Innebygd personvern og risikovurdering

Kontaktkonferansen 2023

Veronica Jarnskjold Buer | Avdelingsdirektør for Teknologi, Analyse og sikkerhet, Datatilsynet

27.April 2023

Tilsyn i to faser

Tilsyn i kommuner og fylkeskommuner

Vi har satt i gang et større tilsynsarbeid med nærmere hundre norske kommuner og fylkeskommuner sin ivaretakelse av personopplysningssikkerheten.

https://www.datatilsynet.no/contentassets/ad8edfe9d6f44d739adceff3aee0eb2f/brevkontroll---palegg-om-a-sende-informasjon.pdf


Art, omfang, formål, sammenheng
Kilder og mottagere
Systematisk beskrivelse av behandlingen
Ansvarsforhold
Informasjonssikkerhet
Personvernprinsipper
Rettslig grunnlag
Nødvendighet og proporsjonalitet
Rettigheter
Friheter
Plikter for alle

Hva skal jeg bruke tiden deres til?

- Eksempel på en arkivsak som gav gebyr
- Hva er innebygd personvern?
- Smakebit fra EDPB /personvernrådets retningslinjer for innebygd personvern
- Risikovurderinger
- Arkivprosjekt i Datatilsynets sandkasse og KI
- Refleksjoner om risiko ved arkiv

DEUTSCHE WOHNEN

Innebygd personvern er å bygge

- **personvernprinsippene,**
- **rettighetene og**
- **frihetene**

inn i arkitekturen.

- sw, applikasjoner, tjenester, roboter, algoritmer for automatiske beslutninger, kunstig intelligens, deep learning osv.

Hvem har plikter og rettigheter

- De **registrerte** har **rettigheter og friheter**
- Behandlingsansvarlig, databehandler, underleverandører har **plikter**

Personvernprinsippene, art 5.

Lovlig, rimelig og gjennomsiktig
Rettslig grunnlag. Respekter de registrertes interesser og rimelige forventninger. Informasjon skal gis på en tilgjengelig og forståelig måte.

Formålsbegrensning
Opplysningene skal brukes til spesifikke, uttrykkelig angitte og legitime formål. Opplysningene skal ikke brukes til andre uforenlige formål

Dataminimering
Personopplysningene skal være tilstrekkelige, relevante og begrenset til hva som er nødvendig for formålet.

Korrekte og oppdaterte
Opplysningene skal være korrekte og om nødvendig ajourførte. Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

Rutiner for lagring og sletting
Personopplysninger skal ikke lagres lengre enn det som er nødvendig for formålet. Automatiske sletterutiner.

Integritet og konfidensialitet
Personopplysninger skal sikres mot uautorisert eller ulovlig tilgang og mot utilsiktet tap, ødeleggelse eller skade. Det skal brukes egnede tekniske og organisatoriske tiltak.

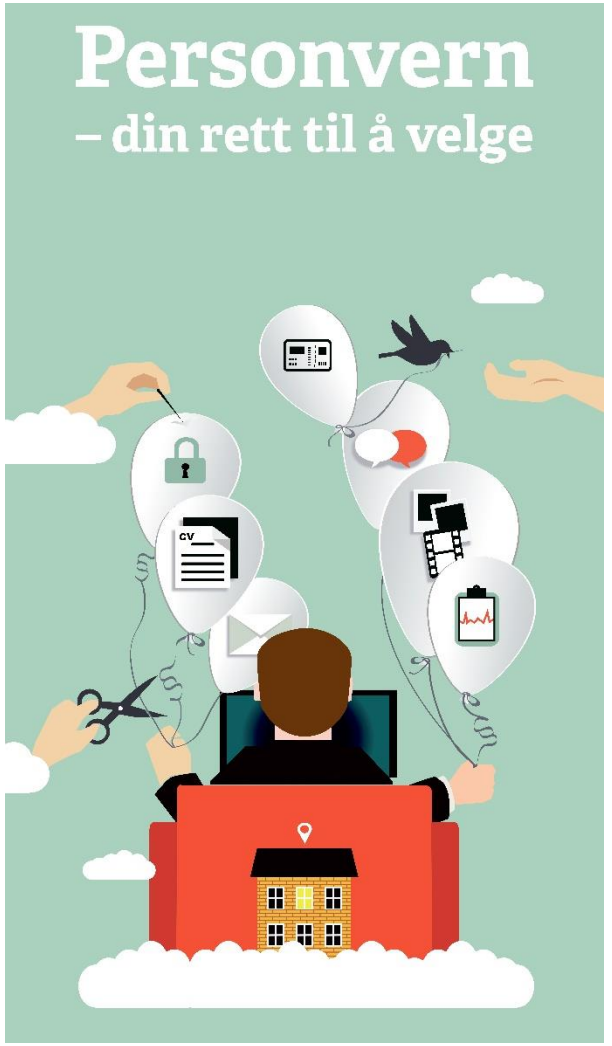
Ansvarlighet
Den behandlingsansvarlige har ansvar for, og må kunne dokumentere, at regelverket blir etterlevd

De registrertes rettigheter

- Informasjon (art 12-14)
- Innsyn (art 15)

Forutsetning for de resterende rettigheter

- Korrigering (art 16 & 19)
- Sletting/Retten til å bli glemt (art 17 & 19)
- Rett til begrensning (ny, art 18 &19)
- Dataportabilitet (ny, art 20)
- Innsigelse (ny, art 21)
- Automatiserte avgjørelser, inkludert profilering (ny, art 22)



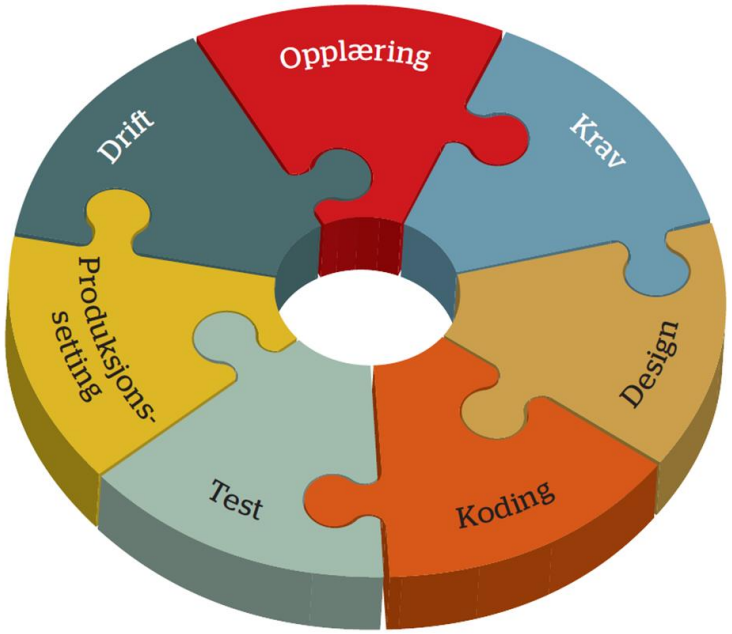
Den registrertes friheter, jf. EMK, fortalen (4) og art. 24 (1).

De registrertes friheter:

- Retten til privatliv
- Kommunikasjonsvern
- Ytringsfrihet
- Tankefrihet
- Bevegelsesfrihet
- Forbud mot diskriminering
- Samvittighets- og religionsfrihet

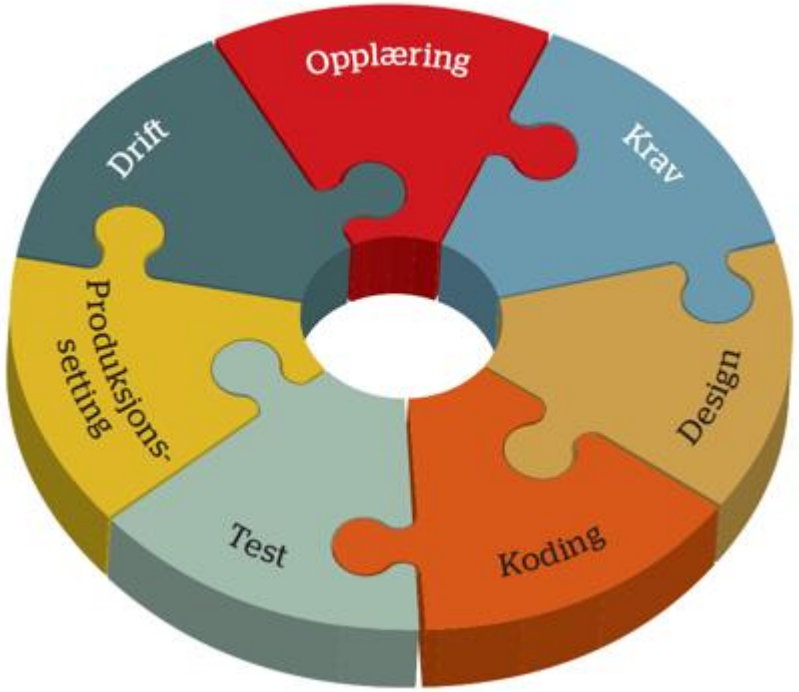
Retningslinjer for Artikkel 25.

- 2017 utarbeidet og lanserte det norske Datatilsynet [Veileder for programvareutvikling med innebygd personvern]



- 2018 ble det norske Datatilsynet tildelt rollen som rapportør for personvernrådets (EDPBs) [Veileder for artikkel 25, innebygd personvern og personvern som standard innstilling]
- 2019: Offentlig høring
- 2020.10.20: Godkjent

Veileder for programvareutvikling med innebygd personvern



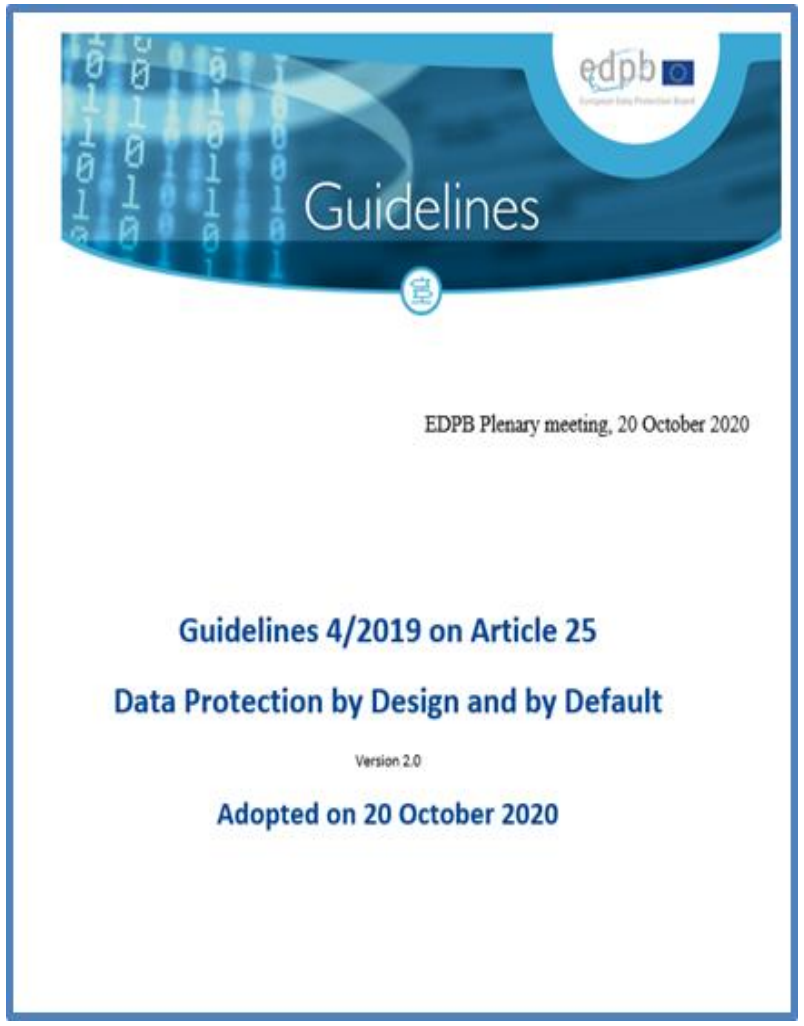
- Ha et rammeverk for programvareutvikling, og inkluder disse sju aktivitetene er i rammeverket.

- Obligatorisk
- Tekniske og organisatoriske tiltak.
- Ivareta **personvernprinsipper** og den **registrertes rettigheter og friheter**.
- Det minst personverninngripende alternativet som standard, mht. mengde, omfang, lagringstid, tilgjengelighet.

- **Behandlingsansvarlige**: Krav til å benytte programvare, løsninger etc. som har innebygd personvern som standardinnstilling.

- Veileder og Sjekkliste (mer teknisk)

EDPBs Veileder for artikkel 25, innebygd personvern og personvern som standard innstilling



- Artikkel 25 en plikt for den behandlingsansvarlige ved anskaffelse, utvikling, revisjon og ROS.
- Kjerne-krav: Implementering av personvernprinsippene, rettigheter og friheter
  - Innebygd og som standardinnstilling
  - Tilstrekkelige tiltak og nødvendige garantier
  - ***Effektivt***
  - Momenter for innebygd personvern
  - Tid: før behandling deretter regelmessig
- Nøkkelelementer ved utforming av tiltak og illustrerende eksempler for personvernprinsippene
- Sertifisering av innebygd personvern
- Håndhevelse av artikkel 25
- Anbefalinger

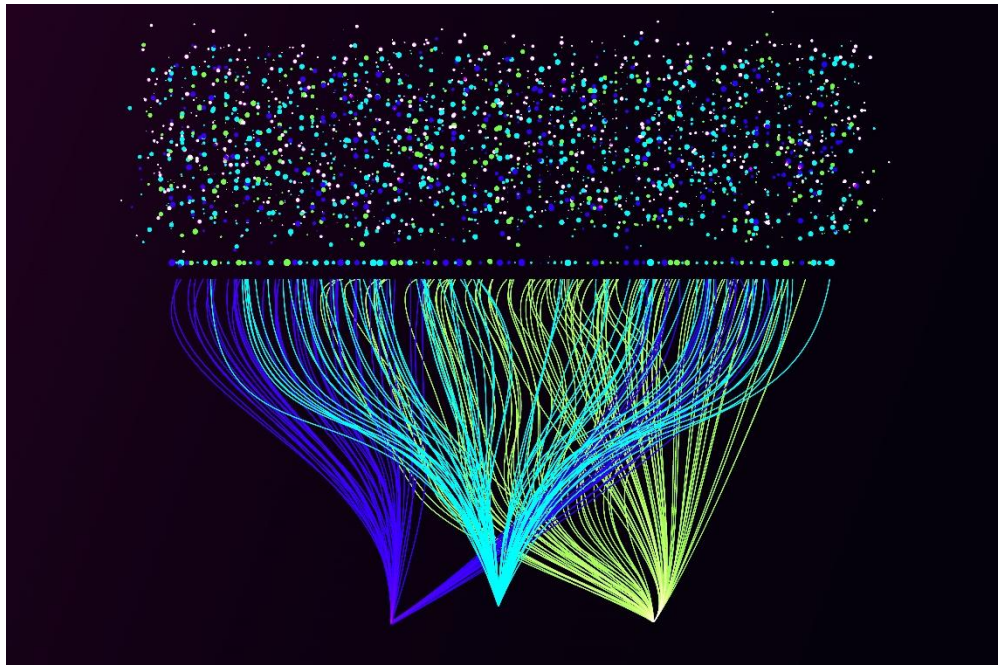
[Innebygd personvern og personvern som standard | Datatilsynet]

Momenter som man skal ta hensyn til ved design av løsning med for innebygd personvern

- "State-of-the-art" / Den tekniske utviklingen
- Gjennomføringskostnadene
- Behandlingens art, omfang, formål og sammenheng
- Risiko, sannsynlighet og alvorlighetsgrad som behandlingen kan medfører for de registrertes rettigheter og friheter

State-of-the-art / den tekniske utviklingen

- Et dynamisk konsept



- Kan være tilknyttet teknologi eller et hvilket som helst annet felt.
  - Eksempel: Trussel ved social engineering. Behandlingsansvarlig må være oppdatert på tiltak til å lære ansatte til å avsløre slike angrep.
- Krever at den behandlingsansvarlige holder seg oppdatert på den tekniske utviklingen for å sikre at personvernprinsippene fortsatt ivaretas
  - Eksempel: Krypteringsteknologi som er tatt i bruk blir utdatert. Det har kommet en algoritme som knekker krypteringsnøkkelen. Behandlingsansvarlig må revurdere/ oppdatere tiltak for å sikre personopplysningene.
- Standarder kan gi en pekepinn på den tekniske utviklingen
  - Holde seg oppdatert
  - Vurdere om den enkelte standard ivaretar personvern i tråd med personvernforordningen

Gjennomføringskostnadene

- Kostnader knyttet til å implementere tiltak for å ivareta personvernprinsippene, rettigheter og friheter

- Ressurser generelt
  - Tid, arbeidskraft, penger

- Må ikke bruke den dyreste løsningen, så lenge tiltak som iverksettes er tilstrekkelige og effektive

- Høye gjennomføringskostnader imidlertid ingen unnskyldning for å ikke ivareta personvern

Behandlingens art, omfang, formål og sammenheng

Art

Behandlingens iboende karakteristikk:

- Vanskelig å utøve sine rettigheter
- Uforutsigbarhet, liten åpenhet og usikkerhet om ivaretakelse av prinsipper
- Systematisk behandling
- Særlige kategorier
- Skjevt maktforhold
- Ny teknologi / gammel teknologi brukt på ny måte
- Kompleksitet
- Automatiske avgjørelser

Omfang

Behandlingens størrelse/rekkevidde:

- Antall registrerte involvert (tall eller %)
- Volumet av data (antall variabler, detaljer)
- Lagringstid (kort, tidsavgrenset, permanent)
- Geografisk omfang (lokalt, regionalt, nasjonalt, internasjonalt, globalt)

Formål

Hva skal personopplysningene brukes til:

- Kontrollformål
- Behandling med mål om å ta beslutninger som får betydning for den registrerte
- Å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personopplysninger

Sammenheng

Hvilken forventning om personvern omgir den konkrete behandlingen:

- Forventning om konfidensialitet (helse, velferd, arbeidsforhold..)
- Forventning om privatliv (hjem, rekreasjon..)
- Behandling av personopplysninger fra ulike datasett som er innsamlet for ulike forhold
- Kjeden av aktiviteter i behandling
- Deling med andre behandlingsansvarlige eller virksomheter

Risiko

- Den risikobaserte tilnærmingen fremkommer i flere av personvernforordningens bestemmelser
  - F. eks. artikler 24, 25, 32, 35.

- Art 25: Risikobasert tilnærming til å identifisere egnede tiltak for å ivareta personvernprinsippene, rettigheter og friheter
  - Personopplysninger/personopplysning svern er «assets» som skal beskyttes
  - Risiko for brudd på prinsippene og rettigheter og friheter
    - Sannsynlighet for og alvorlighet av brudd

Risikovurdering

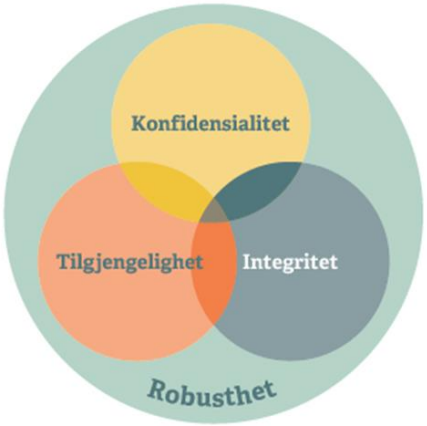
- Risiko betegner forholdet mellom **verdi-trussel-sårbarhet**, og konsekvenser av dette.

- Formål:
  - Iverksette organisatoriske og tekniske sikkerhetstiltak som mitigerer risiko, slik at personopplysningene våre er tilstrekkelig ivaretatt

- Virksomheten skal gjennomføre risikovurdering før, og regelmessig ved endringer i forhold som kan påvirke informasjonssikkerheten
  - for eksempel endringer i behandlinger, informasjonssystem, trusselbildet, sikkerhetstiltak
  - Risikovurderingen skal dokumenteres.

Risikovurdering

- For å gjøre en risikovurdering
  - systematisk beskrivelse av behandlingen
    - Behandlingens art, omfang, formål, sammenheng
    - Kilder, mottagere, dataflyt
    - Informasjonssikkerhet
    - Ansvarsforhold
  - Nødvendighet og proporsjonalitet
    - Personvernprinsippene
    - Rettigheter & friheter
  - Dokumenter risikovurderingene



Artikkel 32
Personopplysningssikkerhet

Personvern som standard

- Standardinnstilling at kun det som er nødvendig for å oppnå formålet kan behandles – nødvendighet og formål

  - Særlig uttrykk for at **dataminimeringsprinsippet** skal være innebygd
    - mengde og detaljnivå
    - Omfanget av behandlingen
    - Lagringstid
    - Tilgjengelighet
      - Hos behandlingsansvarlig og
      - ved offentliggjøring

- Ved bruk av hyllevarer, må behandlingsansvarlig stille krav til, tilpasse og vedlikeholde standardinnstillingene til egne behandlingsaktiviteter

Kapittel 3 Implementering av personvernprinsippene relatert til kravene i DPbDD

Kapittel 3

- Momentene for innebygd personvern skal hensyntas **gjennom hele livsløpet** for behandlingsaktiviteten

- Personvernprisnippene, rettigheter og friheter må implementeres for å oppnå DPbDD
  - Krever forståelse av betydningen av artikkel 5, rettigheter og friheter

- For å operasjonalisere innebygd personvern har vi laget en liste av nøkkelelementer for hver av prinsippene

- Retningslinjene gir ekspempler relatert til personvernprisnippene, men det samme gjelder for implementering av rettighetene og frihetene

- Ansvarlighetsprinsippet er overordnet
  - Krever ansvarlighet ved valg og implementering av nødvendige tiltak.

Lovlighet

- Den behandlingsansvarlige må identifisere et gyldig behandlingsgrunnlag for behandling av personopplysninger.

- Tiltak og sikkerhetstiltak skal sørge for at **hele** behandlingslivssyklusen er i tråd med det relevante juridiske grunnlaget for behandlingen.

Nøkkelelementer	Lovlighet
Relevans	Rett behandlingsgrunnlag skal brukes på behandlingen
Differensiering	Behandlingsgrunnlaget som brukes for hver behandlingsaktivitet skal være differensiert
Spesifisert formål	Det aktuelle behandlingsgrunnlaget må være tydelig knyttet til det spesifikke formålet med behandlingen.
Nødvendighet	Behandling må være nødvendig og ubetinget for at formålet skal være lovlig.
Selvbestemmelse	Den registrerte skal gis den høyeste grad av selvbestemmelse som mulig med hensyn til kontroll over personopplysninger innenfor rammene av det juridiske grunnlaget
Samtykke	Samtykke må være frivillig, spesifikt, informert og utvetydig. Det bør tas særlig hensyn til barn og unges evne til å gi samtykke.
Trekke samtykke	Der samtykke er behandlingsgrunnlaget, skal tilbaketrekking være like enkelt som å gi samtykke. Hvis ikke, er samtykke ikke gyldig i tråd med personvernforordningen.
Interesseavveining	Der legitime interesser er behandlingsgrunnlaget, må den behandlingsansvarlige foreta en vektet interesseavveining, med særlig vekt på maktbalanse, spesielt barn under 18 år og andre sårbare grupper. Det skal være tiltak og garantier for å redusere den negative innvirkningen på de registrerte.
Forutbestemmelse	Det juridiske grunnlaget skal være etablert før behandlingen finner sted.
Opphør	Hvis det juridiske grunnlaget opphører å gjelde, skal behandlingen opphøre tilsvarende
Justering	Hvis det er en gyldig endring av behandlingsgrunnlag, må den faktiske behandlingen justeres i samsvar med det nye behandlingsgrunnlaget.
Ansvarstildeling	Når det er tenkt på felles kontroll, må partene fordele på en klar og gjennomsiktig måte sitt respektive ansvar overfor den registrerte, og utforme tiltakene for behandlingen i samsvar med denne tildelingen

Hvordan skal arkitekturen designes slik at RETTFERDIGHET blir innebygd og standardinnstilling

- Rettferdighet er et overordnet prinsipp som krever at personopplysninger skal behandles slik at behandlingen ikke medfører uberettiget skade, blir ulovlig diskriminerende, er uventet eller villedende for den registrerte.

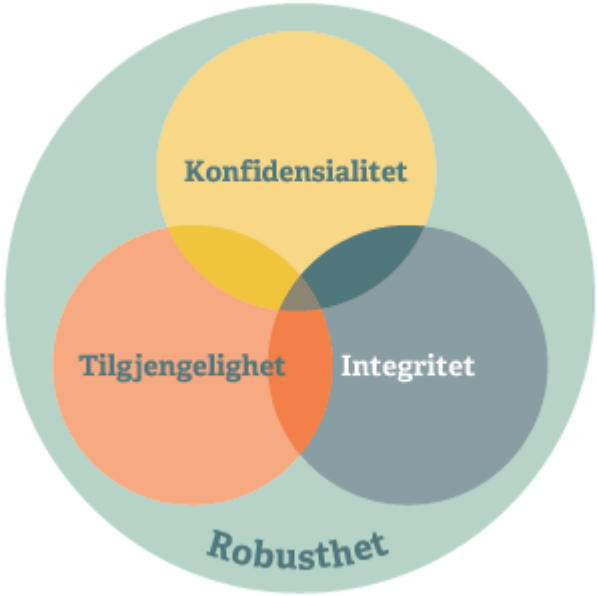
- Tiltak og garantier som implementerer rettferdighetsprinsippet, omfatter også
  - retten til informasjon
  - retten til å gripe inn
  - retten til å begrense behandlingen
  - Men også…

Nøkkelelement	Rettferdighet
Selvbestemmelse	Den registrerte bør gis den høyeste grad av selvbestemmelse som er mulig for å bestemme bruken av deres personlige data, så vel som over omfanget og vilkårene for den bruken eller behandlingen.
Interaksjon	Den registrerte må kunne kommunisere og utøve sine rettigheter med hensyn til personopplysningene som behandles av den behandlingsansvarlige.
Forventning	Behandlingen skal stemme overens med de registrertes rimelige forventninger
Ikke-diskriminering	Den behandlingsansvarlige skal ikke urettferdig diskriminere de registrerte
Ikke-utnyttelse	Behandlingsansvarlig skal ikke utnytte behovene eller sårbarhetene til registrerte
Forbrukervalg	Behandlingsansvarlig skal ikke "låse" brukerne på en urettferdig måte. Hver gang en tjeneste som behandler personopplysninger er proprietær, kan den opprette en innlåsing i tjenesten, noe som kanskje ikke er rettferdig, hvis det forringer de registrertes mulighet til å utøve sin rett til dataportabilitet i samsvar med artikkel 20.
Maktbalanse	Maktbalanse bør være et sentralt mål for forholdet mellom kontrolleren og den registrerte. Ubalanser i makt bør unngås. Når dette ikke er mulig, bør de anerkjennes og regnskapsføres med passende mottiltak.
Ingen risikooverføring	Behandlingsansvarlig bør ikke overføre risikoen ved bedriften til de registrerte
Ingen bedrag	Informasjonsbehandling og alternativer for databehandling skal gis på en objektiv og nøytral måte, og unngå villedende eller manipulerende språk eller design
Respekter rettigheter og friheter	Den behandlingsansvarlige må respektere de registrertes grunnleggende rettigheter og friheter, og iverksette passende tiltak og garantier og ikke berøre disse rettighetene og frihetene med mindre det er uttrykkelig begrunnet i loven.
Etisk	Den behandlingsansvarlige bør se prosessens bredere innvirkning på enkeltpersoners rettigheter og verdighet
Sannferdig	Den behandlingsansvarlige må gjøre tilgjengelig informasjon om hvordan de behandler personopplysninger, de skal oppføre seg slik de erklærer at de vil og ikke villede de registrerte.
Menneskelig inngripen	Behandlingsansvarlig må innlemme kvalifisert menneskelig inngripen som er i stand til å avdekke forstyrrelser som maskiner kan skape i samsvar med retten til ikke å bli gjenstand for automatisert individuell beslutningstaking i artikkel 22
Rettferdige algoritmer	Vurder regelmessig om algoritmer fungerer i tråd med formålene, og juster algoritmene for å redusere avdekkede skjevheter og sikre rettferdighet i behandlingen. De registrerte bør informeres om hvordan behandlingen av personopplysninger fungerer, basert på algoritmer som analyserer eller spår om dem, for eksempel arbeidsytelse, økonomisk situasjon, helse, personlige preferanser, pålitelighet eller atferd, plassering eller bevegelse


SLANE
CO.NZ
DEN EGENTLIGE HENSIKTEN MED URINTESTINGEN ER VEL Å NEDVERDIGE VÅRE ANSATTE?
CHRIS

Integritet og tilgjengelighet

- Personopplysningssikkerhetstiltak skal beskytte mot:
  - Uautorisert, uriktig eller ulovlig behandling
  - mot utilsiktet tap
  - ødeleggelse
  - skade



- Tiltakene skal opprette og forbedre sikkerhetsfunksjonene

- Ansvar for:
  - Vurdere om behandlingen kontinuerlig utføres ved bruk av egnede midler
  - Vurdere om valgte tiltak faktisk motvirker eksisterende sårbarheter
  - Regelmessig evaluering av tiltakene

- Tilrettelegger for
  - overholdelse av de andre prinsippene
  - effektiv utøvelse av enkeltpersoners rettigheter

Nøkkelelementer	Integritet og tilgjengelighet
Informasjonssikkerhets-styringssystem (ISMS)	Ha et operativt middel til å administrere policyer og prosedyrer for informasjonssikkerhet
Risikoanalyse	Vurder risikoen mot sikkerheten til personopplysninger ved å vurdere virkningen på enkeltpersoners rettigheter og mot identifiserte risikoer. For bruk i risikovurdering: utvikle og vedlikeholde en omfattende, systematisk og realistisk "trusselmodellering" og en angrepsoverflate-analyse av den designede programvaren for å redusere angrepsvektorer og muligheter for å utnytte svake punkter og sårbarheter
Sikkerhet ved design	Vurder sikkerhetskrav så tidlig som mulig i systemdesign og utvikling og kontinuerlig integrere og utføre relevante tester
Vedlikehold	Regelmessig gjennomgå og teste programvare, maskinvare, systemer og tjenester, etc. for å avdekke sårbarheter i systemene som støtter behandlingen
Styring av adgangskontroll	Bare autorisert personell som trenger det, skal ha tilgang til de personopplysningene som er nødvendige for behandlingsoppgavene sine, og kontrolleren skal skille mellom tilgangsrettigheter til autorisert personell o Begrensning av tilgang (agenter) - Form databehandlingen på en måte som et minimalt antall mennesker trenger tilgang til personopplysninger for å utføre sine plikter, og begrense tilgangen deretter. o Begrensning av tilgang (innhold) - I sammenheng med hver behandlingsoperasjon, begrens tilgangen til bare de attributtene per datasett som er nødvendige for å utføre denne operasjonen. Videre begrense tilgangen til data som gjelder de registrerte som er under den respektive ansattes ansvarsområde. o Tilgangssegregering - Form databehandlingen på en måte slik at ingen enkeltpersoner trenger omfattende tilgang til alle data som er samlet inn om en registrert, og enda mindre alle personopplysninger for en bestemt kategori av registrerte.
Sikker overføring	Overføringer skal sikres mot uautorisert og utilsiktet tilgang og endringer
Sikker lagring	Datalagring skal være sikret mot uautorisert tilgang og endringer. Det bør være prosedyrer for å vurdere risikoen for sentralisert eller desentralisert lagring, og hvilke kategorier personopplysninger dette gjelder. Noen data kan trenge ytterligere sikkerhetstiltak enn andre eller isolasjon fra andre
Pseudonymisering	Personopplysninger og sikkerhetskopier / logger bør pseudonymiseres som et sikkerhetstiltak for å minimere risikoen for potensielle datainnbrudd, for eksempel ved bruk av hashing eller kryptering.
Sikkerhetskopier / logger	Oppbevar sikkerhetskopier og logger i den grad det er nødvendig for informasjonssikkerhet, bruk revisjonsspor og hendelsesovervåking som en rutinemessig sikkerhetskontroll. Disse skal beskyttes mot uautorisert og utilsiktet tilgang og endring og gjennomgås regelmessig, og hendelser bør håndteres raskt
Katastrofegjenoppretting / forretningskontinuitet	Adresser informasjonssystemets katastrofegjenoppretting og forretningskontinuitetskrav for å gjenopprette tilgjengeligheten av personopplysninger som følger opp større hendelser.
Beskyttelse i henhold til risiko	Alle kategorier av personopplysninger bør beskyttes med tilstrekkelige tiltak med hensyn til risikoen for sikkerhetsbrudd. Data som gir spesielle risikoer bør, når det er mulig, holdes atskilt fra resten av personopplysningene
Sikkerhetshendelsesresponshåndtering	Ha på plass rutiner, prosedyrer og ressurser for å oppdage, inneholde, håndtere, rapportere og lære av brudd på data
Hendelseshåndtering	Behandlingsansvarlig bør ha prosesser på plass for å håndtere brudd og hendelser for å gjøre prosesseringssystemet mer robust. Dette inkluderer varslingsprosedyrer, som forvaltning av varsling (til tilsynsmyndigheten) og informasjon (til registrerte).

Ansvarlighet

- Påvise etterlevelse med alle personvernprinsippene

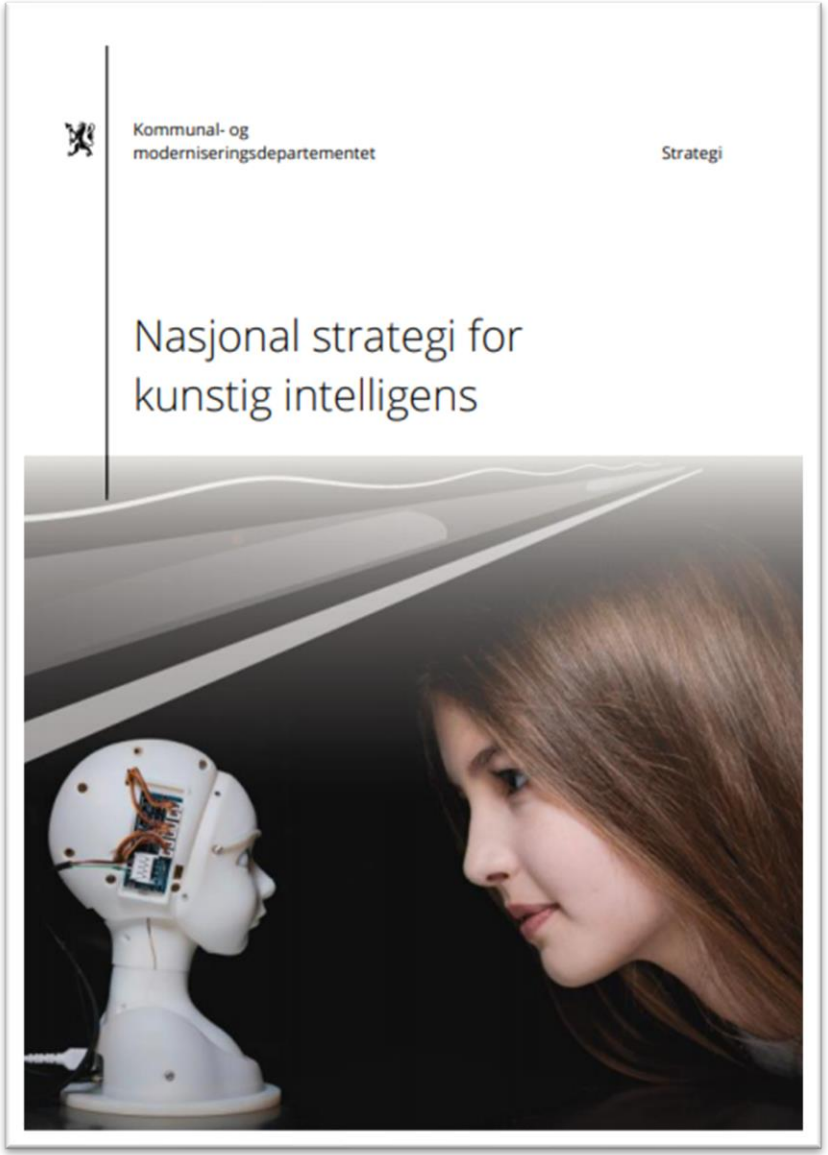
- Demonstrere samsvar med prinsippene
  - Effekten av tiltakene
  - Resonnement bak tiltak

- Ha både kunnskap om og evnen til å implementere personvernkravene

- Forstå og oppfylle forpliktelser ihht. personvernforordningen

Hva er en sandkasse?

Nasjonal strategi for kunstig intelligens



«Regjeringen vil at Norge skal gå foran i utvikling og bruk av kunstig intelligens med respekt for den enkeltes rettigheter og friheter.»

Hva er en regulatorisk sandkasse?

Et dialogbasert verktøy – ny måte å jobbe på for Datatilsynet

Virksom-heter

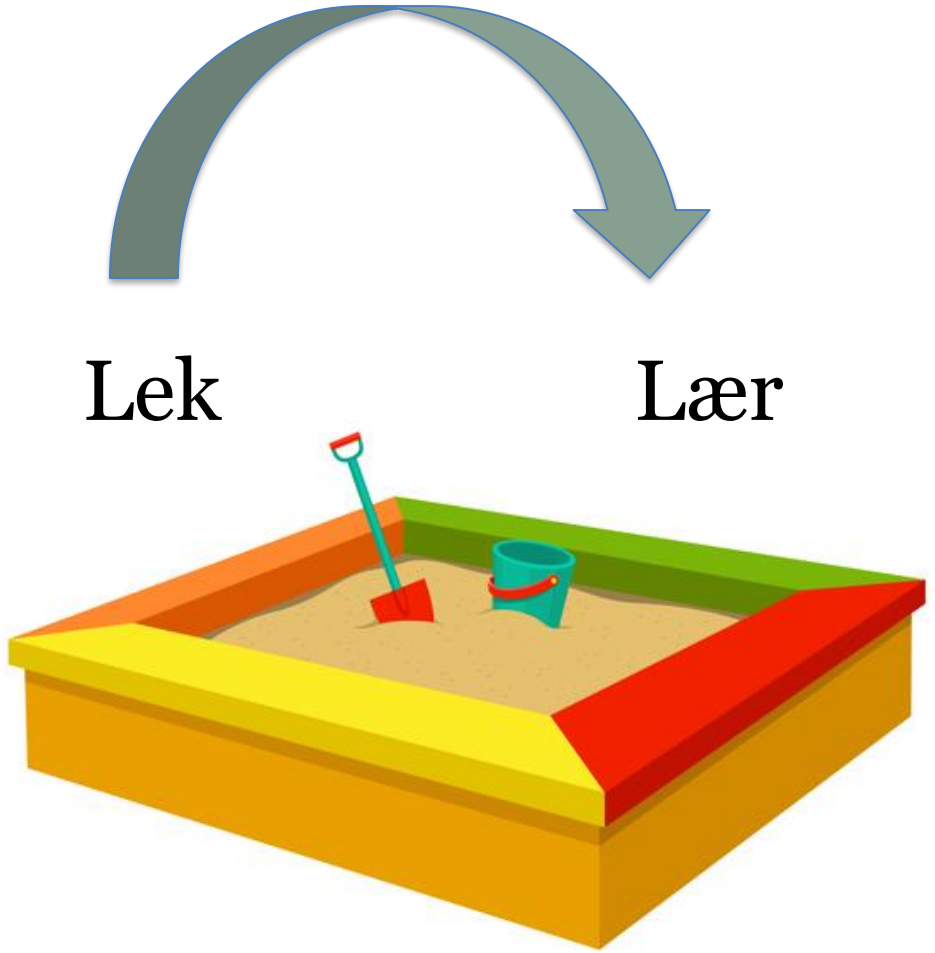
- **Bedre regelverksforståelse** – for de som deltar, og for andre virksomheter
- Legge til rette for **ansvarlig KI-innovasjon**

Datatilsynet

- Øke tilsynets **kunnskap og forståelse av KI-drevne løsninger**

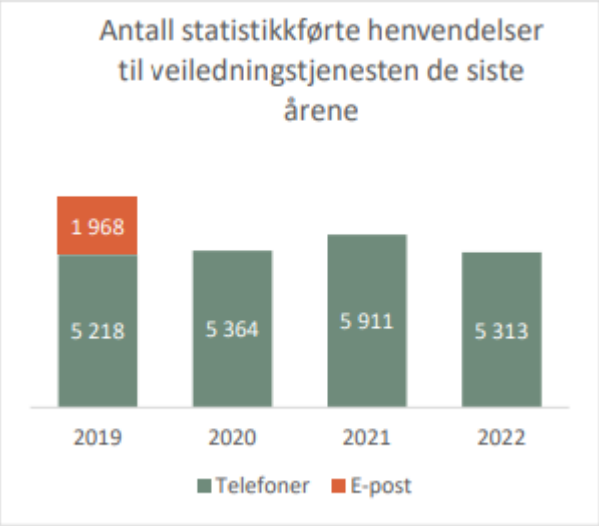
Enkeltindivider og samfunnet

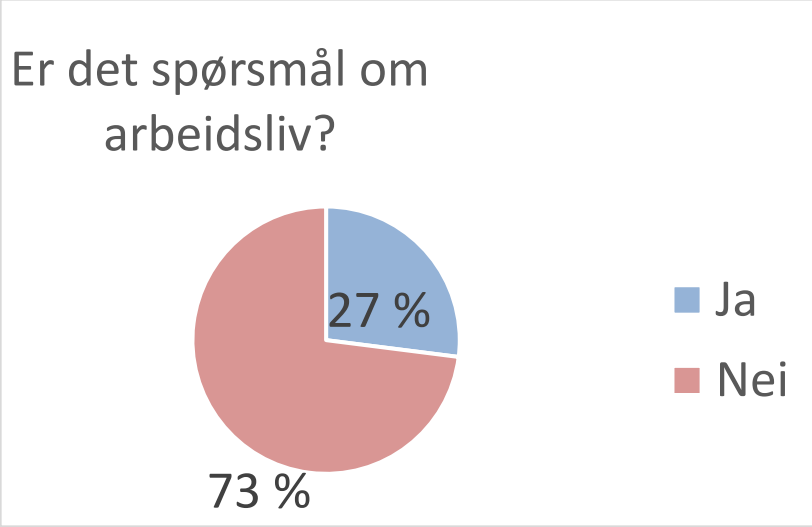
- **Bygge tillit** til nye KI-løsninger foregår innenfor **ansvarlige rammer**



Henvendelser om arbeidsliv

- Veiledningstjenesten mottok totalt 5313 **henvendelser** i 2021, hvorav 1408 var om arbeidsliv. Dette er 27 % av alle henvendelsene vi mottok.
- Overgangen fra analog til digital postgang har utfordret de gamle systemene for journalføring og arkivering av post og viktige dokumenter. En rapport antyder at mer enn 25 prosent av all viktig informasjon i offentlig saksbehandling "går tapt" i sviktende arkiveringsrutiner.





168 av disse angikk "innsyn i ansattes epost og annet elektronisk lagret data".

Disse klagesakene er det flest av innen arbeidsliv

- Arbeidsgivers behandling av personalopplysninger
  - Innsyn og sletting av personopplysninger i personalmappen
  - Innsyn i forbindelse med varslingssaker
  - Arbeidsgivers deling av personalopplysninger

- Arbeidsgivers kontrolltiltak
  - Innsyn i e-post og annet elektronisk utstyr
  - Videresending av e-post
  - Kameraovervåking
  - Ved brudd på disse reglene er det praksis for overtredelsesgebyr (bøter)

DAM
Digital ArkivarMedbeider

Simplifai – et av prosjektene i sandkassa

- Arkivering
  - effektivisering ved digitalisering og bruk av KI
  - Journalføring av eposter som er arkivverdig

- Prosjektets målsetning å avklare hvordan en løsning med kunstig intelligens kan benyttes for automatisk arkivering av korrespondanse.
  - Utforske muligheten for å bruke KI til å identifisere/foreslå hvilke eposter m/vedlegg regnes som arkivverdige.
  - KI-modellen må trenes med alle typer relevante data som kan forekomme i korrespondansen, deriblant personopplysninger og *særlige kategorier* personopplysninger. Om dette kan gjøres med godt personvern, og eventuelt hvordan, er hovedproblemstillingen Simplifai tar med seg inn i sandkassa
  - Simplifai og NVE, sluttrapport: Digital medarbeider | Datatilsynet

- Personvern og arkivering blir ofte oppfattet som motsetninger.
  - Stereotypen er at arkivaren vil spare på alt, mens personvernet krever at alt slettes.
  - Lovlighet
  - Innsyn i epostkasse
  - Overvåkning på arbeidsplassen (Arbeidsmiljøloven og personopplysningsloven)

DAM
Digital ArkivarMedbeider

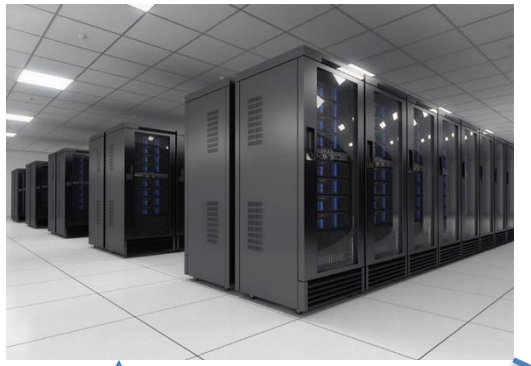
Simplifai – Oppsummering av funn

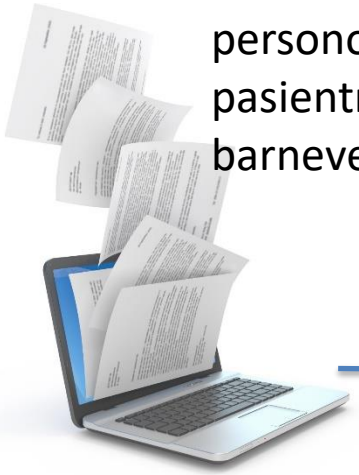
- **Lovlighet.**
  - Offentlige aktører har rettslig grunnlag for å bruke DAM som støtte ved beslutning om arkivering og journalføring.
  - Usikkert om det rettslige grunnlaget åpner for å bruke personopplysninger til å videreutvikle modellen (etterlæring), med mindre personopplysningene er anonymiserte.
  - Bruk av DAM er også lovlig innenfor nasjonale forskrifter til arbeidsmiljøloven. Datatilsynet anbefaler tekniske og organisatoriske tiltak, for eksempel instrukser som forbyr eller begrenser bruk av privat e-post.
- **Innebygd personvern.**
  - Prosjektet har avdekket et stort behov for veiledning om hvordan det offentlige kan sikre innebygd personvern ved kjøp av intelligente løsninger. Prosjektet har gitt overordnede anbefalinger til hvilke steg en offentlig virksomhet kan ta: Skaff kunnskap, vurder om maskinlæring passer til det konkrete behovet og still krav.

DAM

Digital ArkivarMedbeider

Felles refleksjon om risiko:





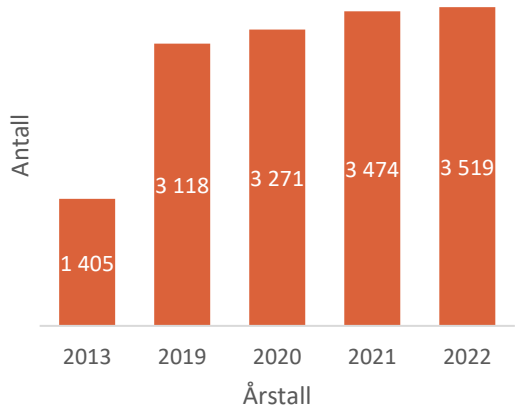
Forvaltningsloven,
personopplysningsloven,
pasientregisterloven,
barnevernloven, osv.

Arkivloven

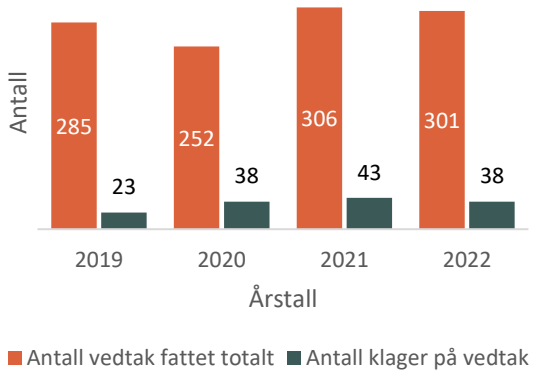
Fulltekstpublisering
eInnsyn - sladding

Hovedtall – økning i saker og henvendelser til Datatilsynet

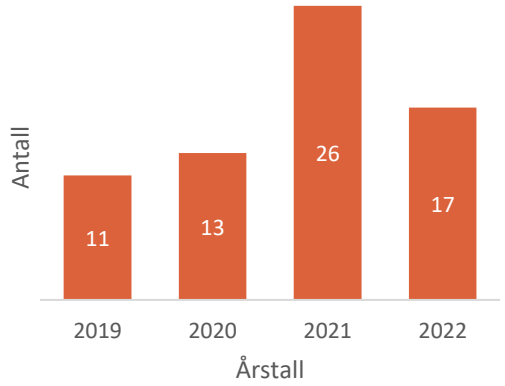
Antall nye journalførte **saker**



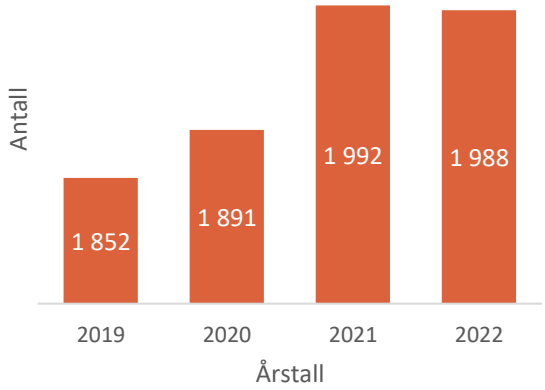
Antall **vedtak** fattet av Datatilsynet og antall **klager på vedtak**



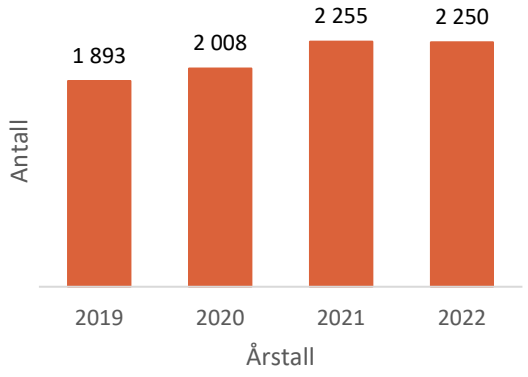
Vedtak om **overtredelsesgebyr**



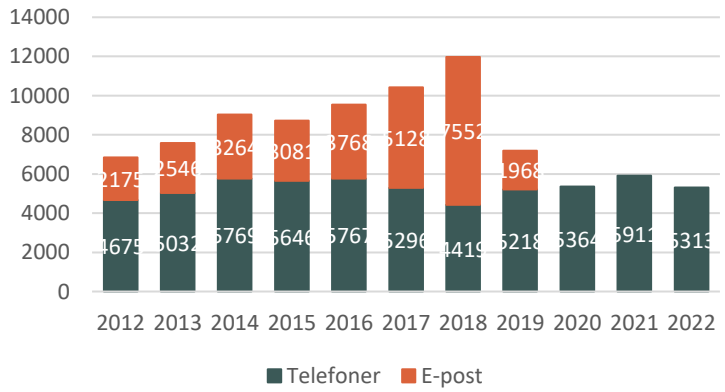
Antall **virksomheter** med personvernombud de siste årene



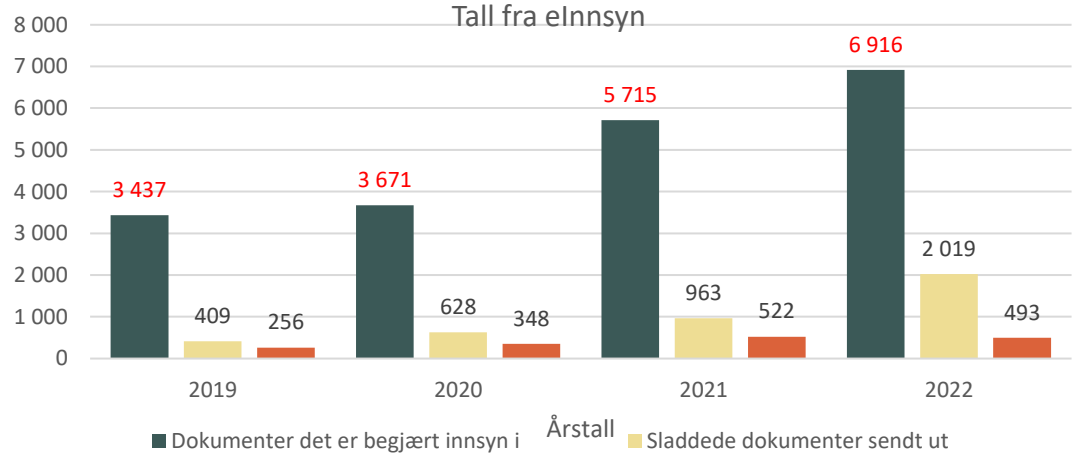
Mottatte avviksmeldinger



Statistikkførte henvendelser til veiledningstjenesten



Tall fra eInnsyn



Takk for meg!