Henning Mortensen 13. sep. 18

Digital verden post GDPR

Målet!

Beskytte de registreredes fundamentale rettigheder mod vores behandlinger
(Jf. EU's charter om fundamentale rettigheder, artikel 8)

GDPR er bare den laveste fællesnævner (og skal ikke stå i vejen for at gøre det fornuftige)

Vores foranstaltninger i form af teknologi, politikker og procedurer er bare midler til at nå målet

Præ 25. maj

Sikkerhed under GDPR

- Sikkerhed ophøjet til princip, artikel 5 stk. 1, litra f
- Sikkerhedsbekendtgørelsen faldt bort
- Foranstaltninger vurderet ud fra en risikovurdering set fra de registreredes perspektiv
- Specifikke krav om meddelelser ved databrud (tidligere god skik)
- Databehandleraftaler – bl.a. med en række it-leverandører herunder krav til sikkerhed og kontroller
- Løbende dialog med DPO/Jurist
- Dokumentation artikel 5, stk. 2 og artikel 30

Artikel 32: Sikkerhed

- ”passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici”:
  - pseudonymisering og kryptering af personoplysninger
  - evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester
  - evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
  - en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
- Risici: hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
- Præambel 83 giver os ikke meget mere at gå efter

Artikel 32 i praksis

- Lav en risikovurdering hvor scope ikke er organisationens risiko, men i stedet krænkelse af de registreredes rettigheder.
- Iværksæt passende foranstaltninger – f.eks. pseudonymisering og kryptering, men principielt set er der frit valg for den dataansvarlige
- Tilvejebring tilgængelighed, fortrolighed, integritet og robusthed – gennem inspiration fra ISO27001/2
- Vær i stand til at genoprette: backup, beredskabsplan
- Beredskabsøvelse
- **Vi skal altså til at tænke os om!**

Artikel 25: Design

- Passende tekniske og organisatoriske foranstaltninger
- Med henblik på effektiv implementering af **databeskyttelsesprincipper**
- Integrering af de fornødne **garantier** i behandlingen for at **opfylde kravene i forordningen**
- Og beskytte de **registreredes rettigheder**
- F.eks. pseudonymisering

Justitsministeriet om DPbD, indhold

Fra Betænkning 1565, pp. 410-423

•"...en *overvejelsesforpligtelse* og en *håndteringsforpligtelse*..."

•"...udtryk for en risikobaseret tilgang til databeskyttelse, og bestemmelsen angiver kun ganske overordnede retningslinjer for, hvilke typer af tiltag bestemmelsen sigter mod. Dette indebærer, at den dataansvarlige overlades et ganske væsentligt råderum..."

•"Referencen til eksempelvis dataminimering i artikel 25, stk. 1, er ligeledes ikke udtryk for, at der skal foretages en anden vurdering end i dag af, hvorvidt de oplysninger der allerede er i f.eks. et IT-system, bør være der..."

•"Databeskyttelsesforordningens artikel 25 etablerer ikke i sig selv nye krav til den dataansvarlige..."

•"Nyskabelsen i artikel 25, stk.1, består således i, at den dataansvarlige er forpligtet til at *overveje* og *håndtere*..."

R&R-artikler

R&R-artikler

Design-delen

- Designbegrebet gælder principperne, rettighederne, alle garantier og dermed basalt hele forordningen
- Design er ikke kun et spørgsmål om at designe sikkerhedstiltag ind i sine løsninger fra starten
- Design har et materielt indhold som vil blive fastlagt gennem praksis, men som må ligge op af Cavokians designprincipper, for det er herfra begrebet stammer
- Opbakning fra det norske datatilsyns vejledning på området.
- **Det er derfor en nyskabelse!**
- Supplerende casesamling fra RfDS.

R&R-artikler

Sikkerhedsdelen

- Trusler
- Risikovurdering
- Case
- Liste over organisatoriske foranstaltninger
- Liste over tekniske foranstaltninger
- **Operationalisering**

Post 25. maj

Datatilsynet om DPbD

Fra Datatilsynets vejledning

- artikel 25 og 32 er "... forskellige bestemmelser..." (side 2)
- "... en nyskabelse, som er inspireret af Ann Cavoukians 7 principper..." (side 2)
- "... ikke blot handler om at "indbygge" behandlingssikkerhed fra begyndelsen, men tillige indebærer,... at alle forordningens grundlæggende principper... kan overholdes". (side 2)
- "...en *overvejelses- og en håndteringsforpligtelse..."* (side 25)

- **Det er altså en god ide at læse Cavoukians principper og i øvrigt Hoepmans designstrategier.**

Datatilsynet om sikkerhed

Fra Datatilsynets vejledning

•”Der er med forordningen i stedet kommet fokus på en risikobaseret tilgang” (side 7)

•”Som eksempel på en risikobaseret tilgang, der allerede kendes i dag, kan nævnes informations-sikkerhedsstandarden ISO 27001, der er en international standard til styring af informationssikkerhed” (side 8) (eller ISO/IEC 29134 (DPIA))

•”gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de konstaterede risici” (side 11)

Datatilsynet om sikkerhed

Fra Datatilsynets vejledning (foranstaltninger til inspiration)

- Antivirus herunder nye typer antivirus, der også kan detektere nye vira
- Firewall
- Antispam og -phishing filtre
- IDPS (system overvågning og alarmering ved ens perimetersikring)
- Endpointsecurity
- Kryptering
- Logging
- Pseudonymisering / anonymisering
- Sårbarhedsskanning og penetrationstests
- Løbende opdatering af software, herunder vedligeholdelse af systemer ved patching
- IAM systemunderstøttelse
- Adgangskontrol baseret på multi-faktor autentifikation
- Klassifikation af data f.eks. almindelige, fortrolige, hemmelige og top-hemmelige
- Netværkssegmentering og isolering
- Mobile device management
- Backup
- Fysisk sikkerhed
- Shadow IT discovery
- Data discovery
- Data loss prevention
- Secure DNS
- Asset management
- Governance værktøj
- Styring af udstyr på netværket
- DRM
- IT-sikkerhedspolitik
- ISMS (information security manage-ment system)
- Fortegnelse over informationsaktiviteter
- Risikovurdering
- Regelsæt med mapping af GDPR og ISO27002
- Procedurer afledt af regelsæt
  - ...
  - Hændelseshåndtering
  - Beredskab
  - Intern brugerpolitik
  - Privacy notification (ekstern)
  - Data breach notification
  - Styring af leverandører
  - Kontroller
- Træning af medarbejdere og løbende awareness
- Løbende identifikation af regler og praksis
- Identity and access governance (personalesikkerhedsprocedure hos mig)

Praksis

Den overordnede plan

1. **Placering af ansvar, ledelse, CISO/CPO, systemejere**
2. **Indledende awareness**
3. **Den juridiske to-do-liste**
4. **Skab sammenhæng mellem GDPR og ISO27002**
5. **Få overblik over hvilke systemer vi har**
6. **Evaluering af lovlighed i systemer**
7. **Tekniske systemer til overvågning – Hennings ønskeseddel**
8. **Bred awareness**
9. **Uafsluttede projekter**
10. **Følge området og vedligeholde**

Hvor er vi?

- Mange af de formelle tiltag i form af politikker og procedurer er på plads
- Der mangler tekniske tiltag, så GDPR er post 25. maj blevet til en række it-projekter/it-sikkerhedsprojekter
- Der her bliver et evindeligt pendul, som svinger frem og tilbage mellem forretningen og "DPO'en", hvor begge parter "win some and loose some", og hvor ledelsen SKAL involveres og tage beslutningen.

Udfordringer

Sletning

Hvad kan vi lovligt beholde?

- Ordre vs. Faktura
- Elektriske apparater
- Selv strukturerede data ligger ikke kun eet sted i systemerne
- Kan systemerne håndtere sletning

Hvad har vi af ustrukturerede data?

- Hvordan gør vi ustrukturerede data strukturerede, så vi kan anvende en politik
- Anarki versus ESDH og hvis vi får ESDH kan det så slette og ikke kun deaktivere/blokere (Jf. Ashley Madison casen)?
- Modstand mod sletning

Cookiesamtykker og oplysning

Er tredjeparts marketingscookies ulovlige?

Er samtykket tilstrækkeligt oplyst?

Hvad gør vi, når konkurrenterne fortsat miner brugerdata?

Indsigtsbegæring

- Meget bekosteligt
- Behov for automatisering
- Indsigtsknap kan reducere omkostninger og skabe transparens
- Hvad vil vi ikke udlevere under henvisning til artikel 15, stk. 4

Tredjelandsoverførsler

- Parlamentet har bedt om at Privacy Shield suspenderes efter Cambridge Analytica
- Standard Contractual Clauses kommer til præjudiciel forelæggelse ved EU Domstolen
- UK bliver næppe godkendt sikkert tredjeland grundet omfattende overvågningslovgivning
- Retstilstanden for tredjelandsoverførsler er ekstremt usikker, hvilket gør det vanskeligt at tage langsigtede strategiske beslutninger

- Et kuriosum: Fælles dataansvar med Facebook.

Bøderne

- Sikkerhedsbrud hos databehandler
  - Systematisk fejl, som ramte alle kunder
  - Databehandler skal formodentlig have en bøde
  - Vi opdagede det, men de andre kunder har formodentlig også tabt data, skal vi så have en bøde, og hvad med de andre kunder?
- Hvad sker der og hvad koster det?

hmo@ao.dk

https://www.linkedin.com/in/henning-mortensen-343b0/