Eskilstuna kommun

Instruktion enligt personuppgiftslagen (1998:204) för Eskilstuna kommunkoncern

Antagen av kommunfullmäktige den 23 september 2010, § 193.

Inledning

Personuppgiftslagen (PuL) trädde i kraft 1998 och bygger på ett EG-direktiv (datadirektivet). Lagen ska hindra att den personliga integriteten kränks genom behandling av personuppgifter.

Personuppgiftslagen gäller all automatiserad behandling av personuppgifter, det vill säga all behandling som sker elektroniskt. Lagen gäller också för manuell behandling av person-uppgifter, om dessa uppgifter ingår eller är avsedda att ingå i en strukturerad behandling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier (manuella register).

Följande riktlinjer gäller för automatiserad behandling av personuppgifter för kommunstyrelsen och samtliga nämnder och kommunala bolag i Eskilstuna kommunkoncern.

Behandling av personuppgifter

PuL ställer inte några krav på licens eller tillstånd från Datainspektionen för behandling av personuppgifter, utan den personuppgiftsansvarige, se definition nedan, svarar självständigt för att behandlingarna av personuppgifter överensstämmer med lagen med mera.

PuL reglerar all behandling av personuppgifter och inte enbart personregister. En grundregel i lagen är att behandling av personuppgifter bara får ske för särskilda, uttryckligen angivna och berättigade ändamål. Uppgifterna får sedan inte behandlas för något annat ändamål, som inte är förenligt med det grundläggande ändamålet.

Huvudregeln är att behandling av personuppgifter bara får ske med samtycke av den som berörs av uppgifterna (den registrerade). Personuppgifter får dock behandlas utan samtycke, om behandlingen är berättigad och nödvändig för vissa i lagen särskilt angivna ändamål.

Beträffande känsliga personuppgifter gäller ett principiellt förbud mot behandling av uppgifterna. Med känsliga uppgifter avses uppgifter om ras eller etniskt ursprung, politiska

åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv. Från detta förbud för behandling finns vissa restriktivt utformade undantag.

Personuppgiftsansvar

Med personuppgiftsansvar avses den som ensam eller tillsammans med andra bestämmer ändamålet med och medlen för behandlingen.

Kommunstyrelsen och nämnderna är personuppgiftsansvariga för all behandling av personuppgifter som förekommer inom styrelsens/nämndens ansvarsområde. I de kommunala bolagen är den juridiska personen personuppgiftsansvarig. Nedan kallas kommunstyrelsen, nämnderna och de kommunala bolagen för den personuppgiftsansvarige.

Ansvaret gäller även den behandling av personuppgifter som sker hos den personuppgiftsansvarige med hjälp av tekniska plattformar och system för informationsbehandling som är gemensamma för kommunens förvaltningar och bolag. Det sistnämnda innebär att flera nämnder/bolag kan vara personuppgiftsansvarig för samma IT-system men endast för de delar som berör den egna verksamheten.

Den personuppgiftsansvarige överlåter den faktiska administrationen av behandlingen av personuppgifter till anställda, men personuppgiftsansvaret kan aldrig överlåtas. Det är alltid styrelsen/nämnden/bolaget som ytterst ansvarar för att PuL följs och att de registrerade behandlas korrekt i enlighet med lagens föreskrifter.

Den personuppgiftsansvarige är skyldig att ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid mot lagen har förorsakat. Skadeståndsansvaret är strikt, men kan jämkas.

Kommunstyrelsens, nämndernas och bolagens skyldigheter

Personuppgiftsansvaret innebär att kommunstyrelsen, nämnderna och bolagen:

- Har det juridiska ansvaret för att all behandling av personuppgifter i verksamheten sker i enlighet med PuL:s bestämmelser och övrig tillämplig lagstiftning på området.
- Bestämmer ändamålet med samt medlen för behandlingarna av personuppgifter, ensam eller tillsammans med annan personuppgiftsansvarig.
- Har ansvaret för att systemen nyttjas etiskt, vilket innebär att det är förbjudet att försöka dölja sin användaridentitet, att försöka skada eller förstöra kommunens/bolagets informationstillgångar, att göra intrång i andras privatliv och att förolämpa och förnedra andra.
- Ansvarar för att det finns rutiner för hur informationsskyldigheten enligt personuppgiftslagen ska fullgöras samt för hur en begäran om rättelse, blockering eller utplåning av uppgifter, som inte har behandlats i enligt med PuL, ska handläggas.
- Ska förvissa sig om att det finns en lämplig skyddsnivå för personuppgiftsbehandlingen genom att det finns rutiner/instruktioner av teknisk, organisatorisk och administrativ art för säkerhetsarbete och behörighetskontroll. Detta innebär bland annat att nödvändiga åtgärder vidtas för att förhindra att personuppgifter förstörs, ändras eller förvanskas vid

överföring via nät och för att skydda anslutna tjänster mot åtkomst från obehöriga samt att den IT-utrustning som används för behandling av personuppgifter har ett tillfredsställande skydd mot stölder och händelser som kan förstöra utrustningen.
- Att personalen informeras om gällande säkerhetsrutiner och vikten av att dessa rutiner följs.
- Svarar för att personalen har erforderlig kompetens för den personuppgiftsbehandling som förekommer i verksamheten genom att se till att all berörd personal ges tillfälle till utbildning och fortlöpande hålls informerad om de bestämmelser som gäller för behandlingar av personuppgifter samt om de interna regler som styrelsen/nämnden/-bolaget har utfärdat avseende befogenhet, ansvar och säkerhet.
- Inom respektive nämnd har förvaltningschefen respektive VD:n i det kommunala bolaget ansvaret för att förekommande personuppgiftsbehandlingar sker i enlighet med de krav PuL och annan lag ställer. Förvaltningschef och VD har inget personuppgiftsansvar, utan ett ansvar att se till att den personuppgiftsansvariges beslut verkställs och är förenliga med lagen.

Förteckning över förekommande personuppgifter

Den personuppgiftsansvarige ska fortlöpande föra förteckning över de behandlingar av personuppgifter som förekommer i verksamheten. Ingen ny behandling av personuppgifter av större omfattning, får påbörjas förrän ändamålet för behandlingen har bestämts och behandlingen har förts in i en förteckning samt blankett för avstämning av behandlingen/IT-systemet utifrån bland annat kommunens tekniska plattform, PuL i övrigt, arkivlagen, de ekonomiska förutsättningarna samt prövning utifrån bestämmelserna i 4 kapitlet 1 § offentlighets- och sekretesslagen (2009:400).

Av förteckningen ska framgå:

- Personuppgiftsansvarig nämnd/bolag.
- I förekommande fall uppgift om personuppgiftsombud.
- Behandlingens status.
- Behandlingens benämning samt ändamålet med behandlingen.
- Uppgift om eventuellt personuppgiftsbiträde.
- Kategorier av personer som berörs av behandlingen.
- Hur och från vem uppgifterna har samlats in.
- Till vilka grupper/myndigheter uppgifterna kan komma att lämnas ut.
- Om överföring till tredje land/publiceras på Internet.
- Allmän beskrivning av säkerhetsåtgärder samt uppgifter om teknisk miljö samt förvaring.
- Om behandlingen kräver samtycke och på vilket sätt detta inhämtas eller på vilken laglig grund som behandlingen sker.
- Vilka uppgifter som behandlas.
- I vilken utsträckning behandlingen innehåller känsliga uppgifter som avses i 13 § PuL.
- Om uppgifterna skyddas av sekretess och i så fall vilken/vilka sekretessregler som gäller för uppgifterna.
- På vilket sätt som information enligt 23-26 §§ PuL lämnas.
- Underskrift av handläggare samt systemägare.

I det fall personuppgiftsombud finns ska kopia av förteckningarna överlämnas till denne för förvarande. Denna uppgift åvilar kontaktpersonen. Ansvarig för förteckningen är den personuppgiftsansvarige.

Personuppgiftsombud och kontaktperson
Ett personuppgiftsombud utses av den personuppgiftsansvarige och ska självständigt se till att personuppgifter behandlas på ett korrekt och lagligt sätt. Personuppgiftsombudet ska hjälpa den personuppgiftsansvarige att uppfylla lagens krav och bidra till att skapa ordning och reda. Av PuL framgår de uppgifter som åligger ett personuppgiftsombud.

Kommunstyrelsen har utsett ett personuppgiftsombud för sitt verksamhetsområde. Övriga nämnder och bolag ska också utse ett personuppgiftsombud för sina respektive verksamhetsområden.

Respektive nämnd/bolag ska i det fall man väljer att utse kommunstyrelsens personuppgiftsombud till nämndens eget ombud utse kontaktperson för frågor om PuL. Kontaktpersonen ska i dessa fall fungera som en länk mellan personuppgiftsombudet och nämnden/bolaget och dess verksamhet. Kontaktpersonen har inga skyldigheter enligt PuL, utan uppdraget, förutom det eventuella stödet till personuppgiftsombudet, får definieras av den personuppgiftsansvarige Kontaktpersonerna ska få utbildning av kommunstyrelsens personuppgiftsombud.

Personuppgiftsbiträde
I de fall personuppgifter för styrelsens/nämndens/bolagets räkning behandlas av någon annan än den egna förvaltningen (kommunen), ska det upprättas ett skriftligt avtal med personuppgiftsbiträdet om att behandlingen av personuppgifter endast får ske i enlighet med instruktioner från den personuppgiftsansvarige. I avtalet ska regleras vilka åtgärder som ska vidtas för att åstadkomma en god säkerhet för behandlingen av personuppgifter samt uppgifter om tystnadsplikt och regressrätt.

Vid utformandet av personuppgiftsbiträdesavtal ska samråd ske med personuppgiftsombudet.

Information enligt 26 § PuL (registerutdrag)
Ansökan enligt 26 § PuL om besked om förekommande behandlingar (registerutdrag) ska handläggas av den styrelse/nämnd/bolag som är personuppgiftsansvarig för behandlingen.

Om begäran om registerutdrag avser personuppgiftsbehandling även hos annan styrelse/-nämnd/bolag och begäran är så formulerad att det klart framgår vilka nämnder som berör, överlämnas omgående en kopia av begäran till de övriga berörda nämnderna för handläggning.

PuL föreskriver en handläggningstid på högst en månad. Om ansökan är särskilt omfattande får beskedet dock lämnas senast fyra månader efter det att ansökan gjorde.

En särskild instruktion för hantering av registerutdrag ska finnas.

Gallring och arkivering
Enligt huvudregeln i PuL ska alla personuppgifter gallras när de inte längre behövs för verksamheten. De grundläggande kraven i PuL innebär att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. En styrelse/nämnd/bolag får enligt PuL, trots bestämmelserna i lagen, arkivera och bevara allmänna handlingar med stöd av bestämmelserna i arkivlagen, arkivförordningen, kommunens arkivreglemente samt varje styrelse/nämnds dokumenthanteringsplan.

Det ska finnas riktlinjer/beslut om under hur lång tid personuppgifter ska bevaras samt hur arkivering och gallring ska ske. Dessa riktlinjer ska framgå av styrelsens/nämndens/bolagens dokumenthanteringsplaner (se kommunen arkivreglemente § 5).

Elektronisk dokumenthantering och protokoll på kommunens hemsida
För att undvika att personuppgifter av känslig karaktär offentliggörs genom elektronisk ärende- och dokumenthanteringssystem eller protokoll på kommunens hemsida, ska det upprättas riktlinjer för hur styrelsen/nämnderna/bolagen ska hantera detta. Detta ska ske utifrån person-uppgiftsförordningens regler.

Riktlinjer för IT-säkerhet och sårbarhetsanalys
Styrelsen/nämnden/bolaget ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Eskilstuna kommun ska ha fastställda skriftliga instruktioner för informationssäkerheten. I instruktionerna bör man lämpligen redovisa organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten.

Som en utgångspunkt för arbetet med informationssäkerheten är det lämpligt att göra risk- och sårbarhetsanalyser för att klarlägga vilken säkerhetsnivå som ska gälla för skyddet av den personuppgiftsansvariges informationstillgångar.

Datainspektionens allmänna råd och rekommendationer
Eskilstuna kommunkoncern ska som huvudregel följa Datainspektionens allmänna råd och rekommendationer om hantering av personuppgifter.

_____