Informationssikkerhed

Torben Abildgaard Pedersen, **TAP**FREELANCE ApS og **TAP**CERT ApS

Baggrund

Tillid til informationssikkerhed er forudsætningen for, at teknologiens muligheder ved digital økonomi og udnyttelse af registrerede persondata kan udvikle sig til gavn for borgerne i Det indre Marked, uden at der opstår nye risici.

Organisationer, der råder over lagrede persondata, må derfor beskytte dem for at hindre brud på fortrolighed (hemmeligholdelse), integritet (fuldgyldighed) og tilgængelighed (at autoriserede har adgang til data, når de skal bruge dem). Sikkerhedskravene skærpes i disse år – navnlig med vedtagelsen af EU-persondataforordningen [1] gældende fra 25. maj 2018. Forordningen er bindende i alle enkeltheder og gælder umiddelbart i alle medlemsstater i Det indre Marked uden implementering i landenes nationallovgivning.

Forordningens krav kan løftes ved at indføre et ledelsessystem efter den i praksis harmoniserede standard ISO/IEC 27001 med inspiration fra regelsættet i ISO/IEC 27002.

Organisationer med et ledelsessystem efter kravene i ISO 9001:2015 har en fordel, fordi de med tilføjelse af få supplerende dokumenter kan bringe deres systemer i overensstemmelse med ISO/IEC 27001 og dermed forordningen.

De, der håndterer følsomme persondata (fx en myndighed, en bank, et forsikringsselskab, en e-handelsvirksomhed eller et sygehus), skal dog ikke undervurdere opgaven med udarbejdelse af de påkrævede "få supplerende dokumenter". Dette betyder, at man bør reservere sig selv god tid til forberedelsen af overgangen til de nye, skærpede krav. Projektet må i gang nu, hvis det ikke allerede er virkelighed.

Organisationer uden ledelsessystem eller tilsvarende lever konstant, måske endda uden at de selv ved det, med en forhøjet risikoprofil og informationssikkerhedstrussel. Måske er det mange gange blot et spørgsmål om tid, førend der vil indtræffe hændelser med alvorlige brud på informationssikkerheden til følge.

De, som fravælger ledelsessystemet eller en anden form for gennemtænkt regelsæt, der beskriver de implementerede it-kontroller, skal være klar over, at bødeniveauer ved overtrædelse af persondataforordningen kan udgøre 2-4 % af virksomhedens årlige, globale omsætning og minimum 10-20.000.000 € i afhængighed i konsekvensen af indtrufne informationssikkerhedsbrud. Sagt på en anden måde kan en dom for uforsvarlig omgang med persondata let føre til afvikling eller betydelig omorganisering af den juridisk ansvarlige enhed. Tilsidesættelse af krav til forebyggelse af risiko kan også føre til sanktioner.

De fleste offentlige og private organisationer håndterer persondata (evt. pseudonyme data) i større eller mindre udstrækning. Persondata dækker nemlig over mere, end man skulle tro.

For hver enkelt person kunne eksempler på almindelige, følsomme eller semifølsomme data være CPR-nummer, navn, køn, adresse, e-mailadresse, webadresse, telefonnumre, pasnummer, kreditkortnumre, kontooplysninger, brugernavne, adgangskoder, sikkerhedskoder, foto, medarbejder-ID, kørekortdata, registreringsnumre og stelnumre på biler, GPS-spor fra elektronisk kørebog, rejseoplysninger, genetisk information, biometriske data, somatiske, psykiatriske og odontologiske patientjournaloptegnelser, oplysninger om sociale problemer, økonomiske og regnskabsmæssige data, aftale-, licens-, samtykkedokumenter, løn-, indkomst-, pensions- og formueoplysninger, bank- og skatteoplysninger, familie-, uddannelses-, job- og helbredsrelaterede oplysninger og -ansøgninger, resultater af intelligens- og personlighedstests, oplysninger om politisk/religiøs/seksuel overbevisning og foreningsmæssige tilhørsforhold, udeståender med myndigheder, officielt udstedte beviser og attester, herunder straffeattest og PET-screening, tøjstørrelse og skonummer, videooptagelser, elektroniske spor samt oplysninger om interesser og forbrugsmønstre samt kundetilfredshed og -loyalitet.

Persondataforordningen medtager krav til udpegning af en datasikkerhedsansvarlig (= DPO, Data Protection Officer), administration af rettigheder til sletning af data og dataportabilitet (overførsel af personoplysninger fra én tjenesteudbyder til en anden). Sidstnævnte transaktionsform kræver normalt indhentning af samtykke eller udtrykkeligt samtykke.

Kun de færreste organisationer kan sige sig helt fri for et ansvar for informationssikkerhedsledelse. Derfor kan man forestille sig, da risikoledelse også er oppe i tiden på andre fronter, at de skærpede krav inden for denne artikels emne faktisk bliver den katalysator, som vedrørende brug af ledelsessystemer – ofte kombinerede systemer – indleder en ny æra. Det ventes, at ISO/IEC 27001 på verdensplan i 2025 vil overhale antallet af ISO 9001-certifikater (flere end 1 mio. i 2014) [2].

Det betaler sig at sætte sig ind i, hvad ISO/IEC 27001 står for, selv om ikke alle behøver at stile efter akkrediteret certificering. Standardens krav knytter sig så meget til virksomheders administrative strukturer, at man må formode, at overensstemmelsesvurdering også kommer til at indgå i ydelsespakker, som traditionelt har været tilbudt af it-supportere, softwareleverandører, erhvervsadvokater og revisionsselskaber.

Akkrediteret certificering på informationssikkerhedsområdet har størst betydning i situationer, hvor man internationalt og over for kunder eller tredjepart skal levere fuld dokumentation for ledelsessystemets overensstemmelse med ISO/IEC 27001 – herunder at til- og fravalget af it-kontroller er relevant.

Kravene til ISO/IEC 27001-systemer

Et eksisterende ISO 9001:2015-system hvilende på risikobaseret tankegang, herunder ISO's proces- og Plan-Do-Check-Act-model [3], afkorter ISO/IEC 27001-implementeringsarbejdet med mindst en tredjedel, fordi procedurer for styring af fx dokumenteret information, intern audit, korrigerende handlinger, målstyring og ledelsens evaluering samt personaleadministration, kompetenceudvikling og styring af processer/produkter/ydelser leveret udefra, kan genbruges uden eller med få tilpasninger.

De ekstra dokumenter, som er nødvendige i de fleste ledelsessystemer til håndtering af informationssikkerhed, er nævnt i fig. 1. Hvor der er anført reference til ISO 9001:2015, vil det typisk være enklest at føje til i et sandsynligvis allerede eksisterende dokument.

Emne	Ref. ISO 9001:2015	Ref. ISO/IEC 27001:2013
Ledelsessystemets omfang	4.3	4.3
Informationssikkerhedspolitik og -mål	5.2, 6.2	5.2, 6.2
Analyse og vurdering af risici og muligheder med handleplaner til adressering af samme	6.1	6.1.2, 6.1.3.e, 6.2, 8.2
Erklæring om it-kontrollers anvendelighed	4.4	6.1.3.d
Ansvar og beføjelser	5.3	A.7.1.2 og A.13.2.4
Fortegnelse over aktiver	7.1.3	A.8.1.1
Acceptabel brug af og omgang med aktiver		A.8.1.3
Adgangsstyringspolitik		A.9.1.1
Driftsprocedurer for informationssikkerhedsledelse		A.12.1.1
Principper for udvikling af sikre systemer	8.3	A.14.2.5
Informationssikkerhedspolitik for leverandørforhold	8.4	A.15.1.1
Håndtering af informationssikkerhedsbrud	10.2	A.16.1.5
Implementering af informationssikkerhedskontinuitet		A.17.1.2
Identifikation af gældende lovgivning og kontraktkrav	4.1, 8.2.2	A.18.1.1

Fig. 1 – Nødvendige ISO/IEC 27001-dokumenter. Referencer indledt med A henviser til standardens anneks over udpegede risikoområder. De tre dokumenter *angivet med kursiv* anses for at være nøgledokumenterne i et informationssikkerhedsledelsessystem. Sammenhængen er illustreret i fig. 2.

Ud over ISO's 10 kernekapitler indeholder ISO/IEC 27001 et anneks med 13 listede risikoområder, som kan være kritiske i typisk forekommende organisationer. Til hvert risikoområde er identificeret kritiske styringspunkter, som i dansk oversættelse kaldes for it-kontroller. Baseret på sin *Analyse og vurdering af risici og muligheder med handleplaner til adressering af samme* skal organisationen i *Erklæring om it-kontrollers anvendelighed* beslutte tilvalg og fravalg af it-kontroller, idet fravalgene skal begrundes.

Risikoanalysen skal tage sit udgangspunkt i *Fortegnelse over aktiver* – fysiske såvel som personelle – så sårbarhederne. Hjælp fås i ISO/IEC 27005, anneks B.

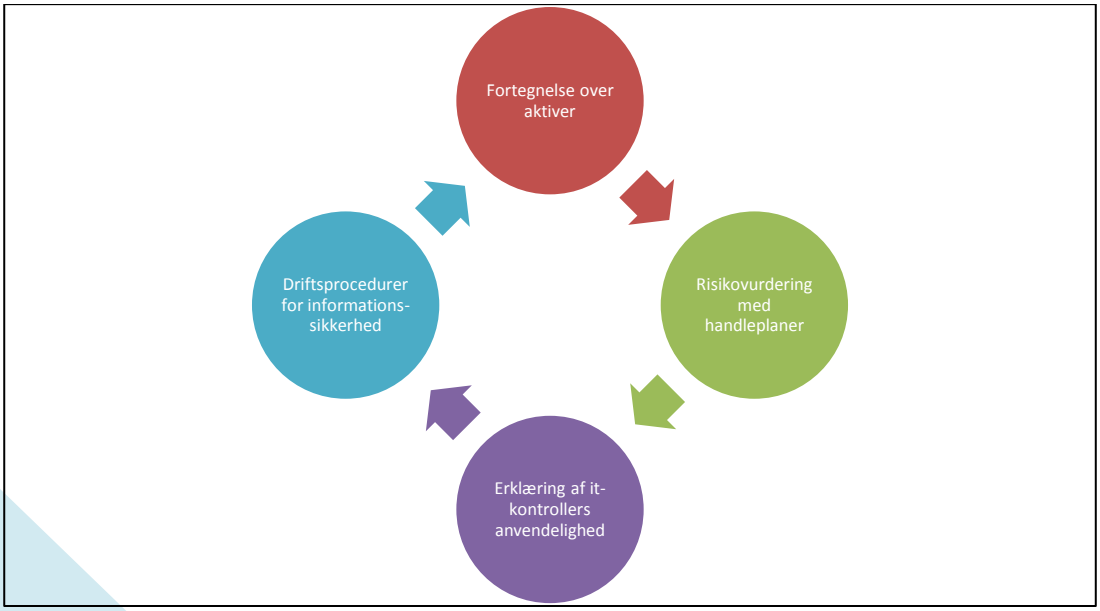

Fig. 2 – Sammenhængen mellem nøgledokumenterne i et ISO/IEC 27001-system. Ud fra relevante aktiver (hardware, software, databaser, personer) adresseres risici (og muligheder) med handleplaner. Anneks A-risikoområder med acceptabel baseline restrisiko fravælges ved erklæring og med begrundelse. Driftsprocedurer – evt. handleplaner for tilvejebringelse af sådanne – iværksættes, således at aktiverne beskyttes bedst muligt for at nå den konfidentialitet, integritet og tilgængelighed af data, som politik og mål definerer.

Afsluttende bemærkninger

Organisationer bør straks gå i gang med at føje en informationssikkerhedsdel til ledelsessystemet. Det er kun forsvarligt at vente, hvis man er sikker på, at aktiviteter og aktiver stort set ikke berøres af persondataforordningens krav.

Rigtigt grebet an behøver der ikke at være så meget bureaukrati i det. Tag fat i ISO/IEC 27001, og brug denne artikel til at få overblik over de tilføjelser, der skal til.

Har man ikke et ledelsessystem, er det et spørgsmål, om man har tænkt nok over sin strategi. I længden hjælper umiddelbar succes ikke den, der forsømmer at forebygge i tide.

Ringe opbakning fra topledelsen med delegering af problemstillingen – også vedrørende informationssikkerhed – til en intern projektleder uden tilstrækkelige ressourcer og kompetencer for at spare udgifter til ekstern hjælp væk kan vel – som den nemme løsning betragtet – i styrke sammenlignes med et bæger skarntydesaft stående klos op ad kaffekoppen. Fejl- og undervurdering kan være dyrt, for ikke at sige fatalt.

Referencer

Referencer til officielle standarder er ikke anført.

[1] EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

[2] http://www.iso.org/iso/iso-survey

[3] T. Abildgaard, DS-håndbog 190:2016, Den nye ISO 9001 i praksis.