



Privacy og databeskyttelse

– en ledelses opgave med sund fornuft

Charlotte Pedersen

12. November 2014

Charlotte Pedersen

- Director
- Cand.scient.pol.
- CIS LA, CIS 2013 UP, CIIP, CISM, CRISC, CGEIT mv.
- Medlem af S411 hos Dansk Standard

Cyber Risk Services

Telefon: 20 85 35 42

Mail: cpedersen@deloitte.dk



Kernekompetencer:

- Cyber Security Management – informationssikkerhedsledelse (ISO2700x), risikoanalyse, politik, governance
- Privacy – analyse, strategi og rapportering vedr. personoplysninger
- Proces- og implementeringskonsulent
- Kommunikation og awareness aktiviteter
- Risikostyring, mål- og resultatstyring
- Projektledelse - forandringsledelse

Databeskyttelse er en ledelsesdisciplin

- Tekniske krav?
- Ikke underkende de tekniske muligheder – og udfordringer
- Forebyggende tekniske kontroller er en forudsætning
- For ensidigt fokus på tekniske kontroller forhindrer databeskyttelse på direktionens – og ledelsesgangen
- Forudsætning for vedvarende forandringer og implementering i organisationerne er ledelsesforankring
- Databeskyttelse er en ledelsesdisciplin – måske ny for nogen



Ledelse

- Prioritering – valg og fravalg på et oplyst grundlag
- Ansvarlighed – stå til ansvar for
- Efterleve lovgivning, andre vedtagne spilleregler og accepterede værdier – ordentlighed f.eks.
- Ledelse baseret på kontekst analyse – aldrig med bind for øjnene
- Evne til at nå fastlagt mål – finansielle og ikke-finansielle
- Risici – negativt og positivt – trusler og muligheder
- FIT – risiko for tab af tilgængelighed, integritet og fortrolighed
- Forebyggende handlinger er i sidste ende bedre og billigere – end opdagende, undskyldende og genetablerende handlinger



Rigtig meget sund fornuft

Ledelsværktøjer – hjælp til virksomhederne

- ISO27001:2013 – best practise – ramme for informationssikkerhedsstyring. Nye udgave af standarden har fokus på ledelsesforankring og risikostyring
- Information om tekniske mulige løsninger
- Formidling af trusselsbilleder og risikoprofiler
- Formidling af vejledninger og eksempler
- Deling af viden om sikkerhedshændelser



- Vejledning og information til ledere på ikke teknisk sprog
- Vi har en salgs- og kommunikationsopgave



Privacy vs. sikkerheds paradokset

Privacy
Stærk privacy forudsætter beskyttelse af borgerens/brugerens identitet fra uautoriseret adgang og brug

Individuel privacy og privatlivets fred

Identity management og uafviselighed

Sikkerhed
Stærk sikkerhed forudsætter at brugerens identitet er knyttet til deres adfærd for at kunne tillade autoriseret adgang, uafviselighed og styring af adgang til data

Sikkerhed er nødvendig for privacy, men jo stærkere den enkeltes identitet er knyttet til deres adfærd – des større trussel for den enkeltes privacy



Fremadrettet rejse – det hårde arbejde

- Trusselsbilledet ændrer sig
- Nye sikkerhedshændelser offentliggøres hver dag – også i Danmark
- Ikke et spørgsmål om – om man bliver ramt – men om hvornår. Fokus på minimering af risiko og beredskab til den dag - det sker
- EU-forordningen om databeskyttelse på vej – indeholder både sikkerheds – og privacy krav
- Sikkerhed handler ikke kun om teknik
- Privacy/privatlivets fred er ikke kun jura og politik
- Tværfaglig opgaveløsning – forudsætter en flerhed af kompetencer
- Databeskyttelse og sikkerhed er en risiko som skal indgå i ledelsesopgaven



10 skridt på vejen til forordningen

- 1 Dataklassifikation – relation til kerneforretningen
- 2 Politik for behandling af personoplysninger og privatlivets fred
- 3 Data flow analyse – hvor er persondata
- 4 Program for awareness
- 5 Privacy politik til on-line medier
- 6 Program for databeskyttelsesansvarlig
- 7 Program for håndtering af datasubjekters rettigheder
- 8 Program for anmeldelse af sikkerhedsbrud
- 9 Program for måling og kontrol
- 10 Muligheder for anvendelse af Privacy Enhancing Technologies – PET





Om Deloitte

Deloitte leverer ydelser indenfor Revision, Skat, Consulting og Financial Advisory til både offentlige og private virksomheder i en lang række brancher. Vores globale netværk med medlemsfirmaer i mere end 150 lande sikrer, at vi kan stille stærke kompetencer til rådighed og yde service af højeste kvalitet, når vi skal hjælpe vores kunder med at løse deres mest komplekse forretningsmæssige udfordringer. Deloitte's ca. 200.000 medarbejdere arbejder målrettet efter at sætte den højeste standard.

Deloitte Touche Tohmatsu Limited

Deloitte er en betegnelse for Deloitte Touche Tohmatsu Limited, der er et britisk selskab med begrænset ansvar, og dets netværk af medlemsfirmaer. Hvert medlemsfirma udgør en separat og uafhængig juridisk enhed. Vi henviser til www.deloitte.com/about for en udførlig beskrivelse af den juridiske struktur i Deloitte Touche Tohmatsu Limited og dets medlemsfirmaer.