KS § 22 D.nr. KS/2021:632 - 003

Uppföljning av Program för efterlevnad av dataskyddsförordningen

Beslut

Kommunstyrelsen föreslår kommunfullmäktige besluta att

1. upphäva tidigare beslut om program för efterlevnad av dataskyddsförordningen, KF § 329, 2020-11-23,
2. anta uppdaterat program för efterlevnad av dataskyddsförordningen daterat 2021-11-29,
3. programmet ska gälla från och med den 1 maj 2022.

Beslutsgång

Ordföranden finner att det endast finns ett förslag till beslut och att det blir kommunstyrelsens beslut.

Beskrivning av ärendet

EU:s dataskyddsförordning, nedan GDPR, reglerar hur personuppgifter ska behandlas med syftet att skydda den enskildes (den registrerades) rättigheter, med fokus på integritetsskydd. Förordningen tillämpas på behandling av helt eller delvis automatiserad personuppgiftsbehandling och på behandling av personuppgifter som ingår i eller kommer att ingå i ett register, i EU-s medlemsländer.

Strängnäs kommun tog fram ett förslag till program för efterlevnad av dataskyddsförordningen, och som sen antogs av kommunfullmäktige 2020-11-23, § 329, dnr KS/2020:531.

I det program som togs fram valde man att skriva in att en årlig uppföljning skall göras. Utifrån den görs nu en revidering av tidigare antaget program. Det innebär mest redaktionella ändringar, så som att datainspektionen bytt namn till integritetsskyddsmyndigheten samt att vi valt att tydliggöra genom att kalla våra tjänstepersoner som jobbar med dessa frågor för dataskyddskoordinator och dataskyddssamordnare istället för tidigare GDPR-koordinator/samordnare. I denna revidering görs skrivningen ”följs upp vid behov” istället för årligen utifrån att vi gått från en införandefas till ett normalläge avseende riktlinjerna för GDPR. I övrigt så följer programmet de riktlinjer som tidigare redan fanns.

Ekonomiska konsekvenser för kommunen

Beslutet medför inga ekonomiska konsekvenser för kommunen.

Övriga konsekvenser
Beslutet medför inga övriga konsekvenser.

Uppföljning
Programmet ska följas upp vid behov.

Beslutsunderlag
Tjänsteutlåtande, Uppföljning av program för efterlevnad av dataskyddsförordningen, 2021-11-30
Styrdokument, Program för efterlevnad av dataskyddsförordningen (GDPR), förslag, 2021-11-29

Beslutet skickas till
Kommunfullmäktige
Socialnämnden, för kännedom
Barn- och utbildningsnämnden, för kännedom
Teknik och fritidsnämnden, för kännedom
Miljö- och samhällsbyggnadsnämnden, för kännedom
Kulturnämnden, för kännedom
Valnämnden, för kännedom
SKFAB, för kännedom
Kommunrevisionen, för kännedom

Beslutad:	åååå-mm-dd § xx
Myndighet:	Kommunfullmäktige
Diarienummer:	KS/2021:632-003
Ersätter:	Program för efterlevnad av dataskyddsförordningen beslutad av KF 2020-11-23 § 329
Gäller för:	Alla nämnder och förvaltningen
Gäller fr o m:	2022-xx-xx
Gäller t o m:	Tillsvidare
Dokumentansvarig:	Kansliavdelningen
Uppföljning:	~~Årligen~~ Vid behov

Program för efterlevnad av dataskyddsförordningen, GDPR

Bakgrund

EU:s dataskyddsförordning, nedan GDPR, reglerar hur personuppgifter ska behandlas, med fokus på integritetsskydd. Förordningen tillämpas på behandling helt eller delvis automatiserad personuppgiftsbehandling och på behandling av personuppgifter som ingår i eller kommer att ingå i ett register, i EU-s medlemsländer.

Dataskyddsförordningen innebär bland annat att varje nämnd i Strängnäs kommun är personuppgiftsansvarig inom sitt verksamhetsområde och den personuppgiftsansvarige ska följa de grundläggande principer som stadgas i förordningen.

Principerna innebär i korthet att personuppgiftsansvarig bland annat:

- Måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- Bara får samla in personuppgifter för specifika, särskilt angivna berättigade ändamål
- Inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- Ska se till att personuppgifterna är riktiga
- Ska radera personuppgifterna när de inte längre behövs
- Ska skydda personuppgifterna till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs

- Ska kunna visa att och hur nämnden lever upp till regleringen i dataskyddsförordningen

Syfte med programmet

Syftet med programmet är att säkerställa det finns en struktur som bidrar till att Strängnäs kommun lever upp till dataskyddslagstiftningens krav och att skapa tydlighet i ansvaret för frågorna inom den kommunala organisationen.

Kopplingar till annan lagstiftning och andra nationella styrdokument

Det finns även andra lagar som samspelar direkt med regleringen i GDPR. Viktiga exempel på sådan reglering är:

- Tryckfrihetsförordningen
- Offentlighets- och sekretesslag (2009:400)
- Arkivlagen (1990:782)
- Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).
- Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning
- Lag (2001:454) om behandling av personuppgifter inom socialtjänsten (SoLPuL).
- Förordning (2001:637) om behandling av personuppgifter inom socialtjänsten.
- Patientdatalagen (2008:355)
- Patientdataförordning (2008:360)

Exempel på andra rättskällor som på ett tydligt sätt påverkar kommunens arbete med dataskyddsförordningen är vägledningar från Europeiska dataskyddsstyrelsen samt praxis från EU-domstolen, europeiska dataskyddstillsynsmannen, ~~Datainspektionen~~ Integritetsskyddsmyndigheten (IMY) och svenska domstolar.

Kopplingar till andra interna styrande och vägledande dokument mm

Tillsammans med detta program tillämpas övriga av kommunen beslutade dokumenthanteringsplaner och övriga styrdokument på området.

Vägledande dokument utarbetas utifrån lagstiftningen, detta program och övriga beslutade styrdokument.

Mål

Målet för Strängnäs kommuns arbeta utifrån GDPR är att säkerställa att enskilda personers integritet skyddas samtidigt som kommunen och dess olika nämnder kan utföra sina respektive uppdrag på ett effektivt sätt. Det ska gå att vid behov visa för tillsynsmyndighet att regleringen följts.

Varje nämnd kan välja att specificera mål och delmål ytterligare, för att tydliggöra kravet på förvaltningens service utifrån sin myndighetsroll och lagens krav.

Ansvar och organisation av arbetet i Strängnäs kommun

Varje nämnd är personuppgiftsansvarig inom sitt respektive verksamhetsområde, enligt lag och respektive reglemente.

Kommundirektören är ansvarig för hur arbetet i förvaltningen samordnas och organiseras, i syfte att uppnå ovanstående mål.

Vid varje kontor ska det finnas en dataskydds-samordnare som har en samordnande roll i förhållande till det arbete som bedrivs inom respektive nämnds ansvarsområde.

Vid kansliavdelningen under kommunstyrelsen ska det finnas en dataskydds-koordinator som samordnar arbetet kring utformningen av vägledande dokument och rutiner inom förvaltningen och stöder dataskydds-samordnarna i deras arbete.

Åtgärder

I detta kapitel beskrivs grundläggande åtgärder som krävs för att regleringen ska följas, indelade efter område. Andra verktyg som kan användas är de handböcker och rutiner som är utarbetade vid förvaltningen

Dataskyddsombud

Den personuppgiftsansvarige kan utnämna ett dataskyddsombud och måste göra det om personuppgiftsbehandlingen utförs av ett offentligt organ eller en myndighet. En koncern får utnämna ett dataskyddsombud om det på varje verksamhetsställe är lätt att nå dataskyddsombudet. Dataskyddsombudet får ingå i den personuppgiftsansvariges personal eller utföra uppgifterna på grundval av ett tjänsteavtal, se också artikel 37 GDPR. Dataskyddsombudets ställning och uppgifter regleras i artikel 38 GDPR. Europeiska dataskyddsstyrelsen (tidigare artikel 29-gruppen) har utfärdat riktlinjer på området. Centralt är att dataskyddsombudet ska ha en i förhållande till personuppgiftsansvariges övriga arbete med dataskydd självständig ställning och rapportera direkt till högsta förvaltningsledningen.

Varje nämnd måste ha ett utsett ett dataskyddsombud, d v s det måste finnas ett beslut på vem som är dataskyddsombud mot respektive personuppgiftsansvarige.

Förvaltningen ska säkerställa att det finns tillgång till ett för nämnderna, kommunrevisorerna och Strängnäs kommunföretag AB gemensamt dataskyddsombud, som ska ha en självständig ställning i sitt granskande uppdrag och som varje organ kan anlita.

Dataskyddsombudet ska ha följande uppgifter:

- Vara ett kunskapsstöd inom kommunerna gällande dataskyddsförordningen och annan tillämplig dataskyddslagstiftning
- Övervaka den interna efterlevnaden av dataskyddsförordningen och annan tillämplig dataskyddslagstiftning, vid behov genomföra granskningar
- Tillsammans med sakkunniga inom kommunen ställa krav och arbeta för att förvaltningen inför säkerhetsåtgärder, inom dataskydd
- Bistå i utredning av misstänkt dataintrång
- Ge råd vid konsekvensbedömningar av dataskydd och övervaka genomförandet av dem
- Arbeta med omvärldsbevakning kunskapsinhämtning rörande dataskyddslagstiftning

Dataskyddsombudet ska inte ha del i beslut eller slutligt underlag till beslut om styrande och stödjande dokument eller beslut i enskilda ärenden, men kan lämna råd i förvaltningens arbete.

Dataskyddsombudet ska rapportera direkt till respektive nämnd och ha en, i förhållande till förvaltningen, självständig ställning.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Personuppgiftsbiträdets roll i förhållande till personuppgiftsansvarig regleras i kapitel IV, GDPR De biträden som den personuppgiftsansvarige anlitar ska kunna ge garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Förvaltningen ska tillgodose att det finns personuppgiftsbiträdesavtal då någon annan behandlar personuppgifter för nämndens räkning. Personuppgiftsbiträdesavtalen ska i största möjliga utsträckning utgå från SKR:s mall för personuppgiftsbiträdesavtal.

Personuppgiftsbiträdesavtalen ska hållas ordnade på ett sätt som gör att det går att sammanställa vilka personuppgiftsbiträdesavtal som tecknats för respektive personuppgiftsansvarigs räkning.

Personuppgiftsbiträdesavtal ska följas upp ~~årligen, samt om~~ vid behov och särskilt när det finns indikationer på att personuppgiftsbiträdet inte behandlar

personuppgifter som överförs från nämnden, i enlighet med avtalet och instruktioner till avtalet.

Förteckning över behandling av personuppgifter

GDPR tillämpas på helt eller delvis automatiserad personuppgiftsbehandling och på behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Varje personuppgiftsansvarig ska ha en förteckning över de behandlingar som utförs åt nämnden. Vilka uppgifter som ska ingå i förteckningen framgår av artikel 30, GDPR.

Att det finns uppdaterade förteckningar är av grundläggande betydelse för nämndernas möjlighet att följa övriga bestämmelser i dataskyddsförordningen. Krav ställs därför på satt:

- Det ska finnas en förteckning över behandlingar av personuppgifter för varje personuppgiftsansvarigt organ (exempelvis för varje nämnd).
- Förteckningen ska innehålla de uppgifter som krävs enligt GDPR (artikel 30).
- Förteckningen ska uppdateras vid behov (när nya behandlingar/register införs) och den ska följas upp vid behov.

Den registrerades rättigheter

Dataskyddsförordningen ger de registrerade rättigheter vad gäller behandling av personuppgifter. Det är personuppgiftsansvariges ansvar se till att processer för att tillmötesgå de registrerade så att de kan tillgodose sina rättigheter finns. Den grundläggande regleringen om rättigheterna finns i artikel 12-20 GDPR.

Det åligger förvaltningen att upprätthålla kunskap om vilka den registrerades rättigheter är och kring befintliga rutiner om hur dessa ska tillgodoses, så att nämnderna kan tillgodose de registrerades rättigheter på sitt respektive område.

Rutiner för behandlande av följande rättigheter ska finnas på plats och uppdateras vid behov.

- Den registrerades rätt till information
- Den registrerades rätt till registerutdrag
- Den registrerades möjlighet till rättelse av felaktiga personuppgifter
- Den registrerades möjlighet att begära att personuppgifter raderas
- Den registrerades möjlighet att begära att behandling av dennes personuppgifter begränsas
- Den registrerades möjlighet att begära att dennes personuppgifter överförs till annan (dataportabilitet)
- Den registrerades möjlighet att göra invändningar

Förvaltningen ska också säkerställa att automatiserat beslutsfattande inte används i strid med GDPR.

Frågor kring uttag av avgift i samband med tillgodoseende av den registrerades rättigheter regleras i separat beslut. (KF/2021-09-27, § 211, dnr KS/2021:131-100)

Säkerhetsåtgärder

En grundläggande bestämmelse angående de avvägningar som ska göras vid införandet av säkerhetsåtgärder finns i artikel 32 GDPR. Personuppgiftsansvarig ska med beaktande av bland annat den tekniska utvecklingen, genomförandekostnaden, och behandlingens art, omfattning, sammanhang och ändamål säkerställa en *säkerhetsnivå som är lämplig i förhållande till risken*.

Säkerhetsincidenter på området, som innebär risker för människors rättigheter och friheter (personuppgiftsincidenter) ska anmälas till Dataskyddsinspektionen. Reglering om hur och när personuppgiftsincidenter ska anmälas finns i artikel 33-34 GDPR samt I Europeiska dataskyddsstyrelsens riktlinjer

Förvaltningen ska vidareutveckla *och* dokumentera arbetssätt som säkerställer att verksamhetssystem som används inom förvaltningen uppfyller kraven i artikel 32 GDPR.

Förvaltningen ska säkerställa att personuppgiftsincidenter hanteras utifrån gällande lagstiftning att inträffade incidenter följs upp och att rutiner för anmälan finns och följs.

Förvaltningen ska tillämpa arbetssätt som säkerställer att behörighetskontroll används för system som innehåller personuppgifter, loggning av åtkomst till personuppgifter.

Förvaltningen ska säkerställa arbetssätt som innebär att obehörig åtkomst till personuppgifter försvåras (inklusive sådana som kan finnas i datorer och mobiltelefoner mm).

Förvaltningen ska säkerställa att personuppgifter inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det ska finnas aktuella dokumenthanteringsplaner som följs.

Förvaltningen ska säkerställa att arbetsverktyg finns på plats, så att gällande regler beträffande tredjelandsöverföringar av personuppgifter följs.

Förvaltningen ska säkerställa att konsekvensbedömningar upprättas om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk vid behandling av personuppgifter.

KF § 329

Dnr KS/2020:531-003

Program för efterlevnad av dataskyddsförordningen

Beslut

Kommunfullmäktige beslutar att

1. anta program för efterlevnad av dataskyddsförordningen GDPR,
2. att programmet ska gälla från och med den 5 december 2020.

Beslutsgång
Ordföranden finner att det endast finns ett förslag till beslut och att detta blir kommunfullmäktiges beslut.

Beskrivning av ärendet
EU:s dataskyddsförordning, nedan GDPR, reglerar hur personuppgifter ska behandlas med syftet att skydda den enskildes (den registrerades) rättigheter, med fokus på integritetsskydd. Förordningen tillämpas på behandling helt eller delvis automatiserad personuppgiftsbehandling och på behandling av personuppgifter som ingår i eller kommer att ingå i ett register, i EU-s medlemsländer.

Strängnäs kommun har ingått i ett samarbete mellan sex sörmländska kommuner. Nämnderna i Strängnäs kommun antog under våren 2019 riktlinjer som skrivits inom ramen för nyssnämnda samarbetet och bygger på att arbetssätt avpassats till det. Avtalet kring samarbetet gäller fram till den 14 november 2020. I samband med att samarbetet upphör föreslås att fullmäktige antar ett program som gäller för samtliga nämnder.

Avsikten är att på att reglera komponenter för att kommunen ska kunna följa GDPR, på en mer övergripande nivå. Skrivningar om det tidigare samarbetet samt delar som utgör ren rättsinformation eller kan regleras i rutiner/handböcker skalas bort.

I det föreslagna programmet lämnas utrymme till nämnderna att anta kompletterande styrdokument, utifrån de grunder som beskrivs i programmet. Det finns också ett pågående arbete inom förvaltningen med att utveckla och vidareutveckla vägledande dokument på området. Dokumenttyperna är av vägledande karaktär.

Ekonomiska konsekvenser för kommunen
Beslutet medför inga ekonomiska konsekvenser för kommunen.

Övriga konsekvenser
Beslutet medför inga övriga konsekvenser.

Uppföljning
Programmet ska följas upp årligen och vid behov.

Beslutsunderlag
Protokollsutdrag, KS § 231 2020-10-28 Program för efterlevnad av dataskyddsförordningen
Tjänsteutlåtande, Program för efterlevnad av dataskyddsförordningen , 2020-10-01.
Program för efterlevnad av dataskyddsförordningen GDPR, förslag.
Riktlinjer för tillämpning av dataskyddsförordningen, beslutade i kommunstyrelsen 2019-02-27 § 24, socialnämnden 2019-02-26 § 20, barn- och utbildningsnämnden 2019-02-26 § 24, teknik- och fritidsnämnden 2019-02-26 § 17, miljö- och samhällsbyggnadsnämnden 2019-02-26 § 23, Kulturnämnden 2019-02-19 § 26 samt valnämnden 2019-03-05 § 17.

Beslutet skickas till
Socialnämnden, för kännedom
Barn- och utbildningsnämnden för kännedom
Teknik och fritidsnämnden för kännedom
Miljö- och samhällsbyggnadsnämnden för kännedom
Kulturnämnden för kännedom
Valnämnden för kännedom
Kommunrevisionen för kännedom