SENTER
FOR IKT I
UTDANNINGEN

Datavask og rutiner

– beste praksis

Veiledning |

Om Senter for IKT i utdanningen

Senter for IKT i utdanningen ble opprettet 1. januar 2010 og er underlagt Kunnskapsdepartementet. Senteret skal bidra til å iverksette regjeringens politikk innenfor grunnopplæringen, barnehageområdet og lærer- og førskolelærerutdanningen, og er en sammenslåing av flere tidligere nasjonale initiativ; ITU, Uninett ABC og Utdanning.no.

Dette dokumentet er en del av senterets dokumentbibliotek og er derfor løftet frem under senterets samlede profil.

Rettigheter

Senter for IKT i utdanningen // Publisert 2007, revidert og trykket februar 2013

Forord

Om FEIDE

Feide står for Felles Elektronisk IDEntitet og er Kunnskapsdepartementets satsing på enhetlig identitetsforvaltning i utdanningssektoren, både for grunnopplæringen og for høyere utdanning.

Senter for IKT i utdanningen har ansvar for å veilede skoleeieer ved innføringen av Feide i grunnopplæringen. Veiledningen er et gratis og leverandørnøytralt tilbud til alle skoleeiere i Norge.

Arbeidet med utvikling av Feides tekniske løsning, juridiske aspekter og annet Feide-arbeid koordineres av den sentrale Feide-organisajonen i UNINETT AS.

Les mer om Feide på **feide.iktsenteret.no**

Om denne veiledningen

Denne veiledningen gir skoleledere, skoleeiere og andre beslutningstakere en innføring i hvordan man kan implementere og oppnå god identitetsforvaltning gjennom datavask og rutiner for behandling av personinformasjon.

Innledningen (kapittel 1–3)

gir en innføring i identitetsforvaltning og hvorfor det er viktig å sikre gode rutiner rundt dette.

Del I (kapittel 4)

gir råd om hvordan man kan gjennomføre datavask.

Del II (kapittel 5, 6 og 7)

viser hvordan man kan utarbeide retningslinjer og regler som bidrar til å opprettholde god datakvalitet.

Del III (kapittel 8)

viser hvordan Rogaland fylkeskommune gjennomførte datavask og innføring av retningslinjer for sine skoler.

Innholdsfortegnelse

DEL II

RUTINER OG RETNINGSLINJER

DEL III

EKSEMPEL

Innledning

1 Om identitetsforvaltning

Identitetsforvaltning handler om å sikre riktig person tilgang til riktig informasjon til rett tid. Det handler med andre ord om å identifisere mennesker, og å kontrollere den tilgangen de har til ulike dataressurser.

Gjensidig tillit

Gode systemer for identitetsforvaltning gjør det mulig å spre personinformasjon, brukernavn og lignende på tvers av ulike systemer og applikasjoner, slik at det holder med ett brukernavn og én enkelt pålogging for de fleste tjenester.

Hele identitetsforvaltningssystemet, og hvorvidt det fungerer riktig, avhenger av kvaliteten på informasjonen som blir produsert i de enkelte organisasjonene som er tilknyttet systemet. Identitetsforvaltningen bygger derfor på gjensidig tillit mellom organisasjonene, og forutsetter at samtlige organisasjoner leverer data av god kvalitet.

Datakvalitet

Elektroniske tjenester ved organisasjoner og fellestjenester på nasjonalt nivå må kunne stole på at brukerdataene i de lokale katalogtjenestene til enhver tid er oppdaterte og korrekte. Dersom det er oppgitt at Andreas er elev i 8. klasse ved Eidsvåg barne- og ungdomsskole, må alle tjenester kunne stole ubetinget på at Andreas faktisk er elev i 8. klasse ved Eidsvåg barne- og ungdomsskole.

Den enhetlige identitetsforvaltningen i utdanningssektoren i Norge, Feide, er avhengig av at enhver tilknyttet organisasjon har god kontroll på sin lokale identitetsforvaltning.

Både staten (i form av lover og regler) og Feide stiller svært høye krav til organisasjonenes kildesystemer med tanke på riktighet og behandling av persondata, og krever rutiner og retningslinjer for håndtering av brukerdata. Dette skal sørge for at opplysningene forblir riktige.

2 Krav til skoleeiere

Siden det er så viktig at persondata er korrekte og blir behandlet riktig, stilles det høye krav til identitetsforvaltningsorganisasjoner, særlig med hensyn til behandling av persondata. Det kan være relevant med ulike krav for ulike deler av organisasjonen. Kravene til behandling av persondata gjelder imidlertid hele organisasjonen.

Erfaring har vist at det er nettopp dette – behandlingen av persondata – som krever mest ressurser i en organisasjon, og ikke innføringen av den tekniske løsningen. Dette gjelder spesielt dersom organisasjonen ikke følger de rutinene som er nødvendige og pålagte av det norske lovverket.

Under finner du en gjennomgang av lover og regler som alle tilknyttede identitetsforvaltningsorganisasjoner må forholde seg til.

2.1 Norsk lovgivning

Staten opererer med særskilte lover og regler som skal beskytte data og regulere behandling av personopplysninger. Flere deler av norsk lovgivning er relevante for identitetsforvaltning. For mer informasjon, se veiledningen *Krav til en vertsorganisasjon i Feide*, kapittel 1.1 på. http://feide.iktsenteret.no/publications.

2.2 Generelle anbefalinger for identitetsforvaltning

Organisasjonen må oppfylle en rekke krav for å oppnå god identitetsforvaltning:

- Ved behandling av personopplysninger må organisasjonen følge gjeldende regelverk og norsk lovgivning.
- Det stilles krav til datakvalitet: Organisasjonen skal sikre at alle personopplysninger som omfattes av identitetsforvaltningen, er godt vedlikeholdte og korrekte, og i elektronisk form.
- For hvert dataelement, f.eks. navn, adresse osv., må den autoritative kilden være definert (se mer om datakilder og autoritative kilder i kapittel 3).
- Det må foreligge skriftlige og veldokumenterte rutiner for å legge inn og endre persondata. Rutinene skal sikre at persondata forblir korrekte. Det innebærer for eksempel at dersom skolene lar tidligere elever beholde sine brukerkonti, skal de ikke lenger ha rollen «elev» i systemet.
- Organisasjonen må kunne dokumentere oppretting av brukernavn benyttet for identitetsforvaltning. Større organisasjoner må i praksis innføre et brukeradministrativt system der man oppretter og vedlikeholder slike brukernavn.
- Organisasjonen må dokumentere og gjennomføre en god, maskinell metode for å overføre persondata mellom systemene som er knyttet til identitetsforvaltningsløsningen. For større organisasjoner vil dette normalt skje ved overføringsjobber knyttet til brukeradministrative systemer. Alle datakorreksjoner skal utføres i kildesystemer og automatisk forplantes videre til de andre systemene. For svært små organisasjoner kan dataene legges manuelt inn i systemene. Forutsetningen er at det gjøres feilfritt og at det eksisterer en pålitelig rutine for å sjekke dataene og sørge for at de er i samsvar med dataene i kildesystemene.
- Krav om bruk av roller: Roller og former for tilknytning som brukere kan ha til organisasjonen, må være klart definerte. Alle brukere i identitetsforvaltningsløsningen skal ha minst én tilknytning til sin vertsorganisasjon.

2.3 Feide-krav til organisasjoner

I tillegg til de generelle kravene i avsnitt 2.2, stiller Feide følgende krav til organisasjoner som ønsker å knytte seg til Feides innloggingstjeneste:

- Feide krever at organisasjonen stiller med en LDAP-katalog som presenterer persondata på et spesifisert format. Denne katalogen knyttes opp til den lokale identitetsforvaltningsløsningen.
- Feide kan kreve å få innsyn i dokumentasjon om hvordan organisasjonen behandler personopplysninger som er inkludert i Feide-skjema og som organisasjonen har utstedt Feide-navn for.
- Organisasjonen skal ha et IKT-reglement som oppfyller visse minimumskrav. Det må blant annet gjøre organisasjonen i stand til å foreta sanksjoner overfor en bruker som har forbrutt seg mot en annen organisasjon eller tjeneste gjennom sin tilknytning til moderorganisasjonen via Feide-systemet.
- Organisasjonen skal inngå avtale med hver enkelt bruker som får Feide-navn. Avtalen forplikter brukeren til å overholde IKT-reglementet.

Dette heftet gjør rede for hvordan din organisasjon kan sørge for korrekte persondata. Det foreslår rutiner som sikrer og forenkler arbeidet med å vedlikeholde slike opplysninger.

3 Kildesystemer for identitetsforvaltning

Skoler og studiesteder har behov for å lagre informasjon om personene som er knyttet til lærestedet. Dette kan være elever, studenter, ansatte eller andre. I grunnskolen kan det i tillegg være behov for å lagre informasjon om elevenes foresatte. En forutsetning for å kunne innføre elektronisk identitetsforvaltning, også for Feide, er at denne personinformasjonen er lagret elektronisk.

3.1 Skoleadministrativt system

Ofte er det snakk om så store mengder data at det kreves spesielle systemer for å lagre dem. Én slik systemtype er skoleadministrativt system (SAS). I dag er flere slike systemer i bruk i sektoren, blant andre SATS, Extens,TP-systemer, Unique skole og Oppad. I tillegg til administrasjon av personinformasjon kan systemene tilby funksjoner som:

- lagring av karakterer og andre vurderinger
- fraværsregistrering

- planlegging og utforming av studie- og timeplaner
- personers tilhørighet til fag, grupper, årskurs osv.

3.2 Kildesystemer

I identitetsforvaltningssammenheng kalles et system for å vedlikeholde persondata, for datakilde eller et kildesystem. Et skoleadministrativt system kan godt være det eneste kildesystemet til et lokalt identitetsforvaltningssystem, men det kan også finnes flere (lønns- og personalsystem, telefonsystem osv.).

3.3 Autoritative kilder

Dersom organisasjonen har flere kildesystemer, er det svært viktig å vite hvilket kildesystem som er autoritativt, det vil si hvilken kilde som til enhver tid er primærkilden for et visst dataelement. Autoritative data er de opplysningene som regnes som mest riktige – de som kommer fra den mest pålitelige kilden. For eksempel er Det sentrale folkeregister (DSF) autoritativ kilde for navn og fødselsdato for alle norske statsborgere. På samme måte er det skoleadministrative systemet autoritativ kilde for en persons tilknytning til skolen, for eksempel om han eller hun er elev eller ansatt.

Autoritative kilder er nødvendig for automatiske og konsistente oppdateringer av identitets- forvaltningssystemet, spesielt dersom ulike kilder overlapper med tanke på personinformasjon, eller det finnes ulike informasjonsbiter om personer i forskjellige systemer. En god identitetsforvaltning knytter en identitet sikkert til opplysninger fra autoritative kilder.

3.4 Rutiner for datakilder

Skal datakildene være tilgjengelige, inneholde pålitelige data og kunne gjenbrukes i identitetsforvaltningen, er følgende viktig:

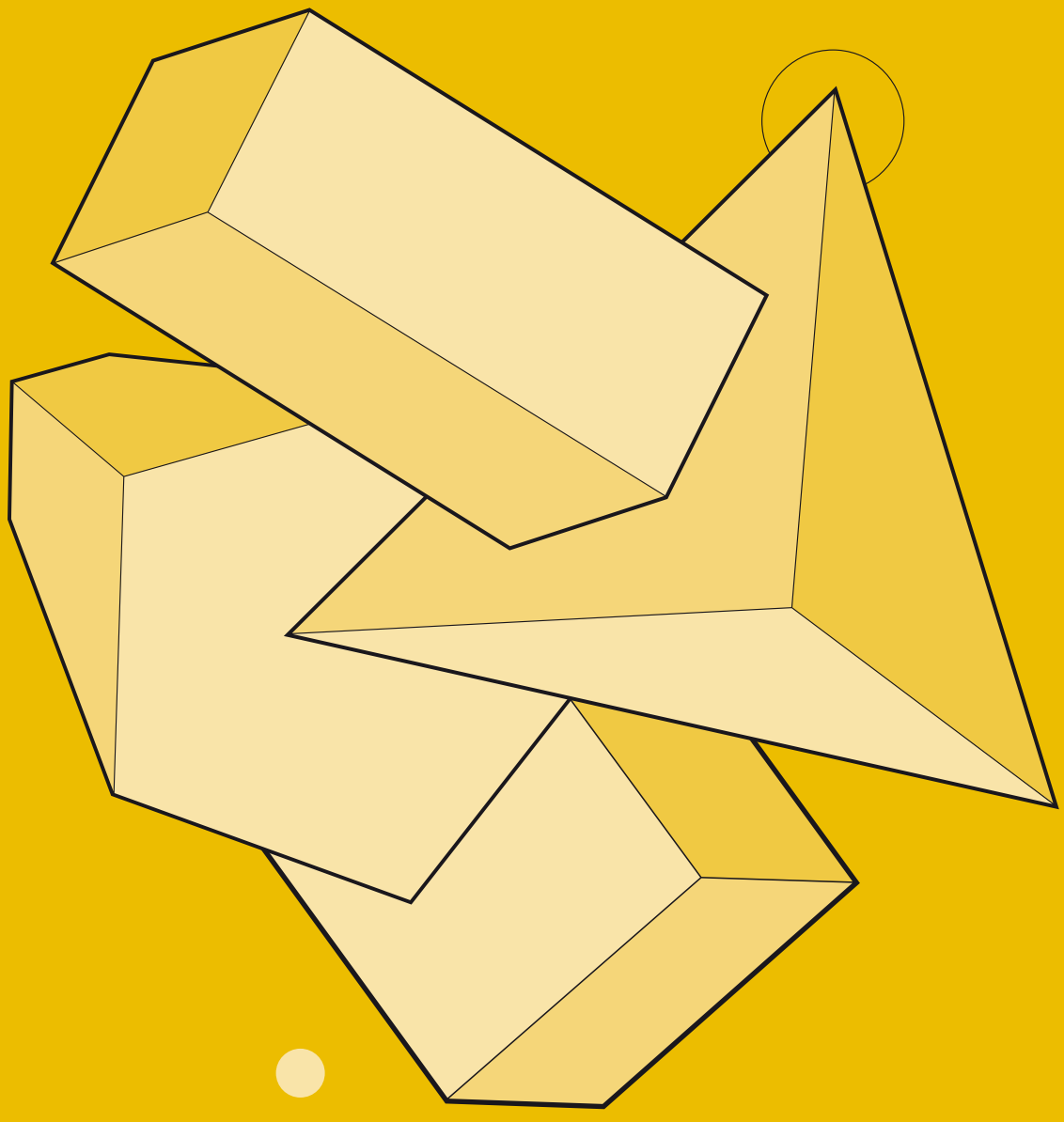
- Organiser dataene: Vit hvilke informasjonsbiter som må finnes om personene som er knyttet til organisasjonen, og hvor dataene er lagret. Foreta om nødvendig en omfattende opprydding i alle kildesystemene.
- Vedlikehold dataene: Identitetsforvaltningens krav om datakvalitet og oppdaterte data krever dokumenterte rutiner for persondatahåndtering og vedlikehold. Rutinene bør dekke hele livssyklusen til dataene.
- Verifiser den registrerte informasjonen.
- Tilrettelegg drift og tekniske forhold: Styrk datakvaliteten gjennom tiltak som backup/sikkerhetskopi, adgangskontroll, drift og systemvedlikehold, endringshistorikk, logging og lignende. Se mer om dette temaet i anbefalingen *Daglige driftsaktiviteter* på http://feide.iktsenteret.no/publications.

I det følgende ser vi nærmere på de tre første punktene i denne listen, nemlig hvordan gjennomføre oppryddingen i datakildene, hvordan sørge for godt vedlikehold med riktige rutiner, og verifisering av den registrerte informasjonen.

Husk at analyse, vask og rutiner alltid må gå om hverandre. I dette heftet er temaene skilt klart fra hverandre for enkelhets skyld, men er altså ikke ment som en sekvensiell inndeling av oppgaver og rekkefølge. Oppgavene kan og bør utføres parallelt som en kontinuerlig prosess.

Del 3 presenterer et eksempel på gjennomføring av datavask og innføring av rutiner. Eksempelet er hentet fra Rogaland fylkeskommune.

DEL 1



Datavask

4 Opprydding i alle kildesystemer – datavask

4.1. Hvorfor datavask?

Kildesystemer skal inneholde korrekt, konsistent og oppdatert informasjon. Dette er nødvendig for at de tjenestene som benytter den valgte identitetsforvaltningsløsningen, skal kunne stole på informasjonen de får.

Dersom eleven Pål går i 9. klasse, men er registrert som elev i 8. klasse i datasystemet, vil han for eksempel ikke få tilgang til de riktige områdene i LMS-et (læringsplattformen). Han kan også oppleve å få tilsendt e-post som skal til 8.-klassingene, og gå glipp av e-post som skal til 9. klassetrinn.

Ved innføring av identitetsforvaltning er det å sikre korrekt, konsistent og oppdatert informasjon vanligvis den største jobben. Hvis din organisasjon ikke allerede har ryddet opp i systemene og kartlagt hvor personopplysninger behandles, bør dere derfor starte med denne prosessen så tidlig som mulig i arbeidet.

Hensikten med en slik kartlegging og kontroll er å sørge for at personopplysninger ikke legges inn og behandles unødvendig mange steder, at de er korrekte, og at de følger et visst format. Oppryddingen innebærer å

- kartlegge og kontrollere alle kildesystemer
- rydde og rette opp dersom det finnes feil eller inkonsistent informasjon i systemene.

For mer om datavask, sjekk veiledningen *Krav til en verts-organisasjon i Feide*, kapittel 1.2 http://feide.iktsenteret.no/publications.

4.2 Kartlegg personopplysningene

Én kilde

I identitetsforvaltningen er det et grunnleggende krav at én type data skal ha kun én autoritativ kilde (det er ok med flere forskjellige systemer dersom de behandler forskjellige typer data). Den lokale løsningen vil sørge for kontrollert gjenbruk av data. Derfor lønner det seg å ha god kontroll på og oversikt over persondata.

Få oversikt

De fleste organisasjoner har flere registre og tjenester som inneholder personinformasjon. En av de store oppgavene i forbindelse med innføring av identitetsforvaltning, er å kartlegge og skape oversikt over alle disse registrene og alle tjenester som benytter seg av informasjonen. Her ligger også en av de store gevinstene med identitetsforvaltning: Kontroll over personinformasjonen i organisasjonen.
Kartleggingen skal avdekke

- hvor ulike personopplysninger legges inn og oppdateres
- hvor det finnes dupliserte data i flere registre og tjenester
- hvor og hvordan informasjonen brukes i forskjellige tjenester
- hvor informasjonen flyter (sørge for kontrollert flyt av data)

Hvor finner dere personinformasjonen?
Typiske registre der informasjon legges inn, er lønns- og personalsystemer, skoleadministrative systemer og inntakssystemer. IKT-avdelingen har ofte andre registre, for eksempel katalogtjenester for telefonsentraler, kataloger som OpenLDAP, Microsoft Active Directory, Novell eDirectory og lignende.

Hvilke tjenester bruker informasjonen?
Typiske tjenester som benytter denne informasjonen, er læringsplattformer (LMS), e-posttjeneste, webportaler og lignende. Dersom registre og tjenester ikke er koblet sammen, må personinformasjonen registreres mange steder. Det innebærer økt ressursbruk og større risiko for feil.

I tillegg kan det finnes nasjonale og regionale tjenester som opptakssystemer, eksamenssystemer og innholdstjenester, som i dag krever registrering av personinformasjon.

Slik kartlegger dere personinformasjonen
Lag en oversikt over alle registre som systemene ved skolen bruker, og hvordan de brukes. Lag også oversikt over hvilke personopplysninger som lagres hvor, og hold denne oppdatert:

- Kartlegg hvilke personregistre som finnes for elever/studenter, lærere og andre ansatte:
  - hos IT-avdelingen
  - hos opplæringsavdelingen
  - hos personalavdelingen
  - andre steder

- Kartlegg hvilke tjenester som benyttes på de ulike skolene og hos kommunen, både lokale og regionale/nasjonale tjenester:
  - snakk med de enkelte skolene
  - snakk med IT-avdelingen
  - snakk med opplæringsavdelingen

- Kartlegg hvilke personopplysninger som finnes i de forskjellige personregistrene:
  - hvilken informasjon lagres om lærere
  - hvilken informasjon lagres om andre skoleansatte
  - hvilken informasjon lagres om elever
  - hvilken informasjon lagres om foresatte

- Kartlegg hvilke personopplysninger som benyttes av de forskjellige tjenestene:
  - hvilken personinformasjon lagres i selve tjenestene
  - hvilken personinformasjon får tjenestene fra personregistre

- Bestem hvilket kildesystem som skal være autoritativt for forskjellige personopplysninger og ulike persontyper (elever, lærere, andre).

Kartleggingen bør være så grundig som mulig, og bør inkludere alle personregistre og tjenester. Sannsynligvis avslører kartleggingsprosessen at dere behandler personopplysninger på langt flere steder enn antatt.

4.3 Kontroller alle personopplysninger

Datavaskingen må inkludere en gjennomgang og kvalitetssjekk av alle data i de ulike systemene:

- Fjern utdatert og fyll inn manglende informasjon. Husk også å korrigere feil informasjon.

- Fjern duplisert informasjon: Ulike registre kan ofte overlappe hverandre. Slike overlapp er uheldige, og må unngås i størst mulig grad. Dersom dere vurderer noen overlappinger som nødvendige, må dere beslutte hvilke registre som skal brukes til autoritative data, og innordne datakildene hierarkisk basert på autoritativt innhold.

- Sørg for konsistent feltbruk: Samme type informasjon bør alltid ligge i samme og riktige felt.

- Sørg for konsistens på inntastede verdier og valgte formater: Hjemmeadressen må ikke bare skrives i feltet for adresse, den må også skrives på et på forhånd definert format. Det samme gjelder andre felter, blant annet for telefonnumre.

Bli enige om bruk av felter og formater for data, og fastslå bruken i en rutinehåndbok (les mer om dette i avsnitt 5.4).
I identitetsforvaltningen er det spesielt tre personattributter som er viktig å håndtere riktig:

- Navn

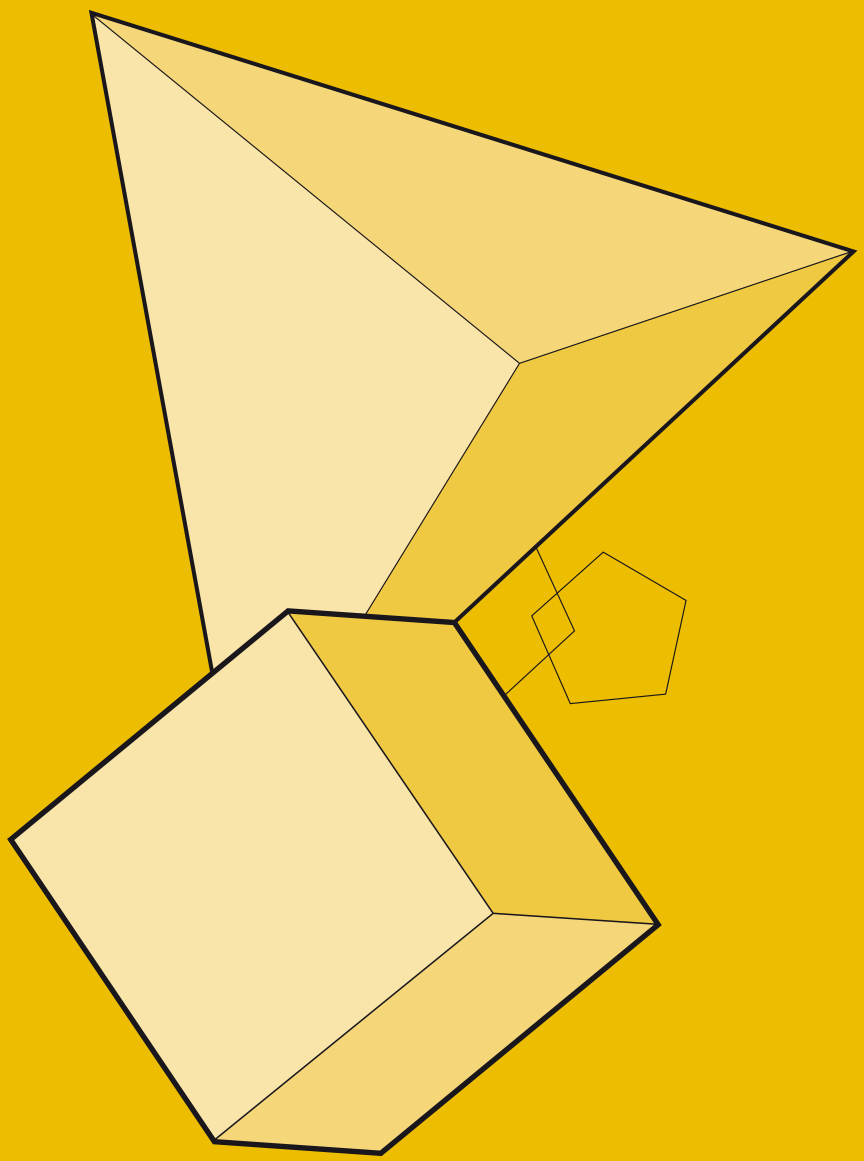
- Fødselsnummer

- Personens tilknytning til organisasjonen/lærestedet (roller)

Vær oppmerksom på at fødselsnummer ikke brukes som brukernavn i identitetsforvaltningen siden dette vanligvis ikke er tillatt. I Feide brukes fødselsnummeret kun internt i systemet, som en unik nøkkel til alle personer som får Feide-navn.

Det finnes muligheter for kontroll og vaskemuligheter for fødselsnummer mot Det sentrale folkeregister (DSF). EVRY er enedistributør av data fra DSF, og tilbyr blant annet datavasktjenester. Les mer om dette på Skattedirektoratets nettsider (http://www.skatteetaten.no/no/person/folkeregister) og EVRYs Infotorg-tjeneste (http://www.infotorg.no).

DEL 2



Rutiner og retningslinjer

5 Opprethold datakvaliteten: Innfør retningslinjer og rutiner

Organisasjonen må ha skriftlige retningslinjer for identitetsforvaltning, og må kunne dokumentere at behandlingen av opplysninger følger de eksisterende rutinene.

Dokumenter oppdateringer i kildesystemene

Det vil i de fleste organisasjoner være lurt å dokumentere hvordan handlinger som utføres jevnlig, fører til oppdateringer i kildesystemene. Handlinger som oftest krever oppdateringer og oppfølging er:

- Ny, endret eller «sletting» av elev. «Sletting» trenger ikke bety fysisk avslutning, men kan også dekke tilfeller som suspendering og permisjon, slik at personen og databrukeren eksisterer, men får en annen (for eksempel inaktiv) tilknytning til lærestedet.
- Ny, endret eller sletting av ansatt.
- I grunnskolen er det i tillegg aktuelt å registrere elevenes foresatte. Også her gjelder ny, endret eller sletting av informasjon.

Lag vanntette rutiner og retningslinjer

Gå gjennom organisasjonens rutiner for å opprette og endre personinformasjon, og forsikre dere om at rutinene er gode nok til raskt å fange opp og oppdatere informasjon som endrer seg. Hver avdeling som er ansvarlig for ett eller flere personregistre, bør lage en slik oversikt.

Sørg også for at rutinene ved fjerning av informasjon er gode. Husk at så lenge en person er registrert som aktiv i faggrupper og klassetrinn, vil vedkommende ha tilgang til tjenestene, selv om han ikke lenger tilhører organisasjonen. Pass derfor på at rutinene fanger opp at personer slutter i organisasjonen, enten det er elever som går ut eller ansatte som skifter stilling eller slutter.

Dette bør rutinene omfatte

Retningslinjene for identitetsforvaltning bør blant annet angi rutiner for:

- hvem som skal tildeles elektroniske identiteter i organisasjonens IKT-infrastruktur (for eksempel elever, lærere, andre ansatte og andre personer som er tilknyttet).
- hva identiteten skal brukes til.
- i hvilke tilfeller personer kan gis flere identiteter (et eksempel kan være personell som har spesielle roller, som IKT-ansvarlige, og som derfor trenger identiteter med utvidede rettigheter). Hold antallet personer med flere identiteter til et absolutt minimum.
- registrering av personopplysninger. Når og hvordan skal identiteten opprettes?
- endring av personopplysninger. Hvordan skal identiteten vedlikeholdes? Hva forårsaker hendelsen? Er organisasjonen passiv (mottaker av informasjon) eller aktiv (sender av informasjon)? Dette siste kan ha betydning for hvilken informasjonsmengde som kreves for å oppdatere systemene.
- sletting av personopplysninger. Når og hvordan skal identiteten termineres?
- om informasjonen må kvalitetssikres på noen måte. Må den for eksempel oversettes fra et format til et annet?
- hvilken informasjonsmengde som skal oppdateres i hvilke kildesystemer.
- hvor lang tid det vil eller bør ta før den korrekte informasjonen er spredd til de andre systemene.
- bruk av datafelter.

Det er viktig at alle som jobber med personopplysninger, er kjent med de etablerte rutinene. Like viktig er det imidlertid at alle faktisk følger dem.

Vi anbefaler at dere lar rutinene omhandle og kategoriseres etter temaene under. I tillegg kan dere ha lokale behov som dere må ta hensyn til, og som kan endre og utvide listen under. La svarene på spørsmålene under hver kategori/tema danne utgangspunkt for en allment kjent praksis i organisasjonen. Ønsker du å vite mer om rutiner og retningslinjer, se veiledningen *Krav til en vertsorganisasjon i Feide*, kapittel 1.3 på http://feide.iktsenteret.no/publications.

5.1 Registrering av personopplysninger

En viktig forutsetning for ryddige kildesystemer er at de som legger inn nye personer i systemene, følger samme regler. Alle som jobber med registrering av personopplysninger, må derfor være enige om følgende:

- Når skal en person registreres?
- Hvilken informasjon skal legges inn om vedkommende (i tillegg til de obligatoriske attributtene)?
- Hvor kommer informasjonen fra?
- Hvilken kvalitet har informasjonen?
- Hvem har ansvar for å registrere og legge inn informasjon om en person? Ansvaret bør knyttes til en rolle heller enn person for å sikre fleksibilitet.

5.2 Endring av personopplysninger

Alle bør følge de samme reglene når personopplysninger skal endres. Alle endringer skal utføres korrekt og konsekvent i de autoritative kildene, som så automatisk oppdaterer andre tilknyttede systemer. Alle som skal ha tilgang til å endre personopplysninger, må være enige om følgende:

- Hvordan meldes endringer?
- Hvem kan initiere endringer av forskjellig type informasjon?
- Hvem har ansvar for å gjøre endringene? Ansvaret bør knyttes til en rolle heller enn person for å sikre fleksibilitet.
- Hvor lang tid (maksimalt) skal det gå fra en endring blir meldt inn til den blir registrert?
- Hvor kommer den nye informasjonen fra?
- Hvilken kvalitet har den nye informasjonen?
- Spres endringene som legges inn i dette kildesystemet til alle andre relevante systemer?

5.3 Sletting av personopplysninger

Alle personer som sletter personopplysninger, må utføre sletting etter samme regler og være enige om følgende:

- Hvordan meldes en sletting?
- Hvem kan initiere en sletting av informasjon? Sletting av informasjon vil typisk skje når en elev eller ansatt slutter og ikke lenger er tilknyttet organisasjonen. Det må være avklart hvem som gir beskjed om slike hendelser.
- Hvem har ansvar for å utføre slettingen? Ansvaret bør knyttes til en rolle heller enn person for å sikre fleksibilitet.
- Hvor lenge etter at en person har sluttet, slettes personopplysningene?
- Hvordan forsikrer en seg om at en sletting faktisk skal gjennomføres (hva må være på plass før slettingen utføres)?
- Skal en person kunne komme tilbake til organisasjonen og få tilbake den samme informasjonen om seg selv? Og hvis dette er tilfelle, hvor lenge skal det være mulig?

5.4 Regler for bruk av datafelter

Mange systemer inneholder såkalte fritekstfelter, det vil si felter hvor en i praksis kan registrere og legge inn hva som helst. Siden det ikke eksisterer tekniske begrensninger for hvilken informasjon som ligger i disse feltene og på hvilket format, er praksis for hvordan slike felt brukes, svært varierende. Det er derfor viktig å innføre konsistente regler for hvordan feltene fylles ut, slik at informasjonen i fritekstfeltene ikke går tapt. Spesielt viktig blir dette når informasjon flyter på tvers av systemer, og mottakersystemet må kunne tolke dataene maskinelt. For å sikre at datafelter brukes på en konsistent måte, må alle være enige om følgende:

- Hvilken informasjon må foreligge om alle personer, dvs. hvilke felter skal være obligatoriske å fylle ut?
- Hvilke felter skal være valgfrie å fylle ut?
- Hvilke felter skal ikke fylles ut?

- Skal et felt kunne inneholde én eller flere verdier? For eksempel kan en tillate flere registrerte telefonnumre per bruker, men bare ett fødselsnummer.
- Hvilken informasjon skal ligge i hvilket felt? Kan det for eksempel være aktuelt å tillate at telefonnummerfeltet fylles ut med mobilnummer dersom det ikke eksisterer noe fasttelefonnummer?
- Hvilke felter skal inneholde tall, og hvilke skal inneholde tekst?
- Etter hvilke standarder eller normer skal hvert felt fylles ut? Typiske data det er viktig å beslutte standarder for, er navn (for eksempel: etternavn, fornavn, mellomnavn) og datoer (for eksempel: dag, måned, år).
- Hvordan brukes roller?

6 Verifiser den registrerte informasjonen

For å øke sannsynligheten for at registrerte personopplysninger er korrekte, bør dere innføre rutiner som verifiserer all registrert informasjon. Det kan gjøres ved å

- innføre selvregistreringssystemer, der brukeren med jevne mellomrom selv må verifisere at registrerte opplysninger er korrekte.
- ta stikkprøver av informasjonen.

I tillegg bør dere ha rutiner som sikrer at informasjonen raskt blir endret dersom den ikke er korrekt.

Husk at rutinene jevnlig bør revurderes og oppdateres. Husk også at alle nyansatte som skal registrere og behandle personopplysninger, må få tilstrekkelig opplæring i rutinene.

Feide-brukere kan logge seg inn på http://innsyn.feide.no for å verifisere registrert informasjon i organisasjonens lokale Feide-katalog.

7 Sjekkliste

Bruk punktene under for å få på plass gode rutiner som sikrer korrekte og oppdaterte data.

7.1 Ansatt-, elev- og foresattdata

- Hva er den eksisterende kilden for ansatt-/elev-/foresatt-data, og er kilden til enhver tid oppdatert med korrekte data?
- Flyter korrekt informasjon fra kildene og ut til andre systemer (og da spesielt informasjonen om roller og tilhørigheter)?
- Hvilke rutiner eksisterer for å vedlikeholde datakvaliteten?

7.2 Roller

- Hvilke roller benyttes i systemet?
- Hvilke regler gjelder for hvem som kan få tildelt hvilken rolle?
- Hva er kilden til opplysningene om personene og deres roller?

7.3 Brukerkontoer

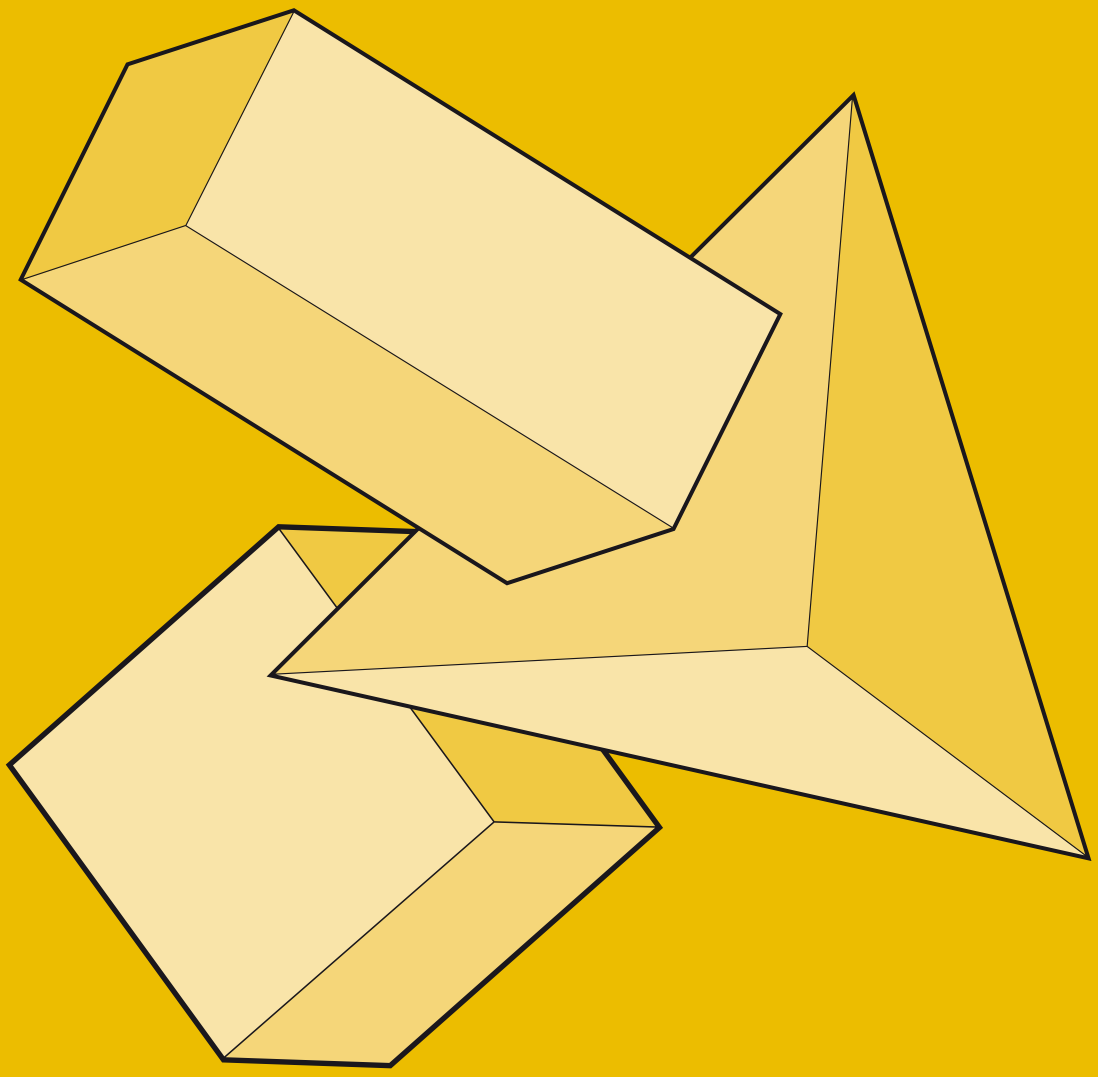
- Hvordan verifiseres identiteten til personer som får tilgang til en brukerkonto?
- Hva er organisasjonens krav til passordsikkerhet og eventuelle andre akkreditiver (som PKI, engangspassord, mobil)?
- Kan en person få flere brukere? Hvis ja, i hvilke tilfeller?

7.4 Prosesskvaliteten

I tillegg bør dere stille dere følgende spørsmål som belyser prosesskvaliteten rundt behandlingen av personopplysninger:

- Hvor godt forstår avdelingene sine roller og oppgaver med hensyn til behandling av personopplysninger?
- Hvor godt er data som flyter mellom avdelinger og systemer, definert og forstått?
- Finnes det én eller flere klare og oppdaterte beskrivelser av organisasjonsstrukturen?
- Finnes det en oversikt over kontaktpersoner for brukerstøtte?
- Finnes det en oversikt over hvilke personer som har ansvaret for behandling av persondata i kildesystemene?
- Hvor godt kjenner de personene som registrerer personopplysninger til organisasjonens rutiner?
- Gir organisasjonen tilstrekkelig opplæring i rutiner og regler for nyansatte som skal behandle persondata?

DEL
3



Eksempel

8 Rogaland fylkeskommune: Datavask og rutinehåndbok

«Ikke undervurder denne jobben. Gå systematisk til verks og gjennomfør de aktivitetene dere bestemmer dere for. Dere har veldig mye igjen for dette i etterkant. Vurder organiseringen rundt løsningen: Hvem har ansvar for hva og hvor disse ansatte er plassert i organisasjonen.»

Rogaland fylkeskommune

Slik oppsummerer Rogaland fylkeskommune noen av sine erfaringer rundt arbeidet med best mulig å tilrettelegge for riktig persondata og persondatahåndtering. Fylkeskommunen har gjennomført et omfattende arbeid med å rydde i sine kildesystemer (datavask) og har utarbeidet en rutinehåndbok som skal følges av alle ansatte som håndterer persondata.

8.1 Datavask

8.1.1 Kartlegging

Første steg ved rydding i kildesystemer er å lage en oversikt og kartlegge alle systemene man har. Rogaland fylkeskommune gjennomførte følgende kartleggingsaktiviteter:

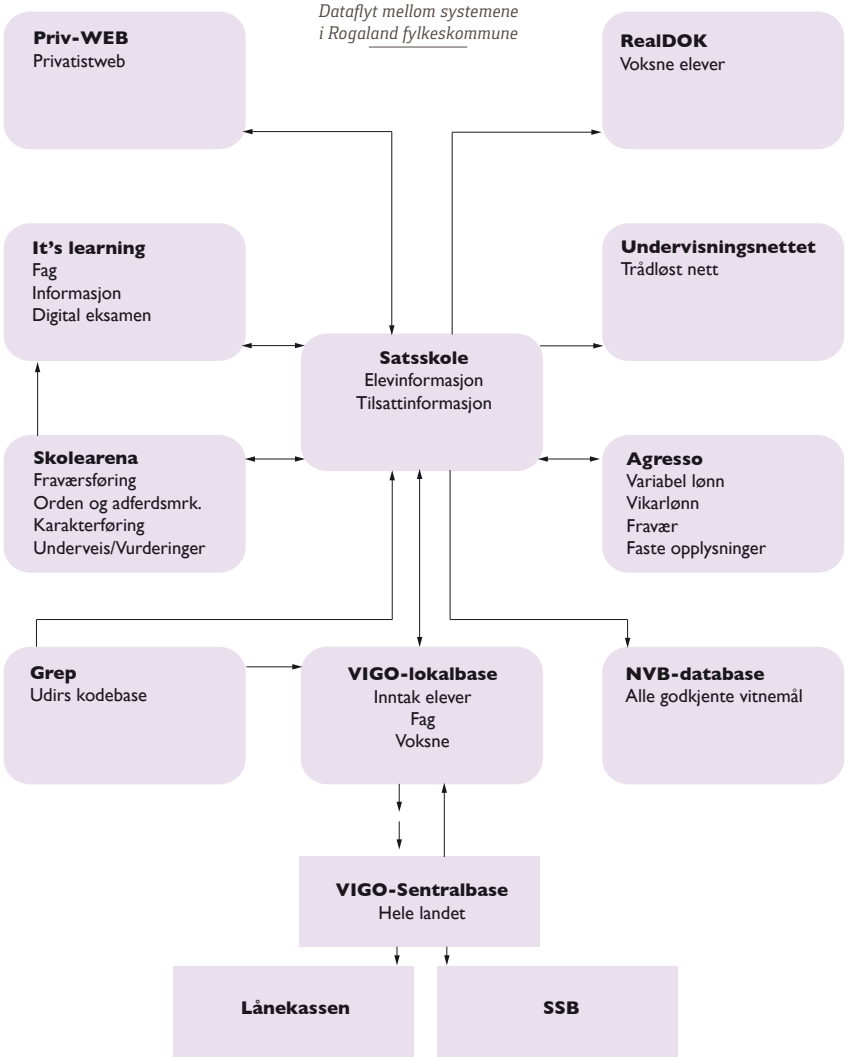
- Identifisere aktuelle systemer: Hvilke systemer har vi? Skal systemet være med i identitetshåndteringen? Hvordan skal systemet være med?
- Identifisere data som skal synkroniseres mellom systemene/dataflyt: Hvilke datafelter, og dermed dataelementer, skal synkroniseres? Hvor hentes dataelementene fra? Skal de synkroniseres begge veier? *Figur 1* viser hvordan Rogaland fylkeskommune har presentert dataflyten mellom sine fagsystemer.
- Identifisere dataeiere: Hvem «eier» dataene? Hvem skal ha siste ordet for et attributt? Hvor skal de forskjellige attributtene redigeres? *Figur 2* viser resultatet av kartleggingen av hvilke avdelinger/instanser som har ansvar for hvilken informasjon i Rogaland fylkeskommune.
- Identifisere prosesser: Hva skal skje hvis brukeren blir deaktivert? Hva skal skje hvis det mangler attributter? Hva skal skje hvis brukeren blir slettet? Følgende aktører bidro til i denne kartleggingsprosessen:
  - Fagpersoner for systemene
  - Personer med god oversikt over organisasjonen
  - Teknisk personell

8.1.2 Opprydding i data

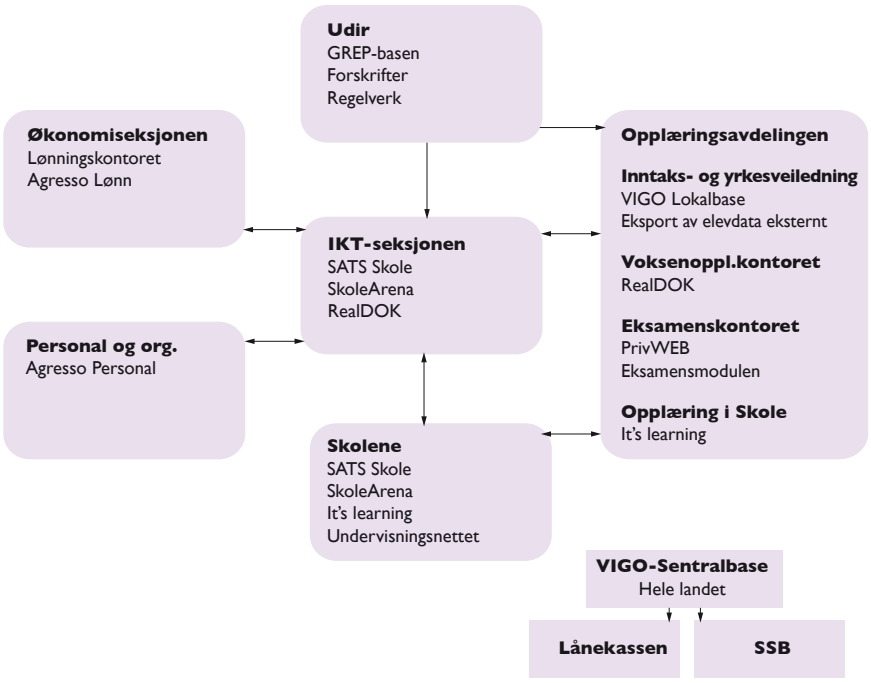
Følgende ble utført:

- Sentral gjennomgang av alle data.
- Informasjon om ny dataløsning ble sendt ut til alle skolene sammen med en oppskrift på hvilken informasjon om elever og ansatte som må sjekkes av hver enkelt skole.
- Det ble satt en frist for gjennomføringen av oppryddingen.

FIGUR 1
Dataflyt mellom systemene i Rogaland fylkeskommune



FIGUR 2
Oversikt over hvilke instanser som har ansvaret for hvilken informasjon



8.2 Rutiner og rutinehåndbok

8.2.1 Prosjektgruppe

Det ble etablert en prosjektgruppe med formål å lage en rutinehåndbok. For å skape forankring og deltakelse blant dem som bruker systemene, bestod gruppen av:

- Systemansvarlige
- SATS-ansvarlige fra 4 skoler (Rogaland fylkeskommune benytter SATS som skoleadministrativt system)
- Ansatte i IKT-seksjonen

Prosjektgruppen gjennomførte følgende oppgaver:

- Kartla forutsetningene for at elever og ansatte skulle bli synkronisert over til under visningsnettet.
- Utarbeidet felles rutiner for elevtabellen.
- Utarbeidet felles rutiner for ansatt-tabellen.

8.2.2 Resultater av prosjektgruppearbeidet (utdrag fra rutinehåndboken)

Rutinehåndboken beskriver rutiner rundt behandlingen av personinformasjon svært detaljert. Figurer og tabeller understøtter tekstlige beskrivelser for å unngå misforståelser. Innholdet omfatter blant annet forutsetninger for at elever og ansatte skal bli eksportert fra SATS og for at nye brukere skal opprettes for disse personene, håndtering av elev- og ansatt-tabeller, håndtering av faggrupper, rutiner rundt synkronisering av informasjon ut til tilknyttede systemer, og oversikter over kontaktpersoner for SATS og brukerstøtte.

Under viser vi et eksempel på hvordan rutinehåndboken presenterer informasjonen. Her gjelder det forutsetningene for eksport av personinformasjonen fra SATS:

Hvilke tabeller er viktige for synkroniseringen:

Elev:

- Korrekt elevstatus
- Må foreligge minst ett fag for det gjeldende skoleåret. Hvis eleven har fag på flere skoler i samme skoleår, blir skolen som først opprettet eleven stående som «eier» helt til eleven settes til sluttet og passiv.

Ansatt:

- Må foreligge et ansettelsesforhold. Den ansatte blir lagt til den skolen han/hun har høyest stillingsprosent. Har de lik tilsettingsprosent på to skoler, blir en av dem tilfeldig valgt.

Likt for elev og ansatt

- Kolonnen Passiv må stå med Nei
- Personnummer (11 siffer må være fylt ut)

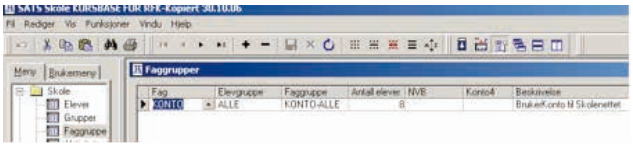
Eksempelet under viser rutinehåndbokens detaljeringsnivå på veiledningene for gjennomføring av rutinene. Her gjelder det håndteringen av faggrupper. For å unngå misforståelser og sørge for at alle utfører rutinene likt, spiller figurene en viktig rolle:

Eleven må ha et fag innenfor gjeldende skoleår for å få tildelt bruker på undervisningsnettet. Hvis eleven ikke har fått tildelt fag innen skolestart, må en legge på et «hjelpefag» . En faggruppe som heter KONTO-ALLE kan opprettes på den enkelte skole til dette formålet.

Hvis fagfordeling ikke er ferdig, bør faget KONTO-ALLE legges på eleven(e) inntil videre. Dette kan gjøres for én og én elev via Elev og Vindu og Elevfag: Ha fremme kolonne for Faggruppe, velg eller skriv inn KONTO-ALLE, og lagre.

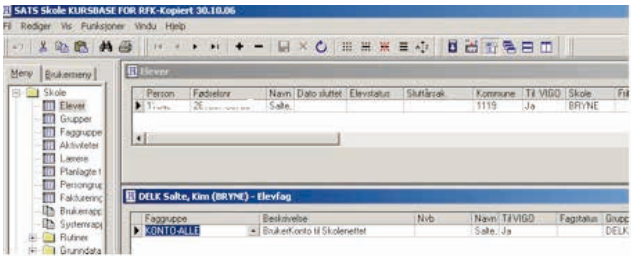
FIGUR 3

KONTO-ALLE brukes for å håndtere tilfeller der eleven ikke har fått tildelt fag innen skolestart.



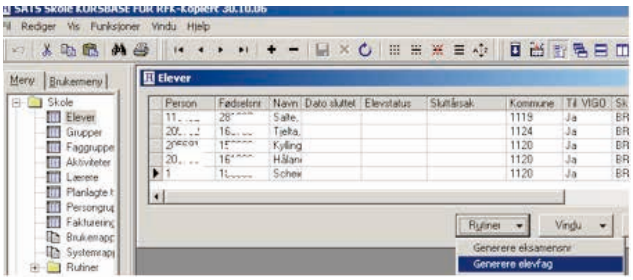
FIGUR 4

Faget KONTO-ALLE legges på eleven(e) – for én og én elev.



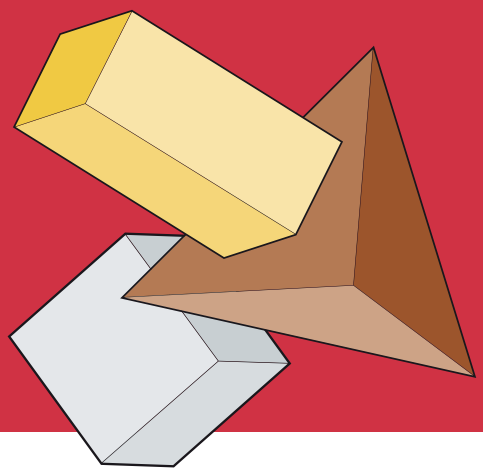
FIGUR 5

Faget KONTO-ALLE legges på flere elever samtidig.



Du finner hele rutinehåndboken til Rogaland fylkeskommune på Feides nettsider
http://feide.iktsenteret.no/publications.

Denne veiledningen gir skoleledere, skoleeiere og andre beslutningstakere en innføring i hvordan man kan implementere og oppnå god identitetsforvaltning gjennom datavask og rutiner for behandling av personinformasjon.



SENTER
FOR IKT I
UTDANNINGEN

www.iktsenteret.no