# Riktlinjer för personuppgiftshantering

## 1. Inledning

*Bakgrund*

Personuppgifter hanteras från och med den 25 maj 2018 enligt EU:s dataskyddsförordning (2016/679) och kompletterande nationell lagstiftning inom dataskyddsområdet.

Dataskyddsförordningen är direkt tillämplig som svensk lag. Målet med det nya regelverket är att stärka den enskildes rättigheter och harmonisera skyddet för personuppgifter inom EU.

*Syfte*

Syftet med riktlinjerna är att ge anvisningar om hur dataskyddsförordningen omsätts i praktiken i Marks kommun.

## 2. Ansvar

*Personuppgiftsansvarig nämnd/bolag*

Varje nämnd och bolag är personuppgiftsansvarig för de behandlingar av personuppgifter som sker i dess verksamhet. För personuppgifts-behandlingar som är kommunövergripande är kommunstyrelsen ensamt personuppgiftsansvarig. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs.

Personuppgiftsansvarig ska se till att en fullgod säkerhetsnivå upprätthålls vid behandling av personuppgifter. Nämnden/bolaget ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå utifrån de kriterier som anges i dataskyddsförord-ningen.

Personuppgiftsansvarig ska säkerställa att dataskyddsombudet involveras och rådfrågas på ett så tidigt stadium som möjligt när behandling av personuppgifter kan komma i fråga.

*Övrigt*

Alla inom kommunen ansvarar för att inte behandla personuppgifter i större utsträckning eller under längre tid än vad som är nödvändigt.

## 3. Organisation för dataskydd

*Dataskyddsombud*

Varje personuppgiftsansvarig ska utse ett dataskyddsombud för sin organisation. Vid valet av dataskyddsombud ska samordning ske inom kommunen. Dataskyddsombudet ska rapportera direkt till förvaltningsledningen.

Dataskyddsombudets uppgifter är bland annat att övervaka efterlevnaden av dataskyddsförordningen samt att informera och ge råd till den personuppgiftsansvarige, dess anställda och vid behov till de personuppgiftsbiträden som anlitas. Dataskyddsombudet har även att vara kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling av personuppgifter.

Dataskyddsombudet ska årligen för nämnden eller bolagsstyrelsen redovisa hur dataskyddsarbetet fortlöper och hur bestämmelserna inom dataskyddsområdet, inklusive dessa riktlinjer, uppfylls. Redovisningen ska inkludera vilka informationsinsatser som har skett under året, vilka brister som har identifierats och hur de åtgärdas samt eventuella personuppgiftsincidenter som har inträffat. Kommunstyrelsen ska få redovisning även vad gäller övriga nämnder och bolag i kommunen.

### *Dataskyddsassistenter*

Varje personuppgiftsansvarig ska utse minst en dataskyddsassistent för sin organisation. Dataskyddsassistenten ska bistå dataskyddsombudet med det praktiska arbetet i den personuppgiftsansvariges organisation genom att bidra med detaljkunskap om verksamheten. Dataskydds-assistenten leder arbetet med att förteckningar över verksamhetens personuppgiftsbehandlingar förs löpande, uppdateras och rapporteras till dataskyddsombudet.

### *Samordning av dataskyddsarbete*

Dataskyddsombudet ska samordna kommunens dataskyddsarbete tillsammans med dataskyddsassistenterna.

Dataskyddsombudet och dataskyddsassistenterna ska träffas minst två gånger årligen för att diskutera gemensamma frågor och följa upp hur dataskyddsarbetet fortgår i verksamheterna.

## 4. Personuppgiftshantering

### *Tekniska och organisatoriska förutsättningar*

Varje personuppgiftsansvarig ska arbeta strategiskt med frågan om dataskydd för att säkerställa att det finns organisatoriska och tekniska förutsättningar i verksamheten för att leva upp till de krav som ställs, däribland innebärande att det i organisationen finns rätt resurser och relevant kompetens.

Personuppgiftsansvarigs förvaltningsledning ska, om nödvändigt, utarbeta en handlingsplan för dataskyddsarbetet i organisationen i samråd med dataskyddsombudet.

### *Förteckning över personuppgiftsbehandlingar*

Varje personuppgiftsansvarig ska föra ett register över personuppgiftsbehandlingar som utförs under dess ansvar (förteckning).

Förteckningen ska uppdateras löpande och förändringar rapporteras, via dataskyddsassistenten, till dataskyddsombudet.

Dataskyddsombudet ska hålla de personuppgiftsansvarigas förteckningar samlade och tillgängliga för andra att ta del av.

*Gallring eller arkivering*

Personuppgifter får inte behandlas i något avseende i större utsträckning än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Personuppgifter som i denna mening inte längre är nödvändiga ska antingen gallras (förstöras) eller arkiveras. Varje nämnd och bolag måste därför fatta beslut om när handlingar som innehåller personuppgifter ska gallras eller att arkivering ska ske, vilket anges i dokumenthanteringsplanen. Varje personuppgiftsansvarig har att upprätta rutiner för hur gallringen ska ske och uppföljning av det. Bedömningen av vad som ska gallras ska göras minst en gång per år.

*Tjänster och produkter som medför behandling av personuppgifter*

För varje tjänst och produkt som används eller som finns planer på att använda, ska särskilt beaktas om avtalsförhållandet eller användandet av tjänsten/produkten kan komma att medföra behandling av personuppgifter. För det fall personuppgifter kommer att behandlas ska säkerställas att det finns förutsättningar att fullgöra skyldigheterna avseende dataskydd.

*Inköp och upphandling*

Vid inköp och upphandlingar av produkter och tjänster som medför behandling av personuppgifter ska krav ställas på att produkten eller tjänsten lever upp till kraven i dataskyddsförordningen och annan nationell lagstiftning inom dataskyddsområdet. Detta inkluderar, i tillämpliga fall, kravet att leverantören ska teckna ett personuppgiftsbiträdesavtal med personuppgiftsansvarig i kommunen.

Både huvudavtalen och biträdesavtalen ska hållas ordnade så att de är lätta att hitta och hänvisa till.

Vid inköp och upphandlingar av produkter och tjänster bör upphandlingsdokumentet, när det är lämpligt, utformas på ett sätt som ger incitament för anbudsgivare att driva på utvecklingen enligt principerna om inbyggt dataskydd och dataskydd som standard (*privacy by design* och *privacy by default*).

Inköp- eller upphandlingsansvarig ska inför anskaffandet av nya produkter eller tjänster, och när det bedöms nödvändigt, involvera dataskyddsombudet i processen.

*Konsekvensbedömning*

Vid införandet av nya personuppgiftsbehandlingar som särskilt rör användning av ny teknik ska personuppgiftsansvarig genomföra en bedömning av konsekvenserna för de registrerades rättigheter och friheter.

Konsekvensbedömningen ska genomföras innan implementeringen av den nya behandlingen och ske i samråd med dataskyddsombudet. Samrådet ska dokumenteras ihop med konsekvensbedömningen.

En konsekvensbedömning ska innehålla en beskrivning av

- personuppgiftsbehandlingen och dess syfte,
- risker för fysiska personers rättigheter och friheter,
- nödvändigheten och proportionaliteten i förhållande till riskerna,
- åtgärder som planeras för att hantera de identifierade riskerna, och
- hur planerade säkerhetsåtgärder ska dokumenteras.

Ansvaret för att utföra konsekvensbedömningen utpekas av berörd chef i varje enskilt fall.

*Systembehörigheter*

Personuppgiftsansvarig ska se till att systembehörigheter som medför åtkomst till personuppgifter ska fördelas och uppdateras på ett ordnat sätt.

Anställda ska endast ges åtkomst till uppgifter då det är motiverat utifrån verksamhetens behov. Om en anställd inte längre har behov av åtkomsten ska behörigheten dras in.

Chefer ansvarar för att avgöra vilka systembehörigheter som deras anställda har behov av och att det finns rutiner för att hålla dessa behörigheter uppdaterade.

*Personuppgiftsincidenter*

Om personuppgiftsincident upptäcks, som sannolikt medför risk för fysiska personers rättigheter och friheter, ska dataskyddsassistenten, i samråd med dataskyddsombud, upprätta en anmälan till tillsynsmyndigheten. Anmälan ska skickas till tillsynsmyndigheten senast 72 timmar efter det att personuppgiftsincidenten upptäckts. Dataskyddsombudet för efterföljande kontakter med tillsynsmyndigheten.

Anmälan ska utformas i enlighet med de anvisningar som lämnas av tillsynsmyndigheten.

Anmälan och utredningen kring denna ska dokumenteras hos den personuppgiftsansvarige. Dokumentationen ska innehålla en beskrivning av

- personuppgiftsincidentens art och omfattning,
- vilka typer av personuppgifter som berörs,
- konsekvenserna för de registrerade,

- personuppgiftsansvariges åtgärdsarbete, och
- information som, i tillämpliga fall, lämnats till de registrerade.

Varje personuppgiftsansvarig ska upprätta rutiner för att kunna förebygga och upptäcka personuppgiftsincidenter.

*Hantering av registrerades rättigheter*

Varje personuppgiftsansvarig ska upprätta rutiner för hur registrerades rättigheter ska tillgodoses, särskilt avseende rätten till information om personuppgiftsbehandlingen och tillgång till sina personuppgifter (registerutdrag), samt rätten till rättelse av felaktiga uppgifter. Informationen har att lämnas skriftligt i samband med att personuppgifter samlas in från den registrerade eller på annat lämpligt sätt.

Om registrerad vänder sig till en enskild personuppgiftsansvarig men gör gällande rättigheter avseende personuppgiftsbehandlingar som förekommer hos flera personuppgiftsansvariga i kommunen, ansvarar den personuppgiftsansvarige som mottagit begäran för att samordna denna tillsammans med berörda personuppgiftsansvariga. Samordningen bör ske genom dataskyddsassistenterna.

## 5. Särskilda hanteringsregler

*Hantering av personuppgifter i fritext (Epost m.m.)*

Personuppgiftsbehandling som sker i fritext, till exempel i ordbehandlingsprogram, epost eller fritextfält i verksamhetssystem, ska ske med respekt för den registrerades integritet och begränsas till sådan omfattning som är nödvändig för verksamhetens behov.

Känsliga personuppgifter och personnummer bör i möjligaste mån undvikas att kommuniceras via epost, internchat eller liknande system. Om det ändå är nödvändigt ska adekvata skyddsåtgärder vidtas för att garantera en säker behandling av personuppgifterna.

*Publicering av personuppgifter på webben*

Personuppgifter får endast publiceras på webben om den registrerade har lämnat ett giltigt samtycke till det, eller då publiceringen kan motiveras utifrån ett allmänt intresse av information om kommunens verksamhet. Personuppgifter som rör förtroendevalda och anställda får publiceras om uppgifterna har samband med deras uppdrag eller tjänsteutövning.

Känsliga personuppgifter och extra skyddsvärda personuppgifter får aldrig publiceras på webbplatsen.

## 6. Personuppgiftsbiträde

När personuppgiftsansvarig anlitar personuppgiftsbiträde som behandlar personuppgifter för personuppgiftsansvarigs räkning, ska personuppgiftsbiträdesavtal tecknas.

I de fall verksamhetsspecifika behandlingar tillhandahålls genom kommunens centrala IT-stöd utgör kommunstyrelsen ett personuppgiftsbiträde till den personuppgiftsansvariga nämnden eller bolaget. Kommunstyrelsen ska i dessa fall endast utföra sådan behandling som är nödvändig för att tillhandahålla IT-stödet och följa de instruktioner som personuppgiftsansvarig lämnar.