ÖRNSKÖLDSVIKS KOMMUN

Policy för informations-säkerhet och dataskydd

Örnsköldsviks kommunkoncern

Antagen av kommunfullmäktige 2019-12-16
§ 248/2019

Dokumentnamn: Policy för informationssäkerhet och dataskydd Örnsköldsviks kommunkoncern		**Ärendebeteckning:** Kst/2019:153
Dokumentägare: Kommundirektör	**Dokumentansvarig:** Avdelningschef utvecklingsavdelningen	**Publiceras:** Intranät, extern webbplats
Ersätter dokument: Kst/2013:526 IT-säkerhetspolicy 2004	**Revideras:** Vid behov	**Utvärderas:** Årligen
Relaterade dokument: Säkerhetspolicy, Informationssäkerhetsstrategi, Strategi för dataskydd och personuppgiftsbehandling		
Målgrupp: Anställda, förtroendevalda och styrelseledamöter inom Örnsköldsviks kommunkoncern		

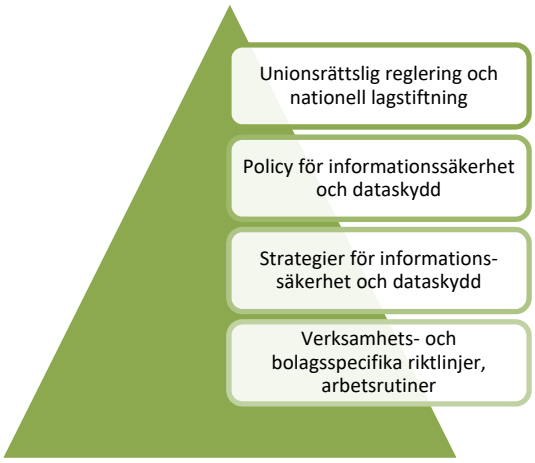
Innehåll

1. Inledning

Denna policy innehåller Örnsköldsviks kommunkoncerns viljeinriktning och övergripande principer för arbetet med informationssäkerhet och dataskydd.

Arbetet med informationssäkerhet och dataskydd är bundet dels av den unionsrättsliga regleringen (förordningar och direktiv) och dels av den nationella rätten (lagar, förordningar och föreskrifter).

Inom kommunkoncernen bygger efterlevnaden av dessa regler på att styr- och stöddokument beslutas på lämplig nivå.



Pyramid som illustrerar hierarkin för regleringar och styrdokument.

1.1 Syfte och mål

Syftet med policyn är att utgöra ett koncernövergripande ramverk för hur kommunkoncernens informationstillgångar ska säkras och medborgarnas integritet ska skyddas.

Målet med policyn är att på en övergripande nivå säkerställa att kommunkoncernen efterlever de krav och villkor som anges i unionsrätt och nationell rätt gällande informationssäkerhet och dataskydd.

1.2 Målgrupp och tillämpning

Policyn gäller för alla verksamheter inom kommunkoncernen, så som nämnder (inbegripet kommunstyrelsen), förvaltningar och kommunala bolag. Policyns huvudsakliga målgrupp är anställda, förtroendevalda och styrelseledamöter inom kommunkoncernen.

Policyn ska tillämpas i arbetet med informationssäkerhet och dataskydd oavsett om det sker i digital eller fysisk form och oberoende av var och hur informationen lagras. Det som föreskrivs i policyn konkretiseras i koncernövergripande strategier samt verksamhetsspecifika riktlinjer och rutiner.

2. Arbetet med informationssäkerhet

För att skapa tillit och förtroende såväl internt som extern och för att nämnder och bolag ska kunna fullgöra sina uppdrag i samhället är det viktigt att information hanteras i kommunkoncernen på ett säkert och ansvarsfullt sätt.

Därför måste kommunkoncernens information skyddas så att:

- den alltid finns när den behövs (tillgänglighet)
- det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- endast behöriga personer får ta del av den (konfidentialitet)
- informationshanteringen går att spåra vid behov (spårbarhet).

För att skydda information och uppnå uppsatta mål om regelefterlevnad ska arbetet med informationssäkerhet i kommunkoncernen:

- vara systematiskt och bygga på standardserien ISO/IEC 27000
- bygga på en helhetssyn som har informationen som utgångspunkt men även omfattar organisation, arbetssätt, processer, människor och teknik
- integreras i arbetet med upphandling och avtalsuppföljning
- vara riskbaserat, vilket innebär att hot, risker och sårbarheter identifieras och reduceras
- vid val av ändamålsenliga och proportionella säkerhetsåtgärder beakta kombinationer av organisatoriska, fysiska och tekniska åtgärder
- löpande förbättras och anpassas i en föränderlig omvärld
- vara förebyggande men även kunna hantera incidenter, allvarliga störningar och kriser
- vara väl kommunicerat i verksamheten där medarbetare genom utbildning och information får en säkerhetsmedvetenhet
- aktivt samverka med det omgivande samhället och ansvariga myndigheter.

3. Arbetet med dataskydd

Dataskyddsförordningens huvudsakliga syfte är att skydda de registrerades grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Utgångspunkten är därmed att arbetet med dataskydd och personuppgiftsbehandling ska ske med hänsyn till den registrerades integritet.

Därför måste personuppgiftsansvarig säkerställa att personuppgifter behandlas med utgångspunkt i dataskyddsförordningens grundläggande principer, vilket innebär att personuppgifter

- behandlas enligt lag och att behandlingen är rättvis och står i proportion till nyttan (laglighet, korrekthet)
- behandlas transparent genom att den registrerade kan förstå syftet med behandlingen och vara införstådd med sina rättigheter (öppenhet)
- endast behandlas för ändamål som är fastställt innan behandlingen påbörjas (ändamålsbegränsning)
- inte behandlas utöver vad som krävs för ändamålet (uppgiftsminimering)
- är korrekta och om nödvändigt uppdaterade (riktighet)
- gallras, avidentifieras eller arkiveras när de inte längre behövs utifrån ändamålet (lagringsminimering)
- behandlas på ett sätt som säkerställer lämplig säkerhet (integritet och konfidentialitet)
- behandlas enligt ovanstående principer och att personuppgiftsansvarig kan uppvisa följsamhet genom dokumentation (ansvarsskyldighet).

För att värna den registrerades integritet och uppnå uppsatta mål om regelefterlevnad ska arbetet med dataskydd i kommunkoncernen:

- bygga på en helhetssyn som har den registrerades integritet i centrum
- bedrivas aktivt av personuppgiftsansvariga nämnder och bolag, genom att nödvändiga åtgärder vidtas och erforderliga personalresurser avsätts
- säkerställa dataskyddsombudets oberoende roll och deltagande i dataskyddsfrågor på högsta ledningsnivå
- vara förebyggande för att säkerställa att nya personuppgiftsbehandlingar sker i överensstämmelse med dataskyddsförordningens bestämmelser
- vara riskbaserad för att skydda personuppgifter från att förändras, gå förlorade eller komma i orätta händer
- bedrivas systematiskt i fråga om dokumentation, uppföljning, egenkontroll och rapportering till tillsynsmyndigheten
- bygga på principerna om inbyggt dataskydd och dataskydd som standard
- vara väl kommunicerat i verksamheten genom styrdokument och informationsinsatser.

4. Styrning och uppföljning

Nämnder och kommunala bolag har inom sina respektive verksamheter ansvar för att

- leda, utveckla, följa upp och utvärdera arbetet med informationssäkerhet och dataskydd samt
- säkerställa att policyn efterlevs och att såväl aktuell lagstiftning som organisationens krav uppfylls.

Kommunledningsförvaltningen har övergripande ansvar att samordna och utöva tillsyn av kommunkoncernens arbete med informationssäkerhet och dataskydd.

Bilaga definitioner

Informationssäkerhet: De åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs.

Dataskydd: Skydd för privatlivet och den personliga integriteten vid behandling av personuppgifter.

Personuppgift: Alla uppgifter som direkt eller indirekt, enskilt eller i kombination med andra upplysningar, kan knytas till en levande fysisk person (kallad ”den registrerade”). Exempel på uppgifter som i sitt sammanhang kan utgöra en personuppgift: namn, personnummer, adress, personfoto, e-post, fastighetsbeteckning, kontonummer, titel/funktion.

Personuppgiftsbehandling: En åtgärd eller kombination av åtgärder beträffande personuppgifter, t.ex. insamling, registrering, strukturering, lagring, ändring, läsning, användning, utlämning, begränsning eller radering.

Personuppgiftsansvarig: Myndighet eller annan organisation som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Inom kommunkoncernen är varje nämnd och bolag personuppgiftsansvarig för den egna verksamheten.

Registrerad (”den registrerade”): Enskild fysisk person vars personuppgifter behandlas och som därigenom har rätt till dataskydd.