# Identifisering, autentisering, elektroniske spor og innebygd personvern

DRI1010 – 15.3.2017

Jon Holden – jobe@holden.no

# Innhold

- Hva er identitet?
- Begrepet personopplysninger
  - Identifisering og autentisering
  - Fødselsnummer og biometri
- Elektroniske spor
- Innebygd personvern

# Identitetsbegrepet

- Prosedural – formell identifikasjon
  - Sosiale og økonomiske forhold, myndighetene
  - Rettigheter, plikter

- Sosialpsykologisk – hvem er jeg
  - Personlighetsutvikling
  - Interaksjon med andre, ulike roller

# Begrepet personopplysning – identifiseringskravet

- Pol § 2 nr 1: «personopplysning: opplysninger og vurderinger som **kan knyttes** til **en enkeltperson**»,
- Personverndirektivets fortale, avsnitt 26: «for at afgøre, om en person er **identificerbar**, tages alle de hjælpemidler i betragtning, der **med rimelighed kan tænkes** bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person»
- Personvernforordningens fortale, avsnitt 26
  - Omformulert med små tillegg: «for at afgøre, om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende."
  - Nytt «For at fastslå, om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning, såsom omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling.»

# Hvor entydig identifisering?

- For mange:
  - Jan Johansen – flertydig, 708 personer
  - Jan Thomas Johansen – 4 personer

- Personopplysning:
  - < 3-4 personer
  - en husstand

- Jan.johansen@gmail.com – entydig

- Formålsbestemmelsen relevant
  - Berører behandlingen personverninteresser? Hvor sterkt?
  - Husstand – noe flere

# Hvem kan identifisere? Hvordan?

- Hvem skal kunne identifisere personen?
  - Enhver
    - Ev. kun personer med lovlig tilgang til opplysningene?

- Hvilke hjelpemidler skal medregnes?
  - Ethvert som med rimelighet kan forventes brukt (nå eller seinere)
    - Kostnader, tid, teknologi
    - Ev. kun lovlige hjelpemidler?

# Grader av identifisering

- Identifisert
  - Entydige (systemovergripende) personalia/identifikator finnes
- Pseudonym
  - Vanlige identifiserende opplysninger holdes adskilt, teknisk og organisatorisk
    - Eks. særskilt angitt pseudonymforvalter, IPLOS-forskriften § 1-7
- Avidentifisert
  - Vanlige identifiserende opplysninger er fjernet, kan re-identifiseres vha. bakgrunnsinformasjon
- Anonym
  - Kan ikke identifiseres – *ikke identifiserbar*

# Bruk av fødselsnummer

- Pol § 12 første og annet ledd
  - «Fødselsnummer og andre entydige identifikasjonsmidler kan **bare nyttes** i behandlingen når det er **saklig behov** for **sikker identifisering** og metoden er **nødvendig** for å oppnå slik identifisering.
  - Datatilsynet **kan pålegge** en behandlingsansvarlig å **bruke** identifikasjonsmidler som nevnt i første ledd **for å sikre** at personopplysningene har **tilstrekkelig kvalitet**.»
- Sentralt moment
  - Konsekvenser av forvekslingsfare
  - Samfunnsbehov kan vektlegges – PVN liberal praksis i
  - «Nødvendig» - viser til risikovurderingen

# Bruk av fødselsnummer - praksis

- Forarbeidene
  - Ikke i «videobutikken på hjørnet»

- Skoleskyssordning – PVN-2009-15
  - Utveksling mellom
- Forvaltningen - sentrale offentlige registre
  - Folkeregisteret
  - Enhetsregisteret
  - Kontakt- og reservasjonsregisteret

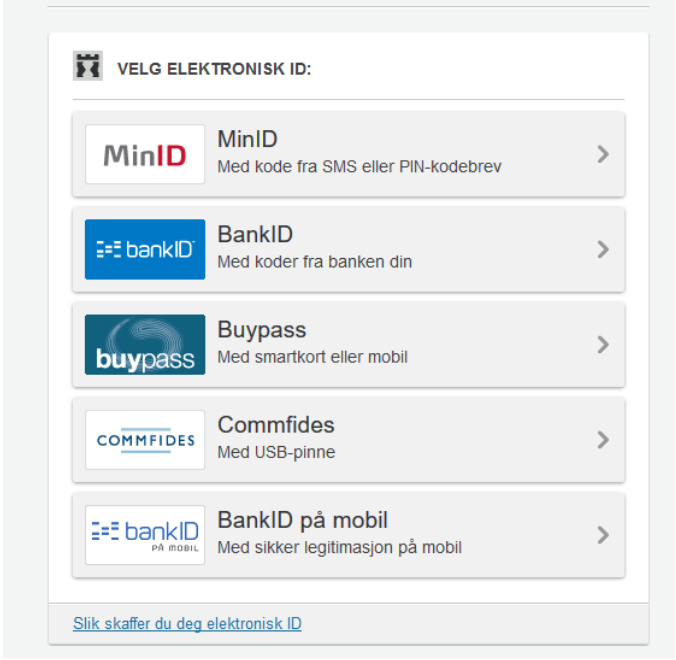
# Pseudonymisering

- Generelt lite brukt i forvaltningen
- PVN-2007-2 Bibliotek-Systemer
  - Mål: Bedre bokanbefalinger vha. korrelasjonsdatabase
  - Middel: Lagre opplysninger om hvilke bøker som lånes av låntakerne
  - Personverntiltak: Pseudonymisering
  - Problem: Hjemmel – ønsket ikke bygge på samtykke
  - Personvernnemndas konklusjon:
    - Ikke sensitive opplysninger
    - Små personvernulemper, ligger til rette for samtykke
    - Kan etableres, men samtykke kreves

# Autentisering og biometri

# Identifisering og autentisering

- Identifisere
  - Individualisere personen, muliggjøre knytning til andre opplysninger
  - Kan brukes om kombinasjonen identifisere og autentisere, men brukes ofte om påstanden alene
    - Eks. «Dette er nn», angitt vha. navn og fødselsdato eller fnr
      - Jon Berge Holden, 071168
      - <fødselsnummer>
- Autentisere
  - Bekrefte påstanden, med valgt grad av tillit (sikkerhet)
    - Egen løsning: lokal brukerkonto
    - Andres løsning (føderering) : BankID, Buypass, Google, Facebook, Microsoft, SPiD



# Sikkerhetsnivåer ved autentisering

- Rammeverk for autentisering og uavviselighet, FAD 2008
  - 4 nivåer
  - Nivå 3 – MinID, folkeregisterert adresse, tofaktor
  - Nivå 4 – BankID, Buypass, Commfides, fremmøtekrav, tofaktor
- Europeiske nivåer, eIDAS-gjennomføringsrettsak 1502/2015
  - 3 nivåer
  - Low-Substantial-High

# Tall

- Hver dag er det i snitt:
  - 250 000 innlogginger til offentlige tjenester (via ID-porten)
  - 2,7 millioner som bruker Facebook
  - 1 million som bruker Snapchat
  - 2 millioner som leser VG på nett
  - 6 millioner betalingskorttransaksjoner (des 2016)
- ? millioner innlogget på Android- eller Apple-enheter
- Finn: 6,3 millioner unike brukere hver uke

  - Kilde: Ipsos SoMe 4.kv 2016  Pressemelding Finn

# Autentisering

- Bekrefte påstand, typisk om identitet, eks. e-postadresse, fnr, navn

- Autentiseringsfaktorer (-midler)
  1. Noe du vet (passord)
  2. Noe du har (mobiltelefon, kodebrikke)
  3. Noe du er (fingeravtrykk, iris, ansikt)

  - 1 & 2 bygger på delte hemmeligheter

# Autentisering av attributter (istf. Identitet)

- Attributtautentisering
  - Eks. «over 18 år»
  - Eks. «under 15 år», «elev ved denne skolen»

# Biometri – noe du er

- Biometri – fra gr. bios=liv, metri=måling
- Mange mulige egenskaper:
  - Iris, fingeravtrykk, ansiktsgjenkjenning, stemmegjenkjenning, ganglag, håndskrift, tastemønster etc
  - Permanens og **unikhet** varierer
    - Unikhet=> ansett omfattet av pol § 12 iht PVN-praksis

- Noe du «er», ikke noe du «har»
  - Varierende motstandsdyktighet mht. manipuleringer - forfalskning og falsk
    - Eks. trelim og grafitt

# Biometri i norsk praksis

- Dekkes iht. PVNs praksis av pol § 12
  - «Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering».
- Flere saker
  - OK: Pålogging PC (Tysvær kommune), Adgangskontroll tankanlegg (Esso)
  - Ikke: Treningssenter
  - Merk:
    - PVN 2011-11 (Visma Retail, alderskontroll ved ølkjøp) gjaldt fingeravtrykk, men ble ikke sett som entydig identifikasjonsmiddel – kun alderskontroll
    - PVN 2011-12 (Fitness24seven, adgangskontroll): fingeravtrykk kun lagret i kort, adgangskortet gav identifiseringen

# Elektroniske spor

# Hva er elektroniske spor

- “Spor” er en type personopplysninger som den aktuelle personen selv etterlater seg gjennom sine egne handlinger (Jon Bing, 2003)

- Tre hovedkilder (vurdert i 2003)
  - Telekommunikasjon
  - Betalingsformidling
  - Adgangskontroll
- Nyere kilder
  - Nett- og mobilbruk
  - Nett-tilknyttede dingser (internet of things)
- Problemstillinger
  - Bruk av spor
  - Pålegg om spor
  - Personvernøkende teknologier
  - Tilgangsregime

# Eksempel - telekommunikasjon

- Før 1993
  - Tellerskritt – ingen lagring av hvem som ringte hvem
- Sentakst (sentral taksering)
  - Lagring av kommunikasjonsdata for takseringsformål
  - Plikt til sletting, når behovet var opphørt
- 2006
  - Datalagringsdirektivet (2006/24/EF)
    - Plikt til lagring, uavhengig av faktureringsbehov (eks. data, sted)
    - Minste lagringstid
  - 2014: Bestemmelser om oppbevaring kjent ugyldig av EU-domstolen pga manglende proporsjonalitet (C-293/12 og C-594/12)

# Eksempel: Nye strømmålere

Alle husstander får en såkalt smartmåler som registrerer strømforbruket på timebasis og sender informasjonen om strømforbruket til nettselskapet. […]

Ved å analysere detaljerte data om strømforbruk kan det i fremtiden være mulig å anta eller å forutsi når personene i hjemmet er på ferie eller på jobb, når de sover og er våkne, om de ser på TV eller bruker elektriske verktøy eller utstyr, hvor ofte de vasker klær eller om de bruker spesielt medisinsk utstyr. […]

Det legges allerede nå til rette for en mulighet til å øke avlesinghyppigheten fra smarte strømmålere fra hver time til hvert kvarter. Det er også aktører som ønsker kontinuerlig avlesing av strømforbruket til en husstand.

- https://www.datatilsynet.no/Teknologi/Strommaling/

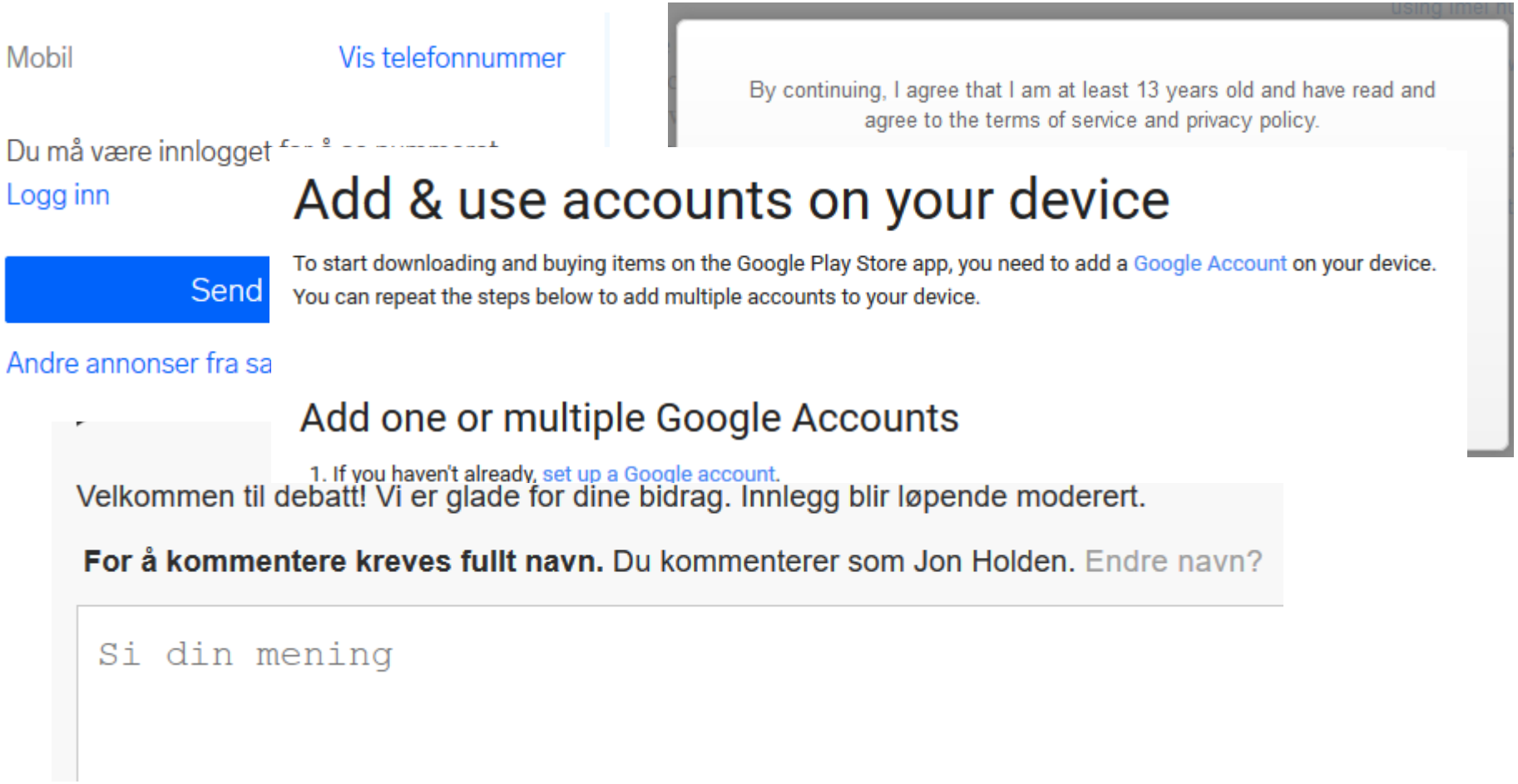
# Strømmålere: Mulige personverntiltak

- Tilpass målehyppigheten til faktureringen
- Smartere målere – lokal behandling av forbruksdata
- For noen formål er kan aggregerte opplysninger (for flere husstander), eller utvalgte data (for tilfeldig valgte husstander), være tilstrekkelig
- Sletting
- https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

# Elektroniske spor - noen identifiseringskilder

- Betalingsmiddel, fordelskort
- Mobiltelefon
  - Sim-kortets nummer (mobilnummer, imsi)
  - Telefonens identifikator (imei)
  - Nettverksadresser (bluetooth, wifi)
- Nettbruk
  - aktive innlogginger (eks. kjent via informasjonskapsler)
    - google, microsoft, facebook, linkedin, twitter, id-porten
  - ip-adresser (særlig IP6)
  - nettlesersignaturer (panopticlick)
  - skreddersydde adresser (url, eks. sporing i nyhetsbrev)
  - informasjonskapsler (cookies)
  - bildesporing/web beacons/bugs
- Bilskilt, bombrikke
- RFID-brikker

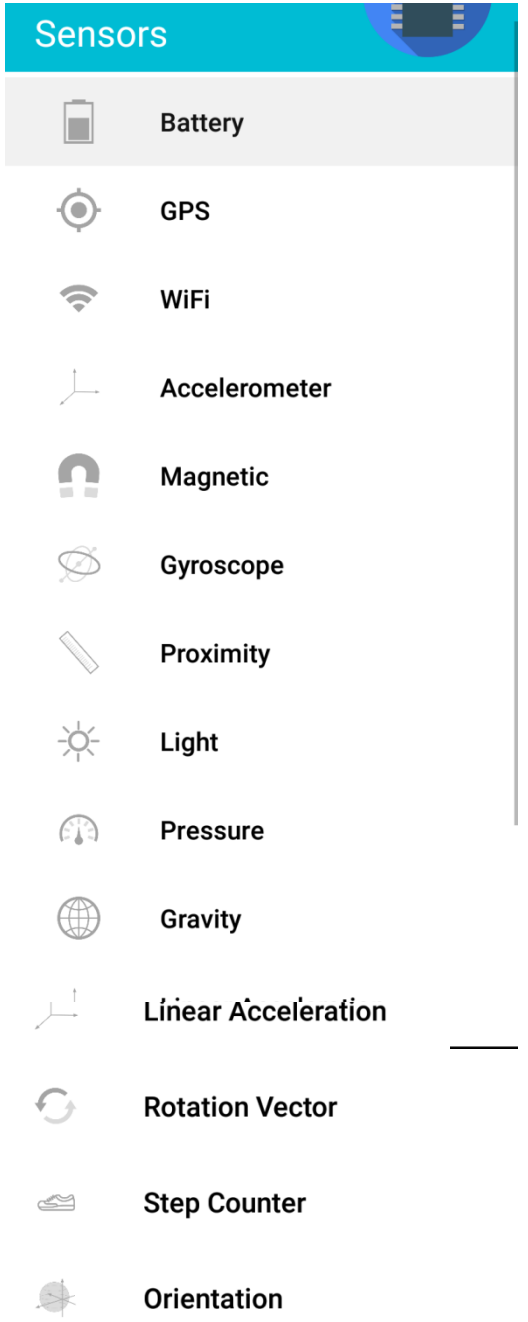
# Oftere krav om identifisering og autentisering



# Hva slags opplysninger?

- Innkjøp
- Nettbruk
  - Klikkstrøm
- Bevegelser
- Strømforbruk

- M.v.



# Noen bruksområder for elektroniske spor

- Grunnlag for målrettet reklame
  - Jf. sammenheng mellom tidligere kjøp og framtidige kjøp
  - Eks. tilbud på babyartikler til antatt gravide

- Grunnlag for prising basert på risiko
  - Jf. sammenheng risiko og atferd
    - Nattkjøring, fart, rask akselerasjon, brå bremsing er indikatorer på høy risiko

- Grunnlag for tilpassede tjenester
  - Venneforslag, anbefalte videoer, søkeresultat, visning av annonser og nyheter

# Bruk av elektroniske spor

- Grunnlag for kontrolltiltak
  - Avfallsservice-saken, Høyesterett 2013, jf. PVN-2011-4.
    - Kjøring av avfallstransport ble logget basert på GPS
    - Opprinnelig formål var administrativt: utarbeide arbeidsplaner og normering av rutene
    - Ved mistanke om timeføringsjuks ble imidlertid denne kjøreloggen kontrollert og sammenholdt med timelister. Dette var ulovlig iht. HR
      - Bruk av GPS-loggen til kontroll var uforenlig med opprinnelig formål, og krevde særskilt samtykke fra de registrerte, pol § 11 c

# Elektroniske spor – og personvernregler

- Er det behandling av personopplysninger?
  - Er personen identifisert?
  - Kan personen identifiseres?
    - Hvilke hjelpemidler er rimelig å anta kan bli tatt i bruk?
  - Hvor sikker vil identifikasjonen være?
    - Færre enn 3-4, ev. ned til familie?
- Hvis ja, bl.a.:
  - Grunnkrav, § 11
  - Hjemmelskrav
  - Formålsbegrensning
  - Sikkerhet mot annen bruk


trumf


coop
liit
diit

# Eksempel Coop litt ditt

- **Innmelding: «**Jeg samtykker i at laget og Coop Norge SA behandler personopplysninger om meg i henhold til de formål mv. som er beskrevet nærmere i "Personvernpolicy for Coop".»
- **Personvernpolicyen:**

  **Hvilke opplysninger registreres om deg?**

  *a)Gjennom medlemskap i Coop*
  … I tillegg blir det registrert opplysninger om medlemskortet, konkrete kjøpsopplysninger ved handel i Coops butikker og kjøpeutbytte. Kjøp blir registrert som et medlemskjøp når ditt medlemskort brukes, og da registreres bl.a. beløp, det enkelte produkt som kjøpes og kjøpstidspunkt. Tilsvarende informasjon kan bli registrert når ditt medlemskort brukes hos samarbeidspartnere for å få medlemsbonus.

  **Hvorfor behandler vi opplysningene om deg og hva brukes opplysningene til?**

  Vi behandler også registrerte personopplysninger, herunder kjøpsopplysninger, slik at vi har mulighet til å varsle deg hvis et produkt du har kjøpt kan vise seg å være skadelig eller lignende.

  Vi behandler i tillegg registrerte personopplysninger herunder din kontaktinformasjon, slik at vi kan sende deg informasjon og tilbud på e-post og/eller mobil, så fremt du har bedt om dette.

  Så fremt du har samtykket, behandler vi dessuten registrerte personopplysninger, som nevnt ovenfor, slik at vi kan tilpasse medlemskapet til deg og dine preferanser. Blant annet kan vi tilpasse medlemstilbud (f.eks. produkttilbud og annen markedsføring fra Coop eller samarbeidspartnere), medlemsinformasjon, nettsider, apper, digital kommunikasjon og de øvrige tjenester og fordeler som tilbys våre medlemmer.

  **Leverer vi ut opplysningene som er registrert om deg?**

  Vi leverer ikke ut registrerte opplysninger om deg til andre organisasjoner eller virksomheter uten ditt frivillige, uttrykkelige og informerte samtykke. Dersom du gir et slikt samtykke, vil vi bare utlevere opplysningene innenfor det formål samtykket omfatter.

# Særlig om elektroniske spor i arbeidslivet m.v.

- Arbeidsmiljøloven kapittel 9
  - Saklig grunn
  - Ikke uforholdsmessig
  - Drøfting, informasjon, evaluering
  - Særregler om innsyn i e-post o.a., personopplysningsforskriften kapittel 9
    - Nødvendig eller mistanke om grovt brudd
    - I utgpkt. varslings- og uttalerett før innsyn, rett til å være til stede og bistås
- Skal logges hvem som har hatt innsyn i opplysningene
  - Pasientjournalloven § 18
- Autorisert bruk og forsøk på uautorisert bruk skal oppbevares minst 3 mnd, personopplysningsforskriften § 2-16

# Personvernøkende teknologi – innebygd personvern

# Innebygd personvern – nytt krav

- Personvernforordningen artikkel 25
  - Beh.ansvarlig skal implementere ”... 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.”
  - Beh.anvarlig gjennomfører ”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. ...
- Prinsippene, jf. art 5:
  - Lovlighet, rimelighet og gjennomsiktighet; formålsbegrensning; dataminimering; riktighet; oppbevaringsbegrensning; infosikkerhet*; ansvarlighet

# Personvernforordningens nye bestemmelser om pseudonymisering

- Art 4 nr 5 – definisjon av pseudonymisering
  - 5) »pseudonymisering«: behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er **underlagt tekniske og organisatoriske foranstaltninger** for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person
- Pseudonymisering er relevant ifmb.
  - Viderebruk til andre formål, jf. art 6 nr 4 e og art 89 nr 1 (statistikk etc)
  - Krav til innebygd personvern, art 25
  - Informasjonssikkerhet, art 32 nr 1 a
  - Bransjenormer, art 40 nr 2 d

# Sensitive personopplysninger

# Sensitive personopplysninger

- Uttømmende definisjon i pol § 2 nr 8:
  - Opplysning **om**
    - Rase/etnisk bakgrunn, politisk, filosofisk, religiøs oppfatning
    - Straffbare handlinger
    - Helse
    - Sex
    - Fagforeningsmedlemskap
- Dekker både opplysningstype (adresse) og -verdi (Ullersmo)
  - Dekker direkte opplysninger (katolikk) og tilstrekkelig sikre slutninger (Ullersmo)
- Betydning: Skjerpet hjemmelskrav (grunnlag også i § 9), konsesjonsplikt (§ 33)