Temadag om persondataforordningen

BLIV KLAR TIL PERSONDATAFORORDNINGEN

ATV i samarbejde med - Aarhus Universitet - Digital Society- infinit |
Advokat (H) og medlem af ATVs Digitale Vismænd- Janne Glæsel jgl@nrlaw.dk – nov. 2017

NYBORG × RØRDAM
ADVOKATFIRMA

Agenda – Persondataforordningen

1. Fra Direktiv/Persondataloven til Persondataforordningen med supplerende dansk lov
2. Persondataforordningens begreber og principper
3. Nye krav til behandling og beskyttelse af persondata, øvrige tiltag og
4. Sanktioner – Bøder, erstatning og godtgørelse samt fængsel indtil 6 mdr.

5. 10 områder, som ledelsen skal have fokus på
6. Status lovgivningsproces
7. Tværorganisatorisk opgave

NYBORG × RØRDAM
ADVOKATFIRMA

01. Fra Direktiv/Persondataloven til Persondataforordningen

NYBORG ⁘ RØRDAM
ADVOKATFIRMA

Direktiv/Persondataloven ➡ Persondataforordning (GDPR)

Europaparlamentet vedtog den nye EU-forordning - General Data Protection Regulation, (GDPR) den 14. april 2016 til ikrafttræden **maj 2018**
Reglerne erstatter i Danmark persondataloven, som er en implementering af EU-direktiv 95/46/EC fra 1995

Modernisering af reglerne om persondatabehandling – "Ny digital grundlov" – skal matche den teknologiske udvikling persondataloven og den danske sikkerhedsbekendtgørelse falder bort (ca. 200 danske særlove skal opdateres)

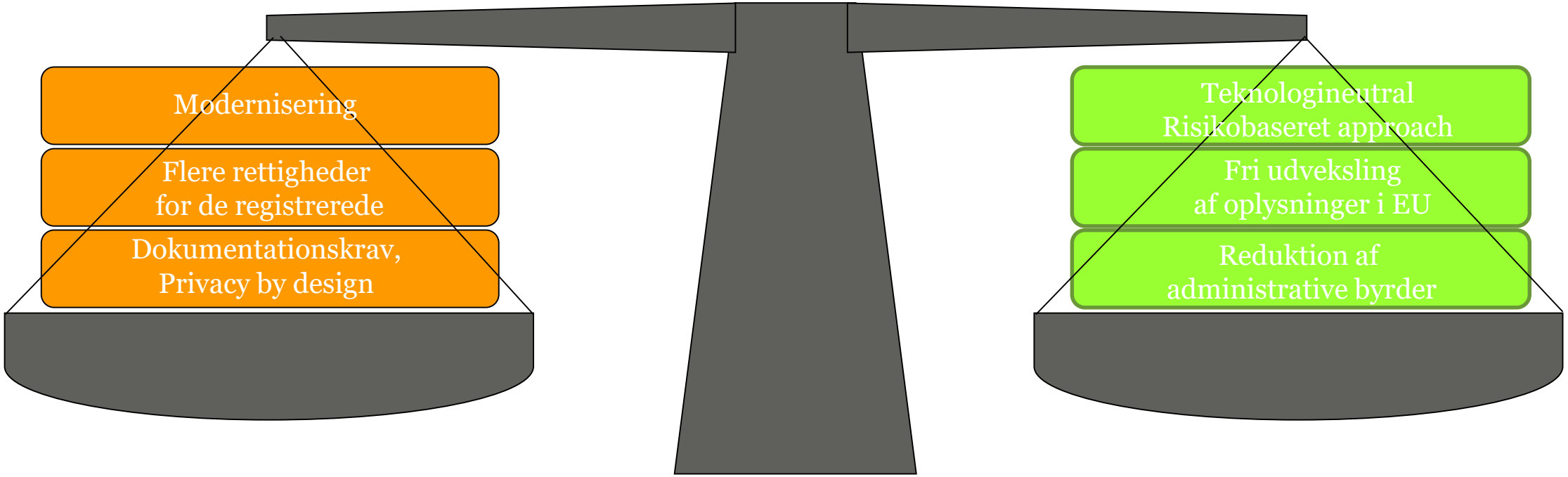
Styrkelse af individets ret til privatliv/databeskyttelse, fri udveksling af data og reduktion af administrative byrder for dataansvarlige (anmeldelsespligt bortalder), men større dokumentationskrav. Forordningen bygger videre på persondataloven, men introducerer nye tiltag. Dansk betænkning 1565 med gennemgang af gældende lov og forordningen. **Lovforslag fremsat oktober 2017.Vejledninger kommer løbende -** www.datatilsynet.dk og www.dbre.dk

NYBORG × RØRDAM
ADVOKATFIRMA

Persondataforordningen - Europa-Parlamentets og Rådets forordning EU 2016/679 af 27/4 2016

Ens regelsæt (næsten) for alle organisationer, der agerer i EU | Global rækkevidde | Stadig mulighed for nationale særbestemmelser - manøvrerum

Balancerer modsatrettede hensyn | Meget skrappe sanktioner | Persondatabeskyttelse er ophøjet til en menneskerettighed



NYBORG × RØRDAM
ADVOKATFIRMA

02. **Persondataforordningens begreber og principper**

NYBORG × RØRDAM
ADVOKATFIRMA

Begreber

Personoplysninger – Art 4 (2) – (Persondata) ctr. anonyme oplysninger

Enhver form for information om en identificeret eller identificerbar fysisk person – Oplysninger, der direkte eller indirekte kan identificere en fysisk person

”Navn, identifikationsnummer, lokaliseringsdata, online-identifikator og et eller flere elementer, der er særlige for en persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet”

Anonyme oplysninger – ingen identifikationsmulighed og derfor ikke personoplysning – i modsætning til krypterede personoplysninger, der er omfattet af begrebet personoplysninger

NB nyt begreb: **pseudonymiserede** oplysninger - særligt sikrede **personoplysninger**

NYBORG × RØRDAM
ADVOKATFIRMA

7

Begreber

Særlige kategorier af personoplysninger – Art 9 (1) – følsomme oplysninger

Race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons forhold eller seksuelle orientering

Almindelige oplysninger

Personoplysninger, der ikke er følsomme - fx navn, adresse, alder, e-mail, men også sociale problemer og andre rent private forhold end følsomme oplysninger

NB – CPR nr. bliver reguleret i DK stort set svarende til nugældende ret

NYBORG × RØRDAM
ADVOKATFIRMA

Almindelige og følsomme oplysninger, CPR og straffedomme/lovovertrædelser

Almindelige oplysninger	Navn, adresse, telefonnr., mailadresse, køn fødselsdato, uddannelse, beskæftigelse, løn, skat, sygefravær, bolig, bil, eksaminer	**Oplysninger, der ikke er omfattet art. 9 og 10 og ikke er CPR – og fortrolige oplysninger (løn, sygefravær, mfl.)**
Semi-følsomme oplysninger	Strafbare forhold, sociale problemer, andre private forhold (bortset fra de følsomme)	Forsvinder
CPR:	Særlig bestemmelse i § 11	Viderefører stort set gældende ret
Følsomme oplysninger	Artikel 9: Race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, Fagforeningsmæssigt tilhørsforhold, genetiske data (fx dna), biometriske data (fx fingeraftryk), helbredsoplysninger eller seksualitet/seksuelle orientering	
Straffedomme og lovovertrædelser	Artikel 10 – kun under kontrol af off. myndighed eller iht. lovgivning, hvis passende garantier og dermed ikke omfattet af § 12	

NYBORG × RØRDAM
ADVOKATFIRMA

Begreber

Behandling – Art 4 (2) Bredt begreb – al håndtering af data fra indsamling til sletning

Enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling, som personoplysninger gøres til genstand for, bl.a.

Indsamling, registrering, organisering, systematisering, ændring, begrænsning, søgning, brug, videregivelse eller enhver anden overladelse, samkøring, sletning, tilintetgørelse

Meget bredt begreb, der står i modsætning til succession – fx ved virksomhedsoverdragelse, hvor en ny ejer indtræder i tidligere ejers sted. Ikke afstemt med begreber i anden lovgivning

Begreber

Samtykke – Art 4 (11)

En viljestilkendegivelse fra den registrerede, der skal være

- **Frivillig**
- **Specifik**
- **Informeret og utvetydig**

Betingelser for samtykke - Art 7

Den dataansvarlige har bevisbyrden for, at samtykke er givet. Den registrerede skal erklære eller bekræfte sin indforståelse med, at dennes personoplysninger behandles.

Begreber

Dataansvarlig – Art 4 (7)

Den, der afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af persondata - virksomheden/organisationen/myndigheden - ikke de enkelte medarbejdere

Databehandler – Art 4 (8) – skærpede krav

Den, der behandler persondata på den dataansvarliges vegne efter skriftlig instruks

NYBORG × RØRDAM
ADVOKATFIRMA

Principper

Principper for behandling

God databehandlingsskik -Art 5 – skal altid opfyldes !

Behandlingshjemmel - Art 6-11 – ikke behandle uden hjemmel !

Rettigheder for den registrerede - Art 12-23

Forpligtelser for den dataansvarlige - Kap. iv

Principper

God databehandlingsskik – Art 5

- Udtrykkelige og legitime formål, senere behandling ikke uforenelig | Formålsbegrænsning
- Relevante og tilstrækkelige - ikke omfatte mere end nødvendigt | Dataminimering
- Konkrete og ajourførte vildledende oplysninger slettes/berigtiges | Rigtighed
- Ikke opbevare længere end formålet tilsiger | Opbevaringsbegrænsning
- Sikkerhed | Integritet og fortrolighed
- Dokumentation for overholdelse | Ansvarlighed

NYBORG × RØRDAM
ADVOKATFIRMA

Principper

Behandlingshjemmel – Art 6 – Almindelige personoplysninger

Behandling er kun lovlig, hvis

- **Opgave i samfundets interesse eller offentlig myndighedsudøvelse**
- **Samtykke** (fx aftale med en kunde)
- **Nødvendig for kontrakt** (fx købsaftale, medlemsaftale, mfl)
- **Retlig forpligtelse** (fx ved indberetning til Skat)
- **Registreredes vitale interesse**
- **Legitim interesse (interesseafvejningsregel)** – gælder ikke i udførelsen af myndighedsopg.

(Børn 13/16 år - Art 8)

NYBORG × RØRDAM
ADVOKATFIRMA

Principper

Behandlingshjemmel – Art 9 – Særlige kategorier oplysninger/de følsomme oplysninger

Hovedregel: Forbud

Undtagelser:

- **Udtrykkeligt samtykke**
- Nødvendigt for regeloverholdelse
- Politisk, filosofisk, religiøse eller fagforening
- Beskyttelse af vitale interesser
- Er offentliggjort af den registrerede selv

- Nødvendigt af hensyn til retskrav
- Væsentlige samfundsmæssige interesser
- Medicinsk diagnose, forebyggelse, mv.
- Samfundsmæssige interesser på sundheds-området (tavshedspligt)
- Arkivformål i samfundets interesse, videnskabelige eller historiske forskningsformål, mv.

NYBORG × RØRDAM
ADVOKATFIRMA

03. Nye krav til behandling og beskyttelse af persondata, øvrige tiltag og sanktioner

NYBORG × RØRDAM
ADVOKATFIRMA

Nye rettigheder for den registrerede

Dataportabilitet – Art 20

- Ret til at modtage persondata i elektronisk format, når behandlingen er baseret på samtykke el. kontrakt
- Struktureret og maskinlæsbart i almindeligt anvendt format
- Ret til at få overført data fra den dataansvarlige direkte til en ny serviceudbyder, hvis teknisk muligt

Omfatter kun personoplysninger som den registrerede selv har givet den dataansvarlige om sig selv

NYBORG × RØRDAM
ADVOKATFIRMA

Nye rettigheder for den registrerede

Retten til ikke at blive profileret – Art 22

Forbud mod profilering, medmindre

- Udtrykkelig samtykke
- Hjemmel – EU-retten eller national ret
- Nødvendig for indgåelse eller opfyldelse af kontrakt

Profilering er afgørelser alene baseret på automatiserede behandlinger, hvis formål er at vurdere særlige personlige forhold

NYBORG × RØRDAM
ADVOKATFIRMA

Nye rettigheder for den registrerede

Retten til sletning – Art 17

"Retten til at blive glemt", når

- **Det ikke længere nødvendigt for at opfylde formålet**
- **Samtykke er trukket tilbage**
- **Indsigelse og ingen legitime formål**
- **Behandlingen er ulovlig**

Nye pligter for den dataansvarlige

Oplysningspligt – Art 13 – giv forretningsbetingelserne et check !

Langt flere oplysninger skal gives til de registrerede:

- Formål
- Kontaktinfo
- Lovlighed
- Evt. overførsel til tredjemand
- Opbevaringsperiode

- Retten til at gøre indsigelse
- Retten til tilbagetrækning af samtykke
- Klagemulighed
- Evt. profilering mv.

Yderligere oplysningspligt, hvis oplysningerne *ikke* er indsamlet hos den registrerede selv – Art 14

NYBORG × RØRDAM
ADVOKATFIRMA

Nye pligter for den dataansvarlige

Privacy by design og default (PbD) – Art 25

Privatlivsfremmende teknologier bør/skal anvendes - (PET) Privacy Enhanching technologies, fx:

Data Loss Prevention | Data Discovery | Identity and Access Governance | Log Management| Backup | Shadow-it discovery | Pseudonymisering | Kryptering| Virtual or partial identities | Anonymisering | mfl. – kilde DI

- Alle systemer skal designes med sikkerhed og regeloverholdelse for øje, så omfanget af indgriben i personers privatliv reduceres
- Tiltag skal slås til som standard
- Melding fra Justitsministeriet– ikke nødvendigt at anskaffe nye systemer - organisatoriske tiltag som alternativ, men i praksis ser situationen anerledes ud…

NYBORG × RØRDAM
ADVOKATFIRMA

Nye pligter for den dataansvarlige

Anmeldelse af brud på persondatasikkerhed – Art 33 og 34 – Vedtag en procedure!

- Uden unødig forsinkelse
- **Om muligt** senest **72 timer efter kendskab**
- Karakteren af sikkerhedsbruddet
- Kontaktperson respektive databeskyttelsesrådgivernes/DPO's navn
- Konsekvenser
- Foranstaltninger for at begrænse skade
- Evt. underretning af de registrerede

NYBORG × RØRDAM
ADVOKATFIRMA

Nye pligter for den dataansvarlige

Dokumentationskrav – Art 30 – fortegnelse over behandlingsaktivitet for dataansvarlig

- Navne og kontaktinfo på dataansvarlig
- Formål
- Kategori af registrerede og af personoplysningerne
- Modtagere, hvis videregivelse
- Overførsel til tredjelande
- Sletning, hvis muligt
- Generel beskrivelse og tekniske og organisatoriske sikkerhedsforanstaltninger,

Den dataansvarlige skal generelt kunne dokumentere, at behandlinger er lovlige, Art 24 - til gengæld forsvinder den nuværende anmeldelsespligt

NYBORG × RØRDAM
ADVOKATFIRMA

Nye pligter for den dataansvarlige

Konsekvensanalyse Art 35 – Data Protection Impact Assesment (PIA)

Hvor der er særlige risici som følge af behandlingens

- **Karakter – fx profilering**
- **Omfang – fx omfattende og systematisk**
- **Formål – fx følsomme oplysninger, straffedomme/lovovertrædelser**

Konsekvensanalysens indhold

- **Generel beskrivelse af behandlinger**
- **Vurdering af risici**
- **Anvendte tiltag for at reducere risici**

NYBORG × RØRDAM
ADVOKATFIRMA

Nye pligter for den dataansvarlige

Databeskyttelsesrådgiver – Art 37 – Data Protection Officer (DPO)

Offentlige myndigheder | følsomme oplysninger i stort omfang | Hvis kerneaktiviteten kræver regelmæssig og systematisk overvågning af registrerede i stort omfang - Professionelle databehandlere

Pligt til at hjælpe

Den **dataansvarlige** får pligt til at hjælpe den registrerede til at varetage hans/hendes rettigheder

Databehandlere får pligt til at hjælpe den dataansvarlige til regeloverholdelse og direkte ansvar i forhold til den registrerede, Art 28 (f)

NYBORG × RØRDAM
ADVOKATFIRMA

Øvrige tiltag

Behandlingssikkerhed – Art 32 - mere detaljerede regler – risikobaseret tilgang

– Sikkerhedsniveau skal afpasses efter de risici, som behandlingen medfører (som efter gældende dansk ret)
– Adfærdskodeks
– Instruks (som efter gældende dansk ret)
– ISO 27001 mfl. kan benyttes for at skabe compliance

One Stop Shop – Art 55, 56, 60 og 63

– Tilknytning til kun ét datatilsyn i EU – hovedvirksomhedens beliggenhed - og mere samarbejde mellem de enkelte landes tilsynsmyndigheder - sammenhængsmekanismen

NYBORG × RØRDAM
ADVOKATFIRMA

Sanktioner

Administrative bøder – Art 83 – dansk lovforslag §§ 41-42 – administrative bøder ikke muligt i DK – Grundlovens § 3, jf. lovudkast § 30

2 % af moderselskabets omsætning eller 10 mio. Euro, efter hvad der er højest

- Manglende efterlevelse af pligter for den dataansvarlige eller databehandleren

4 % af moderselskabets omsætning eller 20 mio. Euro, efter hvad er højest

- Manglende efterlevelse af principperne af de registreredes rettigheder | overførsel til lande uden for EU uden retsgrundlag | manglende efterlevelse af tilsynsafgørelser

NYBORG × RØRDAM
ADVOKATFIRMA

Bøder - Art. 83

Bøderne skal være effektive og afskrækkende - elementer der indgår i vurderingen – ikke udtømmende:

- Karakteren
- Alvor – uagtsomt eller forsætligt
- Varighed
- Skaden - karakter, omfang, formål
- Antallet af berørte personer
- Kategorier af data
- Sikkerhedsforanstaltninger,
- Gentagelse/Selvanmeldelse
- Korrigerende tiltag
- Samarbejde med myndighed

NYBORG × RØRDAM
ADVOKATFIRMA

Bøder – Art. 83

Hvordan vil det foregå i praksis

- Datatilsynet politianmelder
- Anklagemyndighed indleder sag
- Domstolene idømmer bøder, men
- Datatilsynet har mulighed for bødeforlæg – RPL § 832, stk. 1
- Præambel 151 – politi og anklagemyndighed skal høre Datatilsynet

Erstatning – Art. 82, stk. 1 og Godtgørelse – Bet. Side 913

”Enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren”

Det danske lovforslag § 40 gentager bestemmelsen i 82, stk. 1. Omfatter art. 82 og § 40 også godtgørelse – ikke-økonomisk skade? Bet. side 913 – Ja!
(Banedanmark afgørelsem U 218.98 H)

- Krav om culpa, men omvendt bevisbyrde
- Solidarisk ansvar ml. databehandleren og dataansvarlige – Ansvarsfordeling kan aftales – Bet. 916
- Databehandleren hæfter kun for skade, hvis undladt at opfylde forordningens bestemmelser om databehandlere/handlet i strid med instruks
- Mulighed for gruppesøgsmål efter Rpl. Kap. 23 a - §§ 254 a ff.

NB mulighed for fængsel indtil 6 måneder -§ 41 - medmindre højere straf følger af anden lovgivning

NYBORG × RØRDAM
ADVOKATFIRMA

04. 10 områder, som ledelsen skal have fokus på

NYBORG × RØRDAM
ADVOKATFIRMA

Skab overblik via HR, IT, salg- og marketing og juridisk afdeling

| Afdæk konsekvenser for aktiviteterne/forretningsmodellen | sørg for ledelsesforankring | nedsæt et projektteam |

1. Hvilke persondata indsamles og behandles – klassificer oplysningerne

- Særlige kategorier/følsomme oplysninger, herunder HR?
- Behandles oplysninger om børn?
- Er behandlingen forbundet med særlige risici?

2. Til hvilke formål behandles de enkelte typer personoplysninger

- Hvordan er formålet angivet? – Fx i forretningsbetingelser og salgs-og leveringsbetingelser
- Dækker formålsangivelsen den faktiske brug/behovet?
- Behandles persondata uden for formålet?

NYBORG × RØRDAM
ADVOKATFIRMA

Skab overblik

3. Behandles persondata for andre virksomheder

- Er organisationen databehandler for andre?
- Er databehandleraftalerne på plads og på skrift?
- Overholdes kravene i databehandleraftalerne?

4. På hvilket retligt grundlag sker behandling og hvordan indhentes samtykke

- Afklar behandlingshjemmel og dokumenter konklusion
- Hvordan indhentes, opbevares og dokumenteres samtykke
- Gives samtykke for flere behandlinger og er samtykketekst letforståelig og er samtykket tilstrækkeligt utvetydigt

Stiltiende samtykke og afkrydsede samtykkebokse dur ikke

Skab overblik

5. Hvor behandles personoplysninger ?

- Internt – systemoverblik – gennemfør dataflow-analyse
- Eksternt – benytter organisationen databehandlere?

6. Sker der overførsel til andre juridiske enheder / modtagere i tredjelande ?

Afklar det retlige grundlag

- Samtykke – nødvendig for kontraktopfyldelse, retskrav, legitime interesser (snæver), mfl.
- Standard Contractual Clauses (SCC) eller Binding Corporate Rules (BCR)
- Lovgrundlag, godkendte adfærdskodeks eller certificeringer
- EU/US Privacy Shield (ny guideline fra Kommissionen)

NYBORG × RØRDAM
ADVOKATFIRMA

Skab overblik

7. Information til de registrerede og opfyldelse af disses rettighede

- Oplysningspligt og indsigtsret
- Berigtigelse
- Sletning
- Indsigelse, herunder mod profilering
- Retten til at flytte personoplysninger/dataportabilitet

8. Sikkerhed – fysisk, teknisk og organisatorisk

- Status sikkerhed, it-sikkerhedspolitik og tiltag for at sikre compliance
- Systemer i forhold til Privacy by design - eksisterende og nye IT-løsninger – vurder disse!
- Er der eller skal der udarbejdes risikovurderinger/konsekvensanalyser?

Skab overblik

9. Hvem er ansvarlig for persondata?

–Databeskyttelsesrådgiver/DPO og den internt ansvarlige

10. Dokumentation og processer

- Procedure for indberetning af sikkerhedsbrud, den registreredes rettigheder – kontaktinfo.
- Procedure for løbende dokumentation, opfølgning, overholdelse af slettefrister og auditering
- Politik for opbevaring af persondata
- Databehandleraftaler og krav til leverandører
- Uddannelse og træning af medarbejdere

0.5 Status lovgivningsproces – skrider planmæssigt frem

|Dansk betænkning nr. 1565| dansk lovforslag fremsat – vejledninger kommer løbende

EU's Art 29 gruppe - guidelines 2017 om

- Dataportabilitet
- Anmeldelse af brud på sikkerheden
- Konsekvensanalyse/PIA
- Certificering
- Privacy by design
- Databeskyttelsesrådgiver/DPO

Datatilsynet
- Samtykke,
- Dataansvarlige og databehandlere

NYBORG × RØRDAM
ADVOKATFIRMA

0.6 Tværorganisatorisk opgave

Flere lag og personer & forskellige kompetencer og aktiviteter i organisationen berøres

1. Styring af proces og håndtering – forankring på ledelsesniveau og udrulning i organisationen

2. Politikker og processer – Mange processer berøres på tværs i organisationen

3. Data Governance - Indtænkes i governancestruktur – som myndighed og/eller kommerciel aktør

4. Teknologi – skrappere krav til design og anvendelse af IT-systemer,og til sikkerhed

5. Det fysiske lag

Næste Step – et foreløbigt bud – udover tidsplan og ledelsesforankring:

- Systemoversigt
  - Dataflow- analyse
    - Spørgeskemaer – dataindsamling – **fokuser på de relevante områder**
      - Identifikation af interne ressourcer, herunder IT-support
        - Workshops
          - Gennemgang af indsamlede data
            - GAP-analyse og handlingsplan til lukning af huller
              - Implementering, herunder politikker og procedurer

START - Compliant maj 2018

NYBORG × RØRDAM
ADVOKATFIRMA

Tak for opmærksomheden

Janne Glæsel, advokat (H)
jgl@nrlaw.dk
Direkte +45 33 38 70 05
Mobil +45 27 80 25 55

St. Kongensgade 77
1264 København K

T +45 33 12 45 40
www.nrlaw.dk

NYBORG × RØRDAM
ADVOKATFIRMA