Stormøde om databeskyttelsesforordningen - og betænkning nr. 1565

13. juni 2017

JUSTITSMINISTERIET

Dagens program

12.00-12.10: Velkomst ved *afdelingschef Jens Teilberg Søndergaard (Justitsministeriet)*

12.10-12.20: Digitaliseringsstyrelsens vinkel på betænkningen ved *direktør Lars Frelle-Petersen*

12.20-12.30: Erhvervsstyrelsens vinkel på betænkningen ved *direktør Betina Hagerup*

12.30-12.50: Datatilsynets vinkel på betænkningen og det fremtidige tilsyn ved *direktør Cristina Gulisano*

12.50-13.00: Pause

13.00-13.15: Hovedkonklusionerne i betænkningen ved *kommitteret Jens Møller (Folketingets Ombudsmand)*

13.15-13.50: Centrale nedslagspunkter i betænkningen ved Jakob Lundsager og Anders Lotterup *(Justitsministeriet)*

13.50-14.00: Den videre proces ved *afdelingschef Jens Teilberg Søndergaard*

JUSTITSMINISTERIET

DIGITALISERINGSSTYRELSEN

Betænkning om databeskyttelsesforordningen

v/Direktør Lars Frelle-Petersen

Juni 2017

DIGITALISERINGSSTYRELSENS FOKUS

Værdiskabende brug af data

- Eksempelvis: cloud computing, registersamkøring, pragmatisk tilgang til fortegnelseskravet og råderum for fastsættelse af særregler om datadeling

Informationssikkerhed

- Primært: ISO 27001

DIGITALISERINGSSTYRELSEN

KONKLUSIONER FRA ARBEJDET

På en lang række punkter ingen store forskelle mellem databeskyttelsesforordningen og gældende ret.

- Fortsat adgang til at anvende personoplysninger til at skabe værdi efter maj 2018.
- God balance mellem hensynet til beskyttelsen af individets rettigheder og hensynet til, at vi som samfund kan forløse det potentiale, som brugen af ”Big Data”, moderne analyseredskaber, registerbaseret forskning mv. rummer.

DET FREMADRETTEDE ARBEJDE

Styrelsens prioriteter i arbejdet med vejledninger:

- God kobling til digitaliseringsstrategiens centrale emner så som privacy by design, brugen af cloud computing og datadeling.
- At forpligtelser under forordningen kan mødes på en hensigtsmæssig og ressourceeffektiv måde.

DIGITALISERINGSSTYRELSEN

Erhvervsstyrelsens vinkel på betænkningen

ved *direktør Betina Hagerup*

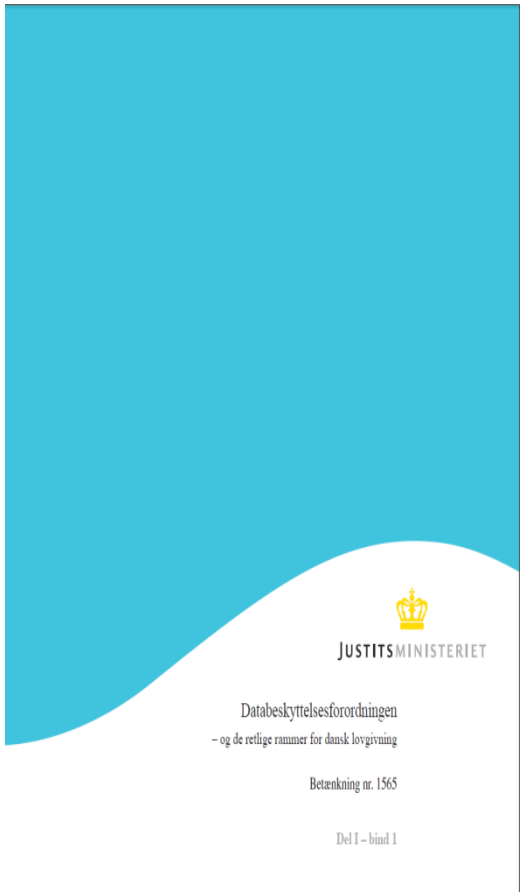
DATATILSYNET

Stormøde den 13. juni 2017

Datatilsynets vinkel på betænkningen og det fremtidige tilsyn

v/ direktør Cristina Angela Gulisano

24. maj 2017 – Justitsministeriets betænkning



Hvem fortolker også ?

- Retningslinjer og fortolkningsbidrag fra navnlig Det Europæiske Databeskyttelsesråd (EDPB) og Datatilsynet
- EU-Domstolens retspraksis – flere milepælsdomme
- Kommissionen kan udstede delegerende retsakter på to områder (artikel 92)
  - Standardiserede ikoner for oplysningspligt (artikel 12, stk. 8)
  - Certificeringsmekanismer (artikel 43, stk. 8)

Artikel 29-gruppen

- Etablering af Det Europæiske Databeskyttelsesråd
- Forberedelser ifht OSS og sammenhængsmekanisme
- 3 vejledninger er udgivet (kommer i en dansk udgave) (dataportabilitet, DPO og ledende tilsynsmyndighed)
- Vejledning om DPIA og høj risiko har været i høring
- Færdiggørelse af 2 vejledninger (administrative bøder og certificering)
- Opstart på 3 yderligere vejledninger (samtykke, profilering og gennemsigtighed)

Hvad så nu ?

- Vejledning, vejledning og atter vejledning
- Datatilsynet skal have forberedt sig – bl.a.:
  - En del nye opgaver (bl.a. sikkerhedsbristanmeldelser, konsekvensanalyser, DPO, adfærdskodekser og certificering, håndhævelse og det internationale)
  - Organisatorisk - det ”nye” Datatilsyn – bl.a. en ny hjemmeside
  - Og så skal vi jo også selv overholde!

DATATILSYNET

Maj 2016 – hjemmeside

DATATILSYNET

Juni 2016 – 12 spørgsmål

Oplæg ved kommitteret Jens Møller, Folketingets Ombudsmand

Ekspertreferencegruppens arbejde med betænkning nr. 1565 om databeskyttelsesforordningen

Arbejdet i ekspertreferencegruppen

- Medlemmer: professor Peter Blume, professor Henrik Udsen og IT-ekspert, ph.d. Gert Læssøe Mikkelsen og undertegnede
- Ikke traditionelt lovforberedende udvalgsarbejde (ikke tid til det)
- Ekspertreferencegruppen er løbende blevet forelagt notater efter, at de var blevet godkendt i projektgrupperne
- Notaterne er nu sammenstillet i betænkning nr. 1565, der skal danne grundlag for det videre arbejde med ny persondatalov og nye vejledninger
- Notaterne er opbygget ens med en gennemgang af *gældende ret*, fortolkning af *forordningen* og et *overvejelsesafsnit*

Arbejdet i ekspertreferencegruppen

- Vi har holdt ca. 13 møder i perioden oktober 2016-maj 2017 med Justitsministeriet om notaterne

- Vi har været inddraget i praktisk talt alle betænkningens beskrivelser af gældende ret og fortolkninger af forordningen

- Slutresultat: Der er taget højde for ekspertreferencegruppens bemærkninger, som er indarbejdet i betænkningen.

Betænkningens centrale pointer

- Databeskyttelsesforordningen svarer i stort omfang til den gældende retstilstand efter persondataloven og databeskyttelsesdirektivet med tilhørende praksis fra bl.a. EU-Domstolen

- Det gælder f.eks. centrale områder som
  - reglernes anvendelsesområde
  - definitioner
  - krav til lovlig behandling af personoplysninger
  - de registreredes rettigheder og
  - behandlingssikkerhed

Betænkningens centrale pointer

- Derudover indeholder forordningen nyskabelser, eksempelvis regler om:
  - databeskyttelsesrådgivere (DPO'ere),
  - konsekvensanalyse,
  - fortegnelser over behandlingsaktiviteter og
  - samt en udtrykkelig bestemmelse om "data protection by design".

- Forordningen har oplagt skabt "awareness" for reglerne – givetvis bl.a. pga. risikoen for større bøder for overtrædelse af forordningens bestemmelser

- Men analysearbejdet viser tydeligt, at der med de nye regler alene er tale om en evolution – *ikke* en revolution

Betænkningens centrale pointer

Eksempel på ”knast” vi skulle løse:

- Er det – i lyset af, at der nu er tale om en forordning – muligt at opretholde den omfangsrige danske særregulering af lovlig behandling af personoplysninger?

- Svar: ja, forordningen indeholder et bemærkelsesværdigt stort rum for national regulering og svarer på dette område således nærmest til et direktiv

Databeskyttelsesforordningen set fra en praktikers synspunkt

Fire vigtige kasser:

- Er vi inden for forordningens anvendelsesområde?
- Er der hjemmel til behandlingen? Er de grundlæggende principper overholdt?
- Håndtering af registreredes rettigheder
- Behandlingssikkerhed

Afslutning

- Databeskyttelse har med forordningen tydeligvis fået forstærket opmærksomhed
- Og det er vigtigt
- Der er jo tale om en grundlæggende rettighed

Centrale nedslagspunkter i betænkning nr. 1565 om databeskyttelsesforordningen

JUSTITSMINISTERIET

5 centrale nedslagspunkter i betækningen

- Databeskyttelsesforordningen svarer i vidt omfang til gældende ret – ingen revolution
- Databeskyttelsesrådgivere
- Fortegnelse over behandlingsaktiviteter
- Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger
- Databehandleres mere fremtrædende rolle

Forordningen svarer i vidt omfang til gældende ret – ingen revolution

JUSTITSMINISTERIET

Forordningens art. 5 svarer til persondatalovens § 5

- De grundlæggende principper for lovlig behandling i forordningens artikel 5 svarer til de gældende principper

- lovlighed, rimelighed og gennemsigtighed
- formålsbegrænsning
- dataminimering
- rigtighed
- opbevaringsbegrænsning
- integritet og fortrolighed

Forordningen svarer i vidt omfang til gældende ret

- Anvendelsesområde
- Definitioner
- Hjemmel til behandling for almindelige og følsomme personoplysninger i artikel 6 og 9
- De registreredes rettigheder svarer også stort set til de gældende regler
- Behandlingssikkerhed
- Overførsel til tredjelande
- Erstatning

Forordningens nationale råderum

- Forordningens artikel 6, stk. 2 og 3, artikel 9, stk. 2, og særligt præambelbetragtning nr. 10

- Der er et meget vidt råderum for medlemsstaterne til at opretholde + indføre nationale regler om behandling af personoplysninger

- F.eks. regler om indsamling, videregivelse, tavshedspligt mv.

- Betænkningens del II: gennemgang af de mange danske særregler om behandling, f.eks. lov om finansiel virksomhed m.fl.

Databeskyttelsesrådgivere

JUSTITSMINISTERIET

Udpegning af en databeskyttelsesrådgiver

- Offentlige myndigheder *skal* altid udpege en databeskyttelsesrådgiver

- I de fleste tilfælde *skal* private virksomheder *ikke* udpege en databeskyttelsesrådgiver

Hvornår skal en privat virksomhed alligevel udpege en databeskyttelsesrådgiver?

Følgende 3 betingelser skal alle være opfyldt for, at en *privat* virksomhed har pligt til at udpege en databeskyttelsesrådgiver:

1. Behandling af personoplysninger skal være virksomhedens *kerneaktivitet*
2. Der skal behandles personoplysninger i *et stort omfang*
3. Behandlingsaktiviteten består i *regelmæssig* og *systematisk overvågning* af personer eller behandlingen vedrører *følsomme oplysninger*, herunder oplysninger om strafbare forhold (artikel 9- og 10-oplysninger)

Databeskyttelsesrådgiveren

- Skal udpeges pba. sine faglige kvalifikationer, ”navnlig ekspertise inden for databeskyttelsesret og –praksis” samt evne til at udføre opgaverne som databeskyttelsesrådgiver

- Databeskyttelsesrådgiveren kan både være intern og ekstern

- Får en central *rådgivnings*- og *overvågningsrolle* i organisationen. Uddannelse af ledelse og medarbejdere.

- Inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger

- Skal være uafhængig, rapporterer til øverste ledelsesniveau

Hvem i organisationen *må* være databeskyttelsesrådgiver?

- Databeskyttelsesrådgiveren *skal* inddrages rettidigt i "alle spørgsmål"
- Databeskyttelsesrådgiveren kan ikke være afskåret fra at være en *aktiv del* af overvejelserne og beslutningerne om, hvordan compliance sikres
- Databeskyttelsesrådgiveren kan og skal således inddrages i organisationens *implementering* af de krav, der følger af forordningen
- F.eks. ifm. indkøb af nyt IT-system og formulering af kravspecifikationer til leverandører
- Kan være organisationens *compliance officer*

Hvem i organisationen må *ikke* være databeskyttelsesrådgiver?

- Databeskyttelsesrådgiveren kan ikke samtidigt være øverste *ansvarlig* for organisationens lovlige behandling af personoplysninger

- Dvs. databeskyttelsesrådgiveren kan ikke f.eks. være den *øverste* IT-ansvarlige eller *øverste* HR-ansvarlige i organisationen

Databeskyttelsesrådgiveren er beskyttet mod afskedigelse

- Må ikke afskediges for udførelse af opgaverne som databeskyttelsesrådgiver, jf. artikel 38, stk. 3, 2. pkt.

- Bestemmelsen sigter på en alm. saglighedsbeskyttelse som efter funktionærloven

- Databeskyttelsesrådgiveren vil kunne afskediges på et *sagligt* grundlag efter almindelige arbejdsretlige regler. Overtrædelse af artikel 38, stk. 3, 2. pkt.-beskyttelsen kan medføre bødestraf efter artikel 83, stk. 4, litra a

Fortegnelse over behandlingsaktiviter, artikel 30

JUSTITSMINISTERIET

Nyt krav om fortegnelse over behandlingsaktiviteter

- Forordningens risikobaserede tilgang og fokus på ansvarlighed (”accountability”)
- Ny pligt om at føre fortegnelse over behandlingsaktiviteter
- Erstatter anmeldelsespligten efter de gældende regler

Fortegnelseskravet

- Fortegnelsespligten er en *intern* pligt for dataansvarlige og databehandlere

- Eventuelle tidligere anmeldelser til Datatilsynet kan i vidt omfang genbruges som fortegnelse

- Ingen særlige formkrav til fortegnelsen – udover skriftligt og elektronisk

Fortegnelseskravet

- Eksempel i betænkningen på, hvordan en fortegnelse kan laves
- Kravet er ikke tiltænkt som en ”belastning” og medfører ikke i sig selv et krav om udarbejdelse af større analyser af datastrømme mv.
- Det følger dog som hidtil, at den dataansvarlige skal leve op til princippet om ”dataminimering”, dvs. man må ikke behandle oplysninger unødigt
- Stadig kunne håndtere f.eks. indsigtsbegæringer

Databeskyttelse gennem design og gennem standardindstillinger

JUSTITSMINISTERIET

Databeskyttelse gennem design, artikel 25, stk. 1

- Indebærer en *overvejelsesforpligtelse* og en *håndteringsforpligtelse* for den dataansvarlige til allerede i forberedelsesfasen at indtænke de relevante foranstaltninger til sikring af overholdelse af databeskyttelsesforordningen.

- Artikel 25, stk. 1, indebærer en pligt for den dataansvarlige til at inddrage tiltag, der konkret fremmer en effektiv implementering af forordningens databeskyttelses-principper i artikel 5 og dens øvrige regler.

- Artikel 32 om behandlingssikkerhed m.fl. skal i forvejen overholdes fra ”dag 1”

Databeskyttelse gennem design, artikel 25, stk. 1

- Fremtidige it-systemer skal designes med henblik på effektiv implementering af databeskyttelsesprincipper – f.eks. dataminimering

  – F.eks. hvis den dataansvarlige selv udvikler et system, vil dette kunne afhjælpes ved at indarbejde *Privacy Enhancing Technologies*

  – F.eks. ved at stille krav herom til leverandøren af et it-system

Databeskyttelse gennem design, artikel 25, stk. 1

- Der er *ikke* krav om, at eksisterende systemer **skal** re-designes
- Større ændringer i eksisterende systemer *kan* kræve tilpasninger:
  - OBS: organisatoriske foranstaltninger vil kunne være *tilstrækkelige*, hvis dette kan etablere et passende sikkerhedsniveau for behandlingen af personoplysninger f.eks. interne procedurer og undervisning af ansatte
  - OBS: tekniske ændringer ses i forhold til implementeringsomkostninger

Databeskyttelse gennem standardindstillinger, art. 25, stk. 2

- **Fremtidige systemers** standardindstillinger skal indstilles, så de fremmer dataminimering og formålsspecifik behandling
- **Eksisterende it-systemer** hvor standardindstillingerne *ikke* kan ændres:
  - Ingen nye krav til it-systemet pr. den 25. maj 2018
- **Eksisterende it-systemer** hvor standardindstillingerne *kan* ændres:
  - Virksomheden er pr. den 25. maj 2018 forpligtet til at ændre systemets standardindstillinger på en måde, der understøtter forordningens krav om bl.a. formålsspecifik behandling

Databehandleres mere fremtrædende rolle

JUSTITSMINISTERIET

Databehandlere har mere fremtrædende rolle i forordningen

- Databehandleren får nye forpligtelser med forordningen, f.eks:
  - Fortegnelser over behandlingsaktiviteter
  - Underretning ved sikkerhedsbrister
  - Evt. databeskyttelsesrådgiver

Databehandlere har mere fremtrædende rolle i forordningen

- Flere og mere detaljerede krav til databehandleraftaler
- Eksplicitte betingelser for, hvornår en databehandler må benytte sig af underdatabehandlere
- Kan ifalde erstatningsansvar over for de registrerede personer
- Kan ifalde bødeansvar

Den videre proces

JUSTITSMINISTERIET

Vejledninger

- Betænkningen vil ikke komme til at stå alene
- Centralt med praktisk anvendelige vejledninger
- Disse vil blive udarbejdet i samarbejde mellem bl.a. Justitsministeriet, Digitaliseringsstyrelsen og Datatilsynet
- Fokus på eksempler

Vejledninger

• Generel informationspjece om forordningen	september 2017
• Databeskyttelsesrådgiver	september 2017
• Vejledning om overførsler af personoplysninger til 3. lande	september 2017
• Databehandlere og dataansvarlige	oktober 2017
• Samtykke	oktober 2017
• Fortegnelse	november 2017
• Adfærdskodekser og certificeringsordninger	december 2017
• Behandlingssikkerhed	december 2017
• Databeskyttelse gennem design og standardindstillinger	december 2017
• Konsekvensanalyse	december 2017
• Cloud computing	december 2017
• Håndtering af brud på persondatasikkerhed	januar 2018
• Registreredes rettigheder	januar 2018

Fremover

- Lovforslag til ny persondatalov sendes i høring inden sommerferien
- Andet lovforslag med konsekvensændringer i særlovgivningen efter sommerferien
- Fremsættelse for Folketinget til efteråret
- Politisk behandling

Stormøde om databeskyttelsesforordningen - og betænkning nr. 1565

13. juni 2017

JUSTITSMINISTERIET