Jämtlands Gymnasieförbund

Granskning av tillämpning av personuppgiftslagen
Revisionsrapport

Advisory
KPMG AB
2014-12-09
Antal sidor: 10

Granskning PUL.docx

Innehåll

1. Sammanfattning

Vi har av revisorerna i Jämtlands gymnasieförbund fått i uppdrag att granska om gymnasieförbundet har förutsättningar att efterleva personuppgiftslagen[1] (PuL). Uppdraget ingår i revisionsplanen för år 2014.

Syftet med granskningen är att bedöma om Jämtlands Gymnasieförbund känner till och efterlever den checklista som SKL tagit fram. Vi har därför granskat om rutinerna främst uppfyller den checklista för skolor som SKL tagit fram som stöd för skolor.

Sammanfattningsvis bedömer vi att rutiner, dokumentation och riktlinjer kring hanteringen av personuppgifter i skolan kan förbättras. Bedömningen är att direktionen inte följer upp förändringar i verksamheten som påverkar PuL på ett tillfredställande sätt. Vi bedömer också att checklistorna används i låg utsträckning och att bättre kännedom ute i verksamheten vore önskvärt. Vidare bedömer vi att det finns inga tydliga rutiner för hur standardavtal ska hanteras och vad som är tillräckligt eller för att säkerställa att rätt villkor uppfylls vid risken att uppgifter överförs till tredje land.

Vi noterar att SKL:s checklista används i vissa fall och viss dokumentation sker i form av förteckningar och personuppgiftsbiträdesavtal men vi bedömer att direktionen inte gjort tillräckligt för att säkerställa sitt ansvar utifrån PuL.

Våra sammanfattade rekommendationer är:

att det alltid bör upprättas biträdesavtal när en externa part får i uppdrag att lagra eller behandla personuppgifter, se punkt 10.

att JGY bör följa upp PuL mer systematiskt. Information om nya system och nya och förfallna förteckningar rekommenderas i samband med delårs- och årsbokslut, se punkt 11.

att JGY bör införa som rutin att använda SKL:s checklista vid införandet av nya IT-system, se punkt 12.

Vi har även lämnat ett antal rekommendationer som är viktiga att beakta om JGY avser att använda sig av s.k. molntjänster med t.ex. extern datalagring, vilket blir allt mer vanligt, se bl.a. avsnitt 10 och 11.

[1] SFS 1998:204

2. Bakgrund

Vi har av revisorerna i Jämtlands gymnasieförbund fått i uppdrag att granska om gymnasieförbundet har förutsättningar att efterleva PuL. Uppdraget ingår i revisionsplanen för år 2014.

Under år 2013 uppmärksammade datainspektionen vid ett antal tillsynsärenden att ett antal skolor i Sverige inte efterlevde PuL. SKL[2] upprättade med anledning av synpunkterna som stöd till skolor en checklista som sammanfattar vad skolorna måste tänka på vid behandling av personuppgifter.

Jämtlands gymnasieförbund använder i likhet med andra skolor IT-stöd för elevadministrationen. Under senare år har nya tekniska lösningar, bl.a. molntjänster, marknadsförts mot skolor. Revisionen bedömer att det finns en *risk* att Jämtlands gymnasieförbund inte efterlever PuL.

3. Syfte

Syftet med granskningen är att bedöma om Jämtlands Gymnasieförbund känner till och efterlever den checklista som SKL tagit fram.

Vi har därför granskat

om rutinerna främst uppfyller den checklista för skolor som SKL tagit fram som stöd för skolor.

4. Avgränsning

Granskningen är översiktlig och avgränsad främst till IT-system och molntjänster.

5. Revisionskriterier

Vi har bedömt om rutinerna/verksamheten uppfyller

- Personuppgiftslagen
- SKL:s skrift "Vägledning om molntjänster i skolan" samt "Mall: PuL-bedömning och riskanalys av molntjänst i skolan".

6. Ansvarig nämnd/styrelse

Granskningen avser Jämtlands gymnasieförbunds direktion

Rapporten är saklighetsgranskad av Mikael Cederberg (förbundschef) och Ingela Carlsson (förbundssekreterare).

[2] Sveriges kommuner och landsting

7. Metod

Granskningen har genomförts genom:

- Dokumentstudie av relevanta dokument
- Intervjuer med berörda tjänstemän och politiker

8. Projektorganisation

Granskningen har genomförts av Kristoffer Bodin, revisorsassistent, under ledning av Lena Medin, certifierad kommunal revisor.

9. Lagar och praxis

9.1 Personuppgiftslagen – PuL

Personuppgiftslagen (PuL) reglerar hur juridiska och fysiska personer (myndigheter, företag, enskilda, m.fl.) får hantera personuppgifter och tar framförallt sikte på databehandling. Lagen bygger på dataskyddsdirektivet (46/95/EG) och har tillkommit i syfte att skydda den personliga integriteten.

Det finns fyra huvudsakliga frågor som bör beaktas:

- om PUL är tillämplig (2-8 §§)

- om behandlingen är tillåten (9-22 §§)

- om den är anmälningspliktig (36-37 §§)

- vilka krav som ställs på behandlingen när den är igång (9, 23-35 och 42 §§).

Det är den personuppgiftsansvarige som ska se till att behandlingen av personuppgifter följer PuL. Den personuppgiftsansvarige är den juridiska person eller myndighet som bestämmer ändamålen och medlen för behandlingen av personuppgifterna. I kommunal verksamhet är det förvaltningsmyndigheten d.v.s. nämnd eller motsvarande som är personuppgiftsansvarig. Hos Jämtlands Gymnasieförbund (fortsättningsvis JGY) är det förbundets direktion som är personuppgiftsansvarig.

Vanligtvis är varje behandling av personuppgifter anmälningspliktig till tillsynsmyndigheten, i det här fallet Datainspektionen. Om den personuppgiftsansvarige har utsett ett personuppgiftsombud (PUO) och anmält detta till Datainspektionen behövs dock inte en sådan anmälan göras. PUO har ansvar att se till att lagar och regler följs och att föra förteckning över de behandlingar av personuppgifter som genomförs. JGY har utsett ett PUO som är anmält till Datainspektionen.

Den personuppgiftsansvarige kan välja att låta någon annan behandla personuppgifterna enligt givna instruktioner. Det skall finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av

personuppgifter för den personuppgiftsansvariges räkning. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldig att vidta de åtgärder som avses i 31 § första stycket, d.v.s. att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda personuppgifterna.

9.2 Datainspektionen

Datainspektionen är tillsynsmyndighet för behandling av personuppgifter och kan genomföra inspektioner för att säkerställa detta. Efter att tillsyn är genomförd skrivs ett protokoll och ärendet kan avslutas utan anmärkning eller så kan tillsynsobjektet få åläggande att inom en viss tid åtgärda uppdagade brister. Är bristerna allvarliga kan Datainspektionen utfärda ett vitesföreläggande.

Datainspektionen riktade 2011 kritik mot en kommun för att avtalet med en molntjänst inte uppfyllde villkoren i PuL, något som blev överklagat men som Förvaltningsrätten fastställde 2013. Datainspektionen har en checklista, "Checklista för skolor", som översiktligt tar upp punkter som är viktiga att känna till för skolor som använder IT-stöd. Datainspektionen har också gett ut en skrift i förebyggande syfte som heter "Personuppgiftslagen och molntjänster i skolan".

9.3 Sveriges kommuner och landsting – SKL

SKL är en arbetsgivar- och intresseorganisation för alla kommuner, landsting och regioner i Sverige. SKL:s uppgift är att stödja och bidra till att utveckla medlemmarnas verksamhet. SKL tar ofta fram vägledningar för kommuner och landsting inom olika aktuella områden.

SKL har gett ut skriften "Vägledning om molntjänster i skolan" för att stötta nämnder i bedömningen om molntjänster som ska implementeras i verksamheten stämmer överens med kraven i PuL. Skriften tar bl.a. upp ansvar, behandling av personuppgifter, riskanalys, personuppgiftsbiträdesavtal, överföring till tredje land. Till skriften finns också en mall "PuL-bedömning och riskanalys av molntjänst i skolan". I den mallen finns alla punkter nämnden behöver stämma av inför bedömningen och även en mall för en risk- och sårbarhetsanalys.

10. IT-system och tjänster

JGY använder idag e-postsystemet First Class för kommunikation och målet är att byta ut detta system mot en molntjänst eller ett vanligt nyare e-postsystem. För närvaro och dokumentation används ett system som heter Dexter. Servrarna för First Class står hos Regionförbundet och servrarna för Dexter hos en leverantör i Växjö. Enligt uppgift finns det inget personuppgiftsbiträdesavtal (biträdesavtal) mellan JGY och Regionförbundet eller leverantören i Växjö. Andra system som hanterar personuppgifter med externa parter inblandade är bland annat passeringssystemet till lokalerna, register för busskort, elevregistreringssystemet Extens och elevenkäter.

Då känslig information registreras i Dexters omdömesmodul ställs krav på IT-säkerheten, nivån på säkerheten bestämmer nivån på informationens känslighet. För vanliga användarkonton i Dexter är det en relativt låg nivå på säkerhetslösningen med ett enkelt inlogg med användar-ID och lösenord.

Det innebär att det hanteras inte känsliga personuppgifter i det systemet. Det finns inget fritextfält i frånvaroanmälan och begreppet "sjuk" används inte som frånvaroorsak. I omdömesmodulen registreras däremot elevens nuvarande nivå och framåtsyftande åtgärder vilket räknas som känsliga uppgifter. När modulen infördes utbildades personalen och det finns riktlinjer för utvecklingssamtal i Dexter[3]. I riktlinjerna finns utdrag ur Datainspektionens "Checklistor för skolor", en arbetsgång samt exempel på omdömen. Dexter är kopplat till olika roller. En lärare ser bara elever kopplade till sin roll. Elever och föräldrar ser bara sig själva medan administratör och rektor ser alla inom enheten. Behörigheten delas ut av personaladministratörerna utifrån befattning. Gamla konton ska administratörerna gallra bort. Behörigheten för elever och vårdnadshavare hanteras av elevadministratörerna.

Många skolor vill använda sig av molntjänster för att enkelt lösa behovet av e-post, lagring av arbetsmaterial med mera. JGY använder vid tidpunkten för granskningen ingen molntjänst men olika alternativ har eller ska utvärderas. Google Apps eller Google Apps For Education som verktyget heter är ett plattformsoberoende, kommunikations- och samarbetsverktyg. Denna molntjänst har utvärderats av en arbetsgrupp tillsammans med övriga kommuner i Jämtland genom Regionförbundet Jämtlands län. Från JGY deltog IT-samordnaren i arbetsgruppen. Syftet med att använda verktyget är för att tillgängliggöra undervisningsmaterial och omvärldsinformation genom delning av material mellan elev och lärare samt att öka det digitala lärandet och kompetensen. Enligt uppgift kommer elever och lärare få ett e-postkonto enbart för det digitala lärandet. Lärarna kommer i övrigt att använda det lokala e-postsystemet. Inga känsliga uppgifter som frånvaro, betyg och individuella omdömen kommer enligt uppgift att registreras i Google Apps. Arbetsgruppens bedömning blev att Googles standardavtal uppfyllde villkoren i PuL samt att risk- och sårbarhetsanalysen som gjordes utifrån SKL:s mall visade på låga risker.

Bedömningen blev vidare att Google Apps kunde införas men att det var upp till varje huvudman att själv bestämma om tjänsten skulle införskaffas eller inte. JGY valde att inte införskaffa Google Apps då JGYs representant i arbetsgruppen inte delade gruppens bedömning av riskerna. IT-samordnaren såg det betydligt mer sannolikt att känsliga uppgifter registreras av misstag än arbetsgruppen. Det ledde till att direktionen aldrig fattade beslut i frågan utan istället ska Microsofts molntjänst Office 365 utvärderas. Det skulle kunna ge en helhetslösning för e-post och delning av material utan att det behövs två system, en molntjänst och ett lokalt e-postsystem. Då JGY inte vill registrera alltför känsliga uppgifter i en molntjänst utvärderas även en teknisk lösning där information kan lagras på egna servrar om informationen bedöms vara för känslig för att läggas ut på externa servrar.

Kommentar

Vi noterar att JGY har servrar och databaser utlokaliserade hos externa parter där det saknas biträdesavtal. Vår bedömning är att det alltid bör upprättas biträdesavtal när en externa part får i uppdrag att lagra eller behandla personuppgifter.

Vi noterar att JGY gjorde en annan riskbedömning av Google Apps än Regionförbundet och att JGY såg att det finns en betydande risk att känsliga uppgifter registreras av misstag i systemet.

[3] Fastställt 2012-10-10.

Vi noterar också att JGY är ute efter en molntjänst med en e-postlösning för att undvika två system. Då skillnaden mellan de två molntjänsternas e-posttjänster bedöms vara små är det viktigt att kritiken mot Google Apps beaktas i utvärderingen av Office 365. Om elever ska få ett e-postkonto måste det finnas tydliga riktlinjer för vilka uppgifter som får skickas till vem. Som exempel skulle kommunikation mellan personal kunna kallas intern och all övrig kommunikation för extern och sedan upprättar man riktlinjer för intern respektive extern kommunikation. Även risken för felaktig delning av dokument bör vara relativt lika i båda molntjänsterna vilket innebär att oavsett molntjänst har direktionen ett ansvar att den information som tillåts registreras i de olika verktygen regleras och att kraven på användarna tydliggörs.

Vidare bedömer vi det som viktigt med en systematisk uppföljning av användandet genom stickprov från dataloggar, utdelat material till elever eller liknande.

Vi rekommenderar:

att det alltid bör upprättas biträdesavtal när en externa part får i uppdrag att lagra eller behandla personuppgifter.

att om JGY inför en molntjänst bör riktlinjer utarbetas som tydligör krav och ansvar utifrån PuL vid handhavandet av molntjänstens verktyg.

11. Rutiner och ansvar kring PuL

JGYs PUO, Ingela Carlsson, har bland annat ansvar för att se till att det finns förteckningar över behandlingen av personuppgifter. Det finns förteckningar över en rad system och aktiviteter där behandlingen av uppgifter som kan vara känsliga utifrån Pul framgår. PUO uppger att det bör finnas förteckningar över alla system men att det kan saknas föteckningar över de äldsta systemen. Detta åtgärdas allt eftersom hon får kännedom om dem. Det finns inga allmänna skriftliga rutiner om PuL t.ex. vad som ska göras vid införandet av ett nytt system. Däremot finns det instruktioner för vad som får och inte får skrivas i specifika system.

Direktionen får sporadiskt information om arbetet med PuL. Vid införandet av nya större system får direktionen en dragning av ansvarig tjänsteman. Enligt uppgift har det förekommit en dragning om PuL och molntjänster men PuL tas inte upp rutinmässigt. Nya förteckningar föredras eller delges inte direktionen. Ordförande skriver under biträdesavtalet men i övrigt informeras inte direktionen. PUO planerar att ordna utbildning i PUL för nya direktionen efter årskiftet och för personalen.

Enligt SKL bör en risk- och sårbarhetsanalys genomföras vid införandet av en ny tjänst. En sådan analys gjordes vid utvärderingen av Google Apps och kommer göras vid utvärdering av Microsoft Office 365. Enligt uppgift görs det inte en risk- och särbarhetsanalys för alla system utan bara när det är större system som ska införskaffas. Dessutom är SKL:s och Datainspektionens skrifter enligt uppgift relativt okända ute i verksamheten. IT-samordnaren och PUO har använt SKL:s skrift praktiskt men har enligt de själva begränsad kännedom om Datainspektionens checklista.

Kommentar

Vi bedömer att förteckningar är ett systematiskt sätt att dokumentera hur personuppgifter behandlas. Det är viktigt att förteckningar uppdateras löpande för alla system och att direktionen har kännedom om dessa. Bedömningen är därför att direktionen inte följer upp förändringar i verksamheten som påverkar PuL på ett tillfredställande sätt. Direktionen borde åtminstone delges nya, ändrade och förfallna förteckningar eller på annat sätt systematiskt få informationen till sig.

Vi bedömer också att checklistorna används i låg utsträckning och att bättre kännedom ute i verksamheten vore önskvärt. Checklistorna är till för att fungera som stöd till personer som hanterar personuppgifter och då bör checklistorna vara kända ute i verksamheten.

Vi rekommenderar:

att JGY bör följa upp PuL mer systematiskt. Information om nya system och nya och förfallna förteckningar rekommenderas i samband med delårs- och årsbokslut.

att JGY bör genomföra en utbildning om PuL i samband med molntjänster samt att checklistorna implementeras i verksamheterna.

12. Avtal

Biträdesavtal tecknas alltid vid införandet av nya system medan det för äldre system inte alltid finns avtal upprättade. Om det finns standardavtal kollas dessa igenom först för att säkerställa att villkoren uppfyller PuL. I de flesta fall när nya system ska införas utformas ett separat biträdesavtal som reglerar ansvaret för att PuL följs av leverantören. IT-samordnaren har inte stött på så många standardavtal än.

Leverantörer av molntjänster kan ibland ha servrar utomlands och det ställs speciella krav på avtalet beroende på i vilket land servrarna finns. Vid utvärderingen av Google Apps framkom att deras servrar fanns i tredje land. Detta reglerades dock i Googles standardavtal där det angavs att Google hade ett Safe Harbor-avtal, vilket krävs enligt SKL:s skrift om servrarna finns i USA. Microsoft har uppgett att deras servrar finns på Irland men utvärderingen kring Office 365 har inte kommit igång än.

Kommentar

Vi bedömer att det finns inga tydliga rutiner för hur standardavtal ska hanteras och vad som är tillräckligt. Enligt SKL kan standardavtal mycket väl gå att använda under förutsättning att nödvändiga villkor framgår tydligt.

Vidare bedömer vi att det inte finns tillräckliga rutiner för att säkerställa att rätt villkor uppfylls vid risken att uppgifter överförs till tredje land. I SKL:s checklista redogörs för vad som gäller när uppgifter överförs till tredje land och vilka avtal som behövs.

Vi rekommenderar:

att JGY bör införa som rutin att använda SKL:s checklista vid införandet av nya IT-system.

KPMG, dag som ovan

Kristoffer Bodin
Revisorsassistent

Lena Medin
Certifierad kommunal revisor