E-samhället i praktiken

PuL-bedömning och riskanalys av molntjänst i skolan

Detta dokument är ett fiktivt exempel på hur en genomförd PuL[1]-bedömning och riskanalys[2] av en molntjänst i en skola skulle kunna formuleras. Vid varje avsnitt finns en kommentarsruta där bedömningen motiveras. Använd 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.

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 referenser återfinns i vägledningen Molntjänster i skolan, Center för eSamhället, SKL, november 2013, nedan kallad ”vägledningen”.

[1] Personuppgiftslagen (SFS 1998:204), PuL
[2] Läs mer om risk- och sårbarhetsanalyser i vägledningen.

Post: 118 82 Stockholm
Besök: Hornsgatan 20
Telefon: 08-452 70 00
www.skl.se

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, IUP, omdömen eller liknande.

Dessutom kommer samtliga användare att få tillgång till tjänsterna 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 SKOLSYS. Grundinformation om elever och medarbetare hämtas från skoladministrativt respektive personaladministrativt system för att skapa elev- och personalkonton i MIH-tjänsten.

För dokumentation av Individuella utvecklingsplaner (IUP) används SKOLSYS.

2. Behandling av personuppgifter

I detta avsnitt görs en bedömningen 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 efterföljande 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 Vägledningen om molntjänster i skolan.

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 tycker heller inte att det finns behov av att dokumentera några direkta elevuppgifter i molntjänsten, då använder man istället sitt vanliga verksamhetssystem, SKOLSYS.

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 DIs 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. Detta kommer att genomföras genom att ett informationsblad delas ut till varje elev och dess vårdnadshavare. Information till medarbetare delas ut via e-post. Information kommer även att finnas på intranät, webbplats och andra kanaler.

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 Personsuppgiftbiträde

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 Överföring av personuppgifter till tredje land

DreamClouds molntjänst innebär att man använder sig av samarbetspartners i USA och lagring av personuppgifter kommer att ske där. Det kommer därför att tecknas ett särskilt tillägg till avtalet som visar att DreamCloud har ett Safe Harbor-avtal.

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. Vid överföring till USA ska det finnas ett Safe Harbor-avtal.

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 DIs 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 Solutions Agreement”
- Tillägg i form av bilaga: Data Protection Addendum
- Tillägg i form av bilaga: Safe Harbor Addendum

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 kallas ett ”Safe Harbor-avtal”. Man kan även använda sig av särskilda Standardkontraktsklausuler som är framtagna inom EU. Läs mer om olika delar av avtal i vägledningen.

Hänvisningar till olika delar och paragrafer i avtalen för DreamCloud är enbart 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 Addendum”)
- 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 har anslutit sig till Safe Harbor-principerna (Se Safe Harbor Addendum).

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 Addendum”.

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 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.

4. Risk- och sårbarhetsanalys

I tabellerna nedan gör skolledningen en bedömning av sannolikhet och konsekvens för ett antal risker som man tycker känns relevanta.

De risker som finns med ska betraktas som exempel på risker som kan vara relevanta när det gäller just användning av molntjänster i skolan med särskilt fokus på personuppgiftsbehandlingen. Använd gärna modellen som stöd för att analysera informationshanteringen i stort med fler verksamhets- eller IT-risker.

Tabellerna ska läsas med färgkoderna där grön färg innebär ”grönt ljus” och rött är stoppsignal och innebär att risken är för stor för att kunna använda tjänsten. Om krysset hamnar på orange måste risken hanteras på något sätt innan man kan gå vidare. Det kan göras genom att undersöka frågan närmare med leverantören eller att vidta åtgärder som t.ex. information eller instruktioner till användarna.

Beskrivning Risk	Elevers arbetsmaterial i skolan går förlorad pga. systemfel				
Konsekvens av det inträffade	Omarbete, förseningar mm. leder till att användare tappar förtroende för tjänsten.				
Konsekvens	Allvarlig				
	Betydande	**x**			
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Analysgruppen bedömer att tjänsten är stabil och tror att det mycket sällan kommer att bli så stora störningar att elevarbeten går förlorade. DreamCloud beskriver i avtalet att det finns back-up-rutiner och att det finns lagring på flera ställen som säkrar att information inte förloras. Det finns möjlighet för kommunen att pröva och säkerställa att dessa rutiner fungerar.

Men man anser ändå att om detta skulle inträffa att elever förlorar sin information, så skulle det ha en betydande påverkan eftersom elever kan förlora elevarbeten och förtroende för tjänsten. Av denna anledning anses det vara en betydande konsekvens om detta skulle inträffa.

Beskrivning risk	Obehörig får del av personuppgifter och arbetsmaterial				
Konsekvens av det inträffade	Oönskad spridning av informationen. Störningar i det pedagogiska arbetet. Osäkerhet när det gäller användares aktivitet om det finns oklarhet i identifieringen. Kan leda till att användare tappar förtroende för tjänsten.				
Konsekvens	Allvarlig				
	Betydande		**X**		
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Om detta skulle inträffa bedömer man att det är relativt illa eftersom det kan sänka förtroendet för tjänsten hos elever och vårdnadshavare och vara svårt att överblicka konsekvenserna. Mot bakgrund av beskrivning av leverantörens interna arbete med säkerhet bedöms risken att detta inträffar som sällan förekommande. Leverantören skall bland annat etablera och upprätthålla en informationssäkerhet som skyddar mot intrång. Denna skall kunna kontrolleras och prövas fortlöpande av kommunen.

Utbildning och instruktioner till användare om t.ex. lösenordshantering kommer också minska sannolikheten för att detta ska inträffa.

Beskrivning risk	Leverantören visar sig inte kunna etablera eller upprätthålla tillräcklig informationssäkerhet				
Konsekvens av det inträffade	Förlust av anseende för kommunen. Krav i lag och/eller förordning kan inte uppfyllas. Kan framtvinga hävning av avtal och/eller byte av leverantör. Risk för informationsförlust.				
Konsekvens	Allvarlig	**X**			
	Betydande				
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Detta skulle kunna ge allvarlig konsekvens eftersom användningen av tjänsten överhuvudtaget skulle ifrågasättas. Om verksamheten oplanerat tvingas byta tjänst kan det ge stor förtroendeskada och avbrott i verksamheten.

Mot bakgrund av leverantörens interna arbete med säkerhet bedöms risken att detta inträffar som mycket sällan förekommande. Leverantörens interna arbete säkerställs genom att DreamCloud är certifierade enligt SS-ISO/IEC 27001 om informations- och IT-säkerhet. Eftersom leverantören därmed har ett antal säkerhetsrutiner i sitt interna arbete ser man detta som ett kvitto på att säkerheten kan godkännas. Det gör det också möjligt för kommunen att själva upprätthålla denna nivå i sin informationshantering.

Eftersom det blir gulmarkering måste man ändå säkerställa ett internt arbete för att följa upp leverantörens granskningsrapporter om säkerhet.

Beskrivning risk	Personal hos leverantör läser elevernas e-post				
Konsekvens av det inträffade	Obehörig får del av information av privat karaktär. Kan leda till att användare tappar förtroende för tjänsten.				
Konsekvens	Allvarlig				
	Betydande				
	Måttlig	**X**			
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Eftersom det främst är frågan om elevernas arbetsmaterial och det inte skulle medföra att information går förlorad, bedömer man att det bara skulle medföra en måttlig konsekvens om detta inträffar. Det är mest en förtroendefråga. Man bedömer att leverantörens skyddsåtgärder är tillräckliga och tror att sannolikheten att det inträffar är mycket sällan.

Beskrivning risk	Leverantören går i konkurs, köps upp av intressent som inte respekterar ingånget avtal eller att tjänsten avvecklas.				
Konsekvens av det inträffade	Kan framtvinga hävande av avtal och/eller byte av leverantör och därmed verksamhetsnyttoförlust och/eller ekonomisk förlust för kommunen. Nedlagt arbete går till spillo, förseningar i produktionen, medarbetar tappar förtroende för sin arbetsmiljö.				
Konsekvens	Allvarlig	**x**			
	Betydande				
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Den här risken är svårbedömd, men om det skulle inträffa kan det bli allvarliga konsekvenser om tjänsten skulle läggas ner eller en ny ägare skulle göra stora ändringar i villkoren. DreamCloud är en stor aktör och det finns ingenting i dagsläget som tyder på att detta skulle inträffa. Det ska finnas back-up av informationen och den ska kunna kontrolleras fortlöpande av kommunen. Sammantaget bedömer man att det inte är stor risk att detta inträffar.

Beskrivning risk	Medarbetares arbetsmaterial i skolan går förlorad pga. systemfel				
Konsekvens av det inträffade	Omarbete, förseningar mm. leder till att användare tappar förtroende för tjänsten.				
Konsekvens	Allvarlig				
	Betydande				
	Måttlig	**x**			
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Konsekvensen bedöms som måttlig eftersom det primärt är frågan om lärares arbetsmaterial och skolan bör kunna genomföra lektioner även utan IT-stöd. Dessutom tror man att det skulle inträffa mycket sällan.

Beskrivning risk	Leverantören förmår inte upprätthålla tillgängligheten av tjänsten				
Konsekvens av det inträffade	Störningar i lärandet, användarna tappar förtroende för sin arbetsmiljö. Ekonomiska konsekvenser vid förlorad arbetstid**.**				
Konsekvens	Allvarlig				
	Betydande	**x**			
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Om det skulle vara vanligt att tjänsten inte fungerar under skoltid skulle detta kunna leda till betydande konsekvenser eftersom lektionstid skulle gå åt till ”datorkrångel”. Eftersom tillgängligheten är reglerad i avtal med leverantören och det finns en tydlig beskrivning från leverantören av hur man upprätthåller hög tillgänglighet, bedömer man att det inträffar mycket sällan.

Beskrivning risk	Virus eller annan fientlig kod kan via tjänsten hota kommunens övriga IT-miljö.				
Konsekvens av det inträffade	Störningar i IT-leveransen. Ekonomiska konsekvenser.				
Konsekvens	Allvarlig				
	Betydande	**x**			
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Här tycker IT-samordnaren att det är svårt att bedöma påverkan som molntjänsten har på kommunens övriga IT-miljö, men om det skulle inträffa skulle det få betydande, eventuellt allvarliga konsekvenser. Eftersom molntjänsten är separat från övrig IT-drift bedömer man ändå att det är mindre sannolikt. Kommunen har ett eget virusskydd och Dreamcloud arbetar också mycket aktivt med att förhindra datorvirus varför risken bedöms som liten.

Beskrivning risk	Information och personuppgifter raderas inte efter att elever har slutat i verksamheten				
Konsekvens av det inträffade	Tjänsterna kan fortsätta användas trots att eleven inte tillhör skolan. Intern information kan spridas till utomstående. Personuppgifter kan bevaras längre än vad som är motiverat från verksamhetens behov.				
Konsekvens	Allvarlig				
	Betydande	x			
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Om detta skulle inträffa skulle det bryta mot kraven i PuL och det finns en risk att elever eller lärare som inte längre är aktuella i verksamheten ändå kan fortsätta använda tjänsterna. Kommunen bestämmer om avslutande av konton och det finns en tydlig beskrivning från leverantören av hur data kommer att raderas och man bedömer det som mindre sannolikt.

Beskrivning risk	Leverantören behandlar personuppgifterna för egna ändamål				
Konsekvens av det inträffade	Kommunen kan anses bryta mot gällande lag. Kan framtvinga hävande av avtal och/eller byte av leverantör och därmed verksamhetsnyttoförlust och/eller ekonomisk förlust för kommunen. Användares brist på förtroende och negativ påverkan på kommunens varumärke.				
Konsekvens	Allvarlig	**x**			
	Betydande				
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Det här är en viktig punkt där nämnden känner stort ansvar. Om det skulle komma fram att leverantören använder information och personuppgifter för egna syften skulle det innebära lagbrott och risk för negativ påverkan för kommunens varumärke. Det skulle motivera att tjänsten sägs upp och det anses som en allvarlig konsekvens. I avtalet tycker man ändå att det tydligt finns beskrivet att det inte är tillåtet och att det inte kommer att ske, så man bedömer risken som mindre sannolik.

Beskrivning risk	Leverantören förändrar innehållet i tjänsten.				
Konsekvens av det inträffade	Avtalet kan behöva förändras för att stämma med ny funktionalitet. Personuppgiftsbehandlingen kan förändras. Kan framtvinga hävande av avtal och/eller byte av leverantör och därmed verksamhetsnyttoförlust.				
Konsekvens	Allvarlig				
	Betydande	**x**			
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Analysgruppen har svårt att bedöma hur sannolikt det är att detta inträffar. Baserat på att man har haft tidigare kontakter med leverantören där man inte har kommit med plötsliga negativa förändringar bedömer man att leverantören kommer att ha god framförhållning även i fortsättningen.

Beskrivning risk	Data och metadata kan inte överföras till annan IT-lösning vid avslutande av tjänsten				
Konsekvens av det inträffade	Information som man vill behålla i verksamheten förloras och man måste börja om från noll varje gång man byter leverantör. Risk för inlåsning till befintlig leverantör.				
Konsekvens	Allvarlig				
	Betydande	x			
	Måttlig				
	Försumbar				
		Mycket sällan	Sällan	Regelbundet	Ofta
		Sannolikhet			

Det finns en tydlig beskrivning av hur data och metadata ska kunna tas ut och flyttas vidare till annat IT-stöd. Man tar även med i bedömningen att den information som finns i tjänsten inte är skolans huvudsakliga dokumentationssystem, utan att det är frågan om arbetsmaterial som ändå kan ha kortare hållbarhet.

5. Slutsats riskanalys

Beskrivning risk	Riskbedömning	Åtgärd	Prioritet
Elevers arbetsmaterial i skolan går förlorat pga. systemfel	Betydande /Mycket sällan	Det skall finnas backup av informationen i tjänsten. Denna skall kunna kontrolleras och prövas fortlöpande av kommunen.	Medel; säkerställ en rutin för kontroll av back-up.
Obehörig får del av personuppgifter och arbetsmaterial.	Betydande /Sällan	Leverantören skall etablera och upprätthålla en informationssäkerhet som skyddar mot intrång. Denna skall kunna	Hög; vad gäller att ta fram instruktioner till användare.

		kontrolleras och prövas fortlöpande av kommunen. Utbildning och instruktioner till användare om t.ex. lösenordshantering.	
Leverantören visar sig inte kunna etablera eller upprätthålla tillräcklig informationssäkerhet.	Allvarlig /Mycket Sällan	Leverantören skall etablera och upprätthålla en informationssäkerhet som kan kontrolleras och prövas fortlöpande av kommunen. Leverantören är certifierad enligt ISO/IEC 27001. Nivån för informationssäkerheten skall göra det möjligt för kommunen att uppfylla motsvarande krav som gäller enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).	Låg
Personal hos leverantören läser elevernas e-post.	Måttlig /Mycket Sällan	Kommunen skall ensamt kunna sätta behörigheter för information i tjänsten.	Medel; undersök behörighets-systemet.
Leverantören går i konkurs, köps upp av intressent som inte respekterar ingånget avtal eller att tjänsten avvecklas.	Allvarlig / Mycket Sällan	Det skall finnas back-up av informationen från tjänsten. Denna skall kunna kontrolleras och prövas fortlöpande av kommunen. Back-up skall kunna användas avkommunen utan leverantörens medverkan eller godkännande.	Medel; säkerställ en rutin för kontroll av back-up.
Medarbetares arbetsmaterial i skolan går förlorad pga. systemfel	Måttlig /Mycket Sällan	Det skall finnas backup av informationen i tjänsten. Denna skall kunna kontrolleras och prövas fortlöpande av kommunen.	Medel; säkerställ en rutin för kontroll av back-up.
Leverantören förmår inte	Allvarlig	Nivån på tillräcklig tillgänglighet	Låg

upprätthålla tillgängligheten på tjänsten.	/Mycket Sällan	skall regleras i avtal. Nivån skall vara konkret och mätbar och konsekvens för leverantören vid återkommande brister.	
Virus eller annan fientlig kod kan via tjänsten hota kommunens övriga IT-miljö.	Allvarlig /Mycket Sällan	Kommunen själv och leverantören har väl etablerade skydd mot virus och fientlig kod. Tjänsten är avskild från kommunens övriga IT-miljö.	Låg
Information och personuppgifter raderas inte efter att elever har slutat i verksamheten	Betydande /Mycket sällan	Avslutande av konton styrs från kommunen. Leverantören garanterar att data raderas i enlighet med instruktioner från kommunen.	Låg
Leverantören behandlar personuppgifterna för egna ändamål	Allvarligt /Mycket sällan	Leverantören garanterar i avtal att personuppgifter endast kommer att behandlas för de ändamål som leverantören har anlitats för.	Medel; säkerställ intern rutin för att undersöka förändringar i tjänsten.
Leverantören förändrar tjänsten.	Betydande / Mycket sällan	Leverantören informerar löpande om förändringar. Kommunen har rutiner för att granska förändringarna och ta ställning till konsekvens. Informationen till användare kan behöva uppdateras.	Låg
Data och metadata kan inte överföras till annan IT-lösning vid avslutande av tjänsten	Betydande / Mycket sällan	Leverantören beskriver i avtalet hur detta ska kunna genomföras.	Låg

6. Sammanfattande bedömning

Endast okänsliga personuppgifter kommer att behandlas i tjänsten. De registrerade kommer att få information och personuppgiftsbiträdesavtal har upprättats. Av detta framgår hur den personuppgiftsansvarige säkerställer sin kontroll över behandlingen och anlitande av underleverantörer.

Riskanalysen utvisar inga risker som motiverar att verksamheten skulle avstå från att använda molntjänsten.

Skolnämnden gör bedömningen att behandlingen av personuppgifter i tjänsten MIH uppfyller de krav som följer av PuL.