Sveriges Kommuner och Landsting

Avdelningen för digitalisering
2016-06-19

Vägledning om molntjänster i skolan

För att en skolnämnd i en kommun ska kunna bedöma om de molntjänster som man vill använda inom skolan stämmer överens med kraven i personuppgiftslagen[1] (PuL), kan denna vägledning användas som stöd vid en intern bedömning.[2] Vägledningen är en del av det stödmaterial[3] SKL tagit fram och konkretiseras genom olika exempel där en fiktiv kommun, Mittköping, bland annat gör en PuL-bedömning och risk- och sårbarhetsanalys. Till materialet finns även kommentarer som visar hur analysen genomförs. Dessutom finns mallar som kan användas för att genomföra en egen bedömning.

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] SFS 1998:204. 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] Fristående skolor som inte drivs i kommunal regi ansvarar självständigt för den personuppgiftsbehandling som sker i verksamheten och att nödvändiga analyser görs. Eftersom samma regler gäller kan dock denna vägledning användas även av dem.

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

1. Bakgrund

Många skolverksamheter vill använda sig av molntjänster[4] som t.ex. Google Apps for Education eller Microsoft Office365, för att på ett enkelt sätt lösa skolans behov av flexibla ytor för lagring av arbetsmaterial och för samarbeten och kommunikation.

Genom att välja en extern leverantör av en molntjänst kommer elever och pedagoger personuppgifter att behandlas av molntjänsteleverantören. Tjänsterna[5] är ofta standardiserade och villkoren för hur information kommer att hanteras av leverantören återfinns i omfattande standardavtal som kan vara svåröverskådliga. Varje verksamhet som vill använda sådana tjänster måste se till att ha klart för sig vilka delar, tillägg osv., som ingår i avtalet.

Det kan även vara svårt att ha full insyn i tjänsternas närmare utformning och funktionalitet och eftersom man har ansvar för vad som händer med personuppgifterna i tjänsten bör man anpassa vilken typ av information man väljer att hantera i standardiserade tjänster. Är det svårt att få överblick eller det inte finns tillräcklig säkerhet i tjänsten, använd den bara för information som inte innehåller personuppgifter och som verksamheten tål att bli av med.

För skolverksamheter som redan använder denna typ av tjänster eller som vill ta fram ett beslutsunderlag, kan denna vägledning fungera som stöd vid en bedömning av om den aktuella molntjänsten följer lagens krav. Eftersom Datainspektionen (DI) aldrig godkänner tjänster eller avtal i förväg måste varje personuppgiftsansvarig nämnd göra en egen, självständig bedömning av om deras användning följer lagen. Även om DI genom sin tillsyn har granskat en tjänst från en viss leverantör och inte haft kritik mot den, finns det i princip alltid saker som avviker när den egna organisationen vill använda samma tjänst. Man ska därför alltid göra en egen analys. Kommande Dataskyddsförordningen kommer att kräva att man kan visa upp att den här typen av analyser är genomförda, så säkerställ också att analysen diarieförs.

Bedömningen ska alltid omfatta:

- En ***laglighetsbedömning***, dvs. om det sätt man vill behandla personuppgifter följer kraven i PuL samt
- En ***risk- och sårbarhetsanalys*** med avseende särskilt på personuppgiftsbehandlingen.

Alla personuppgiftsansvariga måste inför användning av en molntjänst genomföra dessa analyser. Bifogat exempeldokument och mall kan användas som stöd, men tänk på att det är just exempel och att ni gör er bedömning och diskuterar egna exempel.

2. Personuppgiftsansvar

När en kommunal skolnämnd behandlar personuppgifter om medarbetare och elever i ett skoladministrativt system är det tydligt att det är nämnden som är ansvarig för att personuppgiftsbehandlingen sker med berättigade ändamål och att övrig hantering följer lagstiftningen.

---

[4] Molntjänster kan kortfattat beskrivas som tjänster som levereras över Internet, som inte är anpassade för en enskild kund, som inte kräver särskild programvara, som snabbt kan ökas eller minskas och som lagrar kundens information hos molntjänsteleverantören.

[5] Information om molntjänster finns även hos Pensionsmyndigheten som har tagit fram en rapport om molntjänster med en utförlig juridisk analys https://secure.pensionsmyndigheten.se/24304.html

Men även den behandling av personuppgifter som sker vid användning av molntjänster är en del av skolverksamheten. Den nämnd som ansvarar för skolverksamheten ansvarar även för hanteringen i molntjänsterna. Det kan t.ex. vara frågan om lärares pedagogiska material, klass- och grupplistor, dokumentation av elevarbeten, planering och liknande.

Personuppgiftsansvar kan inte delegeras till t.ex. en rektor eller skolledare, utan det är alltid den nämnd som ansvarar för verksamheten som är personuppgiftsansvarig. I det dagliga arbetet genomförs de arbetsuppgifter som följer av personuppgiftsansvaret av de tjänstemän som har olika befattningar och ansvar och agerar för nämnden. Nämnden styr genom beslut och instruktioner, men kan inte besluta om att överflytta ett personligt ansvar för personuppgiftsbehandling till någon tjänsteman.

3. Behandling av personuppgifter

3.1 Ändamål med behandlingen

Vid all behandling av personuppgifter ska det finnas ett tydligt definierat ändamål som ska följa med genom hela behandlingsprocessen och styra hur 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 viktigt att informera de registrerade personerna, inom skolan även vårdnadshavarna. För att kunna informera på ett bra sätt måste ändamålet vara tydligt definierat.

3.2 Typ av uppgifter

Som personuppgift räknas både direkta personuppgifter, som namn och personnummer, men även indirekta uppgifter där man genom kombination med annan information kan få fram individens identitet. Det innebär att även koder, förkortningar och indirekta omnämnanden i löpande text räknas som personuppgifter och omfattas av dessa regler.

I samband med att ändamålet bestäms avgränsas även vilka olika typer av användningsområden och därmed vilka typer av personuppgifter som behandlingen kommer att omfatta.

Vid behandling av personuppgifter skiljer man på ”icke-känsliga” personuppgifter och känsliga eller integritetskänsliga uppgifter.

Inom skolverksamheten är det viktigt att klargöra om behandlingen kommer att omfatta känsliga personuppgifter. Om verksamheten har behov av detta, måste it-lösningen särskilt prövas om den uppfyller de ökade krav på informations- och it-säkerhet som då ställs.

Som känsliga räknas enligt 13 § PuL personuppgifter som avslöjar:

- ras eller etniskt ursprung,

- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- uppgifter som rör hälsa eller sexualliv.

Som *integritetskänsliga* räknas dessutom följande:

- Personuppgifter som rör elevens personliga förhållanden, t.ex. uppgifter som finns i omdömen och utvärderingar om dennes kunskapsmässiga och sociala utveckling,
- Beskrivningar av hemförhållanden,
- Beskrivningar av relationer mellan eleverna.

För båda dessa grupper av känslig information ställs högre krav på säkerhetsåtgärder vid behandlingen, t.ex. i form av kryptering vid kommunikation över Internet och krav på säker identifiering vid åtkomst till informationen, t.ex. bank-id eller liknande.

Inom skolan måste man därför vara medveten om att lärares personliga och summativa omdömen om elever som dokumenteras i it-stöd jämställs med känslig, sekretesskyddad information och kräver att it-system eller andra tjänster kan hantera utvidgade säkerhetskrav.

Typ av information	**Krav:**
”Känslig” information enligt 13 § PuL, t.ex. uppgifter om ras, etniskt ursprung, religion, hälsa, sexualliv samt andra uppgifter i skolan som omfattas av sekretess	Höga säkerhetskrav: - Bank-Id eller annan säker metod för identifiering vid åtkomst till informationen. - Vid kommunikation över öppna nät krävs krypterad förbindelse.
”Integritetskänslig” information, t.ex. vissa summativa omdömen, utvecklingsplaner, stödinsatser	
Personuppgifter som inte omfattas av sekretess eller som är känsligt enligt ovan.	Grundläggande säkerhetskrav, t.ex. enkel inloggning med lösenord, vanlig kommunikation med e-post utan kryptering

En skolverksamhet som vill använda molntjänster använder normalt endast molntjänsterna för icke-känslig information. Det brukar röra sig om begränsade mängder personuppgifter, med information om namn, skola, klasstillhörighet och andra grundläggande fakta för varje elevkonto. Det lagrade innehållet brukar vara begränsat till lärares pedagogiska material och elevers arbeten, kalenderinformation och liknande. Molntjänsterna används för det formativa arbetet, där icke-känslig respons sparas, men också gallras ofta. Som ytterligare stöd i diskussionerna kring vad som är

integritetskänslig information och inte, har SKL tagit fram ett dokument där begrepp reds ut och exempel på olika sorters formuleringar finns[6].

För att säkerställa att tjänsten fortsatt kommer att användas för den typ av information som har bestämts, är det viktigt att kontinuerligt instruera och informera användarna.

3.3 Tillåten behandling

Enligt 10 § punkten d får okänsliga personuppgifter behandlas av skolverksamheten för fullgörande av sina arbetsuppgifter, bland annat för genomförande av pedagogiskt arbete, kommunikation och lagring av pedagogiskt material, utan individens eller vårdnadshavares samtycke.

3.4 Information till registrerade

Den personuppgiftsansvarige ansvarar enligt 23-25 §§ PuL för att självmant lämna information om den planerade behandlingen till de registrerade medarbetarna, elever och vårdnadshavare.

3.5 Risk- och sårbarhetsanalys och informationssäkerhetsklassning

När nya it-system eller tjänster ska börja användas i en verksamhet bör en risk- och sårbarhetsanalys först genomföras för att säkerställa att it-systemet, den it-miljö som systemet ska anslutas till samt andra faktorer håller en tillräckligt god nivå av säkerhet för att kunna hantera informationen. Samma gäller vid anslutning till en molntjänst.

I DI:s informationsskrift om molntjänster och i de tillsynsbeslut gällande molntjänster som har meddelats, finns krav på att den personuppgiftsansvarige ska genomföra en risk- och sårbarhetsanalys. Något som också stärks i kommande Dataskyddsförordning. DI hänvisar i sin informationsskrift även till en modell för riskanalys som är framtagen av EU:s säkerhetsorgan ENISA[7]

Många kommuner har egna modeller för att genomföra risk- och sårbarhetsanalyser. Vägledning för genomförande av risk- och sårbarhetsanalys finns även i Metodstödet för Ledningssystem för Informationssäkerhet (LIS)[8]. Det är det etablerade arbetssättet för Informations- och it-säkerhet som har tagits fram av Myndigheten för Samhällsskydd och Beredskap (MSB) och modellerna följer Svensk standard och ISO-standarder inom området.

I SKL:s stödmaterial för användande av molntjänster[9] finns ett exempel på fiktiv tillämpning av en mall för risk- och sårbarhetsanalys och informationssäkerhetsklassning. Mallen bifogas även som en tom mall som kan användas av den som vill.

4. Personuppgiftsbiträdesavtal

Den som använder sig av en leverantör, ett så kallat personuppgiftsbiträde, för behandling av personuppgifter, ska teckna ett personuppgiftsbiträdesavtal[10] med denna part. Avtalet ska bland

---

[6] http://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster.96.html
[7] Cloud Computing, Information Assurance Framework, samt Security Risk Assessment, November 2009.
[8] https://www.informationssakerhet.se/Metodstod/Metodstodet-riskanalys/
[9] http://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster.96.html
[10] Se 30 § personuppgiftslagen (1998:204), PuL

annat innehålla instruktioner för biträdets personuppgiftsbehandling och vilka säkerhetsåtgärder biträdet ska vidta[11] .

Om personuppgiftsbiträdesavtalet ingår som en del i standardavtalet för molntjänsten måste man säkerställa att de nödvändiga villkoren är urskiljbara från övriga villkor och att de inte kan förändras ensidigt av molntjänsteleverantören. Biträdesavtalet brukar kallas ”Data Processing Agreement” eller ”Data Processing Addendum”.

Ett personuppgiftsbiträdesavtal ska minst behandla följande områden:

- Att personuppgiftsbiträdet är skyldigt att tillämpa svensk lagstiftning när det gäller behandlingen av personuppgifter.
- Att personuppgiftsbiträdet är skyldigt att vidta lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen.
- Att personuppgiftsbiträden endast får behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner och därmed säkerställa att personuppgiftsbiträdet inte behandlar personuppgifter för andra ändamål än dem som personuppgiftsbiträdet anlitats för.
- Att den personuppgiftsansvarige har kännedom om vilka andra personuppgiftsbiträden som kan komma att behandla den personuppgiftsansvariges personuppgifter.
- Att den personuppgiftsansvarige på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och verkligen vidtar lämpliga säkerhetsåtgärder.
- Att det finns tekniska och praktiska förutsättningar att utreda misstankar om att någon hos den personuppgiftsansvarige eller hos något personuppgiftsbiträde haft obehörig åtkomst till personuppgifterna samt säkerställa att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte har åtkomst till personuppgifterna därefter.

4.1 Underbiträden

Personuppgiftsbiträdesavtal upprättas normalt genom att teckna ett separat avtal med varje leverantör som behandlar personuppgifter för den personuppgiftsansvariges räkning. Man kan också ge biträdet mandat att ingå avtal med underbiträden. Om man ger ett sådant mandat måste det framgå i avtalet att varje underbiträde har samma skyldigheter som huvudleverantören av tjänsten, som är kommunens avtalspart.

5. Överföring till tredje land

Enligt PuL räknas det som en överföring av personuppgifter till ”tredje land” att personuppgifter behandlas utanför EU/EES-området. Eftersom molntjänster ofta bygger på att lagringskapacitet används över hela världen blir detta aktuellt.

[11] Av Datainspektionens informationsskrift framgår i detalj vad som måste ingå i ett Personuppgiftsbiträdesavtal, http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/molntjanster/

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.

När personuppgifterna ska överföras utanför detta område kan det variera vilken lagstiftning som finns till skydd för enskildas personliga integritet. För att molntjänstleverantörer ska garantera att samma skydd kan ges som om uppgifterna behandlas inom EU/EES brukar molntjänsteavtal kompletteras med särskilda tillägg.

Om leverantören enbart ska överföra uppgifter till USA fanns tidigare ett s.k. Safe Harbor-avtal. Det innebar att leverantören hade anslutit sig till ett antal skyddsprinciper som EU och USA hade avtalat om. I oktober 2015 ogiltigförklarades avtalet och kommer att ersättas med något som kallas Privacy Shield[12] istället.

Om uppgifter ska överföras till fler länder än så krävs dessutom att leverantören följer EU:s standardkontraktsklausuler ”EU Model Clauses”. Detta ska i så fall finnas med bland de obligatoriska tilläggen till huvudavtalet.

Tabellen nedan beskriver vilka avtal som måste finnas beroende på vilken överföring av uppgifter som kommer att ske.

Anlita personuppgifts-biträde som ska:	**PuL-biträdesavtal behövs**	**Privacy Shield behövs[13] (tidigare Safe Harbor)**	**Standardavtals-klausuler behövs**
Behandla personuppgifterna inom Sverige eller EU/EES	x		
Överföra dem till USA	x	x	
Överföra till resten av världen där leverantören har verksamhet	x		x

[12] Datainspektionen om Privacy Shield: http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/internationell-verksamhet/safe-harbor-domen-far-stora-konsekvenser/

[13] Vid tiden för denna skrivelse är innehållet i Privacy shield med dess olika principer inte färdigställda.