Persondataforordningen og ISO 27001

Hans Chr. Spies, spies@hcspies.dk, 5/3-2017

ISO 27001 beskriver en internationalt anerkendt metode til at implementere informationssikkerhed i en organisation. Det er derfor nærliggende at undersøge, om det ligger inden for rammerne af standarden at implementere kravene i persondataforordningen[1], og hvordan dette i givet fald kan gøres i praksis.

I artiklen argumenteres der for, at det er i god overensstemmelse med tankegodset bag ISO 27001 at implementere kravene i persondataforordningen inden for standarden. Herefter argumenteres der for, at såfremt der skal foretages en implementering af persondataforordningen, bør der foretages en præjudiciel analyse af hvilke krav i forordningen, der i det konkrete tilfælde skal implementeres, og at disse krav herefter så vidt muligt bør håndteres på grundlag af den opdeling, der er foretaget i forordningen for at gøre det enklest muligt at udføre revision og vedligeholdelse.

ISO 27001

ISO 27001[2] beskriver en metode, efter hvilken en organisation kan sikre information af betydning for organisationen.[3]

ISO 27001 er en international standard, og fordelen ved at anvende denne standard fremfor at gå sine egne veje er særligt hensynet til følgende:

- Kvalitet

  ISO 27001 indeholder en opregning af egnede tiltag til at sikre informationssikkerheden.[4] Implementerer man ISO 27001, sikres det derfor, at man i hvert fald har overvejet tiltag, der i "best practice" betragtes som væsentlige.

- Dokumentation

  ISO 27001 stiller krav om udfærdigelse af dokumentation for de tiltag, der tænkes sat i værk.[5] Herved sikres et godt grundlag for, dels at der efterfølgende kan foretages en kontrol af, at de nødvendige sikkerhedstiltag rent faktisk er foretaget, dels et godt grundlag for revision og for den efterfølgende vedligeholdelse, når ændrede forhold i eller uden for organisationen gør dette nødvendigt.

---

[1] Forordning 2016/679.
[2] ISO 27001:2013.
[3] Se hertil Georg Disterer: *ISO/IEC 27000, 27001 and 27002 for Information Security Management*, Journal of Information Security, 2013, 4, 92-100.
[4] Se hertil Annex A.
[5] Se hertil eksempelvis 6.1.3, litra d .

ISO 27001 og persondataforordningen

ISO 27001 forholder sig til helt grundlæggende IT-sikkerhedsmæssige risici, som f.eks. risikoen for at uvedkommende får adgang til fortrolig information gennem uautoriseret adgang til organisationens netværk.[6]

En organisation kan imidlertid ikke nøjes med at forholde sig til de udfordringer, som udspringer af at sådanne IT-sikkerhedsmæssige risici. En organisation må også forholde sig til de udfordringer, der udspringer af lovgivningsmæssige krav, såsom eksempelvis de krav, der stilles i persondataforordningen.[7]

ISO 27001 har øje for denne problematik. Således fremgår det eksplicit af standarden, at der skal tages højde for "Compliance with legal and contractual requirements".[8]

Som udgangspunkt synes ISO 27001 derfor at være tænkt som en ramme, inden for hvilken en organisation kan implementere retlige krav. Følgelig burde persondataforordningen også kunne implementeres inden for denne ramme, hvorved specielt bemærkes, at beskyttelse af personoplysninger eksplicit nævnes i Annex A.[9]

Udfordringen er blot, at mens ISO 27001 forholder sig meget detaljeret til generelle sikkerhedsmæssige risici, forholder standarden sig mere overfladisk til, hvordan man nærmere skal forholde sig til de retlige krav. Således hedder det i Annex A alene, for så vidt angår "Privacy and protection of personally identifiable information", at "Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable."[10]

Skitse til en løsning

Kravene i persondataforordningen kan oversigtsmæssigt rubriceres som følger:

- Grundlæggende principper

  Eksempelvis formålsbestemthedsprincippet, art. 5, stk. 1, litra b, og proportionalitetsprincippet, art. 5, stk. 1, litra c.

- Behandlingsbetingelser

  Eksempelvis samtykke, art. 6, stk. 1, litra a.

- Rettigheder for den registrerede

  Eksempelvis adgang til indsigt, art. 15, og ret til dataportabilitet, art. 20.

- Sikkerhedsmæssige krav

  Eksempelvis pseudonymisering og kryptering af oplysninger, art. 32, stk. 1, litra a.

---

[6] Se hertil Annex A, A.13.1.
[7] Se hertil Peter Blume og Hans Christian Spies: Ret og Digital forvaltning, Jurist- og Økonomforbundets Forlag 2005.
[8] Se hertil Annex A, A.18.1.
[9] Annex A, A.18.1.4.
[10] Annex A, A.18.1.4.

- Organisatoriske og proceduremæssige krav

  Eksempelvis krav om udpegelse af en databeskyttelsesrådgiver, art. 37, og krav om udarbejdelse af en fortegnelse over behandlingsaktiviteter, art. 30, og krav om at foretage en konsekvens-analyse vedrørende databeskyttelse, art. 35.

Disse krav har form som andre retsregler

retsfaktum → retsfølge

hvor retsfaktum typisk vil have karakter af hensyn, der skal afvejes. Eksempelvis kan det sikkerhedsmæssige krav i art. 32, stk. 1, litra a, beskrives som følger:

afvejning {tekniske og økonomiske hensyn mv.} → krav om pseudonymisering/kryptering

Hvis dette krav skal indgå i en ISO 27001-ramme, kan tiltaget A.10.1.1 i Annex A udgøre en inspirationskilde:

Policy on the use of cryptographic controls	Control A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

Dette tiltag rummer i sig et krav om udarbejdelse af en "politik" for brugen af kryptering. En politik har meget lighed med en retsregel, og lader sig beskrive på lignende vis:[11]

Politik	Retsregel
betingelser → handling	retsfaktum → retsfølge

Politikken adskiller sig dog fra retsreglen ved, at politikken ikke har nogen retlig hjemmel. Men tilføjes en retlig hjemmel, lader kravet fra retsreglen sig indpasse i den beskrivelse af tiltag, som anvendes i ISO 27001:[12]

Retningslinjer for brug af kryptering og pseudonymisering	Control Der skal udarbejdes retningslinjer for brug af kryptering og pseudonymisering, jf. forordning 2016/679, art. 32, stk. 1, litra a.

[11] Se hertil Preben Stuer Lauridsen: *Studier i retspolitisk argumentation*, Juristforbundets Forlag 1974.

[12] En tilsvarende tilgang anvendes i Henning Mortensen (red.): *Vejledning. Persondataforordningen - Implementering i danske virksomheder*, DI Digital 2016.

En sådan tilgang synes at være helt i overensstemmelse med ISO 27001, da standarden netop stiller krav om, at man om muligt skal opstille egne tiltag.[13]

Risikovurderingen
ISO 27001 bygger på den filosofi, at man skal identificere potentielle risici, for hver af disse risici vurdere niveauet som en funktion af konsekvens/hyppighed og herefter foranstalte tiltag for at gardere sig mod de risici, der overskrider et på forhånd fastsat niveau.

Grænsen for hvornår risici skal give anledning til foranstaltning af tiltag fastlægger man selv.[14] Herved adskiller situationen sig fra de tilfælde, hvor der er fastsat retsregler. Her er det lovgiver, der har bestemt, hvornår der skal ageres. Derfor synes det rigtigst, når det gælder retsregler, at undlade den risikovurdering, som foreskrives i ISO 27001, men altid foranstalte de tiltag, som er egnede til at håndhæve retsreglerne. En sådan løsning synes også at være i overensstemmelse med ISO 27001, da det efter standarden er et krav, at man identificerer alle relevante retsregler, og da den naturlige konsekvens herefter må underforstås at være, at man overholder disse retsregler.[15]

Fastlæggelse af tiltagene
Kravene i persondataforordningen er fastlagt i den publicerede tekst. Når de enkelte tiltag skal fastsættes, kunne en mulig tilgang derfor være, at lade denne tekst i sin helhed udgøre et tiltag. Et sådan tilgang ville være i overensstemmelse med ISO 27001, men vil skille sig ud fra den måde tiltagene beskrives i ISO 27001 allerede fordi forordningsteksten fylder 88 sider, mens et tiltag beskrevet i Annex A typisk fylder et par linier.

Det synes derfor bedre i harmoni med ISO 27001 at dele forordningen op i mindre dele, som man hver især lader udgøre fundamentet for et tiltag. Denne opdeling ville eksempelvis kunne foretages på artikelniveau eller ved en yderligere opdeling af de enkelte artikler.[16] Med udgangspunkt i det ovenfor nævnte eksempel ville tiltagene eksempelvis kunne formuleres således:

Art. 32, stk. 1, litra a	Control ”pseudonymisering og kryptering af personoplysninger”
Art. 32, stk. 1, litra b	Control ”evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester”

En sådan strategi kan være hensigtsmæssig, idet det sikres, at der ikke overses nogle retlige krav i persondataforordningen.[17] Strategien lider dog af den svaghed, at den giver anledning til udarbejdelse af ganske mange tiltag. Også sådanne som det kan forekomme unødvendigt at skulle

[13] Jf. 6.1.3, litra b.
[14] Jf. 6.1.2, litra a, nr. 1.
[15] Jf. Annex A, A.18.1.1.
[16] Denne strategi anvendes i Henning Mortensen (2016).
[17] Strategien synes at harmonere meget godt med den tankegang, der synes at ligge bag kravet i 6.1.3, litra c, om at man skal forholde sig til samtlige tiltag gengivet i Annex A.

medtage. Eksempelvis synes det overflødigt at forholde sig til kravene i persondataforordningens kapitel V, hvis organisationen slet ikke overfører persondata til tredjelande eller internationale organisationer.

En bedre strategi synes derfor at være at foretage en præjudiciel analyse af, hvilke retlige krav i persondataforordningen, der kan være relevante. Herefter kan man nøjes med at udarbejde tiltag for disse krav.

En sådan strategi er også overordnet set i god harmoni med ISO 27001. ISO 27001 stiller således krav om, at der foretages en analyse af, hvilket område der skal dækkes, hvilket i sagens natur typisk vil indsnævre kredsen af relevante tiltag.[18]

Yderligere bearbejdning af tiltagene?

Spørgsmålet er herefter, om der kan være behov for yderligere bearbejdning af tiltagene, således at et tiltag kan have fundament i stof sammenstykket på tværs af den opdeling, der er foretaget i forordningen. Af forordningens art. 6, stk. 1, nr. 1, fremgår det eksempelvis, at der lovligt vil kunne foretages behandling af personoplysninger, såfremt der foreligger et samtykke. Kravene til dette samtykke er imidlertid ikke beskrevet i art. 6, stk. 1, nr. 1, men derimod i art. 7 og 8. Det kan derfor diskuteres, om det ikke ville være hensigtsmæssigt, at lade teksten i art. 6, stk. 1, nr. 1, udgøre grundlaget for et tiltag sammen med teksten i art. 7 og 8. Umiddelbart virker det som en selvfølgelig løsning, men det er måske alligevel ikke en god løsning, når det haves for øje, at der også stilles et samtykkekrav i art. 9, stk. 2, litra a.

Der kan formentlig ikke gives noget endegyldigt svar på, om man bør kaste sig ud i en egen opdeling af forordningens krav. Mest hensigtsmæssigt er det nok så vidt muligt at følge forordningens opdeling. For dette taler især, at jo tættere man lægger sig op ad den opdeling af kravene, som forordningen anviser, des enklere vil det være at foretage nødvendige ændringer i tiltagene, hvis reglerne eller fortolkningen af disse ændrer sig. I den forbindelse er det også relevant, at kommenterede love i deres opdeling af stoffet traditionelt følger lovteksten.

Sammenfatning og konklusion

At implementere persondataforordningen inden for rammerne af ISO 27001 synes at harmonere godt med tankegodset bag standarden. I praksis vil en implementering overordnet set kunne foretages ved at lade kravene i persondataforordningen udgøre grundlaget for tiltag på linje med de tiltag, der er opremset i Annex A i ISO 27001.

Når det gælder detaljen, foreslås det, at der indledningsvist foretages en præjudiciel analyse af, hvilke krav i forordningen der i det hele taget er relevante i den pågældende sammenhæng. Dernæst opdeles kravene på grundlag af den opdeling, der er foretaget i forordningen, og hvert af disse brudstykker udgør herefter fundamentet for et tiltag. Efter omstændighederne kan man lade et tiltag forholde sig til krav i forordningen på tværs af den opdeling, som forordningen anviser. Det bør dog være vægtige grunde til dette for at tilgodese hensynet til, at det skal være enkelt at foretage revision af implementeringen og at foretage vedligeholdelse, såfremt reglerne eller fortolkningen af disse ændrer sig.

[18] Se hertil A.3 sammenholdt med 6.1.3, litra b.