Stormøde om databeskyttelsesforordningen
9. februar 2017

JUSTITSMINISTERIET

Dagens progam

13.00-13.15: Velkomst *v/Jens Teilberg Søndergaard (Justitsministeriet)*

13.15-13.30: Efterårets workshopforløb med erhvervslivet *v/Katrine Winding (Erhvervsstyrelsen)*

13.30-14.00: Q&A om DPO for private

Q&A om databeskyttelse gennem design og gennem standardindstillinger

14.00-14.20: Pause

14.20-14.50: Q&A om konsekvensanalyse

Q&A om dataansvarlige og databehandlere

Q&A om personoplysninger, behandlingshjemler og håndtering af de registreredes rettigheder

14.50-15:10: Spørgsmål fra salen *(Justitsministeriet og Erhvervsstyrelsen)*

15.10-15.20: Den fremadrettede proces *(Justitsministeriet)*

JUSTITSMINISTERIET

Q&A om DPO for private

JUSTITSMINISTERIET

Q Hvornår skal private udpege en databeskyttelsesrådgiver?

- Private virksomheder *skal* i visse situationer udpege en DPO – men kun når visse særlige forhold gør sig gældende for virksomheden (artikel 37, stk. 1, litra b-c)

- I de fleste tilfælde vil private virksomheder således *ikke* skulle udpege en DPO

- Private virksomheder *kan* i øvrigt frivilligt vælge at udpege en DPO (artikel 37, stk. 4)

Q Hvornår skal private udpege en DPO?

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

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)

Q Hvornår er der tale om ”kerneaktivitet”?

- Begrebet ”kerneaktiviteter” går på, at behandlingen af personoplysninger er virksomhedens *hovedaktivitet*

- Hvis behandlingen af personoplysninger er en *biaktivitet*, skal der *ikke* udpeges en DPO (betyder, at de fleste private virksomheder ikke skal have en DPO)

- Afgørende skillelinje: *Består* virksomhedens produkt eller tjeneste i behandling af personoplysninger eller er aktiviteterne *uløseligt* forbundet hermed? Hvis ja: hovedaktivitet

Q Hvornår er der tale om ”kerneaktivitet”?

- Eksempler på hovedaktiviteter (kerneaktiviteter)
  - Hosting eller lagring af oplysninger, herunder cloud-udbydere
  - Udbydere af marketingsundersøgelser

  - Forsikringsselskab (forsikringsydelsen uløseligt forbundet med behandlingen af personoplysninger)
  - Privathospital (patientbehandling uløseligt forbundet med journalbehandling)

Q Hvornår er der tale om ”kerneaktivitet”?

- Eksempler på biaktiviteter
  - kundekontakt,
  - support/salg,
  - personaleadministration (ofte inkl. helbredsopl. og oplysninger om fagforeningsmæssige forhold),
  - IT-support,
  - advokatfirmaers behandling af klient-oplysninger

- På trods af, at sådanne behandlinger er vigtige for virksomheden, er der ikke tale om *hoved*aktivitet

Q Hvornår er der tale om behandling ”i et stort omfang”?

- Ikke noget direkte i forordningen herom, men der må skulle en del til (kerneaktivitet ikke nok)

- Art. 29-gruppen har gode bud på relevante momenter:

  – Antallet af personer, der behandles oplysninger om
  – Mængden af data
  – Varigheden af behandlingen, herunder hvorvidt den er permanent
  – Den geografiske udstrækning af behandlingsaktiviteterne

Q Hvornår er der tale om behandling ”i et stort omfang”?

Ikke behandling i et stort omfang

- En advokats behandling af personoplysninger
- En praktiserende læges behandling af oplysninger

Behandling i et stort omfang

- Privathospitaler
- Forsikringsselskaber
- Fagforeninger
- Rejsekortet

Q Hvornår er der tale om ”regelmæssig og systematisk overvågning af de registrerede”?

- *Overvågning* omfatter sporing/profilering af personer mhp. at kortlægge f.eks. præferencer, adfærd og holdninger

- ***Eksempler***
  - Drift af et telekommunikationsnetværk
  - Kreditvurderinger
  - Lokations-tracking, f.eks. via apps
  - Adfærdsbaseret markedsføring
  - Smart Cars

Q Hvornår er der tale om behandling af følsomme oplysninger eller oplysninger om strafbare forhold?

- Følsomme oplysninger, artikel 9:
  - Race eller etnisk oprindelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmæssigt tilhørsforhold
  - Biometrisk data med formål om identifikation
  - Helbredsoplysninger og om seksuelle forhold

- Strafbare forhold, artikel 10:
  - Oplysninger om straffe- og børneattest

Q <u>Kort opsamling</u>: hvornår skal private udpege en DPO?

- Der skal meget til:
  - Kerneaktivitet
  - Stort omfang
  - Regelmæssigt/systematisk overvågning *eller* følsomme oplysninger (artikel 9)/oplysninger om strafbare forhold (artikel 10)
- Hvad gør man, hvis man ikke er omfattet af kravet?

  Kræver ikke noget selvstændigt skridt – man skal dog altid kunne "påvise" overholdelse af forordningen (accountability). Ens overvejelser kan i tvivlstilfælde f.eks. dokumenteres i et internt notits.

Q Gælder DPO-kravet både dataansvarlige og data-behandlere?

- Ja, både private dataansvarlige og databehandlere skal udpege en DPO, *hvis* betingelserne er opfyldt

- Kan indebære, at begge eller alene én skal have en DPO (eller ingen af parterne, naturligvis)

- F.eks. lille virksomhed (dataansvarlig) og den store cloud-leverandør (databehandler)

Q Stilles der uddannelsesmæssige krav til en DPO?

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

- Der stilles *ikke* krav om bestemt uddannelsesmæssig baggrund, såsom f.eks. jurist

- Sigtes til en person med juridiske kompetencer inden for databeskyttelsesret + en vis praktisk erfaring

- Niveauet afhænger af mængden, følsomheden og kompleksiteten af data

Q Hvem kan varetage rollen som DPO?

- En af virksomhedens *medarbejdere*
  - Må dog ikke medføre interessekonflikt (mere om lidt)

- En *koncern* kan udpege en "fælles databeskyttelsesrådgiver" for hele koncernen, forudsat at alle etableringer af koncernen har let adgang til DPO'en

- En *ekstern* på baggrund af en tjenesteydelseskontrakt
  - F.eks. en advokat eller en revisor. Interessekonflikt må afgøres af relevante habilitetsregler, såsom de advokatetiske regler

Q Hvad skal DPO'en lave?

- Får en central *rådgivnings-* og *overvågningsrolle* i organisationen. Uddannelse af ledelse og medarbejdere.
- Både forordningen og nationale regler om databeskyttelse
- Skal være kontaktpunkt for de registrerede (kontaktopl. skal offentliggøres)
- DPO'en tager, ifm. prioritering af opgaverne, hensyn til risici forbundet med behandlingsaktiviteterne

Q Hvad ligger der i DPO'ens uafhængige position?

Nedslag fra artikel 38:

- Skal inddrages "tilstrækkeligt og rettidigt i alle spørgsmål vedrørende" databeskyttelse
- Skal have tilstrækkelige ressourcer + tid til rådighed, være tilgængelig
- Må ikke modtage instrukser eller afskediges/straffes for at udføre sine DPO-opgaver
- Rapporterer til det *øverste* ledelsesniveau
- Kan udføre andre opgaver, der dog ikke må medføre en *interessekonflikt*

Q Hvad ligger der i DPO'ens uafhængige position?

- Skal f.eks. inddrages i spm. om *databeskyttelse gennem design*, *behandlingssikkerhed* og håndtering af registreredes *rettigheder*

- …i så god tid, at det er muligt at tage højde for DPO'ens rådgivning

- Må ikke direkte eller indirekte få besked på at komme til et "bestemt resultat", når vedkommende opererer som DPO

Q Hvad ligger der i DPO'ens uafhængige position?

Hvem i organisationen kan så ikke være DPO?

- DPO'en kan ikke samtidigt være øverste *ansvarlig* for organisationens lovlige behandling af personoplysninger

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

Q Hvad ligger der i DPO'ens uafhængige position?

Omvendt er der "grænser for begrænsningerne"

- DPO'en *skal* inddrages rettidigt i "alle spørgsmål"
- DPO'en kan ikke være afskåret fra at være en *aktiv del* af overvejelserne og beslutningerne om, hvordan compliance sikres
- DPO'en 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
- F.eks. ifm. udarbejdelse af organisationens data-politikker
- Kan være organisationens *compliance officer*

Q Er en DPO ansvarlig for brud på reglerne om databeskyttelse?

- En DPO kan *ikke* gøres personlig ansvarlig for en virksomheds manglende overholdelse af databeskyttelseslovgivningen

Det er *altid* virksomhedens ansvar, at behandlingen af personoplysninger sker lovligt, jf. artikel 5, stk. 2, og artikel 24 (den dataansvarlige skal kunne "påvise" compliance)

Q Har en DPO en særlig ansættelsesretlig beskyttelse?

- Må – som nævnt – ikke afskediges eller straffes for udførelse af DPO-opgaverne, jf. artikel 38, stk. 3, 2. pkt.

- Normalt kan man dog i DK ikke afskediges for at udføre sine arbejdsopgaver. Bestemmelsen sigter på en alm. saglighedsbeskyttelse som efter funktionærloven

- DPO'en 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

Q&A om databeskyttelse gennem design og gennem standardindstillinger

JUSTITSMINISTERIET

Q Hvad er databeskyttelse gennem design, artikel 25, stk. 1?

- Det er *ikke* en forpligtelse til noget bestemt, såsom et nyt selvstændigt sikkerhedskrav

- Det består af en generel *overvejelsesforpligtelse* og en *håndteringsforpligtelse* for den dataansvarliges virksomhed til:
  - i forberedelsesfasen at overveje, hvilke foranstaltninger der skal håndteres ved en behandling af personoplysninger for at efterleve databeskyttelsesretten

Q Hvad er 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

Q Hvad er 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

Q Hvad er databeskyttelse gennem standardindstillinger, artikel 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

Q&A om konsekvensanalyse

JUSTITSMINISTERIET

Q Hvornår er der krav om gennemførelse af en konsekvensanalyse?

- De fleste behandlinger af personoplysninger vil *ikke* være omfattet af kravet om en konsekvensanalyse

- Dog når en type behandling af personoplysninger sandsynligvis vil indebære en *høj risiko* for fysiske personers rettigheder og frihedsrettigheder

Q Hvornår er der krav om gennemførelse af en konsekvensanalyse?

En virksomhed skal foretage en konsekvensanalyse ved:

- en systematisk og omfattende vurdering af personlige forhold der er baseret på automatisk behandling, herunder profilering

- behandling i et stort omfang af særlige kategorier af oplysninger

- systematisk overvågning af et offentligt tilgængeligt område i et stort omfang

Bemærk: det er ikke et krav, at den dataansvarlige udarbejder konsekvensanalyse i forhold til allerede eksisterende systemer

Q Skal der udføres en konsekvensanalyse for hver enkelt behandlingsaktivitet?

- Der stilles *ikke* krav i forordningen om, at der skal udarbejdes konsekvensanalyser for hver enkelt behandlingsaktivitet

- Én konsekvensanalyse kan omfatte:
  - flere lignende behandlingsaktiviteter
  - flere systemer med samme behandling af oplysninger

- Flere virksomheder kan udarbejde en *fælles* konsekvensanalyse, når:
  - tilnærmelsesvis den samme type systemer og behandlingsaktivitet

Q Kan den dataansvarlige blive forpligtet til at gennemføre en fornyet konsekvensanalyse?

- Ja, hvis risikoen ændrer sig

  Eksempel:

  - ✓ formålet med behandlingen ændres *eller*
  - ✓ der skal behandles andre personoplysninger, f.eks. at der nu behandles følsomme oplysninger

Der skal *ikke* foretages en ny konsekvensanalyse, når:

- Behandlingen overgår til en ny databehandler eller underdatabehandler

Q&A om dataansvarlige og databehandlere

JUSTITSMINISTERIET

Q Hvad er den dataansvarlige ansvar?

Den dataansvarliges ansvar er det samme, som man kender det i dag:

>> Man skal have styr på sin behandling af personoplysninger <<

OBS på påvisningskrav:

- Man skal kunne **påvise**, at ens behandling er i overensstemmelse med forordningen
  - Dette kan gøres ved at efterleve fortegnelseskravet i artikel 30
  - Der er *ikke* krav om, at der udarbejdes en dataflow analyse af ens behandling
  - Adfærdskodeks eller certificering

Q Hvad er databehandlerens ansvar?

- Databehandleren får nye forpligtelser med forordningen:
  - Fortegnelser over behandlingsaktiviteter
  - Underretning ved sikkerhedsbrister
  - Evt. DPO
  - 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

Q&A om personoplysninger, behandlingshjemler og håndtering af de registreredes rettigheder

JUSTITSMINISTERIET

Q Hvad er en personoplysning?

- Samme som i dag:
  - *Identificeret* fysisk person
  - *Identificerbar* fysisk person, f.eks. pseudonymiserede oplysninger
    - Alle midler, der *med rimelighed* kan tænkes anvendt af den dataansvarlige *eller* en anden person til direkte eller indirekte at identificere. Hensyn til omkostninger, tid og teknologi.
  - Seneste fra EU-Domstolen: dynamiske ip-adresser er personoplysninger

Q Hvad er betingelserne for et gyldigt samtykke?

- Et ”samtykke” er det samme som i dag:
  - Et *frivilligt*, *specifik*, *informeret* og *utvetydig* ”ja” (viljestilkendegivelse). Stiltiende samtykke utilstrækkeligt
  - Ikke nødvendigvis krav om skriftligt samtykke
  - Men den dataansvarlige skal – som i dag – kunne *påvise* (bevise), at der foreligger et gyldigt samtykke
  - Ret til at *trække samtykke tilbage*. Gyldighedsbetingelse for samtykket, at man er oplyst om tilbagetrækningsmuligheden. Ikke eksplicit krav herom i dag

Q Hvad er betingelserne for et gyldigt samtykke?

Betingelserne for et samtykke præciseres i forordningens *artikel 7*

- Stk. 4 (ny): Der skal i vurderingen af det frivillige samtykke tages *størst muligt hensyn til*, om opfyldelse af en kontrakt er gjort betinget af et samtykke til behandling af personoplysninger, *som ikke er nødvendig for kontrakten*

- Et samtykke i kontraktsforhold kan mao. normalt ikke angå behandling af oplysninger til andet end opfyldelse af selve kontrakten

Q Hvad med de eksisterende nationale særregler?

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

- Selvom det er en forordning…
- 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.

Q De registreredes rettigheder

Retten til dataportabilitet (artikel 20)

- En ny rettighed til at *modtage* og *transmittere* data fra én virksomhed til en anden
- Alene, hvis behandlingen er baseret på et samtykke/kontrakt og foretages automatisk
- Art. 29-gruppen-eks.: liste over sine kontaktpersoner fra webmail-udbyder eller eksisterende spillelister fra musikstreamingstjeneste
- Oplysningerne skal modtages i struktureret, almindeligt anvendt og maskinlæsbart format
- Ret til *direkte transmission* til anden dataansvarlig, *hvis teknisk muligt*

Q De registreredes rettigheder

Retten til indsigt (artikel 15)

- Overordnet ikke en ændring af gældende ret
- Dvs. registrerede har ret til indsigt hos private virksomheder om, hvorvidt der behandles oplysninger om vedk. og om
  - formålet, eventuelle modtagere, oplysning om, hvorfra oplysningerne stammer mv.
- Ikke i sig selv nogen undtagelsen i forordningen – kræver national lovgivning efter artikel 23
- Men mon ikke lovgiver vil overveje en ny PDL § 32, stk. 1: ”vige for afgørende hensyn til private interesser”?