Sveriges Kommuner och Landsting

Avdelningen för digitalisering
2016-06-19

Ett fiktivt exempel att använda som diskussionsunderlag

PuL-bedömning av molntjänst i skolan

Detta dokument är ett fiktivt exempel på hur en genomförd PuL[1]-bedömning av en molntjänst för skolorna i en kommun skulle kunna formuleras. Vid varje avsnitt finns en kommentarsruta där bedömningen motiveras. Använd gärna den bifogade tomma mallen för att fylla i de förutsättningar och bedömningar som gäller för just er verksamhet. Kommuner som har egna modeller för PuL-bedömning och för risk- och sårbarhetsanalys kan givetvis använda dem. En PuL-bedömning görs här specifikt, eftersom det inte är helt enkelt när det gäller molntjänster. Utöver den, ska en informationssäkerhetsklassning och risk- och sårbarhetsanalys göras. Även här har SKL tagit fram en mall och ett fiktivt exempel.

I exemplet följer vi företrädare för Skolnämnden i Mittköping och en grupp tjänstemän som genom en workshop besvarar och dokumenterar sin bedömning av frågorna i dokumentet. Deltagare är verksamhetsansvariga chefer för respektive skolområde, grundskola, gymnasiet, vuxenutbildning, osv., it-samordnaren inom skolförvaltningen, kommunjuristen som även är personuppgiftsombud och kommunens IT-chef. När det är dags för riskanalysen tar man hjälp av kommunens beredskapssamordnare som är van vid riskanalyser.

Bakgrundsinformation, fakta och mer vägledning finns i det stöd SKL har tagit fram när det gäller molntjänster i skolan[2].

Viktigt! Materialet ska ses som ett underlag med stödjande exempel för kommuner och huvudmän att göra en egen juridisk bedömning, informationssäkerhetsklassning och ta fram den dokumentation som behövs. Materialet kommer att revideras allt eftersom direktiv kring bland annat kommande Dataskyddsförordning och Privacy Shield tydliggörs. SKL tar gärna emot synpunkter kring innehållet för att kunna hålla det aktuellt och relevant.

[1] Personuppgiftslagen (SFS 1998:204), PuL. Personuppgiftslagen kommer i maj 2018 att ersättas av Dataskyddsförordningen, http://eur-lex.europa.eu/legal content/SV/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=SV

[2] http://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster.96.html

1. Beskrivning av användningen

I detta inledande avsnitt görs en kortfattad sammanfattning av personuppgiftsbehandlingen. Om det behövs för att förklara samband mellan system och integrationer kan man komplettera med skisser och mer detaljerade beskrivningar.

Skolledningen i Mittköping har redan nu valt att avgränsa den typ av information som ska hanteras i molntjänsten. Inga känsliga personuppgifter kommer att hanteras, utan dessa ska istället dokumenteras i skolans interna verksamhetssystem där det finns bättre möjligheter att skydda informationen med it-säkerhetsåtgärder. Skolnämnden har beslutat om instruktioner till samtliga användare så att alla vet vilka avgränsningar som gäller.

Tänk på att om ni i er verksamhet ändå vill kunna behandla känsliga uppgifter om elevers hälsa eller liknande i er molntjänst – då måste riskanalysen nedan kompletteras!

Skolnämnden i Mittköpings kommun kommer att använda DreamClouds molntjänst Make It Happen (MIH) för hantering av den information som genereras inom skolans verksamhet. Skolans verksamhet innefattar förskola, grundskola, gymnasium, vuxenutbildning och särskola.

Elever och personal, anställda under skolnämnden, kommer att få tillgång till MIH-tjänsten, för lagring och redigering av dokument, bilder, film, och annat pedagogiskt arbetsmaterial. Tjänsten används inte för elevadministration, registrering av betyg, utvecklingsplaner, omdömen eller liknande.

Inom ramen för tjänsten, finns funktionerna Talk on Line och Share Your Documents för möjlighet till kommunikation och delning av dokument.

Eleverna får e-postkonto via MIH-tjänsten. Personal använder istället kommunens ordinarie administrativa e-postverktyg.

Förutom ovanstående beskrivning av elevers och lärares e-post och informationslagring kommer skolverksamheten även att ha tillgång till det skoladministrativa systemet ADMIN AB. Grundinformation om elever och medarbetare hämtas från skoladministrativt respektive personaladministrativt system för att skapa elev- och personalkonton i MIH-tjänsten.

För pedagogisk planering kopplad till läroplaner, samt utvecklingsplaner och stödinsatser används it-tjänsten PLANERA AB.

2. Behandling av personuppgifter

I detta avsnitt görs bedömningen av om behandlingen av personuppgifterna i molntjänsten MIH kommer att klara kraven i PuL. Det finns ett antal bedömningssteg i PuL som följs i kapitlet. På www.datainspektionen.se finns en mängd informationsmaterial och stöd för olika delar av bedömningen, särskilt på temasidorna om skolor: http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/skolor/.

2.1 Ändamål med behandlingen

Personuppgifterna kommer endast att behandlas för följande ändamål:

MIH-tjänsten är ett pedagogiskt arbetsverktyg som ska användas för digitalt samarbete i lärsituationen genom samarbeten lärare – elev, lärare – lärare och elev – elev.

Vid all behandling av personuppgifter ska det enligt 9 § PuL finnas ett tydligt definierat ändamål som ska följa med genom hela behandlingsprocessen och styra hur informationen/personuppgifterna får och kan behandlas. När externa leverantörer av molntjänster eller andra it-tjänster anlitas för att genomföra någon del av behandlingen ska ändamålet vara styrande även för dem på så sätt att de inte får tillföra några egna ändamål eller förändra dessa. Personuppgifterna får bara behandlas för de på förhand beslutade ändamålen och endast den personuppgiftsansvarige får besluta om ändring av dessa. Externa parter som behandlar personuppgifter på uppdrag, som t.ex. molntjänsteleverantörer, kallas personuppgiftsbiträden, se mer nedan.

När personuppgifter ska behandlas är det ofta viktigt att informera de registrerade personerna, för skolan även vårdnadshavarna. För att kunna informera på ett bra sätt måste ändamålet vara tydligt definierat.

Här har skolledningen i Mittköping valt en övergripande ändamålsformulering, utan att skriva någon fördjupad beskrivning. Mer information om behandlingen lämnas under följande punkter.

2.2 Typ av uppgifter

Endast personuppgifter om användaridentitet och liknande indirekta personuppgifter kommer att behandlas; elevers och medarbetares namn, klass, skola och liknande. Namn och faktainformation om elevarbeten kommer att förekomma i löpande text.

Strukturerad dokumentation om eleverna, fördjupad information om elevers prestationer och lärares omdömen kommer inte att lagras i tjänsten. Inga känsliga personuppgifter kommer att behandlas. Detta säkerställs genom instruktioner och utbildning av användarna.

Man skiljer mellan okänsliga och känsliga personuppgifter. Läs mer om vad som räknas som känsligt i dokumentet Vägledningen om Molntjänster i skolan[3]

Skolledningen i Mittköping vill göra det enkelt för sig och vill inte ta in känsliga uppgifter i molntjänsten eftersom man är osäker på hur det fungerar med it-säkerhetskrav. Man anser också att det är viktigt att ha en tillgänglig miljö med så mycket information som möjligt öppet. Man tycker heller inte att det finns behov av att dokumentera några direkta elevuppgifter i molntjänsten, då använder man istället sina andra verksamhetssystem, ADMIN AB och PLANERA AB

[3] http://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster.96.html

2.3 Tillåten behandling

Personuppgifter behandlas av skolverksamheten för fullgörande av sina arbetsuppgifter, bland annat för genomförande av pedagogiskt arbete, kommunikation och lagring av pedagogiskt material. Innehållet är av okänslig karaktär. Enligt 10 § punkten d PuL, får detta ske utan individens eller vårdnadshavares samtycke.

Här görs bedömningen av om den planerade behandlingen av personuppgifter är tillåten enligt någon av punkterna i grundbestämmelsen 10 § PuL.

Om man även har behov av att behandla uppgifter som enligt 13 § räknas som känsliga måste man gå vidare och se om det är tillåtet för något av de ändamål som finns i 15-19 §§ PuL. Vägledning finns även i DI:s information riktade till skolor, se referens ovan.

2.4 Information till registrerade

Information om den planerade behandlingen ska lämnas till de registrerade medarbetarna och eleverna. Tydlig information kommer att finnas på intranät och webbplats och informationen kommer att förmedlas till varje elev och dess vårdnadshavare. Medarbetare kommer också få information via e-post.

Enligt 23 och 25 §§ PuL måste den personuppgiftsansvarige självmant se till att alla registrerade personer får information om hur personuppgifterna kommer att behandlas. För elever som går i grundskolan ska även vårdnadshavare informeras. Glöm inte att även informera medarbetare.

2.5 Personuppgiftsbiträde

Vid användning av MIH-tjänsten kommer leverantören DreamCloud att fungera som personuppgiftsbiträde åt Skolnämnden. Mellan parterna kommer ett personuppgiftsbiträdesavtal att upprättas, som en del av standardavtalet för tjänsten. Genom avtalet kommer DreamCloud att ges mandat att anlita underleverantörer för att genomföra personuppgiftsbehandlingen.

Den som på uppdrag behandlar personuppgifter för en personuppgiftsansvarigs (Skolnämnden) räkning kallas i PuL för personuppgiftsbiträde. Det måste enligt 30 § PuL finnas ett särskilt avtal som reglerar hur personuppgifterna får användas.

När standardavtal används kan man ofta inte skriva ett eget separat biträdesavtal utan man måste gå igenom standardavtalet och säkerställa att de villkor som är nödvändiga finns med.

Läs mer om vad som måste ingå i vägledningen.

2.6 Överföra personuppgifter till tredje land

DreamClouds molntjänst innebär att man använder sig av samarbetspartners i USA och lagring av personuppgifter kommer att ske där. Det tillägg som tidigare fanns att teckna, det s.k. Safe Harbor-

avtalet, ogiltigförklarades av EU-domstolen den 6 oktober 2015. De regler som organisationer och företag kunnat ansluta sig till och som EU tidigare bedömt vara ett tillräckligt skydd när det gäller dataöverföring anses nu istället alltså otillräckliga. Det här påverkar mer än användningen av MIH och en förhandling mellan EU och USA har lett till att man tagit fram ett nytt förslag: Privacy Shield.

I avtalen som tecknas med DreamCloud för användandet av molntjänsten, finns utöver Safe Harbor/kommande Privacy Shield, specifika klausuler anpassade för EU:s Dataskyddsdirektiv, s.k. Model Contract Clauses.

Med anledning av domen gör Mittköping, efter samråd med kommunjurist, bedömningen att de ställningstaganden som är gjorda och de avtal som tecknats ändå håller tills vidare, men att bevakning av processen kring Privacy Shield sker aktivt till dess allting är klart och ett nytt ställningstagande eventuellt behövs.

Alla länder inom EU har lagstiftning som motsvarar PuL och som ger de registrerade ett likvärdigt skydd. Personuppgifter får därför behandlas inom EU och EES-området på samma villkor som inom Sveriges gränser. Om personuppgifterna ska överföras utanför detta område kan det variera vilken lagstiftning som finns till skydd för enskildas personliga integritet. För att t.ex. molntjänsteleverantörer ska garantera att samma skydd kan ges som om uppgifterna behandlades internt av Mittköpings kommun, tecknas särskilda avtal. Tidigare fanns möjlighet att teckna ett s.k. Safe Harbor-avtal, men då detta ogiltigförklarades i en dom den 6 oktober 2016, har ett nytt förslag tagits fram: Privacy Shield. Innehåll och principer är vid framtagande av denna skrift inte färdigförhandlade än.

Läs mer i vägledningen.

3. Avtalsvillkor för tjänsten

Efter att man i kapitel 2 har gjort en genomgång av att den planerade personuppgiftsbehandlingen är tillåten är det dags att titta på avtalsvillkoren för den tjänst man har tänkt använda. För vår tjänst MIH gäller standardavtal som är lika för alla kunder och som leverantören DreamCloud inte vill ändra på för enbart Skolnämnden i Mittköping.

Därför måste nu skolledningen titta på villkoren och göra en bedömning av om de här villkoren kommer att stämma med de krav som finns i PuL och det man vill göra. Skolnämnden använder DI:s checklista i ”Molntjänster och personuppgiftslagen”, för att kontrollera att alla delar finns med.

3.1 Standardavtal

Vid användande av MIH-tjänsten finns följande avtal:

- Huvudavtal: ”Education Solution Agreement”
- Tillägg i form av: Model Contract Clauses
- Tillägg i form av: Data processing Amendment

Ta hjälp av leverantören för att vara säker på att rätt avtalsbilagor kommer med. Det ska finnas ett huvudavtal för tjänsten som beskriver övergripande vilken leverans man får.

Dessutom måste det alltid finnas ett personuppgiftsbiträdesavtal som är obligatoriskt. Detta är styrande och innehållet får inte ändras ensidigt av leverantören.

Det brukar också finnas ett ytterligare avtal som gör att leverantören får rätt att behandla personuppgifterna även utanför EU/EES-området, t.ex. i USA. Det som tidigare kallades ett "Safe Harbor-avtal" och som nu ska ersättas av Privacy Shield.

Man kan även använda sig av särskilda Standardkontraktsklausuler som är framtagna inom EU. Läs mer om olika delar av avtal i vägledningen.

Observera att hänvisningar till olika delar och paragrafer i avtalen för DreamCloud enbart är exempel som finns med för att visa hur man bör dokumentera i sin egen bedömning.

3.2 Några viktiga punkter

Skolnämnden kan konstatera att dessa delar uppfylls genom avtalet:

- Leverantören kommer att tillämpa svensk lagstiftning när det gäller personuppgiftsbehandlingen (se paragraf 3.11 i "Education Solutions Agreement")
- Leverantören kommer att vidta lämpliga säkerhetsåtgärder enligt 31 § PuL (se beskrivning i avsnitt 5 i "Education Solutions Agreement")
- Det finns möjligheter till kontroll genom att DreamCloud årligen kommer att tillhandahålla en revisionsrapport av oberoende granskare av tjänsten och av säkerhetsåtgärder. Den personuppgiftsansvarige kommer alltid att kunna ställa frågor om personuppgiftsbehandlingen. (se avsnitt 6 i "Education Solutions Agreement")
- DreamCloud kommer att bistå med information och utredningsunderlag vid utredning av om någon kan ha haft obehörig åtkomst till personuppgifterna. (Se paragraf 6.2 i "Education Solutions Agreement")
- Personuppgifter kommer att överföras till USA och det blir tillåtet genom att DreamCloud tidigare var anslutna till Safe Harbor-principerna och i framtiden kommer ansluta sig till Privacy Shield så fort det är beslutat samt har specifika klausuler anpassade för EU:s Dataskyddsdirektiv (se Model Contract Clauses och Data processing Amendment)

Dessutom ska de områden som beskrivs i avsnitten 3.3-3.5 nedan uppfyllas genom avtalet.

3.3 Ändamål med behandlingen

Varken leverantören eller de underleverantörer som anlitas får behandla personuppgifterna för några andra ändamål än vad som krävs för att leverera MIH-tjänsten eller vad som beskrivs av Skolnämnden. Detta säkerställs genom avsnitt 2 i "Data Processing Amendment".

Det här en extra viktig punkt och här måste Skolnämnden aktivt kontrollera att DreamCloud verkligen inte kommer att behandla personuppgifterna för några ändamål som behövs för deras egen verksamhet eller lämna uppgifterna vidare till affärspartners osv.

3.4 Underleverantörer och kontroll

Personuppgiftsbiträdet kommer att anlita underleverantörer. Av dessa kommer några underleverantörer att ta del av personuppgifter. Den personuppgiftsansvarige kan vid varje givet tillfälle underrätta sig om vilka underleverantörer som för tillfället deltar i behandlingen av personuppgifterna genom att begära att DreamCloud skickar en aktuell lista.

Även detta är en viktig punkt där skolledningen aktivt måste se till att den här rutinen kommer att fungera.

För att inte glömma bort detta ger man skolförvaltningens it-samordnare i uppdrag att varje kvartal begära in vilka underleverantörer som anlitas och bevara dessa rapporter.

3.5 Uppsägning av tjänsten

Vid en uppsägning av tjänsten kommer data och metadata behöva flyttas till annan it-lösning för att viktig information ska kunna bevaras. Personuppgifter eller annan information kommer inte att finnas kvar hos DreamCloud eller dess underleverantörer, utan radering av uppgifter kommer att genomföras i enligt med beskrivningen i ”Education Solutions Agreement”.

För den här punkten kan det vara viktigt att skolledningen gör en bredare bedömning och funderar över hur man kan vilja bevara eller radera/gallra information över en längre tidsperiod.

Skolledningen i Mittköping ber kommunarkivarien om hjälp för den här punkten och de funderar gemensamt över vilken information som ska bevaras och ifall nämndens dokumenthanteringsplan måste uppdateras.