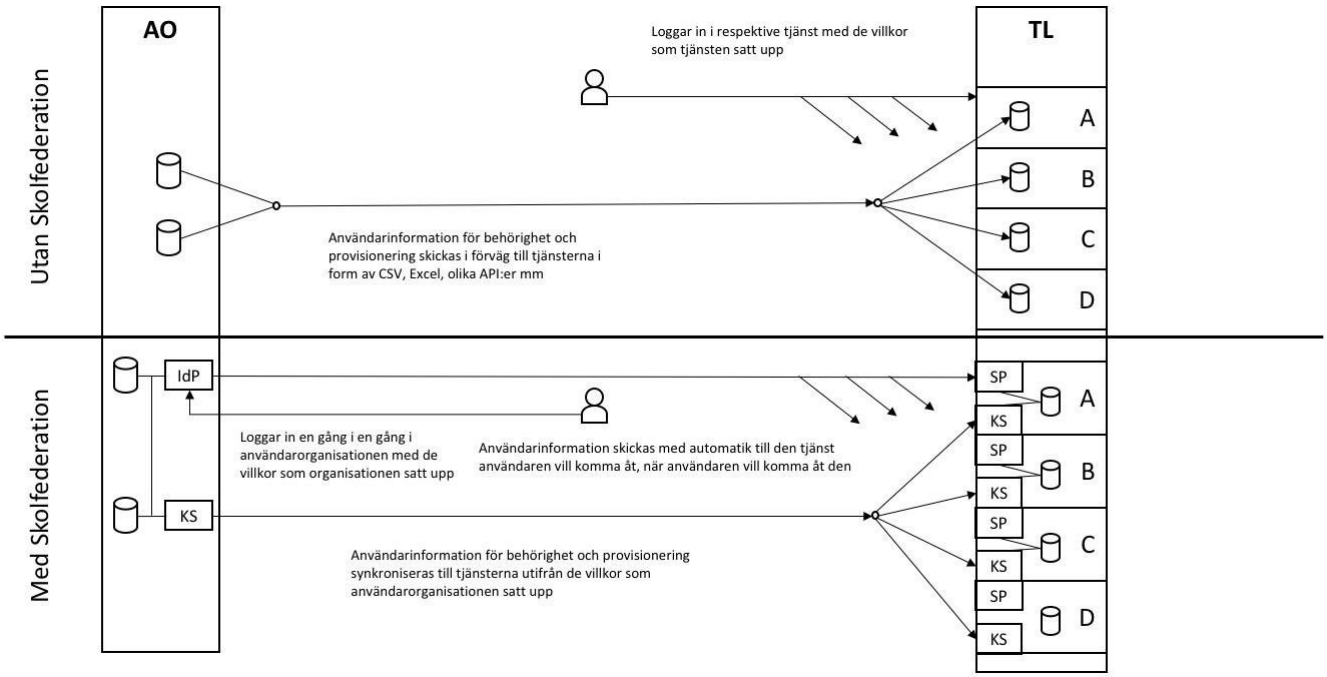

Inledning

Undervisningen i den svenska skolan är på väg in i en digitaliserad värld. För att kunna ta tillvara möjligheterna med digitala tjänster krävs en väl fungerande inloggningslösning för elever och personal. Lösningen måste vara enkel, säker, kostnadseffektiv och lättadministrerad samtidigt som den måste värna om den personliga integriteten.

På grund av att utvecklingen av digitala läromedel gått så fort har tyvärr användningen och distributionen av dessa hamnat på efterkälken. Ju fler digitala läromedel och tjänster som skolorna börjar använda desto mer administration av inloggningar, behörigheter och användare krävs det också av skolan.

Det är här Skolfederation som inloggnings- och provisioneringslösning kan hjälpa till. Skolfederation är ett samarbete mellan skolor och tjänsteleverantörer av digitala tjänster och ger skolorna många bra verktyg och möjligheter att arbeta med inloggning, behörigheter och användare på ett integritetsskyddande och ansvarstagande sätt.

Med Skolfederation använder elever och lärare sin inloggning till skolan för att nå sina tjänster både de inom skolan och externa tjänster. Lärare slipper hantera mängder av konton och lösenord till många tjänster.

Om du precis fått vetskap om Skolfederation eller är ny som medlem inom Skolfederation rekommenderar vi dig att du först lyssnar igenom Skolfederations introduktionskurs för att du ska förstå hur federationen fungerar och du lär dig där de

grundläggande begreppen. I fortsättningen när vi skriver användaren menar vi t.ex. eleven eller läraren som ska använda det digitala läromedlet eller tjänsten hos tjänsteleverantören.

Vi börjar denna information om Skolfederation och integritetsskydd med information om integritetsaspekter och problem som uppstår vid användning av en så kallad traditionell inloggning, alltså inloggning och informationsöverföring utan Skolfederation.

Traditionell inloggning (utan Skolfederation):

En traditionell inloggning innebär ofta att användaren som vill ha tillgång till tjänsten går till tjänsteleverantörens egen webbplats och fyller i användarnamn och lösenord. Vill användaren logga in hos en annan leverantör behöver användaren fylla i användarnamn och lösenord på den andra leverantörens webbplats. Användaren behöver alltså logga in i varje individuell tjänst. Dessutom ska användaren ha ett individuellt lösenord för varje tjänst, det är nämligen inte rekommenderat eller säkert att använda samma lösenord för flera tjänster. Vid användande av Skolfederation behöver användaren bara logga in en gång för att komma åt alla tjänster.

Traditionell inloggning ställer också höga säkerhetskrav på tjänsteleverantören för att den inte ska vara riskabel för användarnas integritet. För att en traditionell inloggning ska fungera behöver tjänsteleverantören ha en databas med användarnamnen och lösenorden uppkopplad mot internet vilket ökar risken för intrång och att dessa uppgifter kommer på villovägar. Det är också tjänsteleverantören som helt sätter villkoren för inloggningen, till exempel vilken information som ska användas för användarnamnet eller vilken teknisk säkerhetsnivå som finns för inloggningen.

För att tjänsteleverantörerna ska veta vilka användare som ska ha tillgång till tjänsterna behöver leverantören få information om användarna och behörigheterna från skolan. Denna information innehåller ofta stora mängder personuppgifter. Denna överföring kan med traditionell inloggning ske på olika sätt, vi har sett många olika exempel, ofta mycket osäkra metoder att skicka dessa personuppgifter på. Informationen kan skickas som excel-ark, via mejl, genom ett API från tjänsteleverantören, webbgränssnitt eller till och med via fysisk post. Varje tjänsteleverantör har ofta en helt egen lösning för behörighetshanteringen. Ur ett integritetsperspektiv är det lätt att förstå att många av dessa sätt inte bra eller att rekommendera.

För skolan innebär också en traditionell inloggning problem med administration av alla användarnas behörigheter hos alla de olika tjänsteleverantörerna. Det kan till exempel handla om att en lärare eller elev slutar på skolan och då inte ska komma åt tjänsterna längre. Då behöver skolan se till att behörigheten stängs av hos alla individuella tjänsteleverantörer. Skolan kan alltså behöva skicka en excel-fil med uppdateringen till en leverantör, hos en annan leverantör behöver de logga in, medan de hos en tredje

behöver skicka uppgifterna i ett mejl. Att personuppgifterna inte hålls uppdaterade och korrekta är då förståeligt men inte acceptabelt enligt Dataskyddsförordningen.

En traditionell inloggning riskerar att bidra till en dålig användarupplevelse, bristfällig säkerhet, onödiga administrativa kostnader och risker för integriteten för användarnas personuppgifter.

Användning av Skolfederation:

Är skolan och tjänsteleverantörerna anslutna till Skolfederation loggar användarna inte in hos tjänsteleverantören, användarna loggar in i sin hemorganisation det vill säga sin skola. Skolan har en användardatabas som innehåller alla elever och lärare som arbetar på skolan. Till den här databasen kopplas en intygsutfärdare, en så kallad IdP, och användaren loggar in i denna.

Skolan kan här skapa en säker inloggning som inte bara behöver bestå av användarnamn och lösenord utan inloggning kan till exempel ske med hjälp av två-faktorsinloggning eller annan, ännu säkrare inloggning. I Skolfederation är det alltså skolan som har kontrollen över inloggningen och sina användares personuppgifter. Till skillnad från en traditionell inloggning där kontrollen över inloggning och hanteringen av personuppgifterna i samband med inloggningen ligger hos tjänsteleverantören.

När användaren loggar in på skolans IdP, skapas ett intyg som sedan kan skickas till den tjänsteleverantör som användaren vill komma åt. Intyget tas emot av tjänsteleverantörens SP (Service Provider). I det här intyget finns det uppgifter om användaren, uppgifterna kallas attribut.

Det som är det fina här är att det är skolan som själv väljer vilken information, alltså vilka attribut, om användaren som ska finnas i intyget. Informationen i intyget kan alltså vara helt anonym för tjänsteleverantören om intyget bara innehåller en pseudonym (t.ex. luerfn#873yniuw) för användaren. Inom Skolfederation kan användarna alltså identifieras med pseudonymer istället för personnummer eller andra personuppgifter och på så sätt förblir användaren anonym för tjänsteleverantören. Eftersom användaren redan är inloggad i skolan verifierar skolan användarens identitet till leverantören.

Olika tjänsteleverantörer ställer dock olika krav på vilka attribut som ska skickas med för att komma åt tjänsten via Skolfederation. Skolfederation rekommenderar att så få attribut som möjligt krävs för att komma åt tjänsten. Vissa tjänster behöver till exempel inte veta mer än att eleven kommer från Skola A, då behöver intyget bara innehålla ett attribut som säger att personen kommer från Skola A.

Det är viktigt att poängtera att inte alla tjänster har rätt till alla attribut utan en minimalistisk princip gäller. Attribut bör därför inte användas utan en noggrann prövning av säkerhet och personuppgiftshantering.

Vi rekommenderar er att tänka igenom om de attribut som tjänsteleverantörerna kräver är nödvändiga eller inte. Om inte, ta gärna upp detta med tjänsteleverantören och se om ni kan minimera de attribut som krävs. Enligt Dataskyddsförordningen ska man alltid minimera antalet personuppgifter som behandlas. Tänk på att det alltid är ni på skolan som är ansvariga för de personuppgifter om lärare och elever som överförs till tjänsteleverantörerna.

Använder sig skolan och tjänsteleverantören av Skolfederations provisioneringslösning för provisionering av konton kan skolan uppnå stora integritetsvinster genom att kunna minimera antalet skickade attribut till ett absolut minimum.

Dataskyddsförordningen, GDPR

Först några viktiga begrepp:

Den registrerade: Den som en personuppgift avser.

Personuppgiftsansvarige: Personuppgiftsansvarig är normalt den juridiska person, till exempel skolhuvudmannen, som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till. Det vill säga den som bestämmer ändamålet med behandlingen.

GDPR är en omfattande och för många komplicerad lagstiftning men en oerhört viktig lagstiftning. All behandling av personuppgifter måste uppfylla de grundläggande principer som anges i GDPR. Det betyder i klarspråk att oavsett vilken typ av personuppgift eller vilken typ av behandling som utförs behöver den personuppgiftsansvarige alltid tänka på och följa principerna nedan.

De grundläggande principerna

a) **Laglighet, korrekthet och öppenhet**: Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

b) **Ändamålsbegränsning**: De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

c) **Uppgiftsminimering**: Personuppgifterna måste vara relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov eller bara för att ”de är bra att ha”.

d) **Lagringsminimering**: Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

e) **Integritet och konfidentialitet**: Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Observera att de grundläggande principerna är just *grundläggande* principer. GDPR innehåller en mängd andra krav som ställs på den personuppgiftsansvarige och som du som personuppgiftsansvarig behöver ha kunskap om och efterleva. Men för att denna informationstext inte ska bli alldeles för lång begränsar vi oss till att prata om hur Skolfederation kan vara ett bra verktyg i ert arbete med GDPR i förhållande till de grundläggande principerna.

Skolfederation och GDPR

Hur kan då Skolfederation vara ett verktyg och underlätta för er i ert arbete med GDPR och för att ni ska kunna värna och respektera era lärare och elevers personliga integritet?

Vi går igenom de grundläggande principerna och ger exempel på fördelar som Skolfederation kan innebära om ni ansluter er och använder tjänsten på ett integritetsskyddande sätt.

Kom ihåg att Skolfederation inte gör att ni per definition efterlever GDPR, utan Skolfederation är ett verktyg som kan underlätta för ert praktiska arbete med efterlevnad. Det är hur ni och tjänsteleverantörerna som medlemmar sätter upp era tekniska lösningar samt till exempel vilka attribut ni faktiskt kräver eller skickar som avgör om ni arbetar på ett integritetsskyddande sätt eller inte.

Laglighet, korrekthet och öppenhet:

- Med Skolfederation är det lättare att hålla personuppgifterna uppdaterade och korrekta. Det är hos skolan som inloggningen sker och skolan väljer vilka uppgifter som skickas till tjänsteleverantörerna. Skolan har då möjlighet att ha större kontroll över personuppgifterna, hålla en bättre ordning på uppgifterna samt hålla dem uppdaterade.
- Med Skolfederations lösning för provisionering behöver skolorna inte längre skicka över listor, Excel-filer eller mejl individuellt till alla tjänsteleverantörer för att hantera konton och behörigheter. Skolan behöver då bara hålla ordning på sitt eget register och ändringar samt uppdateringar av personuppgifterna behöver inte hanteras individuellt för varje tjänsteleverantör.
- Att använda Skolfederation innebär att alla medlemmar i federationen följer en och samma standard vilket skapar öppenhet och förenklar för skolorna att vara transparanta i sin personuppgiftsbehandling. Att leverantören måste ange vilka

attribut som krävs innebär också en ökad transparens och skolan kan då, för att skydda användarnas integritet, välja en leverantör som inte kräver mer än nödvändigt.

Ändamålsbegränsning

- Vid användning av Skolfederation kan skolan lättare se till att behandlingen av personuppgifterna sker inom ramen för det ändamål som de samlades in för. Detta eftersom det är skolan med hjälp av Skolfederation helt är i kontroll över vilka personuppgifter som skickas till vilken tjänsteleverantör i intyget, alltså vilka attribut som tjänsteleverantören får ta del av.
- Det är också viktigt att skolan i sitt avtal och om tillämpligt, personuppgiftsbiträdesavtal med tjänsteleverantören, reglerar vad tjänsteleverantören får göra med de personuppgifter som tjänsteleverantören får del av.

Uppgiftsminimering:

- Vid användande av Skolfederation behöver användaren endast logga in en gång för att komma åt alla tjänster. Detta minskar personuppgiftsbehandlingen väsentligt jämfört med att användaren behöver logga in i varje individuell tjänst den ska använda.
- Skolfederation innebär att skolan på ett enkelt och säkert sätt kan ha kontroll på vilka personuppgifter som skolan lämnar ifrån sig till sina tjänsteleverantörer. Skolan kan på ett enkelt sätt uppgiftsminimera personuppgiftsbehandlingen genom att endast skicka nödvändiga attribut till tjänsteleverantörerna.
- Om båda både skolan och tjänsteleverantören stödjer det kan också en inloggning med hjälp av Skolfederation faktiskt ske utan att tjänsteleverantören får ta del av information som kan identifiera den som loggar in. Tjänsteleverantören får bara ett pseudonymiserat attribut. Skolan kan alltså samla in personuppgifterna för inloggning från eleverna men behöver inte exponera dem för sina tjänsteleverantörer.
- Skolan kan också vid upphandling av leverantörer undersöka vilka attribut som de olika leverantörerna kräver och på så vis minimera personuppgiftsbehandlingen genom att välja en leverantör som kräver få attribut.
- Kom ihåg grundregeln att det inte är tillåtet att samla in personuppgifter bara för att ”de är bra att ha” och det gäller såväl skolan som tjänsteleverantörerna.

Lagringsminimering:

- Personuppgifter får inte heller behandlas längre än vad som är nödvändigt för ändamålet. Personuppgifter som inte längre är nödvändiga för ändamålet ska gallras. Det vanligaste sättet att gallra är att radera personuppgifterna.

- Skolfederation kan underlätta gallring och underlätta lagringsminimering, särskilt vid användning av Skolfederations lösning för provisionering, detta eftersom skolan då själv kontrollerar provisioneringen av konton och behörigheter. Skolan kan centralt i sina register ta bort användare som inte längre ska ha konton eller behörighet hos skolans tjänsteleverantörer.

Integritet och konfidentialitet

- Den som behandlar personuppgifter ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna, detta gäller så klart också vid inloggning i olika tjänster.
- I Skolfederation behöver skolan bara skapa *en* säker inloggning för sina användare på skolan (inloggning i skolans IdP). Det är skolan som själv har kontroll på säkerheten i inloggningen och inloggningen kan då ske med hjälp av till exempel två-faktorsinloggning eller annan, ännu säkrare inloggning.
- Inloggningen på skolan kan sedan användas för att koppla upp sina användare mot alla tjänsteleverantörer inom Skolfederation. Skolorna behöver då inte granska och kvalitetssäkra en mängd olika inloggningsmetoder för olika tjänsteleverantörer.
- Om både tjänsteleverantören och skolan stödjer det i sina tekniska lösningar och i sina implementationer av Skolfederation kan inloggningen ske helt utan exponering av personuppgifter för tjänsteleverantören.
- Med hjälp av Skolfederations provisioneringslösning skickas kontoinformation och behörigheter på ett säkrare sätt. Idag skickas nämligen dessa uppgifter till varje separat tjänsteleverantör med hjälp av till exempel mejl eller excel-filer. Att skicka en mängd listor och dokument på olika sätt till olika leverantörer ökar också risken för att personuppgifterna ska skickas fel eller komma i orätta händer.