

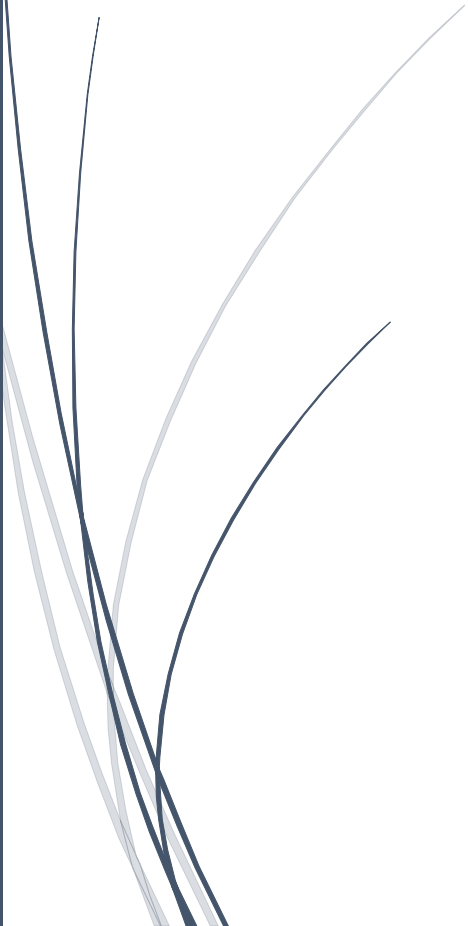


EKERÖ KOMMUN

Dataskydd

Årsrapport 2019

Dnr DPO19/5



Ann-Cathrine Bergström
DATASKYDDSOMBUD
2019-12-19

Bakgrund

Ekerö kommuns hantering av personuppgifter ska ske endast då det finns en laglig grund för att göra detta och då på ett så begränsat sätt som möjligt. Personuppgifter som hanteras ska vara korrekta och det ska vara lätt för utomstående att få insyn i hur hanteringen sker.

Insamlade uppgifter kommer endast att hanteras för det ändamål som uppgivits och lagras endast så lång tid som ändamålet motiverar. Enda undantag från detta är behandling för arkivändamål som motiveras av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

I kommunens processer och digitala lösningar ska ha Dataskydd som standard inbyggt i alla steg genom organisatoriska och tekniska lösningar. Den registrerade ska kunna ta del av de uppgifter som kommunen hanterar och lagrar om personen, rätta felaktiga uppgifter och om det inte strider mot kommunens myndighetsutövning eller andra grundläggande intressen, få uppgifter raderade.

Kommunens dataskyddsombud ska genom fortlöpande kontroller säkerställa att dataskyddet fungerar enligt ovanstående och, om så inte sker, rapportera till personuppgiftsansvariga och kommundirektören samt i vissa fall till dataskyddsmyndigheten (Datainspektionen).

(ur Ekerö kommuns Informationssäkerhetspolicy som antogs av Kommunfullmäktige i april 2018)

Kommunens organisation för dataskyddsfrågor

Personuppgiftsansvarig

Varje nämnd inom Ekerö kommun är personuppgiftsansvarig för sitt verksamhetsområde och har det yttersta ansvaret för att hanteringen av personuppgifter följer den gällande dataskyddslagstiftningen.

Verksamhetsansvarig

Chefer på förvaltnings/enhets/kontorsnivå ansvarar för att personuppgifterna hanteras korrekt inom sitt ansvarsområde. Har ansvar för att behandlingar anmäls, registreras och hålls uppdaterat i vårt förteckningsverktyg Draftit. Ansvarar också för att konsekvensbedömningar (DPIA) är gjorda där det behövs samt att incidenter rapporteras enligt rutin. Minst en dataskyddssamordnare ska utses för att bistå verksamhetsansvarig i detta arbete.

Dataskyddsombud (DPO)

Ett dataskyddsombud är utsett och arbetar idag för Ekerö kommuns samtliga 9 myndigheter (nämnder). Arbetstid som lagts på arbetet under 2019 är ca 60–70% av en heltidstjänst.

Dataskyddsombudet ska utbilda, ge råd och stöd samt övervaka Ekerö kommuns efterlevnad av dataskyddslagstiftningen. Deltar i arbetet runt uppkomna incidenter och är delaktig vid hanteringen av de incidenter som rapporteras in till Datainspektionen.

Dataskyddsbud har även uppdraget att granska efterlevnaden av dataskyddslagstiftningen vilket under året har gjorts via den självskattning som genomförts. Den genomfördes för att DPO och verksamheterna skulle få en överblick över arbetet. Målet var också att få en övergripande bild av hur det ser ut för hela kommunen.

Dataskyddsbudet rapporterar till högsta ledningsnivå och är även kontaktperson för de registrerade och för Datainspektionen.

Dataskyddsbudet är sammankallande till det Dataskyddsnätverk som har startats upp i kommunen.

Dataskyddssamordnare

Samtliga myndigheter utser minst en samordnare som är kontaktperson mellan verksamheten och Dataskyddsbudet. Samordnaren är den som tillsammans med verksamhetsansvarig efterser att arbetet inom nämndens verksamhetsområde sker på ett utifrån dataskyddslagstiftningen säkert sätt.

Samordnaren är den som har hand om den registerförteckning som ska finnas i Draftit. Tillsär (tillsammans med verksamhetsansvarig) att förteckningen är upprättad, inmatad och hålls aktuell.

Samordnaren är aktiv och deltar i det dataskyddsnätverk som finns inom kommunen.

Är behjälplig med att upprätta verksamhetsspecifika rutiner.

Vad har hänt under 2019

Kunskap och utbildning

Under året har DPO haft 7 utbildningstillfällen där samtliga anställda haft möjlighet att anmäla sig. De har varit fullbokade och deltagande har skett från många olika verksamheter inom kommunen. Tanken är att fortsätta med dessa lärarledda utbildningar så länge ett behov och intresse finns att delta. En fördel med de lärarledda utbildningarna har varit den dialog som uppkommer runt olika frågeställningar. Det ger oss alla en större förståelse över vilka svårigheter som finns i de olika delarna av verksamheten.

Dessa utbildningar behöver kompletteras med en introduktionsutbildning för nyanställda samt e-Learning utbildningar på EkNet under nästa år.

DPO har också varit inbjuden till ett flertal enheter för att hålla utbildningar samt för diskussioner kring olika frågeställningar.

Öppna hus har anordnats vid 3 tillfällen under hösten där de som har frågor och funderingar kring enhetens dataskyddsarbete kan komma och ställa frågor utan att behöva boka tid. Har varit uppskattade och DPO kommer att fortsätta med detta även under 2020.

Dataskyddsnätverket har träffats ca 1 ggr/månad (utom juli och aug). Många av årets möten har hanterat frågeställningar runt förändring av systemet Draftit samt funderingar kring registerförteckningar.

Incidenter i kommunen

Ekerö kommun har rapporterat in 4 större incidenter till Datainspektionen. Tre har återrapporterats från Datainspektionen som avskrivna.

Till samordnarnas interna incidentlista har 24 incidenter rapporterats från samtliga myndigheter.

Det kan vid en första anblick se bra ut att vi inte har så många incidenter men utifrån erfarenhet från diskussioner runt om i kommunen så ser jag istället det som att vi i dagsläget inte identifierar händelser som incidenter eller att de inte rapporteras enligt befintlig rutin. Detta innebär att en drive runt incidenthantering behöver genomföras under 2020 för att sprida vikten av att incidenter rapporteras och hanteras enligt den rutin som finns.

Informationsplikten

Övergripande information om hur Ekerö kommun behandlar personuppgifter finns på kommunens hemsida. De olika nämndernas verksamhetsspecifika hantering av personuppgiftsbehandlingar finns också på samma ställe men under flik för respektive nämnd (alla nämnder har ännu inte skrivit och lagt ut den).

Detta förfarande underlättar hanteringen av informationstexterna som måste finnas på alla blanketter e-tjänster och övriga platser där personuppgifter hämtas in.

Hur kommunen behandlar personuppgifter om anställda finns på EkNet.

Systemet Drafit

Under året kom vi i nätverket fram till att vårt verktyg Drafit som användes för att registrera våra personuppgiftsbehandlingar kändes svårjobbat och att frågorna var både svåra att förstå och besvara. Utifrån det så har DPO, tillsammans med samordnare ur nätverket, utvärderat vårt system i förhållande till några andra system på marknaden. Vi kom dock fram till att det system vi redan har ändå är det som fungerar bäst.

Vi (nätverket) har därefter beslutat att vi behövde en nystart med arbetet i Drafit. Tillsammans med leverantören har vi haft en diskussion runt hur vi kan jobba i systemet och vi har fått ny utbildning. Utifrån detta så har DPO skrivit om mallarna i systemet för att de ska vara lättare att fylla i och framförallt att den som fyller i frågorna bättre ska förstå vad som efterfrågas. Efter genomgångar av detta i nätverket så har vi nu kommit fram till nya mallar och texter så att det ska underlätta arbetet ute i verksamheten.

Det finns också mer utrymme för att dokumentera hur man kommit fram till vissa svar. De nya mallarna fanns på plats under december månad och har börjat användas. Det som redan fanns inmatat i systemet behövde inte göras om, men behövde kompletteras.

Det finns också en ny modul i Drafit som heter DPIA. Den är till för att kunna göra de konsekvensbedömningar utifrån Dataskyddsförordningen som efterfrågas vid hantering av känsliga uppgifter. Man får också en hjälp med att undersöka om man behöver göra

en hel konsekvensbedömning. Det stora värdet här är att det dokumenteras att man har tänkt igenom den här frågan.

Det finns en stor nytta med att kunna ha all dokumentation kring vårt Dataskyddsarbete på ett ställe. Här finns en tanke att vi i början av 2020 också ska kunna ha vår interna incidentrapportering i verktyget.

Behörighetshantering och säkerhet

Det har under självskattningen framkommit att det saknas tillräcklig säkerhetsnivå för vissa system i kommunen som hanterar känsliga personuppgifter. Här behöver verksamheten genomföra konsekvensanalyser sk DPIA för att säkerställa att rätt behörighetsstruktur och tillräcklig säkerhet finns för de känsliga och särskilt skyddsvärda personuppgifter som hanteras.

En brist som framkommit är att kommunen inte har någon form av säker kommunikation. E-posten är inte en säker kommunikationsplattform vilket innebär att känslig information och sekretess inte kan hanteras där. Möjlighet att säkert kunna skicka/ta emot känsliga personuppgifter och sekretess behöver komma på plats.

Behörighetshantering i våra system som hanterar personuppgifter behöver ses över utifrån lagkravet att personer inte ska kunna få åtkomst till uppgifter som man inte behöver för att kunna sköta sitt arbete.

Det saknas tillräcklig säkerhetsnivå för inlogg i system i kommunen som hanterar känsliga personuppgifter. Behöver säkerställas.

Genomförd självskattning

Självskattningen gick till på det sätter att tid om ca 3 timmar per enhet avsattes för genomgång av ett antal frågeställningar så som finns en registerförteckning, har en DPIA genomförts där det behövs, har enheten kontroll på incidenter, finns biträdesavtal, hur är kunskapen om dataskydd i den egna organisation hur ser säkerheten ut. Kan dataskyddsombudet hjälpa er vidare och vilken hjälp vill ni ha.

Dataskyddsombudet genomförde 22 självskattningar under perioden mars-juni. De som deltog var förutom DPO, verksamhetsansvarig, dataskyddssamordnare och de övriga som verksamhetsansvarig valt att ta med sig.

Samtliga verksamhetschefer har under sommaren fått en rapport över sin verksamhets efterlevnad av dataskyddslagstiftningen utifrån självskattningen.

Det har också gett mig som Dataskyddsombud en karta över var de framtida insatserna bör läggas.

Det som visat sig är framför allt att de flesta vet vilket arbete som behöver göras men alla har inte kommit lika långt i det arbetet. Det framgår tyvärr att några verksamheter knappt har kommit igång med sitt arbete. Detta behöver åtgärdas snarast.

En enkät skickades ut till samtliga deltagare och utifrån den så känns det som att det har varit uppskattat att få en genomgång av de olika delarna. Många har även sett det som ett lärande. Det framgår också att de flesta vill ha en återkommande typ av granskning/genomgång 1-2 ggr/år.

Uppskattning av hur myndigheten i sin helhet ligger till före och efter självskattningen (OBS! olika enheter inom myndigheten kan ligga bättre eller sämre till)

Myndighet	Uppskattad nivå innan självskattningen	Uppskattad nivå efter självskattningen
Kommunstyrelsen	Har kommit igång	Har kommit igång
Barn- och utbildningsnämnden	Har kommit igång	Har kommit igång
Socialnämnden	Har kommit igång	Har kommit igång
Kultur- och fritidsnämnden	Är en bit på väg	Har kommit igång
Tekniska nämnden	Har knappt börjat	Har kommit igång
Byggnadsnämnden	Har kommit igång	Har kommit igång
Miljönämnden	Har knappt börjat	Har knappt börjat
Överförmyndaren	Nästan framme	Nästan framme

Uppfyller helt	Nästan framme	Är en bit på väg	Har kommit igång	Har knappt börjat
----------------	---------------	------------------	------------------	-------------------

Utifrån självskattningen

Någon form av genomgång/självskattning behöver göras årligen men kanske på ett något annorlunda sätt framöver.

Det var helt nödvändigt att vid första tillfället göra den här typen av granskning som innehöll i stort sett samtliga delar av dataskyddsarbetet för att få en lägesbild över hela kommunens efterlevandenivå. Det visade sig att det i stort sätt är en ganska likartad bild över svårigheterna som framkommit.

Det visar sig också att det behöver göras mer för att alla ska uppfylla lagkraven. Det finns ett flertal punkter utifrån självskattningen som behöver åtgärdas hos i stort sätt alla myndigheter, vilket gör att dessa bör fokuseras på under nästa år.

Att ta sig an de 5 punkterna nedan under nästa år gör att kommunen som helhet tar ett bra kliv i rätt riktning vilket gör att vi kan känna oss tryggare i vårt dataskyddsarbete.

Fokusområden för verksamheterna med hjälp av DPO 2020

1. Att verksamheten tar fram sin registerförteckning och lägger in den i Draftit.

När detta är gjort kan dataskyddsombudet granska och hjälpa till med kompletteringar och ge råd och stöd.

2. Tillse att alla medarbetare har fått eller får utbildning i dataskyddsfrågorna. Verksamheterna kan även behöva ha utbildningar/genomgångar inom det egna verksamhetsområdet.

Ta hjälp av DPO för egna enhetsutbildningar eller genomgångar av verksamhetens frågeställningar på t ex ett APT eller liknande.

Ungefär 6–7 ggr/år håller DPO en utbildning i dataskyddslagstiftningen och våra rutiner i kommunen, som alla medarbetare kan anmäla sig till via EkNet.

3. Hantering av personuppgiftsincidenter och säkerställa att alla incidenter identifieras och rapporteras (internt eller till Datainspektionen).

Ta hjälp av DPO för information och diskussion kring incidenthantering på era arbetsplatser.

DPO informerar och sprider rutinen för incidenthantering på intranätet samt att vi arbetar vidare med frågan i nätverket.

4. Se över er behörighetshantering på samtliga platser där ni hanterar känslig information.

En viktig princip i Dataskyddsförordningen är att den som inte behöver personuppgiften för att kunna utföra sitt arbete inte heller ska ha tillgång till den. Det gäller inte bara i system utan även om hanteringen sker på annat sett och oavsett om det sker digitalt eller inte. Gör en DPIA om ni identifierar känslig information.

Ni kan alltid be DPO att medverka om ni behöver råd och stöd.

5. Säkerställ att verksamheten har en uppdaterad dokumenthanteringsplan.