§ 134 Dnr KS/2015:410

Personuppgiftslagen - förslag på riktlinje för Mjölby kommun

Bakgrund
EU:s dataskyddsförordning (General Data Protection Regulation GDPR) ska börja tillämpas 25 maj 2018. Förordningen kommer att gälla som lag i Sverige och ersätter person-uppgiftslagen (PUL). Syftet med förordningen är att skapa enhetliga dataskyddsregler inom hela EU samt att stärka den personliga integriteten.

Sammanfattning
Riktlinjer har tagits fram i samråd med samtliga förvaltningar för att fastställa det ansvar kommunen har för att följa nuvarande lagstiftning men även den kommande dataskyddsförordningen. Kommunövergripande rutiner kommer att komplettera framtagna riktlinjer.

Avsikten med riktlinjerna och rutinerna är att skapa en enhetlig vägledning för kommunen. I och med den nya lagstiftningen tillkommer några arbetsmoment och några begrepp försvinner för kommunen vilket hänvisas till i riktlinjerna. Förvaltningen föreslås få i uppdrag att justera riktlinjerna i enlighet med detta

Beslutsunderlag
Förslag till riktlinjer
Riktlinjer för PUL och GDPR – missiv daterad 2017-08-30.

Arbetsutskottets förslag till kommunstyrelsen

Kommunstyrelsens arbetsutskott överlämnar ärendet till kommunstyrelsen för beslut.

___

Beslutet skickas till:
Kommunstyrelsen
Akten

Mjölby Kommun
Kommunstyrelsens förvaltning

Missiv

Datum
2017-08-30

Diarienummer
KS/2015:410

Handläggare

Carina Stolt
Tfn 0142-851 11

Kommunstyrelsen

Riktlinjer för PUL och GDPR

Bakgrund

EU:s dataskyddsförordning (General Data Protection Regulation GDPR) ska börja tillämpas 25 maj 2018. Förordningen kommer att gälla som lag i Sverige och ersätter person-uppgiftslagen (PUL). Syftet med förordningen är att skapa enhetliga dataskyddsregler inom hela EU samt att stärka den personliga integriteten.

Sammanfattning

Riktlinjer har tagits fram i samråd med samtliga förvaltningar för att fastställa det ansvar kommunen har för att följa nuvarande lagstiftning men även den kommande dataskyddsförordningen. Kommunövergripande rutiner kommer att komplettera framtagna riktlinjer.

Avsikten med riktlinjerna och rutinerna är att skapa en enhetlig vägledning för kommunen. I och med den nya lagstiftningen tillkommer några arbetsmoment och några begrepp försvinner för kommunen vilket hänvisas till i riktlinjerna. Förvaltningen föreslås få i uppdrag att justera riktlinjerna i enlighet med detta

Beslutsunderlag

Förslag till riktlinjer
Riktlinjer för PUL och GDPR – missiv daterad 2017-08-30

Kommunstyrelsens förvaltnings förslag till beslut

1. Riktlinjerna antas.

2. Förvaltningen ges i uppdrag att anpassa riktlinjerna till den lagstiftning som träder i kraft 25 maj 2018 i form av tidshänvisningar och begreppsförändringar.

Kommunstyrelsens förvaltning

Dag Segrell
Kommunchef

Mjölby Kommun

Riktlinjer för Dataskyddsförordningen (General Data Protection Regulation)/ Personuppgiftslagen –

utkast för Mjölby kommun

Antagen: Kommunstyrelsen 201X-XX-XX § X

Dokumentansvarig: Kommunchef

Allmänna riktlinjer för behandling av personuppgifter enligt Dataskyddsförordningen/Personuppgiftslagen (PuL)

1. Bakgrund

EU:s dataskyddsförordning ska börja tillämpas 25 maj 2018. Förordningen kommer att gälla som lag i Sverige och ersätter personuppgiftslagen. Syftet med förordningen är att skapa enhetliga dataskyddsregler inom hela EU.

Dataskyddsförordningen/ Personuppgiftslagen (PuL) har som syfte att skydda enskilda personer mot kränkning av den personliga integriteten vid behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

Dataskyddsförordningen är underordnad i förhållande till vissa andra författningar, det vill säga om det i en annan lag eller förordning finns bestämmelser som avviker gäller de bestämmelserna istället, till exempel behandling av personuppgifter inom socialtjänsten. Dataskyddsförordningen gäller inte heller om det skulle strida mot tryck- eller yttrandefriheten.

Dessa riktlinjer gäller i enlighet med nu gällande personuppgiftslagstiftning och kommer även att gälla då dataskyddsförordningen träder i kraft.

Sanktioner
Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att förordningen följs, vilket kan medföra krav på ökad dokumentation. Det kommer att införas möjligheter för tillsynsmyndigheten att i vissa fall döma ut en administrativ sanktionsavgift när en organisation missköter sin behandling av personuppgifter.

2. Några begrepp

- **Behandling** omfattar varje åtgärd som vidtas i fråga om personuppgifter. Begreppet är teknikneutralt vilket innebär att det kan handla om manuell eller automatiserad/datoriserad behandling. Det kan enligt lagen vara fråga om insamling, registrering, organisering, lagring, bearbetning eller ändring, utlämnande, utplåning eller förstöring, sammanställning eller samkörning etc
- **Dataskyddsombud** ska informera, ge råd och övervaka efterlevnaden av denna förordning samt samarbeta med tillsynsmyndigheten. Rollen är specificerad i dataskyddsförordningen som gäller från och med 25 maj 2018.
- **Personuppgift** är all slags information som direkt eller indirekt kan hänföras till fysisk person som är i livet. Det kan även uttryckas som så att en person är identifierbar eller sökbar utifrån de uppgifter som förs.
- **Personuppgiftsansvarig** är den som ensam eller tillsammans med annan bestämmer ändamålen med och/eller medlen för behandling av personuppgifter, dvs. kommunstyrelsen och ansvariga nämnder i egenskap av självständiga förvaltningsmyndigheter.
- **Personuppgiftsombud** avses en fysisk person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt. Rollen finns kvar till och med 24 maj 2018.
- **Personuppgiftsbiträde** avses såväl en fysisk som juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning. Endast personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.
- **Personuppgiftsbiträdesavtal** När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal.
- **Den registrerade** är den person som en personuppgift avser.
- **Känsliga personuppgifter** är uppgifter som behöver ett särskilt skydd vilka betecknas som särskilda kategorier av personuppgifter i lagtexten. De är uppräknade i punkt 4.
- **Samtycke** måste vara en fråga om frivillig, specifik och otvetydig viljeyttring genom den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör hen.

3. Tillåten behandling av personuppgifter

Laglig behandling av personuppgifter

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Grundläggande principer inom integritetsskydd är att inte samla in mer information än vad som behövs, inte ha kvar information längre än nödvändigt och inte använda uppgifter till något annat än vad som var syftet när de samlades in.

Har den registrerade lämnat sitt **samtycke** till behandling av personuppgifterna är behandling i regel tillåten. Ett samtycke skall vara **individuellt, frivilligt, tydligt** och **informerat** efter det att den registrerade fått information om tilltänkt behandling.

Den registrerade kan när som helst återkalla sitt samtycke vartefter behandling inte vidare kan ske.

I kommunal verksamhet krävs i många fall inte samtycke enligt artikel 6 i dataskyddsförordningen. Detta gäller för nödvändig behandling för att:

- **Avtal** med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas.
- Personuppgiftsansvarige skall kunna fullgöra en **rättslig förpliktelse** (ex. bokföringslagen).
- Skydda **vitala intressen** för den registrerade (ex. skydda för den enskildas bästa).
- En **arbetsuppgift av allmänt intresse** skall kunna utföras (mot verksamhetens syfte ex. arkivering, forskning, statistikframställning m.m.).
- Utföra arbetsuppgift i samband med **myndighetsutövning.**

Personuppgifter på Internet

Behandling av personuppgifter på hemsida är tillåten om **samtycke** finns.

Fotografier på identifierbara personer kräver samtycke av den registrerade.

Personuppgifter, dock ej personnummer, som ingår i ett justerat protokoll som förts vid ett nämnd-, styrelse-, eller fullmäktigesammanträde får publiceras på kommunens hemsida. Innan materialet läggs ut på Internet skall det granskas så att inga integritetskänsliga eller sekretessbelagda personuppgifter publiceras.

Personuppgifter, ej personnummer, som rör en förtroendevalds uppdrag får även publiceras efter samtycke.

Offentlighetsprincipen

Offentlighetsprincipen innefattar en rätt för var och en att hos myndigheter ta del av allmänna handlingar. Denna rätt gäller dock inte om handlingarna innehåller uppgifter för vilka gäller sekretess enligt offentlighets- och sekretesslagen. Enligt den gäller exempelvis sekretess för personuppgift om det kan antas att ett utlämnande skulle medföra att uppgiften behandlas i strid med dataskyddsförordningen.

4. Otillåten behandling

Särskilda regler om känsliga personuppgifter

Enligt artikel 9 är det förbjudet att behandla känsliga personuppgifter. (13 § PUL)

Känsliga personuppgifter är uppgifter som avslöjar

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiösa eller filosofiska övertygelser
- Medlemskap i fackförening
- Uppgifter som rör sexualitet och hälsa
- Genetiska och biometriska uppgifter. Gäller från och med 25 maj 2018.

Undantag från förbudet finns om behandlingen är absolut nödvändig eller vid samtycke.

5. Information till de registrerade för samtycke

Vid insamlande av personuppgifter måste enligt dataskyddsförordningen lämnas viss information, till exempel

- identitet (vem är det som kräver in personuppgifter?)
- ändamål med behandlingen (vad ska uppgifterna användas till)
- Rättsliga grunder för behandlingen
- hur länge personuppgifterna lagras
- möjligheten att lämna klagomål till tillsynsmyndigheten om man anser att ens personuppgifter har hanterats felaktigt

Informationen som lämnas ska vara kortfattad, lättbegriplig och utformad med ett tydligt och enkelt språk. Enligt förordningen förtjänar barn särskilt skydd vilket gör att information som riktar sig till barn ska vara skriven på ett tydligt och enkelt sätt som barn förstår.

6. De registrerades rättigheter

De viktigaste rättigheterna för de registrerade är att:

- Få tillgång till sina personuppgifter
- Få felaktiga personuppgifter rättade
- Få sina personuppgifter raderade. Betänk att arkivlagen är överordnad.
- Invända mot att personuppgifter används automatiserat beslutsfattande och profilering
- Flytta personuppgifterna (dataportabilitet)

Dataskyddsförordningen innehåller en skyldighet att på begäran lämna information till de registrerade om vilka uppgifter som behandlas om dem. Detta kan vid begäran göras kostnadsfritt en gång per år. När en sådan begäran hanteras behöver man även lämna viss ytterligare information, som

exempelvis hur länge personuppgifterna kommer att lagras och att man har rätt att få felaktiga uppgifter rättade. Om en sådan begäran görs elektroniskt ska den registrerade också kunna begära att få ut informationen elektroniskt.

7. Personuppgiftsincidenter

Personuppgiftsincidenser/ dataintrång ska anmälas till Datainspektionen inom 72 timmar. Om intrånget har lett till allvarliga risker för den registrerade ska den registrerade kontaktas. Gäller från och 25 maj 2018.

8. Barnperspektivet

Barn förtjänar ett särskilt skydd enligt dataskyddsförordningen.
Den information som riktar sig till barn ska vara skriven på ett tydligt och enkelt sätt.

9. Kommunens ansvar

Kommunens ansvar i enlighet med dataskyddsförordningen kan sammanfattas med att kommunen behöver ha kännedom om var personuppgifter förekommer, hur de används och även kunna informera berörda personer vid begäran.

Registerförteckning

Dokumentation som på något sätt behandlar personuppgifter ska sammanställas i en registerförteckning. Även ostrukturerat material ska ingå i denna förteckning.

Samtycke

När kommunen inte har tillåtelse att använda personuppgifter vid myndighetsutövning eller av allmänt intresse ska ett samtycke inhämtas.

Konsekvensbedömning

Vid dokumentation med personuppgifter ska vid varje tillfälle en konsekvensbedömning genomföras för att bedöma risken och allvaret om uppgifter skulle spridas. Resultatet av bedömningen ska beaktas då lämpliga åtgärder fastställs. Om risken anses som hög behöver åtgärder planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna i förhållande till genomförandekostnaderna. Det kan vara aktuellt med samråd med tillsynsmyndigheten om det inte är genomförbart.

Gällande principer är att inte samla in mer information än vad som är nödvändigt, inte ha kvar informationen längre än nödvändigt samt att inte använda uppgifterna till annat än till angivet syfte. Beakta möjligheten att minimera tillgång till uppgifterna.

Upprätta personuppgiftsbiträdesavtal

När kommunen ingår nya avtal där personuppgifter behandlas ska personuppgiftsbiträdesavtal upprättas.