hva er personvern?* (2019) https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-personvern/id448290/ hentet 06.05.2020.

Standard Norge *Informasjonssikkerhet, cybersikkerhet og personvern Informasjonssikkerhet, cybersikkerhet og personvern - Retningslinjer for revisjon av ledelsessystemer for informasjonssikkerhet* (NS-ISO/IEC 27007). 2020.

Standard Norge *Informasjonsteknologi — Sikringsteknikker — Ledelsessystemer for informasjonssikkerhet — Oversikt og terminologi* (ISO/IEC 27000). 2016.

Standard Norge	*Krav til risikovurderinger* (NS 5814). 2008.
Standard Norge	*Risikostyring. Prinsipper og retningslinjer* (NS-ISO 31000). 2018.
Standard Norge	*Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Terminologi*. (NS 5830). 2012.
Standard Norge	*Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse* (NS 5832). 2014.
Statens vegvesen (2019)	*Statens vegvesen brev til Fylkesmannen 19/355002-1*. https://www.vegvesen.no/om+statens+vegvesen/om+organisasjonen/om-statens-vegvesen hentet 16.06.2020.
Store norske leksikon (u.å.)	https://snl.no/.search?query=Robusthet hentet 23.05.2020.
UiB. Risikoakseptkriterier for sannsynlighet og konsekvens innen HMS-feltet (2018)	http://ekstern.filer.uib.no/poa/Hms/Risikovurdering/Risikoakseptkriterier27.02.18.pdf hentet 17.05.2020.
WP29 (2010)	Article 29 Working Party. "Opinion 3/2010 on the Principle of Accountability» (WP173, 13 July 2010).
WP29 (2017)	Article 29 Working Party. "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to results in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01."

Vedlegg

Excel-verktøy for risikovurdering

Referat fra intervju

Skjermbilder BO

Skjermbilde VV