Stenungsunds kommun

Policy för personuppgifts-behandling

i Stenungsunds kommun

Typ av dokument Policy	**Beslutat av** Kommunfullmäktige	**Beslutsdatum** 2018-10-08	**Diarienummer** 2018/333
Dokumentägare Kansliet	**Giltighetstid**	**Framtagen av** Kansliet	**Reviderad**

1. Inledning

1.1 Om Policy för personuppgiftsbehandling i Stenungsunds kommun

EU:s dataskyddsförordning (nr 679/2016) (GDPR) och kompletterande svensk dataskyddslagstiftning reglerar hur och för vilka ändamål personuppgifter får behandlas och ska tillämpas av Stenungsunds kommun samt av kommunens bolag. Syftet med GDPR är att skydda den enskildes personliga integritet när personuppgifter behandlas av myndigheter och andra organisationer.

Personuppgifter behandlas inom Stenungsunds samtliga verksamheter för att utföra kommunens uppdrag. GDPR ställer krav på organisationens förhållningssätt till den personliga integriteten när personuppgifter behandlas i verksamheten och innebär att kontinuerliga åtgärder ska vidtas.

Denna policy har tagits fram som ett led i Stenungsunds anpassning till GDPR:s nya krav och gäller för kommunens nämnders verksamheter samt för kommunens bolag. Denna policy anger kommunens förhållningssätt till dataskyddslagstiftningen vid behandling av personuppgifter i kommunen och bolagens verksamheter och är vägledande för beslut och styrning.

Med begrepp som används i denna policy avses betydelsen enligt GDPR och annan tillämplig dataskyddslagstiftning. Behandling av personuppgifter innefattar all slags automatiserad hantering av uppgifter om en direkt, eller indirekt, identifierbar fysisk person som registreras i kommunens verksamhet. Manuell hantering omfattas när den ingår i ett register eller kommer att ingå i ett register.

1.2 Personuppgiftsansvarig

Respektive kommunal nämnd, såväl myndighetsnämnder som övriga nämnder, kommunstyrelsen samt kommunens bolag är personuppgiftsansvariga och har därmed det yttersta ansvaret för att GDPR och kompletterande svensk lagstiftning för behandling av personuppgifter efterlevs inom den egna verksamheten.

Det organisatoriska ansvaret för att personuppgifter i Stenungsunds kommun behandlas i enlighet med tillämplig dataskyddslagstiftning följer dels av det delegerade verksamhetsansvaret, dels ansvaret som följer med informationsägarskap. Det här innebär att varje anställd som är ansvarig för en verksamhet, eller får ett delegerat verksamhetsansvar, också är ansvarig för att behandling av personuppgifter i verksamheten utförs i enlighet med GDPR och svensk kompletterande lagstiftning för behandling av personuppgifter.

1.3 Syfte

Syftet med denna policy för behandling av personuppgifter inom Stenungsunds kommun är att säkerställa att dataskyddsarbetet utgör en integrerad del i kommunens verksamheter och i de kommunägda bolagens verksamheter. Policyn är en grund för kommunens hantering av personuppgifter och kompletteras av tillämpliga rutiner.

Policyn syftar till att uppnå följande mål:

- Behandling av personuppgifter inom kommunens verksamheter utförs med utgångspunkt i den enskildes personliga integritet och rättigheter.

- Kommunen hanterar personuppgifter i enlighet med såväl gällande lagar som kommunens riktlinjer och rutiner.

- Följsamhet till GDPR utgör en integrerad del i kommunens verksamhetskultur.

- Invånare och andra personer som vänder sig till Stenungsunds kommun känner sig trygga med att deras personuppgifter hanteras med beaktande av den personliga integriteten.

- Inga personuppgifter hanteras i onödan eller riskerar att hamna i orätta händer.

2. Policy för hantering av personuppgifter

2.1 Principer för behandling av personuppgifter

Vid behandling av personuppgifter ska ett förhållningssätt iakttas som innebär att gällande lagstiftning för personuppgiftsbehandling ska följas och att risken för skada för den registrerades personliga integritet minimeras.

Behandling av personuppgifter inom kommunens verksamheter, eller på uppdrag av Stenungsunds kommun, ska ske med utgångspunkt i de grundläggande principerna som anges i GDPR. Nedan framgår principerna enligt GDPR och kommunens övergripande förhållningssätt:

Princip om laglighet, korrekthet och öppenhet
Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till dem som personuppgifterna berör.

Med detta menas att Stenungsunds kommun alltid ska se till att personuppgifter behandlas med stöd av ett lagligt ändamål och att annan lagstiftning som inverkar på informationen efterlevs. Kommunen ska alltid ha avvägningen mellan den registrerades integritet och den egna verksamhetens effektivitet i åtanke. Den vars personuppgifter behandlas ska ges möjlighet till insyn i hanteringen när sådan kan ske på ett pedagogiskt sätt och uppgifter ska alltid hanteras med hänsyn tagen till den registrerades integritet.

Princip om ändamålsbegränsning
Uppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Med detta menas att Stenungsunds kommun känner till och dokumenterar anledningen till att en viss personuppgift hanteras och personuppgifterna inte används för en helt annan anledning som går emot den ursprungliga.

Princip om uppgiftsminimering
Uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Med detta menas att Stenungsunds kommun endast ska använda sig av de personuppgifter som krävs för att uppnå målet med hanteringen av personuppgifterna. Kan samma mål uppnås genom att använda färre personuppgifter, eller mindre känsliga personuppgifter, ska så ske.

Princip om korrekthet
Uppgifter ska vara korrekta och om nödvändigt uppdaterade. Åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga raderas eller rättas utan dröjsmål.

Med detta menas att Stenungsunds kommun måste verka för att personuppgifter som är felaktiga rättas. Verksamhetsspecifika bestämmelser, som inom hälso- och sjukvård, ska beaktas vid rättning av uppgifter.

Princip om lagringsminimering
Identifierbara uppgifter får inte förvaras under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Med detta menas att personuppgifterna inte får sparas längre än vad som behövs utifrån syftet med att de samlades in. När syftet är uppnått ska de gallras eller avidentifieras med beaktande av de bevarande- och gallringsregler som gäller för Stenungsunds kommun.

Princip om integritet och konfidentialitet
Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Med detta menas att personuppgifter ska skyddas genom tekniska och organisatoriska åtgärder på en nivå som motsvarar uppgifternas skyddsvärde. Är uppgifterna av särskilt skyddsvärd art ska också högre tekniska och organisatoriska krav ställas. Utgångspunkten ska vara att endast behöriga personer ska ges tillgång till skyddsvärd information.

Princip om ansvarsskyldighet
Den personuppgiftsansvarige ska ansvara för och kunna visa att de nu nämnda grundläggande principerna enligt GDPR efterlevs.

Med detta menas att det ska finnas en förmåga att öppet och tillgängligt kunna visa GDPR efterlevs.

2.2 Organisatoriska och tekniska förutsättningar
Vid planering av kommunens verksamhet ska kontinuerligt säkerställas och särskilt beaktas att det ges såväl organisatoriska som tekniska förutsättningar att uppfylla krav enligt gällande lagstiftning för personuppgiftsbehandling.

2.3 Kontroll över personuppgiftsbehandlingar
För att uppnå följsamhet till GDPR ska Stenungsunds kommun ha kontroll över hur personuppgifter hanteras av kommunens verksamheter och vilka krav som hanteringen

omfattas av enligt den lagstiftning som är tillämplig på personuppgiftsbehandlingen vid den aktuella verksamheten.

2.4 GDPR och offentlighetsprincipen

Offentlighetsprincipen innebär en rätt för var och en att hos Stenungsunds kommun ta del av allmänna handlingar. Detta innebär att även personuppgifter kan begäras och lämnas ut som en del av allmän handling oavsett för vilket ändamål personuppgiften ursprungligen behandlades. Denna rätt gäller dock inte om handlingarna innehåller uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Detta innebär att personuppgifter som förekommer i allmänna handlingar skyndsamt ska lämnas ut på begäran, om de inte omfattas av sekretess.

2.5 Känsliga personuppgifter och skyddsvärda personuppgifter

Känsliga uppgifter enligt GDPR är; uppgifter om ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter eller biometriska uppgifter.

Vid behandling av känsliga uppgifter i kommunens verksamhet ska särskilt säkerställas att det finns stöd i lag och att rätt säkerhetsnivå iakttas.

Enligt GDPR är personnummer och samordningsnummer särskilt skyddsvärda uppgifter och ska endast hanteras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Innan personuppgifter och samordningsnummer används i kommunens verksamhet ska en avvägning göras av om syftet med hanteringen kan uppnås utan att dessa uppgifter används.

2.7 Säkerhetsåtgärder i samband med behandling av personuppgifter

Vid planering av kommunens verksamhet, särskilt vid upphandling och användning av IT-system, ska GDPR:s krav på lämpliga tekniska och organisatoriska åtgärder beaktas för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för de registrerades rättigheter vid behandling av personuppgifter. Uppgifternas karaktär av känslighet ska beaktas vid val av säkerhetsåtgärd.

2.8 Registrerades rättigheter

Stenungsunds kommun ska tillmötesgå och hjälpa invånare, och andra registrerade vars personuppgifter behandlas av kommunen, att ta tillvara sina rättigheter enligt GDPR.