Gemensamma anvisningar för säkra digitala meddelanden

Diarienummer:	2024/00206
Paragraf:	§
Beslutsinstans:	
Beslutsdatum:	
Informationsklassning:	
Dokumentansvarig:	
Giltighetstid:	
Föregående diarienummer:	
Föregående beslutsdatum:	
Föregående beslutsinstans:	
Föregående paragraf:	

Motala kommun
Gemensam Ledningsförvaltning

Motala kommun

Gemensamma anvisningar för säkra digitala meddelanden

Inledning

Anvisning för säkra digitala meddelanden.

Detta dokument specificerar riktlinjerna för kommunikation inom organisationen, särskilt när det gäller hantering av känsliga personuppgifter och information som omfattas av sekretess.

Definition av Känsliga Personuppgifter

Enligt GDPR inkluderar känsliga personuppgifter information som kan identifiera en person baserat på:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i en fackförening
- Genetiska och biometriska data för unik identifiering av en individ
- Hälsorelaterad information
- Uppgifter om en persons sexualliv eller sexuell läggning

Tänk på att:

- Säkerställ att det finns godtagbar laglig grund vid behandling av känsliga personuppgifter.
- Vid behandling av känsliga personuppgifter behöver i regel särskilda skyddsåtgärder vidtas.
- Om känsliga personuppgifter skickas i e-post är det särskild viktigt att märka det med Känslig eller Mycket känslig.

Personnummer

Personnummer är inte en känslig personuppgift men betraktas som extra skyddsvärd. Behandling av personnummer får endast ske om den enskilde har gett sitt samtycke, om behandlingen är klart motiverad med hänsyn till ändamålet, vikten av en säker identifiering eller något annat beaktansvärt skäl. Vi måste därför vara försiktiga med att använda personnummer och alltid säkerställa att behandlingen sker med godtagbar laglig grund.

Foton

Foton på personer är personuppgifter och får, liksom andra personuppgifter, behandlas endast för dokumenterade ändamål. Publicering av foton på personer kan ske med stöd av samtycke eller avtal som rättslig grund. Om samtycke används som rättslig grund måste det vara lika enkelt att återkalla samtycket som att samtycka till behandlingen för den registrerade. Samtycken samlas in på en särskild blankett. Foton på anställda och konsulter som kommunen använder för säker identifiering och kommunikationsändamål får inte behandlas för andra ändamål.

Sekretess

Offentlighet och sekretesslagen styr vilken information som är underlagd sekretess. Denna information får inte delas med obehöriga, varken muntligt eller skriftligt. Alla medarbetare är bundna av tystnadsplikt, vilket de informerats om och godkänt vid anställningens start.

Vid hantering av kommunens information är varje medarbetare ansvarig för att inte röja en uppgift om den är belagd med sekretess. Delvis har Motala kommuns informationssäkerhetspolicy (19/KS 0116) utformats utifrån den bakgrunden. Varje informationsmängd ska vara klassad utifrån konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Riktlinjer för säkra digitala meddelanden

Kommunikationskanaler

När det kommer till utbyte av känsliga personuppgifter eller sekretessbelagd information, är det avgörande att använda godkända och säkra kommunikationskanaler. Det är viktigt att notera:

- **Outlook och Teams:**
  Dessa plattformar ska **inte** användas för utbyte av känsliga personuppgifter eller sekretessbelagd information. Även om de erbjuder bekvämlighet för daglig kommunikation inom organisationen, uppfyller de inte kraven för säker överföring av känsliga uppgifter.
- **Sefos:**
  Detta är den godkända plattformen för säkra meddelanden inom organisationen. Sefos är speciellt utformat för att hantera känsliga personuppgifter och sekretessbelagd information, med lämpliga säkerhetsåtgärder och kryptering som skyddar dataintegritet och konfidentialitet.

Ytterligare Säkerhetsåtgärder

För att ytterligare stärka säkerheten vid hantering av känsliga meddelanden, bör följande riktlinjer följas:

1. **Verifiera Mottagaren**
   Säkerställ mottagarens identitet innan känslig information skickas.
2. **Begränsa Tillgången**
   Endast behöriga personer med ett verkligt behov av att känna till informationen bör ha tillgång till den.
3. **Undvik Vidarebefordran**
   Meddelanden som innehåller känsliga uppgifter får inte vidarebefordras utan uttryckligt godkännande.
4. **Hantering av Data**
   Följ organisationens policy för lagring och radering av känsliga meddelanden.
5. **Du ansvarar även för att e-post hanteras korrekt**
   Använd endast arbetsrelaterad e-postklient för att skicka och ta emot e-post och använd inte din Motala-adress för privata ändamål.

Medvetenhet

Dessa riktlinjer är avsedda att säkerställa att all kommunikation av känsliga uppgifter inom organisationen sker på ett säkert sätt, i enlighet med gällande lagstiftning och interna policyer. Varje medarbetare har ett ansvar att följa dessa anvisningar i sitt arbete.