EN DAG OM PERSONDATAFORORDNINGEN

STU – Foreningen

7. december 2017

Oplæg v/ Peter Sindal Lundsberg
Advokat, underviser, fast værge

Hovedvagtsgade 6, 4. sal
1103 København K
T: 3311 3636
M: 5373 2100
E: psl@petersindal.dk
www.petersindal.dk

Seneste inspektioner

- Inspektion i 16 kommuner i 2016: Datatilsynet udtalte kritik til alle. 'Meget kritisabelt' til 5 kommuner.
- Inspektion i fem regioner i 2016 og 2017: Kritik til alle. 'Meget kritisabelt' udtalt til 2.
- Inspektion i 8 statslige myndigheder i 2017: Kritik til 7. 'Meget kritisabelt' er udtalt til 4 (Beskæftigelsesministeriet, Sunheds- og Ældreministeriet, Vejdirektoratet og Sundhedsdatastyrelsen). Kun Udbetaling Danmark bestod.

Er vi klar til forordningen?

- Undersøgelse fra Opinion/Trend Micro:
- 93% ved de bliver omfattet af persondataforordningen.
- 18% har ikke gjort sig bekendt med de nye regler
- 38% kender ikke bødernes størrelse
- 6% ved ikke de kan få bøder

- Forventningen er er flere end hver anden europæisk virksomhed ikke vil være i stand til at leve op til forordningen ved udgangen af 2018.

Baggrund og anvendelsesområde

- Forordningen erstatter persondatadirektivet og træder i kraft 25. maj 2016 med anvendelse fra 25. maj 2018
- Forordningen har direkte retsvirkning i DK. (Modsat persondatadirektivet der er implementeret i form af persondataloven)
- Adgang til fastsættelse af visse særregler – hvilket vil ske i databeskyttelsesloven (aktuelt i høring)
- Forordningen har grundlæggende samme struktur som persondatadirektivet.
- Dog en række nyskabelser såsom: pligt til en databeskyttelsesrådgiver, ret til at blive glemt, orienteringspligt til Datatilsynet, skærpede sanktioner.
- Personoplysninger omfatter foruden de kendte nu også stemme, fingeraftryk og biometriske data m.v.

Persondatareguleringen i dag

- Databeskyttelsesdirektivet
- Persondataloven (Lov nr. 429 af 31. maj 2000)
- Div. bekendtgørelser og vejledninger. (Fx sikkerhedsbekendtgørelsen og bekendtgørelse om anmeldelse af behandlinger)

Fremtidig regulering

Å EU – persondataforordning

Å Lov om supplerende bestemmelser til EU – Persondataforordningen (Databeskyttelsesloven)

- 54 punkter i forordningen skal reguleres i dansk lov.

Å Div. bekendtgørelser og vejledninger.

- Vejledningerne kommer løbende pt.

Hovedlinjer i persondataforordningen

Større kontrol til den registrerede!

- Ret til detaljeret og klar information om behandlingen af personoplysninger. Herunder om indsamling, opbevaring, sletning og videregivelse.
- Ret til at få berigtiget forkerte oplysninger.
- Ret til sletning af personoplysninger (Retten til at blive glemt).
- Ret til begrænsning i perondatabehandlingen. Begrænsninger ifht. profilering (præferencer, sociale profiler osv.)
- Ret til at få udleveret sine data (dataportabilitet)

- Ret til indsigelse mod behandling.
- Personoplysninger skal registreres og behandles i overensstemmelse med udtrykkeligt angivende og legitime formål.
- Behandling skal være rimelig og gennemsigtig.
- Passende tekniske og organisatoriske sikkerhedsforanstaltninger.
- Sikkerhedsforanstaltninger skal baseres på en dokumenteret risikovurdering.
- Både dataansvarlig og databehandler skal kunne dokumentere opfyldelse af forordningens krav.

- Underretning om brud på persondatasikkerheden til Datatilsynet og evt. den registrerede.
- DPO (Databeskyttelsesrådgiver)
- Administrative bøder på op til 20 mio. Euro eller 4 % af den globale omsætning.

Centrale begreber

- Personoplysninger – alle oplysninger om en identificeret eller identificerbar person (forstås bredt) – kendt fra pdl. Art. 4 (1)
- Behandling – en hver aktivitet hvor personoplysninger anvendes (forstås bredt) – kendt fra pdl. Art. 4 (2)
- Register – kendt fra pdl. Art. 4 (6)
- Dataansvarlig – kendt fra pdl. Art. 4 (7)
- Databehandler – kendt fra pdl. Art. 4 (8)
- Samtykke – frivillig, spcifik, informeret og utvetydig viljestilkendegivelse – stiller øgede krav til dokumentation og information. Art. 4 (11)

Drøft med sidemanden – 5 min.

- Hvilke personoplysninger behandler vi?

Grundlæggende behandlingsbetingelser!

- Art. 5 – er i vidt omfang identisk med pdl. § 5.
- Den grundlæggende betingelser skal overholdes hver gang personoplysninger behandles
- God databehandlingsskik, formålsangivelse og saglighed, proportionalitet, dataminimering, datakvalitet, tidsbegrænsning, sikkerhed.

Å Lovlighed

- Baseret på forordningen, særlovgivning eller samtykke.

Å Rimelighed

- Tilstrækkeligt, relevant og korrekt.
- Kun de nødvendige oplysninger.
- Ikke opbevares længere end nødvendigt.

Å Gennemsigtighed

- Registrerede skal oplyses om: rettigheder, formål, grundlag for behandlingen, tidspunkt for sletning.

Lidt om samtykke

- Frivilligt
- Specifikt
- Utvetydigt
- Viljestilkendegivelse (ikke passivitet)
- Krav om at samtykkeerklæringer skal have oplysninger om: dataansvarliges identitet, formålet med behandlingen, oplysninger om adgang til tilbagekaldelse (art. 7, (3))

- Børns samtykke
- Børn fra 13 år kan selvstændigt samtykke

Almindelige personoplysninger

- Art. 6
- Navn, adresse, sygedage, cpr, indtægt, væsentlige sociale problemer m.v.
- Behandlingsbetingelser er:
- samtykke, art. 6 (1a)
- Kontrakt, art. 6 (1b) – fx ansættelseskontrakt – særregel i databeskyttelsesloven
- Retlig forpligtigelse, art. 6 (1c) – fx afgørelser
- Vitale interesser, art. 6 (1d) - værdispring
- Samfundsinteresser eller offentlig myndighedsudøvelse, art. 6 (1e) - myndighedsudøvelse
- Interesseafvejningsreglen, art. 6 (1f) – værdispring – gælder ikke for offentlige myndigheder

Følsomme personoplysninger

- Art. 9
- Race, etnicitet, politisk. religiøs, filosofisk overbevisning, fagforening, genetiske, biometriske data, helbredsoplysninger, seksuelle forhold
- Ligner til dels pdl. § 7.
- Behandlingsbetingelser er:
- Forbud, art. 9 (1)
- Undtagelser er:
- Samtykke, art. 9 (2a)
- Arbejdsret, sundhedsret, socialret, art. 9, (2b)
- Foreninger m.v., art. 9 (2d)
- Offentliggjort af den registrerede, art. 9 (2e)
- Retskrav, art. 9 (2f)
- Væsentlige samfundsinteresser, art. 9 (2g)
- Sundhedssektoren, art. 9 (2h)
- Folkesundhed, art. 9 (2i)
- Arkivering, forskning, art. 9 (2j)

Særlige situationer

- Å Art. 10
- Å Straffedomme
- Å Art. 87
- Å cpr.

Drøft med sidemanden – 10 min.

- Å Hvilken lovhjemmel kan I henvise til når I behandler personoplysninger?
- Å Indsamles der flere oplysninger end nødvendigt for at udføre jeres opgave?
- Å Hvornår slettes indsamlede og registrerdede oplysninger?
- Å Er borgeren bekendt med formålet med behandlingen?
- Å Har borgeren modtaget oplysninger om sine rettigheder?

Oplysningspligten

- Oplysningspligten
- Indsamlet hos borgeren, art. 13
- Dataansvarliges identitet
- Kontaktoplysninger på databeskyttelsesrådgiver (ny)
- Formål med behandlingen (udvidet)
- Retsgrundlaget for behandlingen
- Hvis interesseafvejningsreglen anvendes – da krav om redegørelse for de saglige interesser.
- Modtagerer/kategoriere af modtagere
- Tredjelandsoverførsler og hjemmel (ny)
- Opbevaringsperiode (ny)
- Oplysninger om rettigheder
- Evt. adgang til tilbagekaldelse af samtykke (ny)
-
- Indsamlet hos andre, art. 14

Rettigheder

- Indsigtsretten Art. 15.
- Visse skærpelser i form af pligtig til oplysninger om klageret og brug af automatiserede afgørelser.
- Berigtigelse Art. 16
- Sletning - Retten til at blive glemt Art. 17.
- Ret til begrænsning af behandling, art. 18

- Dataportabilitet – Art. 20
- Ret til flytning af personoplysninger til ny databehandler. (offentlige myndigheder er undtaget)

- Indsigelse mod behandling Art. 21

- Automatiske individuelle afgørelser – Art. 22
- Ret til at protestere mod automatiske oplysninger hvis behandlingen skal baseres på konkret vurdering af personoplysninger.

Den dataansvarliges ansvar

- Å Dokumentation for at forordningen overholdes – krav til sagsbehandlingsprocedure. Art. 24
- Å Krav om fortegnelser over behandlingsaktiviteter Art. 30
- Å Krave om passende interne databeskyttelsespolitikker/sikkerhed Art. 25
- Å Indgåelse af databehandleraftaler Art. 28 (3)
- Å Anmeldelse af brud på persondatasikkerheden Art. 33 og 34.

Behandlingssikkerhed

Å Implementering af tekniske og organisatoriske sikkerhedsforanstaltninger.

- Passende sikkerhedsniveau herunder også tilgængelighed og robusthed af behandlingssystemer og tjenester.
- Implementering af databeskyttelsespolitikker, sikkerhedsregler og instrukser der årligt skal gennemgås og tilpasses, baseret på risikovurderingen.
- Tilrettelæggelse og gennemførelse af uddannelse og interne awarness kampagner.

Risikovurdering Art. 35

Å Fortegnelse over behandlingsaktiviteter

Å Tilrettelæggelse af behandlingsskikkerhed:

- Behandlingens karakter, omfang, sammenhæng og formål.
- Aktuelle tekniske niveau

Å Identifikation af risici

Å Fastlæggelse af sikkerhedsniveauet

Drøft med sidemanden – 10 min.

- Å Hvilken sikkerhedsforanstaltninger har I?
- Å Kendskab til sikkerhedsforanstaltningerne?
- Å Kendskab til instruks?
- Å Overholdes sikkerhedsforanstaltningerne?

DPO

Å Art. 37 – 39

- Obligatorisk for offentlige myndigheder.
- Underretning og rådgivning om pligter i henhold til forordningen.
- Samarbejde med tilsynsmyndigheden mv.

Å Evt. delt DPO

Lidt om databehandleraftaler

- Art. 28
- Skriftlig kontrakt skal indgås mellem den dataansvarlige og databehandleren.
- Regulering af genstand for og varigheden af behandlingen, karakter og formål, typen af personoplysninger og kategori af registrerede. Samt dataansvarliges pligter og rettigheder.
- Behandling skal ske efter dokumenteret instruks.
- Krav om fortrolighed eller underlagt tavshedspligt.
- Sletning eller returnering af alle persondata.
- Adgang til nødvendige oplysninger med henblik på dokumentation for overensstemmelse med forordningen.

Brud på persondatasikkerheden Art. 33 og 34

Å Procedure for rettidig anmeldelse af brud på datasikkerhed.

Å Anmeldelse hurtigst muligt og indenfor 72 timer.

Å Anmeldelse skal min. indeholde:

- Karakter af bruddet (kategori af registrerede, personoplysninger og antal berørte).
- Kontaktoplysninger
- Sandsynlige konsekvenser
- Foranstaltninger

Lidt gode råd

1) Gå ikke i panik!
2) Behandling af personoplysninger – Lovlig (lovbestemmelse eller samtykke) og begrænset til det nødvendige. Og må ikke opbevares længere end nødvendigt.
3) Instruks om behandlingen (oplæring af personale)
4) Fysiske papirer og arkiver – opbevares aflåst når de ikke anvendes. Og makulering.
5) Adgang til personoplysninger – kun adgang for personer med arbejdsbetinget behov, adgangskode til pc som ikke må overlades til andre.

6) Opdateret IT system, firewall og viruskontrol

7) Eksterne datamedier (fx USB) krav om beskyttelse (kryptering)

8) Reparation og service af dataudstyr – krav om forødende foranstaltninger så persondata ikke kommer til uvedkommende.

9) Eksterne databehandlere – krav om databehandleraftaler.

10) Videregivelse af personoplysninger – i henhold til lovgivning eller samtykke.

11) Dokumentation – fortegnelse, risikovurdering, beskrivelse af beskyttelse af personoplysninger.

Spørgsmål?