Datainspektionen informerar

Nr 1/2010

Allmänna råd

Enligt 1 § landskapslagen (2007:89) om Datainspektionen skall Datainspektionen följa den allmänna utvecklingen inom sitt verksamhetsområde och ta nödvändiga initiativ. Datainspektionen skall informera om gällande regler samt ge anvisningar och råd om behandlingen av personuppgifter.

Datainspektionens allmänna råd är inte bindande. De är rekommendationer om hur de bindande kraven i landskapslagen (2007:88) om behandling av personuppgifter inom kommunal- och landskapsförvaltningen (personuppgiftslagen) kan uppnås inom de kommunala myndigheterna.

Datainspektionen

den 8 februari 2010

di.ax datainspektionen

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

Innehåll

1 Allmänt

Datainspektionen anser att den grundläggande rättigheten i grundlagen som gäller skyddet av privatlivet väger tyngre än de grundläggande rättigheterna som gäller offentlighet och yttrandefrihet. Därför bör kommunerna särskilt beakta värnandet om skyddet av privatlivet när kommunerna behandlar personuppgifter och överväger att offentliggöra dem.

Enligt kommunallagen ska information ges om beslut som gäller skötseln av kommunens angelägenheter och om beredningen av dem.

Datainspektionen anser att kommunerna bör försöka samordna kravet på god informationshantering, god informationsbehandling och information så att en persons integritetsskydd inte omotiverat äventyras när kommunerna informerar om sin verksamhet.

2 Några grundläggande begrepp

2.1 Vad är personuppgifter?

Som personuppgifter betraktas information som beskriver en fysisk person eller hans eller hennes egenskaper eller levnadsförhållande och som kan hänföras till personen i fråga eller hans eller hennes familj, t.ex. namn eller fotografi som kan sammankopplas med en viss person eller uppgifter om bedömning och hälsotillstånd.

2.2 Vad avses med behandling av personuppgifter?

Med behandling avses varje åtgärd som vidtas i fråga om personuppgifter såsom t.ex. insamling, registrering, organisering, bearbetning, inhämtande, användning eller spridning.

2.3 Vad är ett register med personuppgifter?

Ett personregister är en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

2.4 Vem är ansvarig för behandlingen av personuppgifter?

Den som ansvarar för att personuppgifter behandlas på lagligt sätt kallas registeransvarig. Registeransvarig är den som bestämmer[1] vilka personuppgifter som skall behandlas och till vad uppgifterna skall användas. Enligt personuppgiftslagen[2] avses här myndighet, nämnder och andra därmed jämförbara organ som med stöd av lag eller beslut tillsatts för att utföra en uppgift. Som myndighet fungerar även juridiska och fysiska personer som utövar offentlig makt och som med stöd av landskapslag utövar ett offentligt uppdrag.

2.5 Rätten till insyn enligt personuppgiftslagen

Var och en har trots sekretessbestämmelserna i regel rätt att på ansökan få information från den registeransvarige om personuppgifter som rör honom eller henne behandlas i ett register eller inte (13, 14 och 15 §§). Den registeransvarige skall utan onödigt dröjsmål ge sökanden rätt att ta del av informationen. Om den registeransvarige vägrar lämna information skall ett skriftligt intyga utfärdas. I intyget skall även nämnas orsaken till att insynen förvägrats. Har den registeransvarige inte lämnat ett skriftligt svar tre månader efter det att ansökan gjordes jämställs det med en vägran att lämna ut information. Vid vägran att lämna ut information kan sökanden begära att tillsynsmyndigheten (Datainspektionen) prövar ärendet. I enlighet med god förvaltningssed bör den registeransvarige i sitt beslut hänvisa till Datainspektionen.

[1] Med myndighet avses närmast fasta, kontinuerligt och självständigt arbetande organ. De myndigheter som räknas upp i lagens 10 § definieras på organisatoriska grunder. Med myndigheter avses landskapets myndigheter, det vill säga landskapsregeringen (Ålands landskapsregerings allmänna förvaltning) och den underlydande myndigheter och inrättningar. Förutom den allmänna förvaltningen omfattas till exempel även Ålands hälso- och sjukvård, Ålands miljö- och hälsoskyddsmyndighet, landskapets skolor, Ålands statistik- och utredningsbyrå och motorfordonsbyrån av lagen. Även juridiska och fysiska personer som inte hör till den egentliga offentliga förvaltningen, men som med stöd av lag fått ett offentligt uppdrag omfattas av det som i lagen föreskrivs om myndigheter. Den medelbara förvaltning som här avses förutsätter dessutom att offentlig makt utövas. Lagen tillämpas enbart på den verksamhet som har formen av myndighetsutövning. Således gäller bestämmelserna även andra som utöver tjänstemän som sköter offentliga uppdrag såsom till exempel offentligrättsliga föreningar.

[2] Med personuppgiftslagen avses här landskapslag (2008:88) om behandling av personuppgifter inom landskaps- och kommunalförvaltningen.

3 E-förvaltning i kommunerna

Det är viktigt att den nya tekniken används på ett sätt som inte äventyrar skyddet för den personliga integriteten. En utökad e-förvaltning innebär bland annat ett utökat informationsflöde inom och mellan myndigheter. Genom digitalisering av dokument och nya sökfunktioner finns personuppgifter att tillgå på ett helt nytt sätt. Frågor om tillgänglighet och säkerhet utgör därför kärnfrågor inom e-förvaltning.

Enligt personuppgiftslagen får personuppgifter enbart behandlas för berättigade ändamål. Det innebär att personuppgifter inte får beskådas eller användas enbart av det skälet att de finns tillgängliga. Det är till exempel inte tillåtet att utan urskiljning publicera alla offentliga handlingar på en myndighets webbplats. En publicering av en handling måste vara tillåten enligt personuppgiftslagen.

Kommunen bör göra klart för sig vilken hotbild som finns, det vill säga vilka händelser som skulle kunna drabba den egna IT-miljön, hur stor risken är att ett hot blir verklighet, vilka konsekvenserna kan bli om ett hot blir verklighet samt vilka resurser en obehörig behöver för att realisera ett hot, det vill säga vilken kunskap, utrustning eller omständighet som krävs för att hotet skall bli verklighet. En viktig bedömningsgrund är uppfattningen om informationens ”värde” med utgångspunkt från aspekter på tystnadsplikt och hemlighållande, krav på riktighet och tillgänglighet, liksom krav på spårbarhet och oavvislighet (en princip inom informationssäkerhet som går ett steg längre än spårbarhet och som innebär att en utförd handling inte ska kunna förnekas av den som utfört den. För att uppnå detta används olika former av elektroniska signaturer.

Kommunen är skyldig att på eget initiativ lämna information i enlighet med personuppgiftslagen till användare av e-tjänster. Information skall lämnas till användarna oavsett om uppgifterna samlas in med eller utan de registrerades samtycke. Kommunen behöver inte informera om sådant som användarna redan känner till eller kan antas känna till.

Personuppgiftslagen innehåller en uppräkning av den information (personuppgiftsansvarigs identitet, ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter) som kommunerna är skyldiga att lämna.

Det innebär att information ska lämnas om vilka kategorierna (registerbeskrivningarna) är och rätten att ansöka om information och få rättelse.

För att undvika en i varje enskilt genomgripande och krävande översyn av när information måste lämnas, är det lämpligt att kommunen rutinmässigt lämnar information i samband med att den tillhandahåller e-tjänster. Information kan ofta lämnas i en särskild ruta eller i ett särskilt fönster på webbplatsen, i anslutning till e-tjänsten.

3.1 Säkerhet för personuppgifter

Kommunens val av autentiseringsmetod bör utgå från känsligheten hos de personuppgifter som behandlas och de risker som är förknippade med behandlingen. E-tjänster där användarna kan ta del av uppgifter som är att beteckna som känsliga enligt personuppgiftslagen, uppgifter som rör lagöverträdelser som innefattat brott samt uppgifter som omfattas av sekretess fordrar i regel mer avancerade metoder för autentisering (t.ex. e-legitimation eller engångslösenord).

Personuppgifter som överförs via öppna nät måste skyddas särskilt.

Om uppgifterna endast får lämnas ut till identifierade användare ska mottagarnas identitet säkerställas[3].

Kommunerna måste ha väl avvägda rutiner för behörighetstilldelning och tydliga riktlinjer för när det är tillåtet för personal att ta del av personuppgifter inom respektive nämnd eller förvaltning. För att kunna följa upp obehörig användning av personuppgifter bör det dessutom, beroende av känsligheten hos personuppgifterna, finnas en behandlingshistorik som sparas viss tid. Behandlingshistoriken bör naturligtvis följas upp, och den måste skyddas mot otillåtna ändringar. Det är viktigt att göra klart för de anställda vad som är tillåtet, vilka konsekvenserna blir om man bryter mot en regel och hur efterlevnaden av reglerna följs upp.

[3] Datainspektionen i Sverige rekommenderar i sina anvisningar att det kan ske till exempel genom signerat servercertifikat och SSL/TLS, det vill säga säkra kommunikationsprotokoll som främst används för att krypteringsskydda kommunikation på webben.

4 Publicering av diarier och protokoll på internet

Diarier och protokoll får innehålla direkta personuppgifter, såsom till exempel namn, förutsatt att övriga uppgifter inte är känsliga eller rör lagöverträdelser som innefattar brott. En förutsättning för att uppgifterna får publiceras på Internet är att det saknas skäl att anta att det finns risk för att den registrerades personliga integritet kränks genom överföringen.

Uppgifter som direkt pekar ut en registrerad som är föremål för sanktioner av typen avgifter, vite m.m. får i regel inte göras tillgängliga på Internet.

Kommunerna skall se till att ärendemeningarna i diarierna utformas på ett sådant sätt att integritetskänslig information inte röjs.

Sammanfattningsvis gäller personuppgiftslagen då kommunen gör handlingar elektroniskt åtkomliga via diariet på Internet.

Vad avser övrig publicering av information på kommunens webbplats får personuppgifter inte publiceras på kommunens webbplats enbart av det skälet att de finns tillgängliga och inte är hemligstämplade.

5 Mellankommunalt samarbete

Mellankommunalt samarbete kan enligt kommunallagen bedrivas i form av samverkan genom avtal, gemensamma förvaltningar som kommunförbund och mellankommunal ombudsstämma.

5.1 Registeransvar

Enligt 2 § personuppgiftslagen är det den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter som är registeransvarig. Registeransvaret i en kommun ligger i allmänhet hos kommunstyrelsen, nämnderna och andra organ som är så självständiga att de kan anses utgöra förvaltningsmyndigheter.

När kommunala nämnder och andra organ samarbetar genom att dela på ansvarsområden och ta över handläggningen av varandras ärenden, kan det uppstå oklarheter om registeransvaret. Det är i och för sig möjligt att överlåta den faktiska behandlingen av personuppgifter, men registeransvaret kan aldrig överlåtas. Det är därför viktigt att göra klart vem som är registeransvarig innan någon personuppgiftsbehandling äger rum, i synnerhet när behandlingen sker för gemensamma syften. Registerbiträde är enligt 2 § 5) punkten personuppgiftslagen den som behandlar personuppgifter för den

registeransvariges räkning. Om en kommunal nämnd anlitar en annan kommunal nämnd för att utföra vissa uppgifter, blir den nämndens personal som utför uppdraget ett registerbiträde som får behandla personuppgifter enligt den registeransvariges instruktioner. Registerbiträdet är skyldigt att vidta de säkerhetsåtgärder som den registeransvarige kräver eller instruerar om. Ett skriftligt avtal som reglerar förhållandet mellan registerbiträdet och den registeransvarige skall upprättas enligt 19 § 2 mom. personuppgiftslagen. I avtalet ska bland annat säkerhetsåtgärderna vid behandlingen av personregister regleras. Den registeransvariga nämnden är skadeståndsansvarig gentemot den registrerade, även för åtgärder som en medhjälpare eller ett registerbiträde har utfört. Ett biträde kan enligt avtal eller allmänna regler bli skadeståndsskyldig gentemot den registeransvarige.

Hanteringen av personuppgifter måste regleras särskilt i avtal. Det är alltid den registeransvarige som ytterst svarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt. Ansvaret är straff- och skadeståndssanktionerat. En konstruktion med ett delat registeransvar kan vara vanskligt, eftersom alla nämnderna då blir solidariskt ansvariga om någon av dem skulle använda uppgifterna på ett sätt som strider mot bestämmelserna i personuppgiftslagen.

5.2 Säker kommunikation

I de fall kommunerna väljer att använda gemensamma IT-system för ärendehantering, biblioteksadministration, personaladministration, GIS och IT-servrar riskerar att sprida personuppgifter på ett sätt som är oförenligt med personuppgiftslagen. Personuppgiftslagen kräver inte att alla kommuner använder separata system, men tillgången till personuppgifter måste begränsas. Därför bör systemet alltid innehålla behörighetsbegränsningar

I syfte att förhindra att personuppgifter förstörs, ändras eller förvanskas vid överföring via nät och för att skydda anslutna tjänster mot obehörig åtkomst bör den personuppgiftsansvarige vidta lämpliga åtgärder för att åstadkomma en tillfredsställande säkerhet. Personuppgifter som överförs via nät bör, beroende på hur känsliga de är, skyddas genom kryptering.

5.3 Tillgång till befolkningsregister

Befolkningsregistret innehåller många personuppgifter varför det är angeläget att endast anställda med behov av uppgifterna i sitt arbete får ta del av dem. Kommunernas behov av en effektiv hantering av invånarnas personuppgifter skall vägas mot de enskildas intresse av skydd för den personliga integriteten. Stora personregister är alltid förenade med stora integritetsrisker då den registeransvarige sällan kan visa en anknytning till de registrerade för att registrets ändamål ska anses berättigat.

6 Uppdrag av en myndighet

Med uppdrag avses situationer där en uppgift som hör till en myndighet enligt ett separat avtal utförs av en enskild person eller någon organisation som inte hör till den aktuella myndigheten.

Enligt 3 § 1 mom. landskapslagen om planering av och landskapsandel för socialvården kan en kommun ordna de uppgifter som hör till kommunen

- genom att själv ombesörja verksamheten
- genom att med stöd av avtal tillsammans med en annan kommun eller andra kommuner ombesörja verksamheten
- genom att låta kommunförbund där kommunen är medlem sköta verksamheten, eller
- genom att köpa tjänster från landskapet, av annan kommun, av kommunalförbund eller av annan som tillhandahåller de aktuella tjänsterna

6.1 Avtal om köptjänster

I avtal om köptjänster definieras vilka rättigheter och skyldigheter kommunen och den privata serviceproducenten har. När avtal om köptjänster ingås är det skäl att i avtalen ta in bestämmelser om hur handlingarna skall förvaltas, hur de skall göras upp, uppbevaras, utplånas eller arkiveras . Det är dessutom skäl att i avtalen anteckna hur upplysningar[4] om handlingarna skall ges till den registrerade eller till en person i partsställning eller till någon annan utomstående.

6.2 Avtal med systemleverantörer

Om kommunen anlitar en extern systemleverantör som även sköter driften och lagrar myndighetens personuppgifter i sina datorer krävs det att myndigheten ingår ett avtal med leverantören som reglerar hur personuppgifterna får hanteras. I avtalet bör ansvaret och förpliktelserna i samband med registreringen definieras. Till exempel får leverantören behandla personuppgifterna bara i enlighet med instruktioner från kommunen och leverantören är skyldig att vida åtgärder för att upprätthålla god IT-säkerhet.

[4] Vid Dataombudsmannens byrå i Helsingfors har en kombinerad modell för informationsregisterbeskrivningar för informationen till socialvårdsklienter utarbetats. Modellen innehåller även klientens möjlighet att kontrollera sina registeruppgifter http://www.tietosuoja.fi/35043.htm
http://www.tietosuoja.fi/14592.htm

7 Checklista

- Definiera först ändamålet med behandlingen av personuppgifter (registrets användningsändamål)
- Planera behandlingen av personuppgifterna
- Instruera och utbilda personalen och övervaka behandlingen av personuppgifterna
- Försäkra dig om att du endast behandlar uppgifter som behövs i ditt arbete och se till att uppgifterna är felfria. Försäkra dig också om att behandlingen av uppgifterna är sakligt motiverad med hänsyn till verksamheten och att behandlingen lämpar sig för sitt ändamål
- Använd uppgifterna endast för det ursprungliga ändamålet
- Informera den registrerade om principerna för registreringen
- Gör upp en registerbeskrivning[5] och håll den tillgänglig för var och en
- Ta hänsyn till rätten till insyn och lämna de begärda uppgifterna eller ett intyg om vägran ifall du inte kan lämna uppgifterna
- Iaktta sekretess- och tystnadsplikten
- Skydda uppgifterna så att utomstående inte får tillgång till dem
- Lämna ut uppgifter endast med den registrerades samtycke eller med stöd av lag
- Utplåna uppgifterna efter att kundförhållandet har upphört eller arkivera dem.

[5] Blankett i pdf-format finns på Datainspektionens hemsida www.di.ax