Deloitte.

Rapport Hantering av personuppgifter och personuppgiftsansvar.

Östersunds Kommun

Augusti 2013

Marianne Harr
certifierad kommunal revisor

Veronica Blank
revisor

Innehåll

Sammanfattning 1
Inledning 1
Rutinbeskrivning 4
Granskningsresultat 8

Sammanfattning

Personuppgifter som behandlas inom kommunen behöver hanteras och skyddas enligt de bestämmelser som finns inom området. Om det brister i rutiner kring behandling av personuppgifter finns risken att den enskildes integritet kränks och det kan dessutom leda till både skadestånd och böter eller fängelse för den som är personuppgiftsansvarig.

I kommunen är normalt både kommunstyrelsen och nämnderna-om de är så självständiga att de är förvaltningsmyndigheter – personuppgiftsansvariga, var och en för sin verksamhet. På uppdrag av de förtroendevalda revisorerna har Deloitte utfört en granskning av rutinerna för hantering av personuppgiftsansvar.

Den övergripande revisionsfrågan är om rutiner för hantering av personuppgiftsansvar är tillräckliga för att säkerställa den interna kontrollen?

Efter genomförd granskning är vår bedömning är att de rutiner som finns för hantering av personuppgifter inte är tillräckliga för att säkerställa den interna kontrollen. Det genomförs ingen regelmässig uppföljning och kontroll av hur personuppgifter hanteras och det behövs utbildning och information.

Det finns en arbetsfördelning för behandling av personuppgifter som ska klargöra vilket ansvar som finns och hur det kan fördelas på olika nivåer. Den är reviderad under 2012 och omfattar nu även fördelning till områdes- enhetschefer. I vissa fall har den ansvarsfördelningen inte behandlats i nämnden sedan år 2006. Respektive nämnd bör se till att uppdaterade och underskrivna arbetsfördelningar finns.

För att förankra reglerna på området är det viktigt att det hålls regelbundna utbildningar och ges löpande information. Det är viktigt att komma ihåg är att det är varje nämnd eller styrelse för sig som är personuppgiftsansvariga. Rutiner kan med fördel upprättas gemensamt men det är de ansvariga nämnderna som måste se till att riktlinjer och rutiner antas samt att en regelbunden kontroll av efterlevnaden genomförs.

Efter genomförd granskning rekommenderar vi följande:

- ✓ Regler och riktlinjer bör antas av respektive nämnd/styrelse. För att stärka kontrollen vid förvaltningarna rekommenderar vi att ansvar fördelas ut även till områdes- och enhetschefer,vilka har kännedom om de personuppgifter som behandlas ute i verksamheterna.

- ✓ Det bör upprättas en rutin för kontroll av att personuppgiftsansvaret hanteras enligt lag. En sådan rutin kan upprättas gemensamt men varje nämnd/styrelse måste anta rutiner och ansvarar för att kontrollera efterlevnaden. En sådan rutin kan exempelvis ingå i det årliga arbetet med intern kontroll.

- ✓ Avtal måste tecknas med alla parter som hanterar personuppgifter för nämndernas/styrelsernas räkning. Det gäller externa parter, men avtal behöver också

upprättas mellan nämnderna och det nya kundcentret, som kommer att hantera personuppgifter på nämndernas begäran.

- ✓ Varje nämnd/styrelse bör tillse att det genomförs utbildningar inom nämndens verksamhetsområde. Att informera om reglerna kring PuL bör ocks regelmässigt göras när en person nyanställs.

- ✓ För att det ska vara möjligt att få en överblick över var personuppgifter behandlas bör det regelbundet göras en inventering av vilka behandlingar som görs inom nämndens verksamhetsområde. En behandling kan exempelvis ske genom system, molntjänster eller socialt medium.

1. Inledning

1.1 Uppdrag och bakgrund

Personuppgifter som behandlas inom kommunen behöver hanteras och skyddas enligt de bestämmelser som finns inom området. I kommunen är normalt både kommunstyrelsen och nämnderna-om de är så självständiga att de är förvaltningsmyndigheter – personuppgiftsansvariga, var och en för sin verksamhet.

1.2 Revisionsfråga

Den övergripande revisionsfrågan är:

Är rutiner för hantering av personuppgiftsansvar tillräckliga för att säkerställa den interna kontrollen?

Granskningen ska besvara följande kontrollmål:
Vilka riktlinjer finns för personuppgiftsansvaret?

Är riktlinjer och rutiner kända och hur kontrolleras efterlevnaden?

1.3 Revisionskriterier

Bestämmelser enligt personuppgiftslagen, datainspektionens faktablad och informationsskrifter samt kommunens interna riktlinjer.

1.4 Avgränsning

Granskningen avser 2013.

1.5 Metod

Dokumentstudier av riktlinjer och styrdokument. Intervjuer med personuppgiftsombud och ansvariga för informationshantering.

2. Rutinbeskrivning

2.1 Bestämmelser kring behandling av personuppgifter

Personuppgiftslagen (PuL 1998:204) trädde i kraft år 1998 och har till syfte att skydda människor mot att deras integritet kränks när personuppgifter behandlas. Datainspektionen är tillsynsansvarig för personuppgiftshantering och ger ut riktlinjer och information på området. Nedan en definition av de roller som finns gällande personuppgiftsansvaret:

Personuppgiftsansvarig
"Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter"(3§, PuL).
Det är den juridiska personen eller myndigheten som behandlar personuppgifter som är ansvarig. I undantagsfall kan en fysisk person vara personuppgiftsansvarig så som enskilda näringsidkare.

I en **kommun** är normalt både kommunstyrelsen och de kommunala nämnderna om de är så självständiga att de är förvaltningsmyndigheter – personuppgiftsansvariga, var och en i sin verksamhet. Vilket organ i kommunen som är personuppgiftsansvarig kan variera; de faktiska omständigheterna måste prövas i varje enskilt fall, till exempel om nämnden självständigt förfogar över de personuppgifter som behandlas (Datainspektionen).

Personuppgiftsombud
Normalt måste en personuppgiftsansvarig, dvs. en nämnd eller styrelse anmäla all behandling av personuppgifter till datainspektionen.(36 §,PuL). Om ett personuppgiftsombud utses behöver inte en sådan anmälan ske. Det ska då istället anmälas vem som utsetts till personuppgiftsombud. Ett personuppgiftsombud är ofta en anställd som har ansvar inför den personuppgiftsansvarige för att personuppgifter behandlas på rätt sätt och enligt lag inom verksamheten. Personuppgiftsombudet ansvarar för att självständigt se till att personuppgifter behandlas på ett korrekt sätt och enligt god sed. Eventuella brister ska påpekas till den personuppgiftsansvarige.

Om personuppgiftsombudet misstänker att den personuppgiftsansvarige bryter mot de bestämmelser som finns och den inte åtgärdar bristerna så ska det anmälas till datainspektionen (38 §, PuL).

Personuppgiftsbiträde
Ett personuppgiftsbiträde är alltid en extern part som anlitas av en personuppgiftsansvarig (i kommunens fall en nämnd eller styrelse) för behandling av personuppgifter. Leverantörer av så kallade "molntjänster" är att betrakta som personuppgiftsbiträden. Molntjänster innebär att man, istället för att installera program lokalt på en server eller dator, köper en tjänst som är internetbaserad. Det kan gälla en lagringsplats, ett program osv. Exempel på molntjänst är webmail eller löneprogram.

Utöver personuppgiftslagen regleras en del av kommunens verksamhet i patientdatalagen. Regleringen i denna lag kompletterar PuL och avser behandling av personuppgifter inom

hälso-och sjukvård. Personuppgiftsansvarig enligt patientdatalagen är den kommun eller landsting som ansvarar för vården.

Den som fått sina personuppgifter lagrade har rätt att vid förfrågan få reda på vilka uppgifter som lagrats. Dessutom ska information ges i förväg om att uppgifterna kommer att behandlas.

2.2 Typer av personuppgifter som behandlas i kommunen

I kommunen behandlas personuppgifter vid alla förvaltningar. Både anställdas personuppgifter och medborgarnas personuppgifter behandlas.

Personuppgifter som behandlas är exempelvis namn, personnummer, adressuppgifter, bilder och familjeförhållanden. För de anställda sker behandling av personuppgifter genom lönehantering, pensionslistor, medarbetarsamtal, passersystem m.m. För medborgarna lagras personuppgifter när medborgaren gör en ansökan, genom uppgifter i skolan, när de får vård m.m.

Under hösten 2013 kommer ett nytt kundcenter att startas upp i kommunen. Ett syfte med det nya kundcentret är att medborgarna ska få en bättre service genom att kundcentret till exempel ska kunna ta emot ansökningar och hantera enklare ärenden som tidigare hanterats ute på förvaltningarna. I och med att det nya kundcentret tas i drift kommer en del av behandlingen av personuppgifter att läggas ut från nämnderna/styrelserna, där de tidigare behandlats, till personalen på kundcentret.

2.3 Riktlinjer i kommunen

Regler för hantering av personuppgifter har tagits fram år 2005 och har reviderats under år 2012. I de nya reglerna omfattas även områdeschefer/enhetschefer etc. Under 2013 har också riktlinjer för mobila tjänster och sociala medier tagits fram. Dessa är under uppdatering.

Regler för hantering av personuppgifter och fördelning av ansvar för behandling av personuppgifter

I reglerna definieras personuppgiftsansvarig och vilken uppgift denna har och det klargörs att ansvarig ska teckna avtal med personuppgiftsbiträden.

Varje personuppgiftsombud ska skriva på ett avtal där det framgår vilka arbetsuppgifter som ingår i uppdraget. Det är bland annat:

- Vara väl insatt i lagen och rättigheter och skyldigheter.
- Hålla sig underrättad om utvecklingen av lagstiftningen.
- Hålla en aktuell förteckning över de behandlingar av personuppgifter som sker inom den personuppgiftsansvariges ansvarsområden
- Utarbeta rutiner för förteckningsskyldigheten
- Kontrollera att lämpliga tekniska och organisatoriska åtgärder vidtagits för att skydda behandlade personuppgifter
- Bedriva rådgivning till ledning och personal
- Anmäla till datainspektionen om åtgärder inte vidtagits för behandlingar som står i strid mot lagen.

I riktlinjer finns också regler för förvaltningschef vilken ska:

- Organisera behandlingen av personuppgifter inom förvaltningen och ansvara för ledning och kontroll.
- Med hjälp av personuppgiftsombudet bedöma om personuppgiftshandling som man vill överlåta till en molntjänstleverantör är tillåten.
- Teckna avtal med personuppgiftsbiträde om behandling för nämndens räkning.

Även områdes/avdelnings/enhetschef omfattas av ett avtal.

Personuppgiftsansvarig ska reglera förhållandet mellan sig och personuppgiftsbiträden genom ett avtal. Exempelvis är det enligt kommunstyrelsens delegationsbestämmelser kommundirektören den som ansvarar för att sådana avtal upprättas gällande kommunstyrelsens verksamhetsområde.

Riktlinjer för sociala medier och mobila applikationer

Riktlinjerna har beslutats av kommundirektören och reviderades senast 2012-11-30. De berör exempelvis definitioner, juridisk information, bemötande och arkivering. Det finns också ett särskilt avsnitt om behandling av uppgifter enligt personuppgiftslagen och vad som gäller för exempelvis chattar eller insändarfunktion.

2.3 Organisation för behandling av personuppgifter i kommunen

Personuppgiftsombud

I kommunen är varje nämnd/styrelse personuppgiftsansvarig. Varje nämnd/styrelse har utsett ett personuppgiftsombud. Några nämnder har samma ombud.

Avtal med personuppgiftsbiträden

Kommunen använder sig av flertalet tjänster där en annan part hanterar uppgifter för kommunens räkning. Personuppgiftsbiträdet är alltid en extern part och enligt personuppgiftslagen ska ett avtal finnas med de som hanterar personuppgifter för kommunens räkning. I kommunstyrelsens delegationsordning anges att kommundirektör är delegat för att teckna avtal med personuppgiftsbiträden, exempelvis när det gäller molntjänster.

Personuppgiftsombudets uppföljning och kontroller av efterlevnad

Personuppgiftsombuden i de olika nämnderna har enligt uppgift begärt att få in förteckningar från verksamheten över vilka uppgifter som behandlas. De förteckningar som inkommer sparas i en pärm hos personuppgiftsombudet.

Personuppgiftsombudet för kommunstyrelsen har tillsammans med kommunledningens IT-strateg tagit fram utbildningsmaterial för att öka förståelsen kring hantering av ansvaret.

Någon skriftlig rutin för kontroller av att personuppgifter hanteras på rätt sätt finns inte i kommunen. Enligt uppgift har personuppgiftsombud tidigare träffat exempelvis enhetschefer två gången årligen och då gjort en förfrågan om det tillkommit några system

och någon hantering av personuppgifter. I övrigt har ombuden förlitat sig på att uppdateringar av förteckningar inkommer till ombudet.

.

Iakttagelser från intervjuer och stickprov

Synpunkter från intervjuer

Nedan några åsikter som framkommit vid intervjuer med personuppgiftsombud:

- Svårt område att greppa och förstå, och det gäller både för oss och ansvariga för verksamheterna.

- De här frågorna prioriteras inte, det finns så mycket annat att göra.

- Önskar ha regelbundna träffar med de andra ombuden.

- Många kanske tycker att det är ok att skriva på ett papper men när de sedan arbetar så är det inte lika självklart att de tänker på när personuppgifter behandlas och vad det får för konsekvenser.

Stickprov hantering personuppgifter

För att få en bild av hur rutiner för personuppgiftsansvaret fungerar i praktiken har vi sänt ut en förfrågan till nämnder i kommunen. Förfrågan har sänts till förvaltningschefer och personuppgiftsombud.

I granskningen har vi efterfrågat uppgifter om vilka personuppgifter som behandlas, förteckningar över hanteringen samt de avtal som finns med personuppgiftsbiträden (som hanterar personuppgifter för nämndens räkning).

Resultatet från förfrågan visar att det vid flera nämnder saknas avtal med parter som är personuppgiftsbiträden. Avtal finns, men inte med samtliga biträden. Under granskningens gång har några personuppgiftsombud angett att de ska uppdatera avtal som funnit en längre tid, dessutom har nya avtal tecknats.

Förteckningar finns men inte för all hantering av personuppgifter. I vissa förvaltningar finns förteckningar som är daterade 2001, huruvida den hanteringen förekommer fortfarande har vi inte undersökt. Några förteckningar är inte daterade.

3. Granskningsresultat

3.1 Riktlinjer

Det finns en skriftlig arbetsfördelning för personuppgiftsansvaret som har reviderats under slutet av 2012 och det har också tagits fram riktlinjer för sociala medier och mobila tjänster.

Den reviderade arbetsfördelningen har inte tagits upp för beslut i nämnderna/styrelserna. Det är viktigt att komma ihåg att varje nämnd/styrelse ansvarar för behandling av personuppgifter inom sitt verksamhetsområde och om de krav som ställs i personuppgiftslagen inte efterföljs så är det nämnden/styrelsen som kan bli föremål för åtal. Från respektive nämnds sida är det därför viktigt att se till att rutinerna för hantering av personuppgifter fungerar tillfredställande. Ett steg i den processen är att se till att riktlinjer är antagna i nämnden/styrelsen.

Det är viktigt att riktlinjer förankras i förvaltningarna, även hos dem som faktiskt hanterar personuppgifter. Detta åligger varje nämnd att se till att riktlinjerna blir kända.

3.2 Rutiner

Utöver ansvarsfördelningen så anser vi att det bör finnas skriftliga rutinbeskrivningar för vad som ska göras i samband med personuppgiftshantering. Enligt lagen ligger ansvaret för att utarbeta rutiner för förteckningar på personuppgiftsombudet. Datainspektionen ger ut informationsblad och skrifter som kan vara till hjälp i utformningen av rutiner. Det finns inga skriftliga rutiner för hur kontroller av efterlevnad av personuppgiftslagens krav ska ske. Rutiner och riktlinjer behöver utarbetas och antas i respektive nämnd/styrelse.

Frågor kring personuppgiftshantering beskrivs som besvärliga och svårförståeliga. För att hanteringen ska kunna fungera på ett tillfredställande sätt är det nödvändigt att det skapas en förståelse, dels för hur hanteringen ska ske, men också för hur viktiga de här frågorna är och vilka konsekvenser en felaktig hantering kan få. Den förståelsen kan öka genom utbildning och löpande information. Utbildning behövs både för personuppgiftsombuden och för dem som hanterar personuppgifterna ute i verksamheten. Personuppgiftsombudet för kommunstyrelsen har tillsammans med IT-strateg tagit fram material för utbildning vilket är en bra start. Nämnderna bör se till att utbildningar genomförs.

3.4 Kommentarer

Den sammanfattande bedömningen är att rutinerna kring hantering av personuppgifter inte är tillfredställande. Det har tagits fram en ansvarsfördelning kring hanteringen som ska skrivas på av personuppgiftsombud, förvaltningschefer och enhetschefer. Det är ett bra steg på vägen och kan öka förståelsen för vad som ingår i ansvaret. Eftersom varje nämnd/styrelse ansvarar förbehandling av personuppgifter måste regler och riktlinjer också antas av respektive nämnd/styrelse, något som ännu inte skett.

Vi rekommenderar respektive nämnd att se till att se till att regler och arbetsfördelningar inom nämndens verksamhetsområde samlas in och vid behov uppdateras samt undertecknas av berörda chefer.

För närvarande finns inga skriftliga rutiner för kontroll av att ansvaret enligt personuppgiftslagen efterföljs. Vi rekommenderar att sådana utarbetas. Rutiner kan utarbetas gemensamt och anpassas till den egna verksamheten. Det ska dock påpekas att det alltid är berörd nämnd eller styrelse som ansvarar för den behandling som sker inom nämndens/styrelses ansvarsområde därför kan inte ansvaret läggas på en övergripande nivå. Varje nämnd måste anta rutiner för kontroll och uppföljning och ansvarar sedan för att de efterföljs inom nämndens/styrelsens verksamhetsområde.

Reglerna kring behandling av personuppgifter upplevs som komplicerade och därför krävs det att det sker kontinuerlig utbildning och information. Utbildningen bör omfatta alla de som personer som antingen har ett personuppgiftsansvar eller som hanterar personuppgifter för den personuppgiftansvariges räkning. Nyanställda bör alltid få en introduktion i ämnet.

Vår förfrågan till personuppgiftsombuden om förteckningar och avtal har det framkommit att det inte finns förteckningar över alla behandlingar och inte heller avtal med alla personuppgiftsbiträden. Respektive nämnd/styrelse måste följa upp att nödvändiga förteckningar och avtal finns. För att det ska vara möjligt att kontrollera så bör en regelbunden inventering av system där personuppgifter kan behandlas genomföras. Vi ser det som positivt att åtgärder har vidtagits under granskningens gång, exempelvis genom att avtal har uppdaterats och nya har tecknats.

Efter genomförd granskning har vi följande rekommendationer:

- ✓ Regler och riktlinjer bör antas av respektive nämnd/styrelse. För att stärka kontrollen vid förvaltningarna rekommenderar vi att ansvar fördelas ut även till områdes- och enhetschefer,vilka har kännedom om de personuppgifter som behandlas ute i verksamheterna.

- ✓ Det bör upprättas en rutin för kontroll av att personuppgiftsansvaret hanteras enligt lag. En sådan rutin kan upprättas gemensamt men varje nämnd/styrelse måste anta rutiner och ansvarar för att kontrollera efterlevnaden. En sådan rutin kan exempelvis ingå i det årliga arbetet med intern kontroll.

- ✓ Avtal måste tecknas med alla parter som hanterar personuppgifter för nämndernas/styrelsernas räkning. Det gäller externa parter, men avtal behöver också

upprättas mellan nämnderna och det nya kundcentret, som kommer att hantera personuppgifter på nämndernas begäran.

- ✓ Varje nämnd/styrelse bör tillse att det genomförs utbildningar inom nämndens verksamhetsområde. Att informera om reglerna kring PuL bör ocks regelmässigt göras när en person nyanställs.

- ✓ För att det ska vara möjligt att få en överblick över var personuppgifter behandlas bör det regelbundet göras en inventering av vilka behandlingar som görs inom nämndens verksamhetsområde. En behandling kan exempelvis ske genom system, molntjänster eller socialt medium.