MELLERUDS KOMMUN

Riktlinje för informationshantering

Styrande dokument inom Socialförvaltningen		**Övergripande processområde** Riktlinje	**Verksamhetens process** Informationshantering	
Dokumentägare, sektor/enhet Stab och administration		**Upprättad av** Adis Pepic, verksamhetsutvecklare	**Godkänd av** Socialnämnden 2025-09-23, § 145, dnr. SN-2025-00127	
Upprättad 2025-09-10	**Publicerad** 2025-09-24	**Giltighetstid** Tillsvidare	**Revisionshistoria** 2025-09-10	**Version nr** 2.0

Socialförvaltningen
Besöksadress: Storgatan 13, 464 80 Mellerud **Telefon**: 0530-180 00 **E-post**: kommunen@mellerud.se
Bankgiro: 5502-2776 **Organisationsnummer**: 212000-1488 **Webbplats**: www.mellerud.se

Innehåll

Syfte och principer för informationshantering 3
Allmän handling 3
Hantera personuppgifter 4
Skicka och ta emot sekretessbelagd, extra skyddsvärd eller känslig information 5
Behörighetstilldelning i verksamhetssystem 5
Kontroll av åtkomst till personuppgifter, loggkontroll 6
Sekretess 6
Inre sekretess 6
Tystnadsplikt 6
Lagringsytor som rekommenderas 7
Lagringsytor för användning i begränsad omfattning 8
Lagringsytor som ska undvikas 8
Lagra privat information 8

Syfte och principer för informationshantering

Förvaringsplatsen för var handlingar ska lagras beror på typ, användningsområde och vad som anges i gällande dokumenthanteringsplan. Av planen framgår även vilka handlingar som ska gallras och när det ska ske. Dessa riktlinjer ska stödja och underlätta en enhetlig informationshantering.
Handlingar kan delas in i intern, offentlig eller sekretessreglerad. Du som medarbetare har en skyldighet att sätta dig in i de lagar och regler som gäller inom ditt ansvarsområde och lagra den information du behöver i ditt arbete på ett riktigt och strukturerat sätt. Oavsett var information lagras lyder den under offentlighetsprincipen och kan komma att begäras ut.

Riktlinjerna baseras på:

- Tryckfrihetsförordning (1949:105)
- Offentlighets- och sekretesslag (2009:400)
- Arkivlag (1990:782)
- General Data Protection Regulation (EU 679/2016)
- Socialtjänstlag (2025:400)
- Lagen om stöd och service till vissa funktionshindrade (1993:387)
- Patientsäkerhetslag (2010:659)

Allmän handling

Offentlighetslagstiftningen (Tryckfrihetsförordning, Offentlighets- och sekretesslag samt Arkivlag) ställer krav på hur myndigheten hanterar allmänna handlingar.
Tryckfrihetsförordningen är en av Sveriges fyra grundlagar. Grundlagarna ska skydda vår demokrati och står över alla andra lagar. Det betyder att innehållet i andra lagar aldrig får strida mot vad som står i grundlag.

I Tryckfrihetsförordningens 2 kap Allmänna handlingars offentlighet definieras handling samt allmänhetens rätt att ta del av allmänna handlingar.

Handling - lagrad information som man kan ta del av gång på gång, medieoberoende.

Allmän - om en handling förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos en myndighet.

Begäran om utlämnande av allmän handling ska ställas till den myndighet som förvarar handlingen. I en kommunal nämndorganisation är varje nämnd med underlydande förvaltning en myndighet. Offentliga handlingar som begärts ska lämnas ut ”genast”. Sekretessreglerade handlingar som begärts ska lämnas ut ”skyndsamt”. Den som begär ut en handling har rätt att vara anonym och behöver inte ange syfte.

Allmänna handlingar är antingen offentliga eller sekretessreglerade i enlighet med någon bestämmelse i Offentlighets- och sekretesslag. Sekretessreglerade allmänna handlingar måste i princip alltid registreras enligt Offentlighet- och sekretesslag 5 kap 1 §. Dessa handlingar ska registreras samma dag eller senast dagen efter att de upprättats, inkommit eller expedierats (skickats ut). Registreringsskyldigheten gäller inte om det är uppenbart att en allmän handling är av ringa betydelse för myndighetens verksamhet, då behöver den varken registreras eller hållas ordnad. Exempelvis enklare förfrågningar, reklam, kurserbjudanden med mera. Handlingar som inte omfattas av sekretess behöver inte registreras om de hålls ordnade så att de utan svårighet kan fastställas om de har inkommit eller upprättats.

Arbetsmaterial och minnesanteckningar (intern information/dokument) är inte allmänna handlingar. Vem som är avsändare och mottagare samt innehållet i ett e-postmeddelande avgör om meddelandet är en allmän handling. Här följer en närmare beskrivning av vilken typ av e-post som är en allmän handling.

Extern e-post;

- som skickas mellan myndigheten och en extern person är som huvudregel en allmän handling.

Intern e-post;

- som inte tillhör något ärende men som färdigställts på något sätt, till exempel färdiga mötesanteckningar som skickas ut efter ett möte eller färdigställd information som skickas till en större grupp, exempelvis ett internt nyhetsbrev är en allmän handling.
- som tillhör ett pågående ärende blir allmän handling först när ärendet avslutats. Ett ärende kännetecknas av att handläggningen avslutas med ett beslut.

Privat e-post som inte rör verksamheten är inte en allmän handling. Detta gäller oavsett om meddelandet skickas externt eller internt.

Om en handling ska registreras ska följande uppgifter finnas enligt offentlighets- och sekretesslagen:

- Datum då handlingen kom in eller upprättades.
- Diarienummer eller annan beteckning handlingen fått vid registreringen.
- I förekommande fall uppgifter om handlingens avsändare eller mottagare.
- I korthet vad handlingen rör (ärendemening).

Hantera personuppgifter

Dataskyddsförordningen (GDPR) har sedan 2018 ersätt Personuppgiftslagen och reglerar hur myndigheten får behandla av personuppgifter. Med personuppgift avses i Dataskyddsförordning varje upplysning som avser en identifierad eller identifierbar fysisk person. Det övergripande syftet med förordningen är att säkerställa människors rätt till skydd av sina personuppgifter och därmed rätten till skydd för privatlivet. Ett annat mycket viktigt syfte är att fastställa regler för det fria flödet av personuppgifter inom EU och därmed lägga grund för en ökad digitalisering inom EU.

Den personuppgiftsansvarige och personuppgiftsbiträdet får behandla personuppgifter endast på de grunder som framgår av Dataskyddsförordning.

Personuppgifter får behandlas om:

- den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål
- behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås
- behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige
- behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person
- behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
- behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Den personuppgiftsansvarige är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen

för behandlingen av personuppgifter. Personuppgiftsbiträdet är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Enligt Dataskyddsförordning ska den personuppgiftsansvarige ansvara för att dessa principer och krav efterlevs. Dessutom ska den personuppgiftsansvarige kunna visa att principerna och kraven har efterlevts.

Som känsliga personuppgifter enligt dataskyddsförordningen betecknas uppgifter som avslöjar:

- etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som entydigt identifierar en person

Exempel på personuppgifter som normalt är att anse som känsliga ur ett integritetsperspektiv:

- enskilds ekonomiska förhållanden
- uppgifter om lagöverträdelser

Personuppgifter som är extra skyddsvärda är:

- personnummer
- samordningsnummer

Sammanfattningsvis är inrådan att låta bli att samla in, använda eller lagra personuppgifter om du inte behöver det och radera uppgifterna så snart syftet för att du samlade in uppgifterna är uppnått.

Skicka och ta emot sekretessbelagd, extra skyddsvärd eller känslig information

All kommunikation som omfattas av sekretess, innehåller extra skyddsvärd eller känslig information om personer får endast skickas via digitala media om det är krypterat med en av kommunen godkänd standard för kryptering. Detta gäller således för såväl e-post som snabbmeddelanden eller annan digital kommunikation.

I Mellerud har enheten för digital service beslutat att vi internt inom kommunen får använda mailen i Microsoft 365 för sekretessbelagd information, men vi får inte långtidsförvara den där. Det innebär att vi under kort tid kan hantera informationen i Microsoft 365, men efter att mailet är skickat eller mottaget måste den raderas helt (både från in- och utkorgen samt papperskorgen).
Om du behöver kommunicera med extern innehållande sekretessbelagd, extra skyddsvärd eller känslig information använder vi tjänsten ”Säkra meddelanden". Precis som vid all användning av personuppgifter måste det även vid säkra meddelanden finnas ett tydligt ändamål för behandlingen och en laglig grund (det vill säga stöd i lagen) alternativt ett samtycke.

Behörighetstilldelning i verksamhetssystem

I verksamhetssystem är det viktigt att behörigheter är satta för att inte visa vare sig mer eller mindre information än vad respektive medarbetare behöver för att kunna utföra sitt arbete. Systemförvaltare för respektive system är ansvarig för att sätta behörigheter. Behörighetstilldelning sker av respektive chef efter behovs- och riskanalys. Det är även respektive chefs ansvar att underrätta systemansvarig om medarbetare slutar eller om behörighet ska ändras.

Kontroll av åtkomst till personuppgifter, loggkontroll

I de system där det finns en loggfunktion så ska loggkontroll genomföras. Det innebär att det som en användare gör i systemet kan spåras. Det finns en behandlingshistorik som berättar vem, vad, när och var i systemen det har varit en händelse. Systemförvaltare bör i första hand använda testpersoner för felsökning och andra arbetsuppgifter där personuppgifter krävs. Systemförvaltare för respektive system gör stickprov med urval av loggar enligt rutin för det systematiska kvalitetsarbetet. Utgångspunkten är att den som har rätt att utdela behörighet till system också ska granska loggen.

Sekretess

Sekretess innebär att det finns uppgifter i handlingen som inte får röjas vare sig muntligen eller genom utlämnande av handlingen. Innehållet i en handling som berörs av sekretess som begärts ut ska därför alltid sekretessprövas av myndigheten utifrån Offentlighets- och sekretesslagen innan handlingen kan lämnas ut. När man gör en sekretessprövning bedömer man om syftet med begäran är rimlig. Sekretess gäller inom socialtjänsten för uppgift om enskilds personliga förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men enligt 26 kap 1 § Offentlighets- och sekretesslag.

En handling som innehåller sekretessbelagda uppgifter ska lämnas ut i de delar som inte omfattas av sekretess. När sekretessbelagda uppgifter behöver döljas i en handling som i övrigt ska lämnas ut, ska handlingen maskas så att det tydligt framgår vilka delar av handlingen som har sekretessbelagts. Den som utlämnar sekretessbelagda uppgifter ska i dessa fall maskera personuppgifter och sådana uppgifter som man bedömer är av en känslig natur och/eller kan komma den som handlingen rör till skada. Om det som begärs ut inte bedöms utgöra en allmän handling, eller om hela eller delar av handlingen inte kan lämnas ut på grund av sekretess så har den som begärt handlingen rätt att begära att myndigheten prövar om handlingen ska lämnas ut i sin helhet. Om myndigheten bedömer att handlingen inte kan lämnas ut i sin helhet har den enskilde rätt att få ett överklagbart avslagsbeslut. Av delegationsbestämmelserna framgår vem som kan lämna ett sådant beslut. För uppgift i allmän handling inom socialtjänst gäller sekretessen i 70 år från det att handlingen inkommit eller upprättats.

Inre sekretess

Sekretessen gäller utåt, det vill säga gentemot enskilda och andra myndigheter.
Men även inom samma nämnd kan det ändå finnas sekretessgränser. Exempelvis hälso- och sjukvårdsverksamhet som styrs av andra sekretessbestämmelser såsom 12 § Patientsäkerhetslagen och 25 kap Offentlighets- och sekretesslag. För att dela information över sekretessgränser om det inte i lag finns sekretessbrytande bestämmelser krävs att den enskilde samtycker till detta.

Om den enhet eller avdelning som du avser kontakta ligger inom samma nämnd och inte utgör någon självständig verksamhetsgren, gäller inte sekretess enligt Offentlighets- och sekretesslagen. Däremot gäller så kallad inre sekretess, vilket innebär att personuppgifter bara får lämnas ut i den utsträckning som är normal eller behövlig för ett ärendes handläggning eller för verksamhetens bedrivande i övrigt, inte i större omfattning. Inre sekretess handlar förenklat om att du har en skyldighet att hantera uppgifter om den enskilde på ett ansvarsfullt sätt, även internt.

Tystnadsplikt

Tystnadsplikt gäller för den som har varit eller är yrkesmässigt verksam i enenskild verksamhetvars insatser avses bedrivas enligt Socialtjänstlagen och/eller Lagen om stöd och service till vissa funktionshindrade och får inte obehörigen röja vad därvid erfarit om enskilds personliga förhållanden.

Inom den kommunala myndigheten ska samtliga som kommer i kontakt med känsliga uppgifter eller personuppgifter ha skrivit på ett särskilt sekretessavtal, vilket binder dem att inte sprida denna typ av uppgifter vidare eller att på annat sätt missbruka information som de i sitt arbete kommer i kontakt med.

Lagringsytor som rekommenderas

Verksamhetssystem
Information ska företrädesvis lagras i verksamhetssystem. Om verksamhetssystem saknas eller det av annan anledning inte är motiverat, så kan information lagras på andra strukturerade sätt.

Diariet
Diarium är en form av register som används för att hålla ordning på kommunens allmänna handlingar. I kommunen är varje nämnd en egen myndighet med ett eget diarium. Syftet med diarieföring är att skapa ordning och struktur samt göra sekretessreglerade uppgifter ”synliga” och sökbara. Handlingar kan också hållas ordnade på annat vis om kraven på återsökning och kontroll uppfylls.

I diariet finns mycket av den kommunikation som har varit med myndigheter och aktörer inom verksamhetsområdet. Exempel på handlingar som ska diarieföras:

- Beslut, tjänsteskrivelser, tjänsteanteckningar, rapporter och sammanställningar av statistik
- Inkommande skrivelser som kan föranleda beslut, yttrande eller förslag
- Utgående skrivelser (till exempel anmälan, remisser och yttranden)
- Avtal och kontrakt samt kommunikation kring dessa
- Avvikelser, Lex Sarah, lex Maria, synpunkter och klagomål

Hemsidan
Publik information av allmänt intresse som aktivt ska publiceras/delges allmänheten läggs upp på hemsidan. Exempel på handlingar är politiskt antagna styrdokument, verksamhetsbeskrivningar och kontaktuppgifter.

Microsoft SharePoint
SharePoint är den gemensamma lagringsyta som alla medarbetare har tillgång till. Lagringen är molnbaserad vilket gör informationen tillgänglig även utanför kommunens nätverk, om du är ansluten till internet. I SharePoint ska dokument så långt som möjligt sparas synligt för andra medarbetare för att förenkla samarbete, kompetens- och informationsöverföring.
Melleruds kommun har en riktlinje för styrande dokument. Denna riktlinje beskriver vilka styrande dokumenttyper kommunen använder och på vilken nivå dessa ska fastställas/antas. Alla av nämnden eller förvaltningen fastställda styrande dokument läggs på SharePoint.

Exempel på sådana styrande dokument är riktlinjer fastställda av nämnd och rutiner antagna på ledningsgruppnivå. Alla rutiner ska fastställas på ledningsnivå eller av ansvarig chef. Rutiner som rör hela förvaltningen eller fler än ett verksamhetsområde antas i förvaltningsledningsgruppen, rutiner som rör flera enheter men bara ett verksamhetsområde antas av verksamhetsområdets ledningsgrupp och rutiner som bara rör en enhet antas av enhetschef och förankras på APT. När en rutin är antagen av ledningsgrupp och/eller chef ska den publiceras på SharePoint. Senast uppdaterade och därmed gällande rutiner ska således alltid finnas på SharePoint.

Microsoft Teams
Teams är en digital plattform för samarbete och gemensam lagringsyta. Löpande arbetsmaterial och gemensamma arbetsdokument läggs på teams. I Teams kan du enkelt hålla reda på kommunikation, filer, anteckningar, planering och annat innehåll som projektet eller den samarbetande gruppen behöver. Lagringen är molnbaserad vilket gör informationen tillgänglig även utanför kommunens nätverk, om du är ansluten till internet.

NOTERA! Uppgifter och dokument som omfattas av sekretess, personuppgifter som är extra skyddsvärda samt känsliga personuppgifter får inte lagras i SharePoint eller Teams.

Lagringsytor för användning i begränsad omfattning

Microsoft OneDrive
OneDrive är en personlig lagringsplats för alla medarbetare. Lagringen är molnbaserad vilket gör informationen tillgänglig även utanför kommunens nätverk, om du är ansluten till internet. Informationslagring ska vara öppen för andra medarbetare så långt det är möjligt. Du ska därför vara restriktiv med att lagra information som bara är tillgänglig för dig. OneDrive ska ses som en tillfällig lagringsyta eller för lagring av information som endast är till nytta för dig. När du slutar din tjänst raderas innehållet i din OneDrive vilket är ytterligare en anledning att undvika att spara verksamhetsviktig information där.

Lagringsytor som ska undvikas

Du ska undvika att lagra information på följande lagringsytor:

- Lokalt på din dator (C:)
- Lokalt på din mobiltelefon/läsplatta.
- Minneskort, USB-minnen, externa hårddiskar eller liknande.
- I grupper på intranätet
- I e-postsystem
- I externa molnlagringstjänster

Dessa lagringsytor kan utgöra en säkerhetsrisk med svårighet att ha kontroll på informationen, om den lagras tillförlitligt utifrån lagar och rekommendationer. Dessa lagringsytor saknar också backup-rutiner och informationen kan vara svår att återskapa/söka fram om det skulle behövas.

Gemensam filserver (R:)
Verksamhetssystem och SharePoint ersätter den gemensamma filservern som därav är under avveckling. Således ska lagring av ny information/dokument undvikas.

Lagra privat information

Du får i begränsad omfattning lagra privat information. Denna information får inte vara olaglig eller av sådan art att den kan betraktas som oseriös eller anstötlig och får heller inte leda till försämrad funktion hos utrustningen. Även den privata informationen omfattas av offentlighetsprincipen och kan komma att begäras ut om den är lagrad på kommunens utrustning.