Difi
Direktoratet for
forvaltning og ikt

Veiledning til Foranalyse del 1 – Identifisering av arbeidsoppgaver og informasjonstyper

Dette er veiledning til deltrinn 1 i en foranalyse under aktiviteten «Få oversikt og prioritere». Formålet er å identifisere typiske arbeidsoppgaver og informasjonstyper i virksomheten, for bruk i det videre arbeidet med informasjonssikkerhet.

Foranalysen gir grunnlaget for arbeidet med å gruppere og prioritere, hvor og når det bør gjennomføres nye/oppdaterte risikovurderinger og eventuell risikohåndtering.

Innhold

1 Hvem er ansvarlig?

Alle som har ansvar for en arbeidsoppgave eller -prosess i virksomheten bør gjennomføre denne aktiviteten. Kartleggingen kan gjerne gjennomføres med bistand fra fagansvarlig informasjonssikkerhet. Det er opp til virksomheten selv å velge hvor i organisasjonen denne oppgaven utføres. Den kan for eksempel gjennomføres på laveste organisatoriske nivå, eller samlet i ledergruppen på nivået over.

Difi anbefaler at man involverer fagpersoner som kjenner arbeidsoppgavene og informasjonstypene gjennom sine daglige arbeidsoppgaver.

2 Organisering

Det bør pekes ut en som er ansvarlig for å lede gjennomføringen. Vi kaller denne personen for prosessleder.

Kartleggingen kan med fordel gjøres i arbeidsmøter ledet av prosessleder. Difi har laget en dokumentmal med støtteskjema som kan brukes som grunnlag. Prosessleder bør få støtte av en ansatt som kan bistå med praktisk utfylling av dokumentet. Da blir møter mer effektive og man kan se resultater av gjennomføringen raskere. Prosessleder kan da fokusere på å lede diskusjonen, og møtedeltakerne ser hvordan innholdet i dokumentet utvikler seg.

Ettarbeid etter møter kan gjerne gjøres av prosessleder og støtteperson i fellesskap. Ferdigstilling av dokumentet bør gjøres av den aktuelle organisatoriske enhet. Det er de som skal eie resultatet.

Det vil normalt være behov for å gjennomføre 1-2 arbeidsmøter pr enhet.

3 Forberedelser

Prosessleder bør gjøre seg kjent med den aktuelle enheten før arbeidsmøtene.

Dokumentmalen med støtteskjema bør tilpasses til den aktuelle virksomheten og enhetens behov.

Kommentarer og noen enkle råd som er skrevet underveis i malen bør fjernes før bruk som en del av tilpasningen. Disse rådene og kommentarene er skrevet med blå skrift i kursiv, slik som dette:

Dette er et eksempel på tekst som bør fjernes før de benytter malen i din virksomhet.

Oversikten over arbeidsoppgaver må tilpasses virksomheten. I tillegg bør det legges inn delvis utfylte støtteskjema for arbeidsoppgaver man forventer å finne i enheten. Det er lettere å ta utgangspunkt i eksempler og justere disse, enn selv å identifisere og finne riktig nivå på informasjonstyper.

4 Gjennomføring

Det er fornuftig å begynne med å identifisere arbeidsoppgaver eller tjenester som utføres. Informasjonsbehandlingen skjer normalt som en del av disse. Deretter må man identifisere informasjonstypene som behandles og relevante forhold knyttet til dem.

4.1 Oversikt over arbeidsoppgaver

Arbeidsgruppen begynner med å identifisere hvilke arbeidsoppgaver som utføres innen ansvarsområdet.

Eksemplene som er listet i malen benyttes som utgangspunkt, men tilpasses behovene i virksomheten og den enkelte enhet. Man kan supplere, stryke, eller presisere i løpet av gjennomgangen.

Det er viktig å omtale arbeidsoppgaver på et overordnet nivå slik listen under indikerer. For større grupper av oppgaver kan det være hensiktsmessig å dele de i undergrupper slik det er vist i eksempelet under. Det gjelder spesielt når enkelte varianter av oppgavene har høye konfidensialitetsbehov, mens andre ikke har det. Navnet bør si noen om det faktiske innholdet i oppgaven. Noen oppgaver vil også være spesialiserte varianter av andre. Man bør da forsøke å plassere dem under den hovedgruppen som passer best.

Oppgave
Tilsyn
Systemrettet tilsyn med organisasjoner (herunder virksomheter og kommuner)
Individrettet tilsyn med organisasjoner (herunder virksomheter og kommuner)
Tilskuddsforvaltning
Tilskuddsforvaltning organisasjoner (herunder virksomheter og kommuner)
Tilskuddsforvaltning enkeltpersoner
Kompetanseutvikling
Veiledning/rådgivning
Kurs/konferanser o.l.
Lage kompetansemateriell
Kunnskapsforvaltning
Undersøkelser

Analyser (av eksisterende datagrunnlag)
Planarbeid (eksternrettet)
Planarbeid ugradert
Planarbeid gradert (helt eller delvis etter sikkerhetsloven el. besk.instruksen)
Oppfølging av eksterne grupper/spesialfunksjoner
Oppfølging råd og utvalg
Oppfølging spesialfunksjoner (sensorer, verger, mv.)
Annen saksbehandling

Støtteoppgaver
Personaloppfølging i linjen
Anskaffelser
Økonomioppfølging i linjen
Personalforvaltning - fellesfunksjon
Økonomiforvaltning – fellesfunksjon
IKT drift og forvaltning
Arkiv drift og forvaltning
Eiendom - drift og forvaltning
Publikumstjenester

Styringsoppgaver
Virksomhetsstyring

4.2 Identifisering av informasjonstyper som behandles i arbeidsoppgavene

Når arbeidsoppgavene er identifisert, er neste oppgave å identifisere hvilke informasjonstyper som behandles i de ulike arbeidsoppgavene.

For hver arbeidsoppgave bør man fylle ut et støtteskjema. Dersom virksomheten har tilgang til helt eller delvis utfylte skjemaer for noen av oppgavene, bør disse brukes som utgangspunkt. Man kan også bruke Difis eksempler i dokumentet «[STØTTE] Typiske arbeidsoppgaver og tilhørende informasjonstyper».

Arbeidsgruppen kan da diskutere hvor relevante de foreslåtte informasjonstypene er for deres enhet, før de arbeider seg gjennom resten av kolonnene for hver informasjonstype.

4.2.1 Om beskrivelsen av informasjonstyper

Dersom det ikke er tilgjengelig eksempler/utgangspunkt, må arbeidsgruppen utforme hele beskrivelsen selv.

Informasjonstypene bør beskrives på et overordnet nivå.

Når prosessene er komplekse og sammensatte, kan det være nødvendig å kategorisere informasjonstypene annerledes, for eksempel for IKT-drift, der naturlige informasjonstyper kan være «IKT-utstyr», «Brukere», «Driftsrutiner» etc. Se for øvrig Difis dokument «[STØTTE] Typiske arbeidsoppgaver og tilhørende informasjonstyper», for veiledning om anbefalt nivå.

4.2.2 Bruk av Difis støtteskjema for arbeidsoppgaver og informasjonstyper

Utformingen av støtteskjemaet er et eksempel. Den må oppdateres ut fra virksomhetens behov.

4.2.2.1 Forkortelser

Følgende er eksempel på ofte brukte forkortelser, og enkelte av dem benyttes i støtteskjemaet. Legg gjerne til flere forkortelser og lenker som er aktuelle i din virksomhet.

Forkortelse	Betydning (ev. lenke)
arkl	arkivlova
besk.instr	beskyttelsesinstruksen
fvl	forvaltningsloven
offanskl	anskaffelsesloven
offl	offentleglova
offveil	rettleiar til offentleglova og tillegssvedlegg
pol	personopplysningsloven
pvf	personvernforordningen
sl	sikkerhetsloven
øk. bestemmelsene	bestemmelser om økonomistyring i staten

4.2.2.2 Lovhenvisninger og spørsmålstegn (?)

I lovhenvisninger skal tall etter punktum vise til det aktuelle leddet, nummeret og bokstaven i bestemmelsen.

Spørsmålstegn (?) kan benyttes når relevansen av et spørsmål i stor grad kan variere fra sak til sak, mellom konkret henvendelser, e.l. Eksempler på dette er

- om det er taushetsplikt på informasjonen iht. et konkret regelverk
- om noe kan, men ikke nødvendigvis skal, unntas offentlighet
- om noe er personopplysninger og eventuelt det personvernregleverket definerer som særlige kategorier av personopplysninger
- om noe har et spesielt behov for konfidensialitet, integritet eller tilgjengelighet
- om noe er skjermingsverdig informasjon etter sikkerhetsloven

4.2.2.3 Relasjon til personopplysningsloven, sikkerhetsloven mv.

I eForvaltningsforskriften § 15 heter det at sikkerhetsstrategien og internkontrollen *«skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks»*. Det betyr at når man etablerer internkontroll/styringssystem etter kravene i eForvaltningsforskriften, så skal det inkludere relevante krav om informasjonssikkerhet og internkontroll på området som fremkommer i personopplysningloven, sikkerhetsloven og andre relevante lover, med tilhørende forskrifter. Dette er både mer effektivt og gir bedre samlet styring og kontroll enn å ha ulike system for ulike regelverk som omhandler informasjonssikkerhet.

Difis veiledningsmateriell er tilrettelagt for dette. Det omfatter likevel bare de kravene i annet regelverk som gjelder informasjonssikkerhet.

Når det gjelder personopplysningsregelverket er det viktig å merke seg at internkontroll på informasjonssikkerhetsområdet kun dekker personvernforordningens bestemmelser om

informasjonssikkerhet (artikler 32-34), personvernkonsekvensvurdering (artikkel 35) og deler av behandlingsprotokollen [1](artikkel 30). Virksomheten må ha egne rutiner, og eventuelt egne støttefunksjoner som fagansvarlig personvern, for å sikre etterlevelse av personvernregelverket for øvrig. Difis veiledning om informasjonssikkerhet dekker ikke dette.

Støtteskjemaet er imidlertid tilrettelagt for å også dekke tilgrensede kartleggingsbehov for etterlevelse av personvernregelverket på områder som går utover informasjonssikkerhet.

Støtteskjemaet skal hjelpe virksomhetene til å etterleve personvernforordningens krav på en effektiv og risikobasert måte. Skjemaet vil dekke hoveddelen av kravet til behandlingsprotokoll iht. pvf artikkel 30, samtidig som det avdekkes hvilke områder som bør få særlig oppmerksomhet i det videre arbeid, for å ivareta krav til informasjonssikkerhet og personvern. Virksomheten må følge opp dette i etterkant av kartleggingen.

Vær oppmerksom på at støtteskjemaet legger opp til kartlegging på et mer overordnet nivå, enn hva som foreslås i Datatilsynets mal for behandlingsprotokoll. Difi har dialog med Datatilsynet for å avstemme anbefalingene.

Støtteskjemaet kan hjelpe virksomhetene til å etterleve sikkerhetsloven ved å identifisere informasjon og informasjonssystemer som kan være skjermingsverdig etter sikkerhetsloven. Dette kan danne grunnlaget for videre arbeid iht. til dette regelverket. Veiledning fra Nasjonal sikkerhetsmyndighet (NSM) må benyttes i det videre arbeidet med å vurdere om, og i hvor stor grad, det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

Difi mener det er fornuftig å ta utgangspunkt i støtteskjemaet, siden det innebærer en risikobasert tilnærming, i tråd med både personvernregelverket, sikkerhetsloven og godt arbeid med informasjonssikkerhet generelt.

Når det gjelder etterlevelse av personvernregelverket og sikkerhetsloven er det henholdsvis Datatilsynet og Nasjonal sikkerhetsmyndighet (NSM) som har veiledningsansvaret. Vi henviser til dem for spørsmål om disse regelverkene.

4.2.2.4 Utfylling av skjemaet

Nedenfor finner du veiledning for utfylling av noen av feltene i skjemaet.

Navn, formål og kort beskrivelse av arbeidsoppgaven, og Dato:
Øverst i støtteskjemaet bør oppgaven få et forståelig kortnavn, som det kan refereres til i de neste trinnene i foranalysen etter denne kartleggingen.

---

[1] Skjemaet er lagt opp til å dekke kravene til behandlingsprotokoll iht. artikkel 30 nr 1, med unntak av opplysningene som kreves i bokstav a (kontaktopplysninger til den behandlingsansvarlige, personvernombudet og ev. representanter og ev. felles behandlingsansvarlige). Dette er opplysninger som bør vedlikeholdes ett sted. Skjemaet støtter registrering av kategoriene av registrerte (bokstav c) for hver arbeidsoppgave, men det vil også være mulig å føre denne oversikten sentralt. Foranalysen bidrar til å kartlegge lagringsbehov (herunder arkivverdighet) og gi grunnlag for konkrete sikkerhetskrav. Personvernforordningens krav om at tidsfrister for sletting skal angis om mulig for ulike kategorier opplysninger, og kravet til generelle beskrivelser av sikkerhetstiltak (bokstaver f og g i art 30 nr 1), anbefaler vi at ivaretas i andre prosesser enn foranalysen. En mulig tilnærming er at dette inntas i kassasjonsreglene (jf. arkivlovens krav, se veiledning hos Riksarkivet) og en generell beskrivelse av hvilke sikkerhetstiltak som er iverksatt.

Under «*Formål med arbeidsoppgaven»* bør man kort tydeliggjøre formålet med oppgaven. Det kan f.eks. være å utføre en nødvendig tjeneste, nå et spesielt mål for virksomheten, eller etterleve et konkret regelverk.

Behandler man personopplysninger må de være samlet inn «*for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene».* (jf. pvf artikkel 5 nr 1 bokstav b).

I «*Kort beskrivelse»* kan man supplere med informasjon om arbeidsoppgaven, dersom ikke kortnavnet og formålet til sammen gir tilstrekkelig informasjon. Et eksempel kan være dersom man beskriver oppgaven «Tilsyn», og dette omfatter flere områder man gjør tilsyn på.

Feltet «*Dato*» fylles ut med dato når et støtteskjema er ferdig utfylt, og hver gang noe endres i etterkant. Det kan være nyttig informasjon når man jevnlig skal sjekke ut behov for oppdateringer av kartleggingen.

Paragraf for potensiell taushetsplikt / unntak fra offentlighet
Her fyller man inn relevante bestemmelser.

Man bør vise til lov, paragraf og ev. alternativ. Eksempel: fvl §13 nr 1. Ytterligere detaljer kan gjøres som etterarbeid, slik at man ikke bruker tiden på dette i arbeidsmøtet. For kompetanseheving eller ved spesielle behov, kan man i forkant eller etterkant også støtte seg på Justisdepartementets «*Rettleiar til offentleglova*» samt vedlegg til denne.

Dersom noe er underlagt taushetsplikt i lov eller i medhold av lov, er det unntatt offentlighet iht offl §13. Skriver man taushetspliktbestemmelsen i støtteskjemaet, er det ikke nødvendig å også ta med offl §13, da det er implisitt.

For henvisninger til offentleglovas øvrige bestemmelser, vil vi minne om **plikten til å vurdere meroffentlighet**. Det er ingen automatikk i at alt som kan unntas skal unntas. Her anbefaler vi at spørsmålstegnene brukes som støtte.

Sikkerhetsgradert informasjon er underlagt taushetsplikt, og man kan fylle inn sl §5-4 her. Samtidig bør man markerer at det er skjermingsverdig informasjon etter sikkerhetsloven i kolonnen for dette.[2]

Spesielt obs. mht. info.sikkerhet
Støtteskjemaet har tre kolonner under overskriften «*Spesielt obs. mht. info.sikkerhet*». Disse dekker konfidensialitet (K), integritet (I) og tilgjengelighet (T). Vi anbefaler at man skriver inn bokstavene K, I og T der det er relevant for hver informasjonstype. Det gjør det lettere å lese.

Integritet og tilgjengelighet vil normalt alltid ha et minimumsbehov. For å få fokus på det som er viktig, anbefaler vi at man bare fyller ut kolonnene dersom behovet for å ivareta integritet og tilgjengelighet på en informasjonstype er høyere enn normalt.

Vi viser ellers til bruken av spørsmålstegn (?), som også er svært relevant i disse kolonnene.

Personopplysninger

[2] Konfidensialitet for sikkerhetsgradert informasjon skal selvfølgelig sikres på andre måter enn personers taushetsplikt, men kombinasjonen av bruken av disse to kolonnene kan benyttes for å markere behov for videre arbeid med sikkerhetsgradert informasjon iht. veiledning fra NSM.

Støtteskjemaet har to kolonner under overskriften «*Personopplysninger*.». Disse dekker om informasjonstypen normalt er en personopplysning og om den eventuelt dekkes av begrepet «særlige kategorier av personopplysninger», jf. personvernforordningen artikkel 9 nr 1[3]. Det siste har spesiell betydning for personvernregelverkets bestemmelser om vilkår for å kunne behandle opplysningene. Det er også en indikasjon på at personverninteressene er store, slik at det kan være behov for en personvernkonsekvensvurdering.

Vi anbefaler at man i støtteskjemaet kun fyller ut «J» eller spørsmålstegn i «Ja/?»-kolonnen, når den aktuelle informasjonstypen er eller kan være personopplysninger. Ellers bør kolonnen være tom. Kolonnen for «Særlig kategori?» benyttes bare når man allerede har fylt inn at informasjonstypen er en personopplysning. Da fylles den ut med «J», «N» eller «?».

Merk at i offentlig sektor er det bestemmelsene i offentleglova med forskrifter som avgjør om noe kan unntas offentlighet, og dermed kan ha spesielle konfidensialitetsbehov. At noe er en personopplysning eller at opplysningen tilhører en særlig kategori, er ikke i seg selv nok, selv om det siste ofte gir en indikasjon.

For offentlig sektor er det her i hovedsak taushetspliktbestemmelsene i fvl §13 nr. 1, om «noens personlige forhold», som er avgjørende. Merk samtidig at særlover for enkelte områder kan ha mer omfattende taushetspliktsbestemmelser om personopplysninger, og at andre deler av u.off. bestemmelsene i offentleglova kan være relevante.

Skjermingsverdig informasjon
Denne kolonnen kan benyttes til å markere om informasjonstypen er skjermingsverdig eller sikkerhetsgradert informasjon iht. sikkerhetslovens §§ 5-1 eller 5-3. Vi anbefaler at man i støtteskjemaet kun fyller ut «J» eller spørsmålstegn i «Ja/?»-kolonnen, når den aktuelle informasjonstypen er eller kan være skjermingsverdig. Ellers bør kolonnen være tom.

Notater som vil være til nytte i videre arbeid iht. sikkerhetsloven kan fylles inn i feltet «Etterlevelse av sikkerhetsloven» lenger ned i skjemaet.

Ytterligere informasjon
Overskriftene til feltene gir rettledning til bruken av denne delen. Feltet «Merknader» kan benyttes til notater som kan være nyttig i det videre arbeidet.

Behandlingsgrunnlag for personopplysninger
Denne opplysningen er nyttig for å kunne etterleve informasjonsplikten overfor den registrerte, jf. personvernforordningen artikkel 13 (ev. artikkel 14) nr 1 bokstav c.

Dersom man behandler personopplysninger i arbeidsoppgaven/tjenesten bør altså dette feltet fylles ut. Man skriver da inn pvf artikkel 6 og ev. artikkel 9 + bokstaver eller lovhjemmel. Det er disse som klargjør hvilket behandlingsgrunnlag man har.

Kategorier av registrerte, kategorier av mottakere av personopplysninger

[3] Personopplysninger om «rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering»

Disse feltene tjener til å oppfylle krav til behandlingsprotokoll, jf. personvernforordningen artikkel 30 nr 1 bokstav c og d. Virksomheten kan alternativt registrere dette i én sentral behandlingsprotokoll.

Høy personvernrisiko
Dette feltet brukes hvis virksomheten ser behov for å gjennomføre en personvernkonsekvensvurdering av behandlingen, jf. personvernforordningen artikkel 35. Virksomheten skriver da inn momentene som taler for at det foreligger «høy risiko for fysiske personers rettigheter og friheter», jf. forordningen artikkel 35 nr 1.

Slike risikoer vil typisk foreligge for behandlinger som tidligere ble regnet som konsesjonspliktige, herunder omfattende behandlinger av sensitive personopplysninger (tilsvarer «særlige kategorier» i pvf). Videre kan det foreligge høy risiko ved profilering (automatisert vurderinger av personens egenskaper) som danner grunnlaget for en avgjørelse, eller som på annen måte i betydelig grad kan påvirke personen.

Datatilsynet og artikkel 29-gruppen[4] har utarbeidet veiledninger til bestemmelsen.[5]

Utleveres eller behandles personopplysninger utenfor EØS
Dette feltet tjener til å oppfylle krav til behandlingsprotokoll, jf. personvernforordningen artikkel 30 nr 1 bokstav d og e.

Dersom personopplysningene utleveres til mottakere utenfor EØS-området eller til internasjonale organisasjoner, skal dette anmerkes. Dere må da påse at utleveringen er i overensstemmelse med personvernforordningens regler, slik at opplysningene behandles med et tilstrekkelig beskyttelsesnivå. Flere grunnlag er mulige, jf. personvernforordningen kapittel V, blant annet ved bruk av standardavtaler godkjent av Kommisjonen (art 46 nr 2 bokstav c) eller ved overføring til virksomheter som er etablert i EØS og som har fått godkjent bindende virksomhetsregler iht. art 47 (jf. artikkel 46 nr 2 b).

Etterlevelse av sikkerhetsloven
Dette feltet kan benyttes til utfyllende informasjon som vil være til nytte for videre arbeid iht. sikkerhetsloven m/forskrifter og veiledning fra Nasjonal sikkerhetsmyndighet (NSM).

Det kan f.eks. benyttes til notater om:

- hvorfor informasjonen anses som potensielt skjermingsverdig
- i tillegg til markeringen av K, I og T under «Spesielt obs. mht. info.sikkerhet» kan man her legge inn beskrivelser som vil være nyttige i skadevurderingen[6]
- graderingsnivå der dette er relevant
- informasjonsystem som benyttes til behandling av skjermingsverdig informasjon

[4] Artikkel 29-gruppen var EUs rådgivende organ i personvernspørsmål, jf. personverndirektivet artikkel 29. Den uttalte seg også om personvernforordningen, før den hadde trådt i kraft. Gruppen er fra 25.5.2018 avløst av Det europeiske personvernråd, jf. pvf. artikkel 68. Rådet har sluttet seg til artikkel 29-gruppens uttalelser om pvf, jf. dets «Endorsment 1/2018».
[5] Se Datatilsynets veiledningsside og artikkel 29-gruppens veileder wp248 av 13.10.2017.
[6] Sl § 5-1 «dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig»

Informasjonssystem som brukes til behandling av skjermingsverdig informasjon er *skjermingsverdig informasjonsystem* iht. sikkerhetsloven § 6-1. Denne foranalysen kan inngå i arbeidet med identifisering av slike system.

Deling av data

Dersom man er forvalter av et register andre bruker, bør det registreres i felles datakatalog slik at andre vet at virksomheten har disse dataene. Følgende bør vurderes:

- hvilke datasett kan man dele beskrivelser av?
- kan datasett tilgjengeliggjøres som åpne data?