

**[Tittel]**Vurdering av personvernkonsekvenser (DPIA) for innføring av nytt skolesystem

Innhold

[Innhold 1](#_Toc183517984)

[1 Innledning 2](#_Toc183517985)

[2 Innledende vurderinger 3](#_Toc183517986)

[3 Beskrivelse av behandlingen 5](#_Toc183517987)

[4 Nødvendighet og rimelighet 8](#_Toc183517988)

[4.1 Vurdering av personvernprinsippene 8](#_Toc183517989)

[4.2 Vurdering av de registrertes rettigheter og friheter 9](#_Toc183517990)

[4.3 Vurdering av de registrertes friheter 11](#_Toc183517991)

[5 Risikoer for de registrerte 12](#_Toc183517992)

[5.1 Risiko for manglende reell åpenhet 12](#_Toc183517993)

[5.2 Risiko for manglende reell medbestemmelse 12](#_Toc183517994)

[5.3 Risiko for manglende reell forutsigbarhet 13](#_Toc183517995)

[5.4 Andre risikoer 14](#_Toc183517996)

[6 Synspunkter 15](#_Toc183517997)

[7 Ledelsens validering 16](#_Toc183517998)

# Innledning

*Byskogen skole ønsker å ta i bruk et nytt skolesystem. I den forbindelse er det behov for å gjennomføre en vurdering av personvernkonsekvenser (DPIA). Vurderingen omfatter behandlingen som skal gjennomføres i skolesystemet.*

|  |
| --- |
| Innledende informasjon |
| Navn på skolesystemet |  |
| Leverandør av skolesystemet |  |
| Er personvernombudet involvert? |  |
| Er de registrerte involvert? |  |
| Vurdering gjennomført dato |  |
| Vurdering gjennomført av (arbeidsgruppen) |  |

# Innledende vurderinger

*DPIA skal gjennomføres dersom behandlingen sannsynligvis vil innebære en høy risiko for de registrertes rettigheter og friheter, jf. GDPR artikkel 35. Vurderingen av høy risiko avklares i dette kapitlet. Vurderingen tar utgangspunkt i Artikkel 29 gruppens kriterier for å vurdere behov for DPIA. Dersom noen av vurderingskriteriene resulterer i ja, så er det behov for å gjennomføre en fullstendig DPIA.*

|  |  |
| --- | --- |
| Vurderingskriterier | Ja/Nei |
| Omfatter behandlingen evaluering eller poengsetting av de registrerte?  |  |
| Innebærer behandlingen automatiserte avgjørelser med rettslig virkning?  |  |
| Innebærer behandlingen en systematisk overvåking av de registrerte (eksempelvis videoovervåking av offentlig tilgengelig område, bruk av lokasjonsdata, kontroll av ansatte)? |  |
| Omfatter behandlingen sensitive personopplysninger (særlige kategorier)? |  |
| Omfatter behandlingen mange registrerte? |  |
| Omfatter behandlingen matching eller sammenstilling av flere datasett? |  |
| Omfatter behandlingen personopplysninger om sårbare registrerte (eksempelvis barn, pasienter, ansatte, eldre)? |  |
| Omfatter behandlingen innovativ bruk av teknologi eller organisatoriske verktøy, hvor tilknyttet risiko ennå ikke er kjent?  |  |
| Hindrer behandlingen de registrerte i å utøve sine rettigheter?  |  |

**Konklusjon fra den innledende vurderingen:**

**\*** DPIA må gjennomføres

**\*** DPIA må ikke gjennomføres

# Beskrivelse av behandlingen

*Dette kapitlet gir en systematisk beskrivelse av den planlagte behandlingen som skal utføres i skolesystemet. Beskrivelsen skal omfatte behandlingens art, omfang, formål og sammenhengen behandlingen utføres i (kontekst). Beskrivelsen sees opp mot GDPR artikkel 24 (den behandlingsansvarliges ansvar), artikkel 25 (innebygd personvern), artikkel 28 (databehandler), artikkel 30 (behandlingsprotokoll) og artikkel 32 (sikkerhet ved behandlingen).*

|  |
| --- |
| Behandlingens formål |
| * Beskriv formålet med behandlingen
* Beskriv hvorvidt personopplysningene vil viderebehandles til nye eller andre formål
 |
| **Beskrivelse av skolesystemet behandlingen utføres i** |
| * Beskriv formålet med behandlingen
* Beskriv hvorvidt personopplysningene vil viderebehandles til nye eller andre formål
 |
| **Beskrivelse av behandlingen som skal vurderes** |
| Om de registrerte, og om personopplysningene som samles inn * Beskriv hvem det samles inn personopplysninger om (eks ansatte, elever)
* Beskriv hvilke personopplysninger som samles inn (eks navn, adresse)
* Beskriv hvordan personopplysningene samles inn (eks fra de registrerte selv)
* Beskriv om det samles inn personopplysninger fra sårbare registrerte (eks barn)
* Beskriv om det samles inn sensitive personopplysninger (eks helseopplysninger)
* Beskriv kommunens relasjon til de registrerte
* Anslå hvor mange registrerte som omfattes av behandlingen

 Om selve behandlingen * Beskriv hvordan personopplysningene skal brukes
* Beskriv behandlingsaktivitetene som inngår i vurderingen
* Beskriv hvor personopplysningene lagres
* Beskriv hvor lenge personopplysningene lagres
* Beskriv hvem som skal ha tilgang til personopplysningene
* Beskriv om behandlingen omfatter bruk av ny teknologi, hvor personvernkonsekvenser ikke har blitt vurdert

Om de registrertes rettigheter * Beskriv hvordan de registrerte kan utøve sine rettigheter
* Beskriv i hvilken grad de registrerte har kontroll over egne personopplysninger
* Beskriv hvordan behandlingen vil oppfattes fra de registrertes perspektiv. Kan de registrerte oppfatte behandlingen som uforutsigbar?
* Beskriv om de registrerte har en særskilt forventning om konfidensialitet
* Beskriv om de registrerte har en særskilt forventning om at personopplysningene er nødvendige og korrekte
* Beskriv om de registrerte har en særskilt forventning om privatliv

Om bruk av databehandler (dersom relevant) * Beskriv hvilke databehandlere som brukes
* Beskriv hvilken databehandleravtale som er etablert
* Beskriv hvilke garantier databehandlerne gir for at de gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at behandlingen gjennomføres i samsvar med personvernregelverket

 Om tekniske og organisatoriske sikkerhetstiltak * Beskriv hvordan personopplysningssikkerheten (informasjonssikkerheten på personopplysningene) skal ivaretas i skolesystemet, herunder sikring av konfidensialitet, integritet, tilgjengelighet og robusthet. Eksempler på sikkerhetstiltak kan være sterk autentisering, kryptering, logging, overvåking, tilgangskontroll, sikkerhetsinstruks og taushetserklæring.

 Om innebygd personvern * Beskriv hvordan skolesystemet ivaretar kravet til innebygd personvern

 Om mottak og overføring av personopplysninger * Beskriv alle kildene til personopplysningene (skjema, import etc)
* Beskriv alle mottakere av personopplysninger (eksport etc)
* Beskriv om personopplysningene overføres til land utenfor EU/EØS-området, og i så fall hva som er overføringsgrunnlaget
* Beskriv om personopplysningene overføres til tredjestater eller internasjonale organisasjoner, og i så fall hva som er overføringsgrunnlaget
 |

# Nødvendighet og rimelighet

*Dette kapitlet inneholder vurderinger om hvorvidt behandlingen, og de enkelte behandlingsaktivitetene, er nødvendige og står i et rimelig forhold til formålet. Vurderingene omfatter en kvalitetssikring av hvorvidt skolesystemet oppfyller personvernprinsippene, og hvordan de registrertes rettigheter og friheter skal ivaretas. Vurderingene sees opp mot GDPR artikkel 5 (personvernprinsippene), artiklene 12-22 (de registrertes rettigheter), artikkel 35, samt EMK artikkel 8.*

## Vurdering av personvernprinsippene

|  |
| --- |
| Lovlighet, rettferdighet og åpenhet |
| * Beskriv om behandlingen baseres på et tydelig rettslig grunnlag, og hvorvidt det rettslige grunnlaget er gyldig og rimelig
* Beskriv hvordan åpenhet skal ivaretas i behandlingen
 |
| **Formålsbegrensning** |
| * Beskriv om formålet er klart definert
* Beskriv om formålet samsvarer med forventningene til de registrerte
* Beskriv om formålet kan oppnås med anonyme eller pseudonyme alternativer
 |
| **Dataminimering** |
| * Beskriv om alle personopplysningene som samles inn er nødvendige for å oppnå formålet
* Beskriv om det er mulig å begrense innsamlingen av personopplysninger
* Beskriv om det er mulig å redusere detaljgraden av personopplysninger
 |
| **Riktighet** |
| * Beskriv hvordan personopplysningene holdes korrekte og oppdaterte
* Beskriv om de registrerte må involveres i å holde opplysningene korrekte
* Beskriv hvorvidt det er behov for kontradiksjon, det vil si de registrertes anledning til å imøtegå det som den behandlingsansvarlige har registrert
 |
| **Lagringsbegrensning** |
| * Beskriv hvordan personopplysningene slettes når formålet er nådd
* Beskriv hvorvidt enkelte personopplysninger skal langtidsbevares og lagres i kommunens sak- og arkivsystem, jf. riksarkivarens forskrift (for eksempel elevmapper)
 |
| **Integritet og konfidensialitet** |
| * Beskriv om det er gjennomført en ROS av skolesystemet, jf artikkel 32. Gjør rede for eventuelle høye risikoer som ikke kan reduseres med sikkerhetstiltak, og som bør inkluderes i denne DPIAen
* Beskriv om personopplysningssikkerheten er tilstrekkelig ivaretatt
 |

## Vurdering av de registrertes rettigheter og friheter

|  |
| --- |
| Rett til informasjon |
| * Beskriv hvordan informasjon om behandlingen skal gis de registrerte (eks personvernerklæringer, informasjon i skolesystemet)
 |
| **Rett til innsyn** |
| * Beskriv hvordan de registrerte skal utøve retten til innsyn i egne personopplysninger (eks profilside i skolesystemet, skjema for innsynsforespørsel)
 |
| **Rett til retting** |
| * Beskriv om det skal være mulig for de registrerte å korrigere sine egne personopplysninger, og i så fall hvordan de registrerte kan utøve denne rettigheten
 |
| **Rett til sletting** |
| * Beskriv om det skal være mulig for de registrerte å slette sine egne personopplysninger, og i så fall hvordan de registrerte kan utøve denne rettigheten
 |
| **Rett til begrensning** |
| * Beskriv om det skal være mulig for de registrerte å utøve retten til å begrense behandlingen til egne personopplysninger, og i så fall hvordan de registrerte kan utøve denne rettigheten
 |
| **Rett til dataportabilitet** |
| * Beskriv om det skal være mulig for de registrerte å utøve retten til dataportabilitet, og i så fall hvordan de registrerte kan utøve denne rettigheten
 |
| **Rett til å protestere** |
| * Beskriv om det skal være mulig for de registrerte å utøve retten til å protestere, og i så fall hvordan de registrerte kan utøve denne rettigheten
 |
| **Rettigheter ved automatiserte avgjørelser og profilering** |
| * Beskriv om det gjennomføres automatiserte avgjørelser og profilering av de registrerte. Beskriv i så fall hvordan de registrerte kan utøve denne rettigheten
 |

## Vurdering av de registrertes friheter

|  |
| --- |
| Vurderinger rundt de registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK)  |
| * Beskriv hvordan behandlingen tar hensyn til retten til privatliv og kommunikasjonsvern
* Beskriv hvordan behandlingen tar hensyn til retten til å ikke bli diskriminert
* Beskriv hvordan behandlingen tar hensyn til retten til tanke-, tros- og religionsfrihet
* Beskriv hvordan behandlingen tar hensyn til retten til ytrings- og informasjonsfrihet
 |

# Risikoer for de registrerte

*Dette kapitlet omfatter vurderinger av personvernkonsekvenser for de registrertes rettigheter og friheter, samt relevante tiltak for å redusere risiko. Alle vurderingene skal ta utgangspunkt i de registrertes perspektiv, og omfatte vurderinger av risikoer for manglende reell åpenhet, medbestemmelse og forutsigbarhet. Dette gjøres for å kontrollere om behandlingen kan gjennomføres på en måte som er akseptabel og tillitsskapende ovenfor de registrerte.*

## Risiko for manglende reell åpenhet

*Åpenhet vurderes i denne sammenheng å være tiltak knyttet til informasjon og innsyn.*

|  |
| --- |
| Risikovurdering av åpenhet |
| Innspill til risikovurderingen: * Er informasjon som gis tilstrekkelig til at de registrerte forstår alle sider av behandlingen? Henviser kommunen til informasjon hos databehandler, som fremstår som lite tilgjengelig eller er komplisert utformet?
* Er informasjonen som gis tilpasset målgruppene? Fortalepunkt 58 fremfører at behandlinger som gjelder barn, skal være formulert på et klart og enkelt språk som barnet lett kan forstå.
* Gis informasjon også når personopplysninger samles inn fra andre kilder (dvs ikke fra de registrerte selv)?
* Hvis informasjonen gis i selve skolesystemet, er informasjonen korrekt og tilstrekkelig, eller må det gis supplerende informasjon?
 |
| **Tiltak for å redusere risiko** |
| * Beskriv relevante tiltak
 |
| **Vurdering av restrisiko** |
| * Beskriv restrisikoen (risikoen etter at tiltakene er gjennomført)
 |

## Risiko for manglende reell medbestemmelse

*Medbestemmelse vurderes i denne sammenheng å være tiltak knyttet til de registrertes rettigheter etter personvernregelverket.*

|  |
| --- |
| Risikovurdering av medbestemmelse |
|  Innspill til risikovurderingen: * Har de registrerte en reell innflytelse på hvordan hans eller hennes personopplysninger skal behandles?
* Har de registrerte muligheten til å utøve sine rettigheter? Dersom for eksempel behandlingen er hjemlet i rettslig forpliktelse (artikkel 6 c), så har ikke de registrerte rett til å protestere. Det er et eksempel på redusert medbestemmelse.
 |
| **Tiltak for å redusere risiko** |
| * Beskriv relevante tiltak
 |
| **Vurdering av restrisiko** |
| * Beskriv restrisikoen (risikoen etter at tiltakene er gjennomført)
 |

## Risiko for manglende reell forutsigbarhet

*Forutsigbarhet vurderes i denne sammenheng å være tiltak for å gjøre en behandling mindre kompleks, og dermed lettere å forstå.*

|  |
| --- |
| Risikovurdering av forutsigbarhet |
| Innspill til risikovurderingen: * Gjennomføres automatiserte avgjørelser som skaper usikkerhet om hva som ligger til grunn for avgjørelsen?
* Brukes kunstig intelligens i skolesystemet som skaper usikkerhet om hva som ligger til grunn for handlingene som gjennomføres?
 |
| **Tiltak for å redusere risiko** |
| * Beskriv relevante tiltak
 |
| **Vurdering av restrisiko** |
| * Beskriv restrisikoen (risikoen etter at tiltakene er gjennomført)
 |

## Andre risikoer

*Andre risikoer kan være relatert til vurderingene rundt personvernprinsippene, de registrertes rettigheter eller høye risikoer som er dekket av ROS.*

|  |
| --- |
| Risikovurdering |
| Innspill til risikovurderingen: * Er det andre risikoer som kan påvirke tilliten til kommunen?
* Er det andre risikoer knyttet til personvernprinsippene?
* Er det andre risikoer knyttet til de registrertes rettigheter?
* Er det andre risikoer knyttet til frihet etter EMK?
* Er det andre risikoer knyttet til gjennomført ROS?
 |
| **Tiltak for å redusere risiko** |
| * Beskriv relevante tiltak
 |
| **Vurdering av restrisiko** |
| * Beskriv restrisikoen (risikoen etter at tiltakene er gjennomført)
 |

# Synspunkter

*Dette kapitlet omfatter synspunktene til de relevante interessentene.*

|  |
| --- |
| Behandlingsansvarliges synspunkter på behandlingen og dens risikoer |
| * Beskriv behandlingsansvarliges vurdering av behandlingen
* Beskriv behandlingsansvarliges vurdering av om restrisiko er akseptabel
 |

|  |
| --- |
| Personvernombudets synspunkter på behandlingen og dens risikoer |
| * Beskriv personvernombudets vurdering av behandlingen
* Beskriv personvernombudets vurdering av om restrisikoen er akseptabel
 |

|  |
| --- |
| De registrertes synspunkter på behandlingen og dens risikoer (dersom aktuelt) |
| * Beskriv de registrertes vurdering behandlingen
* Beskriv de registrertes vurdering av om restrisiko er akseptabel
 |

# Ledelsens validering

*Dette kapitlet omfatter vurderinger som ledelsen har gjort, herunder ledelsens beslutning.*

|  |
| --- |
| Arbeidsgruppens innstilling til ledelsen |
| * Skriv et sammendrag av vurderingene som er gjort, herunder det samlede risikobildet, de planlagte tiltakene og eventuell restrisiko
* Skriv en innstilling til ledelsen (konklusjon fra arbeidsgruppa)
 |

|  |
| --- |
| Ledelsens vurderinger |
| * Skriv når og i hvilket møte ledelsen har behandlet DPIAen
* Skriv hvilke vurderinger ledelsen har gjort
 |

|  |
| --- |
| Ledelsens beslutning |
| \* DPIA er godkjent. Behandlingen kan gjennomføres. \* DPIA er avvist. Behandlingen kan ikke gjennomføres. \* DPIA er godkjent med følgende betingelser: \* DPIA viser at restrisiko fortsatt er høy. Gjennomfør forhåndsdrøftelse med Datatilsynet. |