



ORKLAND
KOMMUNE

Etterlevelse av personvern på oppvekstområdet

Orientering kontrollutvalget 30.04.25



Oppdraget

Orientering til kontrollutvalget - personvernregelverket

På kontrollutvalgets møte 20.02.2025 ble det under sak 9/25 Innspill til kontrollarbeidet, vedtatt å be kommunedirektøren om en orientering om personvernregelverket.

Kontrollutvalget fattet enstemmig følgende vedtak:

Kontrollutvalget ber kommunedirektøren om en orientering om etterlevelse av personvernregelverket på oppvekstområdet. Orienteringen gis på kontrollutvalgets møte 30.04.2025

Under henvisning til kontrollutvalgets vedtak i sak 9/25, ber vi herved om at kommunedirektøren i Orkland kommune orienterer på kontrollutvalgets møte 30.04.2025.



Hva er personopplysninger?

- Personopplysninger er alle opplysninger som kan knyttes til deg som enkeltperson.
- Eksempel på personopplysninger er navn, adresse, telefonnummer, e-postadresse, familierelasjoner
- Sensitive personopplysninger krever spesiell beskyttelse, for eksempel helseopplysninger, rase, politisk oppfatning, religiøs overbevisning, fagforening, genetikk, biometri, seksuell legning





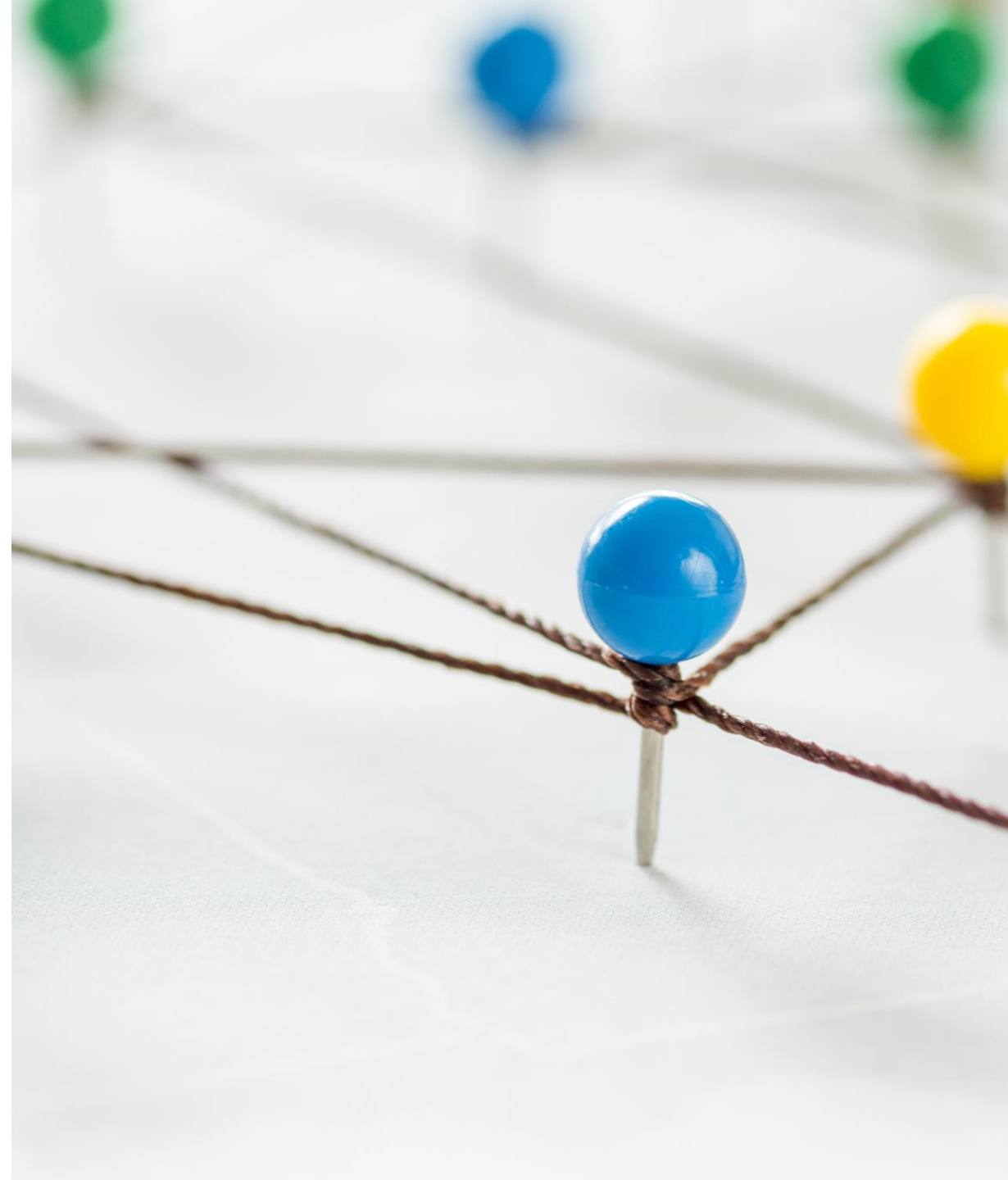
Personvernforordningen art 5 - grunnprinsipper

1. Behandlingen må være lovlig etter artikkel 6 og 9, og den registrerte skal være informert om behandlingen (lovlighet, rettferdighet og åpenhet)
2. Det skal være klare og spesifikke formål med en behandling (formålsbegrensning)
3. Det skal ikke samles inn mer data enn nødvendig for å oppnå ønsket resultat (dataminimering)
4. Personopplysninger som samles inn, skal være korrekte (riktighet)
5. Personopplysninger skal ikke lagres lenger enn det er behov for å oppnå formålet (lagringsbegrensning)
6. Sørg for tilstrekkelig sikring av data (integritet og konfidensialitet)
7. Vis at personvernforordningen etterleves (ansvar)



Hvorfor samler vi inn personopplysninger?

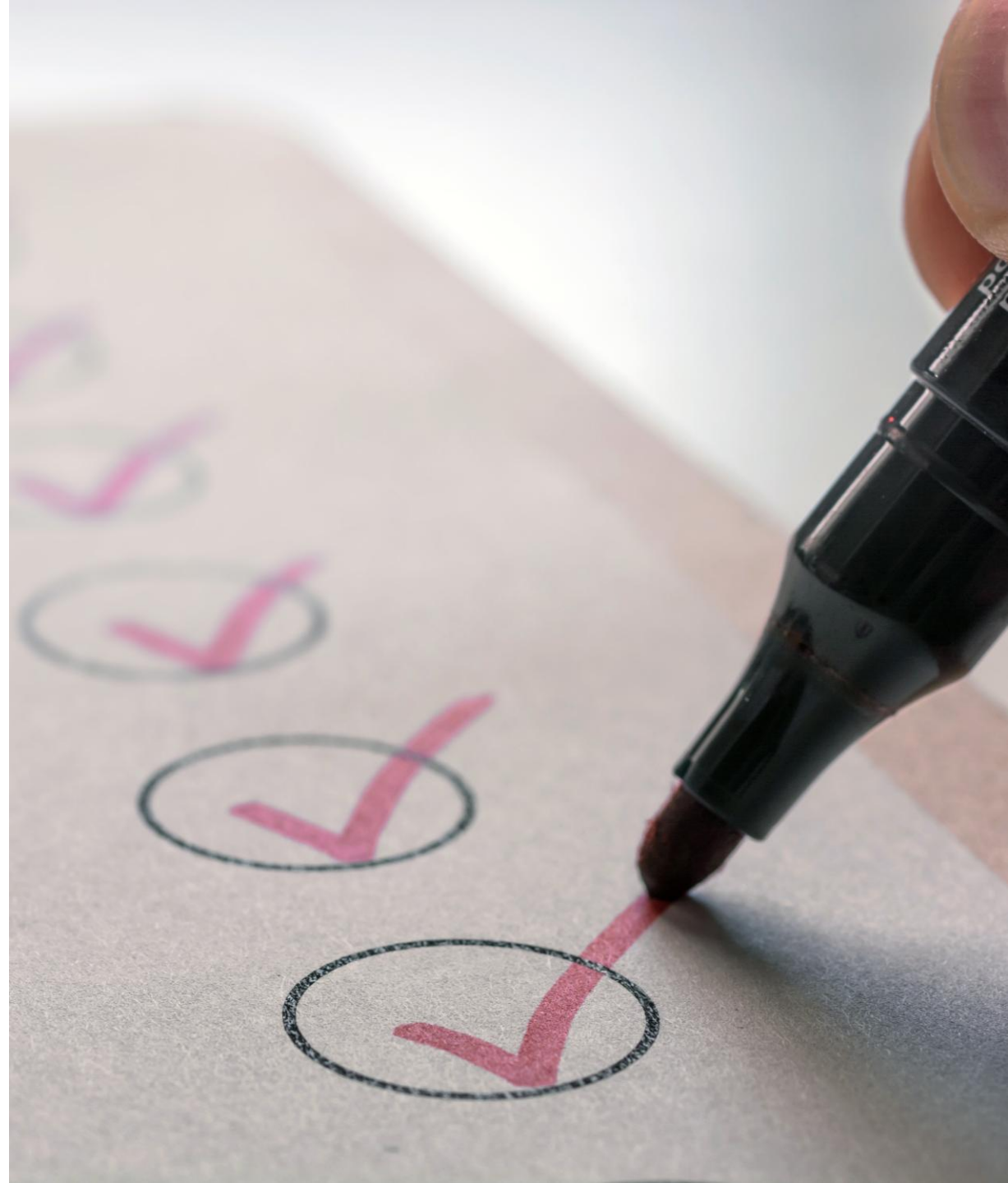
- For å kunne utføre lovpålagte oppgaver gitt i barnehage- og opplæringsloven (barnehageloven §47a og opplæringsloven §25-1)
- For å kommunisere med foreldre og foresatte





Hvordan beskytter vi personopplysninger?

- Administrative system med tilgangsstyring og flerfaktorgodkjenning
- Kryptering
- Diverse tekniske sikkerhetstiltak
- Opplæring av ansatte i databeskyttelse





Grunnleggende beskyttelse av personopplysninger

- Orkland kommune sitt nettverk er beskyttet av brannmurer og overvåkes kontinuerlig for å forhindre/oppdage datainnbrudd
- Ansatte blir en del av kommunens nettverk gjennom registrering i kommunens IAM-system (Identity and Access Management - identitetsstyring) - Kildesystem er Visma HRM (Human Resource Management) som er tilkoblet folkeregister og for pålogging benyttes flerfaktorgodkjenning (BankID)
- IAM-systemet er rollebasert (RBAC - Role Based Access Control), det vil si at rollen din bestemmer hva du skal/kan ha tilgang til av ulike systemer i kommunen – for eksempel vil styrer og rektor ha andre tilgangsnivåer enn barnehage- og skolelærere.



Grunnleggende beskyttelse av personopplysninger, forsetter:

- Oppvekstadministrativt system (OAS) - Visma Flyt skole: Her registrerer nødvendige personopplysninger om elever og foreldre. Systemet er direkte koblet opp mot Folkeregisteret, og dette gjør at opplysninger om den/de som har foreldreansvar, ikke automatisk begge foreldre, som tas inn i systemet. Systemet overvåkes kontinuerlig for å forhindre/oppdage datainnbrudd.
- Informasjonen fra kildesystemet går så til Orkland brukerkatalog (AD - Active Directory og Microsoft Entra). Denne overføringen gjør det mulig for lærere og elever å logge seg på iPad og PC og bruke ulike programvare som kontorstøtteprogram (Microsoft Office) m.m. Informasjonen som går hit fra kildesystemet, er svært begrenset – følger «dataminimerings-prinsippet» - kun informasjon som er nødvendig for å lage brukerkonto registreres her (navn, tittel, personnummer (pga Feide-pålogging), skole, klasse/trinn).



Grunnleggende beskyttelse av personopplysninger, fortsetter:

- Tjenester rettet mot skole og elever, som digitale læremidler og ressurser, benytter Feide innlogging som autentiserer mot kommunens brukerkatalog (styrt av IAM)
- Feide-innlogging gjør at ansatte og elever ikke behøver å registrere opplysninger om seg selv, som f.eks e-postadresse, nytt brukernavn og passord, men gjør at de får direkte tilgang til klarerte datasystemer med samme konto som er registret i kommunens brukerkatalog



Spesiell beskyttelse av personopplysninger – elever:

- Hver iPad og PC er sikret med antivirusprogram som hindrer muligheten til å gå inn på enheten for å hente ut info. Alle iPad og PC-er er i tillegg kryptert.
- Det er aktivert Kriposfilter (webfilter - filtrerer nettverkstrafikk på brannmur – filteret blokkerer uønskede kategorier og skjermer elevene mot ulovlig innhold på nettet (eks porno, gambling). Ved søk på uønskede kategorier, vil eleven oppleve at de ikke får «treff». Dette filteret fungerer bare på skolen.
- Alle iPader vil få installert Jamf Safe Internett til skolestart høsten 25. Dette er et filter som stenger muligheten å finne/søke opp ulovlig eller upassende innhold på nettet. Funksjonen virker både hjemme og på skolen fordi den er installert direkte på elevenes iPad og dermed virker uavhengig av hvilket nett man er tilkoblet.



Rett til innsyn og retting

Alle registrerte har rett til å

- Få innsyn i hvilke personopplysninger som er lagret
- Be om retting av uriktige eller ufullstendige opplysninger
- Be om sletting av personopplysninger under visse omstendigheter





Oppbevaring av personopplysninger

Vi oppbevarer personopplysninger så lenge det er nødvendig for å oppfylle formålene de ble samlet inn for, og i samsvar med gjeldende lovgivning





Fra hjemmeskole til vanlig skole...





Grunnskole

- Har tatt en faglig gjennomgang i samarbeid med ansatte i skolen og redusert antall apper og nettsteder elevene hadde tilgang til fra ca. 600 til ca.20
- Vi har vurdert og valgt digitale læreverk i kombinasjon med fysiske læreverk
- Vi har utarbeidet prosedyrer for innspill, vurdering og valg av eventuelt nye apper
- Vi har opprettet et felles register for digitale ressurser i DigiOrden
- Kontinuerlig evaluering av programmene vi benytter – også økonomisk motiv
- Gjennomfører brevtilsynet Datatilsynet har i andre kommuner i egen kommune





Sjekkliste

- Vær godt kjent med grunnprinsippene i personvernforordningen (GDPR)
- Ha oversikt over hvilke personopplysninger som behandles, og hvorfor.
- Se til at personopplysninger behandles lovlig
- Sørg for at dataene er tilstrekkelig sikret
- Gi tydelig og god informasjon til de det registreres opplysninger om.
- Ha god kontroll på underleverandører
- Slett data som ikke brukes eller som ikke er nødvendig.
- Meld eventuelle brudd til tilsynsmyndigheten.
- Sørg for å ha et velfungerende styringssystem og internkontroll

