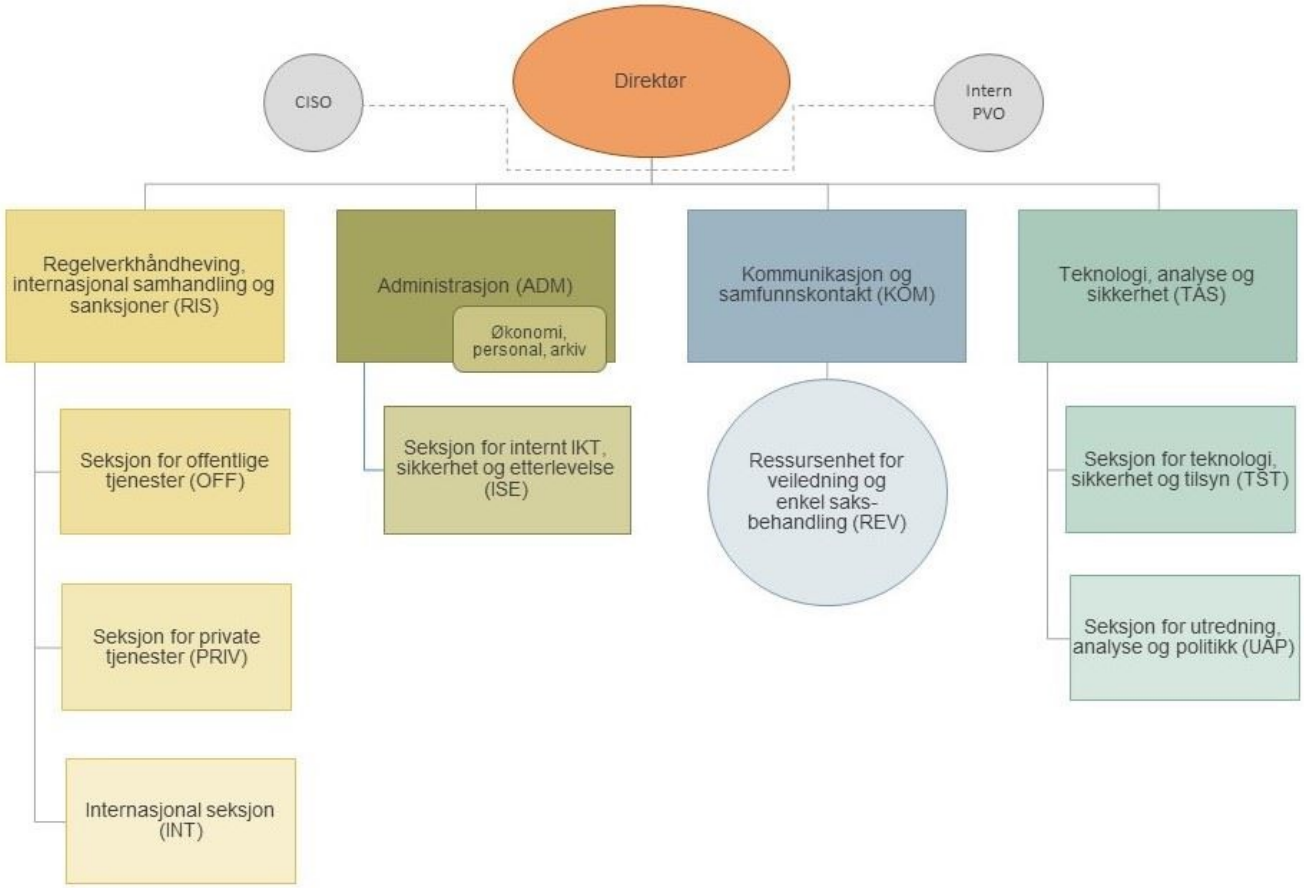
Fagsystemer og personvernet til barn og unge i undervisningssektoren

Arkiv Troms kontaktkonferanse

Juridisk fagdirektør Susanne Lie

Datatilsynet

Om Datatilsynet



Datatilsynets oppgaver

Barns rett til beskyttelse etter personvernregelverket

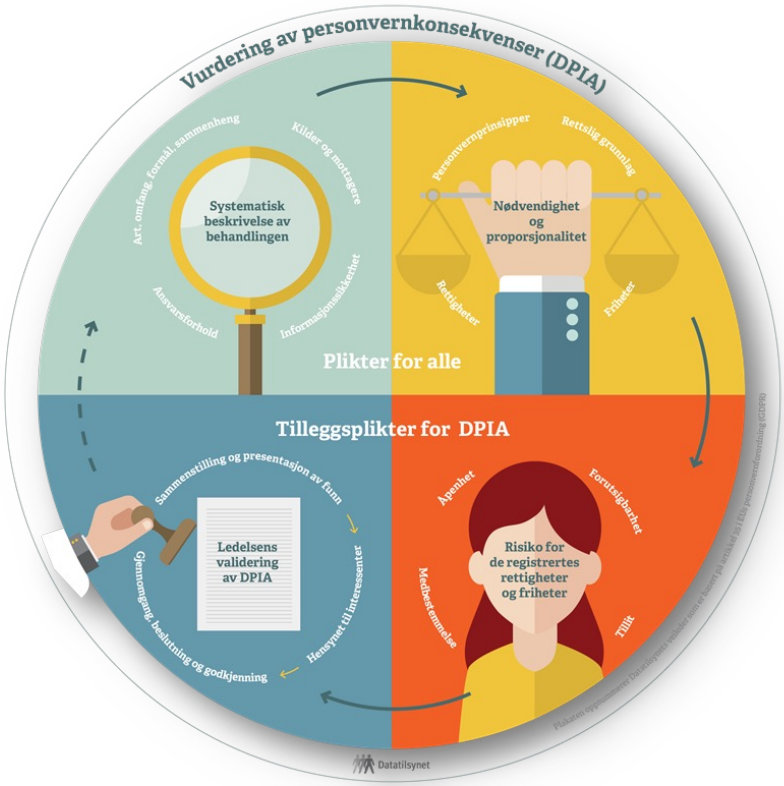
- Ingen egne aldersgrenser for barns samtykkekompetanse
  - Følger vergemålslovens og barnelovens system

«Barns personopplysninger fortjener et særlig vern, ettersom barn kan være mindre bevisste på aktuelle risikoer, konsekvenser og garantier samt på de rettigheter de har når det gjelder behandling av personopplysninger».

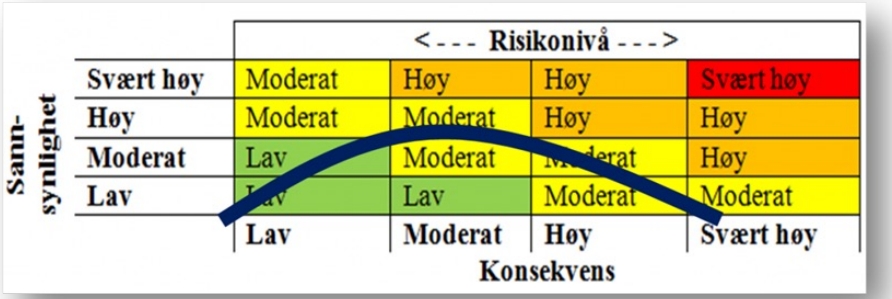
(Fortalepunkt 38 til personvernforordningen/GDPR)

- Vern om barnets personopplysninger
  - Overfor omverdenen/uvedkommende
  - Også overfor foresatte

Grundige risikovurderinger kreves



Personvernkonsekvensvurdering (DPIA)



ROS-analyse

(Eksempelbilde: Digitaliseringsdirektoratet)

Personvernforordningen artikkel 32

- Behandlingsansvarliges ansvar for sikkerhet ved behandlingen
  - ⇨ Risikovurdering av *personopplysningssikkerhet*

- ROS-analyse

- Vurderingen skal ta hensyn til:
  - Den tekniske utviklingen
  - Gjennomføringskostnadene
  - Art, omfang, formål og kontekst
  - Risikoene for de registrerte

- Egnede tekniske og organisatoriske tiltak kan være:
  - Regelmessig testing, analyse og evaluering av sikkerhetstiltak

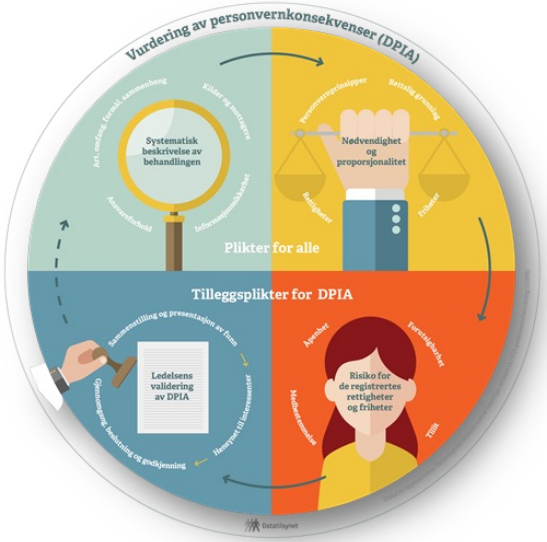
Personvernforordningen artikkel 35

- Behandlingsansvarliges plikt til å gjøre personvernkonsekvensvurdering (DPIA)
  - ⇨ Risikovurdering av *personvernkonsekvenser*

- Forutsetter høy risiko
  - Risiko for *personvernet* – ikke informasjonssikkerhetsrisiko

- Personvernrisiko vurderes høyere hvis:
  - Personopplysningene gjelder barn
  - Store mengder personopplysninger og/eller
  - Opplysninger om mange personer

- DPIA skal minst inneholde:
  - Beskrivelse av art, omfang, formål og kontekst
  - Vurdering av risikoene for de registrertes rettigheter og friheter
  - Mottakere, dataflyt og lagring
  - Beskrivelse av hvordan personopplysningssikkerheten er ivaretatt
  - Planlagte tiltak for å håndtere risikoene



Vigilo – Bergen kommune

- Digital kommunikasjonstjeneste mellom skole og hjem
- Avviksmelding til Datatilsynet
  - Tilgang til opplysninger for foreldre uten foreldreansvar
  - Fortrolig adresse (tidligere kode 4, 6 og 7) ikke skjermet
  - Kommunikasjon i gruppechat
- Mangelfulle risikovurderinger
  - Kun risikovurdert pålogging, ikke selve løsningen
- Barn har krav på særskilt vern
  - Risiko for liv og helse
- OTG på kr. 3 000 000
  - Ikke påklaget

Strava – Ålesund kommune

- Avviksmelding under pandemien
- Påla elever å laste ned treningsappen Strava til bruk i gymtimer
  - Gjaldt to ungdomsskoler
  - Åpen gruppe per klasse med navn på elever
  - Bruk av lokasjonsdata (GPS)
- Risikovurdering ikke gjennomført – heller ikke vurdering av personvernkonsekvenser (DPIA)
  - Stravas bruk av data til egne formål
  - Skolens behandling av personopplysninger
- Ingen rutine for/kontroll med apper som ble tatt i bruk
- OTG på kr. 50 000
  - Ikke påklaget

https://www.strava.com/mobile

Showbie – Rælingen kommune

- Avviksmelding til Datatilsynet
- Digital læringsplattform (app)
  - For lærere til bruk i undervisning
  - For kommunikasjon mellom skole og hjem
- Fungerte som «meldingsbok»
  - Barn med funksjons-/utviklingshemninger, tilleggsdiagnoser, medisinbruk m.m.
- Risikovurdering ikke gjennomført – heller ikke DPIA
  - Lavt sikkerhetsnivå i løsningen
  - Ingen rutiner for/kontroll med bruk
  - Særlige kategorier av personopplysninger – sårbare barn
- OTG på kr. 500 000
  - Ikke påklaget

Spekter – Arendal kommune

- Klage fra foresatt
- Kartleggingsverktøy
  - Undersøker bl.a. mobbing
  - Innlogging via Feide – elevene var identifiserbare
- Datatilsynet identifiserte flere risikoer:
  - Behandling av særlige kategorier av personopplysninger?
  - Ikke tilstrekkelig rettslig grunnlag i opplæringsloven
  - Manglende åpenhet og forutsigbarhet – feilinformasjon
  - Korrekte opplysninger?
  - Manglende protokoll, ikke gjennomført risikovurderinger
- Personvernnemnda vurderte det annerledes (PVN-2020-13)
  - Kommunen hadde rettslig grunnlag i opplæringsloven
  - Barns subjektive oppfatninger legges til grunn – rettigheter ivaretas ved kontradiksjon
  - Særlige kategorier av personopplysninger ⇨ strengere krav til risikovurderinger og personopplysningssikkerhet

Publisering på postliste/eInnsyn

- Askim (nå Indre Østfold) kommune
  - Publisering av elevmappe med taushetsbelagte opplysninger (beredskapshjem, slåsskamper, bekymring om faglig utvikling, bilde av eleven m.m.)
  - Journalføring av innsynsbegjæringer – publisering av dokumentet det er gitt innsyn i
  - Publisering av fulltekstdokumenter krever ekstra høyt sikkerhetsnivå
  - Opplæring viste seg ikke tilstrekkelig effektivt
  - OTG på kr. 200 000 – ikke påklaget

- Lillestrøm kommune
  - Publisering av særlige kategorier av opplysninger om elev (navn, fødselsdato, diagnoser, spesialundervisning m.m.)
  - 10 av 21 vedlegg til et dokument inneholdt slike opplysninger
  - Ikke oppdaget til tross for tre manuelle kontroller
  - Rutiner forelå, men var åpenbart ikke tilstrekkelige

Nemndsavgjørelser – barns personopplysninger i skolen

- Flere saker behandlet i Personvernnemnda
  - PVN-2015-03, PVN-2018-06, PVN-2020-05, PVN-2020-13

- Sletting i elevmappe (PVN 2020-05)
  - Datatilsynet: Tilstrekkelig at opplysningene lå lagret hos barneverntjenesten – vedtok sletting
  - PVN: Dokumentasjonsplikt og arkivhensyn avgjørende – begrensning av tilgang ved skolen tilstrekkelig

- Foreldreinnsyn (PVN-2015-03)
  - Barn over 15 år
  - Datatilsynet nektet forelder innsyn i barnets aktivitetslogg i skolens systemer
  - Eget innsyn vs. innsyn på vegne av barnet
  - Barnets gradvise selvbestemmelse

Personvernkommisjonen

- NOU 2022: 11 *Ditt personvern – vårt felles ansvar – Tid for en personvernpolitikk*
  - Skole og barnehage som eget fokusområde
- Konklusjon: Digitaliseringen av skole og barnehage på bekostning av barns personvern
  - Omfattende endringer for å digitalisere skolehverdagen
  - Ikke kompetanse og ressurser til å ivareta personvernet
- Behov for profesjonalisering og sentralisering
  - Risikovurderinger
  - Testing og utvikling av digitale løsninger
  - Lov-/forskriftsfesting av behandlingsansvar for fellesløsninger
  - Styrke forhandlingsmakt overfor tech-giganter
  - Forholdet til kommunalt selvstyre
- Anbefaler egen personvernpolitikk

Hvordan hjelpe kommunene?

- Svært varierende kompetanse og ressurser
- KS – kan ha viktig rolle
  - Nettverk og fagråd for informasjonssikkerhet og personvern
  - Utvikle rammeverk, veiledere og maler
    - Prosjekt for felles risikovurderinger (ROS-analyser) og DPIA
  - Potensielt rask effekt!
  - Fellesløsninger – behandlingsansvar hos KS?
    - I tråd med anbefaling fra Personvernkommisjonen
- Personvernombud i alle kommuner
  - Egen kanal for oppfølging fra Datatilsynet
  - Kommunalt/fylkeskommunalt nettverk, egen forening
- KiNS – Foreningen Kommunal Informasjonssikkerhet

Takk for meg!

Susanne Lie
Juridisk fagdirektør
suli@datatilsynet.no

Datatilsynet

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no