Introduktion til persondataforordningen

PSF temadag d. 24.1.2018, lektor Dorthe Høilund, Metropol

FORMÅLET: At beskytte personoplysninger og samtidig give offentlige institutioner og andre et effektivt arbejdsredskab. I dag hvor så mange data findes elektronisk stiller det nye krav til sikkerhed. Se desuden www.dbreform.dk hvor de nyeste oplysninger ligger

- Anvendelse fra 25. maj 2018
- Direktiv contra forordning
- Mange muligheder for nationale særregler
- Opbygning og struktur

PT har vi et EU-direktiv fra 1995. Ved et direktiv skal medlemslandene hver især lave deres egen lovgivning, der lever op til intensionerne i direktivet. I modsætning hertil, så er en forordning direkte gældende i medlemslandene.

Der er mange ligheder med det nuværende direktiv, men der er også mange skærpelser. Til gengæld er der over 50 dispensationsregler med mange muligheder for at lave nationale særregler.

Lige nu behandler Folketinget et udkast til en dansk databeskyttelseslov, der supplerer forordningen. Det samlede billede består af forordning + lov.

Emner

- Anvendelsesområde og centrale begreber
- Regler for behandling af personoplysninger
- Registrerede personers rettigheder
- Den nye rolle som databeskyttelsesrådgiver
- Krav til datasikkerhed
- Sanktioner

Behandling: Alle former for håndtering

Personoplysninger: Alle oplysninger, der kan føres tilbage til en identificerbar person fra cpr-nummer og e-

Forordningen gælder først og fremmest for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register jf. art. 2(1).

Gælder både for offentlige myndigheder og private virksomheder

mailadresser til billeder af særlige tatoveringer.

Register: Hvis det er struktureret med henblik på at finde frem til bestemte personer

Grundlæggende principper (art. 5)

- God databehandlingsskik
- Udtrykkelige og saglige formål
- Proportionalitetsprincippet
- God datakvalitet
- Tidsbegrænsningsprincippet
- Sikkerhedsprincippet

De grundlæggende principper skal alle være opfyldte HVER gang

Det er f.eks. god databehandlingsskik, at gøre folk opmærksomme på, at de er registrerede

Hvis man ønsker at bruge data til andet formål end det oprindelige, må dette nye formål ikke være i modsætningsforhold til det oprindelige

Man må ikke registrere mere end man har behov for (proportionalitet)

Man skal sørge for at opdatere oplysningerne (datakvalitet)

Man må ikke opbevare data længere end formålet tilsiger (tidsbegrænsning)

Man skal opbevare data forsvarligt (sikkerhed), se endvidere artikel 32 om dette

Betingelser for behandling af personoplysninger

- Alm. personoplysninger (art. 6)
- Følsomme personoplysninger (art. 9)

Artikel 6: Almindelige personoplysninger

- Borgeren har givet sit samtykke
- Opfyldelse af en kontrakt
- Overholdelse af en retlig forpligtelse
- Beskyttelse af vitale interesser
- Samfundsinteresse eller offentlig myndighedsudøvelse
- Interesseafvejningsreglen

Artikel 6 og 9 udgør hjemmelsgrundlaget. Man skal kunne finde mindst 1 grund i én af disse artikler

Angående samtykke er der kommet en ny bestemmelse, nemlig at et samtykke til enhver tid kan tilbagetrækkes. Personen skal gøres opmærksom på dette. Samtykket skal være frivilligt, og i visse tilfælde, f.eks. ved et asymmetrisk magtforhold, kan man sætte spørgsmål ved frivilligheden. Af disse grunde vil det være godt/enklere, hvis man kan finde en anden hjemmel end samtykke.

Samtykke og alder. Der er vejledende retningslinjer men ingen regler angående aldersgrænser. Normalt vil en forælder kunne give samtykke på barnets vegne. Men her kan der også gøres en skønsmæssig vurdering gældende.

Vær opmærksom på, at man skal kunne dokumentere samtykket.

Visse oplysninger under artikel 6 kan være 'fortrolige' (f.eks. cpr-nummer), i så fald må der stilles større krav til risikovurdering og sikkerhed.

Artikel 9: Følsomme oplysninger

Oplysninger om:

- Race
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske data og biometriske data
- Helbredsoplysninger (fysiske og psykiske)
- Seksuelle forhold eller seksuel orientering

Udgangspunktet er, at der ikke må behandles følsomme personoplysninger, medmindre en af undtagelserne i artikel 9(2) er tilstede.

Den nuværende §8 om væsentlige sociale problemer overgår til artikel 6, men man skal selvfølgelig stadig leve op til reglerne i artikel 5.

Helbredsoplysninger: En generel bemærkning om at 'personen er syg' hører under artikel 6, men en specifik bemærkning om at 'personen fejler det og det' hører under artikel 9.

Med hensyn til samkøring af oplysninger: Her risikerer man at komme til at bruge data til andre formål end det oprindelige.

Anonyme oplysninger, der på ingen måde kan føres tilbage til personer, er ikke omfattet af forordningen. Personoplysninger kan 'pseudonymiseres' (f.eks. i forbindelse med forskning).

Registrerede personers rettigheder

- Ret til at få information
- Ret til indsigt
- Ret til at få urigtige oplysninger berigtiget
- Retten til at blive glemt
- Ret til begrænsning af behandling
- Ret til dataportabilitet
- Ret til at protestere mod at behandling af oplysninger finder sted
- Ret til at protestere mod visse automatiserede individuelle afgørelser

Oplysningspligt (art. 13 og 14)

- Dataansvarliges identitet + **eventuel DPO**
- Formål + **behandlingsgrundlag**
- **Hvis interesseafvejning – angiv interesser**
- (Kategorier af) modtagere
- **Evt. tredjelandsoverførsel og hjemmel hertil**
- **Opbevaringsperiode (eller kriterier)**
- Oplyse om rettigheder
- **Ret til at tilbagekalde samtykke**
- **Klage til Datatilsynet**
- **Om afgivelsen følger af lov eller er nødvendig for at indgå en aftale**
- **Om den registrerede har pligt til at give oplysningerne og evt. konsekvenser af ikke at give oplysninger**
- **Oplysninger om behandling baseret på automatiseret afgørelse**
- **Ved indsamling hos tredjemand: typen af oplysninger, der er indsamlet, samt hvor de er indsamlet fra.**

Nyt formål kræver ny meddelelse herom

Institutionen har oplysningsPLIGT: personer har ret til, til enhver tid, at få at vide, hvad der registreres, hvorfor og hvorlænge data opbevares.

Standardiseringer f.eks. i form af formularer er ofte en god ting.

Man skal aktivt forholde sig til, hvor længe man har en saglig grund til at opbevare oplysninger, og hvilke kriterier, der ligger til grund herfor.

Retten til indsigt er videreført og skærpet fra det nuværende direktiv. Man har ret til at se ALLE data, og man behøver ikke at begrunde sit krav.

Databeskyttelsesrådgiver (DPO)

Obligatorisk for offentlige myndigheder

Stilling

- Må ikke modtage instrukser vedrørende udførelse af sine opgaver
- Må ikke afskediges eller straffes for at udføre sine opgaver
- Rapporterer direkte til den øverste ledelse
- Kan udføre andre opgaver, men der må ikke være interessekonflikt

Databeskyttelsesrådgiver er obligatorisk for alle offentlige myndigheder og også for nogle selvejende institutioner.

Man kan evt. købe sig til ydelsen, men det kan også være en medarbejder, der varetager andre opgaver.

Databeskyttelsesrådgiverens opgaver (minimumskrav):

- Underrette og rådgive om forpligtelser iht. forordningen og anden EU-ret eller national ret om databeskyttelse
- Overvåge overholdelse af forordningen, anden EU-ret eller national ret om databeskyttelse samt politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteterne
- Rådgive, når der anmodes herom, med hensyn til konsekvensanalyse vedrørende databeskyttelse og overvåge opfyldelse iht. art. 35
- Samarbejde med og fungere som kontaktperson for Datatilsynet

Design: Det er et lovkrav, at systemer (f.eks. databaser) skal opbygges sådan, at de nemt kan leve op til kravene

Standardindstillinger: Skal være så privatlivsfremmende som muligt. Altså så man kun kan se de nødvendige oplysninger.

Man behøver ikke nødvendigvis at udskifte f.eks. IT-systemer, men man kan i stedet gøre organisatoriske og fysiske tiltag med indbygget beskyttelse.

I princippet skal man overholde de ændrede krav fremadrettet. Men hvis der er en naturlig anledning, vil det være godt at opdatere f.eks. en gammel samtykkeerklæring.

Accountability

Den dataansvarlige skal kunne dokumentere at de grundlæggende principper i art. 5(1) overholdes, jf. art 5(2).

Den dataansvarlige har pligt til at gennemføre passende og effektive foranstaltninger og til at påvise, at behandling af personoplysninger overholder forordningen, jf. artikel 24(1).

Risikovurdering – sikkerhedsniveau skal passe til risici

I det nuværende system anmelder man til datatilsynet. Med den nye forordning erstattes dette af egen-registrering, hvor man løbende dokumenterer, at man lever op til kravene.

Undgå så vidt muligt følsomme oplysninger.

Art. 30 - fortegnelse

Både dataansvarlig og databehandler skal fører fortegnelser over behandlingsaktiviteter under deres ansvar, jf. art 30.

Dokumentationen skal som minimum indeholde:

- Navn og kontaktinformation på dataansvarlig, og hvis relevant DPO
- Formålene med behandlingen
- Kategorier af registrerede personer og kategorierne af personoplysninger
- Kategorier af modtagere af oplysninger
- Hvis relevant: overførsler til tredjelande
- Hvis det er muligt angivelse af tidsfrister for sletning af de forskellige kategorier af oplysninger
- En generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i art. 32, stk. 1.

NB: Undtagelser i art. 30, stk. 5

Fortegnelserne skal efter anmodning stilles til rådighed for Datatilsynet

Fortegnelse: Tag evt. udgangspunkt i de nuværende anmeldelser (se datatilsynet, under produktionsskoler), eller se bogen "Persondataret" s. 101.

Hvis ikke vi ved, hvilke oplysninger vi har, og hvordan vores arbejdsgange er, så er det svært at sikre dem. Gennemse og revider evt. databehandleraftaler, så de lever op til kravene. Den dataansvarlige har tilsynspligt.

I princippet behøver man ikke at oprette et register, hvis man har under 250 medarbejdere og ikke har personfølsomme data. Men man skal under alle omstændigheder kunne dokumentere, hvad man har og hvad man gør.

Vi ved endnu ikke, hvor omfattende det bliver, men vi skal som minimum leve op til ovenstående. Vær en lille smule pragmatiske og start med at arbejde med det. For Datatilsynet er det vigtigt, at man kan vise, at man er i gang med at arbejde med det.

Beskriv procedurer, f.eks. procedure for behandling af elevklager. Det er med til at dokumentere, at I overholder forordningen

Datasikkerhed

Artikel 32 Gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risici.

- Teknisk sikkerhed - rettet mod teknologien. Fx firewalls, backup, kryptering mv.
- Organisatorisk sikkerhed – rettet mod de personer, som foretager behandling af personoplysninger. Fx begrænsning af adgang, udd. af medarbejdere og kontrolforanstaltninger.
- Fysisk sikkerhed – Rettet mod risikoen for, at uvedkommende offline får adgang til personoplysninger. Fx aflåsning, alarmer, brandsikring mv.

Indfør f.eks. autorisationer, så medarbejdere ikke har adgang til flere oplysninger end højst nødvendigt.

Hav en dynamisk tilgang med f.eks. ½årlige eftersyn og opdateringer.

Det man mangler teknisk må man klare organisatorisk. F.eks.: Alle der behandler data skal kende reglerne. Og Fysisk: Stil skærme, så udenforstående ikke kan se dem, lad ikke udprint ligge og flyde

Logning: Mailboksen kan ikke logges, derfor bør mails kun ligge 30 dage. Selvom mailen i princippet er låst for andre, regnes det ikke for sikkert.

Typiske eksempler på sikkerhedsbrud: Ikke ajourførte oplysninger, manglende tilsyn, åben adgang til journalsystemer, manglende kontrol af autorisation, manglende aftale med databehandler, manglende logning.

I dag er vi ikke omfattede af journaliseringskrav. Men vi skal sikre den registreredes rettigheder, herunder indsigtsretten. Dvs. man skal kunne finde det hele frem, hvis den registrerede beder om det.

Den nuværende sikkerhedsbekendtgørelse forsvinder, men den er stadig god som inspiration ift. f.eks.: logningssystemer, autorisationer, adgangskontrol, passwords, låsepc'en, når man forlader den, regler for hjemmearbejdspladser eller møder ude i byen, procedurer, …

Datasikkerhedsbrister

Orientering Datatilsynet (art. 33): Anmeldelse af brud på persondatasikkerheden til Datatilsynet inden 72 timer, medmindre det er usandsynligt, at bruddet indebærer en risiko

Orientering af den registrerede (art. 34): Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet

NB: visse undtagelser

Fejl med risiko skal indberettes

Alt skal registreres og dokumenteres.

Administrative bøder

Overtrædelser af artikler 5, 6 og 9

Manglende samtykke

Rettigheder, oplysningspligten

Manglende anmeldelse af sikkerhedsbrud

Vigtigt at foretage risikovurderinger og foretage passende foranstaltninger

Noget af det, der mangler at blive beskrevet, er back-up af f.eks. mails mm, der ligger hos udbyderen. F.eks. kunne man forestille sig specifikke forpligtigelser i databehandleraftaler.