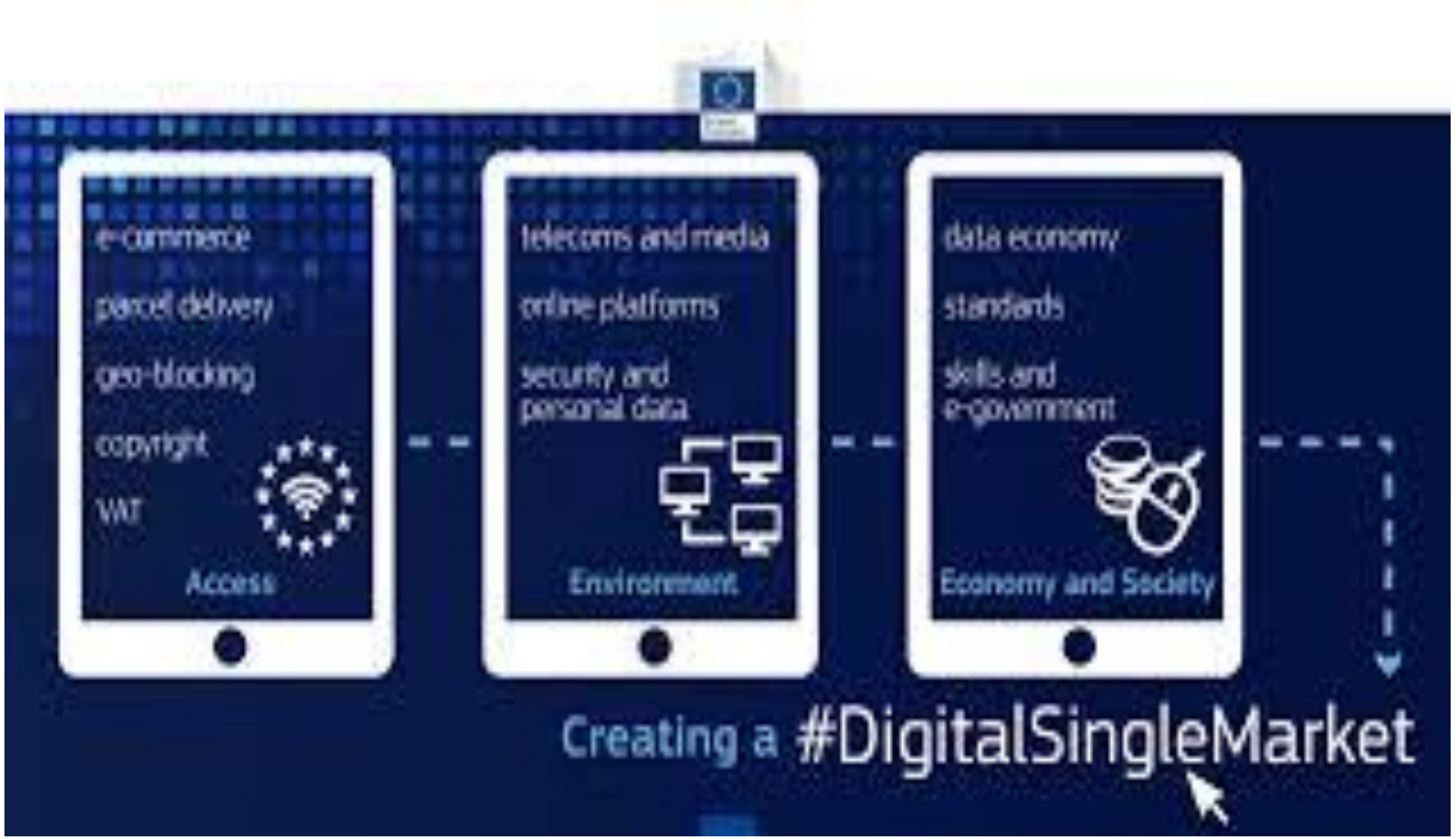
Persondatareguleringen

Hvorfor, hvornår, ”systemet” og lidt om maj 2018

Hvorfor?

I er ***så*** meget i et brændpunkt for persondataretten, at vi er nødt til at stige op i helikopteren ….

Hvad tænker EU?



Hvad tænker EU ***også***?

Drøft med sidemanden:

- Hvad er det bagvedliggende og grundlæggende formål med den regulering, som vi taler om her?

  – Overvej hvorfor jeg ofte bruger følgende vendinger:
    - Den samlede sum af *alle* EU-borgers holdning til indsamling og brug af persondata, især massebehandling
    - Balancepunkt

Ja, tak, det var jo spændende nok …

…men er det brugbart i praksis?

- Satakunnan, Sag C-73/07
- Markus Schecke, forenede sager C-92/09 og C 93/09
- Digital Rights / logningsdommen, forenede sager C-293/12 og 594/12
- Google Spain, Sag C-131/12
- Maximillian Schrems, Sag C-362/14
  - Og mange, mange flere….

Tjaaa….

Hvornår?

Artikel 2, stk. 1:

*Denne forordning finder anvendelse på **behandling af personoplysninger**, der 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*

Definitionen af personoplysninger

Artikel 4, nr. 1:

»personoplysninger«:enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der ***direkte eller indirekte*** *kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer,* ***lokaliseringsdata****, en* ***onlineidentifikator*** *eller* ***et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet***

Reguleringens grundlæggende systematik

- **Principper**
  - Retligt grundlag (oftest forpligtelse eller samtykke)
  - Fairness
  - Formålsbestemthed
  - Proportionalitet (incl. dataminiering)
  - Datakvalitet
  - Tidsbegrænsning
  - Sikkerhed, herunder adgangsbegrænsninger og databehandleraftale
  - Data Protection By Design (By Default samt Impact Assesment)
  - Særlige regler for børn
- **Administrative bestemmelser**
  - Anmeldelse, tilladelse og høring af Datatilsynet – afløses formentlig af fortegnelse over egne behandlinger, dokumentation og indberetning af sikkerhedsbrister.
- **Rettigheder**
  - Information, indsigt, indsigelse, korrektion mv.
- **(Sanktioner og tilsyn)**

Drøft med sidemanden:

- Mht. apps er det så ok, at vi bare registrerer hvor brugeren færdes *eller skal vi som minimum lade brugeren acceptere dette*?
  - Hvilken betydning har samtykke?

Systematik: Forholdet til andre regler:

- Generelt:
  - Bestemmes det i national ret, at en oplysning skal behandles, så er det retlige grundlag til stede
- Men:
  - Medmindre det fremgår af den danske lov, er forordningens (øvrige)regler ikke fraveget!
  - Er andre dele af forordningen faktisk fraveget, skal der opstilles garantier for databeskyttelsen på anden måde!

Lad os tage et eksempel:

Artikel 9, stk. 2, litra h:

- Behandling er nødvendig med henblik på (…) ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social-og sundhedsomsorg og -tjenester på *grundlag af* EU-retten eller *medlemsstaternes nationale ret* (…) og underlagt de betingelser og garantier, der er omhandlet i stk. 3
  - (Stk. 3: Behandles af person med tavshedspligt eller på vegne af en person med tavshedspligt)

Drøft med sidemanden:

- Lovbestemt at kommunerne skal opspore ”sårbare” borgere i gruppen på 65-79 år
  - Sagsbehandlerne vil gerne have en mulighed for at finde disse borgere på et fælles kort.
    - Parametrene er: Køn, enlig, anden etnisk baggrund, barnløs (derudfra en liste med disse borgere og deres cpr-nummer)

Er det retlige grundlag til stede?
Hvilke elementer skal projektet (så) være opmærksom på (se slide 9)?

Forordningen maj 2018

En del nyt, men vigtigst:

1. Muligvis nye aspekter ift. organisering
2. Data Protection by Design and by Default
3. Data Protection Impact Assesment
4. DPO og klarere krav til dataansvarsfordeling

Ad 1: Aspekter ift. organisering

Artikel 83, stk. 7:

- *”Uden at det berører tilsynsmyndighedernes korrigerende beføjelser i henhold til artikel 58, stk. 2, kan hver medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.”*

Drøft med sidemanden …

Hvorfor mener jeg, at *det* er en vigtig nyskabelse?

- Læs artikel 83, stk. 4 og 5 i:
  - http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN
- Hvordan har I hidtil organiseret jeres arbejde?
  - Hvilken betydning har det efter den 25. maj 2018, hvorvidt jeres organisation regnes som myndighed eller som privat?

Ad 2: Data Protection by Design

Artikel 25, stk. 1:

Under hensyntagen til det aktuelle tekniske niveau, implementerings-omkostningerne og den pågældende behandlingskarakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tids-punktet for selve behandlingen ***passende tekniske og organisatoriske foranstaltninger,*** *såsom pseudonymisering, som* ***er designet med henblik på effektiv implementering af databeskyttelsesprincipper****, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.*

Data Protection by Default

Artikel 25, stk. 2:

- *Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på **gennem standardindstillinger** at sikre, at kun personoplysninger , der er nødvendige til hvert specifikt formål med behandlingen, behandles. Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben **stilles til rådighed for et ubegrænset antal fysiske personer.***

Ad 3: Data Protection Impact Assesment

Artikel 35, stk. 1:

- 1.Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen **en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger**. (…)

Artikel 35, stk. 3:

- En konsekvensanalyse vedrørende databeskyttelse som omhandlet i stk. 1 er navnlig påkrævet i følgende tilfælde:

  (…)
- b) behandling i stort omfang af **særlige kategorier af oplysninger**, jf. artikel 9, stk. 1, eller af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10, eller
- c) **systematisk overvågning af et offentligt tilgængeligt område i stort omfang**

Drøft med sidemanden

- En af jer beskriver et projekt, der aktuelt planlægges i jeres organisation
  - Hvordan vil I lave en PiA, sikre Data Protection By Design og By Default?
- Jeg er enig:
  - http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Konsekvensvurdering-for-privatlivet

Ad 4: DPO hhv. fælles dataansvar

- Artikel 37: Krav om DPO
- Artikel 26: Klarlæg jeres roller

I er velkommen til:

….. at kontakte os på SDU:

– Hanne Marie Motzfeldt, hama@sam.sdu.dk
– Sten Schaumburg-Müller, stsm@sam.sdu.dk
– Kristina Siig, kms@sam.sdu.dk

https://www.waset.org/conference/2017/01/durban/ICEGSCDS