



Riktlinjer för behandling av personuppgifter enligt

Beslutad av KS 2017-09-20/§ 189

Diarienummer: KS/2017:107

Dokumentansvarig nämnd: Kommunstyrelsen

Dokumentansvarig tjänsteperson: Dataskyddsombud

Vision

Policy

Strategi

Plan

Riktlinje

1. Sammanfattning

Mjölby kommuns riktlinjer ska vara ett stöd för alla anställda som behandlar personuppgifter, men även för registrerade (den som lämnar sina personuppgifter direkt eller indirekt till Mjölby kommun) som vill veta mer hur Mjölby kommun arbetar med Dataskyddsförordningen.

I kommunens riktlinjer ges förklarande exempel på viktiga artiklar (paragrafer i lagtexten och även länkar till Datainspektionen och Dataskyddsförordningen för den som vill veta mer.

2. Inledning

EU:s dataskyddsförordning gäller från 25 maj 2018. Förordningen gäller som lag i Sverige och ersätter personuppgiftslagen. Syftet med förordningen är att skapa enhetliga dataskyddsregler inom hela EU och att skydda enskilda personer mot kränkning av den personliga integriteten.

Det finns även en kompletterande dataskyddslag som är antagen av riksdagen som officiellt heter "Lag med kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:218)

2.1 Definitioner

Nedan redovisar vi några viktiga uttryck som används i texten. I [artikel 4](#) finns samtliga uttryck redovisade.

Personuppgifter: varje upplysning som avser en levande identifierad eller identifierbar fysisk person. Exempel: namn, fotografier och adresser.

Behandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter. Exempel: att samla in, registrera eller lagra personuppgifter.

Register: en strukturerad samling av personuppgifter. Exempel: personuppgifter i ett personalsystem.

Personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Exempel: när en extern leverantör ger teknisk support.

Personuppgiftsansvarig: Det är kommunens politiska nämnder och kommunstyrelsen som är personuppgiftsansvariga och ansvarar för att

säkerställa och kunna visa att all behandlingen av personuppgifter utförs i enlighet med gällande integritetslagstiftning, ([artikel 24](#))

3. Dataskydd

3.1 Information till de registrerade

Vid insamlande av personuppgifter ska den registrerade få klar och tydlig information enligt den nya förordningen (artiklarna [13](#) och [14](#)). Det gäller även de som tidigare fått information eller givit sitt medgivande enligt gamla Personuppgiftslagen.

Vid insamlande av personuppgifter ska den registrerade få information om exempelvis:

- vem är det som kräver in personuppgifter
- ändamål med behandlingen (vad ska uppgifterna användas till)
- rättsliga grunder för behandlingen (exempelvis vid myndighetsutövning eller avtalsskrivning)
- 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.

3.2 Principer för behandling av personuppgifter

I Dataskyddsförordningen finns sex principer för behandling av personuppgifter ([artikel 5.1](#)):

- a) **Laglighet, korrekthet, öppenhet.** Vi ska öppet kunna bevisa att vi är lagliga och korrekta.
- b) **Ändamålsbegränsning.** Personuppgiften får endast användas för ett visst ändamål, inte till något annat.
- c) **Uppgiftsminimering.** Vi ska inte samla in eller använda fler personuppgifter än vad som behövs för ändamålet.
- d) **Riktighet.** Uppgifterna ska vara uppdaterade och korrekta.
- e) **Lagringsminimering.** Uppgifterna får inte sparas längre än nödvändigt.
- f) **Integritet och konfidentialitet.** Uppgifterna ska hanteras och förvaras på ett säkert sätt.

Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges skyldighet att kunna visa att behandlingen är laglig ([artikel 6](#)) samt att de sex principerna följs för behandling av personuppgifter. Det är viktigt att Mjölby

kommun kan visa att de sex principerna efterlevs genom en tydlig och korrekt dokumentation.

Integritetskyddsmyndigheten (IMY) kan komma att döma ut en [sanktionsavgift](#) om kommunen missköter sin behandling av personuppgifter.

3.3 Register över behandling av personuppgifter

Alla kommunens personuppgiftsbehandlingar ska sammanställas i en [registerförteckning](#) enligt ([artikel 30](#)). Även ostrukturerat material ska ingå i denna förteckning. Exempel på ostrukturerat material är enkla textfiler, till exempel Word- och Excel-filer, som lagras lokalt på en hårddisk, det kan vara en lista över konferensdeltagare eller klasslista.

3.4 Säkerhet för personuppgifter

Endast de medarbetare som behöver uppgifterna för att utföra sitt arbete får ha åtkomst till personuppgifterna, ([artikel 32](#)).

Åtkomsten ska styras av en tillräckligt stark lösenordspolicy eller eventuellt tvåfaktorsidentifiering.

Rutiner för åtkomst och behörighet ska finnas dokumenterade för varje register eller system där personuppgifter behandlas. Behörigheterna ska kontrolleras regelbundet så att listan över behöriga användare är aktuell.

Personuppgifter som behandlas inom vård- och omsorg ska beakta särskilda säkerhetskrav utifrån specifik särlagstiftning. Det gäller framför allt säkerhetskrav på åtkomst och behörigheter samt krav på loggning och spårbarhet.

Känsliga personuppgifter samt integritetskänsliga personuppgifter som kan nå över öppna nätverk ska beaktas särskilt avseende säker överföring och identifiering av behörig användare. För att trygga en säker behandling av uppgifter som kan nå över öppna nätverk bör en risk- och konsekvensbedömning genomföras i samråd med dataskyddsombudet (DSO).

3.5 Behandling av personuppgifter

3.5.1 Laglig behandling av personuppgifter

Kommunen får bara samla in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål enligt ([artikel 6](#)), laglig behandling av personuppgifter.

Kommunen får 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.

Vanligt förekommande lagliga grunder som Mjölby kommun använder för behandling av personuppgifter är:

Artikel 6.1.a Samtycke

Ett samtycke är när den registrerade samtycker till att kommunen får behandla

dennes personuppgifter för ett specifikt ändamål. I kommunal verksamhet ska samtycke endast användas i undantagsfall som laglig grund när ingen annan laglig grund är tillgänglig.

Exempel på tillfällen då endast samtycke är tillämpligt som laglig grund kan vara i samband med publicering av bilder i sociala medier. För att ett samtycke ska anses som giltigt måste det vara högst frivilligt. Frivilligheten måste vara tydlig i såväl samtyckesblanketten som i hanteringen av hur frågan ställs och i vilket forum.

För kommunens personal hämtas samtyckesblanketten på intranätet av den som vill vara med på bild så beslutet sker utan påtryckningar.

Artikel 6.1.b Avtal

Behandlingen är nödvändig för att vi ska kunna fullgöra ett avtal med den registrerade. Exempelvis abonnemang på en badet eller fakturering av hyra eller arrende.

Artikel 6.1.c Rättslig förpliktelse

När det åligger kommunen att följa andra lagar och bestämmelser. Exempel: när kommunen har bokföringsskyldighet eller skyldighet att redovisa skatt och sociala avgifter.

Artikel 6.1.e Allmänt intresse och Myndighetsutövning

Om behandlingen är nödvändig för att genomföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Exempel: kravhantering, arkivering, myndighetsbeslut som tillstånd och bygglov.

3.5.2 Extra skyddsvärda personuppgifter

Extra skyddsvärda personuppgifter är uppgifter som kan vara integritetskänsliga men som inte är känsliga enligt förordningen Artikel 9.

Exempel är personuppgifter om barn, uppgifter av personlig karaktär kopplad till familjeförhållanden eller ekonomi. Dessa personuppgifter ska behandlas med försiktighet och bör betraktas som känsliga personuppgifter när rätt säkerhetsnivå ska sättas. Speciellt ska försiktighet iakttas då personuppgifterna är åtkomliga över internet.

3.5.3 Otillåten behandling

Det är förbjudet att behandla känsliga personuppgifter enligt ([artikel 9.1](#)) (personuppgifter av särskild karaktär). Det går att göra undantag från förbudet om behandlingen är absolut nödvändig eller vid samtycke ([artikel 9.2](#)).

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

3.6 Offentlighetsprincipen

Offentlighetsprincipen innebär en rättighet för var och en att ta del av allmänna handlingar. Innan kommunen lämnar ut handlingar genomförs en sekretessprövning. Bara för att viss information förmodligen skulle bedömas som allmän handling vid en sekretessprövning innebär det inte att vem som helst inom förvaltningen får ta del av personuppgifterna om det inte behövs för att vederbörande ska kunna utföra sitt jobb.

3.7 Personuppgifter på sociala medier inom kommunen

Ansvar för behandling av personuppgifter via sociala medier kan delas in i två delar:

- ansvaret för Mjölby kommuns egna inlägg och publiceringar och
- ansvaret för inlägg som publiceras av användare

När det gäller Facebook, Instagram, LinkedIn, bloggar och liknande medier är Mjölby kommun ansvarig för alla personuppgifter som publiceras i våra kanaler. Ansvar gäller både personuppgifter som vi själva publicerar samt de personuppgifter som publiceras av andra, exempelvis genom kommentarer.

Vi är skyldiga att övervaka så att kommentarer som läsare lägger in exempelvis inte är kränkande. Även besökaren har ett ansvar för det som skrivs.

För Twitter ansvarar kommunen endast för det vi själva publicerar, inte för personuppgifter som andra twittrare lämnar, det beror på att vi inte har möjligheter att påverka inläggen som i övriga medier.

I övrigt ska all publicering på sociala medier följa ["Riktlinjer för Mjölby kommuns webbplats, intranät, sociala medier och andra elektroniska forum"](#)

3.7.1 Personuppgifter på webben (hemsida och intranät)

Personuppgifter om enskilda får endast publiceras på webben om det finns rättslig grund för publiceringen. På webbsidan får du publicera harmlösa personuppgifter om tjänstemän och förtroendevalda som har anknytning till deras tjänsteutövning eller uppdrag. Det kan röra sig om exempelvis namn, befattning, telefonnummer, e-postadress eller politisk tillhörighet. Denna publicering bygger på att det finns ett allmänt intresse som laglig grund. Det krävs alltså inget samtycke, men man ska som vanligt informera om alla behandlingar av personuppgifter.

Personuppgifter rörande enskilda får publiceras om uppgifterna inte kan leda till att personens integritet kränks. Tänk på att personuppgifter som enskilt betraktas som harmlösa kan vid en publicering på webben komma att anses som kränkande beroende på sammanhang och övrigt innehåll i texten.

3.7.2 Bilder på webben och övriga sociala medier (Facebook, Instagram o.s.v)

Generellt ska kommunen vara mycket restriktiv att publicera personuppgifter i dessa medier såvida det inte anses nödvändigt av någon orsak och att det finns en rättslig grund och ett tydligt syfte.

Nedan följer några viktiga råd som alltid ska beaktas vid publicering av bilder på webben eller sociala medier.

- Det måste alltid finnas en rättslig grund som för övriga personuppgifter
- Bilderna får inte vara kränkande, i sig eller i sitt sammanhang
- Undvik samtycke som rättslig grund, den är högst tveksam för en kommun att använda för medarbetare och medborgare. Se rubriken artikel 6.1 a Samtycke.
- "Mingelbilder" kan vara tillåtet såvida inte personerna på bilden går att identifiera med enkelhet. För att bilden ska anses som "godkänd" är en tumregel att det ska behövas ett förstoringsglas för att identifiera personen.
- Personuppgifter, inklusive bilder, som läggs ut på webben eller andra sociala medier ska tas bort så fort de inte är aktuella längre. Det är inte tillåtet att spara personuppgifter längre än nödvändigt.

3.8 De registrerades rättigheter

När Mjölby kommun behandlar personuppgifter har den registrerade vissa rättigheter. Den registrerade har naturligtvis rätt till information om personuppgifterna som behandlas ([artikel 15](#)). Kommunen har anmälningsskyldighet när det gäller rättelse, radering eller begränsning av behandling ([artikel 19](#)) och de fall uppgifter har rättats är det viktigt att övriga som tagit del av samma uppgifter får vetskap om det

Övriga rättigheter är:

- Rätt till rättelse av uppgifterna ([artikel 16](#))
- Rätt att få sina personuppgifter raderade ([artikel 17](#))
- Rätt till begränsning av behandling ([artikel 18](#))
- Rätt till portabilitet (den registrerade har rätt att få ut och/eller överföra sina uppgifter till annan personuppgiftsansvarig när det är tekniskt möjligt). ([artikel 20](#))
- Rätt att göra invändningar ([artikel 21](#))
- Automatiserat beslutsfattande, profilering (gäller främst kommersiella verksamheter) ([artikel 22](#))
- Information till den registrerade om personuppgiftsincident ([artikel 34](#))
[Mer information om personuppgiftsincidenter enligt kapitel nedan.](#)

3.9 Barnperspektivet

Barn förtjänar ett särskilt skydd enligt dataskyddsförordningen ([artikel 8](#)). Barn under 16 år ges särskilt skydd vilket gör att information som riktar sig till barn ska vara skriven på ett tydligt och enkelt sätt som barn förstår.

3.10 Personuppgiftsincidenter

Personuppgiftsincidenter ([artikel 33](#)) ska anmälas av den personuppgiftsansvarige (eller personuppgiftsbiträdet) så fort som möjligt till Integritetsskyddsmyndigheten (IMY) men senast inom 72 timmar från det att händelsen upptäcks. Information till den registrerade vid en personuppgiftsincident ska ske utan dröjsmål om det är hög risk för personens rättigheter och friheter ([artikel 34](#))

3.11 Risk- och konsekvensbedömning avseende dataskydd

När kommunen behandlar personuppgifter och upprättar en registerförteckning ska en första bedömning genomföras för att värdera risken för den registrerade om personuppgifterna skulle spridas enligt ([artikel 35](#)). Riskerna bedöms av kommunen som hög i de fall vi behandlar personuppgifter av särskilda kategorier (känsliga personuppgifter) vilket alltid påkallar en risk- och konsekvensbedömning där dataskyddsombudet (DSO) alltid ska rådfrågas. Det kan vara aktuellt med samråd med tillsynsmyndigheten om inte säkerheten kan garanteras för behandlingen.

3.12 Upprätta personuppgiftsbiträdesavtal

Kommunen som personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter, men personuppgiftsansvaret kan aldrig överlåtas.

För att kunna följa lagstiftningen är det viktigt att ha kontroll över vilka externa organisationer som har åtkomst till kommunens personuppgifter. Åtkomst kan vara enbart teknisk support eller att den tekniska miljön hanteras av en tredje part (extern drift).

När en annan part hanterar personuppgifter åt kommunen kallas den parten för personuppgiftsbiträde, ([artikel 28.3](#)). När kommunen har anlitat ett personuppgiftsbiträde ska det upprättas ett skriftligt avtal, personuppgiftsbiträdesavtal, som reglerar dataskyddsfrågorna. Lagstiftningen ställer stora krav på hur avtalet är utformat, därför har Mjölby kommun beslutat att i möjligaste mån använda Sveriges Kommuner och Regioner (SK) mall för dessa avtal. Påskrift av ett personuppgiftsbiträdesavtal ska följa den ordinarie delegationsordningen.

Avtalet ska upprättas, inte bara när vår externa part lagrar personuppgifter och sköter driften av ett system, utan också när biträdet har åtkomst till personuppgifterna på distans, exempelvis för support, service, underhåll eller utveckling.

4. Ansvar och uppföljning

4.1 Organisation för efterlevnad av Dataskyddsförordningen

Mjölby kommun har inrättat ett dataskyddsnätverk för att stötta verksamheterna i arbetet för efterlevnad av Dataskyddsförordningen. Sammanställande för nätverket är kommunens dataskyddsombud (DSO), ([artikel 37,38,39](#)). Övriga deltagare i nätverket är förvaltningarnas personuppgiftssamordnare.

I nätverket deltar dataskyddsombudet som stöd vid framtagande av övergripande rutiner och har en rådgivande och reviderande roll. Nätverket är kontaktytan mellan personuppgiftssamordnare och dataskyddsombud. Säkerhetsansvarig på IT-avdelningen har en adjungerande roll i nätverket

4.2 Roller

4.2.1 Dataskyddsombud

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att Mjölby kommun följer dataskyddsförordningen. Det innebär bland annat att:

- samla in information om hur organisationen behandlar personuppgifter
- kontrollera att organisationen följer bestämmelser och interna styrdokument
- informera och ge råd inom organisationen
- ge råd om konsekvensbedömningar
- vara kontaktperson för Integritetsskyddsmyndigheten (IMY)
- vara kontaktperson för de registrerade och personalen inom organisationen
- samarbeta med Integritetsskyddsmyndigheten (IMY) till exempel vid inspektioner
- stödja verksamheterna vid tecknande av personuppgiftsbiträdesavtal
- bidra till utvecklingen av gemensamma rutiner och arbetssätt för att uppfylla dataskyddsförordningen

4.2.2 Personuppgiftssamordnarens uppdrag

- ser till att alla pågående personuppgiftsbehandlingsdokumenteras i en registerförteckning
- stöttar verksamheterna vid begäran om registerutdrag
- ger råd och stöd till verksamheten och berörd personal i frågor rörande behandling av personuppgifter
- håller sig underrättad om utveckling av lagstiftningen inom området för behandling av personuppgifter
- håller sig underrättad om datainspektionens verksamhet
- rådfrågar och samråder med dataskyddsbudet
- tillsammans med dataskyddsbudet arbetar långsiktigt med att anpassa behandling av personuppgifter så att den sker enligt dataskyddsförordningen

4.3 Kontaktuppgifter dataskyddsbud

Om det råder en osäkerhet om lämplighet, rättslig grund eller annat vad gäller personuppgifter på webben eller sociala medier ska personuppgiftssamordnare eller dataskyddsbud rådfrågas.

Postadress:

Mjölby kommun
Burensköldsvägen 11
595 80 Mjölby

E-postadress: dataskyddsbud@mjolby.se

Tel: 010-234 50 00 (växel)



Kommunstyrelsens förvaltning
Kommunstyrelsens Förvaltning
Telefon: 0142-850 00
E-post: [mjölbykommun@mjolby.se](mailto:mjolbykommun@mjolby.se)
Burensköldsvägen 11-13, 595 80 Mjölby

