2020-11-16

TJÄNSTESKRIVELSE
Dnr AFN 2020/155

Arbets- och företagsenheten

Efterlevnad dataskyddsförordningen

Förslag till beslut
Arbets- och företagsnämnden noterar informationen.

Sammanfattning av ärendet
Den 27 maj 2020 presenterade Nacka kommuns dataskyddsombud sin årsrapport 2019 för arbets- och företagsnämnden. I rapporten framgår rekommendationer för nämndens efterlevnad av dataskyddsförordningens samtliga krav. I nedanstående ärende presenteras rekommendationerna samt vilka åtgärder som vidtas inom arbets- och företagsnämnden vidtar för ska säkerställa att samtliga krav inom förordningen efterlevs. Åtgärderna omfattar fortsatt systematisk genomgång av samtliga personuppgifts-behandlingar i syfte att riskanalyser, konsekvensbedöma, säkerhetsklassa behandlingarna och system där dataskyddsförordningen så kräver samt säkerställa att informationsplikt och gallringsregler efterlevs. Vidare kommer nämnden fortsatt upprätthålla de redan fungerande rutinerna för hantering av personuppgiftsincidenter och begäran om registerutdrag samt diarieföra de företeckningar över underbiträden som inhämtats från nämndens personuppgiftsbiträden.

Ärendet
Dataskyddsförordningen (GDPR) är den lagstiftning som reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Personuppgift är varje typ av information som kan kopplas till en fysisk person. Varje organisation, oavsett verksamhet, som behandlar personuppgifter i någon omfattning måste därför förhålla sig till dataskyddsförordningens regler. I samband med att dataskyddsförordningen den 25 maj 2018 skulle träda i kraft, fattade stadsledningskontoret beslut om 12 fokusområden (där ett är efterlevnad) för att anpassa kommunens verksamheter till förordningens krav. Ett av dessa områden är efterlevnad. Efterlevnad handlar om att varje nämnd ska kunna visa att dataskyddsförordningens krav följs.

I ett ärende den 27 maj 2020 presenterade Nacka kommuns dataskyddsombud (DSO) sin årsrapport 2019 (AFN 2020/57) för arbets- och företagsnämnden. I rapporten framgår hur nämndens arbete med dataskydd genomförts under år 2019. Rapporten ger också en översiktlig granskning av arbets- och företagsnämnden efterlevnad av förordningen samt rekommendationer för nämndens efterlevnad av dataskyddsförordningens samtliga krav. I detta ärende presenteras därför en planering för hur årsrapportens rekommendationer

och de 12 prioriterade fokusområdena hanteras samt vilka åtgärder som redan vidtagits för att efterleva förordningens krav.

1. Registrera personuppgiftsbehandlingar

Varje personuppgiftsansvarig ska enligt artikel 30 ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, kategorier av registrerade, typer av personuppgifter och lagringstid framgår. Arbets- och företagsnämnden har nio personuppgiftsbehandlingar registrerade. Registerförteckningen bedöms vara komplett och innehåller i stort sett all nödvändig information, endast någon enstaka information fattas.

Hantering för efterlevnad av krav

De uppgifter som fattas kommer i förteckningen kompletteras med den enstaka information som efterfrågas under 2020.

2. Rapportera personuppgiftsincidenter

Varje personuppgiftsansvarig ska ha processer för att upptäcka, utreda, åtgärda och anmäla vissa personuppgiftsincidenter till tillsynsmyndigheten Datainspektionen. Rapporterade incidenter följer rutiner för nämndens avvikelsehantering för att förhindra framtida incidenter.

Hantering för efterlevnad av krav

Arbetet med rapporteringen har utvecklats genom en förbättrad och systematiserad konsekvensanalys vid varje rapportering. I övrigt fortsätter personuppgiftsincidenter att anmälas i enlighet med den välfungerande process som finns centralt och på nämndnivå.

3. Konsekvensbedömning (DPIA)

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska den personuppgiftsansvarige göra en konsekvensbedömning. Konsekvensbedömningens syfte är både att säkerställa att enskildas fri- och rättigheter respekteras och är även ett sätt för den personuppgiftsansvarige att visa att dataskyddslagstiftningen följs.

Rekommendation

Nämnden har genomfört en konsekvensbedömning för handläggning och beslut om ekonomiskt bistånd, men en kartläggning över om fler konsekvensbedömningar krävs har ännu inte gjorts enligt DSO. Nämnden rekommenderas att genomföra konsekvensbedömningar där dataskyddsförordningen kräver det.

Hantering för efterlevnad av krav

Workshopar med riskanalyser, i enlighet med Nacka kommuns riktlinjer och checklista, av nämndens personuppgiftsbehandlingar planeras att genomföras under de inledande månaderna av 2021. Det är ett första steg för att bedöma om fortsatt konsekvensbedömning behöver göras och involverar dataskyddssamordnare, informationsägare, systemägare, systemförvaltare och sakkunnig handläggare.

4. Personuppgiftsbiträdesavtal (PUB-avtal)

Personuppgiftsbiträdesavtal ska tecknas om en personuppgiftsansvarig anlitar en extern part som behandlar personuppgifter åt den personuppgiftsansvariga. Den externa parten är då biträde till den personuppgiftsansvariga och ska genom avtalet förbindas att endast behandla personuppgifter efter instruktioner från den ansvarige. Syftet med avtalet är att säkerställa att enskildas personuppgifter skyddas även när det är någon annan än den personuppgiftsansvarige som behandlar personuppgifterna.

Rekommendation

Nämnden rekommenderas att säkerställa att personuppgiftsbiträdesavtalen uppfyller dataskyddsförordningens krav, särskilt vad gäller information om underbiträden. Detta arbete kan göras i samband med en avtalsuppföljning för att kontrollera att ett biträde även lever upp till kraven på personuppgiftshantering.

Hantering för efterlevnad av krav

En förteckning av underbiträden har inhämtats från nämndens personuppgiftsbiträden för nämndens digitala verksamhetssystem i enlighet med rekommendationen från DSO. Förteckningen ska diarieföras i anslutning till varje enskilt personuppgiftsbiträdesavtal i avsett diarieföringssystem. Därmed är det säkerställt att ingen lagring eller behandling av personuppgifter inom dessa system överförs till ett land utanför EU/EES och dataskyddsförordningens krav vad gäller information om underbiträden efterlevs.

5. Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast får behandlas så länge de behövs för ändamålet. Inom offentlig verksamhet innebär lagringsminimering att det finns ordning och reda bland myndighetens information, att information rensas, arkiveras och gallras. Informationshanteringsplanen är det styrdokument som ska visa vilka allmänna handlingar en verksamhet har och hur dessa ska hanteras.

Hantering för efterlevnad av krav

Nämnden har en informationshanteringsplan som antogs i november 2019 och som revideras minst en gång per år. Senaste uppdatering genomförd under november 2020.

6. Registerutdrag (rätten till tillgång)

Registerutdrag eller rätten till tillgång är en rättighet i dataskyddsförordningen som varje enskild har i förhållande till sina personuppgifter. Rättigheten innebär att varje person har rätt att vända sig till en personuppgiftsansvarig för att få bekräftat om ens personuppgifter behandlas och i så fall få tillgång till dessa. Kommuner hanterar generellt personuppgifter i stor omfattning vilket kräver att det finns utarbetade processer på plats om hur ett registerutdrag ska hanteras.

Hantering för efterlevnad av krav

Nämnden fortsätter att följa Nacka kommuns centrala process för hantering av begäran om registerutdrag vilken följer dataskyddsförordningens krav.

7. E-post

I dataskyddsförordningen finns inte som tidigare i personuppgiftslagen ett undantag för personuppgifter i ostrukturerat material, vilket betyder att även personuppgifter i ett e-postmeddelande omfattas av dataskyddslagstiftning. Detta ställer höga krav på att även hanteringen av e-post följer dataskyddsprinciperna, exempelvis att personuppgifter endast behandlas för specifika syften och inte sparas längre än nödvändigt samt att känsliga personuppgifter skyddas med säkerhetsåtgärder. I Nacka kommun finns en framtagen guide för säker e-posthantering som beskriver hur e-post hanteras på ett säkert och med dataskyddsförordningen förenligt sätt.

Hantering för efterlevnad av krav

Rutinen tas upp kontinuerligt med medarbetare och rutiner för att hantera känsliga och extra skyddsvärda personuppgifter på ett säkert sätt har implementerats och utvecklas. Digitala utbildningar i informationssäkerhet ges alla medarbetare kontinuerligt i Nacka kommuns myndighetsorganisation. Kompletterande kunskapshöjande insatser för medarbetare inom arbets- och företagsnämndens verksamhetsområden planeras att genomföras under våren 2021.

8. Systemsäkerhet

En viktig dataskyddsprincip är integritet och konfidentialitet som handlar om att kunna säkerställa personuppgifternas konfidentialitet (att inga uppgifter röjs för obehöriga), tillgänglighet (att uppgifterna är tillgängliga när de behövs) och riktighet (att uppgifterna är korrekta). En metod för att ta fram krav på ett system som uppfyller dessa aspekter är informationsklassning som visar hur skyddsvärd informationen är utifrån de tre aspekterna. System kan därefter anpassas så att kraven motsvarar informationens skyddsvärde.

Rekommendation

Nämndens samtliga system informationsklassades i början av 2018, men har därefter inte följts upp vilket bör göras regelbundet. På en kommunövergripande nivå pågår ett arbete med systematisk informationssäkerhet där klassning av information ingår.

Nämnden rekommenderas att fortsätta med ett systematiskt informationssäkerhetsarbete genom att följa upp informationsklassningar och genomföra övriga analyser som syftar till att nämndens information omfattas av den säkerhet informationen kräver.

Hantering för efterlevnad av krav

Uppföljning av informationsklassningar genomförs under våren 2021 i workshopar och med stöd av medarbetare vid digitaliseringsenheten och den guide för informationsklassning som Nacka kommun tillhandahåller. Arbete involverar dataskyddssamordnare, systemägare, systemförvaltare, informationsägare, sakkunnig handläggare. En planering för hur detta arbete regelbundet ska genomföras tas fram i samband med detta arbete.

9. Behörighet

Korrekt hantering av behörigheter till system och andra ytor som lagrar personuppgifter är en förutsättning för att inte personuppgifter ska bli tillgängliga för obehöriga (det vill säga att personuppgifternas konfidentialitet skyddas) och för att personuppgifter inte behandlas för olovliga syften. Korrekt hantering av behörigheter betyder att behörighet till personuppgifter ges utifrån användarens behov av att behandla uppgifterna och att dessa behörigheter regelbundet ses över.

Rekommendation

Nämnden har framtagna rutiner för behörigheter till sin information, både för anställda inom nämnden och anordnare externt som har tillgång till informationen. Däremot finns behov av att rutinerna även säkerställer att anställda som inom kommunen byter tjänst också får ändrade behörigheter utifrån sina nya arbetsuppgifter.

Hantering för efterlevnad av krav

En inventering och uppdatering av processer och rutiner för nyanställning och hantering av behörigheter i samband med byte av tjänst och nämnd inom kommunen görs inom ramen för utvecklingen av nämndens ledningssystem för systematiskt kvalitetsarbete.

10. Samtycke

I dataskyddsförordningen skärptes kraven på hur och när samtycke kan användas som stöd för en personuppgiftsbehandling. För offentlig verksamhet betyder det att det numera finns begränsade möjligheter att använda samtycke eftersom ett samtycke måste kunna ges helt frivilligt och en myndighet ofta står i maktpositionen gentemot en enskild. Det har i DSO: s granskningen inte framkommit att nämnden använder samtycke som rättslig grund för att behandla personuppgifter.

11. Informationsplikt

Informationsplikten i dataskyddsförordningen betyder att inga personuppgifter får behandlas utan att en enskild vet om detta, detta krav gäller oavsett om uppgifterna samlas direkt in av en enskild eller från en annan källa. Det finns i förordningen dessutom krav på vilken typ av informationen som ska ges samt att detta ska ske på ett enkelt och lättillgängligt sätt. En stickprovsgranskning av nämndens informationstexter visar att nämnden i majoriteten av fallen ger korrekt information enligt dataskydds-förordningen.

Rekommendation

Säkerställ att alla enskilda erhåller komplett och tydlig information om hanteringen av personuppgifter enligt dataskyddsförordningen krav.

Hantering för efterlevnad av krav

En inventering av nämndens behandlingar av personuppgifter har genomförts. Resultaten av denna visar att det vid enskilda kontakterna mellan handläggare och kund, som till exempel SMS-kontakt och kommunikation med kund via Nacka kommuns webbaserade ärendehanteringssystem Artvise, finns åtgärder som behöver vidtas för att säkerställa eller förtydliga information till enskilde om hur personuppgifterna hanteras.

Åtgärder för efterlevnad av kravet om informationsplikt kommer färdigställas genom att samtliga behandlingar som kräver det uppdateras med tydlig information till den enskilde under 2020. I samband med detta arbete ges kunskapsöverföring om informationsplikten till medarbetarna för att säkerställa att vid detta efterlevs vid förändrade eller nya personuppgiftsbehandlingar.

Ekonomiska konsekvenser

Genom att säkerställa att samtliga regler inom dataskyddsförordningen följs minimeras risken för att nämnden beläggs med sanktionsavgifter från tillsynsmyndigheten.

Konsekvenser för barn

Inga konsekvenser för barn har identifierats.

Pia Stark	Karin Axell	Nina Bäckström
Enhetschef	Tf. enhetschef	Kvalitetsutvecklare
Etableringsenheten	Arbets- och företagsenheten	Etableringsenheten