ROS-analyse av Kontakt- og reservasjonsregisteret

Innhold

1 Innledning

Kontakt- og reservasjonsregisteret er en ny felleskomponent for offentlig sektor, hjemlet i forvaltningsloven § 15a, tredje ledd b) og nærmere regulert i eForvaltningsforskriften kap. 7.

Registeret inneholder nærmere spesifiserte kontaktopplysninger om privatpersoner. Opplysningene kan benyttes i forbindelse med saksbehandling og utføring av forvaltningsoppgaver, for øvrig jamfør eForvaltningsforskriften § 29 annet ledd, og skal benyttes til varsling etter eForvaltningsforskriften § 8 tredje ledd. Alle offentlige virksomheter kan bruke kontaktopplysningene til den enkelte, uten eksplisitt samtykke fra den registrerte.

Oppslagstjenesten er de offentlige virksomhetenes grensesnitt mot kontakt- og reservasjonsregisteret.

Herværende dokument er Difis ROS-analyse for Kontakt- og reservasjonsregisteret, med tilhørende Oppslagstjeneste.

Analysen inneholder risiko for informasjonssikkerhetsbrudd, slik Difi ser den, med innspill i fra andre virksomheter. Den enkelte virksomhet som ønsker å ta registeret i bruk må foreta sin egen analyse, men risikoregisteret som er vedlagt kan brukes som innspill til hendelser og scenarier.

1.1 Hva er Kontakt- og reservasjonsregisteret og Oppslagstjenesten?

Kontakt- og reservasjonsregisteret inneholder kontaktinformasjon for mer enn 3,3 millioner brukere. Registeret inneholder informasjon om:

- Hvorvidt innbyggere har reservert seg mot digital kommunikasjon mot det offentlige eller ikke, i henhold til eForvaltningsforskriften § 9.
- Foretrukket e-postadresse og mobilnummer
    - Innbyggere kan kun registrere én e-postadresse og ett mobilnummer i registeret, og må ikke registrere begge deler.
- Adresse til mottakers digital postkasse for mottak av digitale brev fra offentlig sektor
- Sertifikatinformasjon for postkasseleverandører, som har avtale med Difi.
- Sertifikatinformasjon for utskriftsleverandør (kommer når utskrifts- og forsendelsestjenesten produksjonssettes)

Se også kapittelet «Opplysninger i Kontakt- og reservasjonsregisteret» under.

Oppslagstjenesten gir offentlig forvaltning tilgang til opplysningene i kontakt- og reservasjonsregisteret. Dette er innbyggeres egenregistrerte kontaktinformasjon (e-postadresse og mobilnummer), reservasjonsstatus, valgt digital postkasse for mottak av digitale brev fra offentlig sektor, og sertifikatinformasjon som skal benyttes for kryptering til en digital postkasse eller, utskriftsleverandøren.

Tilgang kan gis offentlige virksomheter og virksomheter som utfører tjenester på vegne av det offentlige. Virksomheter kobler seg opp mot Oppslagstjenesten, og kan gjennom forskjellige grensesnitt hente ut kontaktinformasjon om innbyggere, samt informasjon om hvilke innbyggere som har reservert seg mot digital kommunikasjon. På sikt kan Oppslagstjenesten ha mulighet for å gi tilgang også til andre registre, men det er ikke vurdert i denne sammenheng. Registrering og oppdatering av informasjonen ligger til de ulike registrene og er ikke en del av Oppslagstjenesten.

Inntil videre vil Kontaktregisteret levere postkasseleverandørens sertifikat for hver innbygger, men på sikt kan disse erstattes med personlige sertifikater uten endring i avsendervirksomhetenes grensesnitt mot Oppslagstjenesten.

1.1.1 Aktører

Følgende aktører er involvert i Kontakt- og reservasjonsregisteret og Oppslagstjenesten:

Aktør	Beskrivelse
Sentralforvalter	Difi er forvalter av Kontakt- og reservasjonsregisteret og Oppslagstjenesten.
Offentlig virksomhet	Virksomhet som henter kontaktinformasjon fra Oppslagstjenesten. Må akseptere Difis bruksvilkår før integrasjon. Kan være en offentlig virksomhet, eller virksomheter som opptrer på vegne av det offentlige. Benevnes som «virksomhet» i dette dokumentet.
Innbygger	Privatperson som har registrert opplysning i Kontakt- og reservasjonsregisteret. Også omtalt som «person».
ID-porten	Felleskomponent for autentisering i offentlig sektor. Brukes for å få innbyggere til å holde informasjon i kontakt- og reservasjonsregisteret oppdatert. Kan videreformidle informasjon fra kontakt- og reservasjonsregisteret til offentlig virksomhet når sluttbruker autentiseres ved hjelp av saml2. Bruker kontakt- og reservasjonsregisterets interne grensesnitt for å hente opplysninger.
MinID	Elektronisk identitetsbevis på mellomhøyt sikkerhetsnivå (nivå 3), utstedt av Difi for bruk i offentlig sektor. Holdes oppdatert med opplysninger i fra kontakt- og reservasjonsregisteret.
Printleverandør	Leverandør av meldingsformidlertjenesten i Digital postkasse til innbyggere som også leverer utskrifts- og forsendelsestjenesten (Posten Norge AS v/Digipost)

1.1.2 Kilder til endringer i Kontakt- og reservasjonsregisteret

Det er følgende kilder til endringer i Kontakt- og reservasjonsregisteret:

Kilde	Beskrivelse
Personen selv	Hovedårsaken til endringer i Kontakt- og reservasjonsregisteret vil være endringer gjort av personen selv, enten det er kontaktinformasjon som er lagt til, endret eller fjernet, eller om det er reservasjon som er gjort eller opphevet.
Registertjenesten selv eller andre sentrale tjenester	Visse endringer tilknyttet opprydding og verifikasjon gjennomføres av registertjenesten selv, eksempelvis sletting av kontoer som ikke har vært i bruk i en gitt tidsperiode.
Postkasseleverandør	Endringer i registeret kan også komme fra postkasseleverandør i forbindelse med at innbygger har valgt eller endret digital postkasse for mottak av digitale brev fra offentlig sektor, og postkasseleverandøren oppdaterer informasjon i henhold til dette. Postkasseleverandør er den som forvalter sertifikatinformasjonen som avgis til registeret.
Det sentrale folkeregisteret (DSF)	Kontakt- og reservasjonsregisteret ajourføres («vaskes») mot DSF jevnlig. Personer som ikke lenger er oppført i DSF, eller er oppført som forsvunnet, død eller utgått fødselsnummer, eller som har fått nytt F-nummer eller D-nummer, i DSF og ikke lengre er oppført i DSF, slettes fra registeret. Det er ingen direkte integrasjon mellom DSF og Kontakt- og reservasjonsregistret per dags dato så vaskingen er en manuell prosess.
Sentralforvalter	Sentralforvalter vil kunne legge inn testbrukere for kortere perioder. Dette for å understøtte behov for testing. Dette vil kunne medføre at fiktive personer blir opprettet og slettet.
Brukerstøtte	Brukerstøtte kan legge inn reserveringer, endre opplysninger om brukere og slette brukere på forespørsel om bistand fra innbyggeren. Brukerstøtte hos Difi har denne muligheten. I tillegg kan Skatteopplysningen legge inn reserveringer.

1.1.3 Sletting fra Kontakt- og reservasjonsregisteret

En innbygger kan kreve seg slettet i fra Kontakt- og reservasjonsregisteret ihht. eForvaltningsforskriften § 34. I tillegg kan en innbygger bli slettet i fra registeret som følge av vask mot DSF. Årsakene knyttet til hvorfor en person slettes fra registeret er beskrevet i begrepskatalogen. Se kodeverk for feltet *beskrivelse* på person i registeret her: http://begrep.difi.no/Oppslagstjenesten/Person.html.

1.1.4 Overordnet teknisk beskrivelse

For teknisk systembeskrivelse henvises det til oppdatert dokumentasjon, eksempelvis Integrasjonsguidene på http://begrep.difi.no/Oppslagstjenesten/ .

1.1.4.1 Datamodell

Datamodellen og alle begrep brukt i tjenesten er dokumentert i begrepskatalogen, tilgjengelig på http://begrep.difi.no/. Denne datamodellen brukes både i webservicetjenesten og i fil-grensesnittet.

1.1.5 Opplysninger i Kontakt- og reservasjonsregisteret

Konfidensialitetsbehovet for opplysningene som er lagret i Kontakt- og reservasjonsregisteret kan vurderes etter flere innfallsvinkler. Én vil være hvordan innbyggerne håndterer denne typen opplysninger – det vil gi signaler om i hvilken grad de ønsker å begrense distribusjonen.

De fleste innbyggeres telefonnumre er tilgjengelige gjennom åpne nummeropplysningstjenester, som 1881.no. Noen har imidlertid valgt å reservere seg mot slike tjenester, og noen har også valgt å bestille tjenesten Hemmelig telefonnummer hos sin teleoperatør. Hemmelig telefonnummer gjør telefonnummeret utilgjengelig i opplysningstjenester og skjerming mot nummervisning ved utgående kommunikasjon. Det kan også innebære strengere tilgangsstyring internt hos teleoperatøren til abonnentopplysningene. Tjenesten hemmelig nummer er et tilbud til personer som mener de har et sterkt behov for anonymitet, for eksempel personer som har en offentlig utsatt posisjon eller som er offer for sjikane, og av den grunn har behov for den beskyttelsen et hemmelig nummer gir.

For trusselutsatte vil det være viktig å unngå at geolokaliserende informasjon røpes. E-postadresse kan i seg selv gi geolokaliserende informasjon (navn@utsira.kommune.no). E-postadresse kan også brukes som nøkkel inn mot søketjenester, og slik røpe geolokaliserbare opplysninger. Telefonnummer kan brukes på samme måte. E-postadresse og mobilnummer er unike søkebegrep og kan gjerne gi bedre treff enn søk på navn.

Opplysningene i kontaktregisteret ble opprinnelig samlet inn for bruk til innlogging med MinID. Ved endringer i eForvaltningsforskriften februar 2014 ble det åpnet for at opplysningene utleveres til kontaktregisteret, jf. efvf § 38 første ledd. Den registrerte skal i den anledning informeres om utleveringen og adgangen til å slette seg m.v. Det fremgår av efvf § 29 annet ledd at opplysningene i registeret skal brukes til varsling, og kan benyttes «i forbindelse med saksbehandling og utføring av forvaltningsoppgaver for øvrig». Bestemmelsen er ihht. forarbeidene (statsrådsforedraget) ment å dekke forvaltningens totale oppgaveløsning. Det er nærliggende å tolke bestemmelsen ikke bare som en formålsangivelse, men også som en formålsbegrensning, jf. også at bruk av personopplysninger til vesentlig endrede formål i utgangspunktet vil kreve samtykke etter personopplysningsloven § 11 første ledd bokstav c.

Opplysninger som kan føre til oppsporing av trusselutsatte personer (personer med adressesperring i folkeregisteret), må regnes som et personlig forhold, og er derved omfattet av taushetsplikt. Se nærmere omtale i 1.1.6.

Integriteten til opplysningene er viktig. For at registeret skal være nyttig er det viktig at informasjonen som ligger lagret har god kvalitet og er oppdatert. Som tiltak for å ivareta kvaliteten på opplysningene blir innbyggere i forbindelse med innlogging til offentlige tjenester på nett via ID-porten, bedt om å verifisere sine opplysninger med jevne mellomrom (p. t. etter 90 dager). Dersom opplysninger om den enkelte i register over digital kontaktinformasjon og reservasjon ikke har blitt oppdatert eller bekreftet at er korrekte de siste 18 månedene, skal opplysningene ikke brukes til å varsle vedkommende etter eForvaltningsforskriftens § 8 tredje ledd.

Tilgjengeligheten til informasjonen er viktig i utsendelses- og oppslagstidspunkt. Etter hvert som flere systemer tar Kontakt- og reservasjonsregisteret i bruk, vil viktigheten av tilgjengelige opplysninger øke.

Både integritets- og tilgjengelighetsbrudd vil føre til at innbygger ikke får varsel om at vedtak og andre viktige henvendelser er fattet/klargjort og hvor det er tilgjengeliggjort digitalt.

I risikoregisteret som er utarbeidet samtidig med denne rapporten er det beskrevet en rekke risikoscenarioer med vurdering av sannsynlighet og konsekvens. Risikoscenarioene omfatter potensielle hendelser som innvirker på tjenestens konfidensialitet, integritet, og tilgjengelighet.

Følgende opplysninger fra kontakt- og reservasjonsregisteret leveres via Oppslagstjenesten:

Opplysning	Beskrivelse
Personidentifikator	Fødselsnummer eller D-nummer.
Epostadresse	Som innbyggeren selv registrerer
Mobilnummer	Som innbyggeren selv registrerer
Reservasjon	Status som innbyggeren selv setter
Status	Flagg som varsler om innbyggeren er aktiv eller ei.
SikkerPostkasseadresse	Adressen på valgt digitale postkasse for mottak av digitale brev fra offentlig sektor. Adressen settes automatisk fra postkasseleverandørene (Digipost eller eBoks).
Postkasseleverandør-adresse	Digipost eller e-Boks på nåværende tidspunkt
X509Certificate	Sertifikat for kryptering av digital post til innbygger. Inntil videre vil postkasseleverandørens sertifikat benyttes, men løsningen kan støtte personlige sertifikater.
Sist oppdatert dato	Dato for når opplysningene sist var oppdatert.
Sist verifisert-dato	Dato for når en innbygger sist bekreftet at opplysningene er korrekte, eller benyttet opplysningene.

I utgangspunktet er det innbyggeren selv som skal oppdatere kontaktinformasjonen i registeret. Det hentes ikke inn informasjon fra andre kilder for å berike registeret. Første versjon av registeret er hentet inn ved å ta en kopi av brukeropplysningene i MinID.

Kvaliteten på informasjonen som ligger i basen er avhengig av hvor flinke innbyggerne er til å oppdatere informasjonen sin, og at man oppgir rett informasjon.

Ved en spørring mot tjenesten vil man få returnert forespurt data, også for innbyggere som har reservert seg mot å få vedtak og andre viktige henvendelser digitalt. Det er opp til virksomhetene selv å sjekke for reservasjonsstatus ved utsendelser som er omfattet av reservasjonsretten.

1.1.6 Taushetsbelagte opplysninger

For de aller fleste innbyggere er ikke opplysningene som er lagret i registeret taushetsbelagte. Opplysninger som er lagt inn av innbyggere, telefonnummer og e-postadresse, kan bli eksponert for alle offentlige virksomheter som benytter registeret. Om opplysningene ble registrert i tilknytning til bruk av MinID, vil den utvidede bruken med kontakt- og reservasjonsregisteret medføre at eksponering av opplysningene utvides vesentlig. Difi har ikke noen oversikt over status på de opplysningene som er registrert, eksempelvis om opplysningene kan føre til oppsporing av trusselutsatte (personer med adressesperring i folkeregisteret). Om opplysningene kan føre til slik oppsporing vil det være opplysninger om personlige forhold som vil være omfattet av taushetsplikt. Slike opplysninger vil virksomhetene måtte sikre på tilfredsstillende måte ihht. forvaltningsloven § 13, slik som tilgangsbegrensning eller logging. Alternativt kan det gjøres tiltak som fjerner slike opplysninger i fra registeret. Det er innledet dialog med Politiet, som har innspill på hvordan personer som er beskyttet i henhold til kode-6 i folkeregisteret (adressesperring, ikke tilgjengelig for det offentlige) bør håndteres. Politiet er i utgangspunktet positive til at personer i kode-6 skal kunne være digitale, og ser at dette kan være et godt tilbud til trusselutsatte, forutsatt at de legger inn «hvite opplysninger» (opplysninger som ikke inneholder f.eks. geolokaliserbare data og andre sporbare data). Det bør utarbeides spesiell informasjon og fullmakt for personer som trer inn i kode-6-regimet, slik at man kan slette vedkommende i fra registeret, og informerer om hva som er fornuftige opplysninger å bruke ved opprettelse av nytt innslag i registeret. For kode-7 (fortrolig adresse, ikke tilgjengelig for private) ser man ikke behov for tiltak.

1.1.7 Datakvalitet

Det er gjort tiltak for å sikre kvaliteten på formasjonen som ligger i registeret. Det er registrert mer enn 3,3 millioner innbyggere med opplysninger i registeret. Av disse 3,3 millionene, er det 2,6 millioner som har oppdatert eller bekreftet sin kontaktinformasjon i perioden 10. februar 2014 til 6. mai 2014. De resterende er varslet både med e-post og SMS om ny bruk av den registrerte e-postadresse og mobilnummer. Det har her vært mulig å kartlegge om SMSen er levert ved å få statuskode DELIVERD i retur fra mobilleverandør. Dette bekrefter at meldingen er mottatt og at nummeret dermed er aktivt, men ikke om meldingen er lest eller om nummeret er tilknyttet riktig person. E-postene inneholdt en skjult lenke som returnerte en lesekvittering såfremt e-posten ble åpnet i en e-postleser med HTML aktivert.

De personene hvor verken e-post eller SMS ble levert, fikk tilsendt brev. Disse personenes kontaktinformasjon er slettet fra registeret og i brevet ble vedkommende oppfordret til å registrere seg på nytt. Dette omfatter ca. 93 000 personer.

Innbyggere har samtidig blitt informert om mulighet for å reservere seg mot å få enkeltvedtak og andre viktige henvendelser fra forvaltningen digitalt. Innbygger har ikke blitt direkte informert om hvordan de sletter kontaktinformasjonen, dersom de ikke aksepterer endret bruk. De er derimot informert om at det finnes relevant informasjon på norge.no. Her er sletting omtalt.

Oppsummert kan vi si at datakvaliteten med høy sannsynlighet er svært god. Imidlertid vil aldri innholdet være 100 % korrekt. Innbygger kan ha registrert feil informasjon – ved uhell eller overlegg.

Innbyggere kan ha byttet e-postadresse/telefonnummer og ikke endret det i kontaktregisteret. Andre feilkilder vil også forekomme. Antallet feiloppføringer i registeret er svært vanskelig å tallfeste.

1.2 Metode og arbeidsform

Prosjektet har fulgt standarden ISO/IEC 27005:2011 i arbeidet med å gjennomføre ROS-analysen, jf. Standardiseringsrådets anbefaling av 13. mars 2012. Termen *standarden* benyttes isteden for *ISO/IEC 27005:2011* nedenfor. Med Normen menes «*Norm for informasjonssikkerhet i helse- omsorgs- og sosialsektoren*» (2013) og med *Faktaark* de faktaarkene som er utarbeidet i tråd med Normen. Normen med veileder for risikovurdering og Faktaarkene er i denne ROS-analysen benyttet til innspill, sammen med Datatilsynets veileder for risikovurdering i informasjonssystemer, til definisjon av sannsynlighetsnivåer og konsekvens.

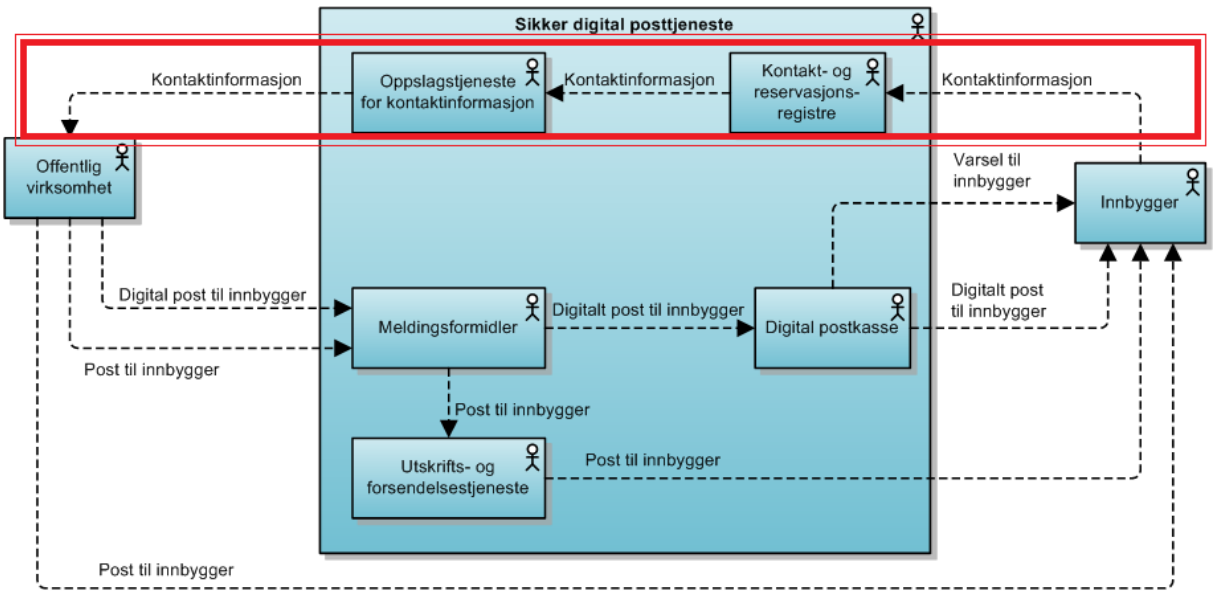
Første del av ROS-analysen var å etablere en kontekst for selve risikoanalysen. Andre del er å forstå hvilke risikoer som verdier i systemet utsettes for, og komme med forslag til tiltak for å redusere risiko.

ROS-prosjektet har diskutert og dokumentert opplevelse av trusler og sårbarheter, sannsynligheter og konsekvenser for derigjennom å kunne strukturere denne informasjonen i en ROS-analyse, hvoretter risiko kan evalueres og risikoreduserende tiltak foreslås. Knytningen mellom prosjektets arbeid og standarden er søkt klargjort ved henvisninger i rapporten, slik at det skal være lett å verifisere at alle aktivitetene omtalt i standarden er behandlet. Denne tilnærmingen vil også forenkle senere oppdateringer av ROS-analysen.

1.2.1 Scope

Denne rapporten omfatter ROS-analyse av Kontakt- og reservasjonsregisteret, med tilhørende Oppslagstjeneste. I tillegg finnes det en egen analyse for Digital postkasse til innbyggere.

Rapporten redegjør for grunnleggende trekk ved Kontakt- og reservasjonsregisteret, med tilhørende Oppslagstjeneste, avklarer involverte aktører, og redegjør for trusselbildet knyttet til denne delen av den totale tjenesten Digital postkasse til innbyggere. Den angir også akseptert risiko og gir anbefalinger på hvilke sikkerhetstiltak som bør iverksettes for å styre et gitt risikoscenario til akseptert nivå.



Figur 1 Scope for ROS-analyse av kontakt- og reservasjonsregisteret og oppslagstjenesten

1.2.2 Avgrensninger

Herværende rapport er avgrenset til å ROS-analysere Kontakt- og reservasjonsregisteret, med tilhørende Oppslagstjeneste. Øvrige komponenter/systemer og tilhørende aktører i den totale tjenesten Digital postkasse til innbyggere faller dermed utenfor scope for denne analysen og tas ikke med i betraktning med mindre det har en direkte innvirkning på de komponentene/systemene som analyseres. Dette omfatter blant annet selve den digitale postkasseløsningen, meldingsformidler, og utskrifts- og forsendelsestjenesten. Det vil bli gjennomført en egen ROS-analyse av Digital postkasse til innbyggere. Virksomhetenes systemer som benytter Oppslagstjenesten og Kontakt- og reservasjonsregisteret faller også utenfor scope. Dette forutsettes gjort av virksomhetene selv. Forpliktelser som Difi har påtatt seg i bruksvilkårene, slik som tjenestenivå og katastrofeberedskap er innenfor scope.

Risiko som ligger hos de forskjellige virksomhetene som skal benytte seg av Kontakt- og reservasjonsregisteret og Oppslagstjenesten inngår således ikke i analysen, ei heller risiko internt hos andre involverte parter. Noen av risikoene som avdekkes i rapporten bør imidlertid håndteres med tiltak hos virksomhetene.

Innbyggers risikoappetitt er ikke inkludert. Vurderingen av risiko knyttet til innbygger gir utfordringer med tanke på at hver innbygger har sitt eget miljø og egne sikkerhetstiltak. Disse miljøene, med sikkerhetstiltak, ligger utenfor vår kontroll, og kan stort sett bare påvirkes med informasjon og opplæring. Det vil være noe risiko som knyttes til innbyggernes informasjon som de selv lagrer i registeret. Se også omtale av denne risikoen under Evaluering av risiko i 4.2.

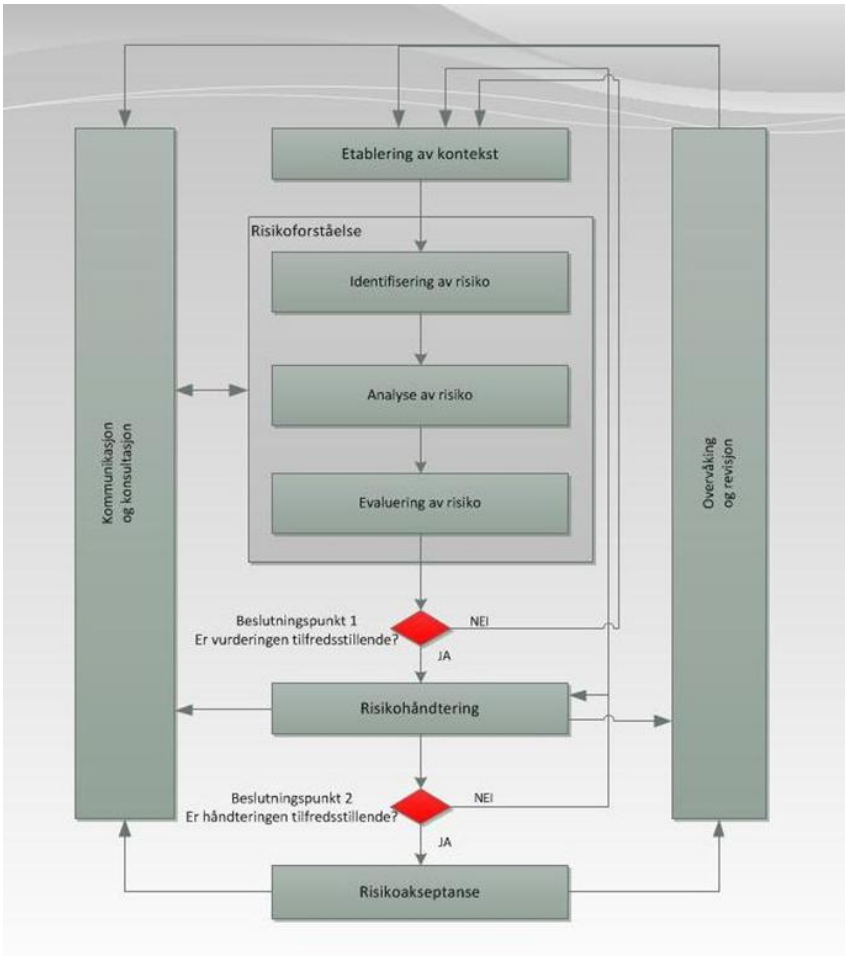
En rekke av de tekniske tiltakene gjennomføres av driftsleverandøren. I og med at driftsleverandøren skal byttes høsten 2014 er det tiltakene hos, og avtalene med, den nye driftsleverandøren (Evry) som ligger til grunn for vurderingene i denne analysen.

2 Risikoforståelse

Målet med å skaffe frem en forståelse av risikoene i systemet er å kunne iverksette de riktige tiltakene. Stegene for å etablere forståelse av risiko følger av standardens kapittel 8.1 og består av tre trinn:

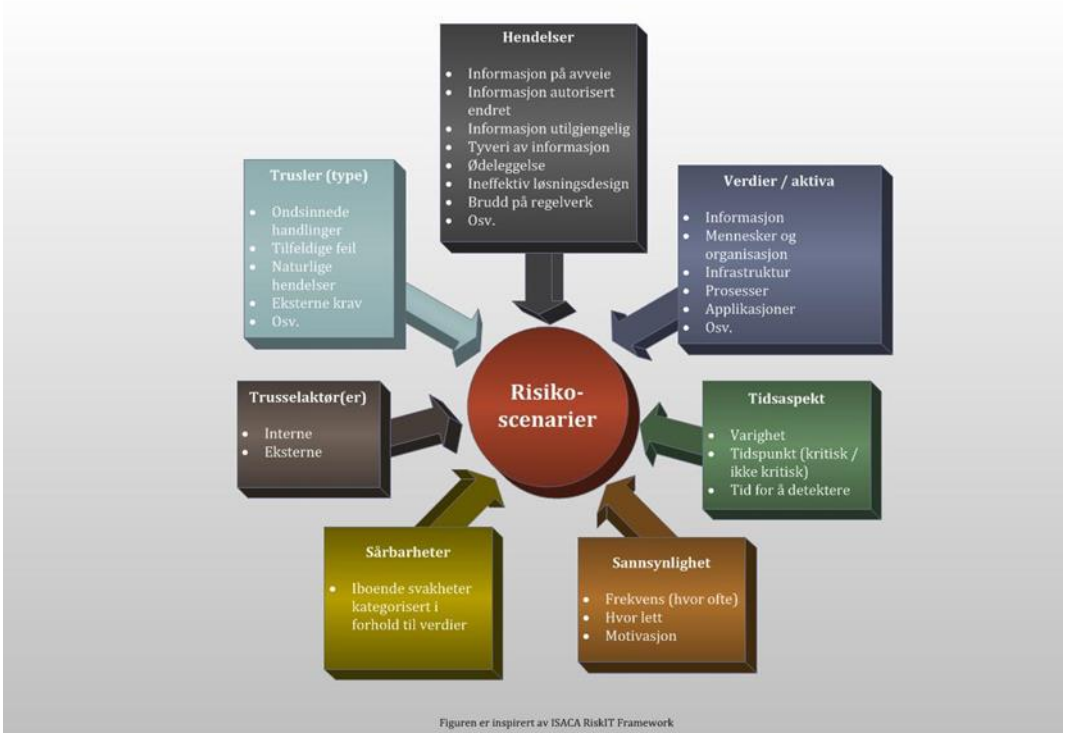
1. Det identifiseres risikoer som utsetter verdiene for fare. Risiko oppstår som en følge av en uønsket hendelse, enten direkte eller indirekte.
2. Risikoen analyseres ved å bestemme risikonivået. Nivået uttrykkes som en kombinasjon av konsekvens av en uønsket hendelse og sannsynligheten for at den skal inntreffe.
3. Risikonivået evalueres opp mot virksomhetens akseptable risiko.

En meningsfylt risikoforståelse forutsetter en veldefinert kontekst. Konteksten inneholder ikke bare kriteriene for risiko, konsekvens og så videre, men også en systemmodell og beskrivelse av hvilke verdier som står på spill. Konteksten beskrives både i de innledende kapitlene samt under hvert av de relevante kapitlene i denne ROS-analysen.



Figur 2 Prosess for ROS-analyse, jf. ISO/IEC 27005:2011

Ettersom risikoene vil bli ordnet etter hvor alvorlige de er sikrer man at tiltak iverksettes i riktig rekkefølge. Dersom restrisikoen vurderes å være for stor etter at rimelige tiltak er iverksatt, må det gjennomføres en ny runde. Dette er i tråd med standarden.



Figur 3 Elementer i risikoscenarioer

Selv om risiko, i teorien, oppstår i møtet mellom en verdi og en uønsket hendelse så er bildet naturligvis mer komplisert. Som vist i «Figur 3 Elementer i risikoscenarioer» så påvirkes risikoen av mange forskjellige elementer.

Når det gjelder uønskede hendelser, så kan man velge å se på dem på forskjellige måter. For eksempel kan man si at *lekkasje av informasjon* er en uønsket hendelse, og at det kan skje som en følge av at *et varsel er sendt til en gal adresse*. Alternativt, og likeverdig, kan man si at *et varsel som kommer på avveie* er en uønsket hendelse og at konsekvensen er *at informasjon lekker ut*. Til syvende og sist er man opptatt av hva resultatet er for den som eier verdien (tap av omdømme, brudd på lov eller forskrift, brudd på ønsket / pålegg om konfidensialitet, og så videre). I dette tilfellet vil informasjonslekkasjen omfatte varselet og den informasjonen som ligger i varslingsteksten. For eksempel: «Skatteoppgjøret ditt er nå tilgjengelig på Skatteetatens nettsider. Vennlig hilsen Skatteetaten». Lekkasjen av informasjon vil ikke omfatte selve skatteoppgjøret.

Resultatet av arbeidet med risikoforståelse er en oversikt over risikoer, prioritert i henhold til kriteriene som er fastlagt.

2.1 Identifisering av risiko

Behovet for å identifisere risiko følger av standardens kapittel 8.2.

ROS-analyser skal besvare (minst) tre spørsmål:

1. Hva kan gå galt?
2. Hvor sannsynlig er det at dette går galt?
3. Hva blir konsekvensen hvis det som kan gå galt går galt?

Hensikten med å identifisere risiko er å finne «ting» som kan skje, som igjen kan føre til et potensielt tap/skade og så undersøke hvor og hvordan et slikt tap/skade kan oppstå. Deretter lokaliserer man eksisterende mottiltak og deres innvirkning på risikoen. Til slutt vurderer man konsekvensen(e).

Risiko blir identifisert gjennom en prosess i fem steg som går ut på å identifisere:

1. Verdier
2. Trusler
3. Eksisterende tiltak
4. Sårbarheter
5. Konsekvenser.

Det er hverken nødvendig eller ønskelig å gjennomføre de fem delene sekvensielt.

2.1.1 Identifisering av verdier

Identifisering av verdier følger av standardens kapittel 8.2.2. En verdi er alt som anses som verdifullt for en virksomhet.

Analysedelen (kap. 3) inneholder en oversikt over verdiene tilknyttet Kontakt- og reservasjonsregisteret og Oppslagstjenesten.

2.1.2 Identifisering av trusler

Identifisering av trusler følger av standardens kapittel 8.2.3. En trussel er et potensiale for at en verdi kan påvirkes negativt.

Trusler kan være naturlige (flom) eller resultatet av en menneskelig handling, de kan komme innenifra eller fra utsiden av tjenesten, med eller uten hensikt, som en (indirekte) følge av et uhell, og så videre. Noen trusler påvirker flere verdier og noen trusler fører til kjeder av uønskede hendelser.

En *trusselaktør* er den eller det som genererer trusselen, eller sagt på en annen måte; det eller den som utnytter en sårbarhet/svakhet ved systemet og dermed skaper en uønsket hendelse. En trusselaktør behøver altså ikke være et menneske, eller for den saks skyld en som handler med overlegg.

2.1.3 Identifisering av eksisterende og planlagte tiltak

Identifisering av eksisterende og planlagte tiltak følger av standardens kapittel 8.2.4. Tiltak benyttes for å kontrollere risiko.

Standarden slår fast at planlagte tiltak skal sidestilles med eksisterende tiltak.

Eventuelle eksisterende tiltak eller risikohåndteringsplaner skal identifiseres og dokumenteres. For virksomheten kan dette være eksisterende kriseløsninger dersom de regulære virksomhetsprosessene av en eller annen grunn gjøres uvirksomme. Et eksempel på dette kan være at man har etablert manuelle eller automatiske utsendelses- eller oppslagsløsninger som kan tre i kraft dersom digitale løsninger feiler.

2.1.4 Identifisering av sårbarheter

Identifisering av sårbarheter følger av standardens kapittel 8.2.5. En sårbarhet er en iboende svakhet.

Med utgangspunkt i identifiserte trusler, de identifiserte verdiene og alle eksisterende og planlagte tiltak søker man å identifisere sårbarheter. En sårbarhet kan ikke i seg selv skade en verdi, dette kan først skje dersom det eksisterer en trussel som kan utnytte sårbarheten. Det er derfor viktig å ha både verdiene og truslene som bakteppe når sårbarheter skal identifiseres.

Det er laget en oversikt over hendelser som er knyttet til sårbarhetene som er relatert til de verdiene som er identifisert, de truslene som er identifisert og eventuelle tiltak som er implementert.

2.1.5 Identifisering av konsekvenser

Identifisering av konsekvenser følger av standardens kapittel 8.2.6. En konsekvens er en skade på noe av verdi (omdømme, liv og helse, økonomi) som resultat av en uønsket hendelse hvor en sårbarhet er utnyttet av en trussel.

Konsekvenser beskrives som resultatet av et risikoscenario. Målet er altså å identifisere mulige konsekvenser.

Uønskede hendelser grupperes i tre kategorier:

- brudd på konfidensialitet,
- brudd på integritet,

- brudd på tilgjengelighet

Disse vil igjen kunne ha følgeskader som for eksempel tap av omdømme, tap av liv og helse og økonomiske tap. Hvor alvorlig en uønsket hendelse er, vil variere med verdien.

Resultatet etter gjennomført identifisering er en liste av risikoscenarioer med deres konsekvenser, og hvordan de er relatert til verdier.

3 Analyse av risiko

Analyse av risiko følger av standarden kapittel 8.3. Formålet er å danne seg et bilde over de forskjellige hendelsesscenariene som er relevante, for dermed å lage et grunnlag for videre evaluering og behandling.

3.1 Oversikt over verdier

Innbyggerne legger opplysninger inn i Kontakt- og reservasjonsregisteret. Opplysningene som blir lagt inn i Kontakt- og reservasjonsregisteret av innbyggeren er mobilnummer og epostadresse.

Postkasseleverandørene legger postkasseadressen og postkasseleverandørens virksomhetssertifikat inn i registeret når innbygger har valgt leverandørens digitale postkasse for mottak av digital brev fra offentlig sektor.

Samlet utgjør disse opplysningene verdien «Innbyggers opplysninger».

Virksomhetene har i tillegg tre andre verdier som indirekte kan påvirkes av informasjonen de benytter i Kontakt- og reservasjonsregisteret.

1. Innbyggerens liv og helse.
2. Sitt eget omdømme.
3. Økonomiske verdier.

Verdiene kan oppsummeres i følgende tabell:

Verdi	Beskrivelse
Innbyggers opplysninger	De samlede opplysningene om innbygger i Kontakt- og reservasjonsregisteret
Innbyggers liv og helse, omdømme og økonomi	Deler av forvaltningen vil påvirke innbyggerens liv og helse, omdømme og økonomi. Dette blir da en verdi som virksomhetene må verne om.
Virksomhets omdømme	Dette er innbyggernes oppfattelse av og forventninger til virksomhetens tjenester, troverdighet, handlekraft, og evne til gjennomføring.
Virksomhets økonomi	Virksomhetens økonomiske tap eller gevinster.

3.2 Kriterier for risikoaksept

Behovet for å fastsette kriteriene for risikoaksept følger av standarden kapittel 7.2.4.

Risiko er sannsynlighet i kombinasjon med konsekvens. Satt sammen blir det en risikomatrise. Risikomatrisen nedenfor er lagt til grunn i denne ROS-analysen og er basert på et eksempel i Faktaark 5[1].

Sannsynlighet/ konsekvens		Ubetydelig	Moderat	Alvorlig	Kritisk
		1	2	3	4
Sannsynlig Hendelsen inntrer daglig eller oftere	4	4	8	12	16
Mulig Hendelsen inntrer en gang i måneden	3	3	6	9	12
Mindre sannsynlig Hendelsen inntreffer årlig	2	2	4	6	8
Sjelden Hendelsen inntreffer omkring hvert 5. år eller sjeldnere	1	1	2	3	4

Tabell 1 Risikomatrise

Nivåene for risikoaksept blir da som følger:

Lav risiko	1 – 3	Ingen tiltak nødvendig
Moderat risiko	4 – 9	Hendelsene skal vurderes nærmere og eventuelle tiltak implementeres eller risiko aksepteres
Høy risiko	10– 16	Tiltak skal iverksettes

Tabell 2 Kriterier for akseptabel risiko

[1] http://www.helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/dokumenter/faktaark/Documents/faktaark-5-fastsette-akseptkriterier.pdf

Graderingen tas bare som et utgangspunkt. En må i hvert enkelt tilfelle vurdere risiko opp mot fordelene. For eksempel kan det vurderes som akseptabelt å ta en høy(ere) risiko i en overgangsperiode.

Ulike virksomheter vil ha ulike kriterier for hvilken risiko de er villig til å akseptere, da dette avhenger av hver virksomhets policyer, mål og hvilket regelverk de er underlagt. Nivåene for hver enkelt virksomhet fastlegges i relasjon til følgende:

- Virksomhetsspesifikke kriterier; for eksempel er helsesektoren underlagt Normen og vil vurdere et sikkerhetsregime i tjenesten med den som målestokk.
- Lovmessige og regulatoriske aspekter vil kunne variere mellom virksomhetene.
- Operasjonelle aspekter.
- Teknologiske aspekter, for eksempel bruk av en eksisterende portal-løsning.
- Økonomi.

3.3 Trusler

Når det gjelder identifisering av utilsiktede og naturlige trusler har vi ikke identifisert noen utover de som er beskrevet i standarden. Vi antar at trusselbildet på dette området i stor grad vil være sammenfallende med truslene mot virksomhetenes systemer.

3.4 Trusselaktører

Trusselaktører er ikke like, og det finnes mange metoder for å kategorisere ulike trusselaktører. Her har vi valgt å fokusere på de samme egenskapene som i risikohåndterings-guiden til NIST, SP 800-30[2], og lagt til utholdenhet:

- Evne - En aktørs tilgang på kompetanse og ressurser.
- Vilje - En aktørs grad av motivasjon for å angripe.
- Målrettethet - En aktørs grad av målrettethet mot brukere eller brukergrupper. Målrettethet vil øke risikoen for individene angrepet rettes mot, pga økt frekvens og tilpasning av angrepene.
- Utholdenhet - En aktørs evne til å opprettholde et angrep over tid og evnen til å utføre flere angrepsforsøk over tid.

[2] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

De viktigste trusselaktørene vurderes slik:

Trusselaktør	Evne	Vilje	Målrettethet	Utholdenhet
Fremmed makt	5	2	5	5
Organisert kriminalitet	4	3	5	4
Hacktivister	4	3	1	2
Hacker	4	3	3	4
Media	3	3	5	4
Utro tjener i virksomheten	3	3	5	3
Utro tjener hos Difi	3	3	5	3
Utro tjener hos tredjepart/databehandler	3	3	1	3
Tiltrodd tredjepart/databehandler	3	1	1	3
Nærstående med fysisk tilgang	3	4	5	4
Nærstående uten fysisk tilgang	2	4	5	4

Skala for evne, vilje og utholdenhet er:

5 Meget høy

4 Høy

3 Middels

2 Lav

1 Meget lav

Skala for målrettethet er:

5 Et spesifikt individ

3 En eller flere individer

1 Generisk angrep ikke spesielt rettet mot bestemte individer

Skalaene og verdiene er tidligere benyttet i ROS-analyse av Sikker digital posttjeneste versjon 1.1 på bakgrunn av tilbakemeldinger fra bl.a. Politiet, Kripos, NAV, SPK, Helsedirektoratet og åpne kilder som PST's og NSM's trusselvurderinger, men justert på bakgrunn av den lavere kritikaliteten til verdiene i Kontakt- og reservasjonsregisteret og Oppslagstjenesten.

Vi har lagt følgende antagelser om motivasjon til grunn for de ulike trusselaktørene:

Fremmed makt

Her er det lagt til grunn at utpressing av ledende personer i Norge eller represalier mot egne (eks-)borgere kan være aktuelt eller at fremmede makter vil kunne utføre sabotasje for å svekke Norges omdømme. Motivasjonen til å få tak i registeret anses som lav, da denne trusselaktøren vil få bedre utnyttelse av sine ressurser ved å angripe registre som inneholder mer nyttig informasjon.

Fra PSTs Åpen trusselvurdering 2013:

Etterretningsvirksomheten mot Norge og norske interesser pågår kontinuerlig, på et stabilt høyt nivå, og retter seg mot et bredt spekter av mål. Vi forventer at virksomheten særlig vil rette seg mot sikkerhets- og beredskapsmål, samt mot teknologiske, økonomiske og politiske mål. I tillegg vil flere stater opprettholde sin flyktningspionasje i Norge og forsøke å kartlegge, true og skremme dissidenter og politiske aktivister som oppholder seg her.

Organisert kriminalitet

Det er lagt til grunn at organisert kriminalitet i hovedsak retter seg mot økonomiske interesser, og at informasjonen som ligger registeret kan brukes som et ledd i ID-tyveri og lignende. I tillegg kan informasjonen brukes i forbindelse med represalier ift. trusselutsatte innbyggere, eller selges videre.

Hacktivister

Hacktivister ønsker ofte å oppnå et politisk mål gjennom sabotasje eller offentliggjøring av informasjon

Hackergruppe / Individuell hacker

For disse er det lagt til grunn at de kan ønske å vise at sikkerheten ikke er god nok i løsningen og at det kan gi status å hacke tjenestene, ønske om å sabotere, eller man kan ha økonomiske motiver bak handlingene.

Media

Virksomhetene har flagget media som en potensiell stor trusselaktør også i Norge. I utlandet har det forekommet hacking fra media og det finnes også ansatte hos avsendervirksomheter som har blitt forsøkt lurt fra norsk media. Den kommersielle gevinsten gjennom økte opplagstall/besøkstall og for eksempel en enkelt journalists status er mulige beveggrunner.

Utro tjener i virksomheten

Det er lagt til grunn at en utro tjener i virksomhetene kan lage en kopi av opplysningene som finnes i registeret. Dette kan benyttes til å se om det finnes opplysninger om bestemte individer, eller registeret kan selges videre. Hvis virksomheten har en lokal kopi, og den utro tjeneren har mulighet til å bytte ut informasjon i registeret, slik som varslingsadresse eller postkasseadresse, kan han/hun få tilgang til kommunikasjonen.

Utro tjener i Difi

Det er lagt til grunn at en utro tjener kan lage en kopi av opplysningene som finnes i registeret. Dette kan benyttes til å se om det finnes opplysninger om bestemte individer, eller registeret kan selges videre. Hvis den utro tjeneren har mulighet til å bytte ut informasjon i registeret, slik som varslingsadresse eller postkasseadresse, kan han/hun få tilgang til kommunikasjonen.

Utro tjener hos tredjepart/databehandler

Det er lagt til grunn at en utro tjener hos tredjepart kan lage en kopi av opplysningene som finnes i registeret. Dette kan benyttes til å se om det finnes opplysninger om bestemte individer, eller registeret kan selges videre. Har den utro tjeneren mulighet til å gjøre endringer på registeret, kan man også bytte ut informasjon i registeret for å få tilgang til kommunikasjon.

Tiltrodd tredjepart/databehandler

Det er lagt til grunn at en tredjepart kan bruke opplysningene i registeret på en uautorisert måte. Dette kan være for utsendelse av reklame, spam eller videresalg, eller berikelse av egne registre. Tredjepart er i denne sammenhengen private aktører som har tilgang til registeret da de leverer tjenester på vegne av det offentlige.

Nærstående med fysisk tilgang / Nærstående uten fysisk tilgang

Hvis det finnes innbyggere som er trusselutsatte i registeret, kan disse spores opp om telefonnummer eller epostadresse røper geografisk tilhørighet. Innbyggere som er i konflikter med andre innbyggere, og som ønsker å påføre disse ulemper, eller bare gjøre «livet surt» for en motpart.

3.5 Vurdering av sannsynlighet

Vurdering av sannsynlighet følger av standarden kapittel 8.3.3.

Vurdering av sannsynligheten for at en hendelse inntreffer har som mål å finne svar på «hvor ofte..». Svaret angis kvantitativt, og sannsynlighetsskalaen ble fastsatt under kontekstetableringen.

For hver av de uønskede hendelser som er identifisert skal man gjøre en vurdering av sannsynligheten for at hendelsen inntreffer. I mange tilfeller kan det være vanskelig å si noe om frekvens, da det ikke finnes noe godt statistisk materiale. I disse situasjonene kan man ta med en aktørs motivasjon for å gjennomføre en handling, eller hvor lett det vil være for en aktør å gjennomføre handlingen.

En integrert del av risikoaksept er å fastsette nivåer for sannsynlighet:

Vurdering	**Frekvens**	**Motivasjon**	**Letthetsbetraktninger**
Sannsynlig at hendelsen inntreffer 4	Hendelsen inntreffer daglig eller oftere	Sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.	- sikkerhetstiltak er ikke etablert - krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes - ikke nødvendig med kjennskap til tiltakene
Mulig at hendelsen inntreffer 3	Hendelsen inntreffer en gang i måneden	Sikkerhetsbrudd kan skje ved uaktsomhet av egne medarbeidere. Utenforstående må ha noe kompetanse, og forsettlig (bevisst eller aktivt) gå inn for å bryte sikkerhetstiltakene.	- sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer ikke etter hensikten - egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene
Mindre sannsynlig at hendelsen inntreffer 2	Hendelsen inntreffer årlig	Sikkerhetsbrudd kan skje ved at egne medarbeidere opptrer med forsett og har en viss kompetanse. Utenforstående må opptre med overlegg og noe kunnskap om interne forhold (med hensikt og plan, eksempelvis ved at flere tiltak brytes i riktig rekkefølge) for å omgå/bryte sikkerhetstiltakene.	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter hensikten - egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse - eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse
Sjelden at hendelsen inntreffer	Hendelsen inntreffer omkring hvert 5. år eller	Sikkerhetsbrudd kan kun skje ved at egne medarbeidere opptrer	- sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet - sikkerhetstiltak fungerer etter

Vurdering	Frekvens	Motivasjon	Letthetsbetraktninger
1	sjeldnere	med overlegg og har spesiell kompetanse eller kunnskap. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten.	hensikten - krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes - eksterne kan ikke omgå tiltakene

Der erfaringstall foreligger, gir disse en indikasjon på framtidig frekvens. På bakgrunn av letthets- og motivasjonsvurderingen gjengitt over kan også forventet frekvens anslås. Til hjelp for vurderingen er det utarbeidet kriterier for letthetsbetraktninger, se over.

Det er imidlertid også verdt å være oppmerksom på at trusselaktørers gevinst av vellykket sikkerhetsbrudd vil påvirke frekvensvurderingen, jf. at verdien vil være styrende for motivasjonen. Det kan således være nødvendig å knytte et anslag over gevinsten for trusselaktøren til opplysningene som inngår i løsningen – i tillegg til taps- og skadepotensialet for virksomheten selv, innbyggeren mv., jf. konsekvenskategoriene. For motivasjonsvurderingen vises til omtalen i Datatilsynets veileder kapittel 7.3.

3.6 Vurdering av konsekvenser

Vurdering av konsekvenser følger av standarden kapittel 8.3.2.

Vurderingen tar utgangspunkt i listen av de identifiserte uønskede hendelsene, og skal gi svar på spørsmål av typen «hva er konsekvensen hvis det som kan gå galt går galt».

At verdiene i systemet er korrekt fastsatt er kritisk for en riktig vurdering av konsekvenser.

Konsekvens kan uttrykkes som økonomiske tap, tap av liv og helse, tap av omdømme, straffeansvar for virksomheten osv.

Behovet for å fastsette kriterier for konsekvens følger av standarden kapittel 7.2.3. Det benyttes fire graderinger på konsekvens:

1. Ubetydelig
2. Moderat
3. Alvorlig
4. Kritisk

Nedenfor er kriteriene som vil bli benyttet videre:

Konsekvens-matrise	Ubetydelig	Moderat	Alvorlig	Kritisk
	1	2	3	4
Innbygger	En mindre uleilighet, økonomisk tap som kan gjenopprettes eller tap av anseelse eller integritet gjennom kompromittering av følsomme opplysninger	Gjenopprettbart økonomisk tap eller tap av anseelse og integritet gjennom kompromittering av opplysninger den registrerte oppfatter som krenkende. Fare for skade eller helsetap.	Helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse og integritet	Tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.
Virksomhet Omdømme	Kun mindre diskusjon i organisasjonen	Avsender må forklare seg for kundene om saken. Enkeltstående presseoppslag.	Offentlig debatt, ledelsen må forklare seg for eierne eller myndigheter	Politisk debatt, betydelig økonomisk erstatning/tap
Virksomhet Økonomisk	Ubetydelige økonomiske tap	Mange små kostnader. Reduserte besparelser.	Stort økonomisk tap. Stor engangskostnad	Betydelig økonomisk erstatning/tap

Disse kriteriene er hentet fra Norsk Helsenetts veileder for risikovurdering[3] og deretter modifisert på bakgrunn av møtene med avsendervirksomhetene, interne vurderinger, og best practice.[4]

3.7 Estimering av risiko(nivå)

Behovet for å estimere risiko følger av standarden kapittel 8.3.4.

Det er lagd en oversikt over identifiserte uønskede hendelser, hva som er årsaken (sårbarhet/trussel) og mulige konsekvenser. Dette er lagt inn i et register for å sikre at man skal kunne holde oversikten og for enkelt å kunne justere vurderingen av risikoen, eksempelvis på grunn av at tiltak innføres.

Sannsynlighet og konsekvens er anslått, basert på skalaer fastsatt i Vurdering av sannsynlighet og Vurdering av konsekvens. Risiko fremkommer som et resultat av dette.

[3] http://www.nhn.no/informasjonssikkerhet/risikovurdering

[4] Liknende/alternative konsekvenskategorier finnes hos Datatilsynet (pkt 6.2, s 14), Difi (pkt 3.2.4), Digitaliseringsstyrelsen (side 24) og NSM (pkt 3.6.2, s 25)

4 Evaluering av risiko

Behovet for å evaluere risiko følger av standardens kapittel 8.4.

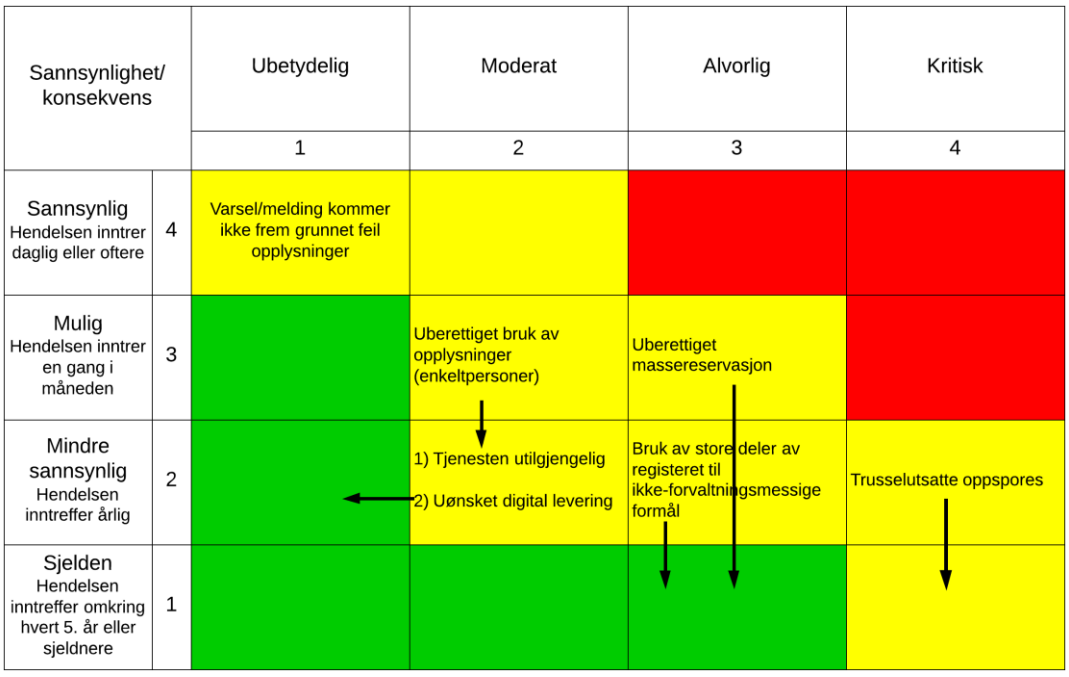
I risikoregisteret evaluerer vi risikoene ved å trekke frem relevante scenarier og knytte disse til verdier for sannsynlighet og konsekvens. Produktet av disse gir en verdi for risiko. Ved vurdering av risiko er eksisterende og planlagte tiltak og effekten av disse på sannsynlighet og konsekvens gjenspeilet i verdiene. I tillegg er det vurdert andre mulige tiltak som kan redusere sannsynlighet eller konsekvens. Effekten av de mulige tiltakene er vurdert, og fremstilt som risiko etter tiltak. På denne måten framstår verdier for risikoene før og etter mulige tiltak og effekten av tiltakene kan måles.

I risikogruppene under har vi slått sammen risikoer med en eller flere fellestrekk. Det kan være risikoer som utløses av samme hendelser eller reduseres av samme type tiltak.

4.1 Omtale av de viktigste risikogruppene – sett fra virksomhetene og Difi

Innføringen av Kontakt- og reservasjonsregisteret medfører ikke noen risikoscenarier med *høy* risiko, risikoer der summen av sannsynlighet og konsekvens krever umiddelbare tiltak. Det er imidlertid avdekket scenarier der risiko er kalkulert som *moderat*. Tiltak må derfor vurderes for å få risikoene ned på akseptabelt nivå.

I dette kapittelet er funnene fra risikovurderingen gruppert for de moderate risikoer, gule risikoer med verdi mellom 4 og 8 i figuren nedenfor. Pilene indikerer risikogruppenes endring i risikoverdi ved gjennomføring av anbefalte tiltak beskrevet i *kursiv* under hver risikogruppe i dette kapittelet. Innbyggers risiko beskrives i 4.2.



Trusselutsatte oppspores - ved uautorisert bruk av registeret kan trusselutsatte innbyggere bli sporet opp (kode 6 i folkeregisteret). Risikoen er størst knyttet til eventuelle opplysninger som er geolokaliserende, slik som navn@arbeidssted.no og telefonnummer registrert på adresse eller arbeidsgiver.

> *Difi vet ikke hvem som har kode 6 i folkeregisteret, men har innledet samarbeid med Kripos. Det anbefales at trusselutsatte fjernes fra registeret inntil man har forsikret seg om at opplysningene som legges inn ikke er geolokaliserende(«hvite» opplysninger). Trusselutsatte bør gjøres oppmerksom på at kontaktopplysningene vil bli tilgjengelige for store deler av forvaltningen og få opplæring/informasjon om å legge inn «hvite opplysninger. Samlet antas disse tiltak å få risikoen ned til akseptabelt nivå.*

Uberettiget massereservasjon. Det er teknisk mulig å reservere et stort antall personer. Urettmessige reservasjoner vil formodentlig raskt oppdages da de som er registrert i kontaktregisteret blir varslet om reservasjonen.

> *Egnede tiltak for å redusere risikoen er informasjon om at det kan være straffbart å utøve skadeverk på denne måte, samt tiltak for å ta ned den elektroniske reservasjonstjenesten ved uvanlig høy pågang og andre beredskapstiltak. Videre kan det vurderes teknisk sperre mot uvanlig høyt antall sperringer fra samme nettverkssegment. Samlet vil dette gi en akseptabel risiko.*

Uberettiget bruk av opplysninger (enkeltpersoner) Det antas at en god del innbyggere har registrert kontaktopplysninger i kontaktregisteret som ikke er tilgjengelige i andre åpne opplysningstjenester. Uberettiget bruk av disse opplysningene kan derfor oppleves som særskilt plagsomt for enkelte (kjendiser, ved samlivskonflikter og lignende).

> *Et risikoreduserende tiltak er å gjøre innbyggerne oppmerksomme på at opplysningene som legges inn i registeret bør være med et innhold som det er greit at en større del av forvaltningen har tilgang til. Det er for eksempel tilstrekkelig å kun registrere e-postadresse, ikke mobilnummer.*

Tjenesten er utilgjengelig Det kan være mange årsaker til at tjenesten blir utilgjengelig. Det kan være at ytelsen i løsningen ikke er god nok for å håndtere uventete trafikktopper, eller at tjenesten utsettes for tjenestenektangrep, og andre tilsvarende handlinger.

> *Kapasitetsplanlegging, beredskapsplaner og tekniske tiltak hos Difi og driftsleverandøren er etablerte tiltak som motvirker eller begrenser effekten av slike hendelser. Virksomheter med lokale kopier, må selv sørge for tiltak for å sikre tilgjengelighet.*

Bruk av store deler av registeret til ikke-forvaltningsmessige formål. En uberettiget nedlasting av hele eller store deler av registeret kan misbrukes til spam, markedsføring mv. Dette forutsetter at en autorisert bruker opptrer som en utro tjener.

> *Informasjon om at dette kan være straffbart, kombinert med tekniske tiltak som hindrer oppslag ut over forventet bruk i virksomhetene, antas å redusere risikoen til et akseptabelt nivå. Virksomheter med lokale kopier må selv innføre tiltak mot uberettiget bruk.*

Uønsket digital levering. Det kan skje at enkeltvedtak eller andre viktige brev leveres digitalt til innbyggere som har reservert seg. Dette kan for eksempel oppstå hvis virksomhetene ikke sjekker reservasjonsstatus før utsending enkeltvedtak eller andre brev som omfattes av reservasjonsadgangen.

> *Virksomhetene må sjekke reservasjonsstatus før utsendelse av enkeltvedtak og andre viktige brev. Forpliktelsen fremgår av bruksvilkårene som virksomhetene må akseptere før de knytter seg til registeret. Ved reservasjon bør innbygger informeres om at det kan ta noe tid før reservasjonen får effekt for alle utsendelser fra offentlig sektor.*

Varsel/melding kommer ikke frem grunnet feil opplysninger. Et register med opplysninger om over 3 millioner innbyggere vil inneholde feil. Dette kan skyldes utilsiktede feilregistreringer fra innbygger selv, at kontaktopplysninger blir utdaterte uten at kontaktregisteret endres etc. En del innbyggere har registrert andres kontaktopplysninger på grunn av fullmaktsbruk av MinID. I hovedsak vil dette være forhold som inngår i innbyggers ansvar og risiko, og som innbygger må håndtere. Restrisikoen mener vi ikke skiller seg vesentlig fra den risiko som i dag aksepteres mht. at noe papirpost forsvinner på vei til mottaker.

> *Difi vurderer tiltak for å gjøre innbyggere og særlig relevante grupper oppmerksom på utfordringer pga fullmaktsbruk for MinID. Forvaltningen må uansett ta høyde for at noen av varslene ikke kommer rette vedkommende i hende.*

4.2 Risikovurdering for innbyggere

Nedenfor beskrives de alvorligste risikoene som innbygger må akseptere:

Sannsynlighet/ konsekvens		Ubetydelig	Moderat	Alvorlig	Kritisk
		1	2	3	4
Sannsynlig Hendelsen inntrer daglig eller oftere	4				
Mulig Hendelsen inntrer en gang i måneden	3			ID-misbruk	
Mindre sannsynlig Hendelsen inntreffer årlig	2		Urettmessig reservasjon (enkeltpersoner)		
Sjelden Hendelsen inntreffer hvert 5. år eller sjeldnere	1				

ID-misbruk for eksempel ifbm. samlivsbrudd. En del ektefeller og samboende praktiserer deling av elektroniske identitetsbevis, dvs. at den ene disponerer den andres e-ID. Dersom dette består etter et samlivsbrudd, vil det fortsatt være mulig for den ene å få tilgang til den andres kommunikasjon med det offentlige.

> *Difi er oppmerksom på utfordringen, og kan veilede innbygger i hvordan vedkommende får sperret e-ID-en. For MinID håndterer Difi sperringen selv, for andre e-ID-er må utsteder kontaktes. Kontaktinformasjon vil innbygger selv kunne endre når vedkommende har fått tilgang til sin egen e-ID. Innbygger vil også kunne kreve kontaktinformasjonen slettet (pt. ved innsending av et papirskjema).*

Urettmessig reservasjon i familieforhold. Ettersom det er enkelt å reservere seg (ingen identitetskontroll), vil det være mulig for et familiemedlem å reservere andre i husstanden fra digital kommunikasjon. Dette medfører at brev leveres i postkassen, og kan dermed kontrolleres av vedkommende. Vi anser denne risikoen for å være lav.

> *Innbygger vil få varsel om reservasjonen. Difi vil vurdere om det også skal gis tydeligere informasjon om at opprettelse av digital kontaktinformasjon og et eventuelt valg av digital*

postkasse ikke gir innbygger sikkerhet for at all kommunikasjon fra forvaltningen vil foregå digitalt, da avsendervirksomhetene i stor grad bestemmer hvordan brev skal sendes.

5 Sluttord

Kontakt- og reservasjonsregisteret har allerede blitt et effektivt og nyttig hjelpemiddel for økt kommunikasjonen på nett med innbyggerne. Skatteetaten har kunnet sende årets skatteoppgjør digitalt til langt flere innbyggere enn tidligere. Med kontakt og reservasjonsregisteret vil innbyggerne slippe å oppdatere sin kontaktinformasjon en rekke steder. Med mer enn 3,3 millioner innbyggere i registeret, er registeret allerede kommet langt i å bli et "komplett" register over innbyggernes digitale kontaktinformasjon.

I all hovedsak består registeret av informasjon som ikke er taushetsbelagt. Det er innbyggerne selv som har gitt informasjonen, og disse blir regelmessig oppfordret til å oppdatere eller bekrefte informasjonen. Dette gjør datakvaliteten høy. Samtidig må innbyggerne være seg bevisst at registeret kan være attraktivt for uvedkommende. Registeret vil bli mye brukt. Tilgjengelighet er derfor viktig. Det vil være mulig å gjennomføre tiltak som sikrer minimalt med taushetsbelagt informasjon i registeret. Enkelte innbyggere vil likevel mene at det er personverninteresser knyttet til opplysningene. De berørte må da vurdere å slette eller endre sin kontaktinformasjon i registeret.

Difi har i samarbeid med ulike virksomheter utarbeidet denne ROS-analysen av Kontakt- og reservasjonsregisteret med tilhørende oppslagstjeneste. Hovedfokus for analysen har vært beskyttelse av innbyggerne og spesielt de som har et ekstra behov for vern. Der det er relevant har analysen også tatt med bekymringer som ble avdekket i ROS-arbeidet i forbindelse med anskaffelsen av Digital Postkasse til innbyggerne.

Risikoanalysen viser at informasjon til innbyggerne er meget viktig for å ivareta tilfredsstillende informasjonssikkerhet ved innføring av Kontakt- og reservasjonsregisteret i forvaltningen. En del av den risikoen registeret medfører, kan reduseres ved at innbyggerne får et bevisst forhold til den informasjonen de gir fra seg. Brudd på integritet og konfidensialitet i registeret vil også påvirke innbyggerne mest.

For virksomhetene vil tilgjengelighet og integritet i registeret være de viktigste faktorene for en vellykket implementering, men det er også viktig at verdiene til innbyggerne forvaltes på en forsvarlig måte.

Det er kartlagt flere risikoreduserende tiltak rundt bruken av Kontakt- og reservasjonsregisteret. Foruten utvidede opplysningstiltak over forvaltningen og visse grupper av innbyggere vil det være sterkere teknisk beskyttelse uten konsekvenser for bruken av registeret.

Innføringen av Kontakt- og reservasjonsregisteret medfører ikke noen risikoscenarier med *høy* risiko, risikoer der summen av sannsynlighet og konsekvens krever umiddelbare tiltak. Det er imidlertid avdekket scenarier der risiko er kalkulert som *moderat*. Tiltak må derfor vurderes for å få risikoene ned på akseptabelt nivå.

Det følger av standardens kapittel 12.2 at styring av risiko er en iterativ prosess hvor risiko kontinuerlig skal monitorers, revideres, og forbedres. Kontakt- og reservasjonsregisteret med tilhørende oppslagstjeneste er i kontinuerlig utvikling, og vil dermed bli endret med hensyn på bruk og tilknyttede systemer. ROS-analysen bør bli revidert regelmessig, og anslagsvis en gang i året.