Kommunal Författningssamling

GDPR-strategi

Dokumenttyp	Strategi
Dokumentnamn	GDPR-strategi
Nämnd	Kommunstyrelsen
Sektor	Styrning och stöd
Antagen	Kommunstyrelsen, 2021-01-20
Paragraf	Ks § 18/2021
Ansvar	Säkerhetschef

2021-01-20
Dnr Ks 2020/473

GDPR-strategi Kävlinge kommun

Innehåll

Antagen av kommunstyrelsen 2021-01-20, § 18/2021

1. Inledning

Denna strategi utgör Kävlinge kommuns övergripande styrdokument för efterlevnad av GDPR, Allmänna Dataskyddsförordningen (EU:s förordning nr 2016/679).

2. Syfte

Syftet med denna strategi är att säkerställa att Kävlinge kommun uppfyller de krav och villkor som GDPR anger. Strategin omfattar alla verksamheter där kommunen har ett huvudmannaansvar. Det är i första hand kommunens anställda som var och en måste ansvara för att Dataskyddsförordningen och kommunens styrdokument efterlevs inom det dagliga arbetet.

3. Vad innebär GDPR för kommunen?

GDPR efter engelskans *General Data Protection Regulation*, har bland annat ersatt Personuppgiftslagen (1998:204) och kallas på svenska Dataskyddsförordningen.

GDPR, tillsammans med kompletterande nationell lagstiftning, innebär i korthet:

- kommunen måste föra register över sin hantering av personuppgifter
- alla incidenter som berör personuppgifter måste anmälas till Datainspektionen
- konsekvensbedömningar måste göras innan nya behandlingar av personuppgifter sker
- ”missbruksregeln” försvinner (personuppgifter får inte behandlas slentrianmässigt i exempelvis löptext och enkla listor).

4. Ansvarsfördelning och roller

4:1 Personuppgiftsansvarig nämnd/bolag

Kommunernas nämnder och bolag är fristående personuppgiftsansvariga[1] och har det yttersta ansvaret för att säkerställa att behandling av personuppgifter inom den egna nämnden sker i enlighet med lagstiftningen och kommunens styrdokument. Det är också personuppgiftsansvarig som ansvarar för att anmälan görs till tillsynsmyndigheten vid personuppgiftsincident[2], samt att vid tillsyn kunna redovisa hur de säkerställer Dataskyddsförordningens krav och villkor[3].

- Varje nämnd/personuppgiftsansvarig ska vid behov utarbeta en handlingsplan för dataskyddsarbetet i organisationen i samråd med informationssäkerhetssamordnare och, om det bedöms tillämpligt, dataskyddsombud.
- Det är upp till varje personuppgiftsansvarig/nämnd att genomföra relevant konsekvensbedömning om ny eller förändrad personuppgiftsbehandling anses utgöra ”hög risk”, se avsnitt 5:3.
- Det är varje personuppgiftsansvarig/nämndernas ansvar att föra in vilka register över behandling som de har inom sin nämnd, se avsnitt 5:4.
- Det är personuppgiftsansvarig/nämnderna, alternativt anlitade personuppgiftsbiträden, som har ansvar för att anmälan görs för incidenter inom sina respektive nämnder, se avsnitt 5:5.

[1] Artikel 4 punkt 7

2 Artikel 33

3 Artikel 56

- Det är ytterst personuppgiftsansvarig/nämnderna som har ansvar för att följa upp det interna arbetet och säkerställa att arbetet följer dataskyddsförordningen.

4:2 Dataskyddsombud

Enligt Dataskyddsförordningens artikel 37 är kommunens nämnder skyldiga att utse ett dataskyddsombud. I Kävlinge kommun är säkerhetschefen tillika dataskyddsombud.

Dataskyddsombudets uppgifter är att

- agera rådgivande åt kommunens nämnder,
- att hjälpa till vid konsekvensbedömningar,
- att på ett övergripande plan övervaka efterlevnaden av Dataskyddsförordningen, samt
- att vara kontaktperson mot tillsynsmyndigheten[4].
- Dataskyddsombudet utgör också en rådgivande och stöttande instans gentemot nämndernas informationssäkerhetssamordnare.

4:3 Nämndspecifika informationssäkerhetssamordnare

Samtliga nämnder/personuppgiftsansvariga ska utse minst en informationssäkerhetssamordnare som bistår dataskyddsombudet med att samordna och utveckla kommunens dataskyddsarbete.

Informationssäkerhetssamordnarnas uppgift är bland annat att agera rådgivande och stöttande gentemot nämndens anställda i deras arbete med Dataskyddsförordningen. Informationssäkerhetssamordnarna leder arbetet med att säkerställa upprättande av förteckningar över system och verksamhetens personuppgiftsbehandlingar samt initierar utbildningsinsatser efter behov.

4:4 Allmänt säkerhetskrav för kommunen

Kävlinge kommun förutsätter att alla anställda inom kommunen tar ett eget ansvar för att leva upp till kommunens styrdokument och förordningen.

Alla nyanställda i Kävlinge kommun ska genomgå en kort utbildning som säkerställer att de anställda får kunskap om kommunens ansvar. Samtliga anställda uppmanas att minst en gång per år uppdatera sina kunskaper genom de utbildningar informationssäkerhetssamordnarna lägger ut.

Kävlinge kommun och dess anställda ska utforma sitt arbetssätt, sina IT-system, sin IT-användning och sina rutiner enligt principen om inbyggt dataskydd och dataskydd som standard (privacy by design samt privacy by default). Detta innebär att kommunen och dess anställda redan från upphandling ska ta hänsyn till de integritetsskyddsregler som förordningen fastställt.

5. Behandling av personuppgifter

Kävlinge kommuns behandling av personuppgifter ska alltid ske i enlighet med de principer och skäl som tas upp i Dataskyddsförordningen[5].

Personer vars personuppgifter blir behandlade av Kävlinge kommun ska alltid få information om *var* personuppgifterna finns lagrade, *vilka* personuppgifter det gäller, *hur* personuppgifterna lagras, samt *vem* den registrerade kan kontakta för frågor gällande lagringen av

[4] Artikel 39
[5] Artikel 5 punkt 1 – artikel 6

personuppgifter[6]. Informationen ska alltid förmedlas på ett tydligt och lättförståeligt sätt [7]. Den registrerade ska också få information om vilka rättigheter den enskilde har gentemot kommunen (se avsnitt 5.5.2). I tillämpliga fall ska den registrerade även meddelas om vilken tidsperiod personuppgifterna kommer lagras. Information om Kävlinge kommuns behandling av personuppgifter ska finnas på kommunens hemsida.

5:1 Utlämnande av personuppgifter

Offentlighetsprincipen innebär att var och en har rätt att ta del av allmänna handlingar. Dataskyddsförordningen hindrar inte att personuppgifter i allmänna handlingar lämnas ut. Om allmänna handlingar lämnas ut digitalt krävs dock att reglerna i dataskyddsförordningen följs. Känsliga personuppgifter som utlämnas på detta sätt måste t.ex. skyddas genom lämpliga säkerhetsåtgärder.

Rätten att ta del av allmänna handlingar gäller inte om handlingarna innehåller uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen. Enligt den gäller till exempel sekretess för personuppgift om det kan antas att den som begär ut personuppgifterna kommer att behandla dem på ett sätt som strider mot dataskyddsförordningen.

För överföring mellan myndigheter gäller att principerna för behandling av personuppgifter uppfylls, samt att den registrerade får tydlig information om syfte, vilka personuppgifter det gäller och när uppgifterna överförs[8]. Vid tillsyn eller liknande visning av personuppgifter måste en anställd från Kävlinge kommun närvara då tredje part tar del av personuppgifterna. Då känsliga uppgifter visas ska ett sekretessavtal skrivas under.

5:2 Begäran om fullständigt registerutdrag

Den registrerade har alltid rätt att begära ut uppgifter om sig själv eller den som personen är vårdnadshavare för[9]. Denna information ska lämnas ut skyndsamt, men senast efter 30 dagar[10]. Den registrerade har rätt att begära ett kostnadsfritt registerutdrag per år. Vill den registrerade begära ut fler registerutdrag per år, kommer en avgift att tas ut[11]. Registrerad ska kunna styrka sin identitet vid begäran om registerutdrag.

5:3 Konsekvensbedömning vid personuppgiftsbehandling

Om någon av kommunens personuppgiftsansvariga planerar en ny eller omfattande förändring i behandling av personuppgifter som innebär hög risk för de registrerade, ska denna föregås av en konsekvensbedömning[12]. Konsekvensbedömningen ska syfta till att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter.

Hög risk definieras i Kävlinge kommun som att

- En stor mängd och/eller olika typer av personuppgifter behandlas, särskilt om dessa är av känslig karaktär.
- Personuppgifterna berörs av delvis eller helt automatiserad behandling (exempelvis systematisk kamera/övervakning, samkörning av register eller bakgrundsgranskning)
- Personuppgifterna rör personer som av något skäl befinner sig i underläge eller beroendeställning

[6] Artikel 13 och 14
[7] Artikel 12 punkt 1
[8] Artikel 13-14 och Artikel 20
[9] Artikel 15
[10] Artikel 12 punkt 3 och 4
[11] Artikel 15 punkt 3
[12] Artikel 35

- Personuppgifterna ska behandlas med hjälp av helt ny teknik

Samtliga konsekvensbedömningar ska klargöra *hur många* uppgifter som samlas in, vilken *rättslig grund* det finns för insamlandet, för vilket *ändamål* uppgifterna får behandlas och hur risker ska hanteras.

Det är upp till varje personuppgiftsansvarig att genomföra relevant konsekvensbedömning samt uppdatera vid behov.

5:4 Registerföring över behandling

Både kommunens personuppgiftsansvariga och kommunens anlitade personuppgiftsbiträden är skyldiga att föra ett register över sin behandling av personuppgifter[13]. Kävlinge kommun har ett kommungemensamt system för att registrera och klassificera system och register över behandling av personuppgifter. Det är varje personuppgiftsansvarigs ansvar att föra in vilka register över behandling som de har inom sin nämnd.

5:5 Anmälan om personuppgiftsincident till tillsynsmyndigheten

Om det inträffar en säkerhetsincident som rör personuppgifter (exempelvis dataintrång eller oavsiktlig förlust av personuppgifter) ska denna incident dokumenteras och anmälas till tillsynsmyndigheten inom 72 timmar[14]. Även om en fullständig anmälan inte kan göras, ska det som kan dokumenteras skickas in till tillsynsmyndigheten inom 72 timmar. Det är personuppgiftsansvarig, alternativt anlitade personuppgiftsbiträden, som har ansvar för att anmälan görs för incidenter inom sina respektive nämnder[15]. Vid upptäckt ska säkerhetsenheten kontaktas som samordnar arbetet med anmälan.

Anmälan behöver dock inte göras om det är osannolikt att incidenten leder till några risker för de registrerades fri- och rättigheter, exempelvis vid kortare tillgänglighetsincidenter.

Personuppgiftsansvariga och deras anlitade personuppgiftsbiträden har också en skyldighet att informera den/de registrerade som drabbas av incidenten om det är hög risk för personernas fri- och rättigheter[16].

6. Kommungemensamma behandlingar av personuppgifter

Kävlinge kommun delar tre verksamheter med Burlövs kommun och Staffanstorps kommun. Dessa tre verksamheter utgörs av *Löneservice* (vilken Burlövs kommun har huvudsakligt ansvar för), *IT-service* (vilken Kävlinge kommun har huvudsakligt ansvar för) och *Geoinfo* (vilken Staffanstorps kommun har huvudsakligt ansvar för).

För att säkerställa att personuppgifter hanteras på ett korrekt sätt av de tre kommunerna inom samtliga tre verksamheter upprättas personuppgiftsbiträdesavtal mellan kommunernas kommunstyrelser.

7. Personuppgiftsbiträden

Vid anlitande av personuppgiftsbiträde ska alltid ett skriftligt personuppgiftsbiträdesavtal tecknas[17]. Avtalet ska klargöra att personuppgiftsbiträdet och dess personal enbart får behandla personuppgifter enligt instruktion från den personuppgiftsansvarige[18], samt att biträdet inte får

[13] Artikel 30
[14] Artikel 33
[15] Artikel 33 punkt 1 och 2
[16] Artikel 34
[17] Artikel 28 punkt 2
[18] Artikel 28 punkt 3

anlita andra biträden utan att ha fått ett skriftligt tillstånd av den personuppgiftsansvarige[19]. De biträden som kommunen anlitar ska dessutom kunna ge tillräckliga garantier för att deras behandling uppfyller kraven i Dataskyddsförordningen[20]. Detta innebär exempelvis att biträdet ska registerföra sin behandling av personuppgifter, samt att biträdet vid tillsyn ska kunna redovisa att de tillhandahåller en lämplig säkerhetsnivå för sin hantering av känslig information[21].

8. Uppföljning och kontroll

8:1 Uppföljning av det interna arbetet

Det är ytterst nämnderna (personuppgiftsansvariga) som har ansvar för att följa upp det interna arbetet och säkerställa att arbetet följer denna strategi samt Dataskyddsförordningen i sin helhet. Specifik uppföljning av ett område inom Dataskyddsförordningen kan göras genom exempelvis intern kontroll.

8:2 Gallring av information/personuppgifter

Kommunen ska i informationshanteringsplaner ha rutiner för att säkerställa att icke-ändamålsenlig information gallras regelbundet. Gallring kan ske genom radering, arkivering enligt arkivlagen, eller pseudonymisering. Samtliga anställda inom Kävlinge kommun ansvarar för att regelbundet och konsekvent gå igenom sina dokument och gallra den information som inte längre uppfyller sitt angivna syfte.

8:3 Revidering av styrdokument

Kävlinge kommuns *GDPR-strategi* ska revideras vid behov, men minst en gång per mandatperiod. Ansvarig för dokumentet är säkerhetsenheten.

[19] Artikel 28 punkt 2
[20] Artikel 28 punkt 1 och punkt 5-10
[21] Artikel 28 punkt 4