§ 102

KS 147/18

Policy och riktlinjer för hantering av personuppgifter

Beslut

Kommunstyrelsen antar förslag till riktlinjer för hantering av personuppgifter, under förutsättning att kommunfullmäktige antar förslaget till policy för hantering av personuppgifter, enligt bilaga 2.

Kommunstyrelsens förslag till kommunfullmäktige

Kommunfullmäktige antar förslag till policy för hantering av personuppgifter enligt bilaga 1.

Ärendet

När allmänna dataskyddsförordningen (GDPR) träder i kraft den 25 maj 2018 krävs att Mölndals stad antagit tydliga styrdokument som visar hur staden arbetar för att uppfylla de krav som ställs i förordningen. Stadsledningsförvaltningen har därför arbetat fram förslag till policy och riktlinjer för hantering av personuppgifter vilka föreslås antas av kommunfullmäktige respektive kommunstyrelsen.

Ärendets behandling

Stadsledningsförvaltningens tjänsteskrivelse daterad 26 mars 2018.
Arbetsutskottet har behandlat ärendet den 11 april 2018, § 65.

Förslag till beslut

Arbetsutskottets förslag till kommunstyrelsen

- Kommunfullmäktige antar förslag till policy för hantering av personuppgifter enligt bilaga 1.
- Kommunstyrelsen antar förslag till riktlinjer för hantering av personuppgifter, under förutsättning att kommunfullmäktige antar förslaget till policy för hantering av personuppgifter, enligt bilaga 2.

Beslutsgång

Ordförande frågar om arbetsutskottets förslag till beslut antas och finner att så sker.

Stadsledningsförvaltningen
Josefin Ludvigsson

Kommunstyrelsen

Policy och riktlinjer för hantering av personuppgifter

Förslag till beslut

Kommunfullmäktige antar förslag till policy för hantering av personuppgifter enligt bilaga 1.

Kommunstyrelsen antar förslag till riktlinjer för hantering av personuppgifter under förutsättning att kommunfullmäktige antar förslaget till policy för hantering av personuppgifter enligt bilaga 2.

Ärendet

När allmänna dataskyddsförordningen (GDPR) träder i kraft den 25 maj 2018 krävs att Mölndals stad antagit tydliga styrdokument som visar hur staden arbetar för att uppfylla de krav som ställs i förordningen.

Stadsledningsförvaltningen har därför arbetat fram förslag till policy och riktlinjer för hantering av personuppgifter vilka föreslås antas av kommunfullmäktige respektive kommunstyrelsen.

Beredning

Den 25 maj 2018 träder Allmänna dataskyddsförordningen i kraft i Sverige. Förordningen, som är direkt tillämplig i Sverige, ersätter den nu gällande personuppgiftslagen och innebär en skärpning av hur personuppgifter får behandlas. Se länk för ytterligare information om dataskyddsförordningen. https://www.datainspektionen.se/dataskyddsreformen/

En nyhet är att den som behandlar personuppgifter inte bara måste uppfylla de krav som ställs i dataskyddsförordningen. Därtill måste det kunna visas att kraven i dataskyddsförordningen verkligen uppfylls. En sådan regeluppfyllnad visas lämpligast genom att organisationen har tydliga styrdokument och att det upprättas rutiner och mallar samt att det med jämna mellanrum genomförs interna kontroller av att reglerna efterföljs.

Något som också utgör en nyhet i dataskyddsförordningen är att tillsynsmyndigheten får möjlighet att utdöma vitessanktioner om reglerna inte följs. Att vitesbeloppet för offentlig verksamhet i en anslutande proposition är satt till högst 10 miljoner kronor visar att lagstiftaren ser allvarligt på brister i hanteringen av personuppgifter.

Varför policy och riktlinjer för hantering av personuppgifter?

Mölndals stad har idag inga styrdokument som behandlar frågan om hanteringen av personuppgifter. Såväl förslag till policy som förslag till riktlinjer utgör tolkning av vilka åtgärder som är nödvändiga för att kraven i dataskyddsförordningen ska kunna uppfyllas och ligger med som bilagor till denna tjänsteskrivelse.

Enskildas personuppgifter behandlas på åtskilliga sätt i kommunal verksamhet och i många fall har saknas reell möjlighet för enskilda att välja bort att få sina personuppgifter behandlade av kommunen. Därför så finns det intresse av att på ett tydligt sätt visa att staden bland annat arbetar för att de, vars personuppgifter behandlas av staden, ska kunna känna sig trygga med att deras personuppgifter hanteras på ett respektfullt sätt.

Förslaget bygger på att Mölndals stad antar en policy som pekar på vikten av att hänsyn tas till gällande lagstiftning redan vid planeringen av verksamheten. För att säkerställa en samsyn inom kommunen föreslås även att kommunstyrelsen får uppdraget att leda, samordna och ha uppsikt över stadens arbete med att uppfylla kraven i dataskyddsförordningen.

Dataskyddsförordningen utgörs till stor del av ett regelverk som kräver ett nytänk som bör genomsyra all verksamhet när det gäller hanteringen av personuppgifter. Det är viktigt att på ett så tydligt sätt som möjligt visa för verksamheterna vilka åtgärder som måste vidtas för att kraven i förordningen ska anses uppfyllda. I de riktlinjer som föreslås visas hur staden ska arbeta inom området och hur staden rent praktiskt ska kunna visa att reglerna uppfylls.

Såväl förslag till policy som förslag till riktlinjer ligger med som bilagor till denna tjänsteskrivelse och kan med fördel läsas parallellt med nedanstående text som är tänkt att tjäna som kommentarer till de föreslagna dokumenten.

Policy för hantering av personuppgifter (bil. 1)

Kommunstyrelsens uppgifter

Det krävs en viss likriktning av hur staden hanterar personuppgifter för att på ett smidigt sätt kunna visa och ha kontroll över att kraven i lagen ska uppfylls. Därför föreslås att policyn stadgar att kommunstyrelsen får i uppdrag att samordna och ha uppsikt över stadens arbete med att uppfylla kraven i förordningen samt att upprätta riktlinjer för att säkerställa att staden hanterar personuppgifter på ett lagenligt sätt.

I och med införandet av dataskyddsförordningen skärps kraven på den kontroll som varje personuppgiftsansvarig ska ha över personuppgifter som denne överlämnar åt en tredje part att behandla (ett så kallat personuppgiftsbiträdesavtal). Eftersom respektive nämnd är personuppgiftsansvarig för de personuppgifter som behandlas inom den egna förvaltningen skulle det, enligt huvudregeln, krävas att det tecknades avtal för varje sådan behandling nämnderna emellan. Att teckna och löpande upprätthålla sådana korsvisa avtal inom Mölndals stad skulle först och främst vara på gränsen till ogenomförbart. Därutöver kan de rättsliga effekterna av sådana avtal ifrågasättas då nämnderna ingår i samma juridiska person och därmed egentligen saknar möjlighet att ingå avtal. SKL har uppmärksammat problemet och gjort tolkningen att kommuner istället på annat sätt kan klargöra vilka nämnder som är

ansvariga för vilka behandlingar. SKL:s tolkning är väl grundad och bör kunna läggas till grund för hur Mölndals stad väljer att ordna med sådant ansvar och sådana säkerhetsinstruktioner internt mellan stadens nämnder. I riktlinjerna har ansvarsdokumentet ifråga inte fått någon benämning annat än att det beskrivs som en förteckning över ansvar och säkerhetsinstruktioner nämnder emellan. Dokumentet går emellertid under arbetsnamnet internt personuppgiftsbiträdesavtal. Detta begrepp kommer för tydlighetens skull att användas fortsättningsvis i denna tjänsteskrivelse. Kommunstyrelsen bör vara den nämnd som formellt administrerar det interna personuppgiftsbiträdesavtalet. I riktlinjerna föreslås vidare att kommunstyrelsens dataskyddsombud ska vara den tjänsteperson som håller det interna personuppgiftsbiträdesavtalet uppdaterat och som lyfter den till beslut till kommunstyrelsen vid behov dock minst en gång per år. Bedömningen är att lagens krav på detta sätt uppfylls utan att formella avtal för varje enskild behandling behöver tecknas mellan respektive nämnd.

Organisatoriska och tekniska förutsättningar
I dataskyddsförordningen framgår att det krävs att tekniska och organisatoriska åtgärder ska vidtas för att säkerställa och kunna visa att all behandling sker i enlighet med förordningen. Vad som är tänkt att utgöra tekniska och organisatoriska åtgärder är inte helt tydligt. En utgångspunkt för staden är dock att de kan tänkas variera utifrån vilken behandling det är fråga om lika mycket som vilken del av organisationen som man diskuterar. För att det överhuvudtaget ska finnas möjlighet att kunna vidta tekniska och organisatoriska åtgärder måste det dock finnas förutsättningar för detta ska kunna göras. I förslaget till policy lyfts det därför fram att det ska tas hänsyn till de tekniska och organisatoriska förutsättningarna redan vid planeringen av verksamheten.

Vidare framhålls i förslaget till policy att staden ska ha kontroll över verksamheternas behandling av personuppgifter och att staden ska vara tillmötesgående och förberedd på att hjälpa de registrerade att tillvara sina rättigheter enligt dataskyddsförordningen. Detta följer indirekt av förordningen och ger en bra struktur för kommunstyrelsen att bygga vidare på i förslaget till riktlinjer.

Riktlinjer för hantering av personuppgifter (bil. 2)
I förslaget till riktlinjer har de rubriker (organisatoriska förutsättningar, kontroll över personuppgiftsbehandlingar och registrerades rättigheter) som finns i förslaget till policy utvecklats enligt nedanstående. Den absoluta huvuddelen av det som stadgas i förslaget till riktlinjerna utgörs av sådana direkta eller indirekta skyldigheter som antingen följer direkt av dataskyddsförordningen eller som utgör en förutsättning för att ett krav ska kunna uppfyllas av stadens organisation.

Organisatoriska och tekniska förutsättningar
Inledningsvis konstateras att varje nämnd är personuppgiftsansvarig. Här ska klargöras att detta följer av lag och att nämnderna således hade varit personuppgiftsansvariga oavsett utformning i stadens reglemente.

Enligt dataskyddsförordningen ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa att behandling av personuppgifter utförs i

enlighet med förordningen. Nämnderna uppmärksammas här på att det åligger dem att säkerställa att det finns tekniska och organisatoriska förutsättningar inom förvaltningen för att uppfylla kraven i dataskyddsförordningen. Förvaltningarna ska å sin sida säkerställa och kunna visa att de har rätt resurser och relevant kompetens inom området.

Central organisation
Även om personuppgiftsansvaret (och därmed även ansvaret att tillse att kraven i dataskyddsförordningen uppfylls) ligger på respektive nämnd så finns det flera anledningar att arbetet görs enhetligt i staden i så stor utsträckning som möjligt. Ett enhetligt arbetssätt underlättar inte bara för kommunstyrelsen när det kommer till uppsiktsplikten. Därutöver skapas gynnsamma förutsättningar för exempelvis dataskyddsombuden och övriga tjänstepersoner som arbetar med dataskyddsfrågor att utbyta erfarenheter och eventuellt samordna utbildningsinsatser. Kommunstyrelsen bör därför samordna de övriga nämndernas dataskyddsombud.

Under arbetet med implementeringen av dataskyddsförordningen i staden har nämndernas personuppgiftsombud (ungefär föregångarna till dataskyddsombud) träffats regelbundet på initiativ av kommunstyrelsen personuppgiftsombud. Under träffarna har funnits tillfälle till diskussioner kring tolkning av det nya regelverket. Därutöver har generella och individuella hjälpbehov kunnat identifieras och åtgärdas genom exempelvis tema-möten eller centralt framtagna mallar och checklistor. Mot bakgrund av att dataskyddsförordningen är ett nytt regelverk som till stora delar behöver tolkas och där den framtida utvecklingen i praxis måste bevakas är det av stor vikt att nämndernas respektive dataskyddsombud håller sig uppdaterade och på detta sätt ges tillfälle att föra diskussioner i ämnet. Att formalisera dessa sammanträden genom att nämna dem i riktlinjerna på ger både tyngd åt sammanträdena och en tydlig fingervisning till nämnderna och deras dataskyddsombud om hur samarbetet nämnderna emellan är tänkt att fungera.

Det ska understrykas att nämndernas dataskyddsombud ska vara självständiga i sitt arbete och att nämnderna själva ansvar för att deras dataskyddsombud innehar rätt kompetens. Även om kommunstyrelsens dataskyddsombud kan agera stöttande i vissa fall så saknar denne möjlighet att utbilda varje dataskyddsombud från grunden. Kommunstyrelsens dataskyddsombud ska emellertid identifiera generella svårigheter hos förvaltningarna och föreslå behövliga åtgärder, exempelvis gemensamma utbildningar eller andra informationsinsatser.

I förslaget föreslås att nämnderna årligen rapporterar in sitt arbete enligt bl.a. riktlinjerna. Denna årliga rapportering fyller främst två syften. Först och främst får nämnderna, som är ytterst ansvariga för den organisation och den teknik som berör hanteringen av personuppgiftsbehandlingar inom den egna förvaltningen, en årlig avstämning av hur arbetet fortlöpt under året. Kommunstyrelsens dataskyddsombud föreslås ge ut anvisningar för vad rapporteringen som minst ska innehålla. Innehållet i anvisningarna kan variera över tid och bör anpassas utifrån utvecklingen av rättspraxis och vad nämnderna rimligen bör ha behov av att få veta för att kunna ha den kontroll som en personuppgiftsansvarig rimligen bör ha. Ett annat syfte med rapporteringen är givetvis att få en kontinuerlig, tydlig och transparent uppföljning av respektive nämnds arbete inom området under det gångna året. Tanken är att

rapporteringen ska göras varje år i september månad från och med 2019.

Vidare ges kommunstyrelsens dataskyddsombud i uppgift att administrera och fortlöpande uppdatera stadens interna personuppgiftsbiträdesavtal.

Dataskyddsombud
Eftersom nämnderna utgör myndigheter måste varje nämnd, var för sig, enligt art. 37.1 a utnämna ett dataskyddsombud. Så som det ser ut i dagsläget så kommer varje nämnd att utse en inom den egna förvaltningen intern tjänsteperson som dataskyddsombud. Det föreligger visserligen inga formella hinder mot att inrätta ett dataskyddsombud för hela staden. Det har också inkommit önskemål om att utreda möjligheten att inrätta ett sådant centralt dataskyddsombud för stadens nämnder. En sådan utredning över vilket som är bäst för staden låter sig emellertid bäst göras först när den nya lagstiftningen har implementerats och då tiden bl.a. fått utvisa hur stor tid i anspråk som varje nämnd kräver från sitt dataskyddsombud.

Ansvaret att se till att uppdraget som dataskyddsombud inte leder till intressekonflikt framgår visserligen i dataskyddsförordningen men lyfts ändå fram i riktlinjerna.

Att dataskyddsombudet ska rapportera direkt till förvaltningsledningen framgår egentligen redan av dataskyddsförordningen. Rekommendationen till förvaltningarnas ledningsgrupper om att bjuda in dataskyddsombudet för avrapportering åtminstone vid två tillfällen per år har till syfte att fungera som en påminnelse för såväl förvaltningsledningen som för dataskyddsombudet.

Den uppdragsbeskrivning över dataskyddsombudets uppgifter som nämnden ska upprätta är tänkt att fungera som ett tydliggörande riktat till både dataskyddsombudet och till förvaltningsledningen. Stadsledningsförvaltningen har upprättat en mall där dels de uppgifter som dataskyddsombudet måste ha och dels den ställning i organisationen som denne ska tillförsäkras framgår. I mallen finns möjlighet för respektive nämnd att lägga till uppgifter för dataskyddsombudet utifrån egna önskemål – så länge som dessa inte leder till intressekonflikt för dataskyddsombudet.

Att dataskyddsombudet ska redovisa förvaltningens arbete för nämnden ligger helt i nämndens intresse i egenskap av personuppgiftsansvarig och alltså den som har det rättsliga ansvaret för att reglerna följs. De uppgifter som har specificerats och som minst ska framgå av redovisningen utgörs av sådant som varje personuppgiftsansvarig rimligen borde ha intresse av att få veta. Rapporteringen som sådan ger också de aktuella förvaltningarna ett naturligt tillfälle varje år att tänka till kring hur hanteringen av personuppgifter och den organisation som byggts upp kring detta fungerar.

Vidare ska kommunstyrelsens dataskyddsombud årligen göra en sammanställning över de övriga nämndernas redovisningar. Kommunstyrelsen får på detta sätt en naturlig uppföljning över de övriga nämndernas arbete med frågorna samtidigt som organisationen i stort får en påminnelse om vikten av att fortsätta att arbeta med frågorna löpande.

Tjänster, produkter och applikationer som medför behandling av personuppgifter
En förutsättning för att uppfylla kraven som ställs på personuppgiftsansvariga är att det finns en mekanism som fångar upp sådana ageranden eller inköp som kan komma att leda till behandling av personuppgifter. En sådan mekanism eller rutin bör lämpligtvis vävas samman med inköpsrutiner i stort så att dataskyddsfrågorna kommer in som en naturlig del redan i den marknadsundersökning som görs innan ett inköp eller en upphandling.

Vidare påminns det i förslagen till riktlinjer om att det finns krav att förhålla sig till i dataskyddsförordningen och som det kan hända att hänsyn måste tas till vid olika inköp.

Eftersom det i särskilda fall kan saknas kompetens inom den egna förvaltningen när det gäller vilka krav som är rimliga eller ens möjliga bör samråd ske med IT-avdelningen vid behov.

Att konsekvensbedömning ska göras om en ny behandling kan komma att leda till att registrerades rättigheter och friheter riskeras är endast en påminnelse om en bestämmelse i dataskyddsförordningen. De konsekvensbedömningar som ska göras ligger mycket nära och överlappar ibland till och med andra säkerhetsbedömningar som ska göras enligt lag. Därför kommer det att upprättas instruktioner som bl.a. kommer att innefatta konsekvensbedömningar. De instruktioner avseende riskanalyser för informationssäkerhet som det refereras till i förslaget till riktlinjer finns ännu inte klara men är planerade att färdigställas under 2018.

Incidentrapportering
Personuppgiftsincidenter ska enligt dataskyddsförordningen rapporteras till tillsynsmyndigheten inom 72 timmar. Vad som exakt utgör en sådan personuppgiftsincident som ska rapporteras till tillsynsmyndigheten är i skrivandes stund ännu inte helt tydligt. När det gäller incidentrapportering är det, särskilt mot bakgrund av den korta tidsfristen, av stor vikt att det finns rutiner för hur alla ska handla och vem som ska kontaktas etc. På samma sätt som när det gäller konsekvensbedömningar hänvisas här till särskilda instruktioner som beräknas finnas på plats under 2018.

Säkerhet i samband med behandlingen
Av dataskyddsförordningen framgår att personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå. Nämnderna påminns här om att de, som personuppgiftsansvariga, ansvarar för att upprätthålla en fullgod säkerhetsnivå utifrån de kriterier som anges i dataskyddsförordningen vid behandling av personuppgifter.

Vidare erinras förvaltningarna om att man redan vid planeringen av verksamheten bl.a. ska beakta regeln om att personuppgifter inte ska hanteras unders längre tid än nödvändigt.

Även när det gäller vad som särskilt ska beaktas ur säkerhetshänseende hänvisas till särskilda instruktioner från informationssäkerhetssamordnaren som ska finnas på plats under 2018.

Kontroll över personuppgiftsbehandlingar
Även här påminns nämnderna om det ansvar som åligger dem som personuppgiftsansvariga.

Förteckning
Redan av den nu gällande lagstiftningen följer att staden ska föra en förteckning över vilka personuppgifter som behandlas. I dataskyddsförordningen har kraven på vad som ska ingå i registret emellertid skärpts.

Registret ska föras löpande och utgör således en ögonblicksbild av varje förvaltnings personuppgiftsbehandlingar.

Stadens nämnder har generellt legat i framkant i arbetet med att föra register och har tillsammans arbetat fram hur registret ska utformas. Mot bakgrund av att registret utgör en del av den årliga rapporteringen som nämnderna förväntas inkomma med till kommunstyrelsen föreslås att kommunstyrelsens dataskyddsombud ges möjlighet att komma med instruktioner gällande registret.

Personuppgiftsbiträdesavtal och gemensamt personuppgiftsansvar
Enligt dataskyddsförordningens ska personuppgiftsansvariga som antingen uppdrar åt en annan aktör att behandla personuppgifter för dennes räkning eller om det av någon anleding föreligger ett gemensamt personuppgiftsansvar fastställa ansvar och skyldigheter i ett avtal. Som exempel så är det aktuellt med ett sådant avtal vid användandet av molntjänster eller om externa leverantörer ges behörighet att få insyn i våra datasystem.

Under detta avsnitt föreslås även att det fastslås att det är kommunstyrelsens dataskyddsombud som ska hålla det interna personuppgiftsbiträdesavtalet uppdaterat.

Registrerades rättigheter
Ett av huvudsyftena med dataskyddsförordningen är att förtydliga de registrerades rättigheter.

Information till de registrerade samt tillgång rättelse, radering och begränsning
Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att tillhandahålla information till registrerade om t.ex. vad ändamålet med behandlingen är. Vidare ska den personuppgiftsansvarige ge tydliga anvisningar om vad den registrerade ska göra för att kunna utöva sina rättigheter. Förvaltningarna ska inte bara kunna hantera begäranden från registrerade om att få tillgång till sina personuppgifter utan även att få sina uppgifter rättade samt i förekommande fall raderade eller begränsade.

Implementering av policy och riktlinjer
Den organisation som föreslås i riktlinjerna motsvarar till stor del den organisation som sattes i staden redan 2014 i samband med att staden började förbereda för den nya förordningen.

Mot bakgrund av att de rutiner som nämnderna och förvaltningarna påbjuds att anta krävs för att staden ska kunna uppfylla kraven i dataskyddsförordningen har en stor del av det arbete som riktlinjerna kan antas medföra redan påbörjats. Därtill ligger en stor del av

förvaltningarna helt i fas när det gäller det tidskrävande arbetet att föra register över alla personuppgiftsbehandlingar.

Som en del av implementeringen planerar stadsledningsförvaltningen en utbildningsinsats gällande dataskyddsförordningen och hur staden ska arbeta med hanteringen av personuppgifter framöver i augusti 2018. Tanken är då att framför allt de föreslagna riktlinjerna ska ligga till grund för den senare delen av utbildningen.

Uppföljning av policy och riktlinjer

Såväl policy som riktlinjer för hantering av personuppgifter kan komma att vara i behov av kontinuerlig uppdatering, särskilt under de första åren.

Det ska här framhållas att dataskyddsförordningen i vissa delar är svårtydd och att många frågor om hur lagen ska tillämpas lämnas obesvarade fram tills att det utbildats en praxis på området genom exempelvis domstolsavgöranden. De organ som kan hjälpa till med tolkningar av vissa specifika frågor har varit lite sega i starten vilket har gjort att det ofta har varit och fortfarande är svårt att ge helt entydiga svar om hur lagen ska tillämpas i konkreta fall. Därutöver är Sverige så sena med den kompletterande lagstiftning som krävs i och med införandet av dataskyddsförordningen att det inte ens har fattats beslut om att anta ens de mest grundläggande lagändringarna. Vissa av de utredningar som gjorts har i skrivandes stund inte ens hunnit leda till någon proposition.

Därför råder fortfarande en osäkerhet kring hur vissa regler ska tillämpas och att man helt enkelt får invänta utvecklingen i praxis. Det finns således en risk att såväl styrdokument och rutiner samt övrigt material som staden producerar för att uppfylla lagens krav kan komma att behöva revideras framöver, allt utifrån den framtida utvecklingen.

I arbetet med förslagen till riktlinjerna har särskild hänsyn tagits till det osäkra rättsläget genom att tjänstepersoner föreslås upprätta särskilda instruktioner. På detta sätt kan en revidering ske enkelt och det ger förutsättningar att snabbt förändra ett arbetssätt som kanske visat sig vara felaktigt.

Ekonomi

De åtgärder som kommer att krävas till följd av införandet av dataskyddsförordningen kan komma att kräva ökade personella resurser. Det kan emellertid ännu inte fastställas hur mycket tid som varje förvaltning kommer att behöva lägga ned på det löpande arbetet som kommer att krävas framöver. Det står åtminstone klart att varje förvaltning måste vidta mer utbildningsinsatser och lägga ner mer resurser på frågor kring hantering av personuppgifter än vad som gjorts under den nuvarande lagstiftningen.

Det ska dock understrykas att de åtgärder som föreslås åläggas nämnderna och förvaltningarna bedöms vara nödvändiga för att såväl nämnderna som staden som helhet ska uppfylla de krav som ställs i dataskyddsförordningen. Antagandet av policyn och riktlinjerna för hantering av personuppgifter medför dock i sig inte några ökade kostnader.

Bedömning

Föreslagen policy med tillhörande riktlinjer bör antas då de utgör ger en god förutsättning för att stadens nämnder och förvaltningar att uppfylla kraven i dataskyddsförordningen. Vidare sätter riktlinjerna en sådan ram kring arbetet med hanteringen av personuppgifter att det läggs en grund för förvaltningarna att arbeta på ett likriktat sätt när det gäller uppfyllnaden av dataskyddsförordningen. Riktlinjerna utgör även ett sådant instrument för intern kontroll av att reglerna i dataskyddsförordningen följs över tid vilket i sig är något som ska säkerställas löpande.

Expedieras till

Samtliga nämnder, bolagen

Carina Nordgren Henriette dé Mare

Bilagor

Bilaga 1 – Förslag till Policy för hantering av personuppgifter
Bilaga 2 – förslag till Riktlinjer för hantering av personuppgifter

Policy för hantering av personuppgifter

Inledning och syfte

Syftet med Mölndals stads policy för hantering av personuppgifter är att säkerställa att

- de som vänder sig till Mölndals stad ska kunna känna sig trygga med att deras personuppgifter hanteras på ett respektfullt sätt,
- staden inte hanterar personuppgifter i onödan och
- att de personuppgifter som staden hanterar inte riskerar att hamna i orätta händer

Policyn omfattar samtliga nämnder i Mölndals stad och utgör ett komplement till gällande lagstiftning som reglerar behandling av personuppgifter.

Kommunstyrelsens uppgift

Av det nämndgemenensamma reglementet framgår att varje nämnd är personuppgiftsansvarig enligt dataskyddsförordningen för de personuppgifter som behandlas i nämndens verksamhet.

Kommunstyrelsen ska leda, samordna och ha uppsikt över stadens arbete med att uppfylla kraven i Allmänna dataskyddsförordningen EU 2016/679 och de nationella dataskyddsbestämmelserna. Kommunstyrelsen ska utfärda riktlinjer för att säkerställa att staden hanterar personuppgifter på ett lagenligt sätt.

Kommunstyrelsen har till uppgift att tydligt definiera ansvaret kommunstyrelsen och de övriga nämnderna emellan avseende de personuppgifter som behandlas för en annan nämnds vägnar, alternativt då ett gemensamt personuppgiftsansvar föreligger. I åliggandet ingår att även att fastlägga de särskilda säkerhetsinstruktioner som ska iakttas vid respektive personuppgiftsbehandling samt att beakta att tillämpliga krav i dataskyddsförordningens art. 26 och 28 uppfylls.

Organisatoriska och tekniska förutsättningar

Vid planering av stadens olika verksamheter ska säkerställas att det ges såväl organisatoriska som tekniska förutsättningar att uppfylla de krav som gäller enligt gällande lagstiftning

Kontroll över personuppgiftsbehandlingar

Mölndals stad ska ha kontroll över verksamhetens behandling av personuppgifter.

Registrerades rättigheter

Mölndals stad ska vara tillmötesgående och förberedd på att hjälpa de registrerade att tillvarata sina rättigheter enligt dataskyddsförordningen.

Styrdokument Policy	**Beslutat av** Kommunfullmäktige datum	**Gäller från och med** 2018-05-25
Ansvarig Stadsjurist	**Gäller för** Mölndals stad	**Senast uppdaterat**

Riktlinjer för hantering av personuppgifter

Inledning och syfte

Mölndals stads riktlinjer för hantering av personuppgifter är ett komplement till stadens policy för hantering av personuppgifter. Riktlinjerna gäller för stadens samtliga nämnder.

Policyn och riktlinjernas syfte är dels att säkerställa att staden hanterar personuppgifter på ett lagenligt sätt men också att visa för allmänhet och anställda att de kan känna sig trygga med att deras personuppgifter hanteras på respektfullt sätt och att inga personuppgifter hanteras i onödan eller riskerar att hamna i orätta händer.

Riktlinjerna är en del av stadens interna regelverk och utgör inte en utfästelse som riktar sig externt.

Organisatoriska och tekniska förutsättningar

Ur policyn för hantering av personuppgifter
Vid planering av stadens olika verksamheter ska säkerställas att det ges såväl organisatoriska som tekniska förutsättningar att uppfylla de krav som gäller enligt gällande lagstiftning.

Av det nämndgemenensamma reglementet framgår att varje nämnd är personuppgiftsansvarig enligt dataskyddsförordningen för de personuppgifter som behandlas i nämndens verksamhet.

Varje nämnd ska säkerställa att det finns såväl organisatoriska som tekniska förutsättningar inom den egna förvaltningen för att uppfylla de krav som ställs på personuppgiftsansvariga i dataskyddsförordningen.

Varje förvaltning ska kunna visa att den innehar rätt resurser och relevant kompetens inom området för att kunna följa dataskyddsförordningen, de nationella dataskyddsbestämmelserna samt dessa riktlinjer.

Central organisation

Kommunstyrelsens dataskyddsombud ska samordna de övriga nämndernas dataskyddsombud.

Nämnderna ska årligen rapportera sitt arbete enligt dessa riktlinjer, dataskyddsförordningen och övriga dataskyddsbestämmelser till kommunstyrelsen. Mer utförliga instruktioner för nämndernas årliga rapportering framgår av anvisningar från kommunstyrelsens dataskyddsombud.

Stadens dataskyddsombud ska sammanträda gemensamt minst fyra gånger årligen. Sammanträdena ska sammankallas och ledas av kommunstyrelsens dataskyddsombud.

Kommunstyrelsens dataskyddsombud ansvarar vidare för att

- Hålla den information om stadens hanteringa av personuppgifter som ska finnas på stadens hemsida uppdaterad.
- Hålla kontaktuppgifter till nämndernas dataskyddsombud uppdaterade på stadens hemsida samt meddela dessa till tillsynsmyndigheten.
- Samla in och sammanställa nämndernas årliga rapportering.
- Identifiera förekomsten av generella svårigheter och problem i förvaltningarna och ta fram förslag till lämpliga åtgärder.
- Administrera och fortlöpande uppdatera ansvarsfördelningen samt särskilda säkerhetsinstruktioner mellan Mölndals stads nämnder (inkl. kommunstyrelsen) avseende de personuppgifter som behandlas för en annan nämnds vägnar, alternativt då ett gemensamt personuppgiftsansvar föreligger två eller flera nämnder emellan.

Dataskyddsombud

Varje nämnd ska utnämna ett dataskyddsombud som ska rapportera direkt till förvaltningsledningen. Vid val av dataskyddsombud ska särskilt beaktas att det inte föreligger intressekonflikter gentemot andra uppdrag som denne eventuellt innehar.

En rekommendation är att dataskyddsombudet bjuds in till förvaltningens ledningsgrupp för avrapportering vid minst två tillfällen per år.

Nämnden ska upprätta en uppdragsbeskrivning över dataskyddsombudets uppgifter.

Förvaltningsledningen ska säkerställa att dataskyddsombudet involveras och rådfrågas på ett så tidigt stadium som möjligt när behandling av personuppgifter kan komma ifråga.

Dataskyddsombudet ska årligen redovisa för nämnden det arbete som förvaltningen för gällande uppfyllnaden av reglerna i dessa riktlinjer, dataskyddsförordningen och annan lagstiftning på området. Av den årliga redovisningen ska som minst framgå

- Vilka interna och externa utbildningsåtgärder som förvaltningen genomfört på området
- Vid vilka ledningsgruppsmöten som dataskyddsombudet har beretts tillfälle närvara vid för att avlägga rapport över förvaltningens hantering av personuppgifter
- Tekniska brister som åtgärdats under året
- Tekniska brister som bör åtgärdas
- Eventuella personuppgiftsincidenter

Kommunstyrelsens dataskyddsombud ska, tillsammans med redovisningen av den egna förvaltningens arbete, återrapportera en sammanställning av de övriga förvaltningarnas årliga redovisningar till kommunstyrelsen.

Tjänster, produkter och applikationer som medför behandling av personuppgifter

För varje tjänst, produkt och applikation som används eller som det finns planer på att använda ska särskilt beaktas om avtalsförhållandet eller användandet av produkten eller applikationen kan komma att medföra behandling av personuppgifter. För det fall personuppgifter kommer att behandlas ska, med hänsyn till den tekniska utvecklingen, säkerställas att det finns tekniska förutsättningar för såväl förvaltningen som för dess personuppgiftsbiträde att kunna fullgöra sina

skyldigheter avseende dataskydd.

Särskilt vid inköp och upphandling
Vid inköp och upphandlingar (av produkter och tjänster) ska särskilt utredas om användandet av det som inköpet avser eller annars som en följd av avtalsrelationen kan komma att leda till behandling av personuppgifter. Förvaltingen ska ha en rutin för under vilka förutsättningar dataskyddsombudet ska engageras vid inköp och upphandlingar och när under inköpsprocessen som denne bör kontaktas.

Vid inköp och upphandlingar av produkter och tjänster som kan komma att leda till behandling av personuppgifter ska krav ställas på att all utrustning lever upp till kraven i dataskyddsförordningen och annan lagstiftning inom dataskyddsområdet.

Vid utredning av vilka säkerhetskrav som bör ställas ska, vid behov, samråd ske med IT-avdelningen.

Konsekvensbedömning avseende dataskydd

Om en ny typ av behandling kan komma att leda till att registrerades rättigheter och friheter riskeras ska en bedömning av den planerade behandlingens konsekvenser utföras.

Konsekvensbedömningen ska hanteras i enlighet med instruktioner som finns avseende riskanalyser för informationssäkerhet. Informationssäkerhetssamordnaren ska rådfrågas vid en konsekvensbedömning.

Incidentrapportering

Varje förvaltning ska kunna upptäcka, hantera och rapportera personuppgiftsincidenter som sker inom den egna verksamheten. Varje förvaltning ska ha en rutin där det framgår hur en personuppgiftsincident ska hanteras internt för att rapporteringen till tillsynsmyndigheten ska kunna göras inom 72 timmar från upptäckt.

Personuppgiftsincidenter ska omedelbart rapporteras både till stadsledningsförvaltningen och till tillsynsmyndigheten. Om rapporteringen till tillsynsmyndigheten görs efter det att 72 timmar förflutit från det att personuppgiftsincidenten upptäcktes ska förseningen motiveras. Rapportering till tillsynsmyndigheten behöver emellertid inte göras om det är osannolikt att incidenten kan komma att medföra en risk för de registrerades rättigheter och rättigheter.

Alla personuppgiftsincidenter ska registreras centralt.

Personuppgiftsincidenter ska i övrigt hanteras i enlighet med de instruktioner som finns avseende informationssäkerhetsincidenter.

Säkerhet i samband med behandlingen

Varje nämnd ansvarar för att en fullgod säkerhetsnivå upprätthålls vid behandling av personuppgifter. Förvaltningen ska vidta lämpliga tekniska och organisatoriska åtgärder för att

säkerställa en säkerhetsnivå utifrån de kriterier som anges i dataskyddsförordningen.

Vid planering av verksamheten ska särskild hänsyn tas till att personuppgifter inte behandlas i högre utsträckning eller under längre tid än vad som är nödvändigt. Anställda som på något sätt kan komma att behandla personuppgifter i sitt arbete ska genomgå utbildning för att säkra att personuppgifter hanteras på ett lagligt och respektfullt sätt.

Mer utförliga instruktioner för vad som särskilt ska beaktas gällande säkerhet i samband med behandlingen framgår av instruktioner från informationssäkerhetssamordnaren.

Kontroll över personuppgiftsbehandlingar

Ur policyn för hantering av personuppgifter
Mölndals stad ska ha kontroll över verksamhetens behandling av personuppgifter.

Stadens nämnder ansvarar för att av de personuppgifter som behandlas inom ramen för dess verksamhet sker på ett lagenligt sätt.

Register över personuppgiftsbehandlingar

Varje nämnd ska löpande föra ett register över vilka personuppgifter som behandlas i den egna verksamheteten

Registret ska föras utifrån instruktioner från stadsledningsförvaltningen och ska årligen rapporteras in till stadsledningsförvaltningen.

Mer utförliga instruktioner gällande registret framgår av anvisningar från kommunstyrelsens dataskyddsombud.

Personuppgiftsbiträdesavtal och gemensamt personuppgiftsansvar

Personuppgiftsbiträdesavtal

Varje nämnd ska teckna personuppgiftsbiträdesavtal när denne uppdrar åt ett externt personuppgiftsbiträde att behandla uppgifter.

Förvaltningarna ska föra en förteckning över aktuella personuppgiftsbiträdesavtal och därtill hörande underbiträdesavtal.

Avtal vid gemensamt personuppgiftsansvar

För de fall där det föreligger ett gemensamt personuppgiftsansvar med en extern part ska nämnden tillse att det tecknas ett avtal där de personuppgiftsansvarigas respektive ansvar för att fullgöra skyldigheterna enligt dataskyddsförordningen och andra nationella dataskyddsbestämmelser fastställs.

Förvaltningarna ska föra en förteckning över aktuella avtal som styr upp gemensamma personuppgiftsansvar.

Personuppgiftsbiträdesavtal och gemensamt personuppgiftsansvar mellan stadens nämnder
Stadsledningsförvaltningen ska administrera en förteckning över ansvarsfördelningen och de särskilda säkerhetsinstruktioner mellan Mölndals stads nämnder (inkl. kommunstyrelsen) avseende de personuppgifter som behandlas för en annan nämnds vägnar, alternativt då ett gemensamt personuppgiftsansvar föreligger två eller flera nämnder emellan.

Förteckningen ska uppdateras löpande men ska som minst godkännas årligen av kommunstyrelsen.

Registrerades rättigheter

Ur policyn för hantering av personuppgifter
Mölndals stad ska vara tillmötesgående och förberedd på att hjälpa de registrerade att tillvarata sina rättigheter enligt dataskyddsförordningen.

Information till de registrerade
Varje förvaltning ska ha rutiner för hur information ska tillhandahållas till de registrerade.

Tillgång, rättelse, radering och begränsning
Varje förvaltning ska ha rutiner för hantering av begäranden från registrerade om att utöva sina rättigheter att

- Få tillgång till information om dennes personuppgifter.
- Rätta eller komplettera sina uppgifter.
- Rader sina uppgifter
- Begränsa sina uppgifter
- Utnyttja möjligheten till dataportabilitet om sådan möjlighet finns.