GDPR – hva betyr det for arkivene?

Herbjørn Andresen

16.10.18

GDPR – HVA BETYR DET FOR ARKIVENE

Disposisjon

1. Felleseuropeiske regler (GDPR) – og ny norsk personopplysningslov
   - Status, hva er gjeldende?
   - Nasjonalt handlingsrommet innenfor GDPR
2. Hovednivåene i GDPR: Formål – behandlinger – opplysninger
3. Virksomhetenes plikter etter GDPR
   - De viktigste «gjøremålene»
   - Hva kan det være naturlig/fornuftig at arkivtjenesten blir involvert i?

Status

- GDPR gjeldende i EU-landene fra 25. mai i år
- Ny personopplysningslov, lov 15. juni 2018 nr. 38
  - Er allerede i kraft, fra 20. juli i år
  - § 1: Personvernforordningen (GDPR), EU 2016/679, «gjelder som lov» i Norge
- De aller fleste, og vesentligste, bestemmelsene finnes i forordningen
  - Den nye, norske personopplysningsloven bidrar med enkelte bestemmelser som utfyller det nasjonale handlingsrommet, så langt GDPR åpner for det

… og status for et par små ting

- Den gamle personopplysnings*forskriften* er også opphevet
  - Forordningen er temmelig detaljert, dekker blant annet sikkerhetskrav som tidligere fantes i personopplysningsforskriften
- To nye forskrifter man bør kjenne
  - Ny personopplysningsforskrift, **15.6.18 nr. 876**
    - Svært slank (kan vokse etter hvert), litt om opplysninger til tredjestater, litt om personvernnemnda
  - Ny forskrift om arbeidsgivers innsyn i ansattes e-post og filområder, **2.7.18 nr. 1108**
    - Nå hjemlet kun i arbeidsmiljøloven, § 9-5 (var tidligere hjemlet også i personopplysningsloven)
    - Omtrent lik som kap. 9 i den gamle personopplysningsforskriften, men uten å gjelde tilsvarende «så langt det passer» for studenter (GDPR åpner kun for nasjonale regler i *arbeidsforhold*)

Nasjonalt handlingsrom

(Status: Norge har valgt å utnyttet det nasjonale handlingsrommet i relativt beskjeden grad)

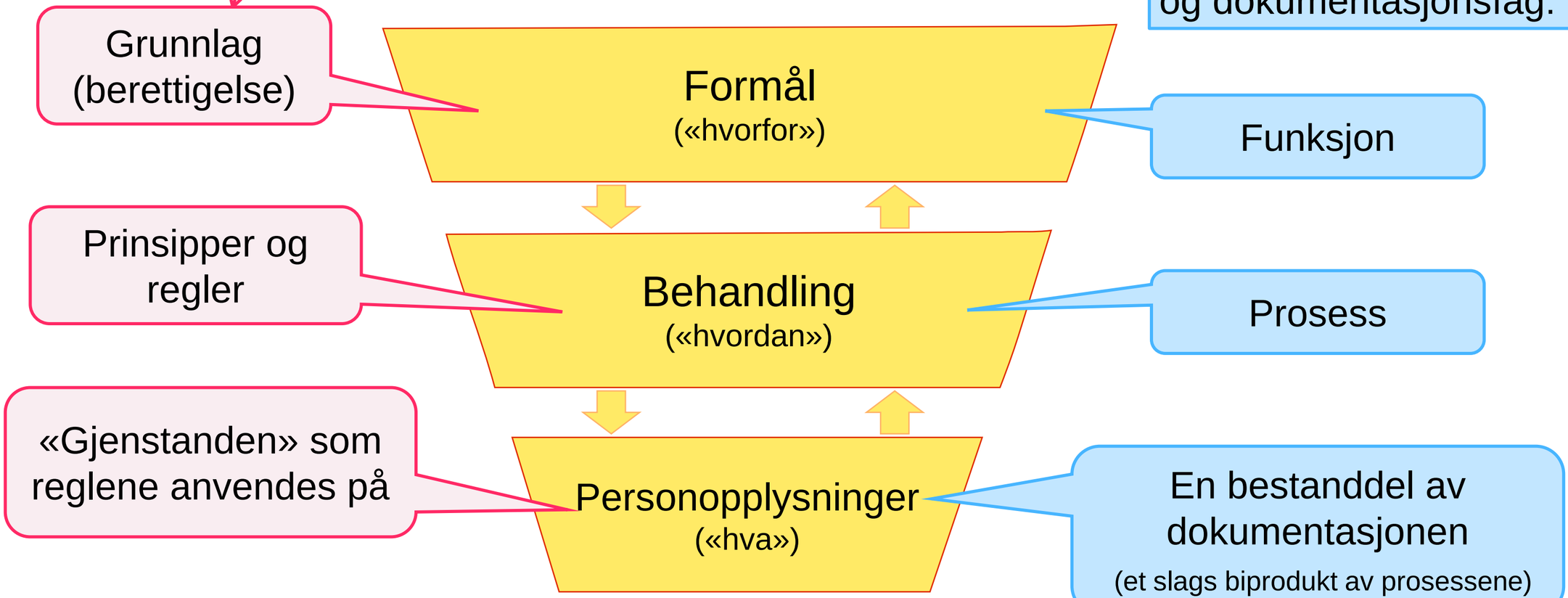
- GDPR er ment å være felles («harmoniserte») regler for hele EU/EØS
- Åpner likevel for nasjonale regler på noen områder
  - Direkte angivelser: «Medlemsstatene kan gi regler om…»
  - Indirekte angivelser: «For å utføre oppgaver på lagt i lov…»
- Rett til informasjon, innsyn, retting osv.: Dels tatt direkte inn i bestemmelser i personopplysningsloven, dels som hjemler for forskrift
- Rett til sletting/ «å bli glemt»: Ikke direkte adgang til å gi nasjonale regler, men underlagt en del nasjonale regler *indirekte* (lovbestemt behandling)
  - Altså ikke anledning til unntak fra sletting i den norske personopplysningsloven

GDPR har først og fremst gitt endringer i midten, «hvordan»-nivået

Personvernrettslige grunnbegreper

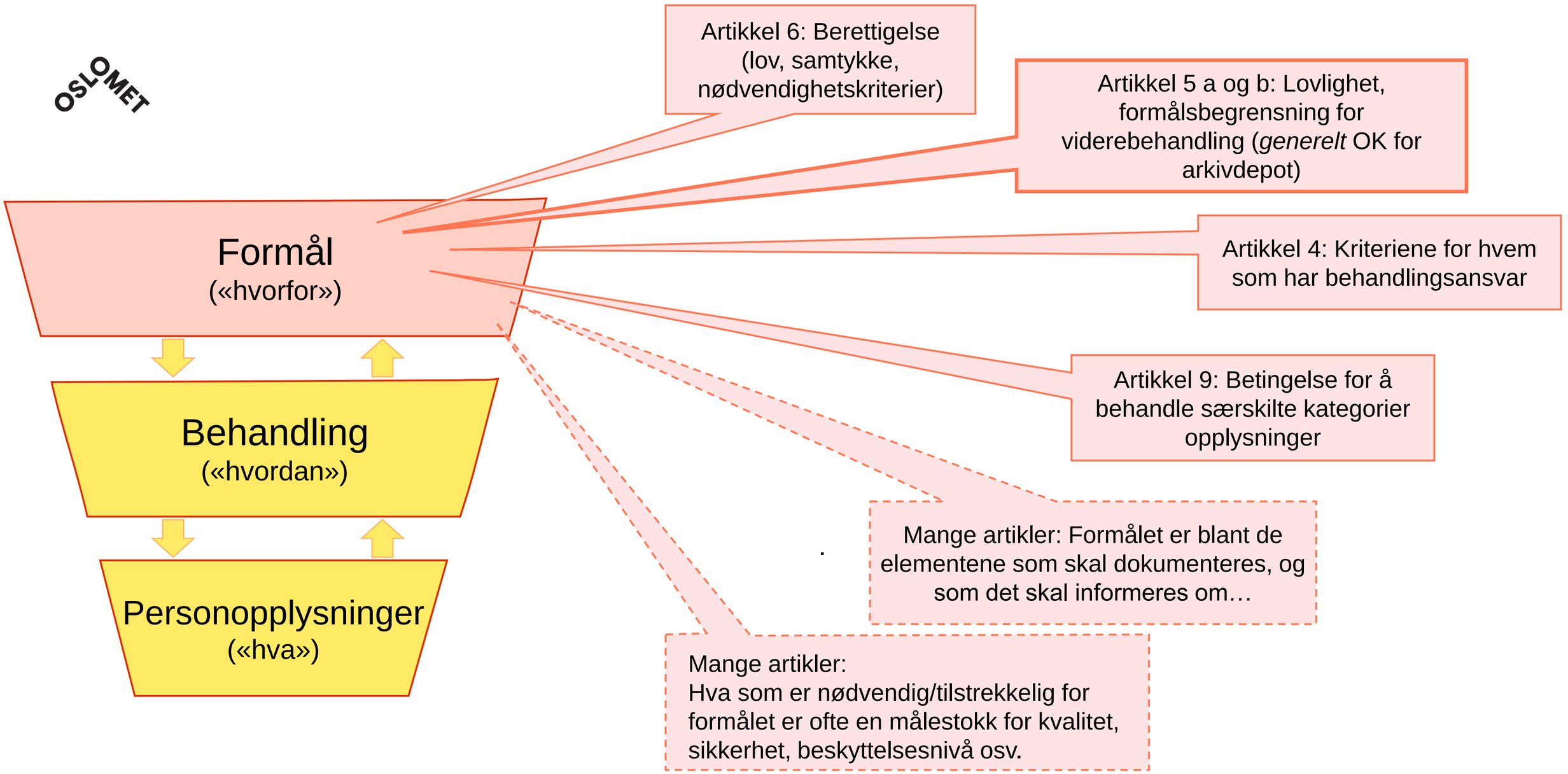
Rettigheter og plikter er primært knyttet til dette (litt abstrakte) begrepshierarkiet:

Assosiasjoner til arkiv- og dokumentasjonsfag:



GDPR inneholder også litt annet…

- Organisatoriske bestemmelser
  - Personvernombud (påbudt i forvaltningen, en viktig alliert)
  - Tilsynsmyndigheter, klageorgan, samordne myndighetene i EU
- Bransjevise adferdsnormer
  - F.eks. sikkerhetsnorm for helsesektoren
- Regler om opplysninger til tredjeland
- Rettshåndhevelse, bøter og den slags


Artikkel 6: Berettigelse (lov, samtykke, nødvendighetskriterier)
Artikkel 5 a og b: Lovlighet, formålsbegrensning for viderebehandling (*generelt* OK for arkivdepot)
Formål («hvorfor»)
Artikkel 4: Kriteriene for hvem som har behandlingsansvar
Artikkel 9: Betingelse for å behandle særskilte kategorier opplysninger
Behandling («hvordan»)
Mange artikler: Formålet er blant de elementene som skal dokumenteres, og som det skal informeres om…
Personopplysninger («hva»)
Mange artikler:
Hva som er nødvendig/tilstrekkelig for formålet er ofte en målestokk for kvalitet, sikkerhet, beskyttelsesnivå osv.

Behandling av personopplysninger må ha et grunnlag

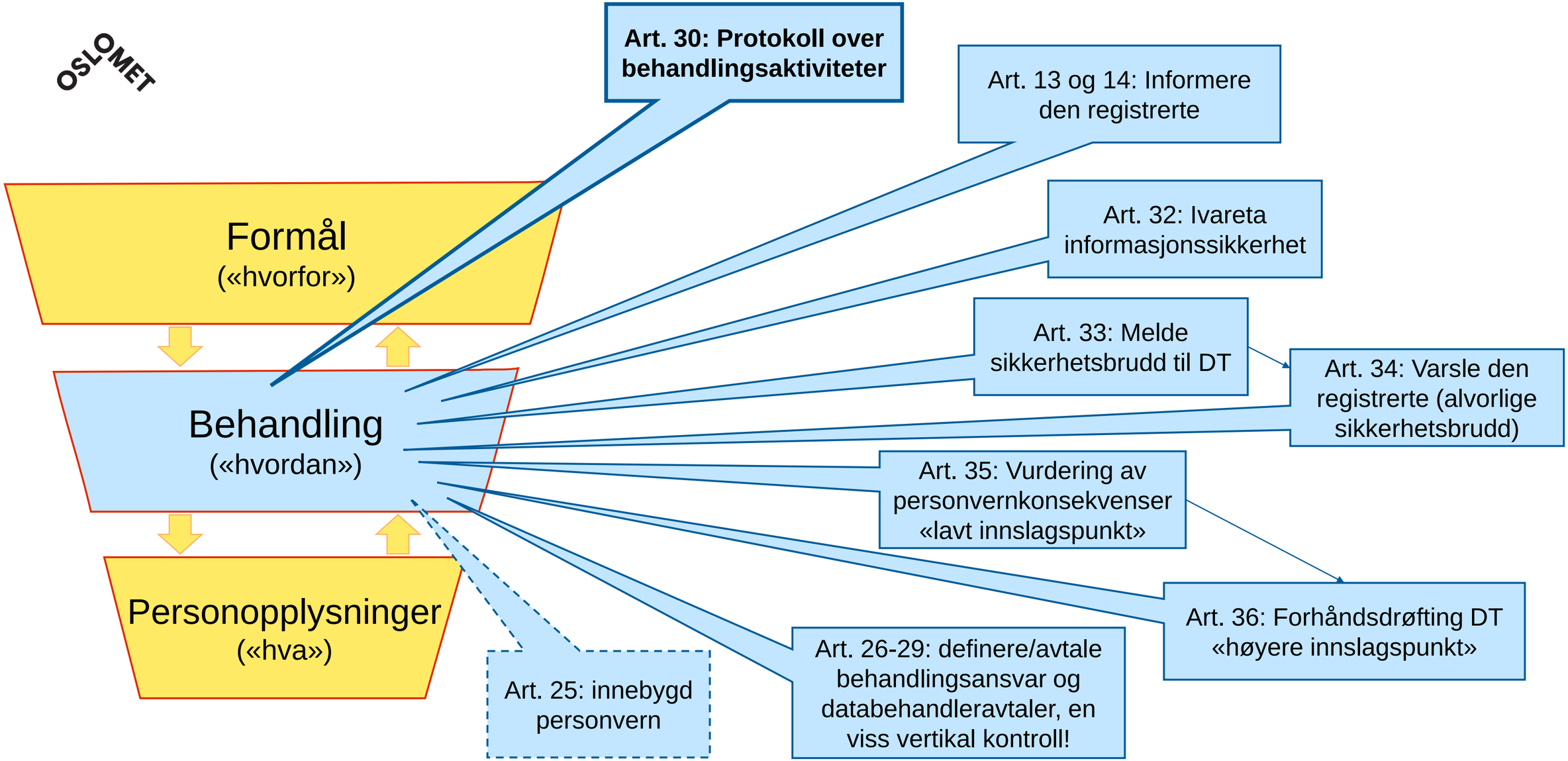
- Ulike muligheter: Samtykke, lovhjemmel, nødvendighetskriterier osv. (omtrent som før)
- Offentlig forvaltning: Forordningen krever ikke så mye, vil normalt være tilstrekkelig at formålet har hjemmel i lov eller forskrift (jf. artikkel 6(1)(c))
  - F.eks. er «administrere bostøtte» et formål, ikke nødvendig at bostøtteloven gir detaljer om behandlingen av personopplysninger
  - Journalføring er ikke formål *i seg selv*, det er formålet/funksjonen, «oppgaven bak», som skal fremgå av lov for å berettige at man behandler personopplysninger
- Selv om forordningen ikke legger lista spesielt høyt, tilsier *legalitetsprinsippet* (i norsk rett) at jo mer inngripende myndighetsutøvelsen er, jo klarere må hjemmelen være

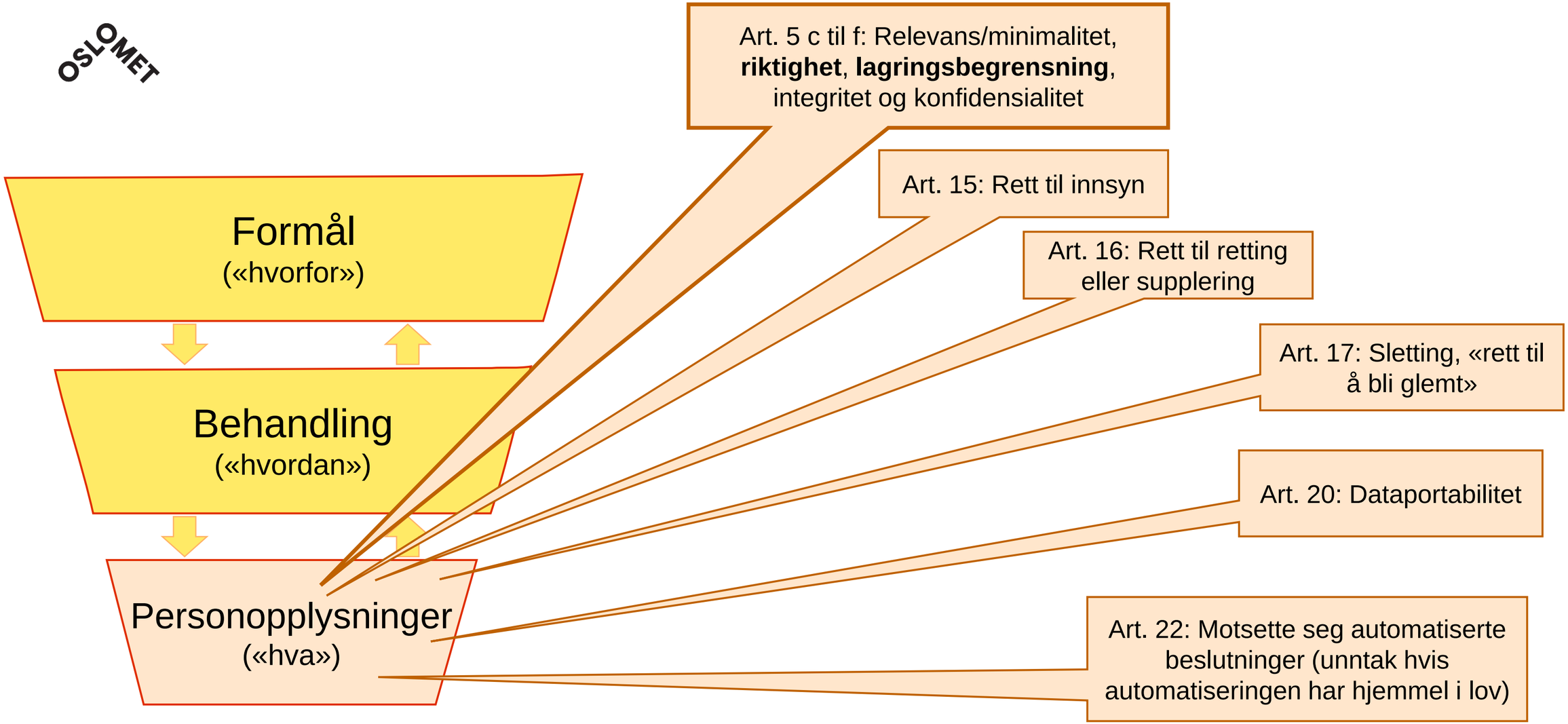
Arkivformål er et *sekundært* behandlingsformål

- Ikke arkiv*danning* – etter opprinnelig formål
- Kan være et legitimt grunnlag for å viderebehandle (og ikke slette) personopplysninger som ikke lenger trengs for det opprinnelige formålet
  - «Allmennhetens interesse» blir neppe en problematisk avgrensning i praksis
- Fortalepunkt 158 – to mer tungtveiende skranker for arkivformålet:
  1. Gjelder institusjoner med en *rettslig forpliktelse* til å bevare arkiver
  2. Gjelder institusjoner som utøver en viss bredde av faglige (depot-)oppgaver

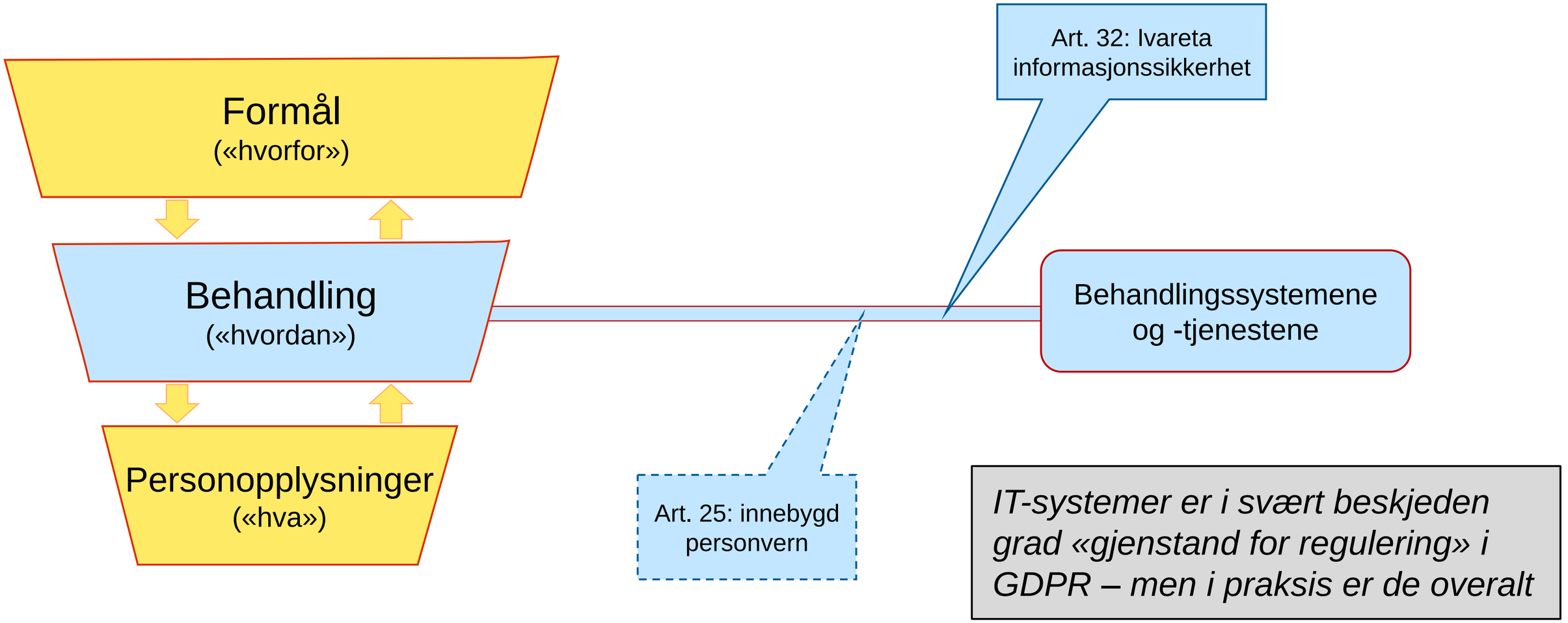
Når skjer «overgangen» til arkivformål?

- Den konkrete regelteksten, GDPR artikkel 5(1)(e): «[personopplysninger skal] lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse […]
- Kan *ikke* ses som et krav til å tagge hver enkelt opplysning/dokument/sak
- Må heller ses i sammenheng med *behandlingsprotokoll*, artikkel 30
  - Særlig art. 30(1)(f), slettefrister, kommer tilbake til den senere


Art. 30: Protokoll over behandlingsaktiviteter
Art. 13 og 14: Informere den registrerte
Art. 32: Ivareta informasjonssikkerhet
Art. 33: Melde sikkerhetsbrudd til DT
Art. 34: Varsle den registrerte (alvorlige sikkerhetsbrudd)
Formål
(«hvorfor»)
Behandling
(«hvordan»)
Art. 35: Vurdering av personvernkonsekvenser «lavt innslagspunkt»
Art. 36: Forhåndsdrøfting DT «høyere innslagspunkt»
Personopplysninger
(«hva»)
Art. 25: innebygd personvern
Art. 26-29: definere/avtale behandlingsansvar og databehandleravtaler, en viss vertikal kontroll!


Art. 5 c til f: Relevans/minimalitet, **riktighet**, **lagringsbegrensning**, integritet og konfidensialitet
Art. 15: Rett til innsyn
Art. 16: Rett til retting eller supplering
Art. 17: Sletting, «rett til å bli glemt»
Art. 20: Dataportabilitet
Art. 22: Motsette seg automatiserte beslutninger (unntak hvis automatiseringen har hjemmel i lov)
Formål («hvorfor»)
Behandling («hvordan»)
Personopplysninger («hva»)

Hvor er IT-systemene i GDPR ?



IT-systemer er i svært beskjeden grad «gjenstand for regulering» i GDPR – men i praksis er de overalt

Virksomhetens plikter

- En del av pliktene etter GDPR er plikter til å «rigge virksomheten»
  - Dokumentere behandlingsansvar (hvor det ligger, delt med andre eller eget ikke)
  - Databehandleravtaler, dersom oppgaver utføres av andre
    - NB, sterkere vertikalt ansvar enn tidligere, sette rammer for sub-kontraktører etc.
  - Plikt til å ha personvernombud, med avklart rolle og fullmakter
    - Pålagt for alle offentlige virksomheter, kan være outsourcet eller konsernfunksjon
- En del andre plikter etter GDPR er «gjøremål», som skal dokumenteres og følges opp

«Gjøremålsplikter» - hvor har arkivtjenesten en rolle?

- Ansvaret ligger hos virksomheten, ledelsen bruker i utgangspunktet arkivtjenesten slik de selv finner det hensiktsmessig
- Det er ganske stor oppmerksomhet om personvernombudets rolle i virksomhetene, arkivtjenesten kan kanskje lett bli usynlige?
  - Må antakelig ofte «melde seg på» selv
  - Et viktig mål, og argument for at arkivtjenesten engasjerer seg, er å unngå dobbeltarbeid i virksomheten, for å please ulike tilsynsmyndigheter
- På de følgende arkene har jeg satt opp de jeg tror er viktigst først…

Artikkel 30, behandlingsprotokoll

- Oversikt over behandlingsaktiviteter (skal være skriftlig)
  - Formål, kategorier av opplysninger, kategorier av registrerte personer, kilder og mottakere
  - «planlagte tidsfrister for sletting» – sammenlignbart med arkivforskriften § 16
  - Behov som overlapper med dokumentasjonspolicy/internkontroll/arkivplan
- Grunnlag for informasjonspliktene i artikkel 13 og 14
  - Det skal blant annet informeres om planlagte tidsfrister for sletting
- Litt bustete unntaksbestemmelser – offentlig forvaltning kan neppe la være
- I norske Datatilsynets veiledninger er artikkel 30 fremstilt som et grunnlag for at virksomhetene må etablere og vedlikeholde et internkontrollsystem
  - Ikke eksplisitt i GDPR, men summen av plikter utgjør i praksis et internkontrollsystem

Artikkel 16, rett til retting

- Uriktige opplysninger skal rettes eller suppleres
  - Formålet har betydning for om det skal rettes eller suppleres
  - Formodentlig den behandlingsansvarlige som vurderer hvorvidt det er retting eller supplering som skal gjøres
    - Ikke helt klart i forordningen, men jeg oppfatter «tas hensyn til formålene» på den måten
- En viss sammenheng med arkivloven § 9 d)
  - Ikke rette ved å slette tidligere uriktige opplysninger, dersom de ut fra *arkivlovens* formål bør kunne dokumenteres
  - Taler i utgangspunktet for at supplering bør være hovedregelen i forvaltningen, men hjemlene er ikke egentlig godt avstemt mot hverandre GDPR
    - (formål med behandlingen ≠ arkivlovens formål)

Artikkel 15, innsynsrett

- I kraft av at en person er registrert, trenger ikke å være part i en sak
- Både selve opplysningene, og en del opplysninger om behandlingen
  - Behandlingsgrunnlaget, lagringstid, eksterne mottakere, automatiserte beslutninger
  - Mye av dette vil være vanskelig å få til, før man har trent i motbakker en stund…
  - Begjæring kan fremsettes skriftlig eller muntlig
- Hvordan få til dette i praksis? GDPR sier ikke egentlig noe om det, men kanskje
  - Rutiner som sikrer at man faktisk fanger opp forespørsler «samme hvor og hvordan de kommer», vet hva som skal gjøres med dem, når ut i hele organisasjonen, gir samlete og gode svar
  - Lage innsynsløsninger, som spar opplysningene ut av systemene
  - Gjennomføre øvelser

Artikkel 17, håndtere slettebegjæringer

- «Fasit» vil for det aller meste, i offentlig forvaltning, være at man har grunnlag for å avslå en slettebegjæring
  - Unntaksbestemmelsen i art. 17(3)(b) er oftest enkel å vise til
    - Kan være visse situasjoner det skal slettes likevel, f.eks. etter en brukertilfredshetsundersøkelse
  - Hvis man utelukkende beholder opplysningene for andre, legitime formål enn det opprinnelige (f.eks. arkivformål), er vurderingene litt mer åpne, og kompliserte
- Uansett viktig å ha rutiner som gjør at man både fanger opp, tar stilling til, og gir ordentlige svar på slettebegjæringer
  - Vimsete eller uvennlig behandling bygger ikke tillit

Artikkel 13 og 14, informasjonsplikter

- Når noen blir bedt om å avgi opplysninger, skal det informeres om hvem som er ansvarlig, slettefrister, hvem de utleveres til, forklare «logikken» bak automatiserte beslutninger osv.,
  - Kan unnlates hvis den registrerte allerede har denne informasjonen
- Når opplysninger mottas fra andre, skal mye av den samme informasjonen gis
  - Unntak hvis innsamlingen *både* er lovhjemlet, *og* det er egnede tiltak som verner den registrertes berettigede interesser
  - Unntak hvis det er lovbestemt taushetsplikt eller annet konfidensialitetskrav

Artikkel 32, informasjonssikkerhet

- Helhetlig arbeid i virksomheten
- Mer «komprimert» enn de bestemmelsene som var i den gamle personopplysningsforskriften, men egentlig det samme som skal gjøres
  - Arkivtjenesten antakelig like mye eller lite involvert som før
- På flisespikkersiden: GDPR legger kanskje lista en ørliten tanke lavere enn de gamle reglene
  - GDPR: «Egnede tekniske og organisatoriske tiltak», i den gamle forskriften var det sterkere understrekete krav til tekniske tiltak
  - Lite praktisk betydning, det er «egnede» som er det viktigste ordet her

Artikkel 33 og 34, meldinger om sikkerhetsbrudd

- Melding til tilsynsmyndigheten, art. 33, senest etter 72 timer
  - En del krav til meldingens innhold
  - I prinsippet alle typer sikkerhetsbrudd som kan ha betydning for personopplysninger
- Underretning til den registrerte, art 34
  - Sikkerhetsbrudd der det er «høy risiko for fysiske personers rettigheter og friheter», altså mer avgrenset omfang enn det som skal meldes til Datatilsynet
  - «Uten ugrunnet opphold», men ikke samme skarpe tidsfrist som i artikkel 33

Artikkel 35, vurdering av personvernkonsekvenser

- Formell vurdering av risiko, nødvendighet, forholdsmessighet osv.
  - Gjøremål som eksplisitt involverer personvernombudet
- Påkrevd ved «høy risiko for fysiske personers rettigheter og friheter»
  - Og særlig ved innføring av ny teknologi
- Viktig styringsinstrument for Datatilsynet, de kan lage liste over hva slags typer behandling («hvordan»-nivået, ikke formålsnivå) dette kreves for
- Kan unntas fra plikten dersom vurdering av konsekvenser har vært en del av den lovgivningsprosessen som har gitt behandlingsgrunnlag for lovpålagte oppgaver

Artikkel 36, rådføringsplikt

- Dersom resultatet av en vurdering av konsekvenser etter art. 35 er at behandlingen kommer til å innebære høy risiko, er det plikt til rådføring med Datatilsynet
- Rådføring kan ha som resultat at man blir enig om at behandlingen er innenfor GDPRs regler
- Hvis behandlingen ikke er innenfor, skal Datatilsynet gi beskjed om at den «sannsynligvis» bryter mot forordningen
  - Datatilsynet har ikke noen helt klokkeklar stoppknapp, men kan sette frister for tiltak og har en del «gjøre-livet-surt-for»-hjemler

Andre…?

- Artikkel 20, dataportabilitet
  - En rettighet dersom opplysninger er gitt med samtykke eller basert på avtale
  - Ikke obligatorisk for lovpålagte oppgaver, men kan for så vidt være en fin gest
  - Ivaretar ikke arkiv- eller «recordness»-egenskaper, det man får med fra virksomhet A sitt arkiv kan mangle arkivsystemintegritet hos ny virksomhet B
- Artikkel 25, innebygd personvern og personvern som standardinnstillinger
  - En plikt til å tvinge gjennom minimalitetsprinsippet i tekniske løsninger
  - Hvis man er «overivrig» vil det kanskje kunne gå på bekostning av tilstrekkelig dokumentasjon av saksbehandlingen, men man bryter ikke GDPR-regler ved å ta hensyn til reelle dokumentasjonsbehov

En slags konklusjon om «gjøremålplikter»

- Artikkel 30 er på mange måter nøkkelen til å kunne ivareta alle de øvrige pliktene som forutsetter dokumentasjon av og kommunikasjon om behandlingsaktiviteter
  - Ikke viktig om man kaller det behandlingsprotokoll eller internkontrollsystem
  - Det er en del krav til hva dokumentasjonen må inneholde
  - Må holdes a jour, være «levende»
- Gode grunner til at arkivtjenesten bør være på banen
  - Konkret: tidsfrister for sletting ≈ oppbevaringsfrister/retention schedule
  - Unngå dobbeltarbeid med tilhørende unødvendige feilkilder: behandlingsprotokoll ≈ styringssystem for dokumentasjon