UiO : Det juridiske fakultet

Behandlingsansvarliges arbeid med sikring av personopplysninger

Kandidatnummer: 746

Leveringsfrist: 25. 04. 2014

Antall ord: 14 369

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn og aktualitet

Personopplysningsloven § 13 stiller krav om tilfredsstillende sikring av personopplysninger som behandles i en virksomhet. Hvordan dette skal oppnås og etterleves er en aktuell problemstilling for jurister, konsulenter, medarbeidere og virksomhetsledere. Jeg har arbeidspraksis fra en offentlig virksomhet i høgskole- og universitetssektoren som er kvalitetsbevisst og har sunn fokus på regeletterlevelse. Med ekstern bistand ble policy for informasjonssikkerhet vedtatt av styret i virksomheten i 2009. Dette var et viktig men ikke tilstrekkelig steg. Virksomheten jobber godt med teknisk IKT-sikkerhet, men har ikke et tilfredsstillende styringssystem for informasjonssikkerhet. Det er flere grunner til dette, blant andre manglende kunnskaper om informasjonssikkerhet som en organisatorisk oppgave, og om hva de rettslige kravene som stilles egentlig innebærer.

Virksomheten som jeg kjenner er ikke unik i denne sammenheng. Tranvik viser at etterlevelse av reglene er en utfordring også i kommuner.[1] Datatilsynets årsmelding for 2012 antyder det samme for andre virksomheter i både privat og offentlig sektor.[2] Det finnes unntak, eksempelvis kan Asker kommune dokumentere et fungerende system for informasjonssikkerhet.[3] Også Larvik kommune har vært sertifisert i mange år.[4] Likevel, og selv om personopplysningsloven trådte i kraft 01.01. 2001, antyder kanskje erfaringene over at flere virksomheter ikke etterlever plikten til informasjonssikkerhet godt nok. Dette er rettssosiologisk interessant i seg selv. Skyldes det temaets natur, reglenes utforming, samspillet mellom regler og tema, eller kanskje behovet for sikring? Eller står det vilje, evne, eller andre ting? Oppgaven kan belyse dette i noen grad. Men oppgaven handler først og fremst om de rettslige kravene i § 13, og personopplysningsforskriftens utdypning av denne, med fokus på hvordan virksomheten må arbeide med et styringssystem for informasjonssikkerhet. Oppgaven ser på hva som skal sikres, hvilke organisatoriske tiltak som kreves, og hvem som har ansvaret for sikringen. Te-

[1] Tranvik (2009) s. 29

[2] Datatilsynet Årsrapport 2012 (2013)

[3] Kvalex (2014)

[4] Hasle (2014)

ma er også hva som kjennetegner tilfredsstillende informasjonssikkerhet rettslig sett i behandling av personopplysninger.

Interessen for samfunnssikring økte noe etter terrorhandlingen den 22. juli 2011, og det omfattet også informasjonssikkerhet. Myndighetene har viet sikkerhet større oppmerksomhet, ved at budsjetter økes og regeletterlevelse følges opp. En overordnet offentlig handlingsplan for informasjonssikkerhet viser at en rekke offentlige etater involverer seg, og det forventes at andre offentlige og private virksomheter følger opp .[5] Uninetts sekretariat for informasjonssikkerhet har gitt tilbud om bistand med gjennomføring av risikovurderinger i universitets- og høgskolesektoren, og dette tilbudet ble akseptert av så å si alle som ikke alt hadde tilfredsstillende informasjonssikkerhet. Riksrevisjonen viste i 2012 og 2013 også interesse for både IKT-drift og informasjonssikkerhet ved sine revisjoner i virksomheten som jeg har kjennskap til.[6] Og i 2013 stiller tildelingsbrevet til virksomheten, med bakgrunn i Digitaliseringsrundskrivet fra FAD[7,] krav om at den må implementere et styringssystem for informasjonssikkerhet basert på anerkjente standarder. Jeg ønsket å forstå dette kravet bedre. Samtidig er det viktigste formålet med informasjonssikkerhet i virksomheter å vareta personvernet. Oppgaven forsøker derfor å belyse de rettslige kravene til et styringssystem for informasjonssikkerhet slik at personvernet blir tilfredsstillende varetatt.

[5] Fornynings-, administrasjons- og kirkedepartementet handlingsplan (2012)

[6] Smolyakova (2012)

[7] Fornynings-, administrasjons- og kirkedepartementet rundskriv nr P-10/2012 (2012)

1.2 Problemstilling

Personopplysningsloven § 13 er relativt kortfattet og ordlyden tilsynelatende enkel. Men teksten kan favne vidt og problemstillingene kan bli komplekse. I hovedsak handler problemstillingene om hvilke krav som stilles til sikring av personopplysningers konfidensialitet, integritet og tilgjengelighet, og videre om hvilke organisatoriske sikkerhetstiltak som er særlig aktuelle. For å svare på dette reises spørsmål om hva som skal sikres og hvem som har ansvaret for sikringen. Det grunnleggende kravet i § 13 er at personopplysningene skal sikres tilfredsstillende gjennom planlagte, systematiske og dokumenterte tiltak. Forarbeidene sier at både tekniske og organisatoriske tiltak kreves.[8] Organisatoriske tiltak innebærer med andre ord krav til arbeidsmåtene som skal brukes i arbeidet med sikring av personopplysninger. Men det stilles også krav til resultatet.

Personopplysningslovens formål og øvrige bestemmelser belyser hva som kreves til en viss grad. Hva som kreves av tiltak og resultater utdypes i kapittel 2 i personopplysningsforskriften. Men for å forstå kravene som stilles bør man forstå formålet med loven, det vil si hva man skal beskytte og hvorfor. For å forstå tiltakene må man også forstå truslene og teknologien, det vil si hva man skal beskytte mot og hvordan. De konkrete kravene som pålegges i lov og forskrift gir også pedagogiske og kompetansemessige utfordringer. Med fremstillingen håper jeg å redusere avstanden mellom det konkrete arbeidet i virksomheten og det som kan oppfattes som abstrakte krav i lov og forskrift.[9]

Skillet og sammenhengen mellom krav og tiltak er grunnleggende men sammensatt. På den ene siden kan man tro at måloppnåelse (ingen alvorlige krenkelser av personvernet) er avgjørende i forhold til om sikringen av personopplysningene er tilfredsstillende eller ikke. Men på den andre siden oppstiller loven spesielle krav til virksomhetens arbeidsmåter, og det tilsier at oppfyllelse av disse kravene kan bli momenter i vurderingen. Dette kan virke paradoksalt, for hvordan kan sikkerheten være tilfredsstillende dersom personvernet krenkes? Forklaring er at man aldri kan oppnå full sikkerhet. Sikkerhet er et sosialt problem.[10] Mangfoldet i menneske-

[8] Ot.prop. nr 92 (1998-1999) s. 115

[9] Tranvik (2009) s. 40, s. 52, s. 63-65

[10] Schneier (2003) s. 43.

lige relasjoner er stort og endres konstant. Det beste man kan oppnå med sikkerhetstiltak er en reduksjon av risiko.[11] Forskriften antar derfor en sammenheng mellom personvern og informasjonssikkerhet og legger opp til reduksjon av risiko for å sikre personvernet. De sentrale tiltakene er organisering av sikkerhetsarbeidet og gjennomføring av tiltak basert på risikovurderinger.[12]

1.3 Særlig om rettskildebildet og metodiske spørsmål

Oppgaven analyserer og drøfter hvordan behandlingsansvarlige skal etterleve sine plikter til personvern og informasjonssikkerhet etter personopplysningsloven § 13 og kapitel 2 i personopplysningsforskriften. Hovedbestemmelsen om informasjonssikkerhet i § 13 er en ganske kort rammebestemmelse. Rettskildene er primært lovteksten og forarbeidene. Datatilsynet tar med lovutvalgets utredning som del av forarbeidene.[13] Schartum påpeker dog at "en NOU gir imidlertid ikke uten videre uttrykk for lovgivers meninger og er ikke uten videre et forarbeid som er rettskilde. Og når det gjelder informasjonssikkerhet og internkontroll var det meningsforskjeller."[14] Slik sett er Odelstingsproposisjonen det sentrale forarbeidet til loven.[15] Proposisjonen gjennomfører bestemmelsen artikkel 17 nr. 1 og 2 i direktiv 95/46 EF, slik at direktivet og eventuell europeisk rettspraksis også blir rettskilder.[16] Vi ser med det en harmonisering over landegrenser. Proposisjonen sier videre at § 13 i hovedsak er en videreføring av utvalgets bestemmelse § 11 i NOU 1997:19.[17] Jeg har derfor brukt utredningen ganske mye. Den korte teksten i proposisjonen om § 13 er mye brukt i både litteratur og i Datatilsynets tekster. Av og til refererer jeg til litteratur som sier det samme som proposisjonen.

Det finnes flere lover og forskrifter som omhandler informasjonssikkerhet. Haug etterlyser bedre samordning av disse .[18] Men i denne sammenheng er poenget dette:

---

[11] ibid s. 83.

[12] Tranvik (2009) s. 13

[13] Datatilsynet (2014)

[14] Schartum (2014)

[15] Ot.prp. nr 92 (1998-1999)

[16] Ot.prp. nr 92 (1998-1999) s. 115

[17] NOU 1997:19

[18] Haug (2006). s. 5-6

- regelsettene har dels ulike formål og anvendelsesområde, de beskytter dels ulike verdier.
- arbeidsformen, måten man sikrer verdier på, er til en viss grad den samme uavhengig av hvilke verdier man sikrer.

Da departementet laget kapittel 2 i personopplysningsforskriften baserte de seg nettopp på slik harmonisering. Departementet påpeker en harmonisering både over bransjer og landegrenser.[19]

Forskriften er gitt som kongelig resolusjon. Departementets forklaringer til forslaget til forskrift blir også en rettskilde. Den er tilgjengelig på internett.[20] Kommentarene fra departementet til den kongelige resolusjonen (forskriften) er også gjengitt i kommentarutgaven til personopplysningsloven. For å kunne vise til et sidetall refererer jeg til kommentarene via denne boken.[21]

Bestemmelsene i forskriften er motivert blant annet av Datatilsynets erfaringer, som igjen var ”basert på kjente teknikker, og anerkjente standarder for kvalitetsstyring, internkontroll, og informasjonssikkerhet.”[22] Dette kan i noen grad kan åpne for bruk av standarder som rettskilde. En av standardene for informasjonssikkerhet som Datatilsynet refererte til var BS-7799 A code of practice for information security management, som er forløperen til ISO 27001.[23] Difi har anbefalt ISO 27001 som standard for informasjonssikkerhet i offentlige virksomheter.[24] De har arrangert kurs i implementering av dette styringssystemet for om lag 100 tilsatte fra ulike offentlige virksomheter, for å gi dem bedre forståelse for hva et styringssystem for informasjonssikkerhet egentlig er, og hvilke tiltak standarden anbefaler organisasjoner å benytte. I odelstingsproposisjonen er det også kort diskutert om sikkerhetstiltak bør baseres på "alminnelige anerkjente metoder" (som standarder). Men dette er ikke tatt inn i lovteksten,

[19] Johansen (2001) s. 346

[20] Justis- og beredskapsdepartementet (2014)

[21] Johansen (2001) s.339 -357

[22] Johansen (2001) s. 233

[23] ISO 27001 (2013)

[24] Difi rapport (2012)

selv om lovgiver i proposisjonen åpner for bruk av slike metoder.[25] Standarder kan slik sett regnes som pedagogisk støtte, det vil si som rettskilder på nivå med litteraturen? Som nevnt over er det økt fokus på informasjonssikkerhetsarbeid i samfunnet. For mange virksomheter kan det være mer nærliggende å basere praktiske arbeid på en bransjestandard enn å ta utgangspunkt i lover og forskrifter. Samtidig vil det være lov og forskrifter som definerer de rettslige kravene som stilles. Dersom bransjepraksis i økende grad baserer seg på ISO 27001 kan standarden kanskje få noe økt rettskildemessig betydning. Jeg har derfor studert ISO 27001 i detalj fordi jeg ønsket å se hvordan den kan belyse § 13 i loven og kapittel 2 i forskriften, samt det praktiske arbeidet i virksomhetene.

Når det gjelder rettspraksis finnes det ikke så mye om krav til styringssystemer for informasjonssikkerhet. Søk i Lovdata gir få eller ingen treff som belyser temaet. Men det finnes noe forvaltningspraksis i Datatilsynets tilsynsrapporter, men jeg har ikke studert denne i detalj. Datatilsynets strategi er en kombinasjon av tilsyn, veiledning og informasjon.[26] De kan treffe vedtak, men de viser en viss varsomhet i forhold til å overprøve virksomhetenes skjønn. Virksomheten kan klage tilsynets avgjørelser, typisk i form av enkeltvedtak, inn for personvernnemda. Klagesak PVN-2007-04 i personvernnemda ser ut til å være den saken i personvernnemdas praksis i perioden 2001 til 2008 som primært omhandler vurderinger av informasjonssikkerhet.[27] Jeg har heller ikke funnet relevante saker i perioden 2009 til 2013.[28] Personvernnemda påpeker i saken fra 2007 at Datatilsynet har en veiledningsplikt etter forvaltningsloven.[29] Denne veiledningsplikten kan fort bli omfattende når tilsynet må gå inn på konkrete saker. Det kan kanskje forklare at Datatilsynet jobber på flere måter. De lager blant annet veiledere på internett som uttrykker deres praksis, og jeg viser til disse i en del sammenhenger. Datatilsynets veiledere, samt standardene, er kanskje de rettskildene som er lettest tilgjengelige for ikke-jurister og de kan derfor ha stor påvirkning på bransjepraksis, særlig i mangel på rettspraksis. Samtidig har de kanskje lavest rettskildemessig vekt. Mer forvaltningspraksis, eller gjerne rettspraksis, kan fylle et veiledningsbehov og være til stor hjelp for virksomheter.

---

[25] Ot.prp. nr 92 (1998-1999) s. 116

[26] Datatilsynet Årsrapport 2012 (2013)

[27] Blume (2009) s. 494

[28] Personvernnemda (2014)

[29] Blume (2009) s. 499

1.4 Oversikt over den videre framstillingen

Jeg forsøker å vise til noen samfunnsperspektiver i noen av kapitlene, men hovedfokus er på forhold og arbeid i virksomheten. I kapittel 2 belyser jeg med utgangspunkt i personopplysningslovens bestemmelser hva som skal sikres. Sikringsarbeidet relateres til personvern, og man kan lure på om det er personvernet, personopplysningene eller egenskaper ved personopplysningene som skal sikres. Deretter fokuserer kapittel 3 på hvem som har ansvaret for sikringen. Hvilket ansvar har den enkelte, hvilket ansvar har virksomhetene, og hvilket ansvar har de ulike aktørene i virksomhetene? I kapittel 4 ser jeg nærmere på hvordan sikring av personopplysninger skal skje, med hovedvekt på organisatoriske tiltak, og særlig bruk av risikoanalyser. Hvilke krav til arbeidsformer stiller regelverket? Deretter kan jeg drøfte hvilket resultat arbeidet med sikring skal gi, i kapittel 5. Her drøftes hva som ligger i tilfredsstillende informasjonssikkerhet og hvordan dette henger sammen med at arbeidet skal være planlagt og systematisk. Disse spørsmålene henger sammen. Jeg oppsummerer i siste kapittel de viktigste konklusjonene.

2 Hva skal sikres?

2.1 Det angår også deg

Behandling av personopplysninger har sosiale sider. Vi er avhengige av å dele opplysninger om oss selv med hverandre. Spørsmålet er bare i hvilket omfang og i hvilke hensikter. I medlemsdebatt i Internet Society i Oslo den 24. oktober 2013, refererte Gisle Hannemyr til historien om hvordan okkupasjonsmyndighetene hadde folketellingsregistre som viste adressene til norske jøder da de i 1941 ble hentet i sine hjem.[30] Det kan illustrere hvorfor opplysninger om religiøs tilknytning anses som sensitive[31] opplysninger, med strengere krav til hvordan de kan behandles. Men det er også et ekstremt eksempel på hvordan personopplysninger kan brukes til formål man ikke hadde tiltenkt da de ble registrert. Denne problemstillingen er også aktuell i universitets- og høgskolesektoren. Jeg tenker da på for eksempel bruk av skytjenesten Office 365 for studenter og/eller ansatte. Da Narvik kommune tok en lignende skytjeneste, "Google Apps", i bruk stilte Datatilsynet krav og gikk i dialog med kommunen. Et av kravene gikk på nødvendige endring av databehandleravtalen med leverandøren. Et annet gikk på at risiko- og sårbarhetsanalyser måtte gjennomføres før tjenesten kunne tas i bruk.[32] Begge deler er krevet i regelverket. Etter dette har Moss kommune og svært mange institusjoner i undervisningssektoren tatt Office 365 i bruk. Noen institusjoner viser stor risikoappetitt, mens andre er mer tilbakeholdne med å lagre personopplysninger i skyen, ikke minst etter avsløringene av PRISM. Varsleren Snowdon viste verden at etterretningstjenesten NSA har stor tilgang til vår informasjon på internettet.[33]

2.2 Personvernbestemmelser som bakgrunn for hva som skal sikres

I boka "Personvern i informasjonssamfunnet" beskriver Schartum og Bygrave personvernlovgivningen som et "halsbrekkende forsøk på å regulere all behandling av personopplysning-

[30] Dagsavisen (2012)

[31] Personopplysningsloven § 2 nummer 8 (a)

[32] Datatilsynet Årsrapport 2012 s. 14

[33] Datatilsynet (2013)

er."[34] Lovgivningen er omfattende og rekkevidden lang. Mange personer skal etterleve regler de kanskje ikke har særlig kjennskap til. Det er økonomiske, juridiske, pedagogiske, kompetansemessige, tekniske og organisatoriske utfordringer som må løses for å behandle personopplysninger på en forsvarlig måte. Arbeidet med informasjonssikkerhet skal bidra til at virksomheten behandler personopplysninger i samsvar med lovens regler.[35]

Personopplysningsloven § 2 nummer 1 definerer personopplysninger som opplysninger og vurderinger som kan knyttes til en enkeltperson. Sensitive personopplysninger defineres i § 2 nummer 8 som personopplysninger om blant annet rase, helse, legning. Opplistingen som er gitt er uttømmende. At det, direkte eller indirekte, gjelder opplysninger om en fysisk og levende person presiseres i NOU 1997:19.[36] Personen som en opplysning kan knyttes til kalles i § 2 nummer 7 for den "registrerte". Det at personopplysninger kan knyttes til et fysisk individ er sentralt, men opplysningens selvstendige innhold er også av betydning. Formålet med loven er etter § 1 å beskytte den enkelte mot at personvernet blir krenket gjennom behandlingen av personopplysninger. Slik sett er opplysningens karakter lite vesentlig dersom en krenkelse faktisk har funnet sted. Dette er poengtert i den offentlige utredningen:

"Selv om en ikke benytter sensitive opplysninger, vil behandling av opplysninger ellers typisk bli omfattet av strenge sikringskrav når sikringsnivået har direkte betydning for ivaretakelse av vesentlige personverninteresser."[37]

At andre kan få kunnskap om personopplysninger kan hemme og påvirke livsutfoldelse.[38] Et svakt personvern kan derfor bli et demokratisk problem, og dypest sett et spørsmål om manglende rettssikkerhet og menneskeverd. Bruk av opplysninger som burde være private kan oppfattes som et tillitsbrudd og skape utrygghet mellom mennesker. Et eksempel kan være målrettet markedsføring mot personer som passer en profil. I NOU 1997:19 påpeker utvalget at

[34] Schartum (2011) s.212

[35] Datatilsynet (2009) s. 8.

[36] NOU 1997:19 s. 5 og s. 66-67

[37] NOU 1997:19 s. 199

[38] Aas (2013)

dette kan oppfattes som manipulerende av den registrerte, men at folk har ulike syn på alvorligheten i dette.[39]

Samtidig er loven klar på at opplysningenes karakter er av betydning. Loven definerer noen opplysningstyper som ”sensitive”, § 2 nummer 8. I NOU 1997:19 påpekes det at det er forskjell på trivielle og sensible personopplysninger og at behandlingen av følsomme personopplysninger undergis en strengere regulering.[40] Den teknologiske utviklingen som gjør informasjon lett og fort tilgjengelig øker også behovet for strengere sikring av sensitive personopplysninger. Utvalget viser til rotasjonspressen for å illustrere dette, men med internettet spres informasjon enda raskere og lenger.[41] ”Behandling” av personopplysninger er etter § 2 nummer 2 ”enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.” Internettet har slik sett medført en eksplosjon i behandling av personopplysninger. Behovet for sikring av personopplysninger er derfor stort.

Lovens § 8 stiller strenge vilkår for å kunne behandle personopplysninger, og enda strengere vilkår stilles i § 9 for å kunne behandle sensitive opplysninger. Særlig er det krav om hjemmel for behandlingen. Det foretrukne grunnlaget er samtykke fra personen til behandlingen. Samtykke er definert i lovens § 2 nummer 7 som ”en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv.” Samtykke gis presumptivt ikke til behandling som oppfattes krenkende etter individets egen vurdering. Selv i situasjoner der samtykke er gitt påpeker NOU 1997:19 at grensen mellom akseptabel og uakseptabel utnyttelse av personopplysningene kan være vanskelig å trekke.[42] Derfor kan Datatilsynet også sette vilkår for behandlingen og krav til informasjonssikkerheten.[43]

I § 11 stilles flere grunnkrav til behandlingen som støtter formålet om å unngå krenkelser. At bruken begrenses til det hjemmelen åpner for, og ikke noe mer, er et sentralt krav for å hindre

[39] NOU 1997:19 s. 18

[40] NOU 1997:19 s. 64

[41] NOU 1997: 19 s. 16

[42] NOU 1997:19 s. 17

[43] Personopplysningsforskriften § 2-2

krenkelser. For å kunne behandle (inkludert å sikre) personopplysninger må virksomheten derfor vite formålet med behandlingen. Og § 15 setter tilsvarende begrensninger på andres bruk av personopplysningene.

Det kan også være krav om konsesjon for behandlingen, §§ 33- 35. Av praktiske årsaker er det unntak for melding og konsesjon for en rekke vanlige behandlinger av personopplysninger, men lovens øvrige krav må allikevel etterleves. Datatilsynet har utarbeidet maler for håndtering av personopplysninger som virksomhetene kan tilpasse egen bruk.[44] Personvernnemdas praksis i perioden 2001 til 2008 viser at spørsmål omkring §§ 8, 9, 11, samt spørsmål om samtykke og konsesjon er gjengangere.[45]

Personopplysningsloven § 14 stiller krav om at virksomheter har internkontroll som sikrer at lovens krav, inkludert de nevnt over, er oppfylt. Som del av internkontrollsystemet inngår sikring av personopplysningene med hensyn på informasjonssikkerhet. At informasjonssikkerhet kreves er sagt eksplisitt i § 13. Det er kravene i § 13 som særlig behandles i denne oppgaven, men det er verdt å nevne at tilfredsstillende informasjonssikkerhet alene ikke er tilstrekkelig i forhold til om behandling av personopplysninger er lovlig. Lovens generelle krav skal sikres via internkontroll. Systemene for styring av henholdsvis internkontroll og informasjonssikkerhet henger sammen, ved at det første omfatter det andre, og de kan være helt eller delvis integrert. Datatilsynet oppsummerer dette slik:

”Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier sikres på en tilfredsstillende måte. Internkontroll handler om å etablere og vedlikeholde planlagte og systematiske tiltak for å sikre at virksomheten oppfyller lovens krav til behandling av personopplysninger.”[46]

[44] Datatilsynet (2012)

[45] Blume (2009)

[46] Datatilsynet (2012)

En virksomhet kan derfor ha (tilsynelatende) tilfredsstillende informasjonssikkerhet, men hvis de bryter de over omtalte grunnkravene til behandling av personopplysninger er behandlingen likevel ikke tillatt.

Vi har påpekt at mennesker har et legitimt om enn varierende behov for både å dele sine personopplysninger og ha et rimelig personvern. Disse behovene er forsøkt varetatt og regulert av de generelle materielle reglene i personopplysningsloven. Nå kan vi spørre hva det er som skal sikres.

Det er selve behandlingen av opplysningene som § 13 om informasjonssikkerhet stiller krav til. Mer presist er det visse egenskaper ved personopplysningene som skal sikres. Dette gjøres i form av krav til sikring av konfidensialitet, integritet og tilgjengelighet til personopplysningene og til systemene som behandler dem. Opplysningens type kan være av betydning, men det er særlig trusselen om uønsket utnyttelse som blir avgjørende for hvor strenge sikkerhetstiltak som er nødvendige, i henhold til lovgiver.[47]

2.3 Personopplysningenes og systemenes konfidensialitet, integritet og tilgjengelighet

Personopplysningsloven § 13 første ledd krever sikring av opplysningene med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandlingen. Dette er det vanligste utgangspunktet for, og formålet med, informasjonssikkerhet.[48] Den offentlige utredningen beskriver disse begrepene som fellesbetegnelse på en rekke mer detaljerte krav til opplysningene, og sier at disse kravene er reflektert i personopplysningslovens bestemmelser.[49] Det er disse kriteriene eller egenskapene som skal sikres etter § 13. Behandlingsansvarlige må klarlegge hvilke krav som må stilles til sikring av henholdsvis konfidensialitet, integritet og tilgjengelighet for personopplysningene som behandles.[50]

[47] Ot.prp. nr 92 (1998-1999) s. 115

[48] Håndbok i datasikkerhet (2006) s. 31

[49] NOU 1997:19 s. 129

[50] Ot.prp. nr 92 (1998-1999) s. 116

Konfidensialitet betyr i utgangspunktet at bare de som har rett til å behandle opplysningene får tilgang til dem. Personopplysningene skal være beskyttet mot uautorisert innsyn under behandlingen.[51] Det samme sies i kommentarene til personopplysningsforskriften.[52] Den offentlige utredningen omtaler dette som den registrertes interesse av diskresjon.[53] Konfidensialitet adresseres konkret i personopplysningsforskriften § 2-11. Både her og i utredningen påpekes det at ikke alle opplysninger nødvendigvis har samme krav til konfidensialitet.[54] Også dette kan begrunne behov for å identifisere og klassifisere opplysningene som behandles i virksomheten, med ulike krav til behandlingen av opplysningene avhengig av deres klassifisering. Datatilsynet viser hvordan klassifisering kan gjøres.[55]

Med integritet menes at informasjon ikke skal kunne endres utilsiktet eller av uvedkommende.[56] Kun de som er autorisert til det skal kunne gjøre endringer. Dette viser også sammenhengen mellom informasjonssikkerhet og opplysningskvalitet, jamfør personopplysningsloven § 14 første ledd. Dersom opplysningene har god kvalitet og integritet, er de fullstendige og gir et best mulig grunnlag for riktige beslutninger. Dette bidrar til rettssikkerhet som også er et av formålene med personvern.[57]

Tilgjengelighet forklares i forarbeidene som at opplysningene er stabilt tilgjengelige etter behov, for dem som har lovlig tilgang til dem.[58] I kommentarene til forskriften beskrives det som å "sørge for at tilstrekkelige og relevante opplysninger er til stede."[59]
Tilgjengelighet adresseres i personopplysningsforskriften § 2-12. Det kan være en lang rekke tiltak involvert i sikring av tilgjengelighet. Departementet påpeker igjen at sikringsbehovet følger fra utført risikovurdering.[60] Mange tiltak er IKT-tekniske, men andre kan være organi-

[51] Ot.prp. nr 92 (1998-1999) s. 116

[52] Johansen (2001) s. 344

[53] NOU 1997:19 s. 22

[54] NOU 1997:19 s. 22

[55] Datatilsynet (2012)

[56] Johansen (2001) s. 344

[57] NOU 1997:19 s. 18-22

[58] Ot.prp. nr 92 (1998-1999) s. 344

[59] Johansen (2001) s. 344

[60] Johansen (2001) s. 355

satoriske eller av andre typer. Eksempelvis nevnes å sikre alternativ behandling dersom informasjonssystemet er utilgjengelig. Når behandlingen blir omfattende kan dette være vanskelig. Kanskje må tilgjengelighetsspørsmålet løses IKT-teknisk, det vil si ved redundante og robuste løsninger. Omfattende IKT-systemer kan gi behov for driftsrutiner basert på utbredte kvalitetsmetoder som ITIL og COBIT.[61] For kravet om alternativ behandling i paragrafen blir forholdsmessighet igjen et stikkord. Ikke all behandling av personopplysninger krever like høy tilgjengelighet. Men kravet om å ha sikkerhetskopi av personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk vil være aktuelt i de fleste tilfeller. Det stilles med andre ord krav om sikkerhetskopiering.[62]

Å vareta konfidensialitet, integritet og tilgjengelighet er som nevnt det klassiske målet for informasjonssikkerhetsarbeid, men å sikre disse egenskapene bidrar også til å oppfylle personvernlovgivningens formål. Dette illustrerer sammenhengen mellom informasjonssikkerhet og personvern.

Det er ikke bare opplysningene selv og systemene som brukes til å behandle personopplysninger som må sikres. Dette omtales i den offentlige utredningen, men det følger også av at den totale sikkerheten ikke blir bedre enn sikkerheten i hvert enkelt ledd.[63] Hvis en svakhet i et system som ikke behandler personopplysninger kan utnyttes, så kan det i verste fall åpne for tilgang til systemene som behandler personopplysninger. Generell IKT-sikkerhet blir slik sett en del av hele informasjonssikkerheten. Dette er et vesentlig poeng: IKT-sikkerhet en viktig men ikke tilstrekkelig del av sikkerhetsarbeidet. Utnyttelse av sårbarheter i IKT-systemer kan blottlegge personopplysninger. IKT-systemene er svært utsatte for trusler, og hvis tekniske tiltak ikke treffes er sannsynligheten for sikkerhetsbrudd nærmest garantert.

Personopplysningsforskriften § 2-13 stiller krav om at opplysningenes integritet skal sikres. Det gjelder både personopplysningene og annen informasjon av betydning for sikkerheten. Igjen er tiltakene mange og varierte, og igjen skal tiltakene følge av risikovurderingene.[64] Men særlig er det snakk om å sikre at bare de rette personene har tilgang til å endre opplys-

[61] Moeller (2013)

[62] Johansen (2001) s.355

[63] NOU 1997:19 s. 200

[64] Johansen (2001) s. 355

ningene på rettmessig måte. Autorisering og autentisering står derfor sentralt, likeså sikring mot ødeleggende programvare, krevet i personopplysningsforskriften § 2-13. Igjen må det kommenteres at ikke alle opplysninger har samme behovet for integritet.

2.4 Avsluttende kommentarer

Både personopplysninger, informasjonssystemer og informasjon av betydning for informasjonssikkerheten skal sikres. Disse kan være av mange typer, så virksomheten må lage en oversikt og benytte klassifisering etter behov. Det som sikres kan oppsummeres som risikoen for systemenes og opplysningenes konfidensialitet, integritet og tilgjengelighet, i forhold til sannsynlighet for og konsekvenser av krenkelser av personvernverdier i henhold til lovens bestemmelser. Bestemmelser i personopplysningsloven og personopplysningsforskriften uttrykker mange sider ved disse begrepene og kravene som stilles.

3 Hvem har ansvaret for sikringen?

Når behandling først kan finne sted er reglene klare på hvem som har hovedansvaret for sikringen: virksomhetenes toppledelse. Virksomheter har et selvstendig samfunnsansvar. I henhold til forarbeidene hadde, naturlig nok, ingen høringsinstanser innvendinger mot forslaget om å pålegge de behandlingsansvarlige et lovfestet ansvar for tilstrekkelig sikring av personopplysninger.[65] Birthe Eriksen har beskrevet hvordan moderne reguleringsteknikk benyttes for å regulere forholdet mellom selskap og samfunn.[66] Poenget i denne sammenheng er at det er *virksomheten* som i stor grad må regulere seg selv for å forvalte risikoforhold, og at lovgiver gir mindre materiell detaljregulering. Virksomheter pålegges rettslige plikter og ansvar, men virksomheten må selv finne ut av hvordan ansvaret skal etterleves. Internkontrollforskriften legger hovedansvaret for sikkerhetsarbeid på arbeidsgiver.[67] I staten regnes den øverste leder som arbeidsgiver; den som råder over midler og utøver styringsretten. Hvis virksomheten har et styre er det styret som kollektivt organ som blir ansvarlig for gjennomføring av arbeidsgivers plikter etter loven. Den øverste daglige leder utøver ledelse i virksomheten i arbeidsgivers sted, med løpende og utøvende arbeidsgiveransvar. Hvem som er arbeidsgiver trenger ikke i denne sammenheng å avgrenses eksakt. Fanebust sier at forarbeidene gjør det klart at det siktes til den øverste bedriftsledelsen som leder virksomheten i arbeidsgivers sted, og til den som har lederfunksjon ved en selvstendig enhet.

3.1 Den behandlingsansvarlige

I personopplysningsloven § 13 legges ansvaret for tiltak først på den behandlingsansvarlige. Databehandlerens ansvar omtales for klarhets skyld senere i oppgaven. Personopplysningsloven § 2 nummer 4 definerer den ”behandlingsansvarlige” som ”den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.” Personopplysningsforskriften § 2-3 første ledd legger ansvaret for informasjonssikkerheten på den daglige ledelsen. Også departementet understreker at i de tilfellene der den behandlingsan-

[65] Ot.prp. nr 92 (1998-1999) s. 95

[66] Taraldset (2010) s. 68

[67] Internkontrollforskriften § 4

svarlige er en juridisk person, vil ansvaret for å etterkomme sikkerhetskravene påhvile ledelsen.[68]

Skillet mellom behandlingsansvarlige og medarbeidere kan være flytende. I forhold til ansvarsforhold anbefaler Fanebust at en driftsleder med lite myndighet må legge saken frem for sin overordnede, klargjøre tiltaksbehovet og be om bevilgning. Dersom driftsleder gjør dette så flyttes arbeidsgiveransvaret opp til overordnede myndighet i den konkrete saken.[69]

Ansvaret for informasjonssikkerhetsarbeidet er for øvrig selvstendig, det vil si at den behandlingsansvarlige ikke kan vente på at andre krever tiltak gjennomført, men må ta initiativ selv. I den offentlige utredningen presiseres det videre at ansvaret er kontinuerlig: "Sikkerhetsvurderingen må skje i forhold til de til enhver tid rådende forhold."[70] Behandlingsansvarlige må føre løpende kontroll. Personopplysningsloven § 14 legger ansvaret for internkontroll på den behandlingsansvarlige. Forskriften nyanserer dette ved å legge ansvaret for etterlevelse av forskriftens regler på den daglige ledelsen.[71] Ledelsen må stille seg bak og slutte opp om sikkerhetsarbeidet. Departementet trekker dette frem som et ansvar for den daglige ledelsen i sin forklaring til personopplysningsforskriften § 2-3.[72] Men det følger også av praktiske årsaker, for fremdrift i arbeidet krever normalt forankring i den daglige ledelsen.

I dette ligger en mulighet for at ansvaret for sikringen ikke ligger på den som har den "endelige" styringsretten? Men den daglige ledelsen har ansvaret for å følge forskriftens regler, og den øverste ledelsen har ansvaret for etterlevelse av personvernreglene inkludert reglene om informasjonssikkerhet. Medarbeidere kan og skal også pålegges ansvar, se eksempelvis personopplysningsforskriften § 2-7 til § 2-9. I § 2-7 kreves det at klare ansvarsforhold etableres, dokumenteres og gjøres kjent i virksomheten.[73] Dette er en ledelsesoppgave. Datatilsynet har

[68] Ot.prp. nr 92 (1998-1999) s. 116

[69] Fanebust (2013) s.181- 183

[70] NOU 1997: 19 s. 199

[71] Personopplysningsforskriften § 2-3

[72] Johansen (2001) s. 348

[73] Johansen (2001) s. 350

maler med forslag til organisering.[74] Departementet sier også at utformingen av informasjonssystemet skal gjøres etter ledelsens anvisninger, slik at tilfredsstillende informasjonssikkerhet oppnås. Men det skal også tas hensyn til økonomi og funksjonalitet. Valgt konfigurasjon skal dokumenteres. Ledelsen skal også bestemme hvordan arbeidet med informasjonssystemet skal foregå, og dette skal gjøres kjent i virksomheten, si i form av rutiner.[75] Medarbeiderne har dog plikt til å bidra, selv om:

”Det vil være opp til ledelsen å beskrive stillinger eller peke ut personer nedover i organisasjonen som skal sørge for at loven etterleves i praksis. Dette vil likevel være et internt anliggende - det overordnete ansvaret for sikkerheten påhviler ledelsen, og tilsynsmyndighetene kan forholde seg til denne.”[76]

Dette viser at ledelsens organisasjons- og instruksjonsmyndighet blir viktig for behandlingsansvaret. Etter § 2-8 skal medarbeidere behandle opplysninger der det blir pålagt dem (av ledere). Departementet påpeker at all bruk medfører risiko, og at bruken av systemene derfor bør begrenses til den nødvendige. Etter forholdene vil bruk av "world wide web" kunne tillates. [77] Etter konfidensialitetsbehov har medarbeiderne også taushetsplikt, ikke bare om personopplysningene de behandler men om alle forhold av betydning for informasjonssikkerheten § 2-9.[78] Datatilsynet tilbyr maler for taushetsplikt.[79]

Fordelingen av oppgaver til medarbeidere er ikke pulverisering av ansvar men en praktisk nødvendighet. Poenget er at kompetanse kan delegeres internt i virksomheten, men den som delegerer fritas ikke for sitt ansvar (uegentlig delegasjon). Det er nødvendig å trekke medarbeidere inn i sikkerhetsarbeidet. For det første har øverste ledelse sjelden kapasitet til selv å utføre det mest praktiske sikkerhetsarbeidet, jamfør at behovet for en organisasjon oppstår når en person alene ikke klarer alle oppgavene. Deretter er det slik at de som utøver det praktiske

[74] Datatilsynet (2012)

[75] Johansen (2001) s. 351

[76] Ot.prp. nr 92 (1998-1999) s. 116

[77] Johansen (2001) s. 351

[78] Johansen (2001) s.352-353

[79] Datatilsynet (2012)

arbeidet har kunnskap og evner som må og bør utnyttes. Det betyr at mange av de ulike tiltakene som forskriften pålegger den behandlingsansvarlige (ved daglig ledelse) må utføres av medarbeiderne i virksomheten. I sine forklaringer til forskriften påpeker departementet også at ansvaret som pålegges i personopplysningsloven § 13 "omfatter å sørge for at tilstrekkelig sikkerhetsfaglig kompetanse er tilgjengelig hos den behandlingsansvarlige." Det samme presiseres i forhold til partner og leverandører.[80] I forhold til informasjonssikkerhet er det som nevnt plikt til å dokumentere medarbeidernes ansvar for informasjonssikkerhetsarbeid, jamfør Datatilsynets mal. Men dette endrer ikke det grunnleggende ansvarsforholdet. Verd å nevne er at ISO 27001 også anbefaler retningslinjer i forhold til medarbeideres brudd på reglene, det vil si om organisatoriske sanksjoner.[81] Datatilsynet på sin side tilbyr en mal for en sikkerhetsinstruks for brukerne og ledere.[82]

3.2 Roller og oppgaver

Etter tolking av lov og forskriften kan det være mange roller i sikkerhetsarbeidet. Etter behov må roller beskrives og ansvar og oppgaver fordeles på alle nivåer i virksomheten, se forskriften § 2-7 og departementets kommentarer til denne.[83] Tranvik trekker frem det samme.[84]
Rollene som er nevnt i lov og forskrift er disse;

Rolle	**Personopplysningslov**	**Personopplysningsforskrift**	**Kommentar**
Den registrerte	§ 2		kalt "den enkelte" i § 1
Behandlingsansvarlige	§ 2, § 13, § 14	(mange)	Kort sagt: øverste ledelse
Databehandler	§ 2, § 13, § 14, § 15	§ 2-15	Også kalt leverandør (eller underleverandør) / samarbeidspartner
Datatilsynet	(mange)	§ 2-2	
Daglig ledelse		§ 2-3	Øverste ledelse, men typisk nivået under øverste ledelse
Medarbeidere		§ 2-8 (§ 2-9)	Ansatte i virksomheten

[80] Johansen (2001) s. 344 og s. 352

[81] ISO 27001 s. 11

[82] Datatilsynet (2012)

[83] Johansen (2001) s. 350-351

[84] Tranvik (2009) s. 23

Også andre roller kan utledes fra regelverket, som for eksempel (daglig) sikkerhetsansvarlige, sikkerhetsrevisor og personvernombud. For, utover daglig ledelse og medarbeidernes "normale" behandling av personopplysninger skal blant annet disse oppgavene utføres (med rolleplassering indikert i parentes): risikovurderinger (ledelse, systemeiere, sentrale medarbeidere, IT-sjef), revisjoner (intern eller ekstern revisor), avvikshåndtering (ledelse, sentrale medarbeidere, IKT-medarbeidere), fysisk sikring (driftsmedarbeidere, IKT-medarbeidere, vaktpersonell) og teknisk ikt-sikring (IKT-medarbeidere). Etter forholdene kan dette utføres av en eller flere personer. Ofte utpekes en person som får et hovedansvar for å koordinere aktivitetene, typisk kalt sikkerhetsleder, informasjonssikkerhetsansvarlig, Chief information security officer (CISO) eller lignende.

I departementets forklaringer til forskriften § 2-7 trekkes forskjellen mellom driftsledelse og sikkerhetsledelse frem. Departementet sier at ideelt sett bør rollene tillegges forskjellige medarbeidere i virksomheten, med mulig unntak for små virksomheter. Sikkerhetsleders oppgaver vil "omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling."[85] Også Tranvik diskuterer hvem som bør ha rollen som sikkerhetsleder. I noen virksomheter legges dette til IT-sjefen (driftsleder). Dette har fordeler og ulemper. En fordel kan være større oppmerksomhet og stort gjennomslag i IT-avdelingen, men det kan samtidig være en ulempe dersom IT-sjefen ikke prioriterer sikkerhetsarbeidet. Ofte vil kanskje ikke en leder ha kapasitet til utøvelse av enda en praktisk og kontinuerlig oppgave? Det kan også være at IT-sjefen ikke har kompetanse nok, si om personvern og regelverk. Dersom sikkerhetsleder ikke er IT-sjef bør lederen ha en fremskutt posisjon for å få tilstrekkelig oppmerksomhet hos ledelsen. Det er ikke uvanlig at sikkerhetsleder derfor rapporterer direkte til daglig leder.[86]

Personopplysningsforskriften § 2-5 sier at revisjon skal gjennomføres jevnlig. Det viktigste formålet med revisjon er å finne forbedringer. Derfor legges resultatene fra revisjonen frem

[85] Johansen (2001) s. 350-351

[86] Tranvik (2009) s. 53

som del av ledelsens gjennomgang av sikkerhetsmål og strategi, se forskriften § 2-3.[87] Ledelsen har ansvar for å følge opp revisjoner og forbedringer, med mer. Forskriften sier ikke om revisor skal være intern eller ekstern. Ekstern revisjon kan utføres av en godkjent revisor, si i forbindelse med sertifisering. Men departementet legger intern revisjon til grunn, når de foreslår at den gjennomføres etter internkontrollforskriften, på samme vis som for HMS-arbeid. De viser til forskrift av 6. desember 1996 nr. 1127 om systematisk helse, - miljø og sikkerhetsarbeid i virksomheten. [88] Datatilsynet legger det samme til grunn.[89] I sin veileder omtaler de revisjon som "egenkontroll".[90] Tilsyn fra Datatilsynet, eller riksrevisjonen i det offentlige, vil kunne ligne på revisjon.

Det er ikke sikkert det er mulig i en mindre virksomhet å utpeke egen intern revisor. Strengt tatt skal man ikke revidere sitt eget arbeid, sammenlign bukken og havresekken, og at det er vesentlig med et nytt syn på ting.[91] Systemet bør derfor ikke revideres av den som har koordineringsansvaret for systemet. For sertifisering etter ISO 27001 vil det være ekstern revisjon i tillegg til krav om regelmessige interne revisjoner for å følge opp om styringssystemet for informasjonssikkerhet gir ønsket sikkerhet og er i tråd med kravene i standarden.[92] Ekstern revisor kontrollerer også at en akseptabel prosess for intern revisjon finnes og er utført tilfredsstillende.

Departementet skriver i sin kommentar til § 2-6 at avviksbehandling skal iverksettes umiddelbart og at den "vil normalt omfatte rapportering, strakstiltak, permanent korrigering av avvik og oppfølging av korrigerende tiltak over tid for å vurdere om dette fungerer etter sin hensikt." Formålet med avviksbehandlingen er å gjenopprette normaltilstand og hindre gjentagelse. [93] Daglig ledelse har ansvaret for dette. Oppgaven kan typisk delegeres helt eller delvis, så lenge ledelsen følger opp arbeidet.

---

[87] Johansen (2001) s. 349-350

[88] Internkontrollforskriften

[89] Datatilsynet (2000) s. 8

[90] Datatilsynet (2009) s. 37

[91] Revisorloven § 4-1

[92] ISO 27001 s. 8

[93] Johansen (2001) s. 350

Personopplysningsforskriften § 2-10 pålegger den daglige ledelsen plikt til å sikre fysisk ønsket tilgang til utstyret, både det som brukes til behandling av personopplysninger og annet utstyr som er av betydning for informasjonssikkerheten. Departementet gir eksempler i sine kommentarer til forskriften.[94] Håndbok i datasikkerhet eller annen litteratur utdyper dette.[95] Ansvaret kan typisk delegeres til si, driftsleder og den enkelte ansatte. Vedlegg A i standarden utdyper og gir eksempler på fysisk sikring som illustrerer nettopp dette.[96]

Ansvaret for IKT-tekniske sikring av konfidensialitet, integritet og tilgjengelighet, personopplysningsforskriften § 2-10, § 2-11 og § 2-12 vil typisk falle på IT-sjefen, som eventuelt delegerer etter behov. Den daglige ledelsen har dog ansvar for sikringstiltak av ikke-teknisk karakter. Typisk kan det helt eller delvis delegeres til informasjonssikkerhetsansvarlige, linjeledere osv. Det er grunnleggende både for samarbeid og for den enkeltes arbeid at ansvaret dokumenteres.

3.3 Om ledelsens, databehandlers og Datatilsynets ansvar

Tranvik påpeker at støtte, eller i det minste en viss interesse, fra ledelsen er avgjørende for at arbeid med informasjonssikkerhet i virksomheten skal tilfredsstille de rettslige kravene som stilles. Dette følger også av regelverkets ordlyd. Men praktisk gjennomføring er typisk bare i liten grad koblet til den øverste ledelsen.[97] Selv om daglig og øverste ledelse kan delegere store deler av ansvaret for praktisk arbeid med sikring av personopplysninger er det noen oppgaver de ikke kan eller bør delegere. Det gjelder for eksempel spørsmål om policy og sikkerhetsmål. Departementet pålegger ledelsen ansvaret for å beskrive virksomhetens sikkerhetsmål.[98] Så selv om ledelsen ikke utformer disse selv må de stille seg bak dem. Når det gjelder hvor stor risikoaksept virksomheten vil ha er dette helt klart en oppgave for øverste ledelse å vurdere. Det samme kan sies om overordnede beslutninger om ressurser til arbeidet.[99]

---

[94] Johansen (2001) s. 353

[95] Håndbok i datasikkerhet (2006) s. 217-233 og s. 337 og s. 350

[96] ISO 27001 s. 14

[97] Tranvik (2009) s. 51

[98] Johansen (2001) s. 348

[99] Tranvik (2009) s. 23

Datatilsynet har ikke ansvar for sikkerheten i en virksomhet. Men de kan gi pålegg om tiltak og fastsette kriterier for akseptabel risiko, personopplysningsforskriften § 2-2. Forarbeidene gjør det klart at ansvaret plasseres hos virksomheten, og at selv om Datatilsynet har utført tilsyn uten bemerkninger er ikke det noen garanti for at "alt er i orden".[100] Se ellers personopplysningsloven kapittel VIII om Datatilsynets oppgaver.

Personopplysningsloven § 13 første ledd legger også ansvaret for informasjonssikkerheten på databehandleren. Også dette ansvaret er selvstendig, jamfør over. Personopplysningsloven § 2 nummer 5 definerer databehandleren som den som behandler personopplysninger på vegne av den behandlingsansvarlige. Typisk vil databehandleren være en leverandør eller en samarbeidspartner og lignende. Personopplysningsloven § 15 krever at leverandørens behandling av personopplysninger på vegne av behandlingsansvarlige skal begrenses til den behandling som er avtalt skriftlig. Med andre ord er databehandlers ansvar i stor grad avgrenset av oppdragsavtalen. Personopplysningsforskriften § 2-15 beskriver nærmere kravene til sikkerhet ved bruk av databehandler. Dersom Datatilsynet ved tilsyn finner manglende eller mangelfull databehandleravtale vil de gi pålegg om at dette rettes.

Essensen er at databehandler pålegges et selvstendig ansvar, og at også databehandleren må etterleve reglene om personvern og sikkerhet. Samtidig har behandlingsansvarlige en plikt til å sørge for at databehandleren oppfyller sine plikter, forskriften § 2-15. Forarbeidene presiserer det samme, og konklusjonen blir at begge har ansvar men hovedansvaret ligger på behandlingsansvarlige.[101] Departementet utdyper dette ytterligere i sin kommentar til personopplysningsforskriften § 2-15.[102] Som et av formålene nevnes her å sikre et harmonisert sikkerhetsnivå i hele kommunikasjonskjeden. Datatilsynet omtaler databehandleravtaler nærmere og tilbyr en mal for innholdet i denne.[103]

[100] NOU 1997:19 s. 117

[101] Ot.prp. nr 92 (1998-1999) s. 117

[102] Johansen (2001) s. 356

[103] Datatilsynet (2013)

4 Hvordan skal sikringen skje?

4.1 Overordnet tilnærming

Utgangspunktet er personopplysningsloven § 13 første ledd som krever at sikringen skal skje gjennom planlagte og systematiske tiltak. Som vi har sett i forarbeidene ligger det i dette en henvisning til bruk av ”anerkjente standarder og teknikker.” Men hva er bakgrunnen til denne henvisningen?

Datatilsynet skriver at ”informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger.”[104] Men risikohåndtering er en viktig oppgave på mange områder i en virksomhet. Eksempler er HMS-, kvalitets- og økonomistyring. Stikkordene i alle sammenhengene er ”internkontroll” og ”styringssystemer”. For virksomheter kan det være av interesse å se disse områdene i en sammenheng og å bruke en felles tilnærming.

Internkontroll er et krav også etter personopplysningsloven § 14. I henhold til forarbeidene til personopplysningsloven er det ikke fastsatt spesielle krav til metode for etablering av internkontrollsystem, men tilnærming bør innebære aktiviteter som kartlegging av krav, risikovurdering, fastlegging av mål, tiltaksvurdering og evaluering.[105] Riksrevisjonen påpeker at risikostyring kan være vanskelig:

”Flere virksomheter har imidlertid fortsatt utfordringer med å implementere og nyttiggjøre seg et system for risikostyring.” [106]

Lindøe observerte noe lignende i forbindelse med internkontroll av arbeidsmiljøet:

”Flere evalueringer og casestudier har vist at internkontroll passet som hånd i hanske til store og ressurssterke virksomheter som hadde en kvalifisert og kompetent stab. […]. Det ble bety-

[104] Datatilsynet (2011) s. 22

[105] NOU 1997:19 s. 202

[106] Riksrevisjonen (2013) s. 82

delige problemer med å få innført internkontrollregimet innen små- og mellomstore bedrifter. […] I 1997 kom en revidert forskrift som la større vekt på handlingskomponenter, dempet kravene til dokumentasjon og gav større rom for lokal tilpasning til virksomhetenes mangfold. […] De fleste småbedrifter hadde ikke erfaringer med formelle systemer for kvalitetssikring før de fikk et krav om 'systematisk helse-, miljø og sikkerhetsarbeid' (internkontroll), og mange opplevde derfor dette som en byrde og et unødig tiltak"[107]

Lovgivning som i stor grad legger ansvaret for risikohåndtering på virksomheten selv er eksempler på refleksiv rett. Denne metodikken er inspirert av kvalitetssikring i industrien og ble tidlig tatt i bruk i nordisk arbeidsliv. Kjennetegn er større frihet og selvstendighet, slik den ble kjent fra den nordiske (eller norske) arbeidslivsmodell, og dette inspirerte EU-retten på HMS-området.[108] Og senere også personvernområdet. Metoden har et preventivt perspektiv. Risiko skal forutses og reduseres med målrettede og kostnadseffektive sikringstiltak. Virksomheten må på forhånd organisere seg for å etterleve krav og formål. Loven trekker rammer, forskrifter utdyper, men virksomheten må regulere seg selv i betydelig grad, ved at rammeverket må implementeres og tilpasses i den enkelte virksomhet. Tranvik trekker frem to kjennetegn ved dette. For det første er det liten grad av detaljert regelstyring; mye overlates til virksomhetens skjønn og tilpasning etter behov og ressurser. Det andre er en strukturbasert formålsregulering. Det angis hvilke styringsteknikker som skal brukes, og formålet med reguleringen. Juridisk teori åpner her for stor frihetsgrad.[109] Samtidig blir det større vekt på etterfølgende kontroll og tilsyn basert på melding eller annet grunnlag.

4.2 Krav til tiltakene

Datatilsynet skriver om internkontroll og informasjonssikkerhet på sine nettsider:

"Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier sikres på en tilfredsstillende måte. Internkontroll handler om å etablere

[107] Lindøe (2002) s. 34

[108] Ibid . s. 24

[109] Tranvik (2009) s. 22-26

og vedlikeholde planlagte og systematiske tiltak for å sikre at virksomheten oppfyller lovens krav til behandling av personopplysninger."[110]

Datatilsynet skriver dette etter tolking av regelverket. Hvis man sammenholder første og andre ledd i personopplysningsloven § 13 ser man at tilfredsstillende informasjonssikkerhet skal oppnås ved planlagte, strukturerte og dokumenterte tiltak. Utover dette innskrenker ikke loven virkemiddelbruken. Personopplysningsforskriften kapittel 2 stiller dog krav om en rekke ulike typer tiltak. Tiltakene kan kategoriseres som tekniske, organisatoriske, juridiske, økonomiske og pedagogiske eller lignende. Forskriften utdyper sikring av konfidensialitet, integritet og tilgjengelighet i § 2-1, § 2-11, § 2-12 og § 2-13, og i andre paragrafer gis krav om spesielle tiltak. Men sikringsbehovet følger prinsippet om forholdsmessighet, forskriftens § 2-1,ved at sikringstiltakene skal stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd. Det vil si sikringen skal stå i forhold til gjennomført risikovurdering.[111]

Det å være tilknyttet internett betyr at en rekke tekniske tiltak må iverksettes for å redusere risikoen for sikkerhetsbrudd. Men forarbeidene påpeker at tilfredsstillende informasjonssikkerhet forutsetter etablering av både organisatoriske og tekniske sikkerhetstiltak. Som eksempler på organisatoriske tiltak nevnes å etablere klare ansvars- og myndighetsforhold i organisasjonen, sørge for tilfredsstillende kompetanse hos den behandlingsansvarliges personell, og bare autorisere personellet for tilgang til personopplysninger i den grad det er nødvendig for å utføre pålagte oppgaver.

Som eksempel på tekniske tiltak nevner forskriften for eksempel konkret at behovet for kryptering må vurderes ved overføring av opplysninger over internett. Lagrede opplysninger skal sikres gjennom hele sitt livsløp.[112] Personopplysningsforskriften § 2-11 siste ledd om sletting av data fra lagringsmedier som ikke skal brukes lenger illustrerer at personopplysninger skal sikres i hele behandlingens varighet.[113]

---

[110] Datatilsynet (2011) s. 22

[111] Johansen (2001) s. 353

[112] Johansen (2001) s. 353-354

[113] Johansen (2001) s. 354

4.2.1 Planlagte og systematiske

Ordene ”planlagte og systematiske” er ikke tilfeldig valgt. I ”planlagt” ligger blant annet at behovet for sikring må vurderes før behandlingen av personopplysninger starter. Det innebærer også at tiltakene skal være gjennomtenkte og tilpasset en helhet. Alle tiltak skal være planlagte, men ikke minst gjelder det de organisatoriske tiltakene som involverer ledelsen. Departementet trekker frem sikkerhetsmål og strategi i sine forklaringer til forskriften § 2-3.[114] De peker på at disse skal gjennomgås jevnlig (si årlig, og gjerne koblet til årlig økonomi- eller virksomhetsplanlegging) for at de til en hver tid skal være i samsvar med virksomhetens behov. Slik danner de også grunnlaget for risikovurderinger, som er diskutert under.

I ”systematisk” kan man innfortolke at arbeidet skal være strukturert regelmessig og at det skal følges opp. For å forstå mer om hva som ligger i kriteriene må man tolke forskriften med loven som en ramme. Forskriftens bestemmelser om ledelsens gjennomgang og revisjon viser for eksempel at arbeidet skal være vedvarende, med aktiviteter som gjentas regelmessig og etter behov. Kontinuerlig forbedring er etter tolkning et stikkord. Men viktigst er nok at risikovurderinger gjennomføres og dokumenteres. Tiltakene som treffes skal være dokumentert ved en risikovurdering.[115]

Sammen fanger ordene ”planlagt og systematisk” en del av essensen i det bransjen oppfatter som beste praksis. Essensen i bransjepraksis er at den uttrykker kvalitetsbaserte former for samhandling mellom mennesker som har vist seg å fungere godt i praksis. I kommentarene til § 13 i forarbeidene for personopplysningsloven diskuteres fordeler og ulemper med å lovfeste sikkerhetstiltak hentet fra bransjepraksis.[116] Et av spørsmålene som diskuteres er normenes rettslige status. Men siden forskriften er påvirket av en standardisert utgave av bransjepraksis, er det ikke unaturlig å bruke denne utfyllende ved tolking av forskriften. Den nyeste versjonen, ISO 27001:2013 er mer detaljert enn forskriften og kan nok gi en mer helhetlig forståelse av systematisk sikkerhetsarbeid en forskriften gjør alene. Men det overordnede poenget i denne sammenheng er at sikring ikke er trivielt, og det er derfor behov for at virksomheten jobber

[114] Johansen (2001) s. 348

[115] Blume (2009) s. 497

[116] Ot.prp. nr 92 (1998-1999) s. 116

målrettet med oppgaven slik at arbeidet utvikler seg og blir bedre over tid. På sikt kan man håpe at rettspraksis presiserer sikringsoppgaven bedre.

4.2.2 Dokumenterte

I paragrafen § 13 andre ledd er det også krav om at informasjonssystemet som brukes til behandling, samt tiltakene for sikkerhet, skal være dokumenterte. Plikten til dokumentasjon er utdypet i personopplysningsforskriftens bestemmelser om informasjonssikkerhet. Dokumentasjon har flere formål. Forarbeidene sier at formålet med dokumentasjonen først og fremst er å bidra til at sikkerhetskravene etterleves i virksomhetens drift, og for å oppnå dette må dokumentasjonen rettes til medarbeiderne i virksomheten. Dokumentasjonen skal også gi grunnlag for kontroll.[117] Dette inkluderer egenkontroll.[118] Sammenhengen med internkontrollbestemmelsen i § 14 trekkes frem i proposisjonen.[119] I forklaringene til forskriften påpeker departementet også at dokumentasjonen skal omfatte beskrivelse av organisering, rutiner for bruk samt registrering av hendelser.[120] Videre bør dokumentasjon også brukes i ledelsens arbeid.[121] Slik gir dokumentasjonen et grunnlag for kontinuerlig forbedring. Mot denne bakgrunn kan dokumentasjonsarbeidet fort bli omfattende og utfordrende? For hva skal man dokumentere, hvilket detaljnivå skal dokumentasjonen ha, når skal den skrives og hvem skal skrive den? Arbeidet krever kompetanse og kan ta tid hvis dokumentasjonen blir omfattende. Ledelsen må slutte opp om slik ressursbruk, men bare etter behov. Departementet i sin kommentar til forskriften § 2-16 trekker også frem poenget med at "dokumentasjonens omfang og detaljeringsgrad må være i samsvar med sikkerhetsbehovet."[122]

Det er to overordnede poenger med kravene til dokumentasjon som inngår i vurderingen av tilfredsstillende informasjonssikkerhet, henholdsvis mønsteret og forholdsmessigheten i dokumentasjonen. Det første poenget, dokumentasjonsmønsteret, fremgår bedre i ISO 27001:2013 enn av forskriften. I forskriften kreves at ulike tiltak skal dokumenteres, men

[117] Ot.prp. nr 92 (1998-1999) s. 116

[118] NOU 1997:19 s. 201

[119] Ot.prp. nr 92 (1998-1999) s. 117

[120] Johansen (2001) s. 344

[121] Tranvik (2009) s. 23

[122] Johansen (2001) s. 357

standarden går lenger. Den foreslår og forklarer dokumentasjonens innhold, struktur og formål. Hvis man systematiserer kravene til dokumentasjon i standarden ser man at dokumentasjonen følger et mønster som støtter den systematiske tilnærmingen. Alt arbeid, alle tiltak og virkemidler skal nemlig planlegges, konkretiseres og utføres, og disse delene skal dokumenteres. Mønsteret er med andre ord å dokumentere både planer, prosesser og resultater. For eksempel skal virksomheten dokumentere hvordan de akter å gjennomføre risikovurderinger (en beskrivelse av metode), inkludert hvem som skal gjøre vurderingene og når (en beskrivelse eller plan for prosessen), og til slutt skal resultatene fra gjennomført plan dokumenteres. (Senere skal det også dokumenteres hva resultatene ble brukt til.) Slik kunnskap er av praktisk verdi når forskrift skal etterleves. Vedlegg 1 viser hvilke dokumenter som kreves for etterlevelse av standarden. Mange av disse dokumentene kreves som nevnt også i forskriften. Vedlegget viser også noen dokumenter som bare kreves i forskriften.

Det andre poenget er forholdsmessighet. Siden dokumentasjon både skal skrives, brukes og vedlikeholdes, bør den være kortfattet.[123] Den bør være konkret og vise forankringen av sikkerhetsorganisasjonen i virksomheten.[124] Sett opp mot standardens prinsipp om kontinuerlig forbedring kan en ”normal” virksomhet med begrensede ressurser starte med svært kortfattet dokumentasjon hvis den er laget i tråd med poenget over og blir fulgt opp i praksis. Motsvarende kan dokumentasjonsplikten etter forholdene bli omfattende. Dokumentasjon skal være i samsvar med det behov virksomheten vurderer som tilstrekkelig. Det er neppe krav om å dokumentere forhold som ikke er relevante i en virksomhet, selv om regelverket bruker ”skal” i bestemmelsen, jamfør forskriften § 2-1 andre ledd. Bestemmelsen gjelder tiltak men etter tolkning må den omfatte tiltakenes dokumentasjon. Det kan være lurt å kommentere hvorfor utelatt dokumentasjon vurderes som ikke relevant.

Tranvik undersøkte regeletterlevelse i kommuner og påpekte en ”etterlevelsesillusjon” ved at sikkerhetsarbeidet kunne være dokumentert, samtidig som at praksis sviktet.[125] Typisk er da overordnet dokumentasjon på plass, slik som policy og prosessbeskrivelser av risikovurderinger, men aktivitetsbasert dokumentasjon mangler, fordi risikovurderinger, revisjoner og

[123] Difi rapport (2012) s. 51

[124] Tranvik (2014)

[125] Tranvik (2009) s. 29

ledelsesgjennomganger ikke blir utført. Bevisst eller ubevisst kan dette være et forsøk på å unngå sterk kritikk, eller å pulverisere ansvaret? Den overordnede dokumentasjon skrevet viser jo tilsynelatende at ansvaret for manglende oppfølging ligger hos andre. Tranvik poengterer at Datatilsynet må kontrollere at dokumentasjonen er styrende for organisering og gjennomføring av sikkerhetsarbeidet, ikke at rettslig logikk styrer dokumentproduksjonen. [126]
Det er det samme som revisor gjør i forbindelse med sertifisering. Ikke bare sjekkes det at aktivitetsbasert dokumentasjon finnes, men at den systematiske tilnærmingen som den reflekterer faktisk er forankret og gjennomført der den skal i virksomheten. Hvis aktivitetsbasert dokumentasjon mangler kan det tilsi at tiltak som revisjon og ledelsesgjennomgang også mangler, og det vil være en systemsvikt som avslører manglende planlegging og ledelsesengasjement i sikkerhetsarbeidet.

4.3 Ledelsens ansvar omfatter grunnlaget for risikovurderinger

Sikring av personopplysninger innebærer å treffe nødvendige tiltak i et omfang etter behov, slik at risikoen for krenkelser av personvernet blir mindre og dermed akseptabel. Tiltakene kan være av mange typer, men gjentatte vurderinger av farene kommer man ikke utenom. I henhold til forarbeidene er behandlingens formål og personopplysningenes omfang og art momenter i risikovurderingene, det vil si at disse skal vurderes opp mot truslene mot informasjonssikkerheten. Vurderingens tema er om risikoen for krenkelser av personvernet som truslene utgjør er større enn risikoen som virksomheten er villig, etter saklig men egen vurdering, til å akseptere. Hva som er akseptabelt skal etter forskriften § 2-4 første jamfør tredje ledd være fastlagt på forhånd. Basert på risikoanalysen må behandlingsansvarlige sette mål og treffe tiltak for å etablere tilfredsstillende informasjonssikkerhet, der analysen har avdekket at risikoen er større enn det som kan aksepteres. Forarbeidene utdyper og gir eksempler på tiltak.[127] Som nevnt før har Datatilsynet anledning til å overprøve virksomhetens risikovurdering, eventuelt stille vilkår om særskilte tiltak.

Risikovurderinger er forutsatt i personopplysningsloven § 13 og eksplisitt krevet i personopplysningsforskriften § 2-4. Dette er en kjernebestemmelse. De andre tiltakene handler i prin-

[126] Tranvik (2009) s. 91 - 95

[127] Ot.prp. nr 92 (1998-1999) s. 116

sipp om å legge grunnen for gjennomføring av risikovurderinger, og oppfølging av resultatene fra risikovurderingene. De ulike leddene i § 2-4 er i samsvar med dette.

Personopplysningsforskriftens kapitel 2 stiller mange krav og tiltak som må tilpasses forholdsmessig for å gi tilfredsstillende sikkerhet. Til tross for ordlydens bruk av ordet ”skal” er det underforstått at tiltak skal baseres på risikovurderinger og forholdsmessighet.[128] I odelstingsproposisjonen heter det: ”det er ikke mulig å på forhånd oppstille uttømmende krav til hvor høy sikkerheten skal være for ulike typer behandlinger.”[129] Departementet skriver i sin kommentar til personopplysningsforskriften:

”Avgrensningene er viktig for å unngå at det etableres for omfattende sikkerhetstiltak. I vurderingen av om sikkerhetstiltak er nødvendig, er opplysningenes art og den fare for tap av liv og helse, økonomisk tap, eller tap av anseelse og personlig integritet behandlingen kan medføre, avgjørende.”[130]

At det skal fastlegges kriterier for hva som er akseptabel risiko er underforstått i forskriften § 2-1 andre ledd og sagt eksplisitt i § 2-4. Der står det at ”virksomheten” må fastlegge kriteriene, men denne paragrafen må ses i sammenheng med § 2-3 som legger ansvaret for sikring på den daglige ledelsen. § 2-3 og § 2-4 utgjør sammen med personopplysningsloven § 13 et pålegg for virksomheter om å etablere et system for informasjonssikkerhetsarbeid som er risiko- og ledelsesstyrt.[131] Tranvik påpeker som nevnt at den øverste ledelsens involvering, eller i det minste støtte, er avgjørende for sikkerhetsarbeidet.[132]

Sett i sammenheng viser §§ 2-4 og 2-3 at risikovurderinger er ledelsens ansvar og at de skal bygge på virksomhetens sikkerhetsmål og sikkerhetsstrategi. Departementet sier sikkerhetsstrategien skal inneholde valg og prioriteringer i sikkerhetsarbeidet.[133] I den offentlige utred-

[128] Personopplysningsforskriften § 2-4

[129] Ot.prp.nr.92 (1998-1999) s. 115

[130] Johansen (2001) s. 347

[131] Tranvik (2009) s. 19

[132] Tranvik (2009) s. 23

[133] Johansen (2001) s. 348

ningen sier utvalget at vurderingene bør inneholde konkret angivelse av mål for sikringsarbeidet i forhold til de enkelte risikotyper.[134]

Etter ordlyden i andre ledd i § 2-3 skal ”sikkerhetsmål” inneholde beskrivelser av formålet med behandlingen, og overordnede føringer for bruken av informasjonsteknologi. At behandlingsansvarlige må klargjøre formålet med behandlingen er forutsatt i personopplysningsloven § 11 bokstav b. Klargjort formål er også en forutsetning for ” frivillig, uttrykkelig og informert” samtykke fra den registrerte.[135]

Departementet sier altså at sikkerhetsmål omfatter beslutninger om hva informasjonsteknologi skal brukes til i virksomheten, og hvordan. For eksempel valg av hvilke personopplysninger som skal behandles med IT, eller om hvordan personopplysninger skal sikres eller om privat bruk av informasjonssystemene.[136] Som andre eksempler gis "fordeling av arbeidsoppgaver for drift og informasjonssikkerhet mellom ledelse, drifts- og sikkerhetspersonell og den enkelte bruker, eventuelt krav til at konfidensielle personopplysninger behandles i informasjonssystem uten tilkobling til eksterne datanett, og bruk av leverandører for å få utført sikkerhetsoppgaver."[137] Tranvik trekker også frem valg og prioriteringer, og sier at det skal dokumenteres hvordan resultatene i strategien skal nås.[138] Schartum skriver at strategien beskriver hvordan alle mål oppnås, men i et omfang tilpasset risikoen. Der anbefales det også at det lages en ”sikkerhetsplan” som viser hvilke konkrete tiltak som skal gjøres.[139] Dokumentet skal være basert på risikovurderinger og svarer kanskje til standardens ”anvendelseserklæring”, SOA.[140] Sentral er at anvendelseserklæringen eller sikkerhetsplanen skal godkjennes av ledelsen, som et uttrykk for ledelsens risikoaksept.

Schartum sier om sikkerhetsmål at ”poenget er å identifisere gjeldende retningslinjer og intern policy som er relevant for bedømmelse av informasjonssikkerheten”.[141] Schartum skriver

---

[134] NOU 1997:19 s. 200

[135] Personopplysningsloven § § 8 og 9, jamfør § 2 nummer 7

[136] Johansen (2005) s. 348

[137] Johansen (2001) s. 348

[138] Tranvik s. 23 fotnote 47

[139] Jansen (2005) s. 121

[140] ISO 27001 s. 4

[141] Jansen (2005) s. 121

samme sted at målformuleringene bør være målbare og formuleres for å sikre henholdsvis konfidensialitet, integritet og tilgjengelighet, eventuelt via underkategorier knyttet til disse. Sikkerhetsmålene er ideelle og de skal konkretiseres i en sikkerhetsstrategi.

Etter vanlig ordforståelse vil ”sikkerhetsmål” kunne omfatte noe mer eller noe annet enn bare overordnede formål og føringer. Standarden gir mer bakgrunn for slik tolkning av paragrafen. Den sier at sikkerhetsmål skal etableres på flere nivåer, ikke bare overordnet. Målene kan dokumenteres i policy for informasjonssikkerhet eller i underordnede dokumenter. Sikkerhetsmål i policy for informasjonssikkerhet kan med fordel være overordnede og generelle, slik at policy ikke må justeres for ofte, jamfør den skal forankres i ledelsen og være kjent i virksomheten.[142]

Også standarden krever at det grunnleggende strategiarbeidet dokumenteres, blant annet i form av en policy som danner grunnlag for utarbeidelse av konkrete planer.[143] Verdt å merke seg er at ISO 27001 kanskje ikke trekker frem "strategidokumenter" i samme grad som departementet og norsk litteratur? De valg og prioriteringer som er nevnt over vil i ISO- rammeverket finne sin plass i policy for informasjonssikkerhet. Men dette utelukker ikke supplerende strategidokumenter. I forskriften § 2-4 første ledd første punktum stilles det krav om å dokumentere hva slags personopplysninger som behandles i virksomheten. Dette må virksomheten ha oversikt over for å kunne fastlegge kriterier for akseptabel risiko, første ledd andre punktum. Departementet sier som forklaring til paragrafen at oversikten benyttes som del av grunnlaget for risikovurderingen. Grunnlaget må angi "hvilke opplysninger det er nødvendig å sikre konfidensialitet, tilgjengelighet eller integritet for." [144] Men hvilke systemer behandler personopplysninger? I noen virksomheter kan det være så mange at det krever systematisk dokumentering for å holde oversikten, med en ITIL tjenestekatalog eller tilsvarende.[145] Har man etablert en slik oversikt er det som regel enkelt for virksomheten å se hvilke av tjenestene i katalogen som behandler personopplysninger og/eller som må inngå i systematisk sikkerhetsarbeid. Det kan tenkes tjenester (systemer) i virksomheten som ikke involverer personopplysninger. Hvis de kan utnyttes for å gi tilgang til personopplysninger så kan de etter for-

[142] ISO 27001 s. 5

[143] ISO 27001 s. 2

[144] Johansen (2001) s. 349

[145] Office of Government Commerce (2007) s. 60 Service Design

holdene likevel bli omfattet, jamfør andre ledd i punkt 4 i standarden utfyller kravet om å dokumentere hvilke opplysninger som skal sikres.[146] Poenget er å fastlegge sikkerhetsarbeidets omfang og anvendelsesområde i den gitte virksomheten. Dette skal dokumenteres i overordnede dokumenter som skal forankres i og godkjennes av ledelsen.[147]

Den behandlingsansvarlige skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.[148] Risikokriterier kan utformes på flere måter. Enkle eksempler er utsagn av type ”vår virksomhet aksepterer ingen brudd på sensitive personopplysningers konfidensialitet”. For å kunne brukes i risikovurderingene må utsagnene knyttes til konkrete opplysninger og/eller systemene som behandler dem. Ideelt sett bør risikokriteriene fastlegges før risikovurderinger gjøres. Dette for å unngå uheldig tilpasning av risikoaksepten etter økonomi, bekvemmelighet eller lignende.

Standarden utfyller forskriften ved å kreve at selve prosessen for risikovurderinger også planlegges og dokumenteres.[149] Det er ikke et eksplisitt krav i forhold til ”tilfredsstillende” informasjonssikkerhet, men det kan inngå i helhetsvurderingen. Det kreves for sertifisering, men siden standarden skal tilpasses den enkelte virksomhet gjelder et prinsipp om forholdsmessighet også i standarden.[150] I forbindelse med revisjon av etterlevelse av ISO 27001 oppsummeres ledelsens plikter som å formulere policy for IT og informasjonssikkerhet, sikkerhetsmål og sikkerhetsplaner i virksomhetens kontekst. Roller og ansvar for informasjonssikkerhet skal etableres, nødvendige ressurser skal settes av, risikokriterier fastsettes, og restrisikoen etter at tiltak er truffet skal eksplisitt aksepteres. Ledelsen må også gå gjennom resultatene fra interne revisjoner årlig. Til slutt må de sørge for tilstrekkelig kompetanse og oppmerksomhet i virksomheten rundt informasjonssikkerhetsarbeidet.[151] Det meste av dette beskrives også i forskriften.

---

[146] ISO 27001 s. 1

[147] Ibid. s. 2

[148] Personopplysningsforskriften § 2-4

[149] ISO 27001 s. 3

[150] ISO 27001 s.v

[151] PECB (2014) s. 25 dag 3

Viktige i denne sammenheng er at risikoappetitten må være et lederskjønn. Om ikke ledelsen selv utformer kriteriene for akseptabel risiko så må ledelsen godkjenne dem. Og skjønnet må være forsvarlig, jamfør da særlig forholdsmessighetsprinsippet. Overdreven risikoappetitt blir et moment som klart taler mot at sikkerheten er tilfredsstillende.

4.4 Gjennomføring av risikovurderinger

Risikovurderinger er i verste fall bare kvalifiserte gjetninger.[152] Samtidig er risikovurderinger det viktigste redskapet i sikringsarbeidet, i det de forsøker å besvare spørsmålet ”hva trenger vi å forbedre?”[153] Kvalifiserte gjetninger, eller enda verre, manglende risikovurderinger, vil ikke være godt nok rettslig sett, i forhold til "planlagt og systematisk."

Risikovurderinger skal gjennomføres for de systemene som behandler personopplysninger, se over, og de skal gjøres på nytt ved systemendringer av betydning for sikkerheten. Dersom slike systemendringer er hyppige bør det vurderes å knytte risikovurderingene til, for eksempel en ITIL endringsprosess.[154] Men risikovurderinger skal uansett følges opp planmessig, om enn bare for å avdekke at det ikke er behov for ny vurdering.

Selve risikovurderingen kreves i § 2-4 andre ledd. Departementet forklarer at risikovurderingene skal gjøres før behandlingen settes i gang. Både Datatilsynet og Personvernnemda følger opp dette synet, se klagesak PVN-2007-04, der manglende risikovurdering beskrives som en så vesentlig mangel at behandling ikke kan settes i gang.[155] Risiko har to dimensjoner: skadevirkning og sårbarhet.[156] Skadevirkning beskriver konsekvensene av sikkerhetsbruddet, mens sårbarhet beskriver sannsynligheten for sikkerhetsbruddet. Formålet med risikovurderingen å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Departementet trekker frem essensen i dette når de sier at resultatet skal benyttes som del av grunnlaget for valg av konkrete sikkerhetstiltak.[157] Med andre ord, dersom kombinasjonen av skadevirkning og sannsynlighet er stor, over en viss grense, må tiltak treffes, sik at skadevirkning og/eller

[152] Tranvik (2009) s. 24

[153] Tranvik (2009) s. 81

[154] Office of Government Commerce (2007) s. 42-65 Service Transition

[155] Blume (2009) s. 497

[156] Håndbok i datasikkerhet (2006) s. 163-164

[157] Johansen (2001) s. 349

sannsynlighet for sikkerhetsbrudd reduseres. Dette er underforstått i forskriften § 2-4 tredje ledd. Ofte uttrykkes kombinasjonen av skadevirkning og sannsynlighet som et produkt av de to, etter at de hver er gitt en størrelse på en angitt skala.

Departementet i sin kommentar kommer videre inn på tre gode poenger som alle handler om forholdsmessighet. For det første at målet er å redusere risiko, ikke nødvendigvis eliminere den. For det andre at Datatilsynet kan overprøve beslutningene, jamfør forskriften § 2-2. Og for det tredje at sikkerhetsarbeidet ikke skal være mer omfattende enn strengt tatt nødvendig.[158] Derfor brukes ordet ”vurdering” fremfor ”analyse”. Departementet sier at risikovurderingen kan utføres med utgangspunkt i norsk standard NS-5814, Krav til risikoanalyser.[159] Datatilsynet sier det samme, men anbefaler ”grovanalyser”, kvalitative og forenklede vurderinger av sannsynlighet og konsekvens. [160] En tilgjengelig fremstilling av slike ”grovanalyser” er gitt av Normann og Tranvik, opprinnelig for bruk i kommuner. [161] Uninett sitt sekretariat for informasjonssikkerhet har utviklet en variant for bruk i universitets- og høgskolesektoren.

For å integrere sikkerhetsarbeidet i virksomheten kan det være et poeng å bruke samme form for risikovurdering som brukes på andre områder i virksomheten. Nye ISO-standarder på ulike virksomhetsområder fremmer av den grunn samme risikotilnærming, se nå norsk standard NS-ISO 31000:2009. Av praktiske grunner kan det være lurt å starte med enklest mulig form for risikovurdering. Dersom analysen oppfattes som vanskelig eller kostbar kan løpende oppgaver ta all oppmerksomhet, særlig der viljen til byråkratisk og langsiktig arbeid er liten.[162] Da blir ikke risikovurderinger prioritert. Det avgjørende må derfor være at tilnærmingen utvikles og blir forholdsmessig og hensiktsmessig over tid. Men det er ikke gitt at Datatilsynet vil akseptere en slik tilnærming i en konkret sak.

Standarden utfyller og går lenger enn forskriften i detaljeringsnivå om risikovurderinger. Den krever at en metodikk for gjennomføring av risikovurderinger utvikles, dokumenteres og bru-

[158] Johansen (2000) s. 347 og 349

[159] Johansen (2001) s. 349

[160] Tranvik (2009) s. 24 fotnote 48

[161] Norman (2012) s. 53

[162] Tranvik (2009) s. 82-85

kes slik at risikovurderingene blir regelmessige, konsistente, og sammenlignbare.[163] I alle tilfeller må resultatene fra risikovurderingene dokumenteres slik at de kan følges opp.

"Grovanalyse" som beskrevet over kan kanskje redusere behovet for å etablere akseptkriterier på forhånd, så lenge man unngår "strategisk" tilpasning av henholdsvis sannsynlighet og konsekvens.

Metoden er i korte trekk slik:

- Sannsynlighet for at en gitt trussel i forhold til henholdsvis konfidensialitet, integritet og tilgjengelighet inntreffer, plasseres på en skala fra si 1 til 4.
- Konsekvensen dersom samme trussel faktisk skulle inntreffe plasseres tilsvarende.
- En "risikofaktor" er da produktet av de to. Dersom beregnet risikofaktor er i:
- intervallet 1-3 (grønn sone) så bør det være unødvendig med flere sikkerhetstiltak.
- intervallet 4- 6 (gul sone) bør det vurderes nærmere om flere sikkerhetstiltak er nødvendig
- intervallet 8 – 16 (rød sone) er det nødvendig med sikkerhetstiltak som bringer risiko ned i grønn, eller minst gul sone.

Slik "grovvurdering" er i utgangspunktet enkel og intuitiv. Med omfattende behandling av personopplysninger kan risikovurderingene likevel bli omfattende. Utfordringen ligger også i å finne de reelle truslene – samt vurdere dem mest mulig korrekt. I dette kan standarden spille en pedagogisk rolle. Ved "reverse engineering" av tiltakene i ISO 27002 vil man finne et stort antall potensielle trusler som virksomheten kan ha behov for å treffe tiltak mot. ISO 27002 utdyper tiltakene i ISO 27001 annex A, og andre standarder i ISO 27000-serien utdyper disse ytterligere. Men disse tiltakene og den oversikten de gir over truslene kan ikke bli uttømmende. Derfor blir det et sentralt poeng at selv om øverste ledelse må avgjøre risikoaksepten, må "de rette folkene" i virksomheten bistå med å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. De rette folkene er typisk risikoeierne (de ansvarlige ledere) og de sentrale medarbeiderne i behandlingen (eksperter og superbrukere, IKT-medarbeidere). Disse har ikke nødvendigvis kunnskaper om metoder for risikovurderinger, og en grovanalyse kan da

[163] ISO 27001 s. 3-4

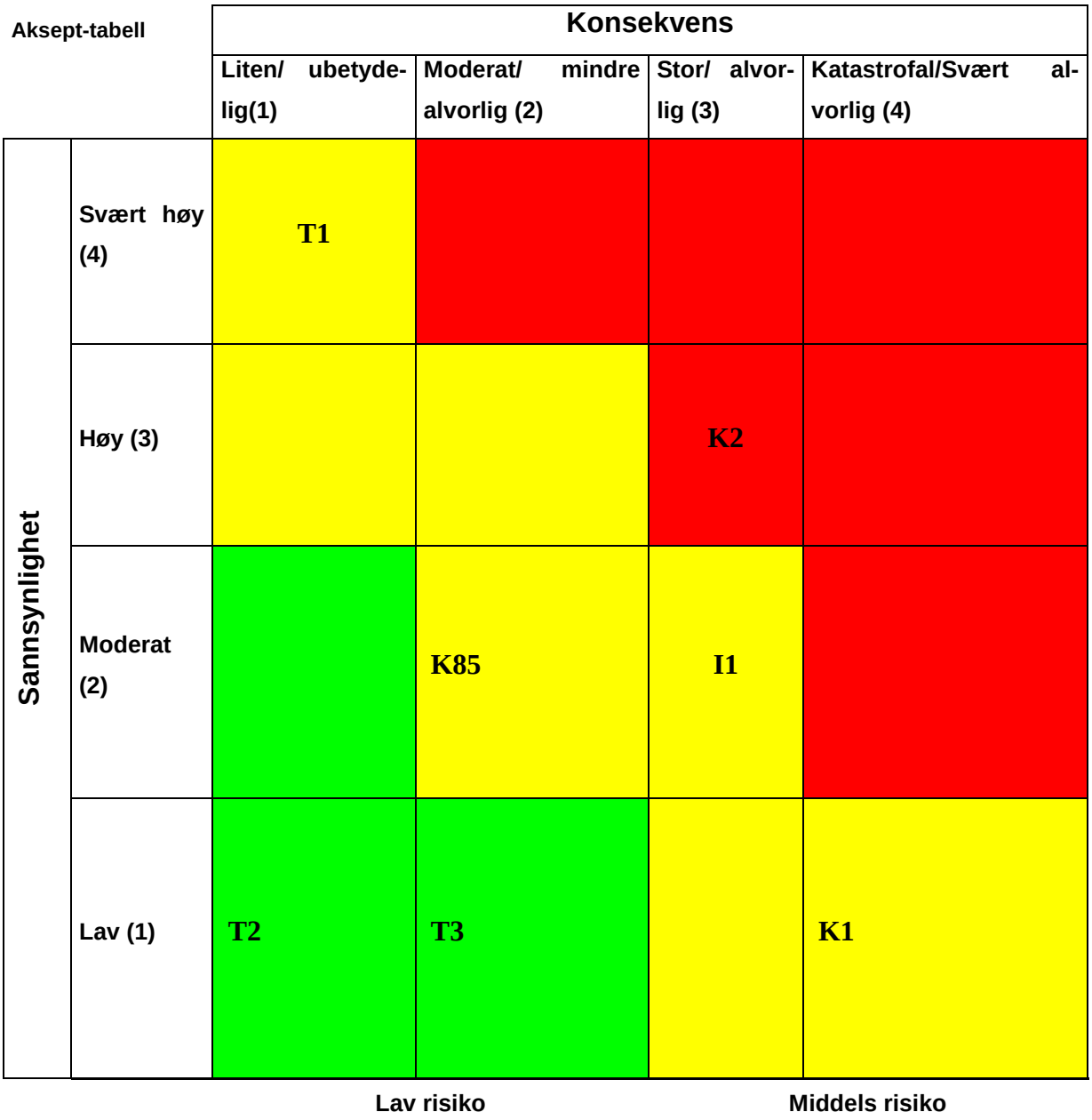
være hensiktsmessig. Med den erfaring som følger med systematisk arbeid over tid bør resultatene kunne utvikle seg tilfredsstillende.

Figur 1 viser eksempelvis at en gitt behandling av personopplysninger, referanse K2, innebærer en risiko for brudd på konfidensialitet fordi det er sannsynlig at utskrifter blir liggende på skriveren i et fellesrom etter utskrift. Samtidig kan konsekvensen av dette bli stor, si fordi personopplysningene som skrives ut kan være av sensitiv karakter. I eksempelet blir risikofaktoren 9, det vil si rød sone. Her kan tiltak redusere sannsynligheten for at utskrifter kommer uvedkommende i hende, for eksempel innføring av et system der utskriften ikke kommer ut av skriveren før mottageren står ved siden av skriveren og autentiserer seg (her kalt "follow me").

Figur 1: Illustrasjon av en risikovurdering:

Ref.	Risiko element - -Hendelse og årsak	Mang-ler/Svakh eter	Be-skyttel-se	Kontroller	Tiltak	Sansyn-lighet S1-S4	Konse-kvens K1- K4	Ri-siko fak-tor
	(S)PO = (Sensitive) PersonOpplysninger							
	Konfidensiali-tet							
K1	tidligere rettigheter fjernes ikke ved rolleendring		Liten turnover, 2 personer må autori-sere		Verifisere rutine for å oppdatere brukerinfo	1	4	4
K2	dårlige rutiner for utskrift, for eksem-pel: ligger lønnslip-per i printrommet	Manglende rutiner og holdninger. Har ikke follow me. Åpent rom			Ansvarlig-gjøring av brukere. Innføre follow me	3	3	9
	Integritet							
I1	inntastingsfeil skjer oftere for engangsut-betalinger		Har kon-trollrutine	Systemet har innebygde tester av leve-randørnummer, beløp	Gjennomfør tiltak for kvalitetssik-ring	2	3	6
	Tilgjengelighet							
T1	System ustabilt - tregt system ved frist for hovedlønn				Kapasiteten bør bedres	4	1	4
T2	Applikasjonen feiler pga menneskelig svikt					1	1	1
T3	Utilsiktet sletting av informasjon - men-neskelig svikt				Sjekk back-up-metodikk	1	2	2

Figur 2: Resultatet fra risikovurderingene i en aksept-tabell:



I figur 2 er "risikofaktorene", kombinasjonen av sannsynlighet og sårbarhet, plottet inn i en aksept-tabell. Aksepttabellen kan deles i tre områder, igjen illustrert med fargene grønn, gul og rød. Trusler med relativt lav risikofaktor havner i grønt sone (nede til venstre), en indikasjon på at det ikke er behov for sikkerhetstiltak. Trusler med høy risikofaktor havner i rød sone (oppe til høyre), som indikerer at risikoen er uakseptabel og at sikkerhetstiltak er nødvendig. Gul sone, området i midten, indikerer at tiltak må vurderes nærmere.

4.5 Oppfølging av risikovurderinger involverer også ledelsen

Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko og eventuelt også mot akseptkriterier fastlagt av Datatilsynet.[164] Resultatet av risikovurderingen skal dokumenteres for oppfølging og revisjon, med mer.

Oppfølgingen kan resultere i at tiltak må treffes for å redusere risiko. Tiltakene kan være av ulike typer, ikke bare IKT-tekniske, men organisatoriske, pedagogiske, fysiske eller kontraktsmessige, osv.

ISO 27002 sier at risiko håndteres ved å akseptere, forsikre mot, redusere eller unngå den.[165] Virksomheten kan etter ISO 27001 benytte alle tiltak de ønsker, men tiltakene i annex A i standarden skal vurderes, og virksomheten må begrunne hvorfor tiltak listet her eventuelt ikke brukes. Også forskriften lister noen konkrete tiltak som skal gjøres, men forskriftens § 2-1 til § 2- 16 er ikke uttømmende, og som tidligere diskutert er de, helt unntaksvis, fravikelige dersom dette opplagt kan begrunnes.

Forskriften sier at resultatene av risikovurderingene skal dokumenteres. Standarden utfyller dette ved å kreve at begrunnelser og status for implementering også dokumenteres. Dette dokumentet kalles SOA, statement of applicability, en erklæring om anvendelse av tiltak (anvendelseserklæring). Det skal også lages et dokument med planer for gjennomføring av tiltakene. Standarden sier videre at planene og restrisikoen etter at tiltak er gjennomført skal kvitteres ut av ledelsen og risikoeierne. Kvitteringen kan gjøres ved signering. [166]

Avsnittene over forklarer litt om den direkte oppfølgingen av gjennomførte risikovurderinger. Men personopplysningsforskriften § 2-3 fjerde ledd stiller også krav om at informasjonssystemet som brukes i behandling av personopplysninger jevnlig skal gjennomgås. Det skal vurderes om systemet er hensiktsmessig og om sikkerhetsstrategien gir tilfredsstillende sikkerhet. ”Tilfredsstillende” er i også denne sammenheng i forhold til behandlingsansvarliges subjektive men saklige skjønn etter en helhetsvurdering.

---

[164] Personopplysningsforskriften § 24 tredje ledd jamfør første ledd og § 2-2

[165] ISO 27002s. 24

[166] ISO 27001 s. 4

Forskriften legger opp til regelmessighet i arbeidet, blant annet ved å stille krav om sikkerhetsrevisjon (§ 2-5) og jevnlig ledelsesgjennomgang (§ 2-3 fjerde ledd). Departementet anbefaler at disse skjer årlig. Departementet trekker frem at poenget med revisjon er å etterprøve sikkerhetsarbeidet, det vil si sjekke at det utføres og at det fungerer etter sin hensikt. Kontinuerlig forbedring trekkes også frem som et ønsket resultat av sikkerhetsrevisjoner. Departementet mener også at revisjonsarbeidet kan følge samme framgangsmåter som benyttes i HMS-arbeidet (det vil si internkontrollforskriften).[167] Naturlig nok er revisjon også sentralt i standarden, da sertifisering innebærer å verifisere etterlevelse av rammeverket i virksomheten. Kontinuerlig forbedring er grunnleggende også i ISO 27001. I sertifiseringskurs for 27001-revisorer poengterer kursholder Anders Carlstedt at revisor ikke er dommer, politi, detektiv eller journalist.[168] Som for Datatilsynet er revisors samarbeid med virksomheten vesentlig. Og når revisor skal sammenfatte resultatene gjøres dette etter en tilnærming forvekslende lik juridisk metode, om enn med standarden som viktigste rettskilde og rettslig regelverk som viktig supplement. Momenter som bevisenes relevans og pålitelighet trekkes frem, avveininger skal gjøres, og til og med prinsippet om rimelig tvil (i forhold til konformitet eller ikke) legges til grunn.[169] Slik sett kan en jurist med IT-sikkerhetskompetanse bli en god informasjonssikkerhetsrevisor. Motsvarende og naturlig nok kan en jurist, eventuelt med bistand fra eksperter innen IT-sikkerhet, treffe gode rettslige beslutninger om informasjonssikkerhetsspørsmål.

Standarden utfyller også helt konkret hva en ledelsesgjennomgang skal inneholde og hva som er formålet med den.[170] Tilsvarende sier siste ledd i personopplysningsforskriften § 2-3 at systemgjennomgangen skal dokumenteres, og danne grunnlag for justeringer i sikkerhetsmål og strategi.

4.6 Avsluttende kommentarer

Som vi har sett kan sikringsoppgaven bli omfattende. Særlig er risikovurderinger utfordrende, ikke minst for virksomheter med omfattende behandling av personopplysninger. En rettesnor er at arbeidet ikke skal gjøres mer omfattende enn nødvendig. Forholdsmessighet blir da avgjørende. Merk at selv om lovens formål er å unngå krenkelser av personvernet, finnes det

[167] Johansen (2001) s. 349 - 350

[168] Carlstedt (2014)

[169] PECB (2014) s. 87-90 day 3

[170] ISO 27001 s. 8

også andre verdier som kan nyte godt at en planlagt og strukturert tilnærming til informasjonssikkerhet. For eksempel kan det ha en positiv effekt på arbeidsmiljøet og på medarbeidernes kompetanseutvikling. Det kan også redusere faren for økonomisk tap, eller tap av liv og helse. Personopplysningsforskriften § 2-1 angir også dette siste som formål, til tross for at lovens formål er knyttet opp mot personvern.

5 Når er sikringen tilfredsstillende?

5.1 Innledning

Utgangspunktet er personopplysningsloven § 13 andre ledd som krever at tiltak og behandlingssystemer skal være dokumenterte for å oppnå tilfredsstillende informasjonssikkerhet. Men dette må sees i sammenheng med paragrafens første ledd om planlagte og systematiske tiltak. Betingelsen etter personopplysningsloven for ”tilfredsstillende” informasjonssikkerhet blir da at virksomheten har planlagte, systematiske og dokumenterte tiltak og systemer slik at virksomheten etterlever kravene om et akseptabelt risikonivå. Etter NOU 1997:19 ville utvalget pålegge virksomheten en plikt til å basere arbeidet på anerkjente standarder, men dette ble ikke lovfestet.[171] Departementet sa:

"Sikkerhetstiltak må etableres etter en konkret vurdering av de personopplysninger som behandles i forhold til de trusler mot informasjonssikkerheten som er til stede. Denne vurderingen skal utføres av den behandlingsansvarlige med utgangspunkt i et styringssystem for sikkerhet. Det er kravene til dette styringssystemet som beskrives i dette kapittelet i forskriften."[172]

Departementet mener med andre ord at informasjonssikkerheten er tilfredsstillende når kravene i forskriften er oppfylt, og arbeidet er basert på anerkjente standarder. Bruken av standarder har også et harmoniseringsperspektiv, sier departementet, ikke minst i forhold til EU/EØS og personverndirektivet 95/46/EF. Slik kan man oppnå "gjenkjennbart sikkerhetsnivå" og "legge til rette for elektronisk samhandling mellom forskjellige sektorer." Forgjengeren til IS0 27001 trekkes frem som eksempel til etterfølgelse, og de presiserer at dette sikkerhetssystemet kan benyttes i alle sektorer.[173]

Departementet skriver dog at "tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av "planlagte og systematiske tiltak". Videre at "begrepet innebærer at kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll, og informasjonssikkerhet skal legges til

[171] NOU 1997:19 s. 133

[172] Johansen (2001) s. 345

[173] Ibid s. 346

grunn ved sikkerhetsarbeidet."[174] Risikovurderinger står her sentralt, for de kan avsløre avvik mellom akseptabel risiko og vurdert (reell) risiko. Men helheten av sikkerhetsarbeidet (planene, systematikken, dokumentasjonen) må vurderes nærmere opp mot forskriftens bestemmelser og lovens rammer for å avgjøre om informasjonssikkerheten totalt sett er tilfredsstillende. Dersom man spør departementet svarer de nok i tråd med dette at arbeidet skal følge systematikken i ISO 27001 eller lignende rammeverk.

Spørsmålet om informasjonssikkerheten er tilfredsstillende kan oppstå av flere grunner. Virksomheten må kontrollere regeletterlevelse ved egenkontroll. Datatilsynet kan føre tilsyn med regeletterlevelsen. Spørsmålet kan også være aktuelt i forbindelse med et eventuelt pådratt erstatningsansvar. Vurderingen kan gå på systemet som et hele, eventuelt kan spesielle deler av systemet være av særlig interesse. En slik undersøkelse kan ha likhetstrekk med en ekstern revisjon i forbindelse med sertifisering, selv om poenget med slik revisjon er å kontrollere etterlevelse i henhold til standarden, og ikke primært (men dog inkludert) loven. I undersøkelsen av spørsmålet om informasjonssikkerheten er ”tilfredsstillende” kan det også være nyttig å trekke inn de delene av etterlevelsen som er spesielt vanskelig, for å vurdere hvordan virksomheten har løst disse utfordringene.

Etter ordlyd i § 13 pålegges behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet. Uttrykket ”å sørge for” tilsier en aktivitetsplikt, men omfanget av tiltakene trenger tydeligvis bare å være slik at sikkerheten blir ”tilfredsstillende”. Tiltakene skal med andre ord sikre opplysningenes konfidensialitet, integritet og tilgjengelighet - til en viss grad.

Selv i et idealsamfunn der det er sosial balanse mellom mennesker vil menneskets natur åpne for at sikkerhetsbrudd vil forekomme. Sosialt sett er full sikkerhet (her: ingen krenkelser av personvernet) neppe oppnåelig. Men årsaken til at (bare) en viss grad av sikkerhet aksepteres som tilfredsstillende er også økonomisk. Risiko skal reduseres, ikke elimineres, uten at det overinvesteres i sikkerhet.[175] Dersom opplysninger behandles helt uten tanke på sikkerhetstiltak kan kostnaden (krenkelsen av personvernet) bli stor. Men sikringstiltak koster penger, derfor blir kostnadene store også ved bruk av (mange eller dyre) tiltak. Dette foreslår at det

[174] Ibid s. 344

[175] Tranvik (2009) s. 24

finnes et ønskelig "balansepunkt" mellom kostnader og sikkerhet.[176] Denne balansen kan være vanskelig å finne. Tranvik påpeker at å behandle minst mulig personopplysninger er den beste løsningen for å unngå krenkelser av personvernet.[177] Denne løsningen omfavnes kanskje for sjelden, for samfunnets behandling av personopplysninger er omfattende og økende.

5.2 Forholdsmessighet er en del av vurderingen av tilfredsstillende sikkerhet

Forarbeidene har en del kommentarer til forholdsmessigheten i sikringsarbeidet. Forholdsmessighet betyr blant annet at detaljnivået må tilpasses formålet. Departementet sier som forklaring til personopplysningsforskriften § 2-1 at "sikkerhetstiltak implementeres i forhold til sannsynlighet for og konsekvens av sikkerhetsbrudd." Det påpekes klart at for omfattende sikkerhetstiltak skal unngås. Men det er verdt å merke seg at tilgjengeliggjøring av personopplysninger på internett (i motsetning til tilgjengeliggjøring kun internt i virksomheten) øker både sannsynligheten og konsekvensen av sikkerhetsbrudd, og dermed kravene til sikring. Dette ble fremhevet i personvernnemdas klagesak 2007-04, der autentisering kun ved brukernavn og passord ikke ble regnet som tilstrekkelig i et internettbasert system. At forholdet her ikke var risikovurdert godt nok på forhånd hjalp ikke på saken.[178] Men vurderingene må også gjøres løpende, jamfør de enhver tid rådende forhold. Ikke minst skal sikringen være tilstrekkelige i forhold til formålene ved behandlingen.[179] I utgangspunktet er behandlingsansvarliges skjønn avgjørende i forhold til hvilke tiltak med videre som gir "tilfredsstillende informasjonssikkerhet". Men et utilstrekkelig skjønn kan føre til krenkelser av personvernet, som igjen kan gi grunnlag for erstatningsansvar.[180] Datatilsynet og personvernnemda har kompetanse til å gjøre sine egne vurderinger av sikkerheten i virksomheter. De kan stille vilkår og gi pålegg om tiltak, se personopplysningsloven §§ 43 og 44, jamfør forskriften § 2-2.[181] Departementet trekker frem det samme.[182] Manglende etterlevelse av pålegg slik at Datatilsynet

[176] Håndbok i datasikkerhet (2005) s. 37

[177] Tranvik (2009) s. 20

[178] Blume (2009) s. 498

[179] NOU 1997:19 s. 199

[180] Personopplysningsloven § 49

[181] Jansen (2005) s. 119

[182] Johansen (2001) s. 349

ikke finner informasjonssikkerheten tilfredsstillende kan lede til overtredelsesgebyr, se personopplysningsloven § 46 jamfør § 13. Datatilsynet kan som nevnt flere ganger overprøve behandlingsansvarliges skjønn. Men departementet påpeker at Datatilsynet i slike tilfeller bør samarbeide med de berørte.[183] Derfor blir både virksomhetens risikovurderinger og Datatilsynets praksis i samspill et grunnlag for å bestemme tiltakene:

"Hvor mange tiltak og hvor strenge hvert tiltak bør være, det vil si hva som anses å være "tilstrekkelig", vil avhenge av forholdet mellom formålet med behandlingen (se over) og risikovurderingen. Datatilsynets praksis i konsesjonssaker og ved kontroll av sikkerhet ellers og spesielt av sikringstiltak etter § 11 vil på sikt angi et forutsigbart sikringsnivå.".[184]

Det er et vesentlig poeng at risikovurderingene i stor grad, men ikke helt, overlates til behandlingsansvarlige:

"Spørsmålet om hva som er tilstrekkelige sikkerhetsnivå må således vurderes konkret av Datatilsynet i en dialog med den behandlingsansvarlige. Tilsynets avgjørelse vil være gjenstand for klage."[185]

I en slik klage kan nok Datatilsynets argumenter veie tung, men NOU 1997:19 presiserer at

"Spørsmålet om domstolsprøving av Datatilsynets og Justisdepartementets avgjørelser etter personregisterloven reguleres av alminnelige sivilprosessuelle regler. I tråd med læren om forvaltningens frie skjønn vil domstolene kun i unntakstilfelle etterprøve tilsynets eller departementets utøvelse av forvaltningsskjønnet, se utvalgets merknader ovenfor under 18.3.8.2.**"**[186]

Hvis behandlingsansvarliges skjønn er saklig og sikringsarbeidet ellers er gjort i tråd med loven så skal det kanskje noe til å overprøve skjønnet. Men Datatilsynet har sagt at dersom

[183] Johansen (2001) s. 347

[184] NOU 1997:19 s. 200

[185] NOU 1997:19 s. 133.

[186] NOU 1997:19 s. 168

risikovurderingen ikke er i samsvar med kravene i personopplysningsforskriftens kapittel 2 eller ikke tilstrekkelig dokumentert, vil dette være "en vesentlig mangel som gjør at løsningen ikke kan brukes." Personvernnemda bekreftet dette synet i nevnte konkrete sak.[187]

Personopplysningsforskriften kapittel 2 stiller en rekke krav som inngår i en totalvurdering av om informasjonssikkerheten er tilfredsstillende eller ikke. Forskriftens pålegg om bruk av virkemidler utfyller lovens krav om en planlagt, systematisk og dokumentert tilnærming.

Det mest sentrale virkemidlet i forskriften er risikovurderinger, men det sentrale prinsippet i risikovurderingen er forholdsmessighet, både i forhold til trusler og skadevirkninger.[188] Dette er en kjernebestemmelse. Prinsippet om forholdsmessighet fremgår også indirekte av lovens bruk av ordet ”tilfredsstillende”.

Forholdsmessighet inngår i en totalvurdering, der også virksomhetens størrelse og ressurser er momenter. Andre momenter er opplysningenes karakter, og truslenes omfang og konsekvenser. Disse momentene henger selvsagt sammen, og tydeliggjøres via risikovurderinger. Personopplysningsloven stiller strengere krav til behandling av sensitive opplysninger og forarbeidene understreker dette.[189] Eksempelvis er kravene til behandling av, si, helseopplysninger høye. Slik behandling er derfor også underlagt særregler som supplerer personopplysningsloven.[190]

Hvis virksomhetens behandling av personopplysninger er beskjeden, hvis farene for, og konsekvensene av et sikkerhetsbrudd og krenkelse av personvernet er små, så kan kravene til tiltakene bli tilsvarende små. Men loven oppstiller en plikt til at denne konklusjonen og dette sikkerhetsnivået er et resultat av planlagte og systematiske tiltak, og at dette fremgår av dokumentasjonen som er laget. I enkleste fall er ikke dette arbeidet veldig omfattende. Men det er en trend å gjøre tjenester og informasjon tilgjengelig over internett. "Information at your fingertips" er svært brukervennlig men gjør varetakelse av integritet, konfidensialitet og tilgjengelighet desto mer utfordrende. Alle ledd i behandlingen (etablering, behandling, endring)

[187] Blume (2009) s. 499

[188] Personopplysningsforskriften § 2-1 andre ledd

[189] NOU 1997:19 s. 199

[190] Helseregisterloven (2001)

må risikovurderes, og nødvendige tiltak treffes. Uten slik helhetlig tilnærming vil det i henhold til Datatilsynets vurderinger foreligge mangler ved sikkerheten.[191]

5.3 Hva er vanskelig og bør sjekkes spesielt?

Vi har sett at risikovurderinger kan være utfordrende men at de også står sentralt i vurderingen av om sikkerheten er tilfredsstillende.

Tranvik omtaler også det at manglende detaljregulering og konkrete holdepunkter for hva som er "godt nok" kan skape hindringer og gjøre det vanskelig å implementere sikkerhetssystemet og etterleve reglene. En del av dette kan skyldes at internkontrolltankegangen øker spenningen mellom rettslig og organisatorisk logikk.[192] I hvilken grad har virksomheten et internkontrollsystem, og i hvilken grad fungerer systemet?

Formaliseringen av organisatoriske rammer stiller større krav til arbeidsdisiplin.[193] Dette kommer til syne i autoritetsutfordringen: IKT-ansatte som typisk har hatt et ansvar for informasjonssikkerhet må i et ledelsesstyrt informasjonssikkerhetsarbeid oppgi noe av sin autonomi. I tillegg må de arbeide tett mot organisasjonen, de må jobbe rutinebasert og planmessig i en evig prosess, endog med regler som er abstrakte og gitt i et vanskelig språk.[194] Har virksomheten organisert sitt arbeid på riktig måte, og er omfanget tilpasset omstendighetene? Og i hvilken grad er regelverket operasjonalisert i egen organisasjon?[195]

Tilsyn fra Datatilsynet eller Riksrevisjonen vekker gjerne ledelsens oppmerksomhet, om enn som regel kortvarig.[196] Det er trolig behov for særskilt motivasjon i virksomheten for arbeid med informasjonssikkerhet, for det er nok ikke mange som er opptatt av dette.[197] I hvilken grad "markedsføres" informasjonssikkerhet i egen virksomhet? I hvilken grad benyttes kampanjer, markedsføringsteknikker og opplæringstilbud? I hvilken grad lykkes dette arbeidet,

[191] Blume (2009) s. 498

[192] Tranvik (2009) s. 15 og s. 114]

[193] Tranvik (2009) s. 49-50

[194] Tranvik (2009) s. 40,s. 52,s. 63-65

[195] Ibid s. 52, s. 55-56

[196] Ibid s. 53

[197] Ibid s. 66-67

jamfør at det er en tendens til at budskap om informasjonssikkerhet taper i kampen om oppmerksomhet?[198] Selv om ikke slike tiltak nødvendigvis er avgjørende kan de vise at ledelsen stiller seg bak sikringsarbeidet, og slik sett bli momenter i vurderingen.

Tranvik skriver i sin undersøkelse om personvernsikring i kommunal sektor om noen av de samme tingene som Lindøe. Han påpeker at i et styringssystem for informasjonssikkerhet (og internkontroll) må det utarbeides plandokumenter.[199] Det gir struktur i arbeidet og gjør arbeidet etterprøvbart.[200] For informasjonssikkerhetssystemer finnes mange eksterne ressurser om plandokumenter, så det å få slik dokumentasjon på plass er ikke det mest kostbare. Hva som er god nok dokumentasjon (omfang og innhold) blir en konkret vurdering som ledelsen må gjøre, basert på innspill fra sikkerhetsmedarbeidere og andre. Som nevnt har datatilsynet mye veiledning om dette. Tranvik påpeker også faren for papiretterlevelse: at det finnes plandokumenter, men at disse ikke er omsatt i praksis i organisasjonen. I verste fall finnes ikke aktivitetsbasert dokumentasjon og/ eller det forekommer ikke regelmessig aktiviteter som revisjoner, ledelsesgjennomganger eller risikovurderinger. Datatilsynet sjekker ved tilsyn at dokumentasjonen reflekterer virksomhetens organisering og gjennomføring av sikkerhetsarbeidet. Men tilsyn per korrespondanse kan gjøre manglende implementering vanskeligere å oppdage.[201]

Revisjon i forbindelse med sertifisering sjekker derimot aktivitetsbasert dokumentasjon ("bevis") nøye, inkludert at disse reflekterer praksis og faktisk etterleves i organisasjonen. Slik revisjon kan avdekke de reelle forhold. Manglende praktisk etterlevelse kan være kjernen i etterlevelsesproblematikken, og dette antyder at sertifiseringsprosesser eller lignende som følger opp at arbeidet er godt og vedvarende kan være del av løsningen. Se til dette at Tranvik rapporterer at den største utfordringen med informasjonssikkerhet er å få på plass et styringssystem for informasjonssikkerhet, inkludert opplæring og kompetanse hos ansatte, og oppfølging av dette.[202] Tranvik påpeker at denne utfordringen ikke er ukjent fra andre områder.[203]

---

[198] Ibid s. 57-58

[199] Ibid s. 23

[200] Ibid s. 79-80

[201] Tranvik (2009) s. 95

[202] Ibid s. 65

Intern praksis blir da nøkkelen til et fungerende system. Men dette kan svikte hvis det er utfordringer med ledelsesforankring, eller med kompetanse og kapasitet.[204] Er det i tillegg organisatorisk motstand, si fra IKT-ansatte som ikke ønsker for mye innblanding i arbeidet kan etterlevelse bli vanskelig.[205]

Organisatoriske utfordringer omfatter også det å etablere et ledelsessystem og en sikkerhetsorganisasjon. Tilstrekkelig med ressurser må tildeles. Man kan ønske seg stillingshjemler men disse koster mye og forventes sjelden.[206] Det er derfor eksempler på at sikkerhetsorganisasjonen i en virksomhet består av en sikkerhetsansvarlig med bare en liten stillingsandel avsatt til sikkerhetsarbeid. En slik utnevnelse kan bli symbolsk.[207] Typisk kan også sikkerhetsarbeid anses som en IKT-oppgave.[208] Og det er det til en betydelig grad, sikkerhetsarbeid omfatter en omfattende mengde tekniske tiltak. Men IKT-sikkerhet er bare en del av informasjonssikkerhet, jamfør andre ledd personopplysningsforskrift § 2-11 til § 2-13. Med mindre sikkerhetsutfordringen etter forholdene er liten, blir det for lite med en ildsjel i en deltidsstilling. Spesielt sårbar blir slike virksomheter dersom sikkerhetsansvarlige slutter uten at systemet er forankret i organisasjonen.[209]

5.4 Helhetsvurdering

Karakteristikken ”tilfredsstillende” er eksempel på bruk av en rettslig standard. Det er lite rettspraksis som setter standarden. Datatilsynet kan gi pålegg etter § 2-2, si i forbindelse med tilsyn, og de er eksperter som generelt nyter generelt stor respekt i forhold til hva som kreves. Der det er tvil om deres vedtak kan de klages for personvernnemda.[210] Men Datatilsynets og personvernnemdas praksis er og blir forvaltningspraksis. Den kan bidra til å skape retningslinjer som kan uttrykke praksis over tid, men rettskildens vekt avhenger til syvende og sist av

---

[203] Ibid s. 89-91

[204] Ibid s. 40

[205] Ibid s. 62

[206] Tranvik (2009) s. 62-63

[207] Tranvik (2009) s. 88

[208] Tranvik (2009) s. 48

[209] Tranvik (2009) s. 53

[210] Personopplysningsloven § 43

argumentenes styrke. Datatilsynet fokuserer trolig derfor på det som de virkelig anser som viktig.

Når det gjelder ISO-standarden er den utbredt og kan sies å uttrykke bransjepraksis. Bransjepraksis vil også kunne få vekt i vurderingene av tilfredsstillende sikkerhet, både etter faglig styrke og som reelt hensyn, men ikke minst som pedagogisk instrument. I NOU 1997:19 uttrykkes det slik:

"Utvalget vil først presisere at atferdsnormer ikke er noe entydig begrep. Normene kan utformes på en rekke ulike måter, og gis forskjellig rettslig status. Utvalget vil for sin del presiserer begrepet slik at det dreier seg om retningslinjer som virksomheter eller bransjerepresentanter selv utarbeider på frivillig basis. Retningslinjene sidestilles ikke med lover, forskrifter eller annen myndighetsutøvelse, og overtredelse resulterer ikke i sanksjoner fra myndighetenes side. Atferdsnormene kan sies å være et internt reglement. […] Fordelen med slike retningslinjer fra bedriftenes side er at de kan avklare tvil, og bidra til klar og rasjonell håndtering av spørsmål som behandlingen av personopplysninger reiser. Atferdsnormene kan utformes mye mer detaljert, nyansert og smidig enn det er mulig å gjøre i en generell lov eller forskrift."[211]

ISO 27001:2013 gir slik sett et godt bidrag til forståelse av problemområdet og lovgivningen.

Oppsummert åpner lovgivningen i noen grad for at behandlingsansvarlig selv avgjør hva som er tilfredsstillende. Dette kommer særlig på spissen i forbindelse med risikovurderingene som pålegges i personopplysningsforskriften § 2-4. Risikovurderinger og tiltak må demonstrere et forsvarlig skjønn tilpasset omstendighetene. Det må kunne dokumenteres at skjønnet er forsvarlig, og at skjønnet er et resultat av planlagt og systematisk arbeid, slik forskriften anviser. Viktig er det også at virksomheten har en organisasjon som fremmer arbeidet med risikovurderingene. En konkret helhetsvurdering avgjør. I helhetsvurderingen inngår formålet med behandlingen, vurderinger av truslene og truslenes konsekvenser for personvernet, sett opp mot sikkerhetstiltakene som er gjort. Vurderingene gjøres både samlet og selvstendig mot henholdsvis konsekvensene for konfidensialitet, integritet og tilgjengelighet. Disse kravene

[211] NOU 1997:17 s. 118

må den behandlingsansvarlige kartlegge, deretter risikovurdere.[212] Så lenge sikkerhetsarbeidet er planlagt, systematisk og dokumentert kan et rimelig skjønn i forhold til utfordringene og forholdsmessigheten i tiltakene bli avgjørende. Særlig bør det undersøkes hvordan virksomheten har arbeidet med det som kan oppfattes som vanskelig.

En slik helhetsvurdering kan virke fremmed for ikke-jurister. Mange vil kanskje heller spørre om sikkerheten blir tilfredsstillende dersom man følger standarden ISO 27001, si ved sertifisering mot denne? Og svaret, gitt ved tolking av standard, lov og forskrift, er langt på vei bekreftende. Men Schartum påpeker at virksomheten også må følge opp overensstemmelse med lovgivningen, i det minste på de mest sikkerhetskritiske behandlingene i virksomheten. [213]

[212] NOU 1997:17 s. 200

[213] Jansen (2005) s. 104

6 Konklusjoner

Utviklingen i arbeidet med informasjonssikkerhet har nok variert med tid, sted og bransje. I den bransjen jeg kjenner litt, som trolig kan sammenlignes med kommunesektoren slik Tranvik beskrev den, kan man kanskje dele utviklingsfasene i tre:

1. IT-ansattes arbeid med fokus på IKT-sikkerhet
2. Ildsjelers arbeid med overordnet rammeverk for informasjonssikkerhet
3. Noe bredere engasjement omkring informasjonssikkerhetens organisatoriske sider

I en fjerde fase kan man se for seg en sammensmelting og utvikling av disse tre fasene i praktisk orientert arbeid med informasjonssikkerhet. Jeg har forsøkt å belyse de rettslige kravene til slikt arbeid.

Personopplysningsloven og personopplysningsforskriften setter rammer for den behandlingen av personopplysninger som kan finne sted. Virksomheten må føre oversikt over hvilke personopplysninger de behandler, fordi personopplysningsloven § 13 krever tilfredsstillende sikring av disse opplysningenes integritet, konfidensialitet og tilgjengelighet (KIT). Personopplysningsforskriften kapittel 2 utdyper sikringskravet til også å omfatte KIT til alle systemene som brukes i behandlingen.

I dagens samfunn er det ikke mulig å overlate ansvaret for sikring av eget personvern til den enkelte, selv om samtykkereglene bidrar til dette. Personvernloven plasserer hovedansvaret for sikringen på virksomhetenes øverste ledelse. Men personvernloven plasseres også et selvstendig ansvar for sikringen på en slik databehandler. Personopplysningsforskriften utdyper dette databehandleransvaret, samt ansvaret som faller på den daglige ledelsen. Medarbeidere har dog en intern plikt til å bidra. Det er viktig å identifisere de sentrale aktørene, for de må trekkes inn i det strukturerte sikringsarbeidet. Samtidig må hver enkelte medarbeider kjenne sitt ansvar for informasjonssikkerheten. Dette siste ansvaret kan være konkret i forhold til praktisk bruk av systemene, men også holdningsmessig, jamfør informasjonsteknologiens, og særlig internettets massive potensial for tilgjengeliggjøring av personopplysninger, som gjør utfordringen stor.

Ledelsen må sørge for organiseringen av sikkerhetsarbeidet i sin organisasjon, inkludert ansvar for den sikringen som eventuelt finner sted hos leverandører og partnere. Loven krever at

dette forholdet avtalefestes. Tradisjonell IKT-sikkerhet utgjør en vesentlig del av arbeidet med informasjonssikkerhet, men loven stiller krav om at dette arbeidet settes i en virksomhetsomfattende organisatorisk ramme, og dette blir et lederansvar. Personopplysningsloven § 13 krever at arbeidet er strukturert og systematisk. Personopplysningsforskriften kapittel 2 utdyper kravene til dette.

Etter tolking av rettskildene inkludert forvaltningspraksis har vi sett at risikovurderinger kanskje er den sentrale kjernen i det systematiske arbeidet. De andre tiltakene kan ses som forarbeid og etterarbeid til risikovurderingene, om enn grunnleggende viktige i seg selv. Virksomheten bør også se informasjonssikkerhetsarbeidet sammen med øvrige virksomhetsprosesser. Dette perspektivet har de som utvikler standarder tatt til seg. Lovgiver åpner for bruk av standarder ved en refleksiv regulering av virksomheter på mange områder. Bruk av ISO 27001 kan da om ikke annet være nyttig pedagogisk og organisatorisk.

Gitt at risikovurderinger står så sentralt kan det være et tankekors at disse kan fremstå som vage og usikre. Dette blir ikke enklere ved at behandlingsansvarliges skjønn er sentralt. Særlig for virksomheter som ikke har erfaring med risikovurderinger eller enda ikke har etablert et styringssystem for informasjonssikkerhet i tråd med regelverkets krav kan dette virke utfordrende.

Verdt å trekke frem er at personopplysningsforskriften stiller "må-krav" om en rekke tiltak. Det kan kanskje tenkes at noen tiltak er lite aktuelle i en konkret virksomhet og at informasjonssikkerheten likevel er tilfredsstillende om de mangler. Men Datatilsynets og personvernnemdas praksis viser at dette ikke gjelder de sentrale tiltakene, de "må" være på plass for at behandlingen skal skje innenfor lovens rammer. Også forholdsmessighet blir da viktig, sammen med prinsippet om kontinuerlig forbedring. Basert på dette må virksomheten utforme planer som svarer på spørsmålet "hvordan kan vi forbedre vår informasjonssikkerhet?"

Men sikkerhet er et sosialt problem. Sikkerhetsutfordringer løses grunnleggende ved å bygge tillit mellom mennesker. Ved å treffe sikkerhetstiltak reduserer man bare noen identifiserte risikoer. Man kan neppe starte tillitsbygging i samfunnet ved å fjerne krav til sikkerhetstiltak i virksomhetene, men dersom samfunnet ensidig fokuserer på sikkerhetstiltak vil virksomhetene aldri oppnå ønsket sikkerhet.

7 Vedlegg 1 Oversikt over dokumentasjon

Dokumenter oppsummert etter ISO 27001 (med henvisning til standard og personopplysningsforskrift):

1. Nåsituasjonsbeskrivelse (anbefalt)
2. Informasjonssikkerhetssystemets omfang og rekkevidde (4.3 (4.1 -4.4), se pof § 2-3)
3. Policy for informasjonssikkerhet (5.2 (5.1 - 5.3,se pof § 2-3, pof § 2-7 Organisasjon)
4. Risikovurdering prosessbeskrivelse (6.1.2 se pof § 2-4)
5. Risikohåndtering prosessbeskrivelse (6.1.3, se pof § 2-4)
6. Risiskovurdering resultater (8.2, 6.1.2, se pof § 2-4)
7. Risikohåndtering resultater (8.3, 6.1.3, se pof § 2-4)
8. Plan for risikovurdering (6.1.2, se pof § 2-4)
9. Plan for risikohåndtering (6.1.3, se pof § 2-14)
10. Anvendelseserklæring (SOA) (6.1.3d, se pof § 2-4)
11. Hvordan sikkerhetsmål etableres og nås (6.2, se pof § 2-3)
12. Sikkerhetsmål (6.2, se pof § 2-3)
13. Kompetansebevis (7.2d)
14. Kompetanseplan (anbefalt, 7.1 - 7.2) ("resources, roles and responsibilities")
15. Kompetanse prosessbeskrivelse (anbefalt, 7.2)
16. Opplysninger nødvendige for styringssystemets effektivitet (7.5.1b)
17. Program for holdninger, bevissthet og sikkerhetskultur (anbefalt, 7.3)
18. Kommunikasjonsplan (anbefalt 7.4)
19. Driftsplanlegging og kontroll (8.1)
20. Måling og overvåking prosessbeskrivelse (anbefalt 9.1, pof § 2-6)
21. Måling og overvåking resultater (9.1, se pof § 2-6, § 2-14)
22. Revisjon prosessbeskrivelse (9.2g, se pof § 2-5)
23. Revisjon resultater (9.2g, se pof § 2-5)
24. Ledelsens gjennomgang prosessbeskrivelse (anbefalt 9.3)
25. Ledelsens gjennomgang resultater (evt. møtereferat osv) og bevis (9.3, se pof § 2-3)
26. Hendelser som har påvirket sikkerheten (10.1 se pof § 2-5 og § 2-6)
27. Avvik og retting prosessbeskrivelse (bare anbefalt, 10.1, se pof § 2-6, § 2-14)
28. Avvik og retting resultater og bevis (10.1f, se pof § 2-6, § 2-14)
29. Retting: resultater/bevis (10.1g)
30. Plan for kontinuerlig forbedring (anbefalt)
31. Kontinuerlig forbedring resultater og bevis (anbefalt)
32. Annex A prosedyredokument (8.1, Anbefalt, var obligatorisk før)

Andre dokumentasjonskrav i personopplysningsforskriften:

a) § 2-7 dokumentasjon av konfigurasjon av informasjonssystemet
b) § 2-7 rutiner for bruk av informasjonssystemet (jamfør pof § 2-8)
c) § 2-8 og 2-14 (u-)autorisert bruk av informasjonssystemet skal registreres og lagres i minst 3 måneder, ref pof § 2-16
d) § 2-16 rutiner og informasjon av betydning skal dokumenteres og lages i 5 år

8 Litteraturliste

Aas, John-Wessel. ISOC medlemsmøte. 24. oktober 2013

Blume, Peter. *Vurdering av personvernnemdas praksis 2001-2008*. Oslo 2009. (Complex; nr. 3/09)

Carlstedt, Anders. Muntlig. 3. Mars 2014.

Dagsavisen. *Da holocaust kom til Norge* (2012). http://www.dagsavisen.no/nye-inntrykk/reportasje/da-holocaust-kom-til-norge/

Datatilsynet. *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer* (2000) http://www.datatilsynet.no/Global/05_regelverk/sikkerhetsbest_personopplforskriften_kom.pdf

Datatilsynet. *En veiledning om internkontroll og informasjonssikkerhet* (2009) http://www.datatilsynet.no/Global/04_veiledere/internkontroll_veil.pdf

Datatilsynet. Årsmelding 2012. 12 februar 2013. http://datatilsynet.no/Global/04_planer_rapporter/aarsmelding/Årsmeldingen2012.pdf .

Datatilsynet. *Internkontroll og informasjonssikkerhet - veileder* (2011) http://www.datatilsynet.no/Sikkerhet-internkontroll/internkontroll_informasjonssikkerhet/

Datatilsynet. *Word-Maler for internkontroll og informasjonssikkerhet.* (2012) http://datatilsynet.no/Sikkerhet-internkontroll/internkontroll_informasjonssikkerhet/Maler-internkontroll-informasjonssikkerhet/

Datatilsynet. *Databehandleravtale – mal* . (2013) http://www.datatilsynet.no/verktoy-skjema/Skjema-maler/Databehandleravtale---mal/ [sitert 03.01.2014]

Datatilsynet. *Forarbeider til det sentrale personvernregelverket.* (2014) http://www.datatilsynet.no/Regelverk/Lover-og-regler1/Forarbeider/ [sitert 03.01. 2014]

Datatilsynet. *Overvåkingsprogrammet PRISM.* (2013) http://www.datatilsynet.no/Sektor/Politi-justis/overvaaking-PRISM/

Difi. *Styringssystem for informasjonssikkerhet.* Rapport 2012:15. 2012. http://www.difi.no/filearchive/difi-rapport-2012-15-styringssystem-for-informasjonssikkerhet.-erfaringer-og-anbefalinger.pdf

Fanebust, Arne. *Innføring i arbeidsrett. Den individuelle delen.* 2. utg. Oslo 2013.

Fornynings-, administrasjons- og kirkedepartementet. Digitaliseringsrundskrivet. Nr. P-10/2012. (2012) http://www.regjeringen.no/nb/dep/kmd/dok/rundskriv/2012/digitaliseringsrundskrivet.html?id=706462

Fornynings-, administrasjons- og kirkedepartementet. Nasjonal strategi for informasjonssikkerhet Handlingsplan. 17. desember 2012. http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf

Hasle, Terje. E-post. 17. januar 2014

Haug, Are Vegard. *Rettslige reguleringer av informasjonssikkerhet.* Oslo, 2006. (Complex; nr. 2/06)

Håndbok i datasikkerhet –informasjonsteknologi og risikostyring. Torgeir Daler…[et al.]. 2. Utg. Trondheim, 2006

Jansen, Arild og Dag Wiese Schartum *Informasjonssikkerhet Rettslige krav til sikker bruk av IKT.* Bergen, 2005

ISO/IEC. Information technology – Security techniques – Code of practice for information security controls. 27002:2013.

ISO/IEC. Information technology - Security techniques - Information security management systems – Requirements. 27001:2013.

Johansen, Michael Wiik, Knut-Brede Kaspersen, og Åste Marie Bergseng Skullerud *Person-opplysningsloven Kommentarutgave.* Oslo, 2001

Justis- og beredskapsdepartementet. *Forskrift til personopplysningsloven (personopplysnings-forskriften* (2000) 15.12. 2000 http://www.regjeringen.no/nb/dep/jd/dok/lover_regler/reglement/2000/forskrift-til-personopplysningsloven-per/2.html?id=278532 [sitert 03.01. 2014]

Kvalex den offisielle ISO-guiden over sertifiseringer i Norge. (2014). http://www.kvalex.no/bedrifter/iso+27001/ [sitert 06.02. 2014]

Lindøe, Preben. *Arbeidsmiljøregulering i de nordiske lande.* Tidsskrift for ARBEJDSLIV, nr. 4. 2002. http://www.nyt-om-arbejdsliv.dk/images/pdf/2002/nr4/ta02-4-23.pdf

Moeller, Robert R. Executive's guide to IT governance: improving systems processes with service management, COBIT, and ITIL. Hoboken, 2013

Norman,Rolf Sture og Tommy Tranvik *Personvern og informasjonssikkerhet i kommunen en håndbok i risikovurdering.* Oslo 2012

NOU 1997:19 Et bedre personvern - forslag til lov om behandling av personopplysninger

Office of Government Commerce. *ITIL Service Design.* London, TSO, 2007.

Office of Government Commerce. *ITIL Service Transition.* London, TSO, 2007.

Ot.prp. nr 92 (1998-1999) Om lov om behandling av personopplysninger (personopplys-ningsloven).

PECB Information security training participant handout.(2014) *Certified ISO/IEC 27001 Lead Auditor.*

Personvernnemda. *Vedtak.* http://www.personvernnemnda.no/vedtak/index.htm [sitert 10.03.2014]

Rapport fra Riksrevisjonen. *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2012 Dokument 1 (2013-2014).* 2013. http://www.riksrevisjonen.no/Rapporter/Sider/Dokument1for2012.aspx

Schartum, Dag Wiese og Lee A. Bygrave *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. 2. utg. Oslo, 2011.

Schartum, Dag Wiese. E-post. 6. mars 2014

Schneier, Bruce *Beyond fear.* New York, 2003.

Smolyakova, Olena. E-post. 8. august 2012.

Taraldset, Birthe. *Arbeidsrett - eller eierstyring og selskapsledelse?* Arbeidsrett. 2010. s. 66.

Tranvik, Tommy. *Personvern og informasjonssikkerhet.* Oslo, 2009. (Complex; nr. 4/09)

Tranvik, Tommy. Telefonsamtale. 16. januar 2014

1956 Lov om tilsynet med finansinstitusjoner mv. (finanstilsynsloven) 7. desember Nr. 1

2000 Lov om behandling av personopplysninger (personopplysningsloven) 14. april Nr. 31

1996 Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften) 6. desember Nr. 1127

1999 Lov om revisjon og revisorer (revisorloven) 15. januar Nr. 2

2000 Forskrift om behandling av personopplysninger (personopplysningsforskriften) 15. desember Nr. 1265

2001 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) 18. mai Nr. 24

2003 Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) 21. mai Nr. 630